Uniwersytet Warszawski

Wydział Prawa i Administracji

Instytut Prawa Międzynarodowego

Tomasz Welanyk

Istnienie i granice suwerenności w cyberprzestrzeni. Analiza prawna

Praca doktorska

Promotor: dr hab. Paweł Czubik, prof. UEK

Promotor pomocniczy: dr Paweł Filipek

Warszawa, 2019

WYKAZ TERMINÓW UŻYTYCH W ROZPRAWIE

ACM - *Association for Computer Machinery*, międzynarodowe stowarzyszenie naukowców i specjalistów z zakresu informatyki. Polskim oddziałem ACM jest Stowarzyszenie dla Maszyn Liczących.

ARSIWA- *Draft Articles on Responsibility of States for Internationally Wrongful Acts*

BotNet- zespół komputerów, których część mocy obliczeniowej została w sposób nielegalny przekierowana do celów sprawcy narusznia integralności ich systemów.

CCDCoE - *Cooperative Cyber Defense Center of Excellence* - Centrum obrony Cybernetycznej NATO, znajdujące się w Tallinnie.

CIO- *Chief Information Officer*, określenie kierowników zespołów zarządzających informacją w rozmaitych instytucjach.

CNE - *Computer Network Exploitation,* grupa operacji cybernetycznych mających na celu naruszenie integralności sieci

CRADA- *Cooperative Research and Development Agreement,* forma partnerstwa publiczno-prawnego znanego prawu USA, dotycząca projektów naukowych i prowadzonych w ramach nowych technologii.

CSIRT- *Computer Security Incident Response Team*- wyspecjalizowane zespoły przeciwdziałające naruszeniom sieci określonego podmiotu.

DDoS-*Distributed Denial of Service*, rodzaj ataku cybernetycznego polegającego na intencjonalnym przeciążeniu serwerów, na których oparta jest witryna cyberprzestrzenna stanowiąca cel ataku i w konsekwencji uniemożliwienie dostępu do niej.

DNS- *Domain Name System*, system przypisywanie adresów do elementów cyberprzestrzeni.

DPI- *Deep Packet Inspection*- metoda lokalizacji adresatów pakietów danych przesyłanych w cyberprzestrzeni.

DRM- *Digital Rights Management,*technologia pozwalająca na ograniczenia dostępności treści cyfrowych do zakresów faktycznie wynikających z umowy.

ENISA- *European Union Agency for Network and Information Security*, Agencja bezpieczeństwa cyberprzetrzennego Unii Europejskiej

EPAG- niemiecka spółka córka ICANN

HUMINT- *Human Intelligence*, wywiad oparty o źródła ludzkie

IANA-*Internet Assigned Number Authority*, poprzednik ICANN

ICANN - *The Internet Corporation for Assigned Names and Number*, instytucja kontrolująca protokół DNS/IP i przyznająca numery IP witryn cyberprzestrzennym.

ICRC/ MKCzK- *International Committee of Red Cross/ Międzynarodowy Komitet Czerwonego Krzyża*

IFCN - *International Fact-Checking Network* organizacja dziennikarska weryfikująca treści publikowane w mediach społecznościowych

IGoE- *International Group of Experts,* Międzynarodowa grupa ekspertów prawa cyberprzestrzeni związanych z CCDCoE, autorzy Tallinn Manual

ILC - *International Law Commission*, Komisja Prawa Międzynarodowego ONZ

IP-*Internet Protocol*, numer identyfikujący określoną witrynę internetową

ISP- *Internet Service Provider (s),* podmioty utrzymujące transfer w cyberprzestrzeni, pośredniczące pomiędzy dwoma użytkownikami cyberprzestrzeni.

ISR- *Intelligence, Surveillance, Recon,* akronim określający operacje wywiadowcze w cyberprzestrzeni.

MTS- Międzynardowy Trybunał Sprawiedliwości

NSA- *National Surveillance Agency* - amerykańska agencja bezpieczeństwa cybernetycznego

OSINT- *Open Source Intelligence*, działania wywiadowcze prowadzone jawnymi i legalnymi środkami, tzw. biały wywiad

SIGINT- *Signal Intelligence*, wywiad elektroniczny

TM/TM 2.0- *Tallin Manual/Tallinn Manual 2.0*

UAV -*Unmanned Aerial Vechicle ,* dron latający

UMS -*Unmanned Maritime System ,* dron morski

UNIDIR-*United Nations Institute for Disarmament Research*, agenda Narodów Zjednoczonych działająca na rzecz światowego pokoju.

UUV - *Unmanned Underwater Vehicle ,* dron podwodny

VPN- *Virtual Private Network,* sieci prywatne, mające możliwość częściowego ograniczenia dostępu z całości cyberprzestrzeni

WHOIS (informatyczny), katalog numerów IP

WIPO- *World Intellectual Property Organization* Światowa Organizacji Własności Intelektualnej

Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.

John Barlow

People of the Cyber World, you light speed stream of ones and zeros. I come from the Real World, the home of the state. On behalf of the present, I demand you follow our rules or you will not be welcome here. We have absolute sovereignty wherever you gather.

Patrick W. Franzese

Wstęp

W ciągu 50 lat, jakie upłynęły od momentu powstania pierwszej globalnej sieci komputerowej *ARPANET* cyberprzestrzeń stała się obecna we nieomal wszystkich aspektach ludzkich działań, zyskując znaczący wpływ na funkcjonowanie państw - a w konsekwencji na prawo narodów. Rozpowszechnienie technologii sieciowych a także liczne ułatwienia przez nie tworzone spowodowały, że w czasach nam współczesnych cyberprzestrzeń staje się kolejnym polem, na którym prowadzą działania podmioty prawa międzynarodowego. Podmioty te muszą wykonywać i chronić swoje interesy w cyberprzestrzeni analogicznie, jak czynią to w świecie rzeczywistym. Charakterystyczną cechą cyberprzestrzeni jest jej uzależnienie od technologii, której rozwój stał się bezprecedensowo szybki. W konsekwencji prawo międzynarodowe nie nadąża z normowaniem, w tym z redefinicją norm leżących u podstaw tego prawa, takich jak suwerenność i jurysdykcja.[1] Podstawowym problemem badawczym podejmowanym przez niniejszą rozprawę jest więc kwestia istnienia suwerenności państwowej w cyberprzestrzeni a także możliwości wykonywania w niej jurysdykcji państwowej, która stanowi tej suwerenności odbicie i konieczny warunek istnienia.

Rozwiązanie tego problemu wymaga zbadania dwóch kwestii. Pierwszą z nich jest analiza, czym w istocie jest cyberprzestrzeń, zarówno z punktu widzenia prawnego jak i faktycznego. Drugą jest rozważenie sposobu normowania cyberprzestrzeni, a także analiza tworzącego się dopiero systemu *lex informatica*. Łączy on normy prawa stanowionego, zwyczajowego i elementy technicznej konstrukcji

[1] Doskonale sytuację tą obrazuje tzw. Prawo Moore'a, sformułowane przez Gordona Moore'a, twórcę koncernu Intel. Według jego obserwacji moc obliczeniowa komputerów ulega podwojeniu w ciągu 18 miesięcy. Od czasu sformułowania tego prawa okres ten uległ wydłużeniu do około 24 miesięcy, jednak z punktu widzenia prawa jest to różnica nieistotna. Okres tworzenia się stabilnych norm prawa międzynarodowego jest bowiem o wiele dłuższy. zob. Moore G.E. *Cramming more components onto integrated circuits*, Electronics Magazine 38:8,(1965)s.1.

cyberprzestrzeni - faktycznie ją normujące. Analiza ta ma znaczenie fundamentalne, ponieważ funkcjonowanie w cyberprzestrzeni jest we współczesnych czasach warunkiem koniecznym realizacji i obrony interesów państwowych (także tych w świecie fizycznym) a więc tego, co stanowi podstawową treść jurysdykcji i suwerenności. Czysto teoretycznie można sobie wyobrazić państwo, które odcina się od cyberprzestrzeni a w związku z tym unika zagrożeń z nią związanych. W praktyce jednak takie działanie jest nie do wyobrażenia. Po pierwsze, nawet odłączenie danego państwa od cyberprzestrzeni, rozumianej jako połączenie ze światową siecią komputerową nie prowadzi do uniknięcia wszystkich zagrożeń dla suwerenności z cyberprzestrzenią związanych. Celem ataku cybernetycznego może być bowiem może być dowolny system elektroniczny. Po drugie, państwo odłączone od cyberprzestrzeni wyłączałoby się ze zdecydowanej większości obrotu towarów i usług, a straty ekonomiczne i technologiczne takiego państwa byłyby tak znaczne, że wielokrotnie przewyższyłyby ewentualne zyski wynikające z ułatwienia obrony przed cybernetycznymi naruszeniami suwerenności. W praktyce więc ochrona suwerenności poprzez odłączenie się od cyberprzestrzeni nie jest możliwa.

Wobec tej konstatacji należy z prawnego punktu widzenia wyjaśnić, czy mowa tu wyłącznie o tradycyjnie pojmowanej suwerenności, która zyskuje nowe pola do jej wykonywania i konieczności ochrony, czy też sam fakt istnienia cyberprzestrzeni redefiniuje czy nawet likwiduje suwerenność państwową w pewnych zakresach. Trudno wskazać jakiekolwiek cechy suwerenności państwowej istniejące zupełnie niezależnie od cyberprzestrzeni - dowolna dziedzina życia, nawet tradycyjnie oderwana od rzeczywistości wirtualnej, może podlegać jej wpływom, pośrednim lub bezpośrednim; wydaje się więc, że ochrona interesów państwowych w cyberprzestrzeni wymaga redefinicji samego pojęcia suwerenności (a co za tym idzie, pojęcia jurysdykcji) w sposób, który umożliwiłby zachowanie jego istoty prawnej w zupełnie nowej rzeczywistości faktycznej. Jednakże w innych zakresach suwerenność ta będzie funkcjonowała w sposób znany z innych dziedzin prawa, a fakt, że pewne zdarzenia prawne będą miały swoje źródło w cyberprzestrzeni, będzie mniej istotny. Taka sytuacja ma miejsce w przypadku ataków cybernetycznych, mających

skutek kinetyczny (a więc w świecie rzeczywistym), do których będą stosować się normy prawa konfliktów zbrojnych. Suwerenność w cyberprzestrzeni będzie więc funkcją norm tradycyjnego prawa międzynarodowego i nowych, dopiero powstających norm prawa cyberprzestrzeni. Działać one będą w zupełnie nowej rzeczywistości prawnej, jaką jest cyberprzestrzeń z jej cechami wszechobecności, anonimowości i braku możliwości fizycznej lokalizacji.

Kolejną, istotną dla odpowiedzi na przedmiotowe pytanie kwestią, jest wskazanie możliwości obrony własnych interesów przez państwa oraz odpowiedź na pytanie do jakiego stopnia państwo może ingerować w cyberprzestrzeń wykonując swoje tradycyjne prerogatywy. Pojawia się więc pytanie: czy istnieje suwerenność (a co za tym idzie jurysdykcja) *stricte* cyberprzestrzenna. Rozstrzygnięcie tego problemu wymaga jednak udzielenia odpowiedzi na pytanie o definicję prawnomiędzynarodową cyberprzestrzeni. Jeżeli przyjmiemy, że państwo ma możliwość i prawo działania w cyberprzestrzeni, konieczne staje się z kolei znalezienie metody delimitacji granic i sposobu rozwiązywania konfliktów interesów aktorów państwowych. Należy rozstrzygnąć, jak przebiegają granice w cyberprzestrzeni, zarówno w jej warstwie technicznej jak i w tej opartej o przepływ danych. Oczywiście granice te mogą być naruszane. Omówione więc zostaną w rozprawie niniejszej zarówno zagadnienia konfliktu cyberprzestrzennego oraz naruszeń suwerenności w cyberprzestrzeni poniżej poziomu użycia siły, jak i remediów pozwalających podmiotom prawa międzynarodowego na ochronę własnych interesów.

Rozdział pierwszy pracy poświęcony został omówieniu pojęć istotnych dla postawionego w niej pytania badawczego. Jest on przede wszystkim próbą odpowiedzi na pytanie czym jest cyberprzestrzeń zarówno w sensie prawnym jak i faktycznym. Przytoczone zostaną definicje i ujęcia cyberprzestrzeni przyjmowane przez państwa w swoich wewnętrznych aktach prawnych, a także definicje wypracowane przez doktrynę prawa międzynarodowego, ze szczególnym uwzględnieniem Międzynarodowej Grupy Ekspertów NATO, autorów tzw. *Tallinn Manual*. Jest on w aktualnym stanie badań uznawany za najważniejszą próbę kompilacji praktyki międzynarodowej i poglądów doktryny w zakresie prawa

cyberprzestrzeni. Pozwoli to odpowiedzieć na pytanie: jakie elementy składają się na cyberprzestrzeń i umożliwiają jej funkcjonowanie. Następnie omówione zostaną techniczne zagadnienia cyberprzestrzeni. Po pierwsze - podział cyberprzestrzeni na część informatyczną (a więc zbiór danych istniejący wyłącznie jako zapis cyfrowy) i fizyczną - zbiór fizycznie istniejących urządzeń służących do przetwarzania danych stanowiących część informatyczną. Po drugie - opisane w literaturze informatycznej cechy cyberprzestrzeni: wynikająca z niej anonimowość, niemożliwość jej fizycznego zlokalizowania i wszechobecność. Wszystkie te cechy mają daleko idące konsekwencje prawne, szczególnie dla suwerenności państwowej i jurysdykcji, a także samego prawa cyberprzestrzeni. Ich rozważanie staje się początkiem dyskusji nad kwestią uznania cyberprzestrzeni za kolejne dobro wspólne ludzkości. Druga część rozdziału zawiera rozważania nad możliwością wykonywania przez państwa własnej jurysdykcji w odniesieniu do cyberprzestrzeni, stanowiąc także próbę praktycznego i faktycznego zdefiniowania narzędzi, które owo wykonywanie umożliwiają.

Rozdział drugi poświęcony został powstającemu dopiero systemowi prawa cyberprzestrzeni. Zawiera on omówienie istotnych dla znaczenia suwerenności zasad prawnych obecnych w prawie międzynarodowym publicznym, wraz z próbą analizy w jakim zakresie stosują się owe zasady do cyberprzestrzeni. Źródłem tego prawa jest głównie praktyka międzynarodowa i tzw. normowanie faktyczne, rozumiane jako tworzenie norm mających charakter prawny, regulujących jednak nie tyle kwestie dozwoleń czy zakazów, ale raczej zachowań (możliwych lub niemożliwych), wynikających z samej architektury cyberprzestrzeni. Następnie omówiony zostanie omówiony wpływ norm *lex informatica* na tradycyjne prawo narodów a także normy istniejące na styku obydwu tych porządków prawnych, ze szczególnym uwzględnieniem tzw. metanorm, czyli norm wynikłych z wzajemnego wpływu norm *lex informatica* i prawa tradycyjnego.

Rozdział trzeci poświęcony jest suwerenności państwowej i wpływowi, jaki zjawiska opisane w dwóch pierwszych częściach rozprawy wywierają na ową instytucję. Przede wszystkim stanowi on próbę przeanalizowania możliwości istnienia

suwerenności państwowej w informatycznej części cyberprzestrzeni; jest więc próbą udzielenia odpowiedzi na pytanie, czy możliwa jest swoista "terytorializacja" cyberprzestrzeni. Po drugie, rozpatrzony zostanie wpływ cyberprzestrzeni na tradycyjnie pojmowaną suwerenność państw, istniejącą w świecie fizycznym. Omówione zostaną także najczęstsze rodzaje cyberoperacji nie stanowiących ataku wraz z dostępnymi państwom remediami, zarówno wynikającymi z tradycyjnego systemu *ius gentium*, jak i mającymi swoje źródło w *lex informatica*.

Rozdział czwarty poświęcony jest wojnie cyberprzestrzennej, a także wszystkim naruszeniom suwerenności, których skutki osiągają poziom przekraczający próg użycia siły w rozumieniu wynikającym z praktyki Organizacji Narodów Zjednoczonych. Zostaną w nim omówione instytucje tradycyjnego prawa konfliktów zbrojnych i ich odpowiednie stosowanie do prawa konfliktu cyberprzestrzennego. Analizie poddane zostaną metody wartościowania skutków ataków cyberprzestrzennych. Ze względu na specyfikę działań cyberprzestrzennych, odnoszących skutek w świecie fizycznym tylko pośrednio, konieczne okazuje się skonstruowanie czytelnej metody określania czy dane zachowanie jest cyberatakiem i przypisanie mu skutków w wywołanych w świecie fizycznym, a także pozwalającej na określenie skutków w świecie fizycznym pozostających w bezpośrednim związku z tym atakiem. Przywołany i szczegółowo omówiony zostanie więc test, skonstruowany przez kierownika Międzynarodowej Grupy Ekspertów, prof. Michaela Schmitta. Ostatnia część rozdziału poświęcona została kwestii legalności odpowiedzi kinetycznych na ataki w cyberprzestrzeni - zarówno jako środków odwetowych jak i możliwości przeprowadzenia ewentualnego uderzenia prewencyjnego.

Rozdział piąty opisuje zjawisko *cyberlawfare* a więc *lawfare* w cyberprzestrzeni. To ostatnie pojęcie oznacza opisanie przez doktrynę metody stosowania prawa międzynarodowego do prowadzenia konfliktów, a więc wykorzystywania ogólnie obowiązujących norm prawa międzynarodowego do wymuszenia określonego zachowania lub zaniechania po stronie przeciwnika konfliktu. Ze względu na konkretyzację norm *lex informatica* w ramach tzw. normowania faktycznego, znaczenie prawa w planowaniu działań zarówno mających na celu naruszenie jak

i obronę suwerenności znacząco wzrasta. Odpowiednia konstrukcja własnego prawa krajowego może bowiem pozwolić danemu państwu na skuteczną obronę przed zewnętrznymi naruszeniami własnej suwerenności, właśnie dzięki normowaniu faktycznemu. Zjawisko *cyberlawfare* musi więc być brane pod uwagę przy kształtowaniu własnych polityk prawnych dotyczących cyberprzestrzeni przez poszczególne państwa.

Podstawową metodą badawczą przyjętą w pracy niniejszej jest analiza praktyki międzynarodowej w zakresie cyberprzestrzeni. Podejmuje więc ona także próbę odpowiedzi na pytanie, czy istnieje prawo do wojny elektronicznej i prawo wojny elektronicznej, odzwierciedlające odpowiednio *ius ad bellum* i *ius in bello*, a także jak należy traktować operacje cybernetyczne nie stanowiące ataku w rozumieniu prawa międzynarodowego. Jest bowiem oczywistością, że jeżeli suwerenność może być łatwo i bez konsekwencji naruszana, to przestaje ona mieć znaczenie prawne i w praktyce oznacza niemożność wykonywania jurysdykcji. Oznaczałoby to, że przestaje ona istnieć.

Należy także pamiętać, że w cyberprzestrzeni mamy do czynienia z bezprecedensowym rozszerzeniem zbioru podmiotów, uczestniczących w obrocie prawnomiędzynarodowym. Przede wszystkim dochodzi do faktycznego zrównania potencjału aktorów niepaństwowych z wieloma innymi aktorami tradycyjnego obrotu. W przypadku działań kinetycznych czy też objętych zasadniczo tradycyjnymi dziedzinami prawa międzynarodowego, kategoria *non-state actors* zakłada istnienie grup działających poza jurysdykcją państw, ale na ich terytoriach. Nie istnieją bowiem terytoria nie podlegające jurysdykcji jakiegoś państwa, organizacji międzynarodowej lub społeczności międzynarodowej jako takiej. W przypadku cyberprzestrzeni natomiast możliwa jest pełna ‘niepaństwowość’, wliczając w to stworzenie własnej quasi-jurysdykcji, służącej do przeprowadzania operacji cybernetycznych. Niezwykle istotnym problemem, powiązanym z przytoczonymi wyżej problemami jurysdykcyjnymi, jest także kwestia atrybucji w cyberprzestrzeni. Zastosowanie podstawowego narzędzia do obrony suwerenności, jakim jest celowana odpowiedź na naruszenie lub uderzenie prewencyjne, wymaga bowiem

zidentyfikowania tego, który tę suwerenność naruszył. Brak możliwości dokonania atrybucji w praktyce wyłącza a przynajmniej istotnie ogranicza możliwość obrony własnej suwerenności. Wielu teoretyków prawa międzynarodowego zupełnie ignoruje tę kwestię, wskazując wyłącznie, że techniczne trudności w dokonaniu atrybucji nie mogą wyłączać prawa państw do obrony. Koncentrują się oni na znalezieniu metod wyłącznie technicznego dostosowania istniejącego prawa dotyczącego konfliktów, suwerenności i jurysdykcji do realiów panujących w cyberprzestrzeni.[2] Takie stanowisko jest niezrozumiałe, ponieważ zakłada, że prawo może funkcjonować zupełnie w oderwaniu od rzeczywistości, którą miałoby normować. Coraz większa część doktryny jednak wskazuje, że prawo konfliktów ulega zmianie, normowanie wyłącznie samego prawa wojny i do wojny przestaje wystarczać, a prawo nie jest już wyłącznie środkiem normowania zachowań stron walczących, ale też samo staje się bronią i środkiem prowadzenia konfliktu. Doktryna określa mianem to mianem *lawfare*, czyli zjawiskiem militaryzacji prawa.[3] W cyberprzestrzeni *lawfare* staje się wręcz istotą prowadzenia konfliktów, ze względu na fakt, że normowanie prawne definiuje posiadane przez beligerentów możliwości ataku, odpowiedzi na ten atak, a także ich cele. Samo w sobie staje się *sui generis* polem walki współczesnej zimnej wojny - w ramach zjawiska *cyberlawfare*. Wynika to oczywiście, z przywołanego wyżej normowania faktycznego. Normy *lex informatica* nie pełnią wyłącznie roli regulującej prawne aspekty cyberprzestrzeni, ale także jej faktyczne możliwości. W efekcie militaryzacja *lex informatica - cyberlawfare* tworzy zjawisko swoistego metakonfliktu, w którym za pomocą jurysdykcji można nie tylko tworzyć ramy prawne prowadzenia wojny, ale wręcz ustalać jakie środki będą mogły być w nim podjęte przez belligerentów. To oczywiście oznacza, że cyberprzestrzenna

[2] Takie stanowisko przyjmuje przykładowo NATO. Sojusz Północnoatlantycki, uznając cyberprzestrzeń za nowe, niezmiernie istotne pole konfliktu zlecił Międzynarodowej Grupie Ekspertów (*International Group of Experts*, [IGoE]) związanych z Centrum Obrony Cybernetycznej Sojuszu (*Cooperative Cyber Defence Center of Excellence* [CCD CoE] w Tallinnie dokonanie opracowania prawnego tej kwestii. zob. Schmitt M.N. *Tallinn Manual on the international law applicable to cyber warfare*, CCD CoE, Oxford University Press (2013) także Schmitt M.N., Vihul L. *Tallinn Manual 2.0 on the International Law Applicable to Cyberoperations* CCD CoE (2017) Dalej powoływane jako TM i TM 2.0

[3] zob. Rozdział pracy niniejszej poświęcony zjawisku *lawfare*

suwerenność nie jest wyłącznie dobrem, które państwa muszą chronić, ale jest też narzędziem tej ochrony. Wobec tej konstatacji nie sposób nie zauważyć, że pogląd, według którego cyberprzestrzeń to po prostu kolejny etap rozwoju technologii, a jedynym problemem jest stworzenie odpowiedniego *opinio iuris* i wypracowanie orzecznictwa, dostosowującego już istniejące normy do cyberprzestrzeni - jest poglądem chybionym. Nie oznacza to oczywiście, że cyberprzestrzeń nie stanowi elementu zakresu przedmiotowego prawa międzynarodowego publicznego - natomiast niewątpliwie będzie stanowić coś więcej niż jego nową dziedzinę.

Rozprawa niniejsza jest więc w pierwszym rzędzie próbą odpowiedzi na pytanie, czy wraz z rozwojem prawa cyberprzestrzeni zachowanie jurysdykcji (a co za tym idzie suwerenności) przez tradycyjnie pojmowane państwa jest możliwe i jakimi środkami państwa mogą tą suwerenność zachować. Oczywiście konieczne jest wskazanie prawnych podstaw tej nowej suwerenności. To z kolei wymaga powstania całego systemu cybernetycznego prawa narodów, niezwykle trudnego do stworzenia ze względu na brak źródeł tego prawa. Nie istnieje bowiem żaden organ, który byłby właściwy do kodyfikacji takiego prawa (a nie jest jasne czy w ogóle byłoby to technicznie możliwe), Prawo zwyczajowe nie istnieje w tym zakresie ze względu na brak powtarzalności stanów prawnych a traktaty międzynarodowe dotyczące cyberprzestrzeni są nieliczne i zazwyczaj dotyczą precyzyjnie określonych kwestii szczególnych. Z tego względu poszukiwanie dla tego zakresu normowania analogii w prawie już ustalonym, jakkolwiek naturalne i słuszne, może odbywać się wyłącznie w ograniczonym zakresie. Dotyczyć on może głównie norm programowych i generalnych, z wyjątkiem przypadku wspomnianych już ataków o efektach kinetycznych, gdzie niewątpliwie możliwe jest stosowanie bezpośrednie norm prawa konfliktów zbrojnych. Jednakże w wypadku tak daleko idących różnic w stanach faktycznych, które normowaniu mają podlegać, nawet we wspominanych, niewielkich zakresach zgodności przedmiotowej można taką analogię uznać wyłącznie za początek tworzenia prawa. Analogie te będą bowiem musiały uwzględniać specyfikę prawa cyberprzestrzeni a podlegać interpretacji w świetle *lex informatica*. Łatwo zauważyć, że za najczęściej przywoływane elementy prawa międzynarodowego,

stanowiące podstawę do konstruowania prawa cyberprzestrzeni przyjmuje się prawo morza i budowane na jego podstawie prawo lotnicze, a później prawo przestrzeni kosmicznej. Prawo lotnicze w wielu aspektach tworzono poprzez inkorporację norm prawa morza, z niewielkimi poprawkami uwzględniającymi techniczne różnice pomiędzy jednostkami latającymi a pływającymi. Stanowią więc one pewną logiczną całość z prawem morza. Z punktu widzenia prawa cyberprzestrzeni, której wspomniane różnice nie dotyczą, stanowią więc gotowy wzór postępowania z globalną przestrzenią wspólną, którą bez wątpienia cyberprzestrzeń jest. W oczywisty sposób wynika to z próby potraktowania cyberprzestrzeni, jako swoistego "morza otwartego".

Ze względu jednak na opisane w rozprawie niniejszej cechy cyberprzestrzeni, ze szczególnym uwzględnieniem niemożliwości jej fizycznego zlokalizowania a także jej wszechobecności, analogia ta nie może dać w pełni pożądanych skutków. Stało się bowiem dla doktryny oczywiste, że dla rozważenia suwerenności w cyberprzestrzeni konieczne jest rozstrzygnięcie czy (1) cyberprzestrzeń można uznać za suwerenną (w zakresie normowania) i (2) czy istnieje *sui generis* prawo cyberprzestrzeni. Pierwsza z tych kwestii została rozstrzygnięta negatywnie, co zostanie szerzej omówione w dalszej części wywodu. Rozwiązaniem kwestii swoistego prawa cyberprzestrzeni stało się ukonsytuowanie tzw. *lex informatica,* konstruowanego w sposób podobny do konstrukcji dawnego i współczesnego *lex mercatoria*. Oznacza to, że państwa muszą niejako przetransponować własną suwerenność oraz jurysdykcję do zupełnie nowego systemu prawnego jakim jest *lex informatica* i wykorzystać narzędzia możliwe w tym systemie prawnym. Nie ulega wątpliwości, że samo istnienie cyberprzestrzeni ogranicza pośrednio także stopień kontroli państw nad prawem prywatnym międzynarodowym. Ponieważ nie jest celem niniejszej pracy badanie skutków istnienia cyberprzestrzeni dla prawa prywatnego, ten problem zostanie omówiony wyłącznie w zakresie, w którym styka on się z problemem jurysdykcji i zakres tradycyjnie pozostawał pod kontrolą *imperium* państwowego.

W zakresie zainteresowania niniejszej rozprawy pozostaje także kwestia tworzenia mikropaństw i wykorzystywania miejsc o statusie *terra nullius* czy

o nierozstrzygniętym statusie jurysdykcyjnym, a także problem ewentualnego zastosowania tak stworzonych podmiotów prawa międzynarodowego do prowadzenia *cyberlawfare* w cyberprzestrzeni. Dotychczas bowiem ewentualne stworzenie takiego podmiotu (pomijając wszystkie zastrzeżenia co do jego legalności, ważności deklaracji niepodległości czy kwestii spełnienia kryteriów państwowości), prowadziło raczej do powstania egzotycznego konstruktu, pozostającego głównie w orbicie zainteresowań prawników, bez realnego wpływu na obrót międzynarodowoprawny. Ta kwestia uległa także zmianie w wyniku powstania cyberprzestrzeni. Sieciowość cyberprzestrzeni, umożliwiająca wpływanie na dowolny punkt na świecie, w czasie rzeczywistym i w przy dużo mniejszych wymogach technicznych w zakresie środków wymaganych do przeprowadzenia skutecznego naruszenia suwerenności, spowodowała, że terytoria takie stają się istotnymi elementami architektury *cyberlawfare*. Łatwo zauważyć, że z tego powodu, cyberprzestrzeń znacząco osłabia związki suwerenności z terytorium państwowym. Tymczasem zasadnicza część aktualnego stanu prawnego kwestię wykonywania jurysdykcji i samą suwerenność mocno wiąże z postwestfalską zasadą terytorialności. Identycznie jak z mikropaństwami, sprawa ma się z podmiotami z kategorii *non-state actors.* Płynący z tych obserwacji oczywisty wniosek - znaczące rozszerzenie katalogu uczestników obrotu międzynarodowoprawnego, gdzie na równi z tradycyjnymi podmiotami prawa międzynarodowego działają aktorzy niepaństwowi czy grupy o nieokreślonym jeszcze w dzisiejszym stanie prawnym statusie, tworzy pytanie o to jak właściwie należy definiować społeczność międzynarodową w cyberprzestrzeni? Czy należy przyjąć, że istnieją dwie społeczności: cyfrowa i fizyczna, czy też zakładamy, że zbiór podmiotów międzynarodowych jest zbiorem łączącym obydwie te społeczności i niektóre elementy obydwu tych zbiorów są po prostu wspólne? Koncepcja dwóch równoległych porządków oczywiście nie może zostać utrzymana, choćby ze względu na możliwość przeprowadzania ataku cyberprzestrzennego o skutkach kinetycznych, a więc wpływających zarówno na świat fizyczny jak i na cyberprzestrzeń. Skoro więc cyberprzestrzeń interpretujemy jako kolejną dziedzinę wykonywania obrotu prawnomiędzynarodowego przez jego uczestników, konieczne staje się określenie

zasad, pozwalających przypisywać znaczenia prawne wspomnianym wcześniej różnicom pomiędzy tradycyjnymi zakresami prawa międzynarodowego a cyberprzestrzenią i normami faktycznymi. Zasady te leżą u podstaw *lex informatica*, z wykorzystaniem własnej jurysdykcji zwyczajnej, których z kolei *non-state actors* ze swej natury są pozbawieni.

Rozprawa niniejsza jest więc próbą zrozumienia konstrukcji prawa cyberprzestrzeni i jego norm, decydujących o sposobie ochrony interesów aktorów prawa międzynarodowego, ze szczególnym uwzględnieniem norm odpowiadających tradycyjnie pojmowanej jurysdykcji i suwerenności. Pozwoli to na udzielenie odpowiedzi na postawione w niej pytanie badawcze, zarówno o istnienie i znaczenie suwerenności *stricte* cyberprzestrzennej jak i o jej korelację z suwerennością pojmowaną tradycyjnie. Analizie poddany więc zostanie sposób konstrukcji suwerenności cyberprzestrzennej i tworzenia *sui generis* 'terytoriów' cyfrowych elementów cyberprzestrzeni, poddanych wyłącznie jurysdykcji jednego z państw, choć ciągle stanowiących część cyberprzestrzeni. Pierwszym pośrednim celem badawczym rozprawy musi więc być podjęcie próby zrozumienia prawa cyberprzestrzeni; zarówno natywnego dla niej *lex informatica* jak i norm mających swoje źródło w tradycyjnym prawie międzynarodowym, a stosowanych do cyberprzestrzeni. Pozwoli to na umiejscowienie suwerenności cybernetycznej we właściwym kontekście prawnym, a także na zrozumienie jej specyfiki. Drugim z tych celów jest natomiast opisanie możliwych naruszeń suwerenności w cyberprzestrzeni lub za jej pomocą – a także narzędzi, za których pomocą suwerenność ta może być chroniona, a jurysdykcja państwowa wykonywana.

Punktem wyjścia i podstawowym środkiem prowadzenia naszkicowanych powyżej rozważań musi być obserwacja praktyki państw dotyczącej cyberprzestrzeni. Ze względu na specyfikę opartego o *lex informatica* systemu prawa cyberprzestrzeni, ma ona podstawowe znaczenia dla określenia sposobu jej normowania. *Opinio iuris* będzie bowiem istotne wyłącznie w zakresie norm prawa międzynarodowego wpływających na cyberprzestrzeń oraz metanorm, wpływających zarówno na *lex informatica* jak i na prawo międzynarodowe. W aktualnym stanie prawnym brak jest

bowiem znaczących traktatów czy kodyfikacji dotyczących *stricte* prawa cyberprzestrzeni. Natomiast normy prawa międzynarodowego stosowane odpowiednio lub w drodze analogii do prawa cyberprzestrzeni mają ograniczony zakres przedmiotowy. Brak także wypracowanych mechanizmów interpretacyjnych tych norm, które uwzględniałyby specyfikę cyberprzestrzeni. Prawo regulujące cyberprzestrzeń jest sumą prawa międzynarodowego publicznego, krajowych porządków prawnych, natywnego dla cyberprzestrzeni *lex informatica* tworzonego poprzez tzw. afordancje[4] normowania faktycznego i metanormy - należące do *lex informatica* i prawa międzynarodowego publicznego jednocześnie i tworzące mechanizm wzajemnego normowania się tych systemów.

Poza przeprowadzeniem opisanych powyżej analiz prawa, metodologia niniejszej rozprawy musi objąć także rozważania i analizę literatury przedmiotu dotyczące stanu faktycznego cyberprzestrzeni. Cyberprzestrzeń jest bowiem zjawiskiem bez precedensu - stanowiąc niefizyczne *quasi-terytorium* działające w oparciu o infrastrukturę zlokalizowaną w świecie fizycznym. Suma wszystkich wspomnianych elementów pozwala na określenie w jaki sposób normowana jest cyberprzestrzeń i określenie skutków prawnych cech natywnych dla konstrukcji cyberprzestrzeni.

Zrozumienie mechanizmów rządzących zarówno faktyczną jak i prawną konstrukcją cyberprzestrzeni pozwala na umiejscowienie norm prawa międzynarodowego publicznego w ich kontekście i przeprowadzenie analizy porównawczej ich funkcjonowania w obydwu systemach prawnych. Umożliwia to rozważenie sposobu funkcjonowania podstawowych dla rozprawy niniejszej pojęć, to jest suwerenności i jurysdykcji w cyberprzestrzeni. Następnie przeprowadzona zostanie analiza porównawcza mechanizmów w drodze których *ratio legis* wspomnianych instytucji zostaje zachowane w zupełnie innym środowisku prawnym.

---

[4] Polskie tłumaczenie terminu *affordances*, oznaczającego możliwe dla jednostki środki interakcji z otoczeniem, w tym wypadku cyberprzestrzenią. zob. Preece J., Rogers Y., Sharp H., Benyon D., Holland S., Carey T.*Human-Computer Interaction*, Addison-Wesley Longman Press, (1994), ss. 6 i n.- Afordancje jako środek służący do świadomego projektowania możliwości cyberprzestrzeni opisuje także Donald Norman [w:*The Design of Everyday Things*, Basic Books, 2002]

W konsekwencji możliwe stanie się wskazanie wskazanie zakresu i sposobu ich redefincji, co pozwoli odpowiedzieć na postawione w rozprawie pytanie badawcze. W pracy niniejszej zostanie dokonane także *case study* przypadków naruszeń suwerenności w cyberprzestrzeni, którego celem będzie uzupełnienie rozważań dotyczących praktyki międzynarodowej także o sposoby reakcji na naruszenia suwerenności w cyberprzestrzeni.

I. Definicje pojęć

1. Cyberprzestrzeń

Pojęcie cyberprzestrzeni jest pojęciem kluczowym dla niniejszej rozprawy. Nie jest jednak łatwe jasne określenie jego desygnatu. Cyberprzestrzeń jest bowiem czymś innym niż tylko sumą danych i urządzeń do niej podłączonych. Początkiem cyberprzestrzeni była stosunkowo prosta z dzisiejszego punktu widzenia sieć komputerowa, służąca głównie do przesyłu danych i w związku z tym powodująca usprawnienie procesów już istniejących, nie tworząc jednak nowych. Tym samym nie tworzyła ona jeszcze nowych elementów zakresowych prawa międzynarodowego. Rozwój cyberprzestrzeni natomiast doprowadził w bardzo krótkim czasie do stworzenia takich elementów, ze względu na powszechność i istotność tejże. Cyberprzestrzeń, w przeciwieństwie do sieci o opisanych powyżej cechach , tworzy nowe zdarzenia prawne pozostające ze światem fizycznym w stosunku logicznym podprzeciwieństwa (jeżeli za klasę przyjmiemy zakres objęty normowaniem prawa międzynarodowego publicznego). Istnieją bowiem elementy świata fizycznego nie dotknięte działaniem cyberprzestrzeni, tak jak i istnieją rejony cyberprzestrzeni istniejące wyłącznie jako zapis danych informatycznych.

1. a. Pojęcie i jego geneza. Próba definicji legalnej

Na początku niniejszych rozważań konieczne jest zdefiniowanie cyberprzestrzeni. Należy zauważyć, że brak jednoznacznej, szeroko akceptowanej, definicji legalnej cyberprzestrzeni, zarówno w aktach prawnych jak i w doktrynie[5] prawa

[5] Ze względu na specyfikę prawa cyberprzestrzeni, pozbawionego kodyfikacji i wobec wymienienia nauki prawa w katalogu *de iure* źródeł orzekania a *de facto* - prawa międzynarodowego przyjętym przez Międzynarodowy Trybunał Sprawiedliwości [w: art. 38 (d) Statutu Międzynarodowego Trybunału Sprawiedliwości, stanowiącego integralną część Karty Narodów Zjednoczonych, Dz.U. 1947.23.90], w pracy niniejszej określenie 'definicja legalna' odnoszone jest także do opinii doktryny.

międzynarodowego Istniejące zaś definicje pozostają ze sobą sprzeczne lub sobie przeciwne. Konieczne jest więc dokonanie przeglądu tych definicji i wskazanie na najistotniejsze z punktu widzenia niniejszej rozprawy ich elementy, poparte dotychczasową praktyką międzynarodową i pracami teoretycznymi.

Punktem wyjścia dla tych rozważań, musi być oczywiście definicja faktyczna cyberprzestrzeni. W 1982 pisarz William Gibson podał pierwszą taką definicję. .[6] Definicja ta, sama w sobie bardzo nieprecyzyjna nieścisła logicznie (co nie może dziwić, ponieważ została zawarta w zbiorze opowiadań *science fiction* Gibsona *Burning Chrome,* a później powtórzona w jego przełomowej powieści *Neuromancer*[7]) i mająca wyłącznie cel literacki, stała się jednak istotna dla prawa międzynarodowego i innych dziedzin naukowych, poprzez sam fakt jej powstania i wyróżnienia cyberprzestrzeni *per se* jako odrębnego zjawiska. Gibson stworzył bowiem pojęcie, które jednym słowem denotowało i zawierało w sobie całe spektrum zjawisk dotyczących postępującej komputeryzacji życia. Istotnym elementem było także zastosowanie określenia "przestrzeń", wskazującego, że mowa o pewnej odrębnej lokalizacji, co miało niemały wpływ na późniejsze analizy prawne dotyczące tego zjawiska. Jednakże stworzenie definicji legalnej, nawet najprostszej, okazało się zadaniem nieporównanie trudniejszym. Zarówno definicja Gibsona jak i kolejne, stosowane w literaturze przedmiotu, były definicjami deiktycznymi, niezbyt przydatnymi jako podstawa do tworzenia skomplikowanego systemu prawnego, dotyczącego cyberprzestrzeni.

Pierwszą próbę dokonania definicji mającej znaczenie prawne podjął Departament Obrony USA, określając cyberprzestrzeń następująco: *a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks,*

---

[6] 'A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding." *Wizualizacja danych z każdego komputera używanego przez człowieka. Niebywałe skomplikowanie. Linie światła sięgające poza umysł, klastry i układy danych. Jak wygasające światła miasta.*

[7] Gibson W. *Neuromancer,* Ace Mass Market (1986) s.134

computer systems, and embedded processors and controllers.[8] Podstawowym problemem tej definicji, umieszczonej w wewnętrznym memorandum Departamentu Obrony Stanów Zjednoczonych dotyczącym obrony przed cyberatakami[9], jest jej nieprzejrzystość. Dodatkowo brak przekonywujących definicji legalnych tych pojęć, które się na przywołaną definicję składają. Ich zdefiniowanie staje się możliwe wyłącznie w odniesieniu do cyberprzestrzeni. Faktycznie, jest to więc definicja obarczona błędem *circulos in definiendo*. Podobne dokumenty, powstałe w innych państwach i dotyczące obrony przed powstającymi zagrożeniami cyberprzestrzennymi, także albo przyjmowały swoiste definicje deiktyczne, albo też ograniczyły się do wskazania jakie działania będą te państwa podejmować w cyberprzestrzeni. Nie precyzowały jednak, jak mają one zamiar precyzyjnie cyberprzestrzeń definiować, niejako uznając zakres ten za oczywisty i nie wymagający dalszego tłumaczenia. Pierwsza zadowalająca definicja legalna cyberprzestrzeni została podana dopiero podczas nieodległej czasowo próby skodyfikowania istniejącego prawa międzynarodowego dotyczącego konfliktu w cyberprzestrzeni, a więc przez Tallinn Manual.[10] Autorzy zdefiniowali cyberprzestrzeń[11] jako *The environment formed by physical and non-physical components characterized by the use of computers and the electro-magnetic spectrum to store, modify and exchange data using computer networks.*[12] Definicja ta jest pozbawiona wszystkich słabości, którymi obciążona była omówiona powyżej definicja Departamentu Obrony. Pozwala bowiem ona na określenie czym jest cyberprzestrzeń w sensie fizycznym, a co za tym idzie - na wyznaczenie jakie elementy świata należą do cyberprzestrzeni a jakie nie. Od momentu jej powstania, jest ona szeroko cytowana i została inkorporowana do większości powstających

---

[8] globalna domena w środowisku informacyjnym składająca się ze współzależnych infrastruktur technologii komunikacyjnych; Internet, sieci telekomunikacyjne, systemy komputerowe wraz z przypisanymi im urządzeniami do przetwarzania i kontroli przepływu danych

[9] England G. *Memo on Cyberspace Defense of USA* , USA Departament of Defense (2008) ss.1-3

[10] Należy pamiętać, że definicje zawarte w TM, nie mają mocy prawnej.

[11] zob. *TM 2.0* s. 564

[12] *środowisko oparte o fizyczne i niefizyczne składniki, charakteryzujące się użyciem komputerów i spektrum elektromagnetycznego do przechowywania, modyfikowania i wymiany danych przy pomocy sieci komputerowych*

współcześnie dokumentów o cyberprzestrzeni. Definicja ta nie została zawarta w akcie prawnym o mocy wiążącej (ani Tallinn Manual ani Tallinn Manual 2.0 pomimo przyznawania mu przez doktrynę w wielu tekstach rangi równej traktatom, nie został uznany nigdy za akt w jakikolwiek sposób wiążący, szczególnie nie ma on rangi prawa zwyczajowego w sensie ścisłym, brak także orzecznictwa *explicite* potwierdzającego wiążącą *erga omnes* rangę dokumentu), niemniej zgodnie z tradycyjnym pojmowaniem źródeł prawa międzynarodowego, można ją przyjąć za obowiązują z dwóch powodów:

a. stanowi ona (tak jak cały *Tallinn Manual* 1.0 i 2.0) zbiór norm zwyczajowych, oparty na pracy międzynarodowego zespołu i będącego aktem wewnętrznym organizacji międzynarodowej, jaką jest Sojusz Północnoatlantycki. Da się też niewątpliwie wykazać istnienie praktyki międzynarodowej, opartej o powołane regulacje;
b. odpowiada aktom prawnym dotyczącym cyberprzestrzeni, promulgowanym przez poszczególne państwa, co można próbować uznać za spełnienie przesłanek zasad uznanych przez cywilizowane systemy prawne, w rozumieniu Statutu Międzynarodowego Trybunału Sprawiedliwości.[13]

Należy także wskazać, że powszechne przyjmowanie *Tallinn Manual* i *Tallinn Manual 2.0* za *black-letter law* w kwestii cyberprzestrzeni, pomimo jego niekompletności i braku niekwestionowanej mocy normatywnej w coraz większym stopniu prowadzi do powstania *opinio iuris* polegającego na wyrażeniu zgody na związanie się państw jego postanowieniami. W związku z tym, w niniejszej pracy za jedyną definicję cyberprzestrzeni przyjęto co do zasady przywołaną powyżej definicję z *Tallinn Manual* (i *Tallinn Manual 2.0*). Nie ma też wątpliwości, że ujęta w TM definicja, pomimo iż pierwotnie umieszczona w źródle dotyczącym działań w cyberprzestrzeni powyżej poziomu "użycia siły" w rozumieniu art. 2(4) Karty Narodów Zjednoczonych, a więc po prostu do konfliktów w cyberprzestrzeni, jest także do stosowalna do działań o intensywności poniżej tej granicy, lub też

[13] zob. Art. 38(1)(c) Statutu Międzynarodowego Trybunału Sprawiedliwości. Dz.U. 1947 poz. 23 nr 90

niezwiązanym z konfliktem. Wskazuje na to przyjęcie tej samej definicji w TM 2.0, mającym według zamiaru Grupy Ekspertów, autorów wspomnianej pracy, być zbiorem regulacji dotyczącym właśnie tego szerszego zakresu przedmiotowego. Wobec tego przy pomocy definicji Grupy Ekspertów można próbować wyznaczać granice zarówno "piątego teatru wojny[14]", jakim stała się w ciągle w niej trwającej swoistej zimnej wojnie cyberprzestrzeń. Można także - choć ten zakres leży zasadniczo poza obszarem zainteresowań pracy niniejszej – wyznaczać pola działań o charakterze wyłącznie policyjnym, mające na celu przeciwdziałanie cyberprzestępczości właśnie w ramach wykonywania przez poszczególne państwa jurysdykcji w cyberprzestrzeni.

Także definicja przedstawiona przez autorów *Tallinn Manual* nie jest jednak pozbawiona wad. Podstawowym jej brakiem jest brak jasnego rozgraniczenia fizycznych i niefizycznych elementów cyberprzestrzeni, a więc tych, które istnieją w świecie rzeczywistym i tych istniejących wyłącznie w cyberprzestrzeni. Podział ten ma doniosłe znaczenie prawne, ze względu fakt oparcia dotychczasowych definicji suwerenności i jurysdykcji głównie o zasadę terytorialności. Z przedstawionej definicji nie sposób wskazać wyraźnie, które z elementów cyberprzestrzeni należą do którego z tych zakresów, a co za tym idzie, czy jurysdykcja wykonywana w oparciu o terytorium stosuje się do nich w jakimkolwiek, choćby ograniczonym stopniu. Problem ten zostanie szerzej omówiony w dalszej części wywodu. Ponadto przywołana definicja nie podaje jasnego rozwiązania co do legalnego statusu danych jako takich. Konstruując bowiem definicję cyberprzestrzeni w oparciu o jej fizyczne aspekty takie jak spektrum elektromagnetyczne, Grupa Ekspertów pomija bowiem fakt, że dane stanowiące wynik odczytania przez pewne urządzenie określonego sygnału mają także wtórne znaczenie dla samej konstrukcji cyberprzestrzeni. Nie są

[14] Analogicznie do przyjęcia, że cyberprzestrzeń jest piątą domeną (piątym res communis omnium), uznana została za piąty (po morzu, lądzie, powietrzu i przestrzeni kosmicznej) teatr działań wojennych. zob. *War in the fifth domain-Cyberwar*, specjalny raport 'The Economist (2010) s.2.Podobnie traktuje cyberprzestrzeń Sojusz Północno-Atlantycki. Sekretarz Generalny NATO Jens Stoltenberg ogłosił, że agresja tam przeprowadzona przeciwko jednemu z państw sojuszu uruchomi jego zbiorową samoobronę [w:Paganini P. NATO officially recognizes cyberspace a warfare domain, raport sporządzony dla 'Security Affairs' (2016)s.1]

więc one wyłącznie niezależnymi nośnikami informacji, dla których cyberprzestrzeń jest wyłącznie środkiem przechowywania lub przesyłania. Pełnią także istotną rolę w architekturze samej cyberprzestrzeni. Wyłączenie tego aspektu istnienia danych z definicji legalnej umieszcza je niejako w luce prawnej, a to z kolei w oczywisty sposób utrudnia normowanie cyberprzestrzeni.[15] Drugą stroną tego samego problemu definicyjnego jest uzależnienie istnienia cyberprzestrzeni od istnienia przepływu danych, co - jak pokazuje praktyka międzynarodowa - nie w każdym przypadku musi być prawdą. Jeżeli rozważymy systemy przygotowywane do przeprowadzenia ataku cybernetycznego, musimy zauważyć, że dopóki nie zostaną one aktywowane, nie wytwarzają żadnych impulsów. To wyłączałoby je z kolei z tak definiowanej cyberprzestrzeni, a w konsekwencji z możliwości wykonywania prawa do samoobrony przez państwo, przeciwko któremu mają one być użyte. Same dane z kolei *Tallinn Manual* definiuje[16] jako the *basic elements that can be processed or produced by a computer.*[17]

Konieczne jest więc zadanie pytania - czy istotnie zamiarem autorów definicji było wyłączenie z cyberprzestrzeni wszystkich urządzeń, które w danym momencie nie przetwarzają danych, czy też należy do normy dekodowanej z obydwu definicji stosować wykładnię funkcjonalną przyjmując, że sama możliwość włączenia danego urządzenia do cyberprzestrzeni jest wystarczająca by uznać to urządzenie za jej element.

W aktualnym stanie prawnym brak wystarczającej praktyki międzynarodowej i orzecznictwa by jednoznacznie rozstrzygnąć tę wątpliwość. Ścisła i literalna wykładnia norm wynikających z zestawienia definicji danych i cyberprzestrzeni zaproponowanych przez IGoE musi prowadzić do wniosku, że o ile komputer nie ma w danym momencie zdolności przetwarzania danych - nie jest on elementem cyberprzestrzeni. Dodatkowo, ponieważ elementy fizyczne i nie-fizyczne wskazane

---

[15] zob. także *Securing data in cyber space*, raport Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA), Heraklion (2013) s.4

[16] zob. słownik definicji TM, hasło *Data* s.258. Także i ta definicja zostaje powtórzona w *TM 2.0* zob.tamże s.552

[17] *podstawowe elementy produkowane lub przetwarzane przez komputer*.

w definicji cyberprzestrzeni znajdują się w jednym zdaniu i nie są w żaden sposób różnicowane, zasady wykładni językowej nakazują przyjąć, że chodzi o ich koniunkcję.

Można więc zakładać, że w obecnym stanie prawnym nie należą do cyberprzestrzeni ani abstrakcyjnie istniejące dane, ani nie podłączone do ogólnoświatowej sieci urządzenia, które mogą zostać w pewnym momencie do niej włączone. Taką interpretację wydaje się wzmacniać także wykładnia językowa. Skoro bowiem w definicji cyberprzestrzeni mowa jest o sieci, uzasadniony wydaje się wniosek, że do jej istnienia wymagane są połączenia poszczególnych elementów. Należy więc przyjąć, że cyberprzestrzeń jest kategorią *sui generis* prawa międzynarodowego, dla której środki techniczne w gruncie rzeczy mają znaczenie drugorzędne. Ich ewentualna zmiana jest nieistotna dla samego funkcjonowania cyberprzestrzeni (przykładowo, jeżeli powstanie sieć niewymagająca oparcia o fizyczne łącza, nie zmieni to definicji cyberprzestrzeni opisanej powyżej). Podobnie nieistotna jest sama technologia przetwarzania danych. Decyduje sam fakt możliwości wpływania na stan danych tworzących cyberprzestrzeń w danym momencie, przez kogokolwiek, niezależnie od innych użytkowników sieci.

Z powyższych konstatacji wynikają przypisywane przez doktrynę cyberprzestrzeni aspekty anonimowości, wszechobecności i niemożliwości fizycznego jej zlokalizowania.[18] Cechy te mają fundamentalne znaczenie dla definiowania cyberprzestrzeni, wymagając stworzenia dla niej zupełnie nowego prawa, z bardzo wąskim zakresem bezpośredniego stosowania analogii do wcześniej powstałego prawa międzynarodowego. Brak możliwości fizycznej lokalizacji sieci implikuje zupełnie inne pojmowanie suwerenności i jurysdykcji, wyłączając terytorializm jako podstawowe kryterium ich określania. Wszechobecność cyberprzestrzeni i możliwość równego do niej dostępu powoduje rozszerzenie katalogu podmiotów, mogących uzyskać wpływ na dziedziny życia dotychczas zarezerwowane dla podmiotów prawa

[18] zob. Herrera G. L. *Cyberspace and Sovereignity: Thoughts on Physical Space and Digital Space,* referat wygłoszony na 1 międzynarodowej konferencji CISS/ETH *The Information Revolution and the Changing Face on International Relations and Security*(2005) ss.1-5

międzynarodowego publicznego (przykładowo - właśnie na suwerenność państw), *de facto* bardzo rozszerzając ten katalog. Dotychczas, z powodów faktycznych, realna możliwość naruszenia suwerenności jakiegoś państwa przez jednostkę w zasadzie nie istniała lub sprowadzała się do niewielkich naruszeń. Rozwój cyberprzestrzeni w zasadzie zrównał możliwości *non-state actors* w tym zakresie z tymi, które są dostępne innym państwom. Ponieważ elementem wszystkich przedstawionych w tej pracy definicji i koncepcji suwerenności państwa jest prawo i możliwość egzekwowania własnego ustawodawstwa na określonym terytorium, należy rozważyć możliwość delimitacji terytorium państwa także w cyberprzestrzeni. Pomimo iż "cyberterytorium" *per se* nie istnieje, można w cyberprzestrzeni określić pewne wyłączone obszary do których odpowiednio stosują się przepisy o terytorialności (choć obszary te nie są fizycznym terytorium, a stosowanie owych norm polega na przyjęciu fikcji prawnej).

Konstrukcje te i ich podstawy prawne są oparte o analogie z regulacjami morza, przestrzeni kosmicznej i Antarktydy. Chodzi więc o przestrzenie eksterytorialne, których statusy prawne oparte są o postanowienia traktatów i konsensus, nie wykluczając jednak pewnych przejawów suwerenności i klasycznie rozumianej jurysdykcji zwyczajnej. Konieczność utrzymania suwerenności (pomimo wszystkich przesłanek wskazujących na jej redefinicję) w cyberprzestrzeni jest niekwestionowana. Na jej istnienie wskazuje choćby fakt, że państwa wykonują w stosunku do cyberprzestrzeni swoją jurysdykcję zwyczajną we wszystkich jej przejawach.

1. b. Podział na część informatyczną i fizyczną. Skutki prawne.

Cyberprzestrzeń, zgodnie z przyjętą definicją, musi składać się z dwóch elementów. Jednym z nich są dane - niematerialne, istniejące wyłącznie w samej cyberprzestrzeni, niewidzialne dla gołego oka. Należy zauważyć, że w części definicji przywołanej w Tallinn Manual 2.0, odwołującej się do części cyberprzestrzeni, która w dalszym ciągu niniejszej rozprawy określana będzie jako „informatyczna" - abstrakcyjnie istniejące dane ją tworzące wymagają dla swego istnienia także fizycznie istniejących

sygnałów, przenoszących te dane. Część autorów wskazuje, że należy je traktować jako osobne elementy cyberprzestrzeni, *de facto* dzielącej się więc na trzy części[19] lub nawet na sześć[20].

Poglądy te wskazane zostały wyłącznie dla komplementarności wywodu i zaznaczenia istnienia innych ujęć tego zagadnienia w literaturze przedmiotu. O ile bowiem oczywista jest różnica pomiędzy danymi a sygnałami użytymi do ich zapisania i przesłania - nie sposób się zgodzić z poglądem, że którekolwiek z nich mogą stanowić odrębną część funkcjonalną. Drugim elementem jest infrastruktura, a więc urządzenia odbierające i wysyłające sygnały, o których mowa w definicji cyberprzestrzeni. Urządzenia te istnieją w sposób fizyczny, postrzegalne są także poza cyberprzestrzenią. Te elementy, zostaną więc określone 'fizyczną' częścią cyberprzestrzeni. Pierwszym skutkiem tego podziału, który musi być dostrzegalny z punktu widzenia niniejszej rozprawy jest problem terytorialności. O ile bezdyskusyjne jest, że fizycznie istniejące urządzenia (niezależnie od tego czy w danym momencie stanowią element cyberprzestrzeni czy też nie) podlegają jurysdykcji zwyczajnej państw, na terytorium których są położone na zasadach ogólnych - wykonywania tego rodzaju jurysdykcji wobec pakietów danych (lub też sygnałów służących jako ich nośniki) za oczywiste uznać nie sposób. Podobnie rzecz się ma z danymi zapisanymi na środkach fizycznych służących do ich przenoszenia, które znajdują się na określonym terytorium. Jednakże należy odróżnić poszczególne zapisy na tych środkach od samych danych. Odróżnienie to jest zbliżone do znanej już prawu cywilnemu operacji rozdzielania pieniędzy w rozumieniu walorów od znaków pieniężnych, które są wyłącznie reprezentacją tych pierwszych. Do rozstrzygnięcia pozostaje kwestia czy jurysdykcji tej poddane są same dane.

---

[19] zob. Benkler Y. *From Consumers to Users:Shifting the Deeper Structures of Regulation Towars Sustainable Commons and User Access* 52 Federal Communications Law Journal (2000) ss. 561-2 . Wskazywał on, że istnieją trzy "warstwy" cyberprzestrzeni. Fizyczna, logiczna i warstwa zawartości (*content layer*). Za tę ostatnią uznawał treści zrozumiałe dla człowieka, w odróżnieniu od treści warstwy logicznej, zrozumiałej dla komputera. Natomiast Lessig uznaje za warstwę logiczną system decydujący „kto ma dostęp do czego i co zostaje posłane dokąd- *the system controls who gets access to what or what gets to run where"* [w: Lessig L. *The Architecture of Innovation* 51 Duke Law Journal (2002)ss. 1783-6]

[20] Tak Solum L.B., Minn Ch. *The Layers Principle: Internet Architecture and the Law* 79 Notre Dame Law Review, 815 (2004) s.816-17

Praktyka i orzecznictwo wskazują, że nie ma takiej możliwości. Sytuacja z danymi jest sytuacją prawną podobną do opisanego w dalszej części wywodu eksperymentu z serwerami wykonanego przez Jona Postela.Wykonanie jurysdykcji miałoby realne znaczenie wyłącznie wtedy, gdyby wszystkie kopie danych istniejące we wszechobecnej sieci zostały poddane takiemu samemu działaniu jednocześnie. Takie rozumienie jurysdykcji nad danymi zostało potwierdzone podczas pierwszego procesu banku *Julius Baer* przeciwko organizacji *Wikileaks*.[21] Powód wnosił o zablokowanie dostępu do strony organizacji *Wikileaks* poprzez wydanie sądowego nakazu usunięcia należących do niej treści (wraz ze wszystkimi kopiami) przez hosta serwerów, na których treści te *Wikileaks* przechowywała czyli *Dynadot*. Uzasadnieniem roszczenia pozwu był fakt, że *Dynadot* jest spółką prawa amerykańskiego a jego serwery znajdują się na amerykańskim terytorium. Domagano się jednak wyłącznie interwencji wobec danych, a celem petitum pozwu było uniemożliwienie pozwanym ich dalszego publikowania, używając fizycznego położenia serwerów do wskazania właściwej jurysdykcji. Strona powodowa uzyskała korzystne dla siebie zarządzenie sądu, które jednak zupełnie nie uwzględniało istoty cyberprzestrzeni, opierając się na (kwestionowanym na tym etapie postępowania) prawie własności ujawnionych dokumentów.[22] Wydane zarządzenie nie zmieniło jednak w żaden sposób sytuacji faktycznej, ze względu na uruchomienie przez *Wikileaks* i jej organizacje pokrewne lustrzanych serwerów zawierających tą samą treść a znajdujących się poza zasięgiem amerykańskiej jurysdykcji zwyczajnej. Z prawnego punktu widzenia, zarządzenie zostało zaskarżone a jego uzasadnienie odparte przez koalicję mediów amerykańskich, które złożyły w sądzie opinię jako *amici curiae,* wziętą pod uwagę przez sąd wyższej instancji rozpoznający środek odwoławczy *Wikileaks*.[23]

Istotnym z punktu widzenia zakresu przedmiotowego dysertacji niniejszej jest uzasadnienie wyłączenia firmy *Dynadot* spod właściwości funkcjonalnej sądu w zakresie wydanego zarządzenia. Powołano się mianowicie na art. 230(c)(1) *Computer*

---

[21] *Bank Julius Baer & Co. Ltd and Julius Baer Bank and Trust Co. Ltd v. Wikileaks, Wikileaks.org and Dynadot LLC 535 F. Supp 2d 980*

[22] zob. Zarządzenie sędziego okręgowego J.S. White'a z dnia 15 lutego 2008 roku o syg. CV08-0824 *[Bank J. Baer v. Wikileaks]* wraz z uzasadnieniem.

[23] *Brief of Amici Curiae...* z 29 lutego 2008 *[Baer v. Wikileaks]*

Decency Act[24], regulujący kwestię wyłączeń odpowiedzialności podmiotu, którego działalność ogranicza się do świadczenia interaktywnych usług internetowych.[25] Przywołany przepis wskazuje, że nie można utożsamiać takiego podmiotu z osobą publikującą treści. Wskazano także, że same *Wikileaks* spełniają przesłankę podmiotową wyłączenia, ponieważ także dostarczają interaktywnych usług internetowych, a przepisy nie precyzują charakteru tych usług.[26] Ta argumentacja jest zgodna z ustaloną już linią orzeczniczą amerykańskich sądów federalnych i stanowych.[27] Przed rozpoznaniem sprawy, o której mowa powyżej, także sąd okręgowy w Kalifornii przychylił się do argumentacji wskazanej przez *Amici Curiae* i uchylił nakaz, wskazując na brak własnej jurysdykcji co do rozstrzygnięcia sporu.[28]

Analiza opisanego przypadku musi prowadzić do wniosku, że sąd krajowy w Stanach Zjednoczonych uznał, że nie ma jurysdykcji nad danymi, nawet jeżeli ich istnienie w cyberprzestrzeni oparte jest o infrastrukturę, nad którą może wykonywać jurysdykcję zwyczajną w oparciu o zasadę terytorialności. Nie jest także możliwe, by co do zasady Stany Zjednoczone wykonywały wobec takich danych jurysdykcję nadzwyczajną, ponieważ prowadziłoby do absurdalnej sytuacji, w której wewnętrzna właściwość sądu jest wyłączona w odniesieniu do jakiegoś zakresu przedmiotowego wyłącznie w takim celu, by wykonywać co do tego zakresu jurysdykcję nadzwyczajną. Sytuacja taka jest niemożliwa do pogodzenia z zasadami pewności prawa, racjonalności ustawodawstwa i subsydiarności jurysdykcji nadzwyczajnej.

---

[24] *Title V of the Telecommunications Act* 1996, kodyfikowany w 47 United States Code §230, tzw. *Communications Decency Act*

[25] Opisywany akt prawny został znowelizowany w kwietniu 2018 roku, poprzez tzw. *FOSTA-SESTA Act*, jednakże wyłącznie w ten sposób, że podmiot udostępniający usługi sieciowe nie może powołać się na wyłączenie odpowiedzialności wynikające z 230(c)(1) *Communications Decency Act* w przypadku oskarżenia o przestępstwo stręczycielstwa lub też w przypadku pozwu cywilnego za szkody ze stręczycielstwa wynikające. Nowelizacja w żaden sposób nie zmienia wyłączeń dotyczących kwestii jurysdykcji nad danymi na serwerach i została wspomniana wyłącznie dla kompletności wywodu.

[26] *Brief of Amici... (Baer v. Wikileaks)*ss. 22-23

[27] por. Orzeczenia zapadłe w sprawach *Delfino v. Agilent Tech.Inc. 52 CAl. Rptr. 3d 376 (2006),*145 Cal. App 4th 790. także *Carfano v. Metrosplash.com Inc. 339 F.3d 1119 9th Circ.* z 2003 roku.

[28] zob. uzasadnienie sędziego J. White'a do zarządzenia z 29 lutego 2008 uchylającego zarządzenie o zakazie publikowania przez Dynadot treści należących do Wikileaks *[Baer... v. Wikileaks...]* s.5 i n.

Identyczną z przedstawioną powyżej argumentację można zastosować także do przepisów obowiązujących w Unii Europejskiej. Jakkolwiek ani sądy państw członkowskich ani unijne nie rozpoznawały nigdy sprawy podobnej do *J. Baer v. Wikileaks*, to ustawodawstwo unijne oparte jest na identycznych wyłączeniach odpowiedzialności.[29] Pomimo iż wspomniany akt jest wyłącznie dyrektywą, a więc wiąże państwa członkowskie wyłącznie pośrednio, należy wskazać, że dyrektywa jest aktem ujednolicającym prawo krajów członkowskich i jej cele muszą zostać przyjęte do porządków prawnych tychże państw, a w niektórych przypadkach może mieć ona skutek bezpośredni. Niewątpliwie rolę ujednolicającą ma więc norma dekodowana z artykułu 12(4) wspominanej dyrektywy, gwarantująca wyłączenie odpowiedzialności za przesyłanie treści podmiotom świadczącym usługi: tzw. z*wykłego przekazu*[30]*:* hostingu lub cachingu. Pamiętać bowiem należy, że jak wskazano powyżej, w razie zwłoki któregoś z państw członkowskich w implementacji dyrektywy, podmioty prawa UE mogą powoływać się na normy pochodzące z tej rangi aktów prawnych w sposób bezpośredni. Regulacja ta definiuje, że *zwykły przekaz* świadczy ten podmiot, który nie jest inicjatorem przekazu, nie wybiera jego odbiorcy i nie modyfikuje danych pomiędzy początkowym a końcowym użytkownikiem.[31] Okoliczności wyłączenia odpowiedzialności dotyczące cachingu są identyczne jak dla zwykłego przekazu, a odrębny przepis istnieje wyłącznie ze względu na techniczne różnice faktyczne pomiędzy samymi rodzajami usług.[32] Usługi hostingowe natomiast dyrektywa definiuje jako przechowywanie niemodyfikowanych informacji.[33] Zgodnie więc z przedstawioną powyżej definicją danych, będą one należały wyłącznie do informatycznej części cyberprzestrzeni i omówione wyżej wyłączenia nie będą miały do tej usługi zastosowania. Zarówno w

---

[29] zob. Dyrektywę Parlamentu Europejskiego i Rady 2000/31 z dnia 8 czerwca 2000 roku w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego. pub. W Dz. Urz. UE z 17 lipca 2000,syg. L178 ss.1-16

[30] W angielskiej wersji dyrektywy *mere conduit*. Chodzi tu o podmiot pełniący rolę wyłącznie przekaźnika, zakres podmiotowy wyłączenia odpowiedzialności jest więc identyczny jak w opisanej wyżej regulacji amerykańskiej.

[31] zob.art 12(1) Dyrektywy 2000/31.

[32] ibid.art 13(1)

[33] ibid.art. 14(1)

europejskich jak i w amerykańskich regulacjach wyłączenia te nie są bezwarunkowe. Niemniej, w żadnym z tych porządków prawnych, konstrukcja wspomnianych wyłączeń nie wskazuje na wykonywanie przez państwa jurysdykcji nad danymi.

Jurysdykcja państw sprowadza się bowiem wyłącznie do zobowiązania operatorów do dokonania określonych czynności faktycznych wobec danych, przy pomocy procedury tzw. *notice and takedown.*[34] Jest to konstrukcja prawna oparta o możliwość wydania przez sąd lub organ administracyjny (na wniosek ewentualnego poszkodowanego przez określone dane) nakazu określonego zachowania się usługodawcy- polegającego na usunięciu, zablokowaniu lub zmodyfikowaniu odpowiednich danych. Procedura ta funkcjonuje zarówno w ustawodawstwie unijnym[35] jak i amerykańskim.[36] Należy jednak zwrócić uwagę, na bardzo istotną różnicę pomiędzy tymi systemami. W Stanach Zjednoczonych opisywana procedura jest elementem prawa prywatnego (sporem pomiędzy podmiotem, który żąda usunięcia danych a tym je przechowującym)[37], podczas gdy w Unii Europejskiej jest to *notice and takedown* regulowane w ramach prawa publicznego.[38] Pomimo jednak tej różnicy, żadne z państw, stosujących *notice and takedown* nie przypisuje sobie możliwości wykonywania jurysdykcji nad danymi w cyberprzestrzeni *in abstracto*. Czym innym jest bowiem nakaz pewnego zachowania (wydawany wobec podmiotu znajdującego się we własnej jurysdykcji zwyczajnej), a czym innym wykonywanie jurysdykcji wobec określonego przedmiotu bezpośrednio. Dodatkowo w ustawodawstwie unijnym odmowa wykonania takiego nakazu sądu jest czynem legalnym, a jedyną sankcją jest utrata wyłączenia odpowiedzialności opisanego powyżej.[39] Innymi słowy, ISP, który nie wykona owego nakazu nie może ponieść odpowiedzialności tylko za to zachowanie, a jedynie zaczyna ponosić odpowiedzialność zarówno karną jak i cywilną za zawartość, którą na własnych

---

[34] Baistrocchi P.A. *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce* 19 Santa Clara High Tech Journal 111 (2002) s.111

[35] zob. art.12-14 *in fine* Dyrektywy2000/31

[36] 17 USC §512

[37] *por. Section 512 Digital Millenium Copyright Act*, 112 Stat. 2860 (1998), Pub.L. 105-304

[38] *por. Art. 14 Dyrektywy 2000/31/WE*

[39] zob. normę dekodowaną z art. 13(1)(e) w związku z art. 13(2) Dyrektywy 31/2000.

serwerach utrzymuje.

Niewątpliwie nie można więc przyjąć, że *notice and takedown* na gruncie prawa UE należy do *imperium* państw członkowskich a co za tym idzie, jest pochodną posiadanej przez nich jurysdykcji zwyczajnej. Tym bardziej byłby nieuprawniony taki wniosek w odniesieniu do regulacji amerykańskich, które *explicite* przenoszą ów mechanizm do domeny niepoddanej własnemu *imperium*. Zastosowanie instytucji związanej z wykonywaniem jurysdykcji wobec danych nie tylko nie jest przewidziane przez wspomniane przepisy, ale wręcz jest przez nie pośrednio wyłączone. Wystarczy do wskazanej powyżej normy zastosować zasadę racjonalności ustawodawcy, by zauważyć, że same państwa członkowskie, przyjmując w takim kształcie wspomnianą regulację, a następnie inkorporując ją do swoich porządków prawnych, uznają to za ograniczenie własnej jurysdykcji. W innym przypadku bowiem, dyrektywa musiałaby przewidywać jakieś środki bezpośrednio wiążące ISP, lub choćby nakładające bezpośrednią sankcję za sam fakt niewykonania *notice and takedown*, analogicznie do mechanizmu przepadku majątku pochodzącego z lub służącego do popełnienia przestępstwa. Musiałoby się tak dziać także dlatego, że dyrektywa, zgodnie ze swoją pozycją w hierarchii źródeł prawa UE, określa wyłącznie minimum legislacyjne i w żaden sposób nie wyłącza możliwości ustanowienia przez poszczególne państwa członkowskie regulacji dalej idących. Należy więc wnosić, że państwa nie uznają swojej jurysdykcji nad częścią cyberprzestrzeni istniejącą wyłącznie cyfrowo. Także grupa autorów *Tallinn Manual* wyraźnie rozdziela elementy fizyczne i informatyczne cyberprzestrzeni, przyznając prawo do wykonywania zwykłej jurysdykcji przez państwa wobec elementów fizycznych cyberprzestrzeni położonych na ich terytoriach, jednocześnie odmawiając państwom suwerenności nad samą cyberprzestrzenią rozumianą jako całość.

Podział ten sprawia pewien podstawowy problem interpretacyjny, stając naprzeciw podstawowej zasadzie kontynentalnego systemu prawa, opartego na tradycji rzymskiej, a mianowicie zasadzie *in toto et pars continentur*. Skoro bowiem sama definicja przyjęta przez autorów TM i TM2.0, zakłada, że cyberprzestrzeń istnieje wyłącznie jako funkcja dwóch elementów, to poddanie jednego z tych

elementów zupełnie innemu reżimowi prawnemu niż poddanie całości musi stwarzać istotne problemy interpretacyjne. Skoro przyjmujemy, że jurysdykcji państwa podlega położony na jego terytorium serwer, to istnieją dwa niewspółmożliwe skutki tego założenia. Możemy więc założyć, że państwo to wykonuje swoją zwykłą jurysdykcję, przynajmniej co do tej części cyberprzestrzeni, która jest uzależniona od istnienia tego serwera. Najprostszy stan faktyczny ilustrujący to założenie to istnienie strony internetowej, umożliwiającej przesyłanie plików i komunikację bez konieczności rejestracji użytkowników, gdzie pliki i wiadomości po wysłaniu przez nadawcę, oczekują na odbiór na serwerze. Jeżeli państwo skorzysta z podstawowego uprawnienia, które daje mu jego jurysdykcja nad tym serwerem i wyłączy go, działanie w ramach tej jurysdykcji zwykłej wpłynie bezpośrednio na cyberprzestrzeń jako taką. Co więcej, jeżeli serwer nie zostanie tylko wyłączony, ale zniszczony (zgodnie z prawem krajowym), to pliki wyłącznie na nim przechowywane przestaną istnieć. Państwo, które serwer zniszczyło działało legalnie, a jego działania wywołały skutek tylko w samej (uznawanej za niepodlegającą jurysdykcji) cyberprzestrzeni. Jeżeli więc legalne wykonywanie własnej jurysdykcji zwykłej obejmuje przedmioty nie objęte tą jurysdykcją, to musi to prowadzić do wniosku, że jurysdykcja ta w jakiś sposób obejmuje je w sposób nadzwyczajny pod warunkiem ich powiązania z fizycznym serwerem znajdującym się na terytorium państwa. Taką interpretację zdaje się przyjmować Grupa Ekspertów, w *Rule 1 Tallinn Manual*[40] przyznając państwom jurysdykcję nad aktywnościami powiązanymi z tą (położoną na danym terytorium) infrastrukturą.[41] TM przyjmuje analogię z prawa morza do prawa cyberprzestrzeni, wskazując że mamy w przypadku danych związanych z serwerem położonym na określonym terytorium do czynienia z czymś w rodzaju cyfrowych "wód terytorialnych", które pomimo faktycznego pozostawania elementem otwartego morza (nie sposób bowiem dokonać faktycznego rozgraniczenia wód) są jednak z prawnego punktu widzenia traktowane jak terytorium państwa a nie morze otwarte.

[40] zob. Rule 1 *TM. t*akże Rule 1-4 TM 2.0

[41] *States may exercise sovereign prerogatives over infrastructure located on their territory as well as activities associated with that cyber infrastructure* [w Rule 1:*Tallin Manual* wraz z komentarzem par. 1 *in fine*.także Rule 1 *Tallinn Manual 2.0,* wraz z komentarzem par.1]

Podobnie też wyglądają konstrukcje wyłączeń. Tak jak jednostki morskie mają prawo do korzystania z prawa swobodnego przepływu przez wody terytorialne, tak wolno w podobnie swobodny sposób przesyłać dane korzystając z serwerów położonych na terytoriach innych, suwerennych państw. Identycznie jak jednostka korzystająca z prawa swobodnego przepływu, użytkownik sieci decydujący się na przesłanie tych plików musi liczyć się z możliwością ich skontrolowania czy wykonania swojej suwerenności w inny sposób przez państwo na którego terytorium łącza tranzytowe są położone. Taka interpretacja *Rule 1* obarczona jest jednak poważną wadą. Po pierwsze, informatyczna część cyberprzestrzeni, jak wskazano powyżej, nie podlega niczyjej jurysdykcji. Nie ma natomiast żadnych wątpliwości, że wody terytorialne państwa jurysdykcji podlegają a analogia ta jest nieuprawniona. Identyczne wątpliwości, paradoksalnie, wydaje się mieć sama Grupa Ekspertów, ponieważ w dalszej części przywołanego wyżej komentarza wskazuje, że nie mogła osiągnąć konsensusu, czy umieszczenie programu *malware* (przykładowo zbierającego dane, których gromadzenie może prowadzić do przestępstw, ale nie wywołującego aktywnie szkód) jest czy nie jest naruszeniem suwerenności.[42]

Argumentacja za poszczególnymi stanowiskami nie została wskazana, ograniczono się wyłącznie do informacji, że nie została rozstrzygnięta. Jeżeli jednak spróbujemy odtworzyć argumentację Grupy, znajdziemy wyłącznie dwa możliwe powody, dla których naruszenie (wyłącznie cyfrowej) integralności systemów informatycznych innego państwa, nie powodujące strat lub innych skutków w świecie materialnym, nie powoduje naruszenia jego suwerenności. Pierwszym z nich może być przyjęcie pewnego progu szkodliwości, podobnie jak czyni to Tallinn Manual 2.0 czy opisany dalej test Schmitta w odniesieniu do naruszeń suwerenności powyżej poziomu użycia siły. Według takiego poglądu, instalacja malware nie narusza suwerenności, ponieważ jej szkodliwość nie jest wystarczająca. Drugim jest natomiast przyjęcie, że państwo w swoich systemach w cybernetycznej części nie jest suwerenne, ponieważ suwerenność w stosunku do samych zapisów cyfrowych nie istnieje. Wobec tego, co

[42] *The International Group of Experts could achieve no consensus as to whether the placement of malware that causes no physical damage [...] constitutes a violation of sovereignty.* [w: ibid par. 6]

oczywiste, nie ma możliwości jej naruszenia. Należy przyjąć, że Grupa Ekspertów zakłada istnienie przynajmniej jednej z przywołanych wyżej możliwości (lub obydwu naraz). Pogląd przeciwny musiałby bowiem prowadzić do wniosku, że jakiekolwiek naruszenie integralności systemów komputerowych, choćby nawet wspomniana instalacja malware, musi prowadzić do naruszenia suwerenności państwa. Jednakże ten wniosek oznaczałby, że państwo ma bronić tej suwerenności za pomocą własnej jurysdykcji ogólnej (a więc także środkami poza cyberprzestrzenią). To z kolei sytuowałoby tą obronę w luce prawnej. Nie tylko bowiem nie istnieje precedens sądowy, *opinio iuris* ani nawet ugruntowany zwyczaj określający granicę wykonywania jurysdykcji bezpośrednio wobec danych albo sygnałów, ale wręcz prawo zwyczajowe w tej kwestii wydaje się dążyć do dokładnie przeciwnego punktu, a więc braku przyjęcia jurysdykcji nad danymi. Niewątpliwie jednak nieprawdziwy jest pogląd, że ów stan faktyczny wynika z braku technicznej możliwości wykonywania takiej jurysdykcji. Stosowanie zarówno wojskowych jak wywiadowczych i kontrwywiadowczych środków walki elektronicznej[43] jest możliwe i rozpowszechnione. Nie istnieją też żadne przyczyny, które by uniemożliwiały stosowanie identycznych środków w odniesieniu do elektromagnetycznego spektrum tworzącego cyberprzestrzeń. Środki takie mogłyby zostać wykorzystane także do wykonywania bezpośredniego wpływu na informatyczną część cyberprzestrzeni w ramach normowania faktycznego. Problem istnieje więc wyłącznie na płaszczyźnie prawnej.

Wynika z tego wniosek, że pomimo istnienia środków technicznych państwa nie wykonują jurysdykcji zwyczajnej w stosunku do (wyłącznie) informatycznej części cyberprzestrzeni. Ten wniosek potwierdza zarówno zwyczaj jak i *opinio iuris* w tym zakresie. Taką normę należałoby zdefiniować jako *lex generalis* i zasadę doznającą jednak licznych wyjątków. Jurysdykcja wobec danych możliwa jest jednak wyłącznie

[43] Zwyczaj i *opinio iuris* dotyczące zastosowania sensu stricto klasycznych środków walki elektronicznej (jak na przykład zagłuszanie systemów naprowadzających), stanowiących element prawa konfliktu zbrojnego, nie mieści się w zakresie niniejszego opracowania, ze względu na oparcie ich na technologiach nie powiązanych bezpośrednio z cyberprzestrzenią. zob. także *Electronic Warfare* Joint Publication 3.13.-1, US Joint Chief of Staff (2015) par.1

wtedy, gdy stanowią one element większej całości, na przykład przeprowadzanej cyberoperacji i w związku z tym, w istotnym tu zakresie danych *in abstracto*, nie będą modyfikować wskazanego *lex generalis.*

Taka interpretacja każe się z kolei przychylić do głosów, traktujących informatyczną część cyberprzestrzeni jako *res communis omnium,*[44] co potwierdza zasadność przeprowadzenia analogii z prawa morza. Przyjęcie takiej interpretacji dotyczy jednak wyłącznie części informatycznej cyberprzestrzeni, nie rozwiązuje więc kwestii jak należy traktować samą jej infrastrukturę fizyczną. Konsekwentne przyjmowanie zasady *res communis omnium* musiałoby bowiem prowadzić do konstatacji, że państwo nie może, ze względu na istnienie części informatycznej cyberprzestrzeni, wykonywać swojej jurysdykcji w stosunku do obiektu, co do którego normalnie mogłoby ją wykonywać. Nie wydaje się aby jakiekolwiek sposoby usunięcia tej sprzeczności z systemu prawa międzynarodowego były możliwe do zastosowania w praktyce. Działanie takie wymagałoby w praktyce przyjęcia, że urządzenia takie jak serwer należy uznać za element eksterytorialny, nawet rozważając ewentualnie prawo państwa do wykonywania swojej jurysdykcji w sytuacjach szczególnych, takich jak samoobrona. Jednakże wystarczyłoby odłączenie owego przykładowego serwera od cyberprzestrzeni, by natychmiastowo podlegał on jurysdykcji zwyczajnej, obowiązującej na terytorium na którym się znajduje (ze względu na brak powiązania z częścią informatyczną cyberprzestrzeni).

Taka konstrukcja, choć spójna i wyobrażalna z punktu widzenia teorii prawa, niczego by jednak nie rozwiązywała. Prowadziłaby bowiem do absurdalnych skutków faktycznych a co najistotniejsze, odmawiałaby przyznawanej niewątpliwie państwom przez istniejące prawo zwyczajowej jurysdykcji nad wspomnianymi powyżej "aktywnościami powiązanymi z infrastrukturą położoną na ich terytorium". Z tego względu konieczne jest przyznanie państwom pewnej ograniczonej jurysdykcji nad

[44] zob. Heinegg v. W.H. *Legal Implications of Territorial Sovereignity in Cyberspace*[w: zbiorowa, red. Czossek C., Ziolkowski K., Ottis R. *4th International Conference on Cyber Conflict* NATO CCD COE Publications(2012)] ss.9-12. także Departament Obrony USA *The global commons consist of international waters and airspace, space and cyberspace. Globalne dobra wspólne to międzynarodowe wody, przestrzeń powietrzna, kosmiczna a także cyberprzestrzeń* [w: *The strategy for Homeland Defense and Civil Support,* US Department of Defense (2005)par. 12]

częścią informatyczną, jurysdykcji związanej właśnie z prawem do wykonywania jej wobec infrastruktury. Oznacza to, że *sui generis "*cyberprzestrzeń terytorialną", żeby zatrzymać się przy analogii z prawa morskiego, stanowiłby ten fragment informatycznej części cyberprzestrzeni, który istniałby w oparciu o infrastrukturę fizyczną dostępną w danym państwie.

Oczywiście jurysdykcja ta nie może być absolutna. Stosowałyby się do niej liczne wyłączenia, które zostaną szczegółowiej omówione w dalszej części wywodu. Tak więc, można w cyberprzestrzeni wskazać trzy zakresy przedmiotowe, ze względu na stosowalność jurysdykcji zwyczajnej:

(a) część fizyczną cyberprzestrzeni, absolutnie poddaną jurysdykcji zwyczajnej państw opartej na zasadzie terytorialności;

(b) część informatyczną cyberprzestrzeni, poddaną jurysdykcji zwyczajnej państwa (wykonywanej za pomocą normowania faktycznego w ramach *lex informatica)*, w oparciu o zasadę terytorialności rozumianą jako oparcie określonych stref informatycznej części cyberprzestrzeni na elementach jej części fizycznej zlokalizowanej wyłącznie na terytorium jednego państwa;

(c)część informatyczną cyberprzestrzeni, nie poddaną żadnej jurysdykcji a więc traktowaną jako rzecz wspólną..

Należy jednak zauważyć, że na część stanowiącą *res communis omnium* mogą mieć wpływ wszystkie jurysdykcje, jednak w stopniu tak ograniczonym, że żadnej z nich nie można uznać za realnie cyberprzestrzeń wiążącą. Szczegółowo kwestia ta zostanie omówiona w rozdziale dotyczącym normowania faktycznego.

Wyznaczenie trwałych granic (w prawnomiędzynarodowym ich pojmowaniu), poszczególnych wskazanych wyżej elementów cyberprzestrzeni, nie jest rzeczą możliwą.[45] O ile bowiem nie ma wątpliwości, że w istocie mamy do czynienia z siecią informatyczną, w której dochodzi do wymiany informacji pomiędzy fizycznymi jej elementami, o tyle nie można pominąć faktu, że permanentność przekazów danych pomiędzy elementami fizycznej części cyberprzestrzeni przenosi

[45] *Rozumiane jako odpowiednik demarkacji i delimitacji. Chodzi więc tu o sytuację, w której można wskazać (na przykład na podstawie oznaczeń zawartych w kodzie), gdzie znajduje się granica owej „terytorialnej" cyberprzestrzeni.*

ciężar analizy prawnej na jej informatyczną część.

1. c. Specyficzne cechy cyberprzestrzeni

Dalsze prowadzenie wspomnianej powyżej analizy części informatycznej cyberprzestrzeni, wymaga jednak opisania jej trzech istotnych cech, które mają bardzo duży wpływ na tworzenie się normy prawa cyberprzestrzeni. Cechy te muszą być wzięte pod uwagę przy konstrukcji wszystkich norm prawnych dotyczących cyberprzestrzeni, zarówno tych bezpośrednio ją normujących jak i tych, które stanowią *lex specialis* dla norm wiążących tradycyjne normy prawa międzynarodowego z cyberprzestrzenią. Zostaną więc szczegółowo omówione poniżej.

1. c. 1. Anonimowość

Anonimowość w cyberprzestrzeni istnieje w dwóch rodzajach.[46] Pierwszy z nich to anonimowość *sensu stricto* oznaczająca rzeczywistą niemożliwość zlokalizowania osoby dokonującej działania w cyberprzestrzeni a także niemożliwość powiązania nawet śladów tej osoby z tym działaniem. Drugim rodzajem jest tzw. pseudo-anonimowość.[47] Oczywiście z czysto logicznego punktu widzenia anonimowość jest pojęciem binarnym, pseudo-anonimowość to tyle co pełna identyfikowalność. Jednakże z punktu widzenia praktycznego pseudo-anonimowość należy odróżnić od identyfikowalności. Po pierwsze bowiem cyberprzestrzeń nie gwarantuje absolutnie rozumianej anonimowości nikomu.[48] Stopień skomplikowania działań i specjalistycznej wiedzy wymagany do dokonania identyfikacji określonego użytkownika cyberprzestrzeni jest jednak tak duży, że osoba starająca się ukryć swoją tożsamość przy pomocy środków anonimowości *sensu stricto* prawdopodobnie

---

[46] zob. m. in. du Pont G.F. *The Criminalisation of True Anonymity in Cyberspace* Michigan Telecommunications and Technology Law Review tom 7:191 (2001) ss.191-215

[47] *Chawki M. Anonimity in Cyberspace: finding the Balance between the Privacy and Security,* Droit-Tic (2006) ss.13-7

[48] zob. *Lidsky L.B. Anonymity in Cyberspace: What Can we Learn from John Doe?* Boston College Law Review 50 (2009) s.1373

odniesie sukces. Niemniej należy zauważyć, że samo zachowanie anonimowości w informatycznej części cyberprzestrzeni, choć technicznie najprostsze - nie musi być wystarczające.[49] Możliwe jest bowiem złamanie zabezpieczenia, a co za tym idzie ujawnienia tożsamości danego użytkownika przy pomocy elementów fizycznej części cyberprzestrzeni.

W związku z niemożliwością rozdzielenia części informatycznej i fizycznej cyberprzestrzeni, najsłabszym ogniwem każdego łańcucha przypisania będzie zawsze człowiek. W związku, z tym należy uznać, że z punktu widzenia jurysdykcji obejmującej - co oczywiste - całość cyberprzestrzeni, anonimowość doskonała nie może istnieć. Natomiast narzędzia umożliwiające ją w zakresie samej części informatycznej, będą podlegały kontroli w ramach opisanego poniżej normowania faktycznego. Nie wpływa to jednak na fakt, iż szansa na przeprowadzenie takiej identyfikacji jest niezerowa. Tymczasem pseudo-anonimowość swoje źródła ma nie tyle w środkach technologicznych co w prawie. Chodzi tu bowiem o sytuację, w której środki techniczne uniemożliwiają identyfikację danego użytkownika cyberprzestrzeni, posiadającego odpowiednie narzędzia do ochrony swojej tożsamości, jednakże w odniesieniu wyłącznie do części pozostałych podmiotów .Przykładem takiej anonimowości może być sytuacja, w której państwo na portalu stanowiącym elektroniczną wersję publikatora prawnego udostępnia moduł komentarzy, pozwalający obywatelom na wyrażanie swoich opinii co do stanowionego w tym państwie prawa. Anonimowość użytkowników tego modułu jest chroniona przed innymi użytkownikami, jednakże organy tego państwa mają dostęp do danych wrażliwych. Jeżeli jeden z komentujących zacznie nawoływać do aktów terroryzmu jako protestu przeciwko promulgowanej ustawie lub innych czynów przestępczych, jego tożsamość może zostać natychmiastowa przekazana odpowiednim organom. Co istotne, w razie ewentualnego procesu, nie będzie on mógł podnieść, że miał on pozostać anonimowy, ponieważ prawo nie gwarantuje mu absolutnej nieidentyfikowalności a wyłącznie pewien jej zakres.

---

[49] *zob. Loshin P. Practical Anonymity: Hiding in Plain Sight Online Syngress,* WalthamElsevier Science (2013) ss. 10-5

Podstawową różnicą w tej sytuacji w porównaniu do ścisłej anonimowości w cyberprzestrzeni jest fakt, że użytkownik ten (ani żaden inny) nie był nigdy technicznie anonimowy. Prawo gwarantowało mu wyłącznie, że państwo zobowiązuje się do nieujawniania zarejestrowanych danych osobom trzecim lub wykorzystywania w normalnym obrocie prawnym pod pewnymi warunkami.[50] Ten rodzaj cyberprzestrzennej anonimowości w oczywisty sposób pozostaje poza zakresem zainteresowania niniejszego opracowania i został wspomniany wyłącznie dla zachowania kompletności wywodu.

Ścisła anonimowość[51] natomiast będzie miała fundamentalne znaczenia dla rozważań dotyczących przede wszystkim prawa międzynarodowego. Wszelkie bowiem aktywne działania mające na celu ochronę interesów podmiotów prawa międzynarodowego uzależnione są od dokonania atrybucji naruszeń tych interesów. Cyberoperacje są więc historycznie najbliższe swoistej międzynarodowej ”zbrodni doskonałej”, której przypisanie (a co za tym idzie wykonanie prawa do obrony) nie będzie możliwe. Przypisanie odpowiedzialności jest jednym z głównych problemów współczesnych działań w cyberprzestrzeni. Pomimo istnienia rozpowszechnionej opinii, że do cyberprzestrzeni stosuje się funkcjonujące normy oparte na Karcie Narodów Zjednoczonych, zdolność do wykonywania gwarantowanego przez nią[52] prawa do samoobrony, ogranicza właśnie atrybucja.

Problem atrybucji stwarzał liczne problemy już w klasycznym prawie międzynarodowym. W przypadku działań cyfrowych, często pozbawionych jednoznacznych śladów, możliwych do wykonania z dowolnego miejsca na świecie, a także często dokonywanych przez aktorów niepaństwowych niemożnośc atrybucji faktycznie paraliżuje możliwość wykonywania wielu aspektów prawa

---

[50] *zob. Także* Branscomb A.W. *Anonymity,Autonomy and Accounatability: Challenges to the First Amendment in Cyberspaces*, Yale Law Journal 104:7 (1995). ss.1639-50 Artykuł wskazuje nawet, że niezależnie od poziomu tych zabezpieczeń, kryptologiczne zabezpieczenia prywatności ‘nie powinny być mylone z kwestią prawdziwej anonimowości w cyberprzestrzeni.

[51] Dla uproszczenia, w dalszej części rozprawy pod pojęciem ‘anonimowości’ rozumiana będzie anonimowość w sensie ścisłym, chyba że wyraźnie zostanie zaznaczone inaczej.

[52] Schmitt. M, Maurer T. *Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?* JustSecurity 5/17 (2017) ss.1-2

cyberprzestrzeni. Dodatkowym problemem jest fakt, że bardzo często atrybucja ta okaże się fałszywa.[53] Standardem działania hakerów jest tworzenie łańcuchów serwerów, przez które łączą się z komputerem stanowiącym właściwy cel.[54] Duża część doktryny zajmującej się prawem nowych technologii problem bagatelizuje, ograniczając się do wskazań, że problemy techniczne z dokonaniem przypisania nie mogą ograniczać działania prawa. Nie wskazuje się jednak, jak te problemy można rozwiązać.[55] Tymczasem prawie absolutna niemożność dokonania atrybucji wymusza zmiany w sposobie wykonywania uprawnień do obrony w cyberprzestrzeni.[56] Każdy z nich wymaga bowiem identyfikacji podmiotów za jakieś działania odpowiedzialnych lub choćby uczestniczących w określonej czynności mającej skutki prawne. Nie chodzi tu więc wyłącznie o przypisanie odpowiedzialności, ale o najbardziej elementarne sprawy - jak choćby wskazanie jakie prawo jest właściwe dla określonego podmiotu czy przedmiotu prawa, określenie *prorogatio fori* czy w ogóle określenie legalności danego zachowania.

Problem atrybucji był doskonale widoczny przy okazji dwóch głównych, albo co bardziej prawdopodobne; najszerzej znanych ataków na fizyczną infrastrukturę należącą do innego państwa przy pomocy cyberprzestrzeni. Pierwszym z nich był atak na syberyjski rurociąg gazowy, należący do Federacji Rosyjskiej, który eksplodował w wyniku naruszenia odpowiedniego działania zaworów; według nigdy jednoznacznie nie dowiedzionego podejrzenia, nastąpiło to w wyniku ataku CIA przy pomocy tzw. bomb logicznych, szczególnej odmiany wirusów komputerowych, zmieniających działanie prostych, programowalnych urządzeń.[57] Drugim przykładem był atak na irańskie ośrodki wzbogacania uranu za pomocą wirusa *Stuxnet* .[58]

---

[53] zob.Klimburg A. *The Darkening web:war for cyberspace,* Penguin editions, London, New York(2014), s. 188 i n.

[54] Shackelford J., Anders R.B. State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem [w:zbiorowa, red. Czosseck C., Podins K. Conference on Cyber Conflict Proceedings, CCD COR Publications (2010)ss.201-7]

[55] zob.Klimburg A. *The Darkening Web*..s.190 i n.

[56] por. Kuerbis B. *Defusing the cybersecurity dillema game through attribution and network monitoring*, Georgia Tech School of Public Policy; IGP 2018

[57] Melito S. *Cyber War and the Siberian Pipeline Explosion*, Defence and Security Alert 7/2019 (2019 s.1

[58] Jansons J. *Was Stuxnet an Acto of War* Lessons Learned and Conflicts History, Baltic Defence College t. 4 (2017) ss.118-121

Ponieważ dokumenty dotyczące obydwu tych incydentów są ciągle objęte klauzulami tajności, prawdopodobieństwo, że to właśnie brak możliwości przeprowadzenia właściwego procesu atrybucji był przynajmniej jednym z powodów, dla których Iran i Federacja Rosyjska nie zdecydowały się na podjęcie jakichkolwiek kroków prawnych w tej sprawie jest bardzo wysokie.[59] Anonimowość cyberprzestrzeni stanowi więc sama w sobie element ułatwiający naruszenia suwerenności i w konsekwencji prowadzący do jej osłabienia.

Problemy z atrybucją wynikają oczywiście z samej konstrukcji cyberprzestrzeni. Jednym z podstawowych narzędzi jej wykonywania (choć nie niezawodnym, co zostanie opisane w dalszej części niniejszego rozdziału) jest przypisanie na podstawie numerów tzw. *Internet Protocol (IP)* i połączonych z nimi nazw. Organizacją prowadzącą katalog numerów IP jest *IANA*, aktualnie stanowiąca część *ICANN*, podmiotu prawa prywatnego. Numery IP pełnią rolę swoistego łącznika pomiędzy nazwami domen, wyrażonymi alfanumerycznie[60] a przypisanym im miejscem na serwerach. Sterują więc niejako przepływem informacji w cyberprzestrzeni. Z tego powodu określenie prawdziwego numeru IP pozwala na dokonanie precyzyjnego przypisania. Numery te nadawane były początkowo przez rząd Stanów Zjednoczonych, który delegował to zadanie poprzez podpisanie kontraktu prawa cywilnego ze stowarzyszeniem *IANA*, przejętym później przez powołane przez podmioty zarówno prawa publicznego jak i prywatnego stowarzyszenie *ICANN*. Należy jednak zwrócić uwagę, że tzw. *Affirmation of Commitments*[61], czyli dokument określający zasady współpracy pomiędzy *ICANN* a rządem Stanów Zjednoczonych, skonstruowany w fazie partnerstwa publiczno-prywatnego był mocno krytykowany jest za jego wątpliwą moc prawną. Duża część doktryny amerykańskiej wyraża wątpliwości, czy można ten dokument w świetle amerykańskiego prawa[62] uznawać

---

[59] por. Brown G.*Why Iran Didn't Admit Stuxnet Was an Attack* Joint Forces Quaterly nr 63 4/2011

[60] DeNardis L. Protocol Politics:The globalization of Internet Governance Massachusets Institute of Technology Press, 1st edition (2009) ss.12-9; 220-8

[61] por. Affirmation of Commitments by the United States Departament of Commerce and the Internet Corporation for Assigned Names and Numbers.sygnowane 30 września 2009 roku, przez rząd Stanów Zjednoczonych i Prezesa ICANN.

[62] zob. Froomkin A.M. *Almost free: An analysis of ICANN's 'Affiramation of*

za wiążącą umową cywilno-prawną, po tym jak w 2016 roku *ICANN* stało się podmiotem prawa prywatnego, pozbawionym wpływów rządowych, co w praktyce wyjęło podstawową metodę monitorowania przepływu danych spod kontroli państw narodowych. Początkowo zasada ta doznawała wyjątku. Zgodnie z podstawowymi dokumentami, określającymi podstawę prawną działania *ICANN* - *Memorandum of Understanding*[63] i *CRADA,*[64] zawartymi pomiędzy Departamentem Komunikacji Stanów Zjednoczonych USA i *ICANN*, domicylem tej ostatniej były Stany Zjednoczone.[65] Wspomniane umowy gwarantowały bowiem Stanom kontrolę nad *ICANN*, poddając ją amerykańskiej jurysdykcji i gwarantując, że ICANN będzie funkcjonował jako podmiot prawa tego kraju, ze szczególnym uwzględnieniem stosowania amerykańskiej infrastruktury[66] i będzie stosował prawo amerykańskie w ramach wyboru prawa w stosunkach z osobami trzecimi. Ta umowa jednak przestała obowiązywać w 2016 roku.[67] Pomimo iż *ICANN* pozostał formalnie organizacją non-profit zarejestrowaną w stanie Kalifornia, nie jest poddany żadnej formie kontroli ze strony rządu USA.

Niejasny status *ICANN* był wielokrotnie poddawany krytyce, proponowano także inne rozwiązania problemu przyznawania adresów internetowych. Indie proponowały powstanie specjalnego komitetu Organizacji Narodów Zjednoczonych, zajmującego się wyłącznie regulacją światowego ruchu internetowego.[68] Model kontroli domen przez *ICANN* był także krytykowany przez Francję, Iran, Federację Rosyjską i Chiny.[69] Jednakże żadna z alternatywnych propozycji nie wyszła nigdy poza

---

Commitments',Journal of Telecommunications and High Technology Law 9 (2011) ss.198-200; 214-5

[63] por.Memorandum of Understanding Between the US Departament of Commerce and ICANN (30 września 2000)

[64] Cooperative Research and Development Agreement

[65] zob. Weitzenboeck E. M. - *Hybrid net: the regulatory framework of ICANN and the DNS*- Internatonal Jorunal of Law and Techonolgy 22:1(2014) s. 51

[66] co gwarantowało pełną jurysdykcję zwyczajną nad wszystkimi działaniami ICANN, zgodnie z zasadą terytorialności infrastruktury fizycznej.

[67] por. Moyer E.-*US hands internet control to ICANN*- CNET(2016) ss.1-2

[68] zob. Mueller M.- *A United Nations Committee for Internet-Related Policies? A fair assessment.*- IGP School of Public Policy at Georgia Institute of Technology Press (2011) s.1-2

[69] Gross G. *New ICANN agreement runs into Criticism*, CIO Review 10/09 (2009) ss.2-3

poziom koncepcji. *ICANN* na krytykę[70] odpowiedział wydaniem (wraz z organizacjami powiązanymi) oświadczenia kończącego szczyt tych organizacji, odbywający się w Montevideo.[71]

Oświadczenie to wskazywało konieczność rozwoju dotychczasowego modelu, opartego o współpracę ICANN i IANA, uznając jednak potrzebę modyfikacji modelu zarządzania ICANN na zglobalizowany, oparty o stworzenie rady interesariuszy, składającej się między innymi z przedstawicieli rządów wszystkich państw.

Regulacja prawna ICANN oparty jest o 5 elementów:[72]

I. Prawo prywatne międzynarodwe
II. Prawo publiczne międzynarodowe
III. Partnerstwo publiczno prywatne
IV. własne regulacje ICANN (bylaws[73])
V. *Lex informatica*[74]

Własne regulacje ICANN w praktyce tworzą precedens w prawie międzynarodowym publicznym. ICANN jest bowiem podmiotem prawa prywatnego. Jest więc jasne, że wewnętrzne regulacje takich podmiotów nie mogą stanowić źródła prawa międzynarodowego publicznego i wiązać jego podmiotów. Tymczasem, *bylaws*[75] tworzone przez ICANN wiążą nawet rządy i organizacje międzynarodowe, o ile utrzymują one obecność w cyberprzestrzeni, co jak wskazano powyżej jest koniecznością. Co więcej, dyskusyjne jest nie tylko wyrażenie przez te podmioty

[70] Szczególnie nasiloną po ujawnieniu prowadzonego przez US National Security Agency programu podsłuchowego o kryptonimie *PRISM.*

[71] zob. *The Montevideo Statement on the Future of Internet Cooperation*,ICANN (2013) ss.3-4; także Mueller M. -*The core Internet institutions abandon the US Government*- Internet Governance Project (2013) s.1

[72] zob. Weitzenboeck *Hybrid Net...* s. 63

[73] "bylaws" to specyficzne pojęcie dla anglosaskiego prawa stowarzyszeń. Określa postanowienia wiążące członków danego podmiotu, różniące się od statutu tym, że są to zobowiązanie kontraktowe wynikające ze swoistej umowy pomiędzy członkami danego podmiotu, do której członkowie ci muszą przystąpić. zob. także hasło "bylaws" w West's Encyclopaedia of American Law 2 wyd. The Gate Group (2008) par.1

[74] Pojęcie pierwszy raz użyte przez prof. Lessiga, konstytucjonalisty i specjalisty od prawa internetu z Uniwersytetu Harvarda[w: Lessig L.- *Code and other Laws of Cyberspace*- wyd. 2 Basic Books, Nowy Jork (2006) ss.5-15]; zob. Też Reidenberg J.R. [w:*Lex Informatica...ss.272-3*] wskazujący na analogię z *lex mercatoria.*

[75] *Bylaws For Internet Corporation For Assigned Names And Numbers*- przyjęte przez zarząd ICANN, stan prawny na 27 maja 2018.

zgody na związanie regulacjami ICANN, choćby w sposób dorozumiany[76], ale nawet sama możliwość wyrażenia takiej zgody. Nawet jeżeli przyjmiemy najszerszy z dyskutowanych zakres jurysdykcji zwyczajnej państw w cyberprzestrzeni, to nie można przyjąć, że którekolwiek z państw ma możliwość przyznawania numerów IP lub DNS witrynom, nawet tym działającym w oparciu o położone na ich terytoriach urządzenia infrastrukturalne. Państwo nie może w umowie międzynarodowej przekazać kompetencji, których samo nie ma.[77] Nie można także przyjąć analogii z organizacjami międzynarodowymi regulującymi postępowanie państw w określonych sprawach (jak Unia Pocztowa) czy tworzącymi standardy normatywne (jak Generalna Konferencja Miar). Wspomniane organizacje nie mają bowiem żadnego praktycznego wpływu na działanie państw czy wykonywanie ich jurysdykcji, są powołane wyłącznie w celu faktycznego uproszczenia procedur wykonywania określonych czynności. Na przykład odrzucenie systemu metrycznego przez pewne państwa, miałoby oczywiście określone konsekwencje faktyczne; utrudniłoby handel czy wspólne projekty inżynieryjne z państwami stosującymi ciągle ten system, ale z prawnego punktu widzenia byłoby zupełnie bez znaczenia. Ze stron państw odrzucających ów system byłoby to po prostu wykonanie własnej jurysdykcji, polegające na wypowiedzeniu umowy międzynarodowej, a wszelkie ewentualne problemy rozwiązywałoby tworzenie kolejnych traktatów. Tymczasem wypowiedzenie systemu *ICANN* oznaczałoby nie tylko uniemożliwienie dokonywania atrybucji jakichkolwiek działań oraz kontroli organów ścigania nad działaniami przeprowadzanymi z terytorium tego państwa. (a takie działania niewątpliwie byłoby złamaniem norm karnego prawa międzynarodowego wiążących *erga omnes* i jako takie stanowiłyby akt bezprawny, oznaczający złamanie obowiązku wykonania jurysdykcji), ale także uniemożliwiałoby łaczenie się tego państwa z cyberprzestrzenią w sposób płynny. W efekcie, państwo to ponosiłoby wszystkie

[76] Zasady interpretacji jako wiążących oświadczeń umocowanych przedstawicieli państw regulują zasady określone przez Stały Trybunał Sprawiedliwości w tzw. Sprawie Ihlena- *Legal status of Eastern Greenland* (Den. v. Nor.) 1933 PCIJ ser. A/B n. 53 z wyrokiem z dnia 5 września 1933 roku i późniejsze *jugde-made law* w sprawie.

[77] zgodnie z fundamentalną zasadą prawa rzymskiego *nemine ad alium plus iuris transfere potest quam ipse habet*- [zob. Komentarze jurysty Ulpiana do Edyktów (Digesta Justiniana 50.17.54)]

negatywne konsekwencje odłączenia od globalnej sieci komputerowej, nie zyskując jednocześnie poprawy własnego cyberbezpieczeństwa. Należałoby więc przyjąć, że przyjęcie owego *sui generis* prawodawstwa *ICANN* jest normą zwyczajowego prawa międzynarodowego. Nie ma wątpliwości, że istnieje również praktyka w tym zakresie, ponieważ do norm *ICANN* stosują się wszystkie podmioty prawa międzynarodowego. Oczywiście istnieje też w tym zakresie *opinio iuris*, ponieważ wspomniane podmioty niewątpliwie wyrażają wolę związania się stanowionymi przez *ICANN* normami, w sposób dorozumiany (poprzez samo korzystanie z tego systemu), i wyraźny (poprzez przyjmowanie i podpisywanie stosownych umów z *ISP* funkcjonujących w strukturze tego podmiotu). Prowadzi to do sytuacji, w której sam *ICANN* - poddany prawodawstwu dwóch państw (Kalifornii i Stanów Zjednoczonych), jednocześnie wiążąc obydwa te państwa (a także pozostałe podmioty prawa międzynarodowego) swoimi normami w innych zakresach normowania. Jednocześnie, od czasu wspomnianego wcześniej rozwiązania umów zakładających nadzór rządu federalnego USA nad *ICANN*, te wzajemne normowania mogą być dokonywane wyłącznie pośrednio. Nie istnieją żadne wspólne więzy prawne pomiędzy *ICANN* a rządami wspomnianych krajów (poza prawem regulującym ogólnie działalność osób prawnych) w zakresie działalności, którą prowadzi *ICANN*, a wspomniana kontrola rządu federalnego Stanów Zjednoczonych, dotyczy wyłącznie regulacji obowiązującej wszystkie podmioty prawne i nie jest w żaden sposób związana z przedmiotową działalnością *ICANN*. Ze względu na doniosłość roli *ICANN* dla społeczności międzynarodowej, ewentualna ingerencja w jej działalność byłaby trudna nawet w zakresie wykonywania przez państwo jurysdykcji zwyczajnej. Potwierdzeniem tej sytuacji może być spór pomiędzy organami Unii Europejskiej a *ICANN* w sprawie *RODO*, dotyczący przyjęcia przez *ICANN* zapisów tego rozporządzenia.[78] Kanwą tego sporu jest prowadzony przez *ICANN* rejestr *WHOIS*, służący do zadawania serwerom rejestrowym zapytań pozwalającym na uzyskanie

[78] Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne Rozporządzenie O Ochronie Danych)- publikacja w Dzienniku Urzędowym UE syg. L 119/1 dalej jako [RODO] lub [GDPR]

skojarzenia *DNS* i *IP*. *WHOIS* zachowuje bowiem wszystkie informacje o serwerach, o które został zapytany.[79] Prowadzenie takiego serwisu stoi w sprzeczności z zapisami RODO, o ile zgodnie z jej zapisami podmiot przetwarzający te dane wdroży odpowiednie polityki przetwarzania i wykona obowiązki informacyjne.[80]W przypadku ICANN obowiązek ten dotyczyłby każdego połączenia wykonanego z jurysdykcji Unii. ICANN musiałby więc albo wykonywać postanowienia RODO wobec nieomal wszystkich połączeń (biorąc pod uwagę wielkość ruchu wykonywanego z krajów członkowskich Unii Europejskiej), albo zaprzestać przyznawania numerów IP dla unijnych urządzeń, co w praktyce oznaczałoby odłączenie Unii Europejskiej od cyberprzestrzeni. Należy też wskazać, że zakres terytorialny RODO może dotyczyć podmiotów w ogóle nie podlegających jurysdykcji zwykłej Unii Europejskiej, o ile prowadzą one jakiekolwiek interesy w jurysdykcji unijnej.[81]

Organy unijne powołane do ochrony danych odmówiły zarówno udzielenia moratorium na stosowanie *RODO* wobec serwerów *WHOIS*, jak i przyjęcia proponowanego przez *ICANN* okresu przejściowego,[82] umożliwiającego *ICANN* dostosowanie się do *RODO*. Skoro z systemu prowadzonego przez *ICANN* zostanie wyłączony tak duży i tak ważny segment domen, biorąc pod uwagę łatwość przeniesienia działalności, system *WHOIS* przestanie mieć jakiekolwiek realne znaczenie. Ten aspekt konfliktu na linii *ICANN* - UE, ma znaczenie także dla formalnego pojmowania jurysdykcji cyberprzestrzeni. Państwa Unii Europejskiej, przyjmując *RODO* w obecnej formie *de facto* rozszerzają własną jurysdykcję na całą cyberprzestrzeń, w jej dzisiejszym kształcie. Bez znaczenia jest fakt, że jurysdykcja ta jest warunkowa, ponieważ tylko podmiot wykonujący jurysdykcję może warunkować ograniczenia jej wykonywania. Sam bowiem fakt spełnienia przesłanek jurysdykcji terytorialnej z art. 3 RODO oznacza że jurysdykcja UE wykonywana jest wobec

[79] *DNS and WHOIS- How it works?*, publikacja własna ICANN(2017) par.1-2

[80] por. art.3 w związku z art.4 w zw. z art. 5 w zw. z art.6 RODO

[81] Art. 3(2) RODO

[82] *Interim Model for Compliance with ICANN Agreements and Policies in Relation to the European Union General Data Protection Regulation- Working Draft for Continued Discussion*, propozycja regulacji na okres przejściowy z dnia 8 marca 2018, przedstawiona przez ICANN Komisji Europejskiej. Ss.2-5

osoby prawnej lub fizycznej, przetwarzającej dane w jurysdykcji, do której stosuje się prawo UE. Jest to niezależne od stopnia rozległości tego podmiotu, o ile dane te zostały pozyskane w związku z działalnością na terytorium UE, lub dotyczą danych jej obywateli. Dodatkowo, *RODO* nie przewiduje ograniczenia czasowego. UE wykonuje więc jurysdykcję co do danych spełniających przesłanki zakresu przedmiotowego *RODO* bez żadnych ograniczeń (jeżeli takie istnieją mogą być usunięte na gruncie *RODO*, przykładowo poprzez jego nowelizację). *ICANN* nie może więc utrzymać dotychczasowego funkcjonowania systemu *WHOIS*, z jednej strony ze względu na jego sprzeczność z normowaniem *RODO*, z drugiej zaś na niemożność ominięcia stosowania jego regulacji, zwłaszcza wobec braku woli UE do jakiejkolwiek ugody z *ICANN*.[83] Należy wskazać, że takie sformułowanie zakresu terytorialnego rozporządzenia jest praktycznym złamaniem zasady wyłączenia cyberprzestrzeni spod jurysdykcji państwowej. UE *de facto* obejmuje zakresem swojego ustawodawstwa podmioty, które mogą w ogóle jej nie podlegać w świecie rzeczywistym, a wyłącznie posiadać związki z podmiotami podległymi temu ustawodawstwu właśnie poprzez informatyczną część cyberprzestrzeni. Jednak wykonywanie obowiązków wynikłych z tego normowania, będzie miało skutek w świecie rzeczywistym. Wydaje się, że spór o *WHOIS* stanie się *de facto* precedensem rozstrzygającym kwestie jurysdykcji w cyberprzestrzeni zarówno materialnie jak i formalnie. Materialna strona odpowiedzi na to pytanie prawne dotyczy stopnia, w jakim podmioty prawa prywatnego mogą faktycznie wpływać na jurysdykcję państw narodowych w kontekście cyberprzestrzeni. Formalnie rozstrzygnięcie to stanowi istotny precedens, w jakim ów wpływ mógłby być wykonywany.

Z powyższego należy więc wnosić, że anonimowość cyberprzestrzeni wpływa dwojako na suwerenność. Po pierwsze, *per se* utrudniając lub w niektórych przypadkach wręcz uniemożliwiając dokonanie atrybucji, znacząco ogranicza

[83] zob. List przewodniczącej tzw. *Article 29 Working Party* (instytucji unijnej chroniącej składającej się z przedstawicieli organów powołanych do ochrony danych osobowych poszczególnych krajów członkowskich, wraz z wejściem w życie RODO zastąpionej przez Europejską Radę Ochrony Danych) (2016) s.1

wykonywanie środków obrony suwerenności przewidzianych przez prawo międzynarodowe, a od atrybucji uzależnione. Po drugie, ze względu na oddanie podstawowej metody identyfikacji podmiotów w cyberprzestrzeni, jaką jest system IP podmiotowi prywatnemu. Ze względu na strukturę *ICANN* i jego niebywale istotną rolę, sprowadzającą się do sprawowania faktycznej kontroli nad światowym ruchem cyberprzestrzennym, a więc także internetowym, wpływanie na jego funkcjonowanie przez państwa czy inne podmioty staje się nieomal niewykonalne. Łatwo to zobaczyć choćby na przytoczonym powyżej w rozprawie przykładzie sporu Unii Europejskiej z ICANN dotyczącym implementacji przez tego ostatniego przepisów RODO. Te same narzędzia, które przydają cyberprzestrzeni cechy anonimowości, spowodowały wyjęcie narzędzi kontroli ruchu cyberprzestrzennego spod kontroli tradycyjnych podmiotów prawa międzynarodowego.

1. c. 2. Wszechobecność informatycznej części cyberprzestrzeni

Wobec ustalenia, że informatyczną część cyberprzestrzeni należy uznać za *res communis ominum*, za zasadne należy uznać pytanie o jej granice. Wszechobecność cyberprzestrzeni może być rozmaicie pojmowana. Zwolennicy prądów transhumanistycznych wskazują, że cyberprzestrzeń stanie się nowym uniwersum.[84] Trwają filozoficzne spory o rzeczywiste granice cyberprzestrzeni, nierozstrzygnięta pozostaje kwestia czy o istnieniu cyberprzestrzeni można mówić, przykładowo w miejscu, przez które przepływają fale służące do przesyłu danych, choć w tym konkretnym miejscu nikt nie ma technologicznych możliwości do ich odebrania czy modyfikowania. Takie jednak rozumienie tej cechy pozostaje poza zakresem prowadzonego tu wywodu. Z punktu widzenia prawa międzynarodowego, najistotniejszą kwestią jest bowiem wpływ tej cechy na suwerenność państw - i w związku z tym na możliwość wykonywania przez nie jurysdykcji. Szybkość przesyłu danychi w informatycznej części cyberprzestrzeni powoduje, że zarówno

[84] por. De Mul J. *Cyberspace Odyssey: Towards a Virtual Ontology and Anthropology,* Cambrgide Scholars Publishing (2010) ss.10-20

położenie podmiotów działających w cyberprzestrzeni jak i odległości pomiędzy nimi przestają mieć znaczenie.[85]

Wszechobecność oznacza więc brak możliwości stosowania do cyberprzestrzeni podziału terytorialnego, obowiązującego w świecie fizycznym. Z dowolnego punktu w cyberprzestrzeni można w każdym momencie wpływać na dowolny inny punkt stanowiący także jej element. Podobnie skutek działania przeprowadzonego w jednym punkcie jest zauważalny w całej cyberprzestrzeni. Relacja ta jest zwrotna, dowolnie wybrany punkt cyberprzestrzeni może się w danym momencie stać celem działania z całej cyberprzestrzeni.

Nie ma jednak wątpliwości, że nawet w informatycznej części cyberprzestrzeni, państwa są obecne *per se*, wyznaczając tam swoiste quasi-suwerenne obszary. Obecność ta może być zupełnie widoczna, (jak choćby witryny rządowe spełniające rozmaite zadania, od oficjalnych publikatorów po cyfryzację administracji publicznej), bądź ukryta - jak infrastruktura do prowadzenia wewnętrznych czy tajnych spraw państwa (np. cyberprzestrzenne środki prowadzenia błyskawicznej komunikacji rządowej czy dyplomatycznej). Łatwo jednak zauważyć, że wpływ państw na owe elementy cyberprzestrzeni, nie jest większy niż jakiegokolwiek innego podmiotu, a wykonywanie co do nich tradycyjnych przejawów suwerenności - niemożliwe.

W świecie rzeczywistym obiekty stanowiące przejaw suwerenności danego państwa, a położone poza jego granicami jak okręty czy misje dyplomatyczne podlegają wyłącznie decyzjom własnego rządu, mogą być w razie potrzeby przenoszone a fizyczny dostęp do nich ograniczany. Co więcej, dostęp ten jest pierwotnie ograniczony w zasadzie do państwa, na którego terytorium się znajdują a którego pozycja międzynarodowa i prestiż zależą od zdolności zapewnienia ochrony przedstawicielstwom państw trzecich, przyjmowanych na własnym terytorium. W razie niemożności wykonania tych obowiązków i wzrostu zagrożenia, państwo wysyłające może wzmocnić ochronę własnych przedstawicielstw lub wręcz je

[85] *zob. Post. D., Johnson D. Law and Borders - The Rise of Law in Cyberspace, 48 Stanford Law Review (1997)* s.1375

ewakuować. Żaden z tych środków nie jest jednak wykonalny w stosunku do własnych ekspozytur cyberprzestrzennych. Wynika to z niemożliwości skutecznego wykonywania jakiejkolwiek polityki granicznej w informatycznej części cyberprzestrzeni. Nie można więc ani chronić ani tym bardziej odwołać z cyberprzestrzeni własnej obecności, która jest narażona na ataki o nieznanej sile i stopniu przygotowania, mogące pochodzić z każdego kierunku. To z kolei jest nie tylko konsekwencją sieciowości cyberprzestrzeni, ale także sposobu, w jaki dane podlegają przesyłowi w jej informatycznej części. Jest to wynikiem technicznej konstrukcji cyberprzestrzeni, mającej korzenie w sieci nazwanej *ARPANET*, sporządzonej według specyfikacji armii USA i służącej do celów łączności wojskowej. Specyfikacje te zakładały, w celu stworzenia systemu łączności jak najbardziej odpornego na zakłócenia[86], oparcie technologii przesyłu danych o rozbicie ich na pojedyncze elementy, bity.[87] Każdy z tych elementów jest przesyłany do określonego adresu IP i zawiera dwie informacje" pewną część pliku, którego jest elementem oraz informację o swoim położeniu względem 'stycznych' z nim pozostałych bitów pliku. Obydwie te informacje, odczytane abstrakcyjnie nie dają żadnych możliwości ich powiązania z określonym plikiem. Elementy te przemieszczają się od numeru IP z którego zostały wysłane do numeru będącego ich celem, omijając serwery niedostępne lub odmawiające dostępu. Nietrudno więc zauważyć, że informacja przestaje istnieć pomiędzy momentem jej wysłania z wyjściowego serwera a momentem dotarcia na serwer docelowy. Z prawnego punktu widzenia ma to dwa istotne skutki. Po pierwsze, nie istnieją żadne narzędzia, które umożliwią wpływ danego państwa na dane, które zostaną przekazane systemom znajdującym się na jego terytorium podczas tego transferu danych.[88] Ewentualne działania wobec pełnej informacji, mogą być podejmowane wyłącznie następczo. Po drugie, wszelkie środki prewencji cybernetycznej muszą więc dla swojej skuteczności być wykonywane zanim państwo uzyska pełną informację co do intencji podmiotu przeprowadzającego

[86] *zob. Yang C. Law Creeps onto Lawless Net, Business Week (1994)* s. 56

[87] zob. LaQuey T. *The Internet Companion: A Beginner's Guide to Global Networking* University of North Carolina (1994) s. 30

[88] Zabezpieczenia informatycznej części cyberprzestrzeni mogą polegać na niedopuszczeniu do połączenia.

operację .[89]

Należy w tym miejscu wspomnieć o licznych głosach, wskazujących na istnienie takiej kontroli, a tym samym o istnieniu narzędzi pozwalających uniknąć naszkicowanych powyżej problemów z ochroną granic cyberprzestrzennych.[90] Opinie te jednak ograniczają się do internetu (a więc wyłącznie niewielkiego wycinka cyberprzestrzeni). Autorzy tych tez przyznają, że do wykonywania tej kontroli stosowane są środki istniejące poza cyberprzestrzenią[91] lub normy wynikające z tradycyjnie pojmowanego prawa międzynarodowego.[92] Zaprojektowanie narzędzi sieciowych filtrujących określone pakiety danych jest technicznie możliwe, ale zabezpieczenia są stosunkowo nieskuteczne i w istocie stanowią bardziej demonstrację celów polityki niż realną ochronę własnych interesów.[93] Należy także zwrócić uwagę, jest brak możliwości zamknięcia granic przez państwa. Te ostatnie nie tylko nie mają skutecznych narzędzi by wykonywać swoje *imperium* w cyberprzestrzeni ale nawet by zakreślić granice, w których mogły by to zrobić.

Konieczne więc staje się zdefiniowanie nowego wymiaru jurysdykcji, wykonywanej w ramach, specyficznego, nowego systemu prawnego, właściwego dla cyberprzestrzeni.[94] Należy tu wskazać, że jeden z pierwszych autorów pojęcia

---

[89] Środki aktywnej obrony obejmują całe spektrum remediów, od tych wymierzonych wyłącznie w samo połączenie naruszające suwerenność do agresywnego kontrataku wymierzonego w systemy naruszającego. zob. Także Hoffman W., Levite A.E., *Private Sector Cyber Defense. Can Active Measures Help Stablize Cyberspace?* Carnegie Endowment for International Peace (2017) ss. 8-12

[90] Tak na przykład.Goldsmith J. Wu T. *Who Controls The Internet?:Illusions Of A Borderless World* Oxford University Press,(2006) s.154

[91] Pozwalają one bowiem na skuteczne kontrolowanie połączeń dokonywanych za pomocą serwerów pełniących rolę pośredników jak na przykład podmioty ISP. Są natomiast bezskuteczne wobec już choćby połączeń peer - to - peer, które oparte są o bezpośrednie połączenie pomiędzy urządzeniem stanowiącym źródło transferu i urządzeniem, do którego połączenie to jest skierowane. zob.Ehlert M. *I2P Usability vs. Tor Usability. A Bandwith and Latency Comparison*, Humboldt Universitaet Berlin(2011) ss. 2-3, także Schimmer L., ZZZ (autor pozostał anonimowy) *Peer Profiling and Selection in the I2P Anonoymous Network*, PET-CON (2009) ss.-1-2

[92] Trend ten widoczny był w orzeczeniach w dwóch najszerzej cytowanych orzeczeniach dotyczących wykorzystywania tradycyjnie rozumianej jurysdykcji zwyczajnej państw w celu powstrzymania naruszeń tejże w cyberprzestrzeni, tj w sprawach Yahoo!, Inc. v. La Ligue Contre Le Racisme et L'Antisemitisme, 145 F.Supp. 2d 1168, 1171 (N.D. Cal. 2001) a także rozpoznaną przez Sąd Najwyższy Australii sprawę Dow Jones Company Inc. v. Joseph Gutnick, HCA 56, 210 CLR 575(2002), dotyczące zastosowania prawa australijskiego wobec firmy amerykańskiej naruszającej to prawa w wyłącznie w cyberprzestrzeni.

[93] zob. Ehlert M. *I2P Usability...* s.4 i n.

[94] Chodzi tu o definicję suwerenności i jurysdykcji spełniającą kryteria *lex informatica*.

wszechobecnej cyberprzestrzeni, uznaje tę właśnie cechę nie za przyczynę stosowania państw wobec cyberprzestrzeni (które dążyłyby w tym ujęciu po prostu do wykonywania własnych interesów w jej informatycznej części) a właśnie za jej skutek (uznając, że niejako państwa - tworząc cyberprzestrzeń same decydują się na utratę części własnych kompetencji, zgadzając się z tym, że będą musiały się w tych zakresach liczyć z innymi użytkownikami cyberprzestrzeni).[95] Nie sposób się z tym poglądem zgodzić. Zakłada on bowiem, z logicznej konieczności pełną kontrolę wszystkich państw nad cyberprzestrzenią (przynajmniej na samym początku jej istnienia).

Istnieją jednak mocne przesłanki by przypuszczać, że nie tylko kontrola taka nigdy nie istniała, ale wręcz że państwa nie są do istnienia cyberprzestrzeni niezbędne. Wskazana więc powyżej koncepcja suwerenności istniejącej w *lex informatica*, jest nie tyle wynikiem jakiegoś określonego sposobu stosowania już istniejącego prawa międzynarodowego przez jego podmioty, co wypełnieniem luki prawnej, której istnienie uniemożliwia państwom wykonywanie swoich podstawowych obowiązków. Jednym z kanonicznych przykładów, podawanych w literaturze informatycznej jako dowód na istnienie takiej luki jest przypadek Dana Kaminskiego,[96] specjalisty od bezpieczeństwa informatycznego. Odkrył on niezwykle istotny błąd protokołu DNS.[97] Zapomniawszy pewnego dnia zabrać swojego przenośnego modemu, w celu uzyskania dostępu do szerokopasmowego internetu, spróbował on identyfikacji swojego łącza za pomocą numerów IP kawiarni do której regularnie chodził w celu

---

zob. Trakman L. *The Law Merchant : The Evolution of Commercial Law* Fred B. Rothman Publishing (1983) ss. 1-2, także Johnson and Post,*Law*... . par. 13

[95] Herrera G.L. *Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space 12* wykład wygłoszony na 47 konwencji rocznej Towarzystwa Studiów Międzynarodowych (ISA Convention),[w: zbiorowa, red. Cavelty M.D., Mauer V., Krishna- Hensel S.F. *Power and Security in the Information Age*,Routledge(2008) s.6).Herrera wskazuje, że rozwój *ICT (Information and Communications Technologies)* nieuchronnie powoduje globalizację informacji, a co za tym idzie coraz dalej idące wyłączanie tych dziedzin życia spod jurysdykcji państw.

[96] zob. Olney M., Mullen P., Miklavcic K. Dan Kaminsky;s *2008 DNS Vulnerability*, Sourcefire Vulnerability Reseearch Team Report, Sourcefire Inc. (2009) s. 4

[97] Chodzi tu o system pozwalający na tłumaczenie alfanumerycznych adresów domen cyberprzestrzennych na języki naturalne. Ponieważ DNS jest elementem całego systemu przyznawania domen, pozostaje pod kontrolą ICANN. zob.Postel J., Zaw-Sing S., *The Domain Naming Convention for Internet User Applications*, Network Working Group (1982) ss.2-5

uzyskania połączenia z jej darmowym Wi-Fi. Kaminsky, analizując później własne działania, doszedł do wniosku, że identyczny mechanizm pozwala na włączenie się do dowolnego systemu na świecie, wliczając w to witryny rządowe. Dzieje się tak ponieważ konstrukcja systemu DNS[98], służąca do identyfikacji danej strony opiera się o tzw. Strefy, których zadaniem jest łączenie numerów IP przyznanych danej witrynie z identyfikującymi je nazwami udostępnianymi użytkownikom końcowym. System przyjmuje jednak identyfikację niejako na wiarę. Wystarczy więc zgłoszenie prawidłowego (choć nielegalnie uzyskanego) numeru DNS, by system uznał chcący uzyskać dostęp do systemu komputer za wiarygodny i połączył go z określonym innym serwerem.[99] W praktyce odkrycie to umożliwiało Kaminskiemu przekierowanie ruchu z dowolnej strony opartej o dowolny serwer DNS (czyli co do zasady z dowolnej witryny aktywnej w cyberprzestrzeni, a nie tylko w internecie) na własny komputer a także uzyskanie wpływu na ten ruch, Miał on na przykład wgląd w pakiety adresowe, wskazujące skąd i dokąd przesyłane są określone dane, a także możliwość ingerencji w dane zlokalizowane na innych serwerach.

Podmiot stosujący metodę, którą opracował Kaminsky, miałby realną możliwość uzyskania dostępu do dowolnej lokalizacji w cyberprzestrzeni, a w efekcie uzyskania z nią bezpośredniego połączenia z dowolnej innej lokalizacji. Łatwo więc zauważyć, że do delimitacji granic cyberprzestrzennych konieczne byłoby wprowadzenie istotnych zmian do systemu przekierowań w cyberprzestrzeni w sposób uniemożliwiający podobne działanie. Pomimo licznych opinii specjalistów w zakresie cyberbezpieczeństwa (wskazujących na liczne niebezpieczeństwa wynikłe z aktualnej konstrukcji systemu DNS) do wprowadzenia znaczących zmian nigdy nie doszło.[100] Wynika to z wyłączenia systemów IP i DNS spod jurysdykcji państwowej. *ICANN*

---

[98] por. Postel J. Zaw-Sing S. *The Domain...* ss.14-7

[99] zob. Wykład Dana Kaminskyego na konferencji informatycznej Black Hat. Także Kernes S.M. *Black Hat: Kaminsky Talks* DNS Enterprise Netwroking Planet (2016) ss.3-5

[100] Grupa największych firm informatycznych, takich jak Microsoft i Cisco wraz z amerykańskim CERT opracowały pakiet zmian po przekazaniu im przez Kaminsky'ego informacji o problemie. Główną osią tego pakietu była zmiana kodowania DNS z 16 bitowego na 32 bitowe, co zwiększyło ilość możliwych numerów DNS, a co za tym idzie utrudniło złamanie identyfikującego daną witrynę numeru. Nie zmienia to jednak samego mechanizmu dostępowego, a wyłącznie oznacza konieczność użycia kopmuetrów o wyższej mocy obliczeniowej do uzyskania dostępu w opisany powyżej sposób. zob. także Vamosi R. *The man who changed internet security*, CNET, (2008) s.1

nie ma bowiem żadnego interesu by zmieniać opisywaną konstrukcję przypisania. Priorytetem organizacji jest otwarta cyberprzestrzeń pozbawiona granic jak i efektywność funkcjonowania systemów przypisania. Musi to oczywiście prowadzić do nierozwiązywalnego konfliktu interesów z państwami, dla których priorytetem musi być jednak ochrona własnej wrażliwej infrastruktury cyberprzestrzennej. Tymczasem dzisiejsza konstrukcja systemów przypisania umożliwia powstrzymanie nawet najbardziej radykalnego działania, za jakie należy uznać próbę odłączenia danego państwa od cyberprzestrzeni przez jego rząd. Każdy odpowiednio przygotowany użytkownik cyberprzestrzeni, działający z dowolnego jej punktu byłby w stanie powstrzymać to odłączenie. Państwo nie ma żadnej możliwości aktywnego przeciwdziałania takiej operacji, o jej sukcesie decydować będzie wyłącznie odpowiednie jej przygotowanie, a więc posiadanie wystarczającej mocy obliczeniowej by przełamać obronę bierną. Sam fakt istnienia takich możliwości każe odrzucić koncepcję Herrery o wszechobecności cyberprzestrzeni pojmowanej jako skutek polityki państw i przyjąć dokładnie przeciwną koncepcję. Wszechobecność cyberprzestrzeni nie tylko jest zupełnie od państw niezależna, ale także stanowi istotne zagrożenie dla ich suwerenności. To właśnie państwa i inne podmioty prawa międzynarodowego zmuszone będą do przyjmowania polityk pozwalających im chronić swoje interesy i wykonywać przynajmniej niektóre przejawy własnej suwerenności w stosunku do przestrzeni, która *per se* pozostaje poza ich kontrolą i mogłaby zupełnie stabilnie bez ich udziału funkcjonować. Za błędne należy uznać (właśnie ze względu na wskazane tu cechy cyberprzestrzeni) poglądy o możliwości realizacji tych polityk przy pomocy ograniczonego pośredniego wpływu na działania rozpoczęte poza własną jurysdykcją.[101] Timothy Wu i Jack Goldsmith wskazują, że

[101] Chodzi tu o sposób realizowania własnych interesów przez państwo, pozbawione jurysdykcyjnych możliwości normowania określonego zagadnienia, poprzez stanowienie we własnej jurysdykcji norm, które pośrednio wypływają na kwestię pierwotną. Kanonicznym przykładem są daleko idące zakazy i sankcje nakładane na własne firmy za sprzedawanie produktów naruszających prawa autorskie, produkowane w krajach pozbawionych sprawnego wymiaru sprawiedliwości. Ponieważ koszty powstrzymania takiej produkcji w innych jurysdykcjach lub powstrzymania w pełni jej przedostawania się przez granicę byłoby niewspółmierne, zakaz obrotu takimi dobrami, czyni cały proceder wielokrotnie mniej opłacalnym. zob. także Levinson D.J. *Collective Sanctions*, 56 Stanford Law Review, (2003)s. 345

identyczna metoda mogłaby być zastosowana przez państwa do kontrolowania przesyłów danych dokonywanych przez użytkowników informatycznej części cyberprzestrzeni, rozpoczynanych poza jurysdykcją danego państwa. Wskazują oni, że ponieważ jakakolwiek interakcja z elementem fizycznej części cyberprzestrzeni musi odbywać się za pomocą pośredników (jak podmioty *ISP*), przynajmniej od granicy państwa.

Działania tego operatora natomiast podlegają normowaniu w ramach jurysdykcji zwyczajnej.[102] Wskazują oni też, że ewentualne wycofanie się przez jakiekolwiek podmioty z działania w danej jurysdykcji z powodu istniejących w niej regulacji jest dowodem na skuteczność jej sfery wykonawczej.[103]

Pogląd taki jest jednak prostą transpozycją opisanego mechanizmu normowania pośredniego do prawa cyberprzestrzeni. Nie bierze on jednak pod uwagę technicznej struktury tworzącej informatyczną część cyberprzestrzeni. Po pierwsze, dowolne dane mogą zostać przesłane za pomocą odpowiedniego rozproszenia tworzącego je ciągu bitów w sposób, który, jak wskazano wcześniej, czyni przechwycenie takiej transmisji niezmiernie trudne. Nie jest także prawdą, że korzystanie z wspomnianych przez Wu i Goldsmitha pośredników będzie zawsze konieczne (choć niewątpliwie najczęściej tak właśnie się dzieje), bowiem możliwe jest dokonywanie połączeń bezpośrednich, jak choćby w sposób opisany powyżej. Nie wydaje się także, by jakiekolwiek regulacje, którym mieliby ci pośrednicy podlegać miały zastosowania do tak skonstruowanego transferu danych, ze względu na brak technicznych możliwości tego pośrednika do rozpoznania z czym ma on w istocie do czynienia. Jeśli pośrednikiem jest duży operator łączy, najczęściej przekazujący miliony tetrabajtów danych w ciągu doby - znalezienie określonego, rozproszonego ciągu danych staje się zadaniem o nieomal zerowym prawdopodobieństwie powodzenia. Istnieje jednak dużo bardziej istotna przyczyna, dla której istnienie poddanych jurysdykcji zwyczajnej pośredników jest nieistotne dla wszechobecnej cyberprzestrzeni. Tą przyczyną jest możliwość wpływania na system regulujący same podstawy funkcjonowania cyberprzestrzeni,

---

[102] Wu T., Goldsmith J. *Who Controls...* s .71

[103] ibid. S. 73 i n.

stanowiące odpowiednik praw natury w świecie rzeczywistym. Dają one tym samym dowolnemu użytkownikowi cyberprzestrzeni, który do tych podstaw uzyskał dostęp możliwość wpływania na interesy podmiotów prawa międzynarodowego. W roku 1998, w niejasnych okolicznościach Jon Postel, inżynier-informatyk z Uniwersytetu Kalifornijskiego i ówczesny kierownik *IANA* poprosił administratorów ośmiu z 12[104] serwerów obsługujących system DNS[105], by przyznali kontrolę nad administrowanymi przez siebie serwerami komputerowi w jego uniwersyteckim laboratorium.[106] Po otrzymaniu zgody, Postel uzyskał kontrolę nad wszystkimi adresami w całej cyberprzestrzeni. Każda zmiana, której dokonał jego komputer, była w czasie rzeczywistym przetwarzana w przez pozostałe systemu DNS, pozwalając mu na faktyczną kontrolę nad całym ruchem w cyberprzestrzeni.[107] Postel uzyskał na przykład pełną możliwość modyfikowania czy kopiowania danych umieszczonych na urządzeniach funkcjonujących w ramach domen .mil czy .gov; uzyskał również dostęp do numerów IP, pozwalających na wejście do krytycznych sieci państwowych, To z kolei umożliwiało mu dokonanie połączenia z urządzeniami stanowiącymi ich elementy przy pomocy mechanizmu odkrytego przez Kaminsky'ego.

Należy jednak uznać za fałszywą, przeprowadzaną przez niektórych komentatorów analogię między działaniami takimi jak wskazane powyżej a teoretycznie możliwym atakiem terrorystycznym na obiekt o znaczeniu strategicznym, na przykład elektrownię atomową. Z punktu widzenia jurysdykcji państwowej bowiem nielegalny jest nie tylko taki atak terrorystyczny, ale nielegalne są wszystkie jego formy stadialne, najmniejsze podejrzenie jego przygotowywania jest przesłanką pozytywną do przyznania służbom kontrwywiadowczym szczególnych uprawnień i uruchomiania licznych porozumień międzynarodowych o współpracy antyterrorystycznej. Tymczasem, to co zrobił Postel, nie tylko było całkowicie legalne *per se*, ale sam zabieg nie wymagał niczego innego niż wewnętrznego przesunięcia kompetencji

[104] Aktualnie jest ich 13.

[105] Których głównym zadaniem jest dokonywanie opisanego powyżej tłumaczenia

[106] Goldsmith J. Wu T. *Who Controls The Internet?:Illusions Of A Borderless World* Oxford University Press (2006) s.29

[107] W dużym uproszczeniu, Postel miał możliwość przekierowywania w dowolny sposób ruchu w cyberprzestrzeni. W przeciwieństwie do Dana Kaminskyego, Postel nie wykorzystywał żadnych luk, a jego działania były w pełni legalne.

przez niezależną instytucję, jaką była *IANA*, w oparciu o *bylaws* tej organizacji. Warto także mieć na uwadze, że następca *IANA*, czyli organizacja *ICANN*, jest już całkowicie niezależną od jakiegokolwiek rządu instytucją opartą na prawie prywatnym. Ewentualne powtórzenie eksperymentu Postela, mogłoby więc zostać wykonane jako wewnętrzna decyzja podmiotu co do organizacji swoich zasobów, na które żadne państwo nie miałoby żadnej możliwości wpływu. O ile więc w okresie istnienia IANA rząd Stanów Zjednoczonych miał pewien ograniczony wpływ na jej działanie (a co za tym idzie, miała też je pośrednio społeczność międzynarodowa), to w przypadku ICANN państwa nie mają żadnej prawnej kontroli nad podstawowymi elementami architektury cyberprzestrzennej. Tymczasem kształt tej architektury decyduje o możliwości ochrony przez te państwa własnej suwerenności. Cyberprzestrzeń bowiem jak zostanie wykazane poniżej jest wszechobecna. Także punkty dostępowe do informatycznej części cyberprzestrzeni (czyli elementy jej fizycznej części), które umożliwiają dostęp do jej całości z jednego punktu(co wynika z jej wszechobecności) , mogą być dowolnie przenoszone. Oznacza to, że na każdy jej element można oddziaływać z dowolnego innego punktu, a więc z dowolnej innej jurysdykcji. O ile jak wskazano powyżej, powstrzymywanie takich działań jest możliwe przy pomocy środków istniejących poza cyberprzestrzenią (jak w przypadku na przykład sprawy *LICRA v. Yahoo!*), w przypadku naruszeń suwerenności *stricte* cyberprzestrzennych, narzędzia te nie są dostępne. W efekcie brak więc prawnych narzędzi, pozwalających na wykonywanie tradycyjnie pojmowanej jurysdykcji wobec zdarzeń prawnych mających źródło wyłącznie w cyberprzestrzeni, ponieważ jej wszechobecność pozwala na obejście tejże jurysdykcji

Drugim aspektem osłabienia jurysdykcji jest status prawny organizacji takich jak *IANA* i *ICANN.* Charakter działalności tych podmiotów, stanowi, że ich rola przypomina rolę organizacji międzynarodowej. Przyznawanie numerów IP a także kontrola nad serwerami DNS stanowią podstawę istnienia cyberprzestrzeni w jej dzisiejszym kształcie, a więc jedno z *global commons.* W konsekwencji organizacje te zyskują bardzo znaczący wpływ na suwerenność i jurysdykcję państw, jednocześnie pozostając poza jakimkolwiek zakresem normowania przez te państwa (lub

organizacje międzynarodowe właśnie). Nie sposób się zgodzić z głosami, że problem ten rozwiązuje pełne poddanie serwerów takich jak te należące do ICANN jurysdykcji terytorialnej państw, w których się one znajdują. Nietrudno zauważyć, że w odniesieniu do fizycznej części cyberprzestrzeni (a element takowej stanowi serwer), jurysdykcja jest wykonywana na zasadach ogólnych. Wobec tego jest ona oparta o zasadę terytorialności, a co za tym idzie - mogłaby być wykonywana wyłącznie w odniesieniu do jednego z serwerów. Natomiast, jak pokazuje eksperyment Postela - byłoby to po prostu niewystarczające z powodów technicznych. Wobec naruszeń integralności danych zastosowanie jurysdykcji nadzwyczajnej, jest niezwykle rzadko stosowanym wyjątkiem, ograniczonym zgodnie z zasadą *exceptiones non sunt extendendae* do sytuacji klarownych, w których państwo domagające się zastosowania takiej formy jurysdykcji byłoby w stanie udowodnić spełnienie odpowiednich przesłanek.[108] Te same dane istnieją bowiem symultanicznie w wielu jurysdykcjach. Efektywne wykonanie jurysdykcji w odniesieniu nich wymagałoby jednoczesnego wykonania jej w odniesieniu do każdej z potencjalnie nieskończonej ilości kopii, co oczywiście możliwe jest wyłącznie teoretycznie. Wynika stąd, że cecha wszechobecności cyberprzestrzeni potencjalnie wyjmuje dowolny jej element spod jurysdykcji zwyczajnej i nadzwyczajnej państw. Rozwiązaniem tego problemu byłoby wyłącznie poddanie serwerów decydujących o architekturze sieci (jak te poddane *ICANN*) specjalnie do tego celu powołanej organizacji międzynarodowej. Rozwiązanie takie niewątpliwie korespondowałoby z uznaniem cyberprzestrzeni za *global commons*.

Nie oznacza to jednak, że państwa nie mogą wykonywać jurysdykcji wynikającej z normowania stanu faktycznego. Jeżeli przyjrzymy się dokładniej opisanemu powyżej eksperymentowi Jona Postela, zauważymy że przejął on kontrolę wyłącznie nad 8 z 12 serwerów. Pozostałe cztery pozostawały pod pełną kontrolą rządu Stanów Zjednoczonych, nie tylko faktyczną, ale także jurysdykcyjną, co pozwalało temu państwu na wykorzystanie cechy wszechobecności na własną korzyść. Kontrolując

[108] Status prawny jurysdykcji nadzwyczajnej ulega znaczącej zmianie w odniesieniu do informatycznej części cyberprzestrzeni, o czym będzie mowa w dalszej części wywodu.

owe serwery, nie tylko mogły dowolnie powtórzyć procedurę opracowaną przez Jona Postela, ale także dysponowały wielokrotnie większą mocą obliczeniową (w oparciu o cztery serwery poddane własnej jurysdykcji), w zasadzie uniemożliwiając innym państwom obronę przed własnymi działaniami. Jest to modelowy wręcz przykład w jaki sposób prawo współdziała z architekturą systemową w epoce *cyberlawfare.*

Stany Zjednoczone dysponowały bowiem zarówno prawną jak i faktyczną możliwością powstrzymania cyberoperacji dokonywanej w ten sposób. Z drugiej jednak strony, mogły one same wykonać dowolną cyberoperację korzystając z opisanej tu luki. Sytuacja prawna państwa, przeciwko któremu byłaby ona skierowana, stawałaby się identyczna, ale sytuacja faktyczna byłaby zależna od tego, czy państwo to ma pod kontrolą jurysdykcyjną jeden z ośmiu pozostałych serwerów czy też nie. Wynika to ze wskazanej już powyżej reguły, według której państwa z rozmaitych powodów nie są w stanie wykonywać swojej jurysdykcji w stosunku do cyberprzestrzeni, jako takiej mając jednak możliwość wykonywania jej w stosunku do niektórych elementów cyberprzestrzeni. Ich pozycja prawna będzie więc różna zależnie od ich faktycznej siły. Wydaje się więc, że nierównomierny dostęp do krytycznej infrastruktury fizycznej cyberprzestrzeni i istnienie wszechobecnej cyberprzestrzeni, stanowi wyłom w dotychczas bezwzględnie obowiązującej w prawie międzynarodowym publicznym zasady równości[109] i w konsekwencji stanowi kolejny argument za poddaniem architektury cyberprzestrzeni nadzorowi międzynarodowemu.

Wszechobecność cyberprzestrzeni *per se* działa na rzecz równości podmiotów prawa międzynarodowego i zwiększenia możliwości ochrony przez nie własnej suwerenności. Każdy z nich ma identyczną możliwość uczestniczenia w cyberprzestrzeni. Możliwość ta jednocześnie niweluje inne nierówności w obrocie międzynarodowoprawnym, jak choćby położenie geograficzne czy znaczące spłaszczenie różnic w możliwości projekcji siły). W połączeniu z możliwościami technicznymi pozostającymi w dyspozycji jurysdykcji zwyczajnej innych państw,

[109] zob. Armstrong S.W. *The Doctrine of Equality of Nations in International Law and the Relation of the Doctrine to the Treaty of Versailles* The American Journal of International Law, 14:4 (1920) ss.540-64

prowadzi to właśnie do uczynienia z prawa środka prowadzenia konfliktu, co stanowi właśnie istotę *cyberlawfare.* Wymogiem efektywnego wykonywania jurysdykcji w warunkach wszechobecnej cyberprzestrzeni, a tym samym ochrony własnej suwerenności jest uzyskanie takiego stopnia zaawansowania technologicznego który gwarantowałby danemu państwu efektywną kontrolę nad interesującymi je aspektami działań w cyberprzestrzeni, przy jednoczesnym zachowaniu tych środków w ramach własnej jurysdykcji zwyczajnej. Skoro bowiem rząd Stanów Zjednoczonych poddał swojej jurysdykcji terytorialnej cztery serwery DNS, to przekazanie kontroli nad nimi *IANA* było aktem suwerennego państwa, które samo mogło ustalić zakres tego przekazania kompetencji. I sam ten fakt był wystarczający, by potencjalnie Jon Postel nie miał żadnej legalnej możliwości uzyskania kontroli nad tymi serwerami. Ewentualna próba dokonania włamania na nie, uzasadniałaby właśnie uruchomienie obiektywnej jurysdykcji nadzwyczajnej i możliwości przeciwdziałania zgodnie z jej normami. Należy tu wskazać, że w aktualnym stanie prawnym, rząd Stanów Zjednoczonych nie jest w stanie zakazać Postelowi przejęcia serwerów DNS[110], tym bardziej nie ma możliwości egzekwować zakazu dokonania eksperymentu, który był on przeprowadził. Pierwsze z tych zachowań wynika bowiem ze swobody działania *ICANN,* drugie natomiast umożliwia sama wszechobecność cyberprzestrzeni. Postel mógł bowiem uzyskać identyczny efekt w oparciu o serwer znajdujący się w innym kraju (nawet fizycznie nie opuszczając terytorium Stanów Zjednoczonych).

W ramach wykonywania swojej jurysdykcji, państwa są jednak w stanie stworzyć narzędzia przeciwdziałania wszechobecności cyberprzestrzeni, a więc remedia, które mogą skutecznie chronić ich interesy, także w sensie prawnym. Należy jednak zauważyć, że o ile remedia te są środkami wynikającymi z prawa, to ich działanie będzie miało raczej charakter faktyczny niż prawny. Ich celem będzie nie tyle zakazanie zachowań takich, jak Postela i stworzenie mechanizmów egzekucji tego zakazu, ile taka konstrukcja własnego, krajowego prawa cyberprzestrzennego, żeby

[110] USA, pomimo braku możliwości ścigania, groziły Postelowi pozwem cywilnym o odszkodowanie za straty finansowe, ostatecznie nigdy jednak owego powództwa nie wytoczono.
zob. Klimburg A. *A Darkening Web:The war for Cyberspace,* Penguin Books, Random House LLC (2017) s. 85 i n.

złagodzić skutki wszechobecności cyberprzestrzeni. Jest to możliwe na przykład poprzez zwiększoną kontrolę nad pakietami danych odbieranych przez serwery położone na własnym terytorium lub też regulację podmiotów *ISP*.

1. c. 3. Cyberprzestrzeń jako miejsce nie podlegające zlokalizowaniu.

Cecha ta także dotyczy wyłącznie części informatycznej cyberprzestrzeni. Część fizyczna oczywiście podlega zlokalizowaniu, ze względu na możliwość określenia miejsca położenia urządzeń istniejących w części fizycznej. Zgodnie jednak z definicją przyjętą na samym początku rozważań do cyberprzestrzeni należą wyłącznie elementy zbioru wspólnego obydwu jej części. Możliwość zlokalizowania jej fizycznej części nie wystarcza więc, by zlokalizować cyberprzestrzeń jako taką. Nie oznacza to jednak, że cyberprzestrzeni nie można uznać za miejsce w sensie prawnym.[111] W istocie praktyka międzynarodowa zmierza ku uznaniu cyberprzestrzeni za jedno z *global commons*[112], a więc terytoriów, do których wszystkie podmioty prawa międzynarodowego powinny mieć równy dostęp. Wynika z tego, że także praktyka międzynarodowa jest coraz bliższa rozpatrywaniu cyberprzestrzeni w kategorii miejsca.[113] Ta praktyka[114] wydaje się rozstrzygającym argumentem w sporze o uznanie cyberprzestrzeni zarówno za miejsce jak i za *commons*.

---

[111] zob. Hunter D. *Cyberspace as Place and the Tragedy of Digital Anticommons,*91 California Law Review 439, (2003), s.453 , także Post D., Johnson D. *Chaos Prevailing on Every Continent:Towards a New Theory of Decentralized Decision-Making in Complex Systems,* 73 Chicago-Kent Law Review, (1998), s.1055

[112] zob. Stang G. *Global Commons: Between cooperation and competition*, Brief Issue 17, European Union Institute for Security Studies, s.1 (2013), także Meyer P. Outer Space and Cyberspace: A Tale of Two Security Realms [w: zbiorowa, red. Osula A.M., Roigas H. International Cyber Norms: Legal, Policy & Industry Perspectives NATO CCD Centre of Excellence(2016)] s.4

[113] Należy zauważyć, że cyberprzestrzeń nie jest miejscem w sensie fizycznym, co oznacza, że przeprowadzenia rozumowania podobnego, które dało początek zakorzenionej już w prawie rzymskim koncepcji rzeczy niematerialnych. zob. Stang G. *Global Commons...,* s. 5

[114] Należy także zauważyć, że także duża część doktryny podtrzymuje pogląd, że cyberprzestrzeń jest miejscem. Niektóre głosy domagają się nawet ustanowienia specjalnych sądów, których wyłączną właściwością miejscową będzie właśnie cyberprzestrzeń. Tak na przykład Perrit Jr. H.H. *Jurisdiction in Cyberspace* 41 Villanova Law Review, (1996),ss. 100-103

Stwierdzenie tego faktu ma doniosłe konsekwencje prawne. Po pierwsze, wpływa ono na sposób dokonywania atrybucji naruszeń suwerenności podmiotów prawa międzynarodowego w cyberprzestrzeni. Te ostatnie muszą być bowiem atrybuowane w samej cyberprzestrzeni. Fizyczne zlokalizowanie podmiotu, który naruszenia dokonał, jest więc możliwe wyłącznie poprzez lokalizację elementu fizycznej części cyberprzestrzeni, z którego naruszenia dokonano. Wynika z tego, że w pierwszym etapie konieczne jest dokonanie atrybucji wyłącznie w informatycznej części cyberprzestrzeni, w drugim zaś powiązanie zlokalizowanego numeru *IP* podmiotu naruszającego z lokalizacją fizyczną. Zgodnie z definicją cyberprzestrzeni, proces atrybucji kompletny jest wyłącznie wtedy, gdy przypisanie dokonane zostanie w obydwu jej częściach.

Ze względu jednak na cechę niemożliwości zlokalizowania, żaden "obszar" części informatycznej cyberprzestrzeni, w tym ten, który uznajemy za podległy terytorialnej jurysdykcji państw, nie może zostać jednoznacznie wskazany bez wiedzy o fizycznym zlokalizowaniu odpowiadającej mu części fizycznej. Oznacza to, że w znaczącej części przypadków naruszeń (kiedy brak tej ostatniej informacji), podmiot dokonujący atrybucji musi odtworzyć cały łańcuch połączeń od urządzenia pod faktyczną kontrolą podmiotu dokonującego naruszenia aż do własnych elementów sieci. Niemożliwość zlokalizowania powoduje więc dalsze komplikacji kwestii jurysdykcji. Skoro bowiem zachowanie w cyberprzestrzeni musi mieć miejsce w jej części informatycznej (nawet jeśli część jego skutków ma później miejsce w świecie rzeczywistym), określenie podmiotów, które czynu dokonały wymaga precyzyjnego określenia terytorialnego położenia infrastruktury fizycznej użytej do przeprowadzenia ataku. Możliwa jest więc sytuacja, w której czyn stanowiący naruszenie suwerenności państwa trzeciego zostaje przeprowadzony przez sprawcę znajdującego się w jednej jurysdykcji, a skutek odnosi w jurysdykcji drugiej - przy czym dokonanie danego czynu następuje wyłącznie w cyberprzestrzeni, a skutki w świecie rzeczywistym wywoływane są pośrednio - nie poprzez sam atak, a wskutek awarii systemu informatycznego, spowodowanego cyberatakiem. Zgodnie z ogólnymi zasadami prawa międzynarodowego stosowanie jurysdykcji nadzwyczajnej (na

przykład do ścigania sprawców zachowania, które w normalnych warunkach nie podlegałoby jurysdykcji państwa ścigającego, gdy sprawcy pozostają poza jurysdykcją państwa, które poniosło szkody) wymaga określenia gdzie sam czyn został dokonany[115]. Czyn dokonany wyłącznie w cyberprzestrzeni, musiałby być więc uznany za niemożliwy do atrybuowania z samej natury. Wynikałoby to oczywiście z faktu, że niemożliwe jest wskazanie miejsca istnienia cyberprzestrzeni jako takiej (ewentualne wykonywanie jurysdykcji nadzwyczajnej w oparciu opartej o *ratione personae* zamiast *ratione locis* uniemożliwiałaby w tym przypadku anonimowość cyberprzestrzeni). Jednocześnie, jak już wskazano, z każdego z elementów części fizycznej dostępna jest (przynajmniej potencjalnie) cała część informatyczna cyberprzestrzeni.[116] Jak z tego wynika, zasada niemożliwości fizycznego zlokalizowania cyberprzestrzeni ma dwie istotne konsekwencje.

Pierwsza z nich to zaistnienie możliwości poddania elementu należącego do eksterytorialnej części informatycznej cyberprzestrzeni jurysdykcji danego państwa na mocy zasady wszechobecności. Element taki może być poddany jurysdykcji zwyczajnej lub nadzwyczajnej, ponieważ państwo może tę jurysdykcję wykonać w stosunku do tego elementu. Do wykonania takiej jurysdykcji nie jest konieczne spełnienie którejś z przesłanek jurysdykcji nadzwyczajnej, ponieważ jurysdykcja ta będzie wykonywana wyłącznie w odniesieniu do cyberprzestrzeni. Przykładem może być przeprowadzenie przez państwo cyberoperacji, mającej na celu usunięcie algorytmu służącego do monitorowania ruchu pakietów danych. Wykonanie takiego działania, należy uznać za w pełni legalne, o ile tylko skutki owego usuwanego algorytmu miałyby miejsce w jurysdykcji państwa, które zamierza ten algorytm usunąć. Wydaje się, że takie pojmowanie jurysdykcji nadzwyczajnej pozwala ją wykonywać w cyberprzestrzeni, pomimo zarówno problemów atrybucyjnych, jak też możliwych trudności z wskazaniem podstawy, na której oparte jest jej wykonywanie. Ponieważ może być ona wykonywana wyłączenie wobec elementów informatycznej

---

[115] zob. Rooney J.M. *The Relationship between Jurisdiction and Attribution after Jaloud v. Netherlands*, Netherlands International Law Review 62-3 (2015) ss.407-28

[116] Luke T.W. *Simulated Sovereignity, Telematic Territoriality: The Political Economy of Cyberspace,* Theory, Culture & Society Conference 2nd ed. (1995) ss.27

części cyberprzestrzeni, nie ma ryzyka nadużycia tego mechanizmu do naruszenia suwerenności (szczególnie w świecie fizycznym) innych państw.

Drugim z wspomnianych wniosków jest konstatacja, że dane położone na serwerze, który sam jest poddany jurysdykcji terytorialnej mogą ulec zniszczeniu w wyniku legalnego działania podjętego przez dane państwo w ramach wykonywania tej jurysdykcji i to pomimo że same dane (rozumiane jako sygnały magnetyczne) nie są tej jurysdykcji poddane. Z drugiej strony, państwo może nie być zdolne do wykonania swojej jurysdykcji zwyczajnej wobec określonych elementów części informatycznej - nawet tych położonych we własnej strefie terytorialnej. ze względu na możliwość potencjalnie nieskończonego kopiowania tych sygnałów, także na serwerach położonych terytorialnie poza ich jurysdykcją. Obydwie te sytuacje wynikają z faktu, że zlokalizowanie elementów należących do części informatycznej cyberprzestrzeni jest niewykonalne (możliwe jest określenie położenie wyłącznie jednej z potencjalnie nieskończonej ilości kopii), a jednocześnie są one osiągalne z każdego elementu części fizycznej cyberprzestrzeni. Dowolne dane są więc faktycznie osiągalne dla jurysdykcji zwyczajnej każdego państwa (ponieważ może ono działać z własnej jurysdykcji).

Zasada niemożności zlokalizowania oznacza więc, że w stosunku do danych istniejących w cyberprzestrzeni możliwe jest wykonywanie jurysdykcji wynikającej z normowania faktycznego lub jurysdykcji nadzwyczajnej, o ile kumulatywnie spełnione zostaną dwie przesłanki: (1) zaistnieje jedna z podstaw jej wykonania, (2) będzie faktycznie możliwe zlokalizowanie określonych danych w cyberprzestrzeni.[117] Konieczne jest odróżnienie tego od pozornie identycznej sytuacji, kiedy w świecie rzeczywistym państwo nie wykonuje swojej jurysdykcji ze względów faktycznych, takich jak na przykład niemożność ustalenia miejsca pobytu sprawcy przestępstwa objętego ściganiem w ramach jurysdykcji nadzwyczajnej, w związku z czym państwo to nie ma możliwości wszczęcia procedury ekstradycyjnej. Taka przeszkoda może

[117] Chodzi tu albo o sytuację ,w której wystarczające jest zlokalizowanie jednej kopii danego pliku - przykładowo, gdy sąd jednego państwa żąda ujawnienia danych w celach dowodowych.

być, w przeciwieństwie do niemożności zlokalizowania konkretnego miejsca wcyberprzestrzeni, usunięta przez prostą zmianę okoliczności. Tymczasem w przypadku cyberprzestrzeni, niemożliwość ta jest pierwotna i wynika właśnie z samej istoty jej konstrukcji.

1. d. Koncepcja suwerenności cyberprzestrzeni.

Konkurencyjną do koncepcji cyberprzestrzeni jako *commons*, była koncepcja cyberprzestrzeni suwerennej. Według jej autorów cyberprzestrzeń miałaby być odrębnym podmiotem prawa międzynarodowego, a jej użytkownicy quasi-obywatelami.[118] U podstaw koncepcji tej leżały poglądy zakładające, że cyberprzestrzeń jest odrębnym od terytoriów państwowych miejscem[119] Założenie takie musiałoby oczywiście w praktyce prowadzić do niezliczonych konfliktów interpretacyjnych i na gruncie prawa międzynarodowego w jego aktualnym kształcie nie mogłoby nigdy zyskać praktycznego znaczenia. W związku z tym, suwerenna cyberprzestrzeń nie była nigdy konstrukcją poważnie rozważaną, nie wspominając nawet o próbach jej praktycznego zastosowania. Niemniej, niektóre wnioski płynące z argumentów na jej rzecz, zostały przejęte do koncepcji *lex informatica* oraz faktycznego normowania cyberprzestrzeni i jak się wydaje, z czasem stają się elementem praktyki międzynarodowej.

Koncepcja ta zostanie krótko omówiona poniżej, ze szczególnym uwzględnieniem przyjętej w niej argumentacji, która później została inkorporowana do systemu *lex informatica.* Fundamentalnym argumentem mającym przemawiać za suwerenną

---

[118] Poza przywołaną już, będącą raczej filozoficznym manifestem, *Deklaracją Niepodległości Cyberprzestrzeni* Johna Barlowa, ściśle prawniczą teorię suwerennej cyberprzestrzeni popierały zasadniczo dwie działające w USA organizacje pozarządowe; *Electronic Frontier Foundation* i *Cyberspace Law Institute*. zob.Johnson D., Post D., *Law and Borders: The Rise of Law in Cyberspace* 48 Stanford Law Review (1996) ss.87, zob. także Wu T.S. *Cyberspace Sovereignty?-The Internet and International System*, Harvard Journal of Law and Technology, 10:3 (1997) ss.662 in.

[119] Założenie to oparte o koncepcję braku położenia informatycznej części cyberprzestrzeni na jakimkolwiek terytorium państwowym pomija jednak fakt, że część informatyczna cyberprzestrzeni może istnieć wyłącznie w oparciu o część fizyczną, a elementy tej ostatniej muszą być umieszczone na terytorium państwa. zob. Też Shen Y. *Cyber Sovereignty and the Governance of Global Cyberspace*, Chinese Political Sciences Review 1/16 (2016) ss. 82-3

cyberprzestrzenią, miałoby być pozytywistyczne pojmowanie suwerenności. Jeżeli bowiem założymy za Austinem[120] i Benthamem[121], że suwerenność to stan przedprawny, a jakiekolwiek ograniczenia wolności muszą wynikać z umowy podmiotów, to w cyberprzestrzeni nie możemy wskazać żadnych podmiotów, które mogłyby takie umowy wobec całości zawrzeć. Powstaje więc w odniesieniu do cyberprzestrzeni pozorny paradoks. Pozytywizm prawniczy oparty o kontynuację myśli *reine Rechtslehre*[122], prowadzi w tym przypadku do powstania *lex informatica*, prawa, które zupełnie wyłącza jakikolwiek normatywizm. Bliższe jest natomiast prawu naturalnemu rozumianemu na sposób średniowieczny. Przyczyną takiego stanu rzeczy jest oczywiście fakt, że próba konstrukcji porządku prawnego w cyberprzestrzeni (w oparciu o zasady pozytywistyczne) musiałaby prowadzić do powstania luki prawnej. Wiąże się ona z zupełną niemożliwością stanowienia prawa według tej koncepcji, wynikającą z braku odpowiednich organów, które mogłyby to prawo stanowić. Jednakże *lex informatica,* jako jedyne źródło normowania, musi oznaczać - podobnie jak w przypadku jego historycznego poprzednika czyli *lex mercatoria* - autonormowanie. Tak jak, niezależnie od rozmaitych nakładających się na siebie jurysdykcji (niewątpliwie wykonywanych przez suwerennych władców) handel w Europie regulowany był przez prawo pozostające poza ich kontrolą, tak dzisiaj cyberprzestrzeń tworzona przez podmioty poddane niezliczonej liczbie rozmaitych regulacji, (które wynikają z także z nakładających się na siebie jurysdykcji) pozostaje w tym ujęciu autonomiczna, czy jak chcą autorzy poglądów uznających teorię suwerennej cyberprzestrzeni - suwerenna właśnie. Suwerenność ta miałaby wynikać właśnie z faktu, że żadna z jurysdykcji, które na cyberprzestrzeń wpływają, nie jest w stanie normować jej w całości - więc pozostaje niejasne, czy w ogóle mamy do czynienia z jurysdykcją, z zasady wykonywaną w sposób niekwestionowany. Oczywiście, “suwerenność cyberprzestrzeni” należałoby w tym ujęciu odróżnić od “suwerenności w cyberprzestrzeni”. To drugie pojęcie odpowiada

[120] zob. Dewey J. *Austin’s Theory of Sovereignty,* Political Science Quaterly, 9:1(1984) ss.32-54

[121] zob. Hart. H.L.A. *Bentham on Sovereignty,* Irish Jurist, 2:2 (1967) ss. 327-35

[122] zob. Kley A., Tophinke E. *Ueberlick ueber die Reine Rechtslehre von Hans Kelsen*, Juristiche Arbeitsblaetter, wyd. 33 nr 2 (2001) ss. 169-74

rozszerzeniu tradycyjnie pojmowanej suwerenności państwa lub innego podmiotu na cyberprzestrzeń. Tymczasem suwerenność cyberprzestrzeni oznaczałaby, że cyberprzestrzeń jest samodzielnym podmiotem prawa międzynarodowego, który dysponuje swoją własną suwerennością, i w koniecznej konsekwencji logicznej - także własną jurysdykcją. Programową ideę suwerennej cyberprzestrzeni po raz pierwszy zaproponował poeta John Perry Barlow[123], późniejszy członek-założyciel *Electronic Frontier Foundation*, amerykańskiej fundacji zrzeszającej zwolenników teorii o niezależności cyberprzestrzeni od państw i tradycyjnego systemu politycznego. Niemniej koncepcja ta, pomimo swoich filozoficznych korzeni, zaczęła być analizowana przez doktrynę prawa międzynarodowego.[124] Założenie 'suwerennej cyberprzestrzeni' miałoby się według jej zwolenników opierać na fakcie niemożliwości jej kontrolowania w pełni, niezależnie od możliwych technicznie ograniczeń, które mogą być nałożone na jednostkę. Jest to więc pogląd, choć niewątpliwie wyrosły na gruncie rozumienia filozofii prawa bliższego naturalistom,[125] zgodny z opisanym wyżej skutkiem konsekwentnego stosowania do cyberprzestrzeni pozytywistycznej teorii suwerenności, choć za pomocą innego ciągu logicznego. Z obydwu bowiem koncepcji musi płynąć wniosek, że ograniczenia, które może państwo na jednostkę nałożyć pozostają w zasadzie bez znaczenia dla istnienia lub nieistnienia cybernetycznej suwerenności państwa. Ta bowiem istnieje zupełnie niezależnie od ograniczeń poszczególnych jej użytkowników, a normy które ich w jakikolwiek sposób wiążą, mogą na nią samą wpływać wyłącznie pośrednio. Z tego faktu obydwie koncepcje wyprowadzają założenie, że suwerenna jest sama cyberprzestrzeń.[126] Nie ma bowiem żadnego podmiotu, który mógłby w stosunku do

---

[123] por. Barlow J. *Declaration of the Independence of Cyberspace,*Electronic Frontier Foundation, Davos (1996) s.1

[124] zob. Post D. *Anarchy, State and the Internet: An Essay on Law-Making in Cyberspace* Journal of Online Law 3:44(1995) s.50,

[125] Argumentacja Barlowa szła tak daleko, że przypisywał, z czym nie sposób się do końca zgodzić, cyberprzestrzeni walor siły natury, *Cyberspace does not lie within your borders [...] It is an act of nature and it grows itself through our collective actions*- Cyberprzestrzeń nie leży w waszych granicach[...] to siła natury, która rozrasta się sama poprzez nasze kolektywne działania [w: *Declaration... s.2]*

[126] Barlow wskazywał nawet,że cyberprzestrzeń ma swoje własne problemy, które rozwiąże poprzez nową umowę społeczną, obejmującą tym razem wyłącznie podmioty operujące w cyberprzestrzeni; *We belive that from ethics, enlightened self-interes,*

całości cyberprzestrzeni wykonywać swoją jurysdykcję. Oczywiście, dla Barlowa wynika to z przeszkód faktycznych[127], dla pozytywistycznej doktryny - z normatywnych,[128] ale zarówno przyczyna jak i skutek pozostają tu tożsame. Zarówno Barlow jak i pozytywistyczni zwolennicy teorii suwerennej cyberprzestrzeni przyjmują, że skoro nie istnieje żadne prawo regulujące cyberprzestrzeń, musi być ona zgodnie ze swoim stanem przedprawnym - suwerenna.[129] Co więcej, wszelkie próby skonstruowania takiego prawa przy pomocy klasycznego *black-letter law* muszą być nieskuteczne, ze względu na brak możliwości ustalenia kto właściwie miałby się z kim porozumieć w celu zawarcia odpowiednich traktatów,[130] w jakiej formie miałyby być one przyjęte i w jaki sposób egzekwowane. Pomimo więc istnienia takich propozycji, do zawarcia podobnego traktatu nie doszło i nie ma żadnych przesłanek by twierdzić, że stanie się to możliwe w najbliższej przyszłości. W ten sposób (poprzez spełnienie zupełnie innych przesłanek) pogląd na cyberprzestrzeń pozytywistów i zwolenników prawa naturalnego w praktyce jest identyczny. Na gruncie argumentacji naturalnej można *in extenso* przeprowadzić rozumowanie, którego skutkiem również jest suwerenna cyberprzestrzeń, ale wymagałoby to pojmowania suwerenności bliższego współczesnemu prawu międzynarodowemu publicznemu, traktującemu suwerenność bardziej jako zbiór

---

and the commonweal, our governance will emerge - wierzymy, że z etyki, oświeconego pojmowania interesu własnego i dążenia do dobra wspólnego będzie wypływać nasza władza.[w: Barlow *Declaration of Independence... ss.3-5]*

[127] Główną nadzieję na suwerenną cyberprzestrzeń widzieli założyciele EEF w realnej niemożliwości państw do wykonywania swojej jurysdykcji w cyberprzestrzeni; *[...]our identities have no bodies so,unlike you, we cannot obtain order by physical coercion[...]- nasze tożsamości nie mają ciał, więc nie podlegamy porządkowi opartemu o przymus fizyczny*[w:Barlow *Declaration...s.3*]

[128] Ponieważ nie ma odpowiednich podmiotów, które mogłby w ogóle zbudować taką władzę, która mogłaby normować cyberprzestrzeń. Takie rozumienie (w odniesieniu do ogólnie pojmowanego prawa międzynarodowego, ale na tym poziomie musimy prawo cyberprzestrzeni traktować jako jako *lex specialis)* szkoły pozytywisycznej świetnie wyraża Oppenheim: *As, however, there cannot be a sovereign authority above the single sovereign state, the Law od Nations is a law between, not above, the single States and is therefore, since Bentham, also called International Law*[w: Oppenheim L. *International Law* 1st ed. Longmans Green & co (1905) s.1

[129] por. Mills A. The Confluence of Public and Private International Law: Justice, Pluralism and Subsidiarity in the International Constitutional Ordering of Private Law Cambrigde University Press (2010)ss.10-5,także Austin J. *The Province...*

[130] Przykładem takiej próby, była francuska propozycja opracowania traktatu o współpracy w internecie, przedstawiona nieistniejącej już Radzie Ministrów UE (której kompetencje przejęły aktualnie Rada Europejska i Rada Unii Europejskiej), tzw. *Karty Międzynarodowej Współpracy w sprawie Internetu*. Propozycja ta nigdy nie weszła w życie.

obowiązków wobec społeczności międzynarodowej.[131] W szczególności chodzi tu o dpowiedzialność za wykonywanie norm wiążących *erga omnes* i wykonywanie wiążących decyzji organów międzynarodowych takich jak agendy Narodów Zjednoczonych. Jednakże wszystkie te koncepcje obciążone są podobnym błędem. Przede wszystkim państwa są zdolne do wykonywania swojej jurysdykcji zwyczajnej w cyberprzestrzeni, także w jej części informatycznej, pomimo wszystkich wcześniej wspomnianych ograniczeń. Kolejną nieusuwalną wadą koncepcji suwerennej cyberprzestrzeni jest brak niezależnego terytorium. Jak już wspomniano cyberprzestrzeń w jej informatycznej części (a to głównie na nią wskazują zwolennicy tezy o suwerenności) może istnieć wyłącznie dzięki oparciu jej o część fizyczną. Nie jest też jasne w jaki sposób cyberprzestrzeń miałaby ową suwerenność wykonywać, wobec faktu, że wszystkie podmioty jej używające istnieją w świecie fizycznym i podlegają jurysdykcji tradycyjnych podmiotów. Autorzy koncepcji suwerenności cyberprzestrzeni zdają się także dokonywać absolutyzacji pewnych stanów faktycznych i uznawać, że: (1) są one niezmienne i (2) są konieczną, logiczną konsekwencją istnienia suwerennej cyberprzestrzeni. Fakt istnienia hakerów, handlu w darknecie[132] czy rozmaitych innych zjawisk cyberprzestrzeni, pozostając *de facto* a w rzadkich wypadkach także *de iure* pozostających poza kontrolą państw i niewątpliwa trudność w pełnym egzekwowaniu własnych praw przez państwa, nie oznaczają jeszcze (jak chcieliby twórcy teorii o suwerennej cyberprzestrzeni), że istnienie tych zjawisk wynika właśnie z tejże niezależności.

Dodatkowo należy wskazać, że suwerenność jest przede wszystkim kategorią prawną. Podobnie jak opisane powyżej problemy z atrybucją same w sobie, nie oznaczają likwidacji suwerenności, tak pewne faktyczne trudności z wykonywaniem jurysdykcji zwyczajnej państw nie mogą być automatycznie transponowane do porządku prawnego. Ogólną zasadą prawa międzynarodowego jest bowiem

---

[131] Tak na przykład Etzioni A.*Sovereignty as Responsibility*, Foreign Policy Research institute, Elsevier ed. (2006) ss.71-5

[132] Chodzi tu o elementy cyberprzestrzeni, niezauważalne dla standardowych przeglądarek, polegające na bezpośrednim, dużo trudniej wykrywalnym łączeniu poszczególnych numerów IP, bez istnienia służących do tego witryn. Termin pochodzi z okresu początkowego rozwoju

wynikanie suwerenności z uznania międzynarodowego.[133] Skoro więc każde państwo uważa, że ma prawo regulować cyberprzestrzeń, nie można mówić o żadnym uznaniu jej suwerenności. Nadto uznanie takie implikowałoby konieczność uznania koniecznych do istnienia cyberprzestrzeni elementów części fizycznej za eksterytorialne. Państwo, na którego terytorium zostały one fizycznie zlokalizowane musiałoby być uznane za *sui generis* państwo przyjmujące w rozumieniu prawa dyplomatycznego. Nietrudno zauważyć, że żadne państwo takiego statusu infrastrukturze cyberprzestrzennej nigdy nie przyznawało. Podobnie sądy poszczególnych państw nie uznawały także cyberprzestrzeni za jakkolwiek suwerenną.

Należy jednak zgodzić się, że wykonywanie jurysdykcji zwyczajnej państw w stosunku do cyberprzestrzeni nie jest jakimś szczególnym wypadkiem, jak w przypadku chociażby okupowania określonego terytorium.[134] Wynika z tego, że sama argumentacja o osłabieniu i redefinicji jurysdykcji państw jest zasadna. Skoro państwa nie mogą wykonywać w całej cyberprzestrzeni własnej jurysdykcji, a stanowione przez nie normy mają na cyberprzestrzeń wpływ wyłącznie pośredni, pozostaje im wykonywanie swojej jurysdykcji faktycznej wobec cyberprzestrzeni[135] i jej wewnętrznego prawa zwyczajowego - *lex informatica*. W ten sposób, państwo może wpływać na efekty działań w tej części cyberprzestrzeni, co do której nie może wykonywać jej bezpośrednio. Działania państw, w szczególności wpływanie na podległe własnej jurysdykcji elementy części fizycznej cyberprzestrzeni, są gwarancją zachowania możliwości wywierania wpływu na kierunki powstawania *lex informatica*, które w istocie będzie tę część cyberprzestrzeni normować. Działania te skutkują przede wszystkim możliwością tworzenia afordancji nakaładających ograniczenia na jednostki - poprzez wprowadzanie zmian w sferze normatywnej dotyczącej cyberprzestrzeni. Mogą one także być wykonywane poprzez traktaty, gwarantujące że

---

[133] zob. Mann F.A. *Recognition of Sovereignty* , The Modern Law Reviewyd. 16 t. 2 (1953) ss. 226-30

[134] zob. Opinię Międzynarodowego Trybnału Sprawiedliwości w sprawie *Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory,* ICJ Reports (2003) s. 428

[135] która nie staje się przez to suwerenna, pozostaje wyłącznie *res communis omnium.*

określone normy znajdą się w porządkach krajowych jak najszerszej grupy państw (i w efekcie zyskają silniejszy wpływ na *lex informatica*) jak i działania faktyczne.

O ile więc łatwo zauważyć, że suwerenność cyberprzestrzeni jest koncepcją chybioną, należy zgodzić się z częścią podawanej na jej uzasadnienie argumentacji, zwłaszcza w zakresie dotyczącym redefinicji jurysdykcji. Poglądy te bez wątpienia stały się początkiem konstruowania współczesnego prawa cyberprzestrzeni, ze szczególnym uwzględnieniem *lex informatica*.

1. e. Koncepcja eksterytorialności cyberprzestrzeni

Fakt, że jak wskazano powyżej cyberprzestrzeń nie jest suwerenna, nie oznacza że cyberprzestrzeń nie może być uznana za eksterytorialną Taka konstatacja koresponduje z zakwalifikowaniem cyberprzestrzeni jako *global commons.*[136] Wynika ono przede wszystkim z uznania międzynarodowego.[137] Istotne jest jednak wskazanie, które z części cyberprzestrzeni można za eksterytorialne uznać. Nie ma wątpliwości, że jakiekolwiek rozważania o eksterytorialności mogą obejmować wyłącznie informatyczną część cyberprzestrzeni, bowiem elementy części fizycznej eksterytorialne być nie mogą. Ze swej natury muszą one być położone na terytoriach państw, które wykonują nad nimi swoją jurysdykcję. To stwierdzenie musi prowadzić do wniosku, że elementy cyberprzestrzeni tworzące jej część informatyczną miałyby stawać się eksterytorialne dopiero w momencie, w którym do cyberprzestrzeni zostaną faktycznie włączone. Byłaby to więc sytuacja analogiczna do rzymskiej koncepcji obejmowania w posiadanie poprzez wyodrębnienie z natury. Tak jak moment wyłączenia z natury, pozwalał (po spełnieniu pozostałych warunków) objąć

[136] Przypisanie cech *commons* cyberprzestrzeni wydaje się być zasadne ze względu na powszechny i niejako 'ponadjurysdykcjny' dostęp do niej. Niemniej, problem ścisłej terytorialności jej fizycznej części pozostaje aktualny. Wydaje się więc, że cechy *res communis* można przypisać wyłącznie informatycznej części cyberprzestrzeni. zob. Także Marchetti R. *Modes of Governance for the Global Commons*[w:zbiorowa, red. Catalano C., *Global Commons: threat or opportunity*, Finmeccanica (2013) ss. 14-8]

[137] Pierwszym podmiotem prawa międzynarodowego, który wyraźnie przyjął koncepcję cyberprzestrzeni jako *res communis omnium* było NATO, uznające za konieczny element swojej doktryny opracowanie działań mających na celu zapewnienie nieprzerwanego dostępu do cyberprzestrzeni członkom sojuszu. zob. Barrett M., Berford D., Skinner E., Vergles E.*Assured Access to the Global Commons*, Supreme Allied Command Transformation, North Atlantic Treaty Organization, Norfolk (2011) ss.36 i n.

daną rzecz w posiadanie, tak moment włączenia do cyberprzestrzeni, jest tym, w którym spełniona zostaje przesłanka eksterytorialności. Część informatyczna cyberprzestrzeni dzieli się więc na eksterytorialną i terytorialną. Część terytorialna jest jednak fizycznie nie do odróżnienia od części eksterytorialnej. Jest to sytuacja analogiczna do istniejących w prawie morza pojęć morza terytorialnego i stref przyległych.[138] W odróżnieniu jednak od tamtych, zakres "terytorialności, będzie wyznaczany przez położenie środków technicznych i znaczenie owej strefy dla podmiotów prawa międzynarodowego. Należy pamiętać, że każde istniejące połączenie z cyberprzestrzenią należy uznawać przesłankę uznania danego urządzenia za jej element.[139] Za poddane jurysdykcji terytorialnej należy niewątpliwie uznać domeny *.gov, .mil* i tym podobne, stanowiące cyfrowe agendy państw.

Dane tam bowiem zawarte, dotycząc bezpośrednio spraw państwowych (na przykład służąc jako środek załatwiania spraw konsularnych), muszą więc być traktowane jako swoista ekspozytura interesów państwa, a ewentualny atak na nie - traktowany jak naruszenie suwerenności.[140] Ponieważ nie sposób założyć, że sam fakt hostingu takich danych daje państwu, do którego dane te należą, jakąś nadzwyczajną podstawę do wykonywania swojej jurysdykcji wobec podmiotów i przedmiotów położonych w jurysdykcjach obcych, należy założyć, że drugim warunkiem 'terytorialności' pewnych stref informatycznej części cyberprzestrzeni jest oparcie ich o infrastrukturę fizyczną zlokalizowaną wyłącznie na własnym terytorium. Tak wykonywana jurysdykcja ma oczywiście bardzo ograniczone zastosowanie i wynika z mocno zakorzenionej w prawie międzynarodowym publicznym zasady terytorialności, stanowiącej element porządku westfalskiego. O ile w przypadku jakichkolwiek działań w świecie rzeczywistym, zasada terytorialności pozwala

---

[138] por.art. 2 Konwencji z Montego Bay Dz. U. 2002 nr 59 poz. 543 (znanej także jako *United Nations Covention on the Lawof theSea* (UNCLOS), Zgromadzenie Generalne ONZ, 1833 UTS 3:21 ILM 1261 (1982)), wejście w życie 1994

[139] zob.Zittrain J., Edelman B. *Empyrical Analysis of Internet Filtering in China* Berkman Center for Internet and Society, Harvard Law School (2003). Autorzy wskazują, że cyberprzestrzeń dostępna chińskim użytkownikim, stanowi nieomal intranet, do szerszej cyberprzestrzeni podłączony poprzez nieliczne, silnie strzeżone punkty dostępowe. Jednak samo istnienie takiej możliwości należy uznać za decydujące dla uznania, że sieć ta jest elementem cyberprzestrzeni jako takiej.

[140] cf. Margulies P. *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility,* Melbourne Journal of International Law 14:2 (2013) ss.496 i n.

ochronić państwu własną suwerenność, w przypadku działań cyberprzestrzennych, *ratio legis* jej zachowywania wydaje się osłabione. Należy także pamiętać, że jurysdykcja żadnego z państw nad całością (pomimo możliwości zlokalizowania jej w oparciu o urządzenia położone wyłącznie na jej terytorium) cyberprzestrzeni nie istnieje. Można jednak wyborazić sobie pewne obszary w informatycznej części cyberprzestrzeni, które podobnie podlegają jurysdykcji wyłącznie swojego państwa i stanowią swoiste rozszerzenie jego terytorium - podobnie jak ma to miejsce z okrętami poddanymi prawu i stanowiącym terytorium przynależności.

Nie może być bowiem wątpliwości, że zgodnie z "doktryną efektu" naruszeniem suwerenności będzie atak na sieć komputerową systemu bankowego czy elektrowni atomowej należących do określonego państwa. Państwa, pomimo wszystkich wyłączeń, mają niewątpliwie pewne możliwości ścigania, a więc nie tylko projektowania ale też wykonywania swojej jurysdykcji w 'otwartej' cyberprzestrzeni. Doktryna nie ma wątpliwości co do dwóch przypadków. Po pierwsze, państwa mają możliwość ścigania obywateli własnych czy też obywateli obcych na zasadach represji wszechświatowej, choćby czyn został popełniony wyłącznie w cyberprzestrzeni (co w pewnym stopniu rozwiązuje problem wynikający z cech wszechobecności i niemożliwości fizycznego zlokalizowania cyberprzestrzeni).[141] Po drugie, państwa mają nie tylko prawo, ale wręcz obowiązek przeciwdziałania atakom skierowanym przeciwko elementom fizycznej części cyberprzestrzeni położonej na ich terytoriach.[142]

O ile ten drugi przypadek wynika oczywiście z klasycznie pojmowanej zasady terytorialności i zasad ogólnych prawa międzynarodowego nakładających na jego podmioty obowiązku przeciwdziałania czynom bezprawnym przeprowadzanym z ich

---

[141] zob. Berg T. *State Criminal Jurisdiction in Cyberspace: Is there a Sheriff on the Electronic Frontier?*, 79 Michigan Bar Law Journal 659 (2000) s.3 zob. Także orzeczenie w sprawie *People v. Blume*, wydane przez Sąd Najwyższy Stanu Michigan 31 września 1993, 505 N.W 2d 843,443 Mich. 476 (1993), w którym przyjęto inkorporowany później do prawa międzynarodowego publicznego i prawa cyberprzestrzeni test, z którego wynika że państwo ma prawo ścigać sprawcę czynu zabronionego w cyberprzestrzeni, poza własnymi granicami i zasięgiem własnej jurysdykcji terytorialnej, o ile wykaże zamiar dokonania czynu zabronionego na jego terytorium.

[142] Ryngaert C.- *The Concept of Jurisdiction in International Law,*[w:zbiorowa, red. Orakhlelashvili A.Research Handbook on Jurisdiction nad Immunities in International Law, Research Handbooks in International Law series(2009)] ss.60-70

własnych terytoriów, ze względu na sieciowość, o której mowa powyżej - jest to także forma wykonywania jurysdykcji w informatycznej części cyberprzestrzeni. Wydaje się, że za przesłankę tak wykonywanej jurysdykcji powinno się uznać, podobnie jak w przypadku terytorialnych stref cyberprzestrzeni, oparcie o infrastrukturę fizyczną położoną na określonym terytorium. Jednakże dalsza projekcja własnej jurysdykcji w opisany powyżej sposób (na przykład stanowienie norm, których celem jest prewencja przestępstw) ma charakter sporny.[143] Nie sposób także nie wskazać, że ściganie tych przestępstw stanowi stosunkowo niewielki obszar działalności państw.[144]

Koncepcja eksterytorialnej cyberprzestrzeni ma także istotne skutki dla prawa konfliktów. Większość z nich zostanie omówiona w dalszej części wywodu. W tym miejscu należy jednak zwrócić uwagę na fakt, że w odróżnieniu od pozostałych *commons*, co do zasady wyłączonych z stawania się areną konfliktów zbrojnych, takich jak otwarte morze lub przestrzeń kosmiczna, z bardzo szczegółowo określonymi wyjątkami dotyczącymi sposobu prowadzenia konfliktu - brak podstaw do określenia nie tyle nawet, jak skonstruowane są te wyjątki, w odniesieniu do cyberprzestrzeni, ale czy w ogóle one istnieją. Ma to oczywiście swoje źródło w charakterze cyberprzestrzeni, łączącej elementy terytorialne i eksterytorialne, przy braku wyraźnych rozgraniczeń pomiędzy nimi, w szczególności z braku narzędzi pozwalających na jasne stwierdzenie, w którym momencie danej cyberoperacji zostają przekroczone granice państwowe. Drugim powodem jest potencjalna duża liczna niepaństwowych aktorów biorących udział w naruszeniach, mogących

[143] Część doktryny wskazuje, że prewencja taka powinna odbywać się nie tyle w drodze stanowienia prawa, ale raczej w zakresie działań politycznych zob. na przykład Chantler A., Broadhurst R. *Social Engineering and Crime Prevention in Cyberspace*, SSRN Electronic Journal 10.2139 (2008) ss.5-8

[144] Pośrednim dowodem na to może być praktyka międzynarodowa w tym zakresie i niskie zainteresowanie konwencjami. Stanowiąca dotychczas w zasadzie martwą regulację Konwencja Budapesztańska o zwalczaniu cyberprzestrzeni ma dopiero w 2019 roku być rozszerzona o dodatkowy protokołów dotyczący rozwiązania problemu z WHOIS (opisywanego w części niniejszego wywodu poświęconej atrybucji w cyberprzestrzeni). Biorąc pod uwagę szybkość rozwoju cyberprzestrzeni i fakt, że problem ten zauważony został w 2017 roku, prawie na pewno przyjęte rozwiązania będą nieaktualne w momencie otwarcia protokołu do ratyfikacji. Podobnie niewielkim zainteresowaniem cieszą się prace Konferencji *Octopus* Rady Europy, powołanej do zwalczania cyberprzestępczości i zacieśniania współpracy państw tej organizacji w tym zakresie. zob. Także *Cybercrime towards a new legal tool on electronic evidence,* Raport *Rady Europy (2016)* ss.4-7

operować z eksterytorialnej części cyberprzestrzeni w konfliktach w niej prowadzonych.[145]

1. f. Podusmowanie

Uznanie cyberprzestrzeni za *commons* nie podlega w aktualnym stanie prawnym dyskusji. Wynika ono przede wszystkim z praktyki międzynarodowej, która nieomal bez wyjątku traktuje cyberprzestrzeń w ten sposób. Należy jednak pamiętać, że zarówno status *res communis omnium,* jak i wynikająca z niego eksterytorialność cyberprzestrzeni, nie są zasadami absolutnymi. Po pierwsze, status ten odnosi się wyłącznie do informatycznej części cyberprzestrzeni. Część fizyczna *per se* nie ma cech wszechobecności, niemożliwości zlokalizowania i nie może być uznana za anonimową. Podlega więc tradycyjnie pojmowanym jurysdykcjom poszczególnych państw. Konsekwencją takiej interpretacji jest oczywiście kolejna grupa wyjątków od zasady eksterytorialności cyberprzestrzeni. Dotyczą one stref terytorialnych w cyberprzestrzeni, a więc infrastruktury kluczowej dla interesów danego państwa, istniejącej w cyberprzestrzeni i opartej o elementy fizyczne położone na terytorium tego państwa.

Należy też pamiętać, że wspomniana eksterytorialność cyberprzestrzeni ma bardzo specyficzne znaczenie. Po pierwsze, nie oznacza ona, że państwa nie mogą wykonywać swojej jurysdykcji wobec cyberprzestrzeni. Brak jej poddania jednej określonej jurysdykcji wynika z faktu, że na cyberprzestrzeń mogą wpływać bardzo liczne podmioty - tak państwa jak *non-state actors*. Ostateczny kształt regulacji cyberprzestrzennych stanowi więc normy faktyczne, na które jurysdykcja państwowa ma znaczący wpływ. Ponieważ jednak prawo to jest zawsze funkcją wszystkich normujących ją jurysdykcji - żadna z nich nigdy nie będzie decydująca.

---

[145] Problem traktowania aktorów niepaństwowych, których liczba zwiększa się także w konfliktach kinetycznych nie jest rozwiązany nawet w tym zakresie, choć prawo konfliktu kinetycznego można uznać za stosunkowo rozbudowane. zob. Radin S. *Global Armed Conflict? The Threshold of Extraterritorial Non-International Armed Conflicts,* US Navy War College, International Law Studies 89, (2003) s. 672 i n.

2. Jurysdykcja w prawie międzynarodowym i jej znaczenie w cyberprzestrzeni.

Jurysdykcja oznacza prawo do stanowienia prawa i tego prawa wykonywania na określonym terytorium. Jest nierozerwalnie złączona z suwerennością państwa. Tylko bowiem suwerenne państwo może wykonywać własną jurysdykcję, w odróżnieniu od podmiotów prawa międzynarodowego, które wykonują jurysdykcję przekazaną (jak powołane do życia zgodą państw członkowskich organizacje międzynarodowe) czy trybunałów międzynarodowych, których jurysdykcja nad danymi państwami wymaga wcześniejszego związania się przez dane państwo odpowiednim traktatem. Wykonywanie jurysdykcji jest istotą istnienia każdego państwa i osią prawa międzynarodowego publicznego,[146] ponieważ każde działanie zewnętrzne państwa jest emanacją jego stosunków wewnętrznych i w istocie sposobem na osiąganie tych celów, których dany podmiot prawa międzynarodowego nie jest w stanie osiągnąć przy pomocy własnej jurysdykcji.

Prawo międzynarodowe natomiast dotychczas było także wypadkową jurysdykcji, ze względu na doktrynę zgody, obowiązującą w prawie międzynarodowym. Oznaczała ona, że z wyjątkiem norm wiążących *ius cogens* na dane państwo możliwe było nałożenie wyłącznie tych obowiązków, które zgodziło się ono przyjąć w traktatach lub w inny sposób wyraziło zgodę.[147] Również na mocy tej powszechnej zgody podmiotów prawa międzynarodowego, państwom przysługuje jurysdykcja nadzwyczajna, a więc prawo do wykonywania swojej jurysdykcji na terytorium innych państw lub w przestrzeni eksterytorialnej. Pojmowanie jurysdykcji w systemie westfalskim, możnaby więc sprowadzić do twierdzenia, że granice wykonywania musiały albo odpowiadać terytorialnie granicom państwa albo też zostać rozszerzone poprzez uzyskanie zgody innego podmiotu i w zakresie w tej zgodzie wyrażonym. Taka koncepcja uległa jednak współcześnie zmianie, a nawet istnieją głosy

---

[146] tak Mann F.A. [...]*what [jurisdction] has been described as a fundamental function public of international law [...] the function of regulationg and delimiting the respective competences of States- która została [jurysdykcja] po wielokroć opisana jako pełniące fundamentalną rolę w prawie międzynarodowym publicznym [...] funkcję regulacji i delimitacji odpowiednich kompetencji państw* [w:*The Doctrine of Jurisdiction in International Law*, 111 RCADI (1964) ss.15-22]

[147] zob. Lister M. *The Legitimating Role of Consent in International Law*, Chicago Journal of Interntional Law 1-1 (2011) ss. 663-7

twierdzące, że nigdy nie była ściśle przestrzegana.[148] Zmiany w pojmowaniu jurysdykcji powstają dwutorowo, zarówno poprzez coraz dalsze rozszerzanie zakresu przedmiotowego normowanego przez *ius cogens* (a więc zakresu prawa, które państwa muszą przyjmować niezależnie od własnej zgody na związanie się nimi) jak i coraz liczniejsze wyjątki od zasady zgody.[149] Oczywiście, wpływa to także na jurysdykcję nadzwyczajną: z jednej strony jej zakres przedmiotowy rozszerza się - ponieważ coraz więcej zachowań podlega jurysdykcji międzynarodowej. Z drugiej natomiast strony coraz częściej wykonywanie tej jurysdykcji przekazywane jest w ręce agend ponadnarodowych. Utrzymanie się tego trendu może prowadzić do dalszego zmniejszenia zakresu poddanego jurysdykcji państw Muszą one bowiem znosić wykonywanie jurysdykcji nadzwyczajnej w odniesieniu do własnego terytorium, a zwiększenie zakresu przedmiotowego poddanego co do zasady jurysdykcji nadzwyczajnej nie zwiększa jednak możliwości wykonywania jej przez państwa.

Wspomniane już podmioty ponadnarodowe są z kolei zbyt duże, by jedno państwo mogło skutecznie wpływać na jego działania nawet w sytuacji prawnej, która w ściśle rozumianym systemie westfalskim gwarantowałaby poddanie danego zdarzenia jurysdykcji nadzwyczajnej owego państwa.[150] Kolejnym elementem rozmywania jurysdykcji zwyczajnej i nadzwyczajnej państw jest zmiana jej zakresu przedmiotowego.[151] Jednym z przykładów najczęściej analizowanych w doktrynie takich rewolucyjnych zmian w pojmowaniu jurysdykcji jest właśnie cyberprzestrzeń.[152] Poza wspomnianymi już zmianami w zakresie zasady terytorialności, redefiniuje ona przede wszystkim teorię zgody.[153] Państwa nie

---

[148] Tak np. Cedric Ryngaert.w *Concept of;...* ss.35-7

[149] por.Henkin L. *International Law After the Cold War* Maryland Journal of International Law 15:147 (1991) ss.1-2

[150] Guzman A. *The Consent Problem in International Law* University of California, Berkeley Working Paper Series,(2011) s. 18

[151] cf. Mills A. *Rethinking Jurisdiction in International Law*, British Yearbook of International Law 84-1 (2014) ss.187-239

[152] zob. Castaneda F.A.C. *A call for rethinking the sources of international law: soft law and the other side of the coin*, Anuario Mexicano de Derecho International 13 (2013) ss.370-5

[153] zob. Menthe D.C. *Jurisdiction in Cyberspace: theory of international spaces*, Michigan Telecommunication and Tech Law Review 69 (1998) ss.69-79

wyrażają zgody na związanie się normami *lex informat*ica (za wyjątkiem wspomnianej możliwości uznania włączenia własnych sieci komputerowych w ogólnoświatową sieć za dorozumianą zgodę). Podobnie, ostateczny kształt tych norm często stoi w sprzeczności z interesami poszczególnych państw.

2. a. 1. Definicja

Jak to się dzieje z wieloma kluczowymi dla prawa międzynarodowego publicznego pojęciami, istnieją liczne spory co do tego, czym w istocie jest jurysdykcja. Nie jest celem niniejszej pracy analizowanie tych wszystkich stanowisk. Istotne dla rozprawy niniejszej jest natomiast wskazanie głównych elementów powszechnie przyjmowanych definicji, co do których istnieje zgodność praktyki, orzecznictwa i doktryny i odniesienie ich do cyberprzestrzeni. Dlatego też, na potrzeby niniejszych rozważań, za definicję legalną jurysdykcji przyjęta zostanie suma następujących elementów:

a) obowiązek i prawo do stanowienia i egzekwowania prawa na określonym terytorium;[154]
b) obowiązek i prawo do organizacji wymiaru sprawiedliwości; egzekwującego stanowione prawo w szczególności na gruncie prawa administracyjnego, karnego i cywilnego.[155]

Tradycyjnie przyjmuje się, że wykonywanie jurysdykcji może odbywać się na podstawie[156]: (a) zasady jurysdykcji terytorialnej subiektywnej i obiektywnej, (b) zasady narodowości przedmiotowej lub podmiotowej, (c) zasady jurysdykcji ochronnej (tzw. *Protective Principle*), (d) zasady jurysdykcji uniwersalnej (represji wszechświatowej). Dla cyberprzestrzeni będzie miała znaczenie kluczowe jurysdykcja wykonywana w oparciu o ciągle kontrowersyjną przesłankę, jaką jest tzw. "doktryna skutku", która zostanie opisana poniżej.

---

[154] zob. Shaw M.N. *International Law* Cambridge University Press 6th ed. (2008) s.212
[155] Shaw M. *International ...*, s.212
[156] zob. Hillier T. *Soucerbook on Public International Law*, Title I, Series II, Cavendish Publishing Ltd. (1998) s.257

2. a. 2. Jurysdykcja terytorialna w cyberprzestrzeni

Prawo międzynarodowe rozróżnia pomiędzy jurysdykcją terytorialną subiektywną i obiektywną.[157] Jurysdykcja subiektywna pozwala państwu na stosowanie swojej jurysdykcji wobec czynów, które rozpoczęły się na terytorium danego państwa, ale swój skutek odniosły poza zakresem jurysdykcji tego państwa. Jurysdykcja obiektywna, odwrotnie, oznacza prawo do stosowania jurysdykcji zwyczajnej co do czynów odnoszących skutek w danej jurysdykcji, pomimo tego, że rozpoczęły się poza jej granicami.[158] Jurysdykcja obiektywna, a więc oparta o przedmiot czynu, stała się niezwykle istotnym problemem prawnym wraz z rozwojem cyberprzestrzeni.[159] Dotychczas bowiem nieomal niemożliwością było dokonanie czynu wyrządzającego szkodę państwu bez fizycznej obecności sprawców. Cyberprzestrzeń, ze względu na zasadę wszechobecności cyberprzestrzeni, umożliwia dokonywanie ataków z dowolnego miejsca świata przeciwko dowolnemu celowi podłączonemu do cyberprzestrzeni.

Najczęstszą sytuacją w przypadku naruszeń suwerenności będzie więc zachowanie mające skutek na terytorium państwa (zarówno fizycznego jak i cyberprzestrzennego), pochodząc spoza tej jurysdykcji. Niemniej należy zauważyć, że każdy element wykonywania jurysdykcji państwa poza jego terytorium stanowi działanie w ramach jurysdykcji nadzwyczajnej, a więc *per se* sytuację wyjątkową i wymagającą spełnienia licznych warunków. W cyberprzestrzeni jednak ten rodzaj jurysdykcji (wraz z tzw. doktryną skutku opisaną poniżej) staje się głównym sposobem ochrony własnej suwerenności przez państwa. W przypadku cyberoperacji zasadą jest, że na terytorium (fizycznym lub cyfrowym) państwa stanowiącego cel tejże występują jedynie skutki operacji (za wyjątkiem sytuacji, w której do przeprowadzenia operacji użyto infrastruktury zlokalizowanej na jego terytorium - w praktyce bardzo rzadkiej).

Jurysdykcja terytorialna będzie więc z prawnego punktu widzenia miała

---

[157] ibid. s.259 i n.

[158] zob.Opinia Rzecznika Generalnego Europejskiego Trybunału Sprawiedliwości Marco Damona w sprawach połączonych 89,104,114

[159] zob. Maillart J-B, *The limits of subjective territorial jursidtiction in the context of cybercrime*, ERA Forum 19:3, (2019) ss.376

podstawowe znaczenie dla wszystkich działań skierowanych do fizycznej części cyberprzestrzeni, ze względu na możliwość ich zlokalizowania. Państwo, które jest celem cyberoperacji, będzie miało prawo do ścigania sprawców naruszenia własnej suwerenności na mocy jurysdykcji obiektywnej, z którą korespondować będzie obowiązek[160] wynikający z nakazu powstrzymania naruszeń suwerenności państw trzecich z własnego terytorium, powstający po stronie każdego państwa, którego (terytorialna) infrastruktura fizyczna cyberprzestrzeni została użyta do ataku. Zawsze jednak skutek wywołany w cyberprzestrzeni będzie naruszeniem wywołującym skutki niefizyczne (w przypadku operacji nie mającej skutków fizycznych, będzie to często jedyny rodzaj naruszeń). Łatwo zauważyć, że ta grupa skutków nie będzie mogła być samoistną podstawą dla stosowania jurysdykcji terytorialnej. Ze względu jednak na konieczność lokalizacji części fizycznych cyberprzestrzeni użytych do operacji w jej części informatycznej, będzie konieczne wzięcie pod uwagę także tego rodzaju jurysdykcji. Jeżeli rozpatrzymy sytuację, w której państwo w celu uruchomienia środków obrony własnej suwerenności musi dokonać przypisania ataku, dojdziemy do wniosku (wobec braku możliwości wykonywania jurysdykcji nad danymi), że musi ono uzyskać informacje zlokalizowane w oparciu o urządzenia położone w innych jurysdykcjach.

W przypadku wykorzystania aktywnych środków obrony własnej suwerenności - będzie z kolei konieczne wykorzystanie infrastruktury eksterytorialnej do oddziaływania na podmiot, który operację przeprowadzał. Dochodzi więc do sytuacji, w której państwo będące celem operacji, może nie uzyskać prawa do wykonywania jurysdykcji terytorialnej, ponieważ skutek operacji wystąpił wyłącznie w eksterytorialnej informatycznej części cyberprzestrzeni, podczas gdy ochrona własnej suwerenności w drodze jurysdykcji terytorialnej wymaga możliwość powiązania skutku z terytorium, na którym skutek ten wystąpił, lub z którego nastąpiła operacja. Wydaje się, że dopóki praktyka międzynarodowa nie wypracuje

[160] zob. Schmitt M. *Targeted Killings and International Law: Law Enforcement, Self-Defense*[w:zbiorowa *International Humanitarian Law and Human Rights Law. Towards a New Merger in International Law* red. Arnold R., Quenivet N., Martinus Nijhoff Publishers (2008) s.540]

mechanizmów rozwiązania owego konfliktu (poza wspomnianym powyżej obowiązkiem państw do uniemożliwiania ataków na państwa trzecie z własnego terytorium, często trudnym do faktycznego stosowania w cyberprzestrzeni), jurysdykcja terytorialna pozostanie wyłącznie narzędziem subsydiarnym w wykonywaniu jurysdykcji państwowej w cyberprzestrzeni.

2. a. 3. Doktryna skutku

Ponieważ należy pamiętać, że trzy z pięciu podstaw wykonywania jurysdykcji nadzwyczajnej, a więc (1) terytorialność (pojmowana jako miejsce zdarzenia naruszenia suwerenności), (2) narodowość osoby dopuszczającej się naruszeń i (3) zasada pasywnej osobowości[161], co do zasady w ogóle nie mogą być stosowane w cyberprzestrzeni.[162] Czwarta z nich, a więc podstawa tzw. represji wszechświatowej,[163] stosuje się wyłącznie do samych naruszeń, niemniej wymaga do swego zastosowania atrybucji i to, ze względu na nadzwyczajny charakter jurysdykcji opartej o nią, przeprowadzonej z bardzo wysokim stopniem dokładności, nieosiągalnym w atrybucjach cyberprzestrzennych. Do cyberprzestrzeni może stosować się natomiast ostatnia z tych przesłanek, a więc opisywana tu przesłanka doktryny skutku. Opisywana tu przesłanka wykonywania jurysdykcji powstała stosunkowo niedawno. Ukonstytuowała się ona w praktyce sądów amerykańskich, które uznawały się za właściwe w odniesieniu do działań obywateli obcych podjętych poza jurysdykcją amerykańską, jeżeli działania te miały skutek na amerykańskich rynkach finansowych.[164] Przyjmuje się więc, że zastosowanie "doktryny skutku" pozwala państwu wykonywać jurysdykcję w stosunku do podmiotów, które nie są poddane w żaden inny sposób jurysdykcji tego państwa, o ile ich działania (choćby

---

[161] Shaw M.N.*International Law* wyd. 6 Cambgride Univeristy Press, (2008)ss.652–68.

[162] Należy także wskazać, że nie są one uniwersalnie przyjmowane jako podstawy jurysdykcji nadzwyczajnej. zob. Bialostozky N.Extraterritoriality and National Security:Protective Jurisdiction as a Circumstance Precluding Wrongfulness, Columbia Journal of International Law, [52:617] ss.620 i n.

[163] Shaw M.N.*International Law*...ss.652–68.

[164] zob. Coppel J. *A Hard Look at the Effects Doctrine of Jurisdiction in Public International Law*, Leiden Journal of International Law 6:1 (1993) ss.74-77

wykonywane w innej jurysdykcji) miały wpływ na przedmioty lub podmioty znajdujące się w *domaine reserve* tego państwa.

Przyjęcie doktryny skutku do systemu prawa międzynarodowego publicznego od samego początku budziło wątpliwości,[165] jednak stało się ono konieczne wobec postępującej globalizacji. W dzisiejszym stanie prawnym nie ma wątpliwości, że jest ona przyjmowana w sposób niekwestionowany w Stanach Zjednoczonych[166] a także w Unii Europejskiej.[167] Brak jednak jasnej regulacji, czym miałby być skutek, a praktykę w tym zakresie należy uznać za niewystarczającą.[168] Głównym wyznacznikiem w tym zakresie wydaje się być sprawa s/s Lotus (szczegółowo opisana w dalszej części wywodu), w której Międzynarodowy Trybunał Sprawiedliwości przyjął za przesłankę wykonywania jurysdykcji opartej o doktrynę skutku sytuację, w której skutki działania poza terytorium danego państwa będą fizycznie odczuwalne w jego jurysdykcji".[169] Takie rozumienie doktryny skutku odpowiada intuicyjnemu rozumieniu jurysdykcji w cyberprzestrzeni i wydaje się być odpowiedzią na wskazane powyżej problemy z wykonywaniem w informatycznej części cyberprzestrzeni subiektywnej i obiektywnej jurysdykcji terytorialnej. Pamiętać należy, że skutek wywarty 'na terytorium państwa' może oznaczać zarówno skutki wywołane w terytorium fizycznym lub cyfrowym. Oparcie wykonywania jurysdykcji o doktrynę skutku oznacza więc możliwość wpływu na dane istniejące w oparciu o elementy części fizycznej istniejącej w innych jurysdykcjach, o ile (zgodnie

---

[165] Przykładowo Komisja Prawa Międzynarodowego przyznała, że *[...]to admit "effects as a basis jurisdiction[...]would be to permit well-established principles of international jurisdiction to be overturned by the sidewind(which , it may be added has blown consistently from one direction only)-doktryna skutku to szkwał, który* (dodatkowo wiejąc wyłącznie z jednej strony) przewróci dotychczasowe, solidnie ugruntowane podstawy wykonywania jurysdykcji. zob. Raport ILA z 45 Konferencji w Hadze 235, (1970) s. 7 Niemniej sama Komisja uznaje stosowania doktryny skutku za konieczne. zob. Samie N. *The Doctrine of "Effects" and the Extraterritorial application of Antitrust Laws*, University of Miami Inter-American Law Review 14:23(1982)ss.25-6

[166] Na jej podstawie rozstrzygnięta została *i.a.* sprawa *United States v. Aluminium Co. Of America*, 148 F 2d 416 (1945), uznawana za precedens w tym zakresie.

[167] Za przyjęcie doktryny do porządku unijnego uznaje się orzeczenie w sprawie *Gencor Ltd v. Commission of the E.C.,* ECLI:EU:T 1999:65 (1995)

[168] Istnieje kilka niewspółmożliwych testów, które miałyby określać przesłanki wykonywania jurysdykcji w oparciu o omawianą podstawę. zob. Berman P.S. *Globalization of Jurisdiction*, University of Pennsylvania Law Review 151:311(2002) ss.447-58

[169] zob. Parrish, Austen L. *The Effects Test: Extraterritoriality's Fifth Business*, Maurer Faculty Paper 893(2008) ss.1471

ze wskazaną powyżej przesłanką) skutek był odczuwalny na terytorium państwa, które będzie tą jurysdykcję wykonywać. Ta argumentacja wydaje się znajdować coraz szersze uznanie międzynarodowe w zakresie wypadkowego wykonywania jurysdykcji wymagającego uzyskania dostępu do danych. Dowodem na to może być inkorporowanie prawa do dostępu do danych zlokalizowanych na serwerach położonych w obcych jurysdykcjach w razie ścigania czynu, który odniósł skutek na terytorium danego państwa.[170] Wykorzystywanie doktryny skutku mieści się także w ramach *lex informatica*, jako wynikające zarówno z architektury cyberprzestrzeni jak i ze zwyczaju i praktyki w niej obowiązujących. Stosowanie doktryny skutku pozwala więc na wykonywanie jurysdykcji w informatycznej części cyberprzestrzeni w oderwaniu od jej części fizycznej (chociaż oczywiście jej nie wyklucza). W efekcie państwo którego suwerenność została naruszona (wyłącznie lub nie) w informatycznej części cyberprzestrzeni, nie musi przeprowadzać pełnego procesu atrybucji w celu uruchomienia własnych narzędzi ochronnych. Może ono uruchomić odpowiedź cyberprzestrzenną wyłącznie po zlokalizowaniu źródła naruszeń w oparciu o wszechobecność cyberprzestrzeni. Odpowiedź taka nie wymaga dla swojej skuteczności pełnego atrybuowania zachowania, w związku z tym może być przeprowadzona w znacznie krótszym czasie, przez co istotnie wzrasta jej skuteczność. Koresponduje to ze zjawiskiem nazywanym w doktrynie 'globalizacją jurysdykcji' - opisującym stopniową utratę znaczenia terytorialności jako podstawy wykonywania jurysdykcji, przy jednoczesnym przenoszeniu ciężaru na właśnie na nawet niematerialnie rozumiane skutki.[171]

2. a. 4. Zasada ochronna

Opisana powyżej doktryna skutku, niewątpliwie zwiększa możliwość obrony przez państwa własnej suwerenności w cyberprzestrzeni W wielu możliwych scenariuszach

[170] Szczegółowo kwestia uzyskiwania takiego dostępu zostanie omówiona poniżej na przykładzie amerykańskiej legislacji, tzw. *CLOUD Act.*

[171] zob.Behrens P. *The extraterritorial reach of EU competition law revisited: The "effects doctrine" before the ECJ*, ECONSTOR Disscussion Paper 3/16. Leibniz Inromationszentrum, (2016) s.15

operacji cyberprzestrzennych także i ona nie będzie mieć zastosowania. Nie jest także dla państw wystarczająca w kontekście możliwości przeciwdziałania niektórym grupom cyberprzestrzennych naruszeń suwerenności. Do tego typu operacji należą przede wszystkim operacje, których skutki są opóźnione w czasie (jak na przykład niektóre rodzaje operacji *CNE* - opisane w dalszej części wywodu). Ze względu na brak zaistnienia jakichkolwiek widocznych skutków (zarówno w świecie fizycznym jak i w cyberprzestrzeni) nie zostaje spełniona przesłanka podstawowa przesłanka doktryny skutku - czyli właśnie wystąpienie tego ostatniego. Należy zauważyć, że do wspomnianej wyżej grupy naruszeń nie ma możliwości stosowania także pozostałych podstaw wykonywania jurysdykcji nadzwyczajnej. Poza opisanymi powyżej trudnościami, należy także wskazać że podstawa represji wszechświatowej[172] stosuje się wyłącznie do samych naruszeń (a nie do omawianych tu operacji o nieokreślonym skutku). Do swego zastosowania wymaga więc atrybucji i to, ze względu na nadzwyczajny charakter jurysdykcji o nią opartej - atrybucji przeprowadzonej z bardzo wysokim stopniem dokładności, nieosiągalnym w atrybucjach cyberprzestrzennych. W takich sytuacjach konieczne stanie się zastosowanie jurysdykcji opartej o zasadę *Protective Principle.*[173] Zasada ochronna jest więc najłatwiej dostępnym państwom narzędziem wpływu na *lex informatica*. Wynika to z kluczowej dla normowania cyberprzestrzeni różnicy pomiędzy nią samą a zasadą represji wszechświatowej. W odróżnieniu od tej ostatniej, służącej do zwalczania wyłącznie najcięższych zbrodni, zakazywanych normami wiążącymi *erga omnes* - państwo ma prawo zawrzeć uruchomienie zasady ochronnej w swoim prawie krajowym, dla ochrony własnych interesów.[174] Jej zakres przedmiotowy jest więc dużo szerszy niż w przypadku pozostałych podstaw jurysdykcji eksterytorialnej.

---

[172] Shaw M.N.*International Law*...ss.652–68.

[173] Dosłownie znaczenie oddaje lepiej oryginalna, wywodząca się z niemieckiej doktryny, nazwa '*Staatsschutzprinzip'*, a więc 'zasada ochrony państwa'. Chodzi tu instytucję prawa międzynarodowego publicznego, pozwalającą na objęcie własną legislacją podmioty i przedmioty nie podlegające własnej jurysdykcji, pod warunkiem zagrożenia przez te podmioty lub przedmioty państwu, które na *Protective Principle* się powołuje. zob.Shaw *International Law...*, s.620, także Ryngaert C. *Jurisdiction in International Law*, Oxford Monographs in International Law, Oxford University Press (2008) ss.158-61

[174] Cameron I. *International Criminal Jurisdiction, Protective Principle* [w: MPIL par.1]

Natomiast dla uruchomienia prawa państwa do wykonania jurysdykcji na podstawie zasady ochronnej wystarczające jest wyłącznie spełnienie przesłanki istnienia zagrożenia dla istotnych interesów państwa, które to zagrożenie pozostaje poza zasięgiem jurysdykcji państwa zagrożonego opartej o którąkolwiek z pozostałych podstaw jej wykonywania.[175]

Ma to szczególne znaczenie w przypadku cyberprzestrzeni, która w odróżnieniu od pozostałych *commons* (za wyjątkiem przestrzeni kosmicznej) przypisuje szczególną rolę zasadzie terytorialności.[176] W jej przypadku państwo stosujące P*rotective Principle* ma prawo wykonywać swoją jurysdykcję zarówno wobec informatycznej jak i fizycznej części cyberprzestrzeni. Przede wszystkim (w odróżnieniu od doktryny skutku) pozwala więc zasada ochronna na wykonywanie jurysdykcji wobec podmiotów *ISP* działających w jurysdykcjach obcych w czasie, kiedy naruszenie trwa (zamiast działań następczych); umożliwia więc zarówno skuteczniejszą atrybucję jak i możliwość przeciwdziałania naruszeniom własnej suwerenności zanim wywołają one jakiekolwiek skutki. Zasada ochronna stanowić będzie także podstawę dla prowadzenia niekinetycznych cyberataków, stanowiących główny środek obrony cybersuwerenności przed naruszeniami.[177]

2. a. 5. Jurysdykcja zwyczajna i stanowienie prawa w cyberprzestrzeni.

Jurysdykcja zwyczajna to jurysdykcja, którą państwo wykonuje na własnym terytorium. Podstawowym bowiem składnikiem jurysdykcji jest prawo państwa do wyłączenia wpływów innych państw.[178] Klasycznie pojmowana jurysdykcja zwyczajna wynika z westfalskiej teorii prawa międzynarodowego; jest więc nierozerwalnie związana z terytorialnością - główną przesłanką istnienia lub

[175] zob. Cameron I The Protective Principle of International Criminal Jurisdiction Dartmouth Publishing Company (1994) s.31

[176] cf. Baslar K. *The Concept of the Common Heritage of Mankind in International Law*, Martinus Nijhoff Publishers (1998) ss. 40-41

[177] Kwestia ta zostanie szerzej omówiona w dalszej części wywodu poświęconej naruszoniem suwerenności w cyberprzestrzeni i remediom przeciwko nim.

[178] Zakaz naruszania jurysdykcji jednego państwa przez pozostałe regulują zasady nieinterwencji i nieinterferencji, które zostaną szczegółowo omówione w dalszej części niniejszej rozprawy.

nieistnienia jurysdykcji danego państwa. Pomimo prób[179] redefinicji jurysdykcji nie udało się w świecie rzeczywistym odłączyć pojęcia jurysdykcji zwyczajnej od zasady terytorialności, Pomimo wszystkich zmian, którym jest ona poddana w ostatnim czasie, jej ostateczny charakter przypomina ten właściwy dla porządku westfalskiego. Zarówno sposób jej wykonywania jak i sam fakt korzystania lub niekorzystania z jurysdykcji jest elementem suwerenności państwa. Nawet jeżeli państwo musi zachować się w określony sposób, wynikający ze związania się przez to państwo traktatem lub pomimo norm wiążących *erga omnes*, możliwe jest wyłącznie dochodzenie wykonania tego zobowiązania.

Nie ma bowiem co do zasady możliwości prawnego zmuszenia suwerennego państwa do określonego zachowania.[180] Tak wykonywana jurysdykcja w zasadzie nie ma zastosowania do cyberprzestrzeni. Tu bowiem nie istnieją jasno określone granice państw i ich interesów, brak możliwości łatwego zawierania traktatów a ewentualne zagrożenia dla suwerenności nie tylko pochodzą spoza tej jurysdykcji, ale najczęściej (w rozumieniu „westfalskiej" terytorialności) w ogóle nie są wykonywane w jurysdykcji państwa, którego suwerenność została naruszona.[181] Z powodów niemożliwości atrybucji i wspomnianej powyżej zasady wszechobecności sieci, państwa zmuszone są co do zasady do chronienia swojej suwerenności przy pomocy mechanizmów ekstraterytorialnych. Jednakże wyprowadzona głównie na zasadzie definicji negatywnej „westfalska" jurysdykcja nadzwyczajna także nie ma większego zastosowania do cyberprzestrzeni. Kluczowym elementem wykonywania jurysdykcji na własnym terytorium jest oczywiście prawo do stanowienia i egzekwowania prawa.[182] Powstaje jednak pytanie w jaki sposób ten aspekt może być wykonywany w informatycznej części cyberprzestrzeni (nie ma natomiast wątpliwości, że

---

[179] Berman P.S. *Global Legal Pluralism* 80 South California Law Review (2007) s. 1155

[180] Zasada ta nie jest jednak pozbawiona wyjątków. Kanonicznym przykładem takiego wyjątku jest zasada *aut dedere aut judicare*, nakazująca państwu albo wydać osobę oskarżoną o przestępstwa ścigane międzynarodowo albo wydać ją innemu państwu, które o ekstradycję zabiega. zob. także Scharf M.P. *Aut dedere aut iudicare* [w:zbiorowa, red.Wolfrum R. *Max Planck Encyclopaedia of Public International Law* (2018) par.2]

[181] cf.Trachtman J.P. *Cyberspace, Sovereignty, Jurisdiction, and Modernism* ,Indiana Journal of Global Legal Studies: t.5:wyd.2 (1998) ss.1-5

[182] zob. Beale J.H. *The Jurisdiction od Sovereign States,* Harvard Law Review 36:3 (1923), ss.242-3

w odniesieniu do części fizycznej jest on wykonywany na zasadach ogólnych). Przede wszystkim w zakresie stanowienia prawa w stosunku do części informatycznej państwo traci monopol na normowanie. Jest bowiem zmuszone liczyć się z wpływem cyberprzestrzeni, opartej o normowanie także innych podmiotów prawa międzynarodowego na własne interesy. Z drugiej strony, informatyczna część cyberprzestrzeni stanowi jedyne *commons*, na które państwa mogą wywierać choćby ograniczony wpływ w oparciu o własną jurysdykcję.[183] Oczywiście, stopień tego wpływu będzie uzależniony od stopnia technicznego rozwoju danego państwa. Przykładowo, możliwość projekcji siły będzie w znaczący sposób uzależniona od procentowego współczynnika ruchu cybernetycznego opartego o znajdujące się na terytorium tego państwa elementy części fizycznej lub od stopnia rozwoju podmiotów *ISP* poddanych własnej jurysdykcji. Ponieważ takie podmioty związane są normami prawa stanowionego we własnym domicylu, pośrednio państwa uzyskują możliwość poddania własnej jurysdykcji części cyberprzestrzeni stanowiącej *res communis omnium*.

2. a. 6. Jursydykcja funkcjonalna

Pojęcie jurysdykcji funkcjonalnej pochodzi i związane jest zasadniczo z prawem morza. Jej wykonywanie oznacza prawo państwa do normowania podlegających jego ograniczonej kontroli obszarów morza, nienależących jednak do jego terytorium.[184] Państwo ma prawo zarówno do normowania jak i egzekwowania norm stanowionych w ramach jurysdykcji funkcjonalnej, jednakże wyłącznie w pewnym ograniczonym zakresie.[185] Nie oznacza to jednak żadnych ograniczeń co do jurysdykcji *per se*. Normy tak stanowione mają moc tak jak wszystkie pozostałe. Inny natomiast jest zakres podlegający normowaniu, ponieważ obszary normowane funkcjonalnie nie podlegają w pełni jurysdykcji zwyczajnej państwa. Podobna konstrukcja stosuje się

---

[183] por. Miller S.F. *Prescriptive Jurisdiction over Internet Acitivity: the need to Deifne and Establish the Boundaries of CyberLiberty*, Indiana Journal of Global Legal Studies 10:2(2003) s.227

[184] Jak na przykład wyłącznej strefy ekonomicznej.

[185] por. Ryngaert C. *The concept... ss.57-63*

także do informatycznej części cyberprzestrzeni, bowiem elementy jurysdykcji funkcjonalnej można odnaleźć w wykonaniu jurysdykcji w drodze normowania faktycznego. Szerzej kwestia ta została omówiona poniżej, w części poświęconej *lex informatica.*

2. a. 7. Zasada nieinterwencji i nieinterferencji

Zasady nieinterwencji i nieinterferencji są jednymi z głównym instytucji dotyczących suwerenności państwowej. Pomimo iż dotyczą one dwóch różnych aspektów suwerenności państwa, wspólnie można z nich dekodować jedną z podstawowych norm prawa międzynarodowego publicznego zakazującą naruszenie suwerenności państw trzecich .[186] O ile więc zasada nieinterwencji dotyczy zakazu naruszenia granic danego państwa, zasada nieinterferencji tworzy zakaz ingerowania w sprawy nie podlegające regulacjom prawa międzynarodowego publicznego, a będące wynikiem wykonywania przez państwa ich dyskrecjonalnych uprawnień wynikających z suwerenności.[187] Takie ich pojmowanie wynika z niekwestionowanej normy międzynarodowego prawa zwyczajowego, jednak pełny zakres obydwu zasad pozostaje niejasny. Częstokroć w doktrynie wskazuje się *a contrario* definicję okoliczności, w których interwencja jest nielegalna. Definicja ta została skonstruowana przez Międzynarodowy Trybunał Sprawiedliwości.[188] MTS wskazał tam, że interwencja jest zakazana, kiedy wyłącza lub choćby ogranicza wolny wybór państwa w kwestiach dotyczących formułowania polityki międzynarodowej lub istotnych dla danego państwa kwestii wewnętrznych, które według interpretacji Trybunału dotyczą w szczególności systemu politycznego, kulturalnego, ekonomicznego czy społecznego. Zakaz ów dotyczy zarówno państw jak i aktorów niepaństwowych. W przypadku naruszenia normy, o której mowa przez aktora niepaństwowego, państwo może zostać pociągnięte do odpowiedzialności za

---

[186] Aloupi N. T*he right to Non-intervention and Non-interference* Cambridge Journal of International and Comparative Law 4:15 (2015) s.1 i n.

[187] ibid.

[188] zob.Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nic v. U.S. of A), International Court of Justice, ICJ Merits Reports (1986) par 205.

bezprawne działanie lub zaniechanie.[189] Bardzo istotne dla tematu niniejszej rozprawy są spory co do dwóch kluczowych aspektów przedmiotowych zasad. Pierwszym spornym elementem jest definicja ogólna wszystkich elementów pozostających domeną wspomnianej dyskrecjonalnej władzy państw, a więc objętych normą dekodowaną łącznie z zakazów konstytuowanych przez obydwie zasady.[190] Drugim - jakie dokładnie środki wpływu na owe elementy są zakazane.[191]

Problemu tego nie rozwiązuje fakt, że Komisja Prawa Międzynarodowego nakłada na każde państwo nakaz wstrzymania się zarówno od interferencji jak i od interwencji - nie rozróżniając pomiędzy tymi dwiema instytucjami.[192] Norma ta jest bowiem zawarta jest w akcie o niewiążącym, nie wyjaśnia o jakich środkach interwencji i interferencji mowa i co najbardziej istotne - nie przewiduje wyjątków co do których istnienia nie ma wątpliwości na gruncie zwyczajowego prawa międzynarodowego.[193] Kwestia dokładnego uregulowania tego zakresu była przedmiotem licznych sporów, zakończonych rozszerzeniem zakresu przedmiotowego ujęcia z Deklaracji przez Zgromadzenie Ogólne ONZ. Rozszerzenie to zakazuje jakiejkolwiek formy interferencji i ingerencji - niezależnie od powodu - w jakiekolwiek wewnętrzne lub zewnętrzne sprawy państw trzecich.[194] Jednakże, z powodów wskazanych już powyżej, także i ta regulacja jest w istocie prawem martwym.[195] Nie sposób więc

---

[189] por.Kees A. *Responsibility of States for Private Actors* [w:zbiorowa, red. Wolfrum R.Max Planck *Encyclopaedia of Public International Law* (2011) par.1]

[190] por.Kunig Ph. *Prohibition of Intervention* [w:zbiorowa, red. Wolfrum R.Max Planck *Encyclopaedia of Public International Law*,(2008) par.par. 1-3], Max Planck Stiftung

[191] ibid. par. 2

[192] zob.art.3 International Law Commission *Draft Declaration on Rights and Duties of States* przyjęte rezolucją Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych 375(IV) z 6 grudnia 1949 , wraz z komentarzem do tego artykułu sporządzonym przez Komisję Prawa Międzynarodowego (1949) [w: *Yearbook of International Law Commission,*(1949)]

[193] W tym przewidziane przez same Narody Zjednoczone, jak choćby interwencja na podstawie rezolucji Rady Bezpieczeństwa. zob. Także orzeczenie MTS, *It is not to be expected that in the practice of States the application of rules in question should have been perfect in the sense that States should have refrained, with complette consistency from intevernetion in each other internal affairs-nie sposób oczekiwać, że w praktyce międzynarodowej stosowanie norm omawianych norm będzie się odbywało w sposób idealny, a więc ,że państwa zupełnie powstrzymają się od ingerowania wzajemnie w swoje wewnętrzne sprawy* [w: *Nicaragua...* par. 186]

[194] zob. Rezolucję Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych 36/103 z 9 grudnia 1981 roku.

[195] Należy zwrócić uwagę, że w żadnym ze wspomnianych aktów prawnych nie ma regulacji odsyłających do norm *leges speciales*, które dopuszczałyby interwencję regulując niewątpliwie istniejące przypadki wtórnej ich legalizacji.

wskazać przekonującej normy regulującej jasno znaczenie zasad nieinterwencji i nieinterferencji oraz przesłanek ich złamania, a kwestie te podlegają praktyce międzynarodowej. W cyberprzestrzeni, gdzie prawo zwyczajowe ciągle jeszcze jest w fazie powstawania, trudności te są jeszcze bardziej zauważalne, a praktyka dużo mniej łatwa do określenia. Jak zostanie wskazane w rozdziale dotyczącym *lex informatica* i normowania faktycznego - zwyczajowi w cyberprzestrzeni najczęściej nie towarzyszy *opinio iuris.* Tymczasem zasady nieinterwencji i nieinterferencji są niezmiernie istotne dla cyberprzestrzeni i konfliktów w niej prowadzonych. Prawie każda bowiem operacja cyberprzestrzenna (w tym, te które nie są atakami) jest wykonywana w jurysdykcji (zarówno w świecie fizycznym jak i we wspomnianym już powyżej „terytorium cyfrowym") państwa innego niż to, które operacji dokonuje. Łatwo też zauważyć, że operacje te najczęściej spełniają przesłanki złamania zarówno zakazu interwencji jak interferencji. Pewną wskazówkę interpretacyjną co do pojmowania zasad nieinterwencji i nieinterferencji w cyberprzestrzeni mogą stanowić prace Międzynarodowej Grupy Ekspertów NATO.

Autorzy Tallinn Manual wskazują, że granicą rozróżniającą w cyberprzestrzeni interferencję od interwencji jest element przymusu, podczas gdy każde cyberprzestrzenne naruszenie *domaine réservé* (niezależnie czy połączone z naruszeniem terytorium państwa czy też nie) należy pojmować jako interferencję .[196] Tallin Manual nie wskazuje jednak definicji legalnej ani nie określa jasnego testu, który pozwalałby na precyzyjne określenie co jest przymusem w tym zakresie. Jedyna norma prawa zwyczajowego (co istotne, powstała przed rozwojem prawa cyberprzestrzeni) zabraniająca przymusu, mająca jednocześnie swoje źródło w traktatach (a więc stanowiąca pewien zapis praktyki międzynarodowej w tym zakresie) także jest raczej deklaracją programową i normą generalno-abstrakcyjną.[197] Praktyka międzynarodowa i orzecznictwo wskazuje jednak użycie siły jako

[196] Określaną w literaturze angielskim terminem *Coercion*. zob. *Rule 66 Tallinn Manual 2.0* wraz z komentarzem IGoE par. 22. Należy zauważyć, że jest to bezpośrednia transpozycja do prawa cyberprzestrzeni normy

[197] zob. Preambuła do Rezolucji Zgromadzenia Ogólnego A/RES/20/2131,tzw. *Declarationon the Inadmissabilitiy of Intervetnion in the Domestic Affairs of States and the Protection of their Independence and Sovereignty*. Przyjęta na 12 sesji plenarnej 21 grudnia 1965 roku.

podstawowe kryterium rozróżniające inteferencję i interwencję. Przyjmuje się bowiem, że interwencja zawsze musi być dokonywana przy jej użyciu, interferencja natomiast jest wykonywana poniżej tego poziomu[198] Nie ma wątpliwości, że przymus konstytuuje użycie siły, trudno też zakwstionować fakt, że konieczną przesłanką pozytywną dla powstania interwencji jest skierowanie działań przeciwko *domaine réservé.*[199] Jednakże nie każde działanie uznawane za przymus w rozumieniu prawa międzynarodowego musi być tożsame z użyciem siły.

2. a. 8. Jurysdykcja hybrydowa

Koncepcja normowania faktycznego wymaga odzwierciedlającej taką teorię normatywną teorii jurysdykcji. Brak przyjęcia takiej teorii musiałby bowiem w istocie oznaczać odrzucenie koncepcji jurysdykcji wykonywanej w oparciu o *lex informatica per se*, a takiemu poglądowi wydaje się przeczyć praktyka międzynarodowa. Skoro bowiem mogą istnieć normy, których źródłem nie jest wykonujące jurysdykcję państwo, a istotą jurysdykcji jest wyłączność na normowanie na określonym terytorium - właściwym wnioskiem wydaje się przyjęcie, że jurysdykcja w normowaniu faktycznym nie istnieje. Jednak, jak wskazano powyżej, wniosek taki nie byłby uprawniony. Po pierwsze, państwa ciągle utrzymują monopol na prawo stanowione i sytuacja ta nie ulega zmianie także w niektórych zakresach cyberprzestrzeni. Po drugie, prawo to jest wykonywanym przez państwa środkiem normowania faktycznego. W istocie mamy więc do czynienia z sytuacją podobną do teorii jurysdykcji hybrydowej, istniejącej w jurysprudencji[200], choć nie mającej szerszego zastosowania praktycznego..[201] Teoria ta miała pierwotnie wyjaśniać

---

[198] zob. Aloupi N. *The Right to Non-intervention and Non-interference*, Cambridge Journal of International and Computer Law 4-556 (2015) ss.556-9

[199] A więc sprawy zastrzeżone do wyłącznego wykonywania w ramach własnej suwerenności.

[200] por. Berman P.Sch. *Global Legal Pluralism* Southern California Review 80 (2007) ss.1155 i n.

[201] Należy odróżnić jurysdykcję hybrydową zwaną w angielskim piśmiennictwie *hybrid legality* lub *hybrid legal space* od mającego zupełnie inne znaczenie terminu *wspólna jurysdykcja* [ang.*hybrid jurisdiction]*,odnoszącego się do klauzuli mającej charakter *prorogatio fori* w międzynarodowych umowach handlowych.zob. także Draguiew D. *Unilateral Jurisdiction Clauses: The Case for Invalidity, Severability or Enforceability.* Journal of International Arbitration 31, n.1 (2014) s.10 i n. wyd. Wolters Kluwer
W dalszej części niniejszej pracy, wszelkie odniesienia do pojęcie jurysdykcji

systemy nakładających się na siebie: (1)norm wynikających z prawa międzynarodowego; zarówno norm *erga omnes* jak i traktatów, jurysdykcji zwyczajnej i norm rozproszonych oraz (2) prawa krajowego (niekoniecznie wykonywanego terytorialnie).[202] Identyczny mechanizm umożliwia jednak wyjaśnienie zależności pomiędzy normowaniem cyberprzestrzeni wynikającym z jej architektury, które w praktyce oznacza dodanie jeszcze jednego czynnika. Jurysdykcja hybrydowa znajduje zastosowanie przede wszystkim do rozwiązywania problemów proceduralnych w procesach.[203] Możliwe wydaje się więc wykorzystanie opisywanej tu konstrukcji do utworzenia w przyszłości *sui generis* prawa procesowego dla wyspecjalizowanych sądów cyberprzestrzennych.

O ile jak wskazano powyżej, prawem materialnym służącym do rozpoznawania sporów musiałoby być *lex informatica*, możliwość przyjęcia formalnych norm krajowych, pozwalałaby na realną możliwość stworzenia systemu sądownictwa uwzględniającego specyfikę cyberprzestrzeni. Brak jednak jakichkolwiek działań w kierunku stworzenia takich wyspecjalizowanych sądów lub trybunałów przez jakikolwiek podmiot prawa międzynarodowego.

Pomijając brak praktyki międzynarodowej w tym zakresie, jurysdykcja hybrydowa wydaje się być jedną podstawą dla stworzenia formalnoprawnego aspektu *lex informatica*. Oczywiście, stworzenie prawa procesowego cyberprzestrzeni (pomimo iż *lex informatica* wynika głównie z praktyki podmiotów działających w cyberprzestrzeni[204]) znacząco zwiększyłoby możliwości wpływu państw narodowych na multicentryczny system w niej obowiązujący. Niewątpliwie byłaby to

---

hybrydowej, będą odnosić się do *hybrid legality*.

[202] zob. Williams S. *Hybrid and Internationalized Criminal Tribunals Jurisdictional Issues*, Durham Univerisity(2009) s.30 in.

[203] zob. Dickinson L. *The Promise of Hybrid Courts* American Journal of International Law 97:2 (2003) ss. 295-300

[204] Tak na przykład Robert Cover, *Law is constantly constructed through the contest of[...] various norm generating communities-Prawo jest stale tworzone jako funkcja sporu[...] wielu niezależnych grup generujących normy.* [w:Cover R.M. *The Supreme Court, 1982 Term- Foreword; Nomos and Narrative* Yale Law School Law Scholarship Repository 2705, (1983)s.4 i n.] Podobna, choć nie tak daleko idąca koncepcja wskazuje, że grupy o których pisze Cover stają się pośrednikami pomiędzy ustawodawcami a adresatami norm, mając udział w dokonywaniu ich konkretyzacji. Tak na przykład Seyla Benhabib [w: Benhabib S. *Another Cosmopolitanism* Oxford University Press (2006) ss.22-5].

pozytywna zmiana z punktu widzenia stosowalności norm generalnych prawa międzynarodowego publicznego (egzekwowalnych dużo łatwiej w przypadku państw niż często anonimowych *non-state actors*). Ostatnią, mocno korespondującą z naturą cyberprzestrzeni, cechą jurysdykcji hybrydowej jest także jej zmienność, zależnie od tego czy jest wykonywana w stosunkach między państwami, między państwem a podmiotem prawa międzynarodowego, czy też pomiędzy państwem a aktorem niepaństwowym.[205]

2. b. Zasady terytorialności i prohibitywności oraz ich wpływ na wykonywanie jurysdykcji w cyberprzestrzeni.

W klasycznym nowożytnym prawie międzynarodowym publicznym zasada terytorialności stanowiła w praktyce odpowiednik negatywnej konstrukcji własności prawie rzymskim.[206] Zakłada bowiem prawo państwa do wykonywania jurysdykcji wszystkich rodzajów w ramach swoich granic. Takie pojmowanie zasady terytorialności upraszcza relacje pomiędzy państwami.[207] Z zasadą terytorialności nieodwołanie łączą się więc pojęcia takie jak wspomniane wyżej: suwerenność czy zasada nieinterwencji. Dla części doktryny działanie państwa na określonym terytorium determinowało kierunek wzruszalnego domniemania, dotyczącego legalności działań lub zaniechań. O ile państwo działało na swoim terytorium - służyło jego działaniom domniemanie legalności. Działanie poza tym terytorium jest tego domniemania pozbawione, a wręcz dla części doktryny - w sposób domniemany nielegalne. Terytorialność we współczesnym rozumieniu stała się podstawowym elementem prawa międzynarodowego w okresie rozpoczętym podpisaniem Traktatu

---

[205] Przez część doktryny, podział ten jest uznawany za przesłankę uznania istnienia kilku niezależnych porządków prawa międzynarodowego, rozróżnianych właśnie podmiotowo zob. Osofsky H.M. *Climate Change Litigation as Pluralist Legal Dialogue,* Stanford Journal of International Law 43:19 (2007)ss.181-7. Twierdzi on, że mamy zamiast globalnego porządku prawa międzynarodowego mamy do czynienia z porządkiem *wielomodułowym (multiscalar)*.

[206] zob. Ryngaert C. *The concept of Jurisdiction in International Law,*[w: *Research Handbook on Jurisdiciton and Immunities in International Law,* Research handbooks in International Law series] wyd. Edward Elgar Pub. (2015) Utrecht Univeristy Repository]ss.10-8

[207] tak Buxbaum HL *Territory, Territoriality, and the Resolution of Jurisdictional Confilict*, American Journal of Comparative Law 57:631 (2009) ss.259-60

Westfalskiego z 1648 roku. Jednakże wraz z powstawaniem silnych instytucji międzynarodowych, terytorializm musiał zacząć tracić na znaczeniu. Podstawową zmianą, stanowiącą w praktyce koniec niekwestionowanego obowiązywania tej zasady, stał się moment, w którym państwa zostały zobowiązane do przestrzegania także tych norm, na które same się nie zgodziły. Stanowiło odejście od rozumienia traktatu jako podstawowego źródła praw i obowiązków międzynarodowoprawnych. Należy jednak wskazać, że istnieją głosy w doktrynie prawa międzynarodowego podtrzymujące takie pojmowanie relacji międzynarodowych.[208] Skoro więc istnieją normy niejako ponadpaństwowe, a co dużo bardziej istotne - możliwości egzekwowania tych norm, nie można już mówić o zasadzie zgody[209] w jej klasycznym rozumieniu. Należałoby też dokonać głębokich redefinicji zarówno pojęcia suwerenności jak i zasad nieinterferencji i nieinterwencji. Problem ten opisał sędzia Simma w swojej deklaracji,[210] w której wskazał, że prohibitywna natura prawa międzynarodowego odchodzi w przeszłość, coraz częściej bowiem państwa muszą wskazywać podstawy prawne i dowodzić legalności własnych działań, w tym nawet wewnątrz własnych granic. Taka koncepcja stoi w sprzeczności z dotychczasowym pojmowaniem zasady terytorialności opartej o doktrynę zgody.[211] Deklaracja sędziego Simmy była też swoistym meta-argumentem za upadkiem zasady prohibitywności, ponieważ wskazywał on, że Międzynarodowy Trybunał Sprawiedliwości powinien w swoim orzecznictwie dążyć do zmiany pojmowania prawa międzynarodowego i dostosować go do zmian w otaczającej rzeczywistości. Takie stanowisko nie może być interpretowane inaczej niż jako dalsze ograniczenie suwerenności państw. Łatwo zauważyć, że logiczną konsekwencją tego poglądu jest przyznanie Międzynarodowemu Trybunałowi Sprawiedliwości swoistej roli

---

[208] Przegląd argumentów przemawiających za utrzymaniem doktryny zgody przedstawił m.in. prof. Andrew Guzman- zob Guzman A. *The Consent Problem in International Law,* Berekely Program in Law and Economics Working Paper Series (2011) ss.14-20

[209] A więc teorii zakładającej, że państwa mogą być związane wyłącznie normami, na związanie którymi same wyrażą zgodę, uznawaną za komplementarną ze ściśle rozumianą zasadą terytorialności. zob. Idib. ss.3-4

[210] Deklaracja sędziego Bruno Simmy w sprawie *Accordance with Interniatonal Law ot the Unilateral Declaration of Independence in Respect of Kosovo (Request for Advisory Opinion*), Gr. Lst. 141, Międzynarodowy Trybunał Sprawiedliwości z dnia 22.czerwca 2010 s.1-6

[211] zob. Guzman A. *The Consent Problem...* ss. 3-10

prawotwórczej, zupełnie sprzecznej zarówno ze ściśle pojmowaną zasadą terytorialności jak i doktryną zgody.[212] Wobec istnienia licznych głosów wskazujących konieczność podjęcia przez trybunały i sądy międzynarodowe roli prawotwórczej[213], a także praktyki międzynarodowej w tym zakresie - należy przyjąć, że taki kierunek przyjmuje prawo międzynarodowe. Przywołana wcześniej opinia sędziego Alvareza była wyłącznie wskazaniem pewnego kierunku orzeczniczego, skierowanego bardziej do orzekających w przyszłości składów sądów i trybunałów międzynarodowych, nie zaś bezpośrednio do państw; może on być porównany do wiążących instrukcji orzeczniczych sądów najwyższych instancji wobec instancji niższych. Tymczasem deklaracja sędziego Simmy jest niewątpliwie skierowana na zewnątrz i jej zamiarem jest tworzenie normy *judge-made law*. Konieczne jest wskazanie, że deklaracja sędziego Simmy normuje zarówno bezpośrednio jak i w warstwie prawa zwyczajowego, ponieważ sam fakt wydania takiej deklaracji oznacza w logicznej konsekwencji posiadanie przez MTS jurysdykcji opartej o podstawowe zasaday prawa międzynarodowego (w tym wypadku o zasadę prohibitywności). Skoro więc MTS tę jurysdykcję posiada, to opinia sędziego Simmy niewątpliwie musi być wiążąca, choćby pośrednio. Wystarczy bowiem powołanie się na tą deklarację dowolnego składu międzynarodowego MTS, by jego orzeczenie uzyskało moc *res iudicata.* Ze względu na autorytet i pozycję orzeczeń Międzynarodowego Trybunału Sprawiedliwości, orzeczenie takie zyskałoby istotną pozycję w systemie prawa międzynarodowego. Sam fakt istnienia możliwości takiego orzeczenia (nawet jeżeli nigdy nie zostanie ono wydane) oznacza, że zasada terytorialności nie może funkcjonować w swoim tradycyjnym rozumieniu. Skoro bowiem to MTS ma jurysdykcję nad zasadami prawa międzynarodowego, ma prawo także je tworzyć i zmieniać swoimi orzeczeniami. Należy także wskazać na precedens, w którym MTS przyjął bezpośrednio bardzo podobną konstrukcję orzeczniczą.[214] Zasady wynikłe ze sprawy *Nicaragua*, omówione poniżej, stały się ważnym elementem zwyczajowego

[212] ibid.

[213] zob. też zdanie odrębne sędziego Alvareza w sprawie *Corfu Channel case, Jugdement of April 9th 1949, ICJ Reports 1949* str. 4

[214] Chodzi o *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Merits)* , ICJ Rep. (1986),par. 105-115.

prawa międzynarodowego w odniesieniu do prawa konfliktów zbrojnych. Nie podlega wątpliwościom nie tylko ważność tak konstruowanych orzeczeń, ale też wola państw do przyjmowania ich w praktyce na forum międzynarodowym.[215] Reguły wynikające z wyłączenia zasady prohibitywności prawa międzynarodowego publicznego nie są jedynym ograniczeniem zasady terytorialności. Stanowią jednak istotną zmianę w stosunku do najważniejszego dotychczas wyłączenia zasady terytorialności, a mianowicie istnienia norm *ius cogens* prawa międzynarodowego publicznego. O ile, *in abstracto*, istnienie tych norm wyłączało zasadę terytorialności nawet w czasach, kiedy funkcjonowała ona niekwestionowanie, problemem było wskazanie, które normy za *ius cogens* należy uznawać. Dotychczas dyskusji nie podlegał wyłącznie sposób przypisywania normom rangi *ius cogens*, polegający na: (1) ukonsytutowaniu się normy w jasnym i nie pozostawiającym wątpliwości brzmieniu (2) uznaniu za normę *ius cogens* przez społeczność międzynarodową.[216] W praktyce więc, *ius cogens* były czymś w rodzaju globalnych traktatów tyle, że zawieranych w sposób domniemany. Nie można było w żaden sposób twierdzić, że wyłączają one terytorialność państwa wyłącznie w tym sensie, że stanowią normy, których państwo nie może zmienić w ramach własnego porządku międzynarodowego. Jednakże samo uznanie normy za mającą taką rangę- wymagało udziału państwa, mieszcząc się w szerokiej interpretacji doktryny zgody. Jeżeli bowiem państwa nie wyraziły zgody na uznanie danej normy za *ius cogens*, to norma taka po prostu nią nie zostawała, a w konsekwencji nie zyskiwała mocy wiążącej *erga omnes*. W dzisiejszym prawie międzynarodowym norma o takiej randze może zostać państwom narzucona, choćby w sposób opisany powyżej przy okazji deklaracji sędziego Simmy czy orzeczeniu *Nicaragua*. Tak judykatura jak i doktryna przyjmuje także, że źródłem norm *ius cogens* mogą być traktaty, o ile spełnione zostają wskazane wyżej przesłanki.[217]

---

[215] Powinno się jednak odnotować, że istnieją w tej kwestii głosy przeciwne. Tak na przykład: Cassese A. -*The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia,* The European Journal of International Law 18:4 (2007) ss.27-30

[216] Art. 53 Konwencji Wiedeńskiej o Prawie Traktatów z 1969 roku, zob. także komentarz Shaw M. [w: *International Law* 5th edition, Cambrigde University Press, Cambridge 2003 ss.222-5]

[217] Tak Orzeczenie MTS w *North Continental Shelf Case,* ICJ Reports 42, 1969

Skoro więc istnieje możliwość tworzenia przez sądy i trybunały międzynarodowego *case law* o randze prawa zwyczajowego, nie sposób utrzymać koncepcji doktryny zgody. Jak bowiem przyjęła Komisja Prawa Międzynarodowego, „żaden traktat ani żadne państwo nie może uznać za legalne poważnego naruszenia normy *ius cogens"*.[218] Judykatura rozszerzyła także nieważność na zastrzeżenia traktatowe[219] i w praktyce przyjęła Kartę Narodów Zjednoczonych za supernormę *ius cogens*, wskazując że zobowiązania wobec niej są priorytetowe.[220]Co najmniej więc od momentu wejścia w życie opisanych powyżej orzeczeń nie sposób twierdzić, że państwo wykonuje jurysdykcję wyłączną na własnym terytorium.Innym wyłomem w zasadzie terytorialności było przyjęcie do prawa międzynarodowego publicznego rzymskiej zasady *sic utere tuo alienum non laedas*, po precedensowym orzeczeniu PTSM w sprawie *Trail Smelter*[221]. Przyjęcie to zapoczątkowało rozwój całej gałęzi prawa zwyczajowego, regulującej kwestie odpowiedzialności za naruszenia prawa uregulowanej finalnie w ARSIWA - mających przecież status *black-letter law*. Zasady wypracowane we wspomnianym arbitrażu także wyłączają pełną wolność do działania na własnym terytorium przez państwa, wprowadzając do prawa międzynarodowego publicznego cały reżim odpowiedzialności za działania, których wyłączne skutki mogą być zlokalizowane na terytorium innych państw.

Jest oczywiste, że cyberprzestrzeń *per se* stanowi jeden z elementów postępującej globalizacji i coraz większego osłabiania powiązań suwerenności i terytorialności. Z drugiej jednak strony, to właśnie kierunek w jakim wydaje się podążać prawo cyberprzestrzeni, gwarantuje państwom najwięcej możliwości zachowania własnej suwerenności i możliwości projekcji siły na arenie międzynarodowej. Porządek prawny w świecie fizycznym, w którym organizacje ponad- i międzynarodowe zyskują coraz większy wpływ na prawo międzynarodowe publiczne jest bowiem

---

[218] Art. 41(2) *Draft Articles on State Reponsibilities for Internationaly Wrongful Acts*, Yearbook of the International Law Commission, 2001, tom II, cz. druga, przyjęty w 2008 roku wraz z późniejszymi zmianami.

[219] Tak MTS (sędziowie Tanaka i Padilla Nervo) w *North Sea...*

[220] Tak sędzia E. Lauterpacht w zdaniu odrębnym do *Case Concerning application of the Convention onf the prevention and Punishment of Crime of Genocide,* ICJ reports 1993 440;95 (1993) s.325

[221] zob. *Trail Smelter Case* (USA, Canada)(1941), United Nations Reports of International Arbitral Awards, t.3 (2006) ss.1905-72

w coraz bardziej widoczny sposób tworzony odgórnie.

Państwa w coraz szerszym zakresie zostają związane prawem tworzonym przez te podmioty, a zakres przedmiotowy normowania poddanego ich jurysdykcjom zmniejsza się. Tymczasem *lex informatica* tworzone jest oddolnie, a państwa dysponujące narzędziami w ramach własnej jurysdykcji nadzwyczajnej i zwyczajnej (w odniesieniu do części fizycznej) stoją w jego tworzeniu na uprzywilejowanej pozycji. Tej cechy nie mają pozostałe *commons*, których status opiera się o traktaty i konsensus państw, w istocie pozostając w zakresie przedmiotowym tradycyjnego prawa narodów.[222] Tymczasem o ile do cyberprzestrzeni mogą stosować się klasyczne regulacje prawa międzynarodowego[223], funkcjonują one wyłącznie w ograniczonym zakresie, opartym o stan faktyczny. Stają się więc regulacje tworzone ponadnarodowo wyłącznie pewnym dodatkowym, pośrednim (bo wiążącym same państwa, a nie normy tworzone przez nie w cyberprzestrzeni) czynnikiem. Czynnik ten oczywiście ma istotny wpływ na działania państw, nie wyjmując jednak normowania cyberprzestrzeni spod ich jurysdykcji. Wydaje się więc, że ze względu na to zróżnicowanie, cyberprzestrzeń podlega zupełnie odrębnemu reżimowi prawnemu niż pozostałe *commons*.[224] W tych ostatnich bowiem jurysdykcję nadzwyczajną należy uznać za *lex specialis* wobec jurysdykcji zwyczajnej. W przypadku cyberprzestrzeni natomiast jurysdykcja nadzwyczajna funkcjonuje niejako niezależnie od zwyczajnej, w oparciu o zupełnie inny zestaw przesłanek. Nie ma wątpliwości, że w taki sposób właśnie funkcjonuje jurysdykcja nadzwyczajna w informatycznej części cyberprzestrzeni. Wynika to z faktu, że dwie uznawane za najmocniejsze, przesłanki wykonywania jurysdykcji nadzwyczajnej[225]- *rationae loci* i *ratione personae*[226], są w cyberprzestrzeni nieomal nieobecne, odpowiednio ze

---

[222] Zhang W. *Extraterritorial Jurisdiction on Celestial Bodies*,Elsevier, Space Policy 47 (2019) ss.148-57

[223] cf. Dunk von der F.G. *The role of law with respect to future space activities*,Elsevier, Space Policy 12(1) (1996) s.40

[224] ibid. s.41

[225] zob. Zhang W. *Extraterritorial...* s. 151

[226] Wynika to z zasady anonimowości cyberprzestrzeni jak i z jej prawnych konsekwencji. Zidentyfikowanie określonej osoby, o ile jest ona kwalifikowanym hakerem jest niewykonalne nawet po udanej atrybucji na poziomie identyfikacji aktora. Z tego stanu faktycznego, wynika odrzucenie przez doktrynę *rationis personae,*

względu na wszechobecność i anonimowość cyberprzestrzeni. Dochodzi więc do dwóch istotnych zmian w pojmowaniu jurysdykcji nadzwyczajnej w cyberprzestrzeni. Pomimo zachowania w rozumieniu prawa międzynarodowego publicznego charakteru środka *de iure* nadzwyczajnego - staje się ona *de facto* podstawowym sposobem wykonywania jurysdykcji w ogóle i ochrony przez państwa własnej suwerenności w cyberprzestrzeni (uzupełnianym przez jurysdykcję terytorialną w odniesieniu do części fizycznej). Tak pojmowane stosowanie jurysdykcji nadzwyczajnej w cyberprzestrzeni w praktyce rozpoczęły Stany Zjednoczone,[227] z czasem jednak stało się przyjętą praktyką międzynarodową. Jurysdykcja nadzwyczajna wykonywana przez państwa wyłącznie wobec informatycznej części cyberprzestrzeni jest nieomal zupełnie oderwana od zasady terytorialności, oparta jest bowiem co do zasady albo o zasadę ochronną albo doktrynę efektu.[228] Staje się więc nowym, odrębnym porządkiem, niezależnym od tego, o który oparta jest jurysdykcja nadzwyczajna wykonywana w pozostałych *commons* (z wyjątkiem przestrzeni kosmicznej). W odróżnieniu od pozostałych *commons* w cyberprzestrzeni jurysdykcja preskrypcyjna ma istotne (choć pośrednie) znaczenie (konstytuując wyjątek od opisanej wyżej zasady, zakładającej obniżenie rangi zasady terytorialności).[229] W cyberprzestrzeni natomiast prawo krajowe zyskuje skutek w odniesieniu do całej cyberprzestrzeni (normując bezpośrednio jej infrastrukturę zlokalizowaną na terytorium danego państwa a pośrednio cyberprzestrzeń jako całość, w ramach *lex informatica*). Także zasada wszechobecności cyberprzestrzeni ma liczne aspekty wzmacniające możliwość ochrony przez państwa własnych interesów, choćby poprzez stwarzanie realnej możliwości skutecznego przeciwdziałania naruszeniom

---

wykonywana poza światem fizycznym. zob. *Smith v. United States* 507 US 197,122, (1993), zdanie odrębne sędziego Stevensa. Także Menthe D.C. *Jurisdiction in Cyberspace: A Theory of International Spaces* Michigan Telecommunications and Technology Law Review 4:1 (2007) ss.83-8

[227] por. Blakesley Ch. *Criminal Law: United States Jurisdiction Over Extraterritorial Crime,* Journal of Criminal Law 73-6 (1982) ss.1109-10

[228] Część doktryny przyjmuje nie tylko, że cyberprzestrzeń znosi zasadę terytorialności, ale że wręcz nie ma możliwości stosowania do niej dzisiejszych instytucji prawnych z zakresu jurysdykcji, ponieważ zmiany stanu faktycznego idą zbyt daleko. cf. Byassee *Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community*, Wake Forest Law Review 30 (1995) s.196

[229] zob. Schrijver N. *Managing the global commons: common good or common sink?*, Third World Quaterly 37:7 (2016) ss.1254-7

własnej suwerenności przy pomocy ograniczonych (bo wyłącznie cyberprzestrzennych) środków, nie wymagających precyzyjnej atrybucji, o ile odpowiedzi te nie konstytuują ekwiwalencji kinetycznej w świecie rzeczywistym.

Cyberprzestrzeń konstytuuje też specyficzne pojmowanie zasady prohibitywności. Funkcjonuje ona bowiem w niej na dwóch, niezależnych od siebie poziomach. Po pierwsze - w systemie prawa międzynarodowego na zasadach ogólnych. Na tym poziomie ma ona wpływ na wszystkie elementy prawa cyberprzestrzennego stanowionego w tradycyjnym procesie legislacyjnym (a więc na przykład na normy prawa stanowionego pośrednio, wpływające na *lex informatica* czy też na jurysdykcję wykonywaną w odniesieniu do fizycznej części cyberprzestrzeni). Drugim etapem jest zasada prohibitywności w rozumieniu *lex informatica* i jego normowania faktycznego. W tym systemie oznacza ona sumę wszystkich możliwości architektury cyberprzestrzeni, która sama jest normowana przez prawo i bezpośrednio normuje zachowania podmiotów w niej samej. Oczywiście, obydwa te znaczenia są ze sobą powiązane na metapoziomie. Przykładowo - norma faktyczna zakazująca komunikacji cyberprzestrzennej, pozbawionej pewnej z góry określonej identyfikacji nadawcy w pakiecie danych, będzie działała na drugim ze wspomnianych poziomów, faktycznie zakazując komunikacji innych niż określone przez kod. Jednak ograniczenie to musi być uprzednio stworzone w drodze normy prawnej, nakazującej podmiotom kontrolującym przepływ danych w określonej sieci wstrzymywanie przesyłu danych, nie odpowiadających określonemu wzorcowi. Odmówienie legalności jednej z tych norm, na którymkolwiek poziomie - będzie skutkowało utratą przez nią mocy normatywnej także na drugim z nich.[230]

[230] Opisany przykład identyfikowalnej komunikacji wzięty został z prawodawstwa stanu Georgia, który wymagał podobnej identyfikacji od pakietów przesyłanych przez położone na jego terytorium elementy fizycznej części cyberprzestrzeni. Ze względu na potwierdzenie przez Sąd Najwyższy prawa do anonimowego wyrażania opinii, norma ta została usunięta. zob.Orzeczenie w sprawie *ACLU v. Miller 977 F. Supp 1228 (N.D. Ga. 1997)*, zob. też Barlett R. et al. *Developments in the Law. The Law of Cyberspace*, 112 Harvard Law Review(1999) ss. 1607-9

2. c. Granice jurysdykcji preskrypcyjnej we współczesnym prawie międzynarodowym publicznym dotyczącym cyberprzestrzeni.

Niezależnie od niejasności dotyczących zasady terytorialności przyjęcie koncepcji cyberprzestrzeni jako swoistego rodzaju miejsca musi implikować istnienie pewnych granic jurysdykcji. Przeprowadzone wyżej rozważania na temat podziału cyberprzestrzeni i podporządkowania jej części fizycznej klasycznemu, terytorialnemu pojmowaniu jurysdykcji, należy uzupełnić o analizę sytuacji, w których jurysdykcja jest wykonywana przez wiele podmiotów. Nie chodzi jednak o klasyczny konflikt jurysdykcyjny (jak w przypadku istnienia podstaw do wykonywania jurysdykcji przez kilka państw w stosunku do jednego podmiotu), a o sytuację, w której podmiot jurysdykcji w cyberprzestrzeni istnieje poza jurysdykcją terytorialną. Faktyczne położenie części fizycznej cyberprzestrzeni, biorące udział w określonym działaniu, jest dla tego działania po prostu nieistotne. Dobrym przykładem może być wspomniana powyżej sprawa *Yahoo! Inc. v. L.I.C.R.A.*. Zarówno położenie serwerów, jak i kraj rejestracji spółki czy prawo, w którym jest ona rejestrowana nie ma znaczenia dla próby wykonania jurysdykcji przez państwo, które chce chronić własną suwerenność przed określonym sposobem działalności w cyberprzestrzeni, choćby działanie to nie tylko nie było wrogie wobec tego państwa, ale wręcz legalne według prawa krajowego innego państwa. Wynika to z faktu, iż wykonywanie jurysdykcji wobec danego podmiotu wymaga spełnienia pewnych zasad, określonych w prawie krajowym.[231] Przeniesienie takiej działalności, nie wymagające prawie żadnego wysiłku po stronie podmiotu ją prowadzącego (serwis umożliwiający wykonywanie określonych działań, może po prostu zostać uruchomiony z serwera znajdującego się w innej jurysdykcji, lub przez spółkę zarejestrowaną w innym systemie prawnym). Wobec takiego działania to państwo wykonujące *imperium* stoi *de facto* na pozycji słabszej gdy próbuje realizować *ratio legis* własnych ustaw. Należy więc rozważyć, jakie kroki musiałoby wykonać państwo w celu wykonania jurysdykcji wobec podmiotu istniejącego

[231] por. Gladstone J.A. *Determining Jursidiction in Cyberspace: The "Zippo "Test or "Effects" Test?* InSite "Where Parallels Intersect", Informing Science (2003)ss. 4-10

w cyberprzestrzeni, przy założeniu że wykonanie jej na bazie terytorialnej, choć teoretycznie możliwe, w praktyce będzie pozbawione znaczenia.[232] Dodatkową komplikację stanowi fakt, że dwa „najmocniej" obecne w cyberprzestrzeni systemy prawne, czyli system Stanów Zjednoczonych i szeroko pojmowanej Europy ze szczególnym uwzględnieniem UE, są niewspółmożliwe. Wykonanie jurysdykcji w systemie amerykańskim wymaga przede wszystkim „związku sprawy, sądu i stron[233]", wyłączając jednak wymóg fizycznej obecności podmiotu, co do którego jurysdykcja ma być wykonywana.[234] W Unii Europejskiej co do zasady obowiązuje prawo domicylu.[235] W oczywisty sposób obydwa te systemy nie są skuteczne w cyberprzestrzeni. W sytuacji działań w cyberprzestrzeni możliwe jest stosowanie dwóch, wykluczających się wzajemnie, zestawów pozytywnych przesłanek istnienia jurysdykcji w stosunku do tego samego zachowania, zaniechania, podmiotu lub przedmiotu. Ponieważ przesłanki jurysdykcji UE są szersze, zwiększają zakres możliwości wykonywania własnej jurysdykcji w cyberprzestrzeni. Kwestia tak ustalanych granic, będzie jednym ze sposób prowadzenia działań w ramach *cyberlawfare*, które zostaną szczegółowo opisane w dalszej części wywodu.

3. Wykonywanie jurysdykcji w cyberprzestrzeni.

Punktem wyjścia do rozważań na temat jurysdykcji w cyberprzestrzeni musi być oczywiście wskazanie rozwiązania problemu, tworzonego przez wielość źródeł regulacji czy też, jak chce część doktryny, multicentryczność współczesnych systemów prawnych. Problem ów nie jest nowy, a jego korzenie sięgają rozwoju

---

[232] por. Hollis D.B. *Why States Need an International Law for Information Operations*, Lewis & Clarck Law Review 11 (2207) ss. 1023 i 1026

[233] Sąd Najwyższy Stanów Zjednoczonych w ten sposób zinterpretował zasadę uczciciwego procesu tzw. *Due Process Clause*. por. Orzeczenie w sprawie *Shaffer v. Heitner* , 433. Supreme Court of United States 186 orzeczenie z 1997 roku.

[234] por. *Burger King Corp. v. Rudzewicz* 471 U.S. 462 1985

[235] por. Konwencja o jurysdykcji i uznawaniu oraz wykonywaniu orzeczeń sądowych w sprawach cywilnych i handlowych, podpisana w Lugano 16 września 1988 roku Dz.U. 2000 nr 10 poz. 132 Wszystkie kraje Unii, z wyjątkiem Danii przyjmują jako główną zasadę postępowań w UE zasadę domicylu, przyjmuje ją także Regulacja Parlamentu Europejskiego i Rady z grudnia 2012 o syg. 1215/2012 *w sprawie jurysdykcji i uzanawania orzeczeń sądowych oraz ich wykonywania [tzw. Bruksela I]*.Dz.U UE L 351, z 20 grudnia 2012 roku.

organizacji ponadnarodowych, ale w cyberprzestrzeni, ze względu na jej uwarunkowania faktyczne podmioty mające na nią wpływ nie tylko nie są ujęte w jakimś zamkniętym katalogu, ale też nie jest nawet do końca jasne o jakie podmioty chodzi. Wobec tego nie można stworzyć zbioru doprecyzowanych zasad postępowania na wypadek kolizji tych normowań ani sposobu wskazywania ich granic. Jeżeli natomiast zasady jurysdykcji określające te granice dla danego zakresu nie są odpowiednio zakreślone, ryzyko kolizji zwiększa się, w skrajnym wypadku uniemożliwiając stosowanie prawa i powodując normatywny paraliż.[236] Szczególnie jasno widać to w prawie międzynarodowym prywatnym, gdzie brak równej pozycji prawnej pomiędzy obywatelem a dysponującym *imperium* państwem. Konieczność dostosowania się do norm stanowionych w ramach jurysdykcji państwowej jest dla jednostki wymogiem bezwzględnym. W przypadku więc, gdy jurysdykcje te nakładają się na siebie i są ze sobą niewspółmożliwe, jakiekolwiek działania jednostki staną się niewykonalne dopóki kolizja nie zostanie usunięta. Sama natomiast jednostka nie będzie zdolna nawet doprowadzić do usunięcia tej kolizji. Może się więc zdarzyć, że prawo dla jednostki przestanie działać a zagwarantowane jej przez którąkolwiek ze skonfliktowanych jurysdykcji przywileje staną się wyłącznie teoretyczne. W praktyce bowiem nie będzie możliwości ich wykonania, ponieważ prowadziłoby to do złamania prawa wiążącego równocześnie tę jednostkę w innej jurysdykcji. Oczywiście problem ten występuje tylko i wyłącznie w układach międzynarodowych, gdzie podmiot jest poddany więcej niż jednej jurysdykcji w danym czasie. Istnienie cyberprzestrzeni odwraca zwroty wektorów tych ograniczeń. Bowiem to państwa w identycznej sytuacji muszą dostosować się do zastanego funkcjonowania cyberprzestrzeni, chyba że są w stanie spowodować określoną zmianę w jej całości. Jednostki natomiast mogą wybierać w ramach wszechobecnej cyberprzestrzeni te jurysdykcje, w których dane działanie może być wykonane. Jest to sytuacja podobna do opisanego już sporu *Yahoo! v. L.I.C.R.A*. Oczywiście w niektórych przypadkach państwa mogą rozstrzygnąć określoną kolizję

[236] Mills A. *Rethinking Jurisdiction in International Law* British Yearbook on International Law t.84 nr 1(2014), Oxford University Press s.188 in.

na swoją korzyść, ale w żaden sposób nie wpływa to na zakres ich jurysdykcji w cyberprzestrzeni. Wskutek tego w cyberprzestrzeni krzyżowanie się zakresów jurysdykcji powoduje (odwrotnie niż w przywołanym powyżej przykładzie) paraliż normatywny po stronie podmiotów jurysdykcję wykonujących. Jednocześnie zaś zwiększa się swoboda podmiotów w cyberprzestrzeni działających (a więc do pewnego zakresu także twórców *lex informatica*). Działając w cyberprzestrzeni, państwo musi więc posłużyć się *lex informatica*, a więc wewnętrznym prawem cyberprzestrzeni, aby chronić dobra prawne, chronione przez własny wewnętrzny porządek prawny. Ten z kolei wpływ państwo wykonywać będzie przy pomocy własnego prawa krajowego.

4. Jurysdykcja nad fizyczną częścią cyberprzestrzeni

Jurysdykcja ta, jak już wskazano powyżej niewątpliwie oparta jest o zasadę terytorialności. Państwo ma te same prawa i obowiązki w odniesieniu do infrastruktury należącej do części fizycznej cyberprzestrzeni położonej na swoim terytorium, jak w odniesieniu do jakiejkolwiek innej instalacji. Nie przeszkadza temu prawu fakt, że w ten sposób państwo wykonuje swoją jurysdykcję w odniesieniu do urządzeń sieciowych.[237] Podobna sytuacja panuje w stanie prawnym dotyczącym podmorskich kabli zapewniających łączność międzypaństwową, a analogia w tym zakresie wydaje się niekwestionowana zarówno przez doktrynę jak i praktykę międzynarodową.[238] Nie ma więc wątpliwości, że ochrona podobnej infrastruktury, nie jest uznawana za dobro prawne tak istotne, by uzasadnione było przyznanie jej ochrony za pomocą normy wiążącej *erga omnes*[239]. Wiele krajów, które nie ratyfikowały traktatów dotyczących ochrony kabli podmorskich nie wykonuje ich postanowień. Nie sposób też wskazać żadnych działań podmiotów obrotu międzynarodowego mających na celu stworzenie normy, która postanowienia te mogłaby tym państwom narzucić w drodze innej niż dobrowolne związanie traktatem. Przykładowo Stany Zjednoczone zobowiązały się do przestrzegania ochrony kabli podmorskich w sposób odpowiadający wskazanemu w traktacie z zastrzeżeniem, że związanie to będzie obowiązywać tylko w takim zakresie, w jakim utrzymanie w dobrym stanie kabli podmorskich będzie zasadne z punktu widzenia interesów Stanów Zjednoczonych; oświadczenie to zostało przyjęte przez społeczność

---

[237] zob. Bressie K. *Marine Jurisdictional Problems for Sumbarine Cables*, SubOptic 2016, Dubaj (2016) s.24 i n.

[238] Davenport T. *Submarine Cables, Cybersecurity ad International Law: An Intersectional Analysis*. Catholic University Journal of Law and Technology t. 25 wyd. 1, .(2015)s. 109

[239] zob. Art. 1 Konwencji międzynarodoej o ochronie kabli podmorskich, sporządzona w Paryżu 14 marca 1884 roku, Dz. U. 1935 nr 17 poz.97

. Przywołana konwencja zobowiązywała wyłącznie swoich sygnatariuszy do wprowadzenia do swoich odpowiednich porządków prawnych zapisu penalizującego celowe naruszenia kabli (o ile nie wystąpią przesłanki eksonerujące, przykładowo w przypadku wojny zapisy nie obowiązywały); także art. 27 Konwencji o Morzu Pełnym i art. 4 Konwencji o Szelfie Kontynentalnym (obydwie podpisane w Genewie w 1958) a także art. 113-115 Konwencji z Montego Bay. Wszystkie te konwencje utrzymywały wprowadzaną przez Konwencję Paryską zasadę wstrzymania się od uznania nawet intencjonalnego naruszania kabli za delikt międzynarodowoprawny.

międzynarodową.[240] Należy więc przyjąć, że sam fakt, że dany przedmiot jest elementem jakiegoś globalnego systemu nie wpływa negatywnie na wykonywanie jurysdykcji przez dane państwo co do jego elementów.

Identycznemu normowaniu podlegają fizyczne elementy cyberprzestrzeni. Skoro więc brak jakiegokolwiek traktatu regulującego tą kwestię, należy przyjąć, że obowiązują normy ogólne. Jednak taka interpretacja powoduje kolejne problemy. W przypadku cyberprzestrzeni nie sposób bowiem oddzielić infrastruktury fizycznej, od powiązanych z nią elementów informatycznej części cyberprzestrzeni. Należy więc rozważyć dwa zagadnienia.

Pierwszym jest wzajemne oddziaływanie na siebie elementów informatycznej i fizycznej części cyberprzestrzeni, a co za tym idzie - wykonywania przez państwa jurysdykcji zwyczajnej w dużo większym zakresie niż wynikałoby to z samej zasady terytorialności. Przykładem takiego wykonania jurysdykcji mogłoby być zniszczenie przez państwo serwera położonego na własnym terytorium jednocześnie eliminujące z informatycznej części algorytmy, umożliwiające działanie istotnego dla państwa trzeciego serwera, zlokalizowanego terytorialnie w jurysdykcji obcej. Kwestie wpływania na część informatyczną zostaną szczegółowo omówione w dalszej części wywodu, jednak sytuację opisaną powyżej należy uznać za wyłącznie teoretyczną.

Dużo istotniejszą kwestią jest natomiast problem obchodzenia jurysdykcji państwa, poprzez oparcie powiązanego z takim działaniem przesyłu danych w cyberprzestrzeni o infrastrukturę fizyczną położoną w jurysdykcji obcej (najczęściej takiej, w której zachowanie takie jest legalne). Ze względu na wszechobecność cyberprzestrzeni jest bowiem obojętne dla użytkownika końcowego, o jaką infrastrukturę fizyczną opiera się dany transfer. Natomiast z punktu widzenia państwa takie przesunięcie może być znaczącym utrudnieniem wykonywania własnej jurysdykcji na własnym terytorium. Przykładem takiego działania może być spór władz francuskich z koncernem Yahoo!, dotyczący umożliwienia przez tą firmę sprzedaży pamiątek po oddziałach Wehrmachtu, SS a także funkcjonariuszach NSDAP i rządu Vichy na stronach

[240] zob. *Statement on United States Oceans Policy,* oświadczenie prezydenta Ronalda Reagana z dnia 10 marca 1983 roku, Administration of Ronald Reagan, Public Papers, National Archives and Records Administration (1983).

aukcyjnych prowadzonych przez Yahoo!.[241] Strony te zostały udostępnione francuskim użytkownikom, znajdującym się i łączącym się z internetem za pomocą serwerów umieszczonych na francuskim terytorium. W związku z zakazem strona powodowa, czyli francuska Liga przeciw Antysemityzmowi wraz z organizacjami stowarzyszonymi wskazywała, że sam fakt dopuszczania podobnych obiektów do obrotu, poza określonymi trybami dotyczącymi muzeów, jest niezgodny z francuskim prawem.[242] Problematyczna okazało się jednak sama kwestia określenia stron w procesie. *Yahoo France* (spółka córka amerykańskiej korporacji, utworzona na prawie francuskim), bez wątpienia miała bierną legitymację procesową w tej sprawie. Jednakże wszystkie jej działania były wykonywane na zlecenie głównego koncernu *Yahoo! Inc.*, będącego podmiotem prawa amerykańskiego i wobec tego znajdującego się poza jurysdykcją sądów francuskich. Niemniej w orzeczeniu z dnia 22 maja 2000 roku, sąd francuski nakazał *Yahoo! Inc.* „uniemożliwienie dostępu do swojej witryny *yahoo.com* dla odbiorców francuskich, by wyłączyć lub choćby zminimalizować ryzyko możliwości naruszenia przez taką osobę francuskiego prawa"[243], dając korporacji dwumiesięczny termin na techniczną implementację orzeczonego zabezpieczenia. *Yahoo! Inc.* wniosło środek odwoławczy argumentując zarówno, że francuskiemu sądowi brak jurysdykcji nad amerykańską spółką, jak i podnosząc niemożliwość sortowania użytkowników ze względu na kraj, z którego łączą się z witryną. Spółka wskazała, że w związku z tym bezcelowe jest usuwanie aukcji z wyszukiwarek dostępnych wyłącznie w serwisie w domenie .fr (dostępnej dla połączeń kierowanych przez francuskie serwery). Każdy użytkownik francuski mógł bowiem połączyć się z domeną *yahoo.com* zlokalizowaną na serwerach w Stanach Zjednoczonych i uzyskać dostęp do tych samych danych, które zostaną zablokowane w domenie .fr. Trybunał odrzucił skargę *Yahoo* i wydał kolejne postanowienie, ponawiając nakaz wydany uprzednio oraz nakładając na *Yahoo* grzywnę w razie

[241] La Ligue Contre le Racisime et L'Antisemitisme (L.I.C.R.A), L'Union des Etudiants Juifs de France (U.E.J.F.) v. Yahoo! Inc., Yahoo France. Zawisła przed Trybunałem Wielkiej Instancji w Paryżu w roku 2000.

[242] zob. Art. R.645-1 *Code Penal*, w jego brzmieniu z roku 2003

[243] Nakaz *interim* wydany przez Trybunał Wielkiej Instancji w sprawie L.I.C.R.A&U.E.J.F. v. *Yahoo Inc & Yahoo Fr.* z dnia 22 maja 2000 roku .

dalszego niewykonania.[244] *Yahoo! Inc. w*skazało natomiast, że nie wykona żadnego postanowienia, które nie zostanie inkorporowane do amerykańskiego porządku prawnego i w związku z tym skierowało pozew do sądu okręgowego w Kaliforni w celu ustalenia, czy jest zobowiązane poddać się orzeczeniom sądu francuskiego.[245] Analizując wskazany stan faktyczny pod kątem opisywanych tu zasad, musimy dojść do wniosku, że sąd amerykański nie mógł na tym etapie chronić zasad nieinterwencji i nieinterferencji, niezależnie od wyroku jaki by wydał. Należy zauważyć, że umożliwianie obejścia prawa dotyczącego regulacji sprzedaży musi być uznane za ingerencję w sprawy wewnętrzne zarezerwowane dla państwa. Działa to jednak w obie strony. Na mocy zasad nieinterferencji i nieinterwencji, czynem bezprawnym jest zarówno umożliwianie takiej sprzedaży przez *Yahoo!* jak i jej zakazywanie przez francuski sąd. Pierwszy z nich byłby bowiem umożliwianiem działania nielegalnego w jurysdykcji francuskiej, drugi natomiast byłby ograniczaniem swobody podmiotu, zupełnie nie poddanego jurysdykcji sądów francuskich (tej bowiem podlegało wyłącznie *Yahoo France*, które nie prowadziło kwestionowanych aukcji, a wyłącznie sprawowało techniczne i pomocnicze działania spółki we Francji).[246] O ile Trybunał Wielkiej Instancji orzekał wyłącznie na gruncie prawa francuskiego, chroniąc francuską suwerenność, pozew wniesiony do sądu dla okręgu Północnej Kalifornii, musiał w istocie prowadzić do złamania obydwu zasad. Sąd amerykański miał bowiem możliwość[247] orzec słuszność jednego ze wspomnianych wariantów.[248]

---

[244] Nakaz *interim* wydany przez Trybunał Wielkiej Instancji w sprawie L.I.C.R.A&U.E.J.F. v. *Yahoo Inc & Yahoo Fr* z dnia 11 listopada 2000 roku.

[245] *Yahoo! Inc.* v. *(L.I.C.R.A) et al.* US District Court for the Northern District of California- 145 F. Supp. 2d 1168, pozew wniesiono dnia 7 czerwca 2001 roku.

[246] Sąd amerykański rozważający sprawę analizował możliwość uznania sądu francuskiego w tym zakresie za przemiennie właściwy miejscowo - ostatecznie koncepcję tę jednak odrzucił. zob. *Yahoo! Inc. V. L.I.C.R.A.* 145 F. Supp 2d at 1168, par.7, szerzej argumentacja ta została omówiona w glosach do orzeczenia zob. Na przykład Greenberg M.H. *A Return to Liliput: The LICRA v. YAHOO! Case and the Regulation of Online Content in the World Market*, Berkeley Technology Law Journal 18 (2003) ss.1241-2

[247] Część doktryny stoi wręcz na stanowisko, że sąd kalifornijski związany był zasadą *stare decisis* na gruncie precedensowego *case law* amerykańskiego. W sprawie *First National Bank of Boston v. Belotti 435 U.S. 765* (1978), uznano że konstytucyjna zasada wolności słowa chroni tak samo osoby prawne jak osoby fizyczne. W sprawie *Texas v. Johnson 491 U.S. 397* (1989) uznano natomiast, że sam fakt, że głoszenie określonych poglądów może naruszać uczucia określonych grup społecznych nie może zostać uznany za podstawę zakazania głoszenia tych poglądów. zob. także Okoniewski E.A. *Yahoo!,Inc. V. LICRA: The French Challenge to Free Expression in the Internet* American University

Uznając postanowienie sądu francuskiego wobec amerykańskiej spółki działającej w amerykańskiej jurysdykcji, musiałby złamać zasadę nieinterferencji wobec Stanów Zjednoczonych. Powodem złamania byłoby nie tyle powstanie obowiązku wobec podmiotu amerykańskiego; jednak ponieważ zobowiązującym byłby *de iure* sąd amerykański, postanowienie Trybunału byłoby więc inkorporowane do amerykańskiego porządku prawnego, co nie byłoby z kolei możliwe gdyż - jak wskazano powyżej - byłoby z tym porządkiem sprzeczne. Ponadto oznaczałoby to różnicowanie sytuacji prawnej *Yahoo Inc.* ze względu na fakt, że jest on właścicielem podmiotu prawa francuskiego, co z kolei byłoby złamaniem obowiązującej w USA zasady równości podmiotów wobec prawa. Stanowiłoby też skuteczny wpływ sądu francuskiego na podmiot prawa amerykańskiego i w logicznej konsekwencji - interferencję Francji w sprawy podlegające wyłącznemu normowaniu Stanów Zjedocznonych. Tymczasem w razie odmowy inkorporacji postanowienia, sąd amerykański *implicite* godziłby się na ingerowanie przez *Yahoo! Inc. w* porządek prawny obowiązujący we Francji, a przecież amerykańskie orzecznictwo interpretuje gwarantującą wolność słowa pierwszą poprawkę do Konstytucji USA jako wiążącą każdego aktora państwowego.[249] Łatwo więc zauważyć, że wynikające z zasady wszechobecności problemy jurysdykcyjne, utrudniają znacząco egzekwowanie prawodawstwa danego państwa w stosunku do elementów infrastruktury fizycznej cyberprzestrzeni (pomimo, że niewątpliwie są one poddane jego jurysdykcji). Z kolei zasada niemożliwości fizycznego zlokalizowania wyłącza jasne określenie jurysdykcji, której prawodawstwo decyduje. Ze względu na fakt, że norma zakazująca danego zachowania jest elementem zwykłego porządku prawnego, a cyberprzestrzeń stanowi wyłącznie nośnik pewnych treści - brak możliwości zastosowania do rostrzygnięcia sporu norm *lex informatica*. Doraźnym rozwiązaniem tego problemu,

International Law Review 18:1 (2002) ss.316-20

[248] Warto zauważyć, że w przedmiotowej sprawie, Sąd Najwyższy Stanów Zjednoczonych, odmówił wydania *writ of certiorari*,o który w sprawie wnoszono.

[249] zob. Opinię Sądu Najwyższego USA w sprawie *Manhattan Community Access Corp. et al. v. Deedee Halleck et al.*, wydaną w odpowiedzi na *writ of certiorari* Sądu Apelacyjnego drugiego okręgu 17-702, 587 U.S. (2019) s.1

sugerowanym przez część doktryny byłoby przyjęcie jurysdykcji miejscowej[250], tzw. „jurysdykcji kraju pochodzenia"[251]. Na mocy takiej regulacji o możliwościach działania określonych spółek decydowałoby prawo domicylu lub prawo państwa, w którym spółki te posiadają centrum swojej działalności. Przyjęcie tej koncepcji nie rozwiązuje jednak podstawowego dla kwestii jurysdykcji nad częścią fizyczną cyberprzestrzeni problemu - możliwości istnienia w cyberprzestrzeni zachowania, będącego legalnym w jurysdykcji, w której ma domicyl podmiot dokonujący tego zachowania, a nielegalnym w jurysdykcji państwa trzeciego. Ewentualne przyjęcie prawa domicylu wyłącznie wskaże prawo - natomiast nie rozwiąże wspomnianej kolizji. W rzeczywistości wdrożenie tej koncepcji czyniłoby stosowanie zasad nieinterferencji i nieinterwencji jeszcze trudniejszym. Wystarczałoby bowiem wybranie jednej jurysdykcji, w której dane zachowanie jest legalne, a następnie stworzeniu podmiotu w tej jurysdykcji, by *de facto* i *de iure* wymagać uznania danego zachowania ze legalne w dowolnej innej jurysdykcji.

Inną propozycją doktryny jest stworzenie specjalnego podmiotu, rozstrzygającego spory podobne do *Yahoo! Inc. V .LICRA* w drodze arbitrażu.[252] Takie środki jednak niezmiernie rzadko byłyby skuteczne, zwłaszcza w przypadku konfliktów dotyczących kluczowych interesów państwowych. Ponieważ opisywana tu sprawa dotyczyła wyłącznie internetu, należy też zauważyć, że w odniesieniu do operacji o dużo wyższym stopniu tajności, odbywających się w pozostałych strefach cyberprzestrzeni arbitraż jest pozbawiony szans powodzenia. Pewnym prostym rozwiązaniem technicznym jest wprowadzenie śledzenie pakietów danych i w efekcie uniemożliwienie dostępu do pewnych serwerów użytkownikom z określonego państwa.[253]

---

[250] Historia tej koncepcji i jej główne założenia zostały opisane szczegółowo w doktrynie, zob. Okoniewski E. *Yahoo! Inc. v. LICRA*.. ss.333-7.

[251] Przyjęcie tej koncepcji co do części obrotu sugerowała też Dyretkywa Rady (UE) 2000/31, tzw. *Dyrektywa o niektórych aspektach społeczeństwa informacyjnego...* O.J. (L 178) par. 1-5.

[252] zob. Okoniewski *Yahoo*... s.339

[253] zob. Hare F. *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?*, Nato Cooperative Cyber Defence Center of Excellence(2018) ss.14-8

Druga istotna zasada określająca jurysdykcję państw wobec części fizycznej cyberprzestrzeni oraz postępowanie wobec naruszeń zasad nieinterferencji i nieinterwencji dotyczy danych przechowywanych w tzw. chmurach informatycznych.[254] Została ona ukonstytuowana w procesie wytoczonym przez korporację Microsoft po tym, gdy rząd USA zażądał od korporacji wydania danych obywateli amerykańskich, umieszczonych na należących do firmy serwerach położonych w Irlandii Północnej.[255] Sąd pierwszej instancji i sąd, który wydał pierwotny nakaz, uznały argumenty częściowo argumentację rządu wskazując, że sprawa terytorialności nie jest w sprawie istotna, a sam fakt, że Microsoft jest podmiotem prawa amerykańskiego wystarczy, by musiał on ujawnić dane. Podstawą był tu *Stored Communications Act*, regulujący zasady wglądu instytucji państwowych w dane cyfrowe prywatnych podmiotów.[256] Jednak Sąd Apelacyjny, do którego odwołał się Microsoft orzekł, że zgodnie z zasadą terytorialności, obowiązującej dla fizycznej części cyberprzestrzeni - skoro serwery znajdują się w Irlandii, podlegają jurysdykcji tego państwa a ich własność nie ma znaczenia.[257] Takie orzeczenie wynika ze wskazanej powyżej zasady, że państwa nie wykonują jurysdykcji co do danych - w związku z tym nie ma znaczenia, że "chmura" należy do podmiotu prawa amerykańskiego a dane na niej zawarte w przeważającej części zostały tam umieszczone przez obywateli tego państwa.[258] W uzasadnieniu sąd wskazał, że wykonanie takie orzeczenia oznaczałoby w istocie eksterytorialne stosowanie amerykańskiej ustawy karnej.[259] Po orzeczeniu wskazanym powyżej rząd USA, odwołał się do Sądu Najwyższego, podczas gdy Kongres Stanów Zjednoczonych

---

[254] Tzw. c*loud computing*, usługa polegająca na udostępnieniu poprzez sieć (najczęściej Internet) hardware komputerów w taki sposób, żeby były dostępne z dowolnego innego komputera podłączonego do tej samej sieci, z możliwością kopiowania, przechowywania uruchamiania i zmieniania tak przechowywanych danych.

[255] zob. *Microsoft Corp v. United States 829 F.3d 197 2d Circ.*(2016)

[256] zob. 18 US Code §§2701-12

[257] zob. Microsoft Corp.v. U.S. Government 829 F.3d 2nd (2016) par.222

[258] Ze względu na brak wykonywania jurysdykcji co do danych, nie jest możliwe jej wykonywanie także w stosunku do abstrakcyjnej „chmury", stanowiącej wyłącznie zapis cyfrowy. zob. Daskal J. *The Un-terrytoriality of Data*, 125 Yale Law Review(2015)ss.327,360

[259] *In re Warrant to Search a Certail E-Mail Account Controlled and Maintianed by Microsoft Corp.* 829 F. 3ed. 197, par. 222. cyt. za Justia, protokół sprawy U.S. v. Microsoft Corp. 584 US, (2018)

uchwalił tzw. *Cloud Act.*[260] Rozszerzał on obowiązek wykonania nakazu wydania danych zawarty w przywołanym już *Stored Communications Act*, na wszystkie dane znajdujące się w posiadaniu dowolnego podmiotu prawa amerykańskiego, niezależnie od faktycznego miejsca ich położenia.[261] Na mocy tego przepisu skierowano do Microsoftu kolejny nakaz, co do którego nie ma wątpliwości, że wiąże korporację.[262] Należy zauważyć, że przesłanki wykonywania jurysdykcji na podstawie *Cloud Act* nie spełniają przesłanek wykonywania jurysdykcji nadzwyczajnej[263], nie może też ich uznać za precedens wykonywania jurysdykcji w stosunku do danych.[264]

Opisane powyżej precedensy potwierdzają koncepcję, według której jurysdykcji zwyczajnej państw jest poddany ten zakres części informatycznej cyberprzestrzeni, który działa w oparciu o położone na terytorium tego państwa urządzenie części fizycznej.[265] W ten sposób nierówność w możliwościach projekcji siły w cyberprzestrzeni, spowodowanej różnicami w stopniu technologicznego rozwoju,

---

[260] *Claryfing Lawful Overseas Use of Data Act (CLOUD), [w:Consolidated Approprations Act Pub.L. 115-41 (2018)],* zmineniający §2701 U.S. Code.

[261] zob.*CLOUD Act §103(a)(1) [service provider] shall comply with obligiations of this chapter to preserve, backup or disclose [...[information [...] regardless of whether such [...] or other infromation is located within or outside of the United States-usługodawca (chodzi o udostępniającego swoje zasoby sieciowe klientom w ramach cloud computing) zobowiąany jest wykonywać obowiązki wynikające z rozdziału niniejszego (chodzi o rozdział dotyczący nakazów przeszukania, wydania danych, wydania rzeczy i współpracy z organami ścigania) niezależnie od tego, czy dane [...] przechowywane są na terytorium Stanów Zjednoczonych czy też poza nim.*

[262] Należy zauważyć, że sprawa przed sądem została umorzona po wydaniu przez Sąd Najwyższy Stanów Zjednoczonych w postanowieniu wydanym po skierowaniu do niego w sprawie przez sąd drugiej instancji *wirt of certiorari*, w którym postanowił uznać za sprawę za *remanded and vacated* (co jest odpowiednikiem polskiego orzeczenia kasatoryjnego przekazującego sprawę do niższej instancji wraz z wydaniem wiążących instrukcji) instruując sąd, który skierował pytanie prawne by umorzył postępowanie ze względu na jego bezprzedmiotowość. Uznał on bowiem, że sprawa dotyczy stanu prawnego sprzed wydania *Cloud Act,* wobec faktu wydania nowego nakazu na podstawie nowego stanu prawnego i braku jego kwestionowania przez Microsoft, rozstrzyganie poprzedniego sporu jest bezprzedmiotowe.

[263] Wynika to z samego zapisu normy. §2713 US Code, nakłada bowiem obowiązek na podmiot ISP umożliwienia rządowi USA wglądu w informacje znajdujące się w posiadaniu tego podmiotu. W oczywisty więc sposób norma ta nie wpływa na jurysdykcję państw trzecich. Podobne zdanie wyraża doktryna amerykańska. zob. Daskal J. *The Un-territoriality*... s.323

[264] Żaden z sądów w sprawie nie odniósł się do kwestii terytorialności danych. Co więcej, glosy do wyroku Sądu Najwyższego podnosiły kwestię braku jasnego podkreślenia przez niego braku poddania danych jurysdykcji.cf. Kerr O.S. *The next Generation Communications Privacy Act*, Univeristy of Pennsylvania Law Review 162:373 (2014) s.408

[265] Koncepcję tą zdaje się popierać część uznanej grupy teoretyków prawa cyberprzestrzeni związanej z Uniwersytetem Harvarda. zob. na przykład Goldsmith J.L., *Against Cyberanarchy, 65* University of Chicago Law Review 1199 (1998)

stanie się podstawą cybernetycznych konfliktów asymetrycznych.[266] Zostaną one omówione w części niniejszej rozprawy poświęconej prawu cyberprzestrzennych konfliktów zbrojnych. Ze względu na bardzo niski stopień regulacji cyberprzestrzeni, dodatkowo opartej o normy wiążące pośrednio,[267] możliwość projekcji siły będzie podstawowym czynnikiem decydującym o pozycji państwa w cyberprzestrzeni.[268] Łatwo więc zauważyć, że wpływ na część fizyczną cyberprzestrzeni stanowi kluczowy środek ochrony przez państwa własnej suwerenności w cyberprzestrzeni.

[266] zob. Zheng Y. *Technological Empowerment: The Internet, State and Society in China* Stanford University Press (2008) s. 103 i n.

[267] zob. na przykład. Art. 5 Konwencji Rady Europy o cyberprzestępczości(tzw. Cyberkonwencja Budapesztańska), otwarta do podpisu 23 listopada 2001. Powołany przepis zobowiązuje państwa,które Konwencję ratyfikowały do wprowadzenia do swoich wewnętrznych systemów prawnych narzędzi umożliwiających ściganie cyberprzestępczości i udzielanie innych państwom-sygnatariuszom pomocy w ściganiu tych przestępstw. Nie wyznacza jednak żadnych, nawet niewiążących, wytycznych.

[268] zob. *National Policy and Guiding Priniciples* [w:*The National Strategy to Secure Cyberspace,* USA Homeland Security, (2003), także Franzoese *Sovereignty in Cyberspace...* s. 35

II. Prawo cyberprzestrzeni.

Jak wskazano już powyżej, cyberprzestrzeń poza normami tradycyjnego prawa międzynarodowego, podlega normowaniu przez normy natywne. Można też łatwo dostrzec, że prawo cyberprzestrzeni jest bardzo słabo określone, odpowiednie stosowanie norm tradycyjnego prawa narodów stwarza poważne problemy interpretacyjne, a próby stosowania analogii z norm regulujacych pozostałe *global commons* są skuteczne tylko w pewnym, stosunkowo niewielkim zakresie. Pogląd o istnieniu odrębnego prawa cyberprzestrzeni był początkowo mocno atakowany przez część doktryny, wskazującej że odrębne prawo cyberprzestrzeni nie istnieje, a tym bardziej nie tworzy żadnego nowego systemu normatywnego.[269] Krytycy tezy o odrębnym prawie cyberprzestrzeni wskazywali, że cyberprzestrzeń stanowi zbiór *leges speciales*, istniejących jednak w ramach typowego prawa międzynarodowego. W przywołanym artykule Easterbrook wskazuje, ze tworzenie odrębnego prawa cyberprzestrzeni jest równie niepotrzebne jak kodyfikowanie tytułowego „prawa konia[270]", regulującego wyłącznie wszystkie aspekty życia dotyczące koni. Zwaca też uwagę, że cyberprzestrzeń w istocie jest tylko pewną nowinką techniczną, która może i powinna podlegać dotychczas istniejącym normom. Nie sposób się jednak zgodzić z jego argumentacją. Istnienie lub nieistnienie koni nie wpływa bowiem ani na sposób czy zakres normowania norm ogólnych ani programowych; nie wpływa też na inne gałęzie prawa materialnego. Ewentualne szczegółowe normy dotyczące wyłącznie koni, nie będą wpływać na prawo dotyczące nieruchomości, ruchu granicznego czy

[269] por. Easterbrook *Cyberspace and the Law of the Horse* (1996) University of Chicago Legal Forum 207/96(1996) ss.210-7

[270] W języku polskim tłumaczeniem precyzyjniej oddającym istotę tego, co Easterbrook opisuje byłoby określenie „Prawo o Koniu".

jurysdykcji. Tymczasem sam fakt istnienia cyberprzestrzeni zmienia interpretację nieomal każdej normy prawnej istniejącej na świecie, a jej normowanie automatycznie wpływa na regulacje dotyczące innych dziedzin życia, choćby w zamyśle twórców tych norm miały być one ograniczone do pewnej partykularnej dziedziny. W miarę upływu czasu od faktycznego powstania cyberprzestrzeni stało się oczywistością, że dotychczasowe jej regulacje prawne nie nadążają za postępem techniki w dużo większym stopniu niż miało to miejsce w przypadku wcześniejszych rewolucji technicznych.[271] Oznacza to, że skoro postęp ten trwa nieprzerwanie, a jego tempo rośnie zgodnie z przywołanym we wstępie prawem Moore'a, dystans pomiędzy prawem a technologią w miarę upływu czasu się zwiększa. To odróżnia rewolucję cyfrową od wcześniejszych przełomów technologicznych, w których prawo ostatecznie wypracowywało skuteczne mechanizmy regulacji, nawet jeżeli dochodziło do tego z pewnym opóźnieniem. Ta sytuacja spowodowała poszukiwanie rozmaitych sposobów na przyspieszenie tworzenia prawa cyberprzestrzeni. Oczywistym rozwiązaniem stało się stosowanie do cyberprzestrzeni analogii z innych unormowań szczególnych, zwłaszcza z prawa morza i przestrzeni kosmicznej. Ze względu jednak na specyfikę techniczną cyberprzestrzeni, rozwiązaniem problemów normatywnych stała się dopiero koncepcja *lex informatica*, oparta o stosowanie do regulowania cyberprzestrzeni w równym stopniu tradycyjnych źródeł prawa jak i rozwiązań technicznych pojmowanych jako normy prawa. Koncepcje te zostaną szczegółowo omówione w dalszej części rozważań.

Niezależnie od powyższych koncepcji, należy pamiętać że stosowanie nawet ogólnych norm prawa międzynarodowego, zgodnie z przedstawionym wyżej stanem faktycznym, może odbywać się wyłącznie w drodze wypracowania odpowiedniego systemu *leges speciales*, mających za podstawę te normy. Muszą one jednak uwzględniać specyficzne uwarunkowania cyberprzestrzeni. Przeciwne głosy doktryny,

[271] zob. Orzeczenie Sądu Najwyższego USA w sprawie *Reno et al. v. ACLU et al.* z 26 czerwca 1997par.(i), uznającego sieć połączonych komputerów za odrębne środowisko prawne. zob. Także *Building an Effective European CyberShield. Takin EU Cooperation to the Next Level*, Biuletyn Komisji Europejskiej/EPSC (European Political Strategy Centre) wyd. 24 (2017) par. 1, dotyczący rozróżnienia regulacji prawnych dotyczących zagrożeń zewnętrznych w świecie fizycznym i cyberprzestrzeni.

pojawiające się w części opracowań na temat prawa cyberprzestrzeni należy uznać za niesłuszne.[272] Prawo cyberprzestrzeni, choć bardzo różne od dotychczasowych regulacji szczegółowych, nie może funkcjonować w próżni prawnej i zupełnie abstrahować od ogólnych zasad prawa międzynarodowego tak publicznego jak i prywatnego. Z drugiej jednak strony, należy uznać za niemożliwe do przyjęcia głosy, które wskazują że koncentrowanie się na cyberprzestrzeni a szczególnie stwarzanie dla niej jakichś specyficznych norm jest nieuzasadnione. Nie jest bowiem prawdą twierdzenie, że konstytuowanie się prawa cyberprzestrzeni oznacza tworzenie konkurencyjnego w stosunku do *ius gentium* porządku, który miałby regulować w sposób odrębny zakresy przedmiotowe podlegające już regulacji na mocy norm ogólnych *rerum communarum* Za podobnie niezrozumiałe należy też uznać głosy wskazujące, że wystarczające jest stosowania analogicznie reżimu prawnego opartego o terytorialność i wybór prawa.[273] Jak wskazano powyżej zasada terytorialności obowiązuje w cyberprzestrzeni w sposób ograniczony wyłącznie do pewnych zakresów cyberprzestrzeni. Podobnie wybór prawa (nawet po rozwiązaniu problemów dotyczących mechanizmów dokonywania tego wyboru) nie daje rozwiązań w zakresach, które w ogóle nie podlegają zakresom normowania tradycyjnego prawa (co jest łatwo zauważalne na przykładzie opisanej już sprawy *Yahoo! V. LICRA*).

W związku ze wspomnianymi już różnicami, niewątpliwie innej interpretacji podlegać będą także naruszenia suwerenności państwowej dokonywane w cyberprzestrzeni. Przytaczane często przykłady naruszeń suwerenności sprzed powstania cyberprzestrzeni, takie jak istnienie radia Wolna Europa, naruszające granice bloku sowieckiego bez fizycznej obecności, możliwości dokonywania nieuczciwych transakcji międzynarodowych czy pomówienia dokonanego przez telefon przez osobę znajdującą się w jednej jurysdykcji rozmówcy przebywającego w

---

[272] zob. Sommer J.H. *Against Cyberlaw,* Berkely Technology Law Journal 3:15,(2000) s.1145 i n.

[273] zob. Goldsmith J.L. *The Internet and the Abiding Significance of Territorial Sovereignty* 5 Indiana Journal of Global Legal Studies (1998) s.475. Przede wszystkim pozostaje kwestią nierozstrzygniętą w praktyce międzynarodowej, jakie dokładnie są mechanizmy wyboru prawa w cyberprzestrzeni zob. Także Reindl A.P. *Choosing Law in Cyberspace: Copyright Conflicts on Global Networks* Michigan Journal of International Law 19:3 (1998) s. 809

innej jurysdykcji,[274]- pomimo zamysłu ich proponentów nie mogą być uznane za odpowiadające naruszeniom mającym miejsce w cyberprzestrzeni. Istnieje bowiem wiele różnic pomiędzy samą cyberprzestrzenią a światem fizycznym i nie może być wątpliwości, że te różnice mają istotne znaczenie prawne.W dalszej części rozdziału omówione zostaną źródła prawa cyberprzestrzeni, ze szczególnym uwzględnieniem specyfiki współczesnego *lex informatica* i koncepcji normowania faktycznego.

1. Odpowiednie stosowanie norm wcześniejszych

Dla każdej nowej dziedziny prawa międzynarodowego, naturalnym kierunkiem rozwoju jest stosowanie analogii.[275] Kiedy więc przeważyła koncepcja zakładająca uznanie cyberprzestrzeni za nowe *res communis omnium,*[276] kierunki poszukiwania analogii, zdawały się być wyznaczone. Sięgnięto bowiem do wzorców regulacji pozostałych *rerum communarum*, ze szczególnym uwzględnieniem najstarszego, najbardziej stabilnego i najbliższego faktycznie cyberprzestrzeni prawa morza.[277] Najnowszą i - jak się wydaje najbliższą - kompletności regulacją w zakresie prawa morza pozostaje Konwencja z Montego Bay. Zastosowanie analogii z tej konwencji, miało przede wszystkim uregulować kwestię prawa równego dostępu państw do cyberprzestrzeni, w identyczny sposób w jaki uznaje ona prawo wszystkich państw świata do określonych działań na wodach międzynarodowych i skutkować powstaniem pojęcia otwartej cyberprzestrzeni (analogicznym do morza otwartego).[278] Drugim elementem, którego doktryna poszukiwała w prawie morza były wskazówki

---

[274] Goldsmith J.L. *The internet...* ss.480 i n.

[275] Wskazuje się, że pierwsze normowania dotyczące cyberprzestrzeni czerpały głównie z reżimów prawnych dotyczących Arktyki, kosmosu i morza otwartego.zob. też Eichensehr K.E. *The Cyber-Law of Nations*, The Georgetown Law Journal 103 (2015) s.340

[276] Wynikające z praktyki międzynarodowej a także międzynarodowego *opinio juris.* Tak Heinegg v. W.H. *Legal Implications of Territorial Soverignty in Cyberspace,* [w:4th International Conference on Cyber Conflict, zbiorowa red. Ziolkowski K., Ottis R., Czosseck C. NATO CCD COE Publications, Tallin (2012) s. 9]

[277] zob. Stahl W.M. *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity,* Georgia Journal of International and Comparative Law 40 (2008) ss. 248 i n.

[278] Art. 87(1)*Konwencji z Montego Bay- Morze pełne jest otwarte dla wszystkich państw, zarówno nadbrzeżnych jak i śródlądowych[...].* zob. też tamże art. 89 - Żadne państwo nie może w sposób ważny zgłaszać roszczeń do poddania swej suwerenności jakiejkolwiek części morza pełnego.

dotyczące rozgraniczenia części informatycznej cyberprzestrzeni na terytorialną i *commons* (analogicznie do wód terytorialnych i morza otwartego). Ze względu na stopień skomplikowania technicznego cyberprzestrzeni, dużo większy niż ten wymagany do delimitacji i rozgraniczenia wód terytorialnych i morza otwartego, ów cel niewątpliwie nie został osiągnięty. Podobnie nieskuteczna okazała się próba zastosowania do cyberprzestrzeni wynikłej z Konwencji regulacji zakazującej wykorzystywania wód międzynarodowych do działań innych niż pokojowe.[279] Podobne regulacje cyberprzestrzeni przewidywały pierwsze koncepcje cyberprzestrzeni. Udostępniona do cywilnego użytku część cyberprzestrzeni (*ARPANET)*, miała być zasadniczo siecią do użytku ośrodków naukowych.[280] Coraz dalej idące interesy państw w cyberprzestrzeni doprowadziły jednak do militaryzacji cyberprzestrzeni, co z kolei wymagało uregulowania. Skutecznie natomiast została inkorporowana do powstającego prawa cyberprzestrzeni norma wyłączająca możliwość nabycia i ogłoszenia suwerenności nad jakąkolwiek częścią morza otwartego.[281] Całe normowanie prawa morza jest oparte o model eksterytorialności morza otwartego. Przyjęcie takiego modelu oznaczałoby w naturalnej konsekwencji przyjęcie wielobiegunowego modelu kontroli nad cyberprzestrzenią.[282] Z powodów czysto technicznych wielobiegunowość ta nie oznaczałaby jednak równego wpływu na cyberprzestrzeń. Oczywiste jest bowiem, że państwa mające dużą przewagę technologiczną nad pozostałymi automatycznie uzyskiwałby też przewagę w owym

---

[279] zob. art. 88*Konw. z Montego...- Morze pełne jest wykorzystywane wyłącznie do celów pokojowych*. Należy jednak zauważyć, że przepis ów należy traktować wyłącznie jako normę programową, jest on *lex imperfecta*.. Pozostaje kwestią otwartą, czy przeprowadzenie analogii z przedmiotowej normy do prawa cyberprzestrzeni miałoby stanowić jego reaktywację czy też, należałoby go przy konstruowaniu tej analogii pominąć. zob. też Eichensehr K. *The Cyber-Law of Nations* The Gerogetown Law Journal 103 (2015) s.317.

[280] zob. Swedin E.G. *Science in the Contemporary World:an Encylopaedia* ABC-CLIO(2005)s.147

[281] Art. 89 *Montego...*

[282] W taki sposób sprawowana jest kontrola międzynarodowa nad pełnym morzem (także innymi *res communis omnium*, przestrzenią kosmiczną, Antarktyką).Należy taki model odróżnić od modelu wynikającego z *lex informatica*, zdecydowanie bliższemu administrowaniu cyberprzestrzenią. W aktualnym stanie prawnym, wykonywanie jakiejś konstrukcji podobnej do *imperium* w stosunku do cyberprzestrzeni przez podmioty prawa międzynarodowego nie jest prawdopodobne. Ze względów na ilość podmiotów, które miałby wykonywać kontrolę nad cyberprzestrzenią, taki model ze względu na swoją nieefektywność nie jest możliwy. zob. też Baird Z. *Governing the Internet:Engaging Government, Business and Nonprofits* Foreign Affairs 11/12 (2002) s.15

modelu zarządzania, wykorzystując po prostu swój dużo większy wpływ faktyczny na funkcjonowanie cyberprzestrzeni.[283] W cyberprzestrzeni nie może być bowiem o mowy o równości podmiotów wobec prawa. Ponadto, konieczne byłoby określenie, które z części cyberprzestrzeni miałaby podlegać normowaniu za pomocą analogii z Konwencji z Montego Bay (czy szerzej z prawa morza). Niewątpliwie, nie podlegałaby mu część fizyczna, regulowana terytorialnie, co musi wykluczać wskazane tu sposoby normowania. Możliwe, przynajmniej w teorii, byłoby natomiast wypracowanie systemu opartego o taką analogię w stosunku do informatycznej części cyberprzestrzeni, gdzie zamiast „wód terytorialnych" istniałaby terytorialna cyberprzestrzeń Byłaby ona oparta o terytorialnie kontrolowaną infrastrukturę, a odpowiednikiem „pełnego morza" byłaby cyberprzestrzeń funkcjonująca poza terytorialną jurysdykcją, czyli ta, którą uznaje się za *res communis*. Taka konstrukcja jest jedną z najbardziej rozpowszechnionych i - jak się wydaje - słuszną koncepcją podziału jurysdykcji w części informatycznej cyberprzestrzeni wobec odrzucenia koncepcji jej bezwyjątkowej eksterytorialności. Jej przyjęcie wymaga jednak wypracowania sposobu określania granic jurysdykcji w informatycznej części cyberprzestrzeni, co jest niezmiernie trudne jak wykazano powyżej.

O ile pewne zasady z prawa morza mogą być stosowane do rozwiązywania istniejących problemów interpretacyjnych dotyczących cyberprzestrzeni, instytucje tego prawa *per se* nie mogą podlegać transpozycji do prawa cyberprzestrzeni. Z podobnymi problemami spotyka się część doktryny wskazująca zasadność przyjęcia do prawa cyberprzestrzeni analogii z prawa kosmicznego.[284] Nietrudno więc zauważyć, że głównym (i jedynym niekwestionowanym) elementem regulacji przejętych do prawa cyberprzestrzeni z praw morza i przestrzeni kosmicznej jest

---

[283] por. Wu T.S. *Cyberspace Sovereignty?-The Internet and the International System*, 10 Harvard Journal of Law and ARV. J.L. & TECH (1997)ss. 647-8. Autor wskazując na brak równomierności wpływu poszczególnych państwa na normowanie cyberprzestrzeni wskazuje-*Beacuse of the pattern of the Internet growth, most of the currently existing norms have been established by individuals from the United States and likeminded countries[...]- ze wzlędu na model wzrostu internetu, zdecydowana większość istniejących norm została stworzona przez podmioty w Stanach Zjednoczonych i innych, podobnie myślących państwach.*

[284] zob. Także Petereson M.J. *The Use of Analogies in Developing Outer Space Law,* International Organization, Cambridge University Press 51/2,(1997)s. 254 .

samo uznanie cyberprzestrzeni za *commons*. Pozostałe elementy wynikłe ze wspomnianych analogii stają się wskazówkami dla powstającego prawa cyberprzestrzeni, nie są jednak analogiami prawnymi w ścisłym sensie. Wynika to oczywiście z istotnych różnic faktycznych, przede wszystkim z ciągłej ewolucji cyberprzestrzeni. W odróżnieniu jednak od pozostałych *commons*, cyberprzestrzeń nie podlega wyłącznie władzy podmiotów prawa międzynarodowego, a jej prawo jest na bieżąco tworzone przez jej wszystkich użytkowników (także aktorów niepaństwowych) i ze swej natury (a w odróżnieniu od statycznych regulacji *commons*) jest dynamiczne.[285]

2. Stosowalność fundamentalnych zasad prawa międzynarodowego do cyberprzestrzeni

O ile istnieje wiele istotnych różnic w konstrukcji prawa cyberprzestrzeni i praw klasycznych *commons*, tak nie ma wątpliwości że programowe zasady prawa międzynarodowego, wynikłe z orzecznictwa i praktyki międzynarodowej stosują się do tej pierwszej w takim samym stopniu jak do innych dziedzin prawa. W odróżnieniu od opisanych powyżej analogii z *commons,* zasady te ze względu na swój abstrakcyjny charakter mogą zostać zastosowane do cyberprzestrzeni, a problematyczna może się okazać wyłącznie ich odpowiednia konkretyzacja. Wystarczającym warunkiem jest tutaj bowiem dokonanie odpowiedniej wykładni lub konkretyzacji w ramach normowania faktycznego, ponieważ zasady opisane poniżej wiążą podmioty prawa międzynarodowego. Chodzi tu przede wszystkim o ogólne zasady dotyczące prawa konfliktów i naruszeń suwerenności, mające szczególne umocowanie w prawie międzynarodowym ze względu na to, że ich źródła leżą w precedensach i w praktyce międzynarodowej. Poniżej omówione zostaną zasady

[285] Eichensehr określa model tradycyjnej kontroli nad *commons* modelem wielopodmiotowym *[multilateral]* ,podczas gdy model normowania cyberprzestrzeni określa jako wspólność udziałów(dosłownie współudział, który jednak w polskim języku prawnym ma inne znaczenie) *[multishareholder].*[w: *The Cyber- Law of Nations...* s.349] Określenie to dobrze obrazuje różnicę pomiędzy wielostronnym (w domyśle traktatowym) regulowaniem określonych materii a wykonywaniem bezpośredniego normowania faktycznego, mniej sformalizowanego i niepodlegającego określonym procedurom.

prawa międzynarodowego publicznego, które wydają się być najistotniejsze dla kwestii suwerenności i ich naruszeń w cyberprzestrzeni.

2. a. Testy przypisania przyjęte w sprawach Nikaragua v. USA i Prokurator v. Tadić.

Obydwa przedmiotowe testy dotyczą oceny przypisania państwu odpowiedzialności za działania jego organów na arenie międzynarodowej.[286] W teście przyjętym w sprawie *Nicaragua,* Międzynarodowy Trybunał Sprawiedliwości przyjął, że państwo odpowiada za działania grup paramilitarnych i o podobnym charakterze, nawet wtedy gdy nie są one w żaden sposób ujęte w oficjalnych strukturach tego państwa Warunkiem jest spełnienie dwóch rozłącznych przesłanek:[287](1) jeżeli grupy te działają dzięki wsparciu materialnemu i organizacyjnemu państwa, a także w ramach jego planów strategicznych lub (2) jeżeli pomimo zachowania pewnego stopnia niezależności organizacyjnej ich działalność jest możliwa wyłącznie przy wsparciu tego państwa.[288] Test ten, jakkolwiek spełnił swoje zadania w przedmiotowej sprawie, poddany został krytyce doktryny jako trudny do praktycznego zastosowania. Przede wszystkim problematyczna okazuje się kontrola stopnia podległości organizacyjnej grup paramilitarnych strukturom państwowym. Często niemożliwe okazuje się nie tylko udowodnienie, ale nawet ustalenie do jakiego stopnia członkowie owych grup wykonywali rozkazy czy instrukcje z zewnątrz.[289] Drugi problem testu (który uwidoczni się szczególnie w cyberprzestrzeni) wynika z faktu, że w istocie MTS przypisuje państwom odpowiedzialność nie tyle za skutek działań owych grup paramilitarnych, co odpowiedzialność za działania własnych organów, które swoimi

---

[286] Orzeczenie Izby Apelacyjnej w sprawie *Prosecutor v. Tadić* (IT-94-1-A), wydane dnia 15 lipca 1999.

[287] *Case Concerning Military and Paramilitary Acitivites in and Against Nicaragua*, ICJ Reports (1986)

[288] zob. ibid. par.106

[289] Wątpliwość tą *explicite* podniósł rząd hiszpański, który w swoim oświadczeniu skierowanym do Komisji Prawa Międzynarodowego - gdy test wynikły z orzeczenia *Nicaragua* stał się podstawą brzmienia art. 7 ARSIWA - wskazał, że test " w praktyce jest legalizacją łamania prawa, ponieważ nigdy nie będzie pewnej drogi by udowodnić, że agent działał na rozkaz" . zob. Crawford J. *The International Law Commissions Articles on States Responsibility - Introduction, Text and Commentaries,* Cambridge University Press (2002)s.106

zachowaniami umożliwiły tym pierwszym działanie, naruszające suwerenność państwa trzeciego.[290]

W odniesieniu do cyberprzestrzeni wydaje się oczywiste, że test wynikający ze sprawy *Nicaragua* jest w praktyce nie do zastosowania. Po pierwsze, daleko posunięta anonimowość w cyberprzestrzeni rzadko kiedy pozwala w ogóle określić tożsamość grup hakerskich (odpowiadających paramilitarnym oddziałom w wojnie konwencjonalnej). Po drugie, grupy takie zawsze działają w sposób niezależny organizacyjnie, a konieczny do przeprowadzenia cyberoperacji sprzęt jest dużo bardziej dostępny niż na przykład broń niezbędna do wyposażenia nieregularnego oddziału. Po trzecie, działania strategiczne państw w cyberprzestrzeni podlegają głębokiemu utajnieniu i nawet badania skutków tych operacji i zgodność z ogólną agendą polityczną danego państwa nie są wystarczające do wykazania, że dana grupa hakerska działała w ramach większej operacji.[291] Innym problemem, który utrudnia stosowanie kryterium "wsparcia logistycznego" w cyberprzestrzeni jest fakt, że państwo, które w jakikolwiek sposób wspiera określoną grupę nieregularną nie ma możliwości sprawowania na tym etapie ograniczenia możliwości działania tej grupy w drodze wyboru rodzaju tego wsparcia. Przykładowo, jeżeli wsparcie to będzie zakładało przekazanie wyłącznie broni defensywnej lub środków medycznych - nie będzie istniała możliwość użycia tej pomocy do dokonania jakiegokolwiek czynu międzynarodowego zabronionego. Tymczasem w cyberprzestrzeni, te same środki mogą zostać wykorzystane do przeprowadzenia operacji o dowolnej skali. Państwo przekazujące grupie nieregularnej algorytm umożliwiający przełamanie obrony cybernetycznej państwa trzeciego w celu dokonania przez tą grupę operacji szpiegowskiej nie może (w przeciwieństwie do środków fizycznych) mieć gwarancji, że grupa ta nie wykorzysta ich do ataku cybernetycznego o skutkach kinetycznych.

---

[290] zob. *Nicaragua* , orzeczenie par. 116

[291] Przykładowo, nigdy nie udało się udowodnić, że grupy rosyjskich "hakerów-patriotów", biorących udział w cyberataku na Estonię w roku 2007 były powiązane z rosyjskimi regularnymi służbami cybernetycznymi czy w jakikolwiek inny sposób pozostawały w strukturach państwa (a wyłącznie stwierdzić brak przeciwdziałania przez Federację Rosyjską), pomimo oczywistej motywacji działań politycznym kryzysem estońsko-rosyjskim. zob. Ottis R. *Analysis of the 2007 Cyber Attacks Against Estonia form the Information Warfare Perspectve,* Cooperative Cyber Defence Centre of Excellence, Tallin (2018) par. 3.3

Kwestią formalnoprawną, również utrudniającą stosowanie testu *Nicaragua* do cyberprzestrzeni, jest fakt, że test ów nie tyle służy przypisaniu odpowiedzialności za naruszenie suwerenności znajdujące się na końcu łańcucha zdarzeń, a jego celem jest raczej przypisanie organom danego państwa odpowiedzialności za nielegalne udzielenie pomocy grupom, które później wykorzystały ją do dokonania czynu zabronionego.[292] W przypadku ewentualnej atrybucji czynu dokonanego w cyberprzestrzeni oznaczałoby to w logicznej konsekwencji konieczność wykonywania w cyberprzestrzeni dwóch testów przypisania - pierwszego, który atrybuowałby samo naruszenie, oraz drugiego, pozwalającego na przypisanie państwu odpowiedzialności za wspieranie grupy, która naruszenie przeprowadziła.

Od opisanych powyżej komplikacji wolny jest natomiast proces przypisania według testu kontroli przyjętego przez Międzynarodowy Trybunał Karny do spraw byłej Jugosławii. Trybunał Karny rozdziela dwie odpowiedzialność państwa za swoich agentów na: (1)odpowiedzialność za działania poszczególnych osób, które działając na zlecenie danego państwa na określonym terytorium, przekroczyły swoje wyznaczone zadania i wskutek tego przekroczenia[293] dokonały czynu międzynarodowo zabronionego;[294]

(2) Odpowiedzialność za działania hierarchicznie zorganizowanych grup, gdzie przesłanką wystarczającą do przypisania państwu odpowiedzialności za jej działania jest sam fakt sprawowania przez państwo ogólnej kontroli nad grupą.[295] Łatwo więc zauważyć, że test ten w ogóle nie wymaga przypisania państwu udziału w określonym

---

[292] Trybunał w orzeczeniu wskazał- W*hat the Court has to investigate is not complaints relating to alleged violations of humanitarian international law by the contras,regarded by Nicaragua as imputable to the United States, but rather unlawful acts for which the United States may be responsible directly in connection with the activities of the contras. The lawfulness or otherwise of such acts of the United States is a question different from the violations of humanitarian law of which the contras may or may not have been guilty - Trybunał musi więc rozstrzygnąć nie tyle skargi dotyczace ewentualnych naruszeń prawa międzynarodowego, którego Nikaragua uważa za atrybuowalne Stanom Zjednoczonym co bezprawne działania, za które Stany Zjednoczone mogą odpowiadać bezpośrednio w związku z działaniami contras. Legalność lub nie tych działań jest kwestią odrębną od legalności lub nielegalności działań contras*. por. *Armed Activities Nicaragua*, orzeczenie par. 116

[293] Nawet gdyby już sam zakres tych zadań, przekraczał działania dozwolone prawem

[294] zob. Orzeczenie I instancji MTKbJ w sprawie *Prosecutor v. Tadić*, IT-94-1, (1995) par.118, 141

[295] ibid. Par. 131, 120

zachowaniu grupy paramilitarnej, żeby przypisać mu za nie odpowiedzialność. Przypisanie państwu odpowiedzialności za działania grup wojskowych i paramilitarnych jest więc znacząco łatwiejsze na podstawie testu wynikłego ze sprawy *Prosecutor v. Tadic* niż przy zastosowaniu zasad *Nicaragua*.[296] Dużo szerzej też pojmowany jest zakres podmiotowy możliwy do wykonania tego przypisania.[297] Jednocześnie z obydwu tych względów, test zastosowany w sprawie Tadicia jest dużo bardziej odpowiedni dla analizowania zachowań odbywających się w cyberprzestrzeni niż test *Nicaragua.*[298] Przede wszystkim istotny w tym zakresie jest drugi test, zakładający możliwość przypisania państwu odpowiedzialności za działania grup hakerskich nie powiązanych ściśle z danym państwem, ale działających na jego rzecz często pod auspicjami rządu; grupy takie istnieją w zdecydowanej większości państw świata.[299] Pozwala on bowiem na przypisania odpowiedzialności państwu o ile wykonuje ono kontrolę nad hierarchicznie zorganizowaną grupą. W praktyce więc jego przeprowadzenie możliwe jest w oparciu o dowody ze świata fizycznego (jak na przykład stwierdzenie istnienia określonej grupy lub jej powiązania z danym państwem). Czyny dokonane w informatycznej części cyberprzestrzeni mogą być (przynajmniej w pewnym zakresie) atrybuowane w świecie fizycznym, co znacząco ułatwia dokonanie tego procesu.Większa precyzja testu odpowiada też wymogowi stopniowania wagi materiału dowodowego w postępowaniach przed trybunałami międzynarodowymi.[300] Łatwo więc zauważyć, że rozważenie stosowania testu *Nicaragua* do cyberprzestrzeni i operacji w niej

---

[296] Dużo szersze przyjęcie testu MTKbJ wskazuje zarówno praktyka międzynarodowa jak i doktryna. Pojawiał się on regularnie w pracach Grup Roboczych ONZ, zob też .Cassese A.*The Nicaragua and Tadic Tests Revisited in the Light of the ICJ Judgement on Genocide in Bosnia*, European Journal of International Law 18 (2007) s.659

[297] Orzeczenie I instancji w sprawie, *Prosecutor v. Naletilić & Martinović* (IT-98-34-T),wydane 31 marca 2003 roku.

[298] zob. Shackleford *From Nuclear War* s.235, także Shackleford, Andres *State Responsibility* s. 997-8 i Roscini *Cyber...* ss.103, 109, 137

[299] zob. na przykład Hang R. *Freedom for Authoritariasnim: Patriotic Hackes nad Chinese Nationalism* The Yale Review of International Studies, 11/14 (2014) ss. 2-5 także Canfil J.K. *Honing Cyber Attribution: A framework for Assesing Foreign States Compliticity,* Journal of International Affairs 70:1 (2016) ss.220-3

[300] tak sędzina Higgins w swoim zdaniu odrębnym do orzeczenia MTS w sprawie *Case Concerning Oil Platforms (Islamic Republic of Iran v. USA)* z dnia 12 grudnia 1996 roku ICJ Reports 1996(1996) s. 217 i n.

przeprowadzanych w istocie musi prowadzić do wątpliwości tożsamych ze zgłaszanymi już uprzednio do testu przez rząd Hiszpanii.

2. b. Działania naruszające suwerenność wykonane w ramach global commons; Oil Platforms (Is. Rep. Iranu v. USA)

Orzeczenie w tej sprawie[301] jest niezmiernie istotne dla cyberprzestrzeni, ponieważ jest w zasadzie jedynym orzeczeniem trybunału międzynarodowego, które można uznać za wydane w sytuacji prawnej przypominającej tę panującą w informatycznej części cyberprzestrzeni. Podczas wojny iracko-irańskiej 1980-88, dwie jednostki; statek zarejestrowany w USA i okręt marynarki wojennej tego kraju zostały uszkodzone w wyniku odpowiednio uderzenia rakietowego i wejścia na minę na wodach międzynarodowych.[302] Stany Zjednoczone oskarżyły o obydwa ataki Iran, który zaprzeczył swojemu udziałowi w którymkolwiek z obydwu ataków. USA, deklarując działanie w samoobronie, przeprowadziło operację przeciwko irańskim instalacjom naftowym położonych w Zatoce Perskiej. W ramach tej samej operacji zatopiono kilka okrętów irańskich, między innymi dwie fregaty.Orzeczenie zapadłe w tej sprawie, uznawało operację USA za nielegalną, uznając, że nie spełniały one przesłanek uzasadniających samoobronę.[303]

Dla prawa konfliktu cyberprzestrzennego istotny jest jednak drugi z elementów orzeczenia w przedmiotowej sprawie. MTS oddalił bowiem twierdzenia Iranu podnoszącego, że atak na platformy konstytuował zagrożenie dla wolności międzynarodowego handlu i zasady morza otwartego.[304] Trybunał nie tylko nie

---

[301] *Case Concerning Oil Platforms... (Is. Rep of Iran v. USA)*

[302] zob. Bothe M. *Oil Platforms Case*, [MPEPIL]Oxford Public International Law, zbiorowa, red. Wolfrum R.,(2011) par. 3

[303] Przede wszystkim Trybunał uznał, że nie udowodniono udziału Iranu. Trybunał przyjął także, że wejścia na minę w na wodach, na których prowadzony jest wielostronny konflikt nie sposób uznać za bezpośredni atak na jednostkę jednego z belligerentów. cf. DeWeese G.S. *Anticipatory and Preemptive Self-Defnse in Cyberspace: The Challenges of Imminence* [w:*Architectures in Cyberspace*, 7th International Conference on Cyber Conflicts, zbiorowa, red. Maybaum M.,Osula A.M., Lindstroem L. (2015)s.86] Przesłanki dotyczące samoobrony w cyberprzestrzeni zostaną szczegółowo omówione w rozdziale poświęconym konfliktom cyberprzestrzennym.

[304] zob. *Oil Platforms...*, memorandum Rep. Iranu, par. 2

podzielił tego punktu widzenia, ale wręcz przyjął, że ewentualne naruszenia wolności handlu morskiego i wolności nawigacji powinny być rozpatrywane wyłącznie w oparciu o zapisy traktatów pomiędzy stronami. Powinny one też być – zdaniem Trybunału - ograniczone wyłącznie do faktycznie następujących ograniczeń w tym zakresie przedmiotowym.[305] Glosy do wspomnianego orzeczenia jednoznacznie podtrzymują, że orzeczenie to wyłącza z zakresu możliwych naruszeń także handel prowadzony pomiędzy stronami.[306] Oznacza to, że niemożliwe jest naruszenie wolności morza *in abstracto.*[307] Przyjęcie i zastosowanie tego rozumowania do cyberprzestrzeni oznacza legalizację działań mogących naruszyć bezpieczny przepływ danych, o ile nie przepływ ten nie został zagwarantowany w drodze traktatów.[308] Ponieważ nie można mówić o *in abstracto* wolnym przepływie danych w cyberprzestrzeni a liczba traktatów, regulujących swobodny przepływ pakietów danych w cyberprzestrzeni - w logicznej konsekwencji ochrona tej zasady zostanie znacząco ograniczona zakresowo.[309] Wobec opisywanego powyżej stosunkowo szerokiego katalogu możliwości wykonywania jurysdykcji ekstraterytorialnej przez państwa, wyłączenie normy nakazującej ochronę swobodę transferu danych *per se* znacząco poszerza możliwości ochrony własnej suwerenności. Sędzia Bruno Simma, w przywoływanym już zdaniu odrębnym do omawianego tu orzeczenia wskazuje, że ograniczenie do oceny zobowiązań traktowych oraz brak jednoznacznego wskazania, że nastąpiło złamanie przez USA normy zakazującej nieuzasadnionego użycia siły

---

[305] zob. *Oil Platforms...*, Awards par. 39

[306] zob.Bekker P.H.F., *The World Court Finds that US Attacks on Iranian Oil Platforms in 1987-1988 were not justifiable as Self-Defense, but the United States Did not violate the applicable treaty with Iran,* Americal Society of International Law 8:25,(2003) par.II

[307] Wydaje się, że ze względu na fakt oparcia konstrukcji "otwartej cyberprzestrzeni" na analogii z "morza otwartego", a zasady swobodnego przepływu danych w informatycznej części cyberprzestrzeni na analogii z wolności handlu na morzu otwartym- wydaje się zasadne stosowanie ninejszego orzeczenia także do cyberprzestrzeni.

[308] Należy wskazać dla komplementarności wywodu, że orzeczenie MTS w tym zakresie bywa krytykowana za zbyt wąskie określenie zakresu ochrony. zob. Zdanie odrębne sędziego Simmy [w: *Oil Platforms*... ss.324-7, 360], także Garwood-Gowers A. *Case Notes. Case Concerning Oil Platforms. Did the ICJ miss the boat on the law on the use of force?* Melbourne Journal of International Law 5(2004) ss.13-5

[309] Trybunał wyłączył możliwość dochodzenia przez Iran reparacji za uszkodzenia platform ze względu na brak ich wykorzystania w handlu pomiędzy z USA, wskazując na embargo nałożone na handel z Iran przez USA po upadku rządów szacha Pahlawiego.

wobec infrastruktury koniecznej do prowadzenia wolnego handlu w przywołanym orzeczeniu[310]- powoduje, że norma ta rozmywa się i w związku z wydaniem tego orzeczenia traci w zasadzie moc. Jednakże zakładając racjonalność działania sądu konieczne jest przyjęcie, że wybór takiej właśnie podstawy orzeczniczej[311] był celowym działaniem i zgodnie z nim dokonywać wykładni jego części kreujących abstrakcyjne normy prawne. Ponieważ cała część informatycznej części cyberprzestrzeni uznawana jest za *commons*, możliwe są więc dowolne działania, które: (1) nie stanowią złamania innych norm prawa międzynarodowego, (2) nie stanowią użycia siły zgodnie z koncepcją ekwiwalencji kinetycznej, do których właściwe jest stosowanie prawa regulującego prowadzenie konfliktów zbrojnych.[312] W oparciu więc o orzeczenie *Oil Platforms* i stosunkowo szerokie podstawy wykonywania jurysdykcji nadzwyczajnej, szczególnie doktrynę skutku i zasadę ochronną, państwa zyskują stosunkowo szerokie uprawnienia w stosunku do danych jako takich. Jest to widoczne szczególnie w związku z rozumieniem zasady prohibitywności *lex informatica* opisanej powyżej. Orzeczenie *Oil Platforms* wyłącza w ogóle normatywny poziom prohibitywności, pozostawiając wyłącznie faktyczny. Możliwe jest więc przykładowo wpływanie na prędkość przesyłu danych w krajach trzecich w celu przeprowadzenia legalnej operacji cybernetycznej, o ile nie łamie to zobowiązań wynikłych z traktatu lub norm wiążących *erga omnes*.

Drugim istotnym aspektem sprawy, mającym wpływ na prawo cyberprzestrzeni jest rozstrzygnięcie dotyczące zastosowania prawa do samoobrony. W *Oil Platforms*, Trybunał przyjął bowiem, że to na stronie powołującej się na prawo do samoobrony spoczywa ciężar wykazania, że samoobrona ta jest uzasadniona i proporcjonalna.[313]

---

[310] Wskazuje on wręcz, że orzeczenie nie tylko powinno chronić wolność handlu i nawigacji bez ograniczeń, ale nawet potencjalną możliwośc jego wykonywania- *the freedom to engage in commerce*. zob. zdanie odrębne sędziego Simmy, *Oil Platforms*... par.25

[311] Nie sposób bowiem przyjąć, jak uzasadniali sędziowie Buergenthal i Higgins[w:*Oil*... aw.par. 32], że powodem takiej podstawy orzeczenia były stosowanie przez MTS zasady *ne ultra petita*. O ile bowiem Iran w istocie zaskarżył w memorandum złamanie zobowiązań traktatowych, przede wszystkim dochodził on naprawienie szkód i przyznanie odszkodowania na jakiejkolwiek podstawie mieściłoby się w granicach żądania powoda.

[312] cf. zdanie odrębne sędziego B. Simmy [w: *Oil Platforms*... par. 7].

[313] zob. Też Bothe M. *Oil*... par. 2

Inkorporacja tej zasady do prawa cyberprzestrzeni jest z kolei znaczącym ograniczeniem możliwości obrony własnej suwerenności przez państwa.[314] Owa proporcjonalność jest niezmiernie trudna do wykazania, ze względu na liczne rodzaje cyberoperacji, których skutki mogą być określone dopiero po ich wystąpieniu, o czym będzie mowa w dalszej części wywodu. Możliwe są więc dwie interpretacje wskazanej zasady. Pierwsza, znacząco ograniczająca prawo do obrony i zakładająca, że państwo może wykonywać wyłącznie te środki, które będą proporcjonalne przy założeniu najmniejszego teoretycznie możliwego naruszenia w danym momencie. Druga, zakłada, że państwo ma prawo domniemywać, iż dana cyberoperacja wywrze możliwie najdalej idące skutki i w oparciu o takie domniemanie będzie wykonywać swoje prawo do proporcjonalnej samoobrony. Pewną wskazówką interpretacyjną zdaje się być przyjęcie przez doktrynę, że naruszenie wyłącznie cyberprzestrzenne może pociągać za sobą odpowiedź kinetyczną (nawet jeżeli nie ma owa cyberoperacja ekwiwalencji kinetycznej).[315] Jest to jednak wyłącznie pewna wskazówka, sugerująca rozszerzającą wykładnię samoobrony w cyberprzestrzeni - brak natomiast wystarczającej praktyki międzynarodowej i orzecznictwa by rozstrzygnąć tą kwestię w aktualnym stanie prawnym.

2. c. Orzeczenie wynikłe z sprawy m/s Rainbow Warrior (Nowa Zelandia. v. Francja)

Sprawa *Rainbow Warrior* jest dla niniejszej pracy istotna z dwóch powodów. Po pierwsze, jest to jeden najczęściej przywoływanych precedensów w zakresie odpowiedzialności państw za naruszenia suwerenności państw trzecich na arenie międzynarodowej. Po drugie, jest to jedyny przypadek, w którym pojedynczy, selektywny atak w czasie pokoju skierowany przeciwko państwu z politycznego punktu widzenia zaprzyjaźnionemu, został holistycznie przeanalizowany przez organy instytucji międzynarodowej. Tymczasem podobne sytuacje mają bardzo często

[314] zob. Zimmermann A. *International Law and 'Cyber Space',* European Society of International Law Reflections 3:1 (2014) s.6

[315] zob. DeWeese G.S. *Anticipatory and Preemptice Self-Defense in CyberspaceL The Challenge of Imminence* [w: zbiorowa, red. Maybaum M., Osula A-M, Lindstroem L. *Architectures in Cyberspace* NATO CCD Center of Excellence, Tallinn (2015) s .90]

miejsce w cyberprzestrzeni. Można więc domniemywać, że rozwiązania prawne zastosowane w tej sprawie mogą być stosowane do zdecydowanej większości cyberoperacji. Dodatkowym elementem upodabniającym atak do tych przeprowadzanych w cyberprzestrzeni było zaangażowanie tak państw jak i aktorów niepaństwowych.

S.S. Rainbow Warrior był trawlerem kupionym przez organizację *Greenpeace* w celu monitorowania zanieczyszczeń mórz. Ponieważ statek utrudniał Francji przeprowadzanie testów nuklearnych,[316] francuskie służby specjalne zaatakowały i zatopiły statek[317] zacumowany w czasie ataku w Auckland w Nowej Zelandii. W ataku poniósł śmierć jeden z członków załogi statku, Fernando Pereira - obywatel Hiszpanii, a sam Rainbow Warrior przewrócił się i osiadł na dnie basenu portowego. Po jego podniesieniu z dna okazało się, że został uszkodzony w stopniu uniemożliwiającym jakiekolwiek naprawy i po przeholowaniu na wody oceanu został ostatecznie zatopiony. Francja początkowo wyparła się jakiegokolwiek udziału w ataku, jednakże po aresztowaniu przez nowozelandzką policję dwóch oficerów DGSE[318], którzy zamach przeprowadzili i postawieniu im zarzutów terroryzmu - francuskie władze ogłosiły, że aresztowani działali na rozkaz rządu tego kraju. W wydanym oświadczeniu prasowym rząd francuski zobowiązał się także do poniesienia międzynarodowoprawnej odpowiedzialności. Wskutek tego oświadczenia sprawa została poddana pod arbitraż Sekretarza Generalnego ONZ. Nowa Zelandia zażądała uznania operacji za nielegalną i w związku z tym przeproszenia. Dodatkowo, rząd nowozelandzki domagał się od Francji wypłacenia rekompensaty dla armatora statku i rodziny Fernando Pereiry,[319] zabezpieczenia przed groźbami embarga wystosowanymi przez rząd francuski[320], oraz skazania sprawców ataku w razie ich

---

[316] Będących przedmiotem sporu przed Międzynarodowym Trybunałem Sprawiedliwości w sprawie *Nuclear Tests Case (Australia & New Zealand v. France)* ICJ 253,457 (1974)

[317] Portem macierzystym s.s. Rainbow Warrior był Amsterdam.

[318] *Direction Generale de la Securite Exterieure*- francuska agencja wywiadu cywilnego.

[319] Greenpeace, Hiszpania i Holandia nie przystąpiły do arbitrażu. Sprawa z rodziną F Pereiry została zakończona nieujawnioną ugodą, Greenpeace otrzymał zadośćuczynienie w dobrowolnego działania rządu francuskiego [w:Hoss Cr., M Morgan-Forster J.*The Rainbow Warrior,* MPEPIL (2010) par.par. 1-2 zbiorowa, red. Wolfram R.]

[320] Na etapie poprzedzającym przyznanie się rządu francuskiego do organizacji ataku,

wydania.[321] Francja zgodziła się na zapłacenie reparacji wszystkim poszkodowanym i uznanie bezprawności przeprowadzonego ataku, wskazała jednak, że nie może gwarantować skazania, zaprzeczając również, jakoby groziła jakimkolwiek embargo.[322] Ugoda zakończyła się ustaleniem, według którego zarówno bezpośredni wykonawcy ataku zostaną natychmiastowo wydani Francji, jednakże zostaną skazani na trzyletni pobyt na wyspie Hao, będącej terytorium zamorskim Francji.[323] Obowiązek ten został jednak wykonany wyłącznie nominalnie. Agentów pod rozmaitymi pretekstami sprowadzono do Europy. Sytuacja ta spowodowała protesty rząd nowozelandzkiego i w efekcie kolejny arbitraż, tym razem dotyczący wykonania ustaleń wynikłych z pierwszego.[324] Podstawowym, mającym wpływ na prawo cyberprzestrzeni aspektem sprawy jest wskazanie problemu ze stosowalnością prawa, któremu podlegają bezpośredni sprawcy czynu. Odpowiedzialność Francji jest niekwestionowana. Jednak wynika ona z ogólnych przepisów o odpowiedzialności państwa za przypisane mu działania jego służb. Nie ma natomiast jasności co do tego, jak traktować bezpośrednich wykonawców ataku. Sam fakt, że działali oni na rozkaz nie jest okolicznością eksoneracyjną ani ekskulpującą.[325] Nie da się też wskazać w prawie międzynarodowym publicznym normy stanowiącej podstawę do ukarania ich bezpośrednio. Jedyne konsekwencje karne jakie można wskazać (pomijając już kwestię ich faktycznego wykonania) ponieśli oni na mocy ustaleń pomiędzy dwoma państwami; jednym z nich była Nowa Zelandia, a więc państwo, które poniosło

---

Francja groziła przeforsowaniem nałożenia przez EWG embarga na produkty nowozelandzkie. zob. Shabecoff Ph. *France must pay Greenpeace $8 Million in Sinking of Ship* notka prasowa w New York Times z 3 października 1987 roku (dostęp w archiwum cyfrowym gazety na październik 2019)

[321] zob.Memorandum rządu Nowej Zelandii do Sekretarza Generalnego Organizacji Narodów Zjednoczonych ILM 1350 [w:United Nations Secretary General: *Ruling on the Rainbow Warrior Affair Between France and New Zealand* 26 ILM 1346(6 czerwca 1986) s.3-7]

[322] zob. Memorandum rządu Francji do Sekretarza Generalnego Organizacji Narodów Zjednoczonych ILM 1350[w: United Nations Secretary General: *Ruling on the Rainbow Warrior... ss.5-7*]

[323] zob.*Ruling on the Rainbow Warrior...s.7*

[324] zob. *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair.* United Nations Reports of International Arbitral Awards t. XX (1990) s. 215-84

[325] ibid. Trybunał powołał się przede wszystkim na ustalenia Międzynarodowego Trybunału Wojskowego w Norymberdze.

wyłącznie niematerialną stratę w postaci naruszenia terytorium.[326] Nie wszczęto nawet procedury ekstradycyjnej, a Francja zobowiązała się do nałożenia na obydwu oficerów DGSE sankcji bez przeprowadzenia procesu, w ramach arbitrażu i niejako w uznaniu procesu już przeprowadzonego, choć w nim stawiano im inne zarzuty.

Sytuacja z atakiem na wspomniany statek jest bardzo .bliska sposobowi przeprowadzania wszelkich operacji cyberprzestrzennych. Normalną praktyką jest bowiem zajęcie serwerów położonych w krajach trzecich, przez które przeprowadzany jest właściwy atak; odpowiada to wykonywaniu operacji w świecie fizycznym na terytorium państwa trzeciego, w ogóle w dany konflikt nie zaangażowanego. Ponieważ operacja taka wymaga ingerencji w serwery (a więc naruszenia jurysdykcji terytorialnej poprzez wykorzystanie infrastruktury znajdującej się terytorium obcym, najczęściej kilku państw), sytuacja tych państw staje się analogiczna do sytuacji, w której znalazła się Nowa Zelandia w opisywanej sprawie. Wskutek takiego zachowania wobec jednej cyberoperacji, jurysdykcję nadzwyczajną może wykonywać kilka lub nawet kilkanaście państw. Z arbitrażu w opisywanej sprawie wynika, iż za zasadną uznano argumentację Nowej Zelandii, podnoszącą, że poniosła ona szkodę w postaci uszczerbku na reputacji jako państwa, a ochronę przed takimi uszczerbkami uznano za istotny interes państwa. Przeniesienie tej zasady na grunt cyberprzestrzeni oznacza, że każde nieuprawniona ingerencja w jej fizyczną część, położóną na terytorium jakiegokolwiek państwa narusza jego istotny interes w analogiczny sposób.[327] Skoro więc możliwe jest uznanie naruszenia jurysdykcji za czyn nie tylko *per se* zabroniony, ale także uruchamiający prawo do samoobrony państwa, którego jurysdykcja została naruszona, (nawet wtedy, gdy dana operacja nie jest skierowana przeciwko jego suwerenności) łatwo wyciągnąć wniosek, że ściśle interpretowany zakaz nieinterwencji i nieintereferencji musi być także stosowany do

[326] Nowa Zelandia podnosiła w swoim memoriale, że przeprowadzenie podobnej operacji na jej terytorium, spowodowało uszczerbek na jej honorze, wiarygodności jako państwa praworządnego i pozycji międzynarodowej.

[327] zob. też Schmitt M.N. *In Defense of Due Dilligence in Cyberspace* The Yale Law Journal Forum 125:68 (2015) ss. 77-8, gdzie wskazano przesłanki za wykonywaniem prawa do samoobrony w cyberprzestrzeni, zawsze gdy naruszone są istotne interesy państwa.

cyberprzestrzeni.[328] Nie ma tu znaczenia fakt, że najczęściej samoobrona ta najczęściej nie jest wykonywana przez państwa, których infrastruktura jest wyłącznie pośrednio wykorzystywana.[329] Przyjmuje się bowiem, że w takiej sytuacji właściwym prawem jest prawo karne, obowiązujące na terenie, na którym czynu dokonano. O ile w przypadku działań na terenie tego państwa, istnieje realna szansa na wykonanie tego prawa, w przypadku cyberprzestrzeni możliwość taka jest wyłącznie teoretyczna. Po pierwsze, ataki cybernetyczne dokonywane są najczęściej spoza terytorium państwa zaatakowanego i jak wskazano powyżej, prawidłowa atrybucja jest niezmiernie trudna. Szanse na ujęcie sprawców a co najistotniejsze w przypadku normalnej sprawy karnej, zgromadzenie materiału dowodowego są więc marginalne. Podobne przyczyny utrudniałyby żądanie ekstradycji. Państwo, od którego żądano by wydania sprawców mogłoby jej odmówić a następnie, zgodnie z zasadą *aut dedere aut iudicare* wykorzystać luki dowodowe do dokonania pozornego procesu, w celu faktycznej ochrony osób odpowiedzialnych za atak na państwo będące jego rywalem i w istocie działających na rzecz jego interesów.[330] Dodatkowo, jeżeli wybór celu został dokonany zgodnie z opisanymi zasadami *cyberlawfare*, a więc wybrano cel o wysokim stopniu tajności, państwo zaatakowane zdecydowanie ukryje atak. Ewentualne osądzenie sprawców będzie bowiem dużo mniej istotne od zachowania integralności jego systemów bezpieczeństwa. Istnieje więc możliwość

---

[328] Racjonalne wydaje się przyjęcie, że aktor niepaństwowy nie działa w ramach struktur państwa, o ile nie spełnia testu wynikającego z *Prosecutor v. Tadic*, jako bardziej restrykcyjnego niż ten ze sprawy *Nicaragua.*

[329] Fakt, że państwa nie zawsze są w stanie (z powodów faktycznych) przeciwdziałać mniej istotnym z punktu widzenia ich interesów naruszeniom cyberprzestrzennym, ze względu na jego genezę w aktualnych technicznych możliwościach nie powinien być uznawany za praktykę międzynarodową w tym zakesie. zob. Też Ekstedt V., Parkouse T., Clemente D. *Commitments, Mechanisms & Governance* [w:zbiorowa, red. Klimburg A. *National Cyber Security. Framework Manual* NATO Cooperative Cyber Defence Centre of Excellence, Tallinn(2018)s.157]

[330] Ten mechanizm wykorzystywała Federacja Rosyjska po ujawnieniu cyberataków dokonanych przeciwko Estonii w 2007 i 2008 roku, co do których zostało ujawnione że przeprowadzono je z terytorium rosyjskiego. Rząd tego kraju ogłosił, że zostały one dokonane przez grupę haktywistów bez powiązań z rządem federalnym,rosyjskimi służbami specjalnymi czy armią a co za tym idzie Federacja nie może za nie odpowiadać w żadnym sensie na forum międzynarodowym. Pomimo to FR działała aktywnie przeciw próbom wykrycia sprawców, przykładowo poprzez nałożenie na Estonię sankcji i odmowę pomocy prawnej.zob.Kozłowski A. *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan.* European Scientific Journal 2/2014 t.3 (2014)ss.236-40, także Goodman W. *Cyber Deterrence: Tougher in Theory than in Practice?* Strategic Studies Quaterly 4:3 (2010)s.110

praktycznego uniemożliwienia ścigania sprawców określonego ataku. Jak przyjmuje większość doktryny w glosach do sprawy *Rainbow Warrior*, brak odpowiedniej do skazania normy prawa karnego tworzy z punktu widzenia prawa międzynarodowego lukę prawną Z drugiej jednak strony, precedens ustanowiony w tej sprawie tworzy potencjalną możliwość ścigania naruszeń polegających na samym naruszeniu zaufania do państwa, co stanowi często jeden z podstawowych celów cyberoperacji.[331]

Wydaje się więc, że uznanie przeciwdziałania naruszeniom wiarygodności państwa za istotny interes państwa, a w konsekwencji przyjęcie, że jest ono samodzielną podstawą wykonywania samoobrony uznaną przez społeczność międzynarodową może rozszerzyć katalog zachowań zakazanych i w konsekwencji ułatwić państwom obronę ich suwerenności. Z drugiej strony faktyczna (ale nie prawna) praktyka państw w tym zakresie pozwala uniknąć trudnego do rozstrzygnięcia konfliktu jurysdykcji nadzwyczajnych, który mógłby wyniknąć z wykonania jej przez wszystkie uprawnione państwa w tym samym czasie.

2. d. Sprawa S.S. Lotus (Francja. v. Turcja) i opinia MTS w sprawie Nuclear Threats

Orzeczenie rozstrzygające spór w sprawie *S/S Lotus* jest dla prawa cyberprzestrzeni istotne z dwóch niezależnych od siebie powodów. Po pierwsze, z orzeczenia tego wynika zasada utrzymania prohibitywności prawa międzynarodowego, pomimo naszkicowanych wcześniej uzasadnionych wątpliwości co do utrzymania jej w systemie prawa międzynarodowego publicznego.[332] Po drugie, orzeczenie to jest istotnym rozstrzygnięciem dla kwestii rozgraniczenia *commons* i jurysdykcji państwowej. Prohibitywność prawa międzynarodowego oznacza, że zakazy zachowania wiążące podmioty prawa międzynarodowego nie mogą być dorozumiane.[333] Trzecią istotną kwestią wynikłą ze sprawy *Lotus* jest zagadnienie

---

[331] zob. Stauffacher D., Kavanagh C. *Confidence building measures and international cyber security,* Cyber Policy Process Brief, ICT for Peace Foundation (2013)s.25

[332] cf. Stone J. *Non Liquet and the Function on Law in International Community*, 35 *British Yearbook of International Law. s*. 136 (1959)

[333] zob.*S/S Lotus...,*PCIJ Ser. A, nr 10 s. 18

dopuszczalności *non liquet*[334] w prawie międzynarodowym. Dopuszczenie stosowania tej zasady w prawie cyberprzestrzeni w praktyce wyłączałaby jurysdykcję sądów i trybunałów międzynarodowych. Brak procesowego i - co istotniejsze - materialnego prawa cyberprzestrzeni w tradycyjnym jego pojmowaniu (nie wydaje się bowiem możliwe by istniejące współcześnie sądy i trybunały międzynarodowe orzekały w oparciu o *lex informatica*), musiałby w logicznej konsekwencji wyłączać jurysdykcję tychże w sprawach mających swoje źródło w cyberprzestrzeni. Wydaje się jednak że zasada *non liquet* nie ma zastosowania we współczesnym stanie prawa międzynarodowego publicznego.[335] Należy jednak zauważyć, że poza przypadkami naruszeń norm wiążących *erga omnes*, niemożliwe jest wskazanie przypadku skutecznej obrony swoich praw przez podmiot prawa międzynarodowego na drodze sądowej, o ile naruszenie tych praw nastąpiło wyłącznie w cyberprzestrzeni. Co więcej, można wskazać liczne przykłady, kiedy nie sposób tłumaczyć zaniechania takiej obrony przez państwa inaczej niż właśnie specyfiką cyberprzestrzeni.[336]

Należy zauważyć, że chociaż brak prawa nie stałby na przeszkodzie temu, by skargę taką dane państwo złożyło (ponieważ sąd nie może się wyłączyć z braku prawa),[337]

---

[334] Chodzi tu o dopuszczalność uznania się przez sąd lub trybunał międzynarodowy za niewłaściwy do orzeczenia ze względu na brak odpowiedniej normy prawnej(*sibi non liquere*). W rozprawie niniejszej przyjęto pogląd większościowy doktryny (choć nie niekwestionowany), że orzeczenie *non liquet* jest niedopuszczalne w prawie międzynarodowym. cf. Rabello A.M. *Non Liquet From Modern Law to Roman Law*, Annual Survey of International and Comparative Law10:1 (2004)s.16; Wydaje się, że wyłączenie *non liquet* jest naturalną konsekwencją przyjęcia zasady prohibtywności prawa międzynarodowego publicznego, która w praktyce międzynarodowej nie jest kwestionowana, choć cf. Deklaracja sędziego Bruno Simmy [w:*Case Concerning Accordance with international law of the unilateral declaration of independence in respect of Kosovo*, Advisory Opinion z 22 czerwca 2010, ICJ Rep. 2010, Declaration of Judge Simma par. 2] wskazująca, że prohibtywne prawo międzynarodowe, jest poglądem przedawnionym [*old, tired view of international law*].

[335] Część doktryny analizuje także możliwość uzasadniania wyłączenia zasady *non liquet* prawnonaturalną interpretacją prawa międzynarodowego cf. Handeyside H. *The Lotus Principle in ICJ Jurisdprudence: Was the ship ever afloat?*, 29 Michigan Journal of International Law 71 . (2007) s.78 i n W dalszej części rozważań przyjęto iż sąd lub trybunał międzynarodowy nie może wyłączyć się z braku prawa, chyba że co innego wyraźnie wskazano inaczej w ogólnych normach prawa pozytywnego.

[336] Jak choćby braku reakcji Iranu na tzw. *atak Stuxnet,* Stanów Zjednoczonych Ameryki Północnej na działania północnokoreańskiej jednostki cyberprzestrzennej, dokonującej włamań przeciwko firmom amerykańskim na amerykańskim terytorium czy braku odpowiedzi NATO i Estonii na cyberataki przeprowadzone na to ostanie państwo w 2008 roku.

[337] Taką zresztą interpretację przyjmuje konsekwentnie Międzynarodowy Trybunał Sprawiedliwości. zob. *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion,* ICJ Reps. 1996 226 par.105(2)(E), gdzie Trybunał przyjął, że o ile brak prawa

nie zostanie ona uwzględniona z braku normy zakazującej określonego zachowania w systemie prawa dostępnego sądowi (przy utrzymaniu wcześniejszego założenia, że ewentualne zachowanie cyberprzestrzenne nie łamało by jednej z norm tradycyjnego prawa międzynarodowego - przykładowo poprzez ekwiwalencję kinetyczną lub złamanie normy wiążacej *erga omnes*).

Sytuacja ta koresponduje z faktem, że stosowanie zasady prohibitywności niezmiernie zwiększa swobodę legalnego działania w cyberprzestrzeni (ponieważ brak jasnych norm wyraźnie zakazujących licznych grup zachowań). Potwierdza to zresztą obserwacja praktyki i sądownictwa międzynarodowego w tym zakresie. Przyczyną tego stanu rzeczy są trzy czynniki. Po pierwsze, brak jasnych i kompleksowych norm pozytywnego prawa cyberprzestrzeni.[338] Po drugie, nawet w zakresie istniejących norm - brak wyraźnej praktyki i jasnych wytycznych interpretacyjnych.[339] Trzecim problemem jest brak wyspecjalizowanego sądownictwa międzynarodowego dotyczącego cyberprzestrzeni lub choćby jasnego rozwiązania kwestii kognicji istniejących już sądów i trybunałów międzynarodowych wobec spraw powiązanych z cyberprzestrzenią.[340] Wobec tego, konsekwentne i ścisłe stosowanie prohibitywności do cyberprzestrzeni i działań w niej prowadzonych, musi prowadzić do braku uznania licznych zachowań cyberprzestrzennych za *de iure* nielegalne, choć niewątpliwie zachowania te naruszają dobra prawne chronione przez prawo międzynarodowe.[341] Zachowania te jednak niewątpliwie nie są akceptowane *de facto.* Obydwie te kwestie powodują powstanie znaczących rozbieżności pomiędzy brzmieniem prawa międzynarodowego publicznego w zakresie normującym cyberprzestrzeń, a praktyką w tym samym zakresie. Jak wskazano powyżej, wiele

---

nie zwalnia go od wydania orzeczenia,nie zmienia to prohibtywności prawa międzynarodowego. Część doktryny wskazuje wręcz, że pomimo zabiegów ze strony Narodów Zjednoczonych, by przy wydawaniu tej właśnie opinii Trybunał uchylił precedns STSM w sprawie Lotus i wyłączył prohibitywność, zasada ta została utrzymana. cf. Glennon M.J. *The Road Ahead:Gaps, Leaks and Drips,* 89 International Law Studies US Navy War College, (2013) s.372

[338] zob.Schmitt M.N., Vihul L. *The nature of International Law CyberNorms*, Tallinn Paper 5 (2014) ss.2-3

[339] ibid. S.6-7

[340] zob. Freeman E.H. *Cyber Courts and the Future of Justice*, Legally Speaking, Information Systems Security 14:1 (2005) s.5

[341] zob.Buchan R. *Cyber Espionage and International Law*, Bloomsbury Publishing PLC, Oxford (2019) ss. 15-20, 235-42

działań państw prowadzonych w cyberprzestrzeni pozostaje w swoistej luce prawnej, niejako sankcjonowanej zasadą prohibitywności. Z tego samego względu brak podstaw do wydawania przez sądy i trybunały międzynarodowe orzeczeń specyficznych dla cyberprzestrzeni.

Należy jednak dla komplementarności wywodu wskazać, że Międzynarodowy Trybunał Sprawiedliwości w sprawie *Nuclear Threats*[342] powołał się na *non liquet.*[343] Według MTS nie jest możliwe jednoznaczne przesądzenie kwestii prawa państwa do wykonywania uderzenia atomowego w razie zaistnienia zagrożenia dla bytu państwa jako takiego.[344] Wydanie tej opinii nie wpłynęło znacząco na pogląd doktryny wskazujący, że zasada *non liquet* nie może być stosowana przez sądy i trybunały międzynarodowe.[345] Należy jednak zauważyć, że sam fakt wydania tak sformułowanej opinii jasno potwierdza, że Trybunał uznaje niektóre kwestie za niepodlegające rozstrzygnięciu na gruncie aktualnego stanu prawa międzynarodowego. Niewątpliwie za jedną z takich kwestii można uznać prawo cyberprzestrzeni. Nie przesądzając o kwestii samego *non liquet*[346]*,* nietrudno zauważyć, że konsekwencją możliwości wydania podobnego orzeczenia w ewentualnej sprawie cyberprzestrzennej musi być przesunięcie ciężaru sposobu obrony własnej suwerenności z domeny prawa tradycyjnego do domeny *lex informatica* i normowania faktycznego.

---

[342] zob. *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion, ICJ Reports (1996) s.226

[343] Sam fakt wydania takiego orzeczenia był mocno krytykowany. zob. McCormack T.L.H., *A non liquet on nucelar weapons- The ICJ avoids the application of general principles of international humanitarian law.* International Review of the Red Cross 316 (1997) par.2-3. zob także zdanie odrębne sędzi Higgins w sprawie *Legality of the Threat...* par.32

[344] zob. Opinia w sprawie *Nuclear Threats...* par. 105(2)F

[345] zob. Enabulele A.O. *The avoidance of non liquet by the International Court of Justice, the completness of the sources of international law in Article 38(1) of the Statue of the Court and the role of judicial decisions in Article 38(1)(d)* Commonwealth Law Bulletin 38:4 (2012) ss.620-5

[346] por.Stone J.*Non Liquet and the Fucntion of Law in The International Community* 35 British Yearbook of International Law 124 (1959) par. I

2. e. Klauzula Martensa

Tak zwana klauzula Martensa została sformułowana w Preambule do Konwencji Haskiej z 1899 roku[347] przez umawiające się strony na propozycję delegata Imperium Rosyjskiego, Fiodora Martensa. Jej aktualne brzmienie zostało ustalone przez art. 1 § 2 I Protokołu Dodatkowego[348] i §4 Preambuły do II Protokołu Dodatkowego.[349]Jest to klauzula generalna prawa międzynarodowego, wskazująca, że wszystkie sprawy niepoddane Protokołom, w których Klauzula została zawarta ani innym traktatom międzynarodowym - podlegają zasadom wynikającym z prawa zwyczajowego, zasadom humanitaryzmu i dyktatowi sumienia publicznego. Pomijając *superfluum* dotyczące prawa zwyczajowego (nie wymagającego dla swego obowiązywania dalszej normy), powszechne uznawanie Klauzuli niewątpliwie tworzy istotną wskazówkę dotyczącą postępowania w przypadku konfliktów zbrojnych. Niejasna jest jednak jej ranga. Obowiązywanie Klauzuli potwierdził Międzynarodowy Trybunał Sprawiedliwości w opinii *Nuclear Threat*[350], nie wskazano jednak jednoznacznej metody jej interpretacji. Stanowiska państw dotyczące praktyki stosowania Klauzuli wnoszone podczas do Zgromadzenia Ogólnego ONZ[351], były niejednoznaczne i niemożliwe stało się określenie jednoznacznej praktyki międzynarodowej.[352] Komentarz Międzynarodowego Komitetu Czerwonego Krzyża

---

[347]zob.Preambuła do Międzynarodowej Konwencji dotyczącej praw i zwyczajów wojny lądowej (Haga IV)Dz.U 1927 nr 21 poz. 16.

[348] *Pierwszy Protokół Dodatkowy do Konwencji Genewskich z 12 sierpnia 1949 dotyczący ofiar konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 roku Dz.U. 1992 nr 41 poz. 175 -Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)* (1977)

[349] *Pierwszy Protokół Dodatkowy do Konwencji Genewskich z 12 sierpnia 1949 dotyczący ofiar konfliktów zbrojnych (Protokół I) oraz dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych (Protokół II), sporządzone w Genewie dnia 8 czerwca 1977 roku Dz.U. 1992 nr 41 poz. 175 -Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-international Armed Conflicts (Protocol II), 8 czerwca 1977*

[350] zob. *Legality of the threat ...* par. 87

[351] zob. Rezolucja Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych 49/75 K z dnia 6 stycznia 1995 roku w sprawie skierowania do Międzynarodowego Trybunału Sprawiedliwości pytania prawnego o legalność użycia lub zagrożenia użyciem broni atomowej.

[352] Ta ostatnia waha się od uznania Klauzuli wyłącznie a normę traktatową (wiążącą

do Protokołu I, w którym Komitet wskazuje, że podstawową (i, jak się wydaje, jedyną niekwestionowaną) rolą Klauzuli we współczesnym stanie prawnym jest jej rola jako *lex specialis* normującego wyłączenie zasady prohibitywności prawa konfliktów zbrojnych. ICRC pisze *prevents [Martens Clause] assumption that anything which is not explicitly prohibited by the relevant treaties is therefore permitted- [Klauzula Martensa] wyłącza więc pogląd jakoby wszystko, czego nie zabraniają odpowiednie konwencje, było dopuszczalne.*[353] Jej współczesne pojmowanie jest więc zgodne z przedstawioną wyżej opinią sędziego Simmy, mówiącej o zmierzchu prohibitywności prawa międzynarodowego publicznego (oczywiście wyłącznie w zakresie prawa konfliktów zbrojnych).[354] Także MTS w opinii *Nuclear Weapons* wskazał, że Klauzula Martensa może być skutecznym narzędziem dla prawa międzynarodowego publicznego w nadążaniu za coraz szybszym rozwojem technologii wojskowych.[355]

Niewtpliwie, Klauzula stanowi zasadę istotną dla prawa cyberprzestrzeni. Przede wszystkim, jak wskazano powyżej - wyłącza ona prohibitywność w zakresie prawa konfliktów. Ponieważ nie ma wątpliwości co do stosowalności ogólnych norm prawa konfliktów zbrojnych do prawa konfliktów cyberprzestrzennych - ze względu na istnienie Klauzuli można przyjąć, że nie obowiązuje w tym zakresie prohibitywność. W związku z tym do najbardziej istotnych naruszeń cyberprzestrzeni jakimi są cyberataki, nie będą stosować się opisane wyżej problemy z nią związane. Ze względu jednak na wcześniej wskazane problemy z interpretacją statusu Klauzuli[356], nie jest jasne do jakiego stopnia może ona wpływać na prawo cyberprzestrzeni

---

wyłącznie sygnatariuszy Protokołów i w zakresie przez nie przewidzianym) do uznania jej za normę *erga omnes*. zob. Sandoz,Swiniarski Zimmerman *Commentary...* s.39 także Ticehurst R. *The Martens Clause and the Laws of Armed Conflict,* International Review of the Red Cross 317 (1997) par. 3-5

[353] por. Cameron L., Demeyere B., H. J-M, La Haye E., Lackner-Niebergall H. *The updated Commentary on the First Geneva Convention-a new tool for generating respect for international humanitarian law.* International Review of The Red Cross, 97 (900) 2015 s.1209-26

[354] zob. także Sandoz Y., Swinarski Ch., Zimmermann B *Commentary...* ss.37-43.

[355] *Nuclear...* par. 84

[356] Przyjmuje się, że stanowi ona podstawę dla norm zwyczajowych prawa konfliktów zbrojnych, *per se* nie ma statusu normy wiążącej *erga omnes* zob. Crawford E. *The Modern Relevance of the Marten Clause* ISIL Yearbook of International Humanitarian and Refugee Law t.6 (2006) ss.3-10 także Cassese A. *The Martens Clasue: Half a Loaf or Simply Pie in the Sky?*, EJIL 11:1 (2000) ss.190-200

w całości. Nie ma wątpliwości, że Klauzula odnosi się do działań przekraczających poziom użycia siły zgodnie z doktryną ekwiwalencji kinetycznej. Atak na infrastrukturę cywilną, na przykład systemy lotnisk, prowadzący do ofiar w ludziach, na mocy samej Klauzuli będzie więc nielegalny, niezależnie od zastosowanej technologii informatycznej. Nie sposób zastosować do cyberprzestrzeni powołanego wyżej orzeczenia MTS, że Klauzula będzie racjonalnym i skutecznym środkiem odpowiedzi na rozwój technologii wojskowych (wydanym zresztą w sprawie dotyczącej broni funkcjonujących w wyłączenie w świecie rzeczywistym).[357] Rozwój cyberprzestrzeni prowadzi bowiem do coraz szerszego rozwoju technologii, które mogą być użyte do prowadzenia działań o ekwiwalencji kinetycznej lub nawet bezpośrednio w świecie rzeczywistym. Użyte w Klauzuli pojęcia „sumienia publicznego" czy „humanitaryzmu" pozwalają więc na delegalizację cyberataków ze względu na ich skutki. Tym samym stanowiąc jedno z nielicznych kryteriów, pozwalających na skuteczne normowanie cyberprzestrzeni w drodze tradycyjnego prawa międzynarodowego. Przykładem może być korespondujący z Klauzulą, wskazany przez CGOE NATO wyjątek od zasady, że samo zniszczenie danych nie może być uznane za atak z użyciem siły. Grupa przyjęła, że istnieją sytuacje, w których dane mogą być natychmiastowo przekształcone w przedmioty istniejące w świecie rzeczywistym [*tangible*][358](chodzi tu głównie o pliki pozwalające na coraz szersze zastosowanie drukarek 3d przez krytyczne dla bezpieczeństwa branże jak służba zdrowia czy przemysł lotniczy).[359] Jest więc jasne, że ewentualny atak na takie dane mógłby łamać kryterium „humanitaryzmu" przewidziane klauzulą. Jednocześnie

---

[357] Wątpliwość tę wyraża też Grupa Ekspertów, wskazując że ze wzlędu na przytoczone w rozdziale niniejszym problemy interpretacyjne, stosowanie prawa konfliktów (a więc także Klauzuli Martensa) zbrojnych w cyberprzestrzeni, powinno być ograniczone wyłącznie do operacji mających ekwiwalent kinetyczny przekraczający poziom użycia siły zob. Tallinn Manual 2.0 Rule 80 i Komentarz IGoE do tegoż par. 5, [w:*Tallinn Manual 2.0* s.376]

[358] zob. Schmitt M. *Cyber Operations in International Law: The use of Force, Collective Security, Self-Defense and Armed Conflicts* [w: *Proceedings of a Workshop on Deterring Cyberattacks:Informing Strategies and Developing Option for U.S. Policy*National Academic Press (2010) s. 164

[359] Wraz z rozpowszechnieniem tej technologii cyberataki na tego typu mogą mieć skutki porównywalne z zamachami terrorystycznymi. zob. też Choi Ch.Q. *Defending 3D printers from hackers*, IEEE Tech Talks (2017) s.1 także Schmitt M.N.*Rewired warfare: rethinking the law of cyber attack*, International Review of the Red Cross 96:893(2014) s.195

konstrukcja normy zakazującej podobnego zachowania, byłaby w prawie cyberprzestrzeni nieomal niemożliwa do zrealizowania. Przyjęcie Klauzuli umożliwia jednak jego penalizację, właśnie ze względu na ostateczny skutek możliwy do osiągnięcia przy pomocy takich działań. Należy więc uznać ją za istotny element normowania przez tradycyjne prawo międzynarodowe działań w cyberprzestrzeni.

3. Lex informatica

Opisane powyżej źródła prawa cyberprzestrzeni tworzą wyłącznie ramę prawną jej funkcjonowania: głównie zasady programowe i normy abstrakcyjno-generalne. Powstaje jednak pytanie, w jaki sposób normy te mogą być konkretyzowane i jakie normy regulują obrót prawny w cyberprzestrzeni. Wydaje się, że takim systemem jest tzw. *lex informatica*. Pojęcie to zostało wprowadzone do doktryny prawa międzynarodowego stosunkowo niedawno.[360] Kluczową koncepcją w tworzeniu *lex informatica* jest przyjęcie analogii ze średniowiecznego *lex mercatoria.* Było to specyficzne prawo kupieckie powstające w Europie, wraz z rozwojem międzynarodowego handlu i powstawania ponadnarodowych związków kupieckich takich jak Hanza. Wszystkie te podmioty miały daleką idącą autonomię w normowaniu handlu, często niezależnie od państw, na terytoriach których były położone ze względu na liczne przywileje w tym zakresie. Ponieważ w średniowieczu nie istniało międzynarodowe prawo handlowe we współczesnym jego rozumieniu, *lex mercatoria* tworzyła się oddolnie: w oparciu o konsensus, swoistą funkcję praw państwowych, zwyczaj i zasadę *ex aequo et bono*. Konstrukcja taka była bliska współczesnej konstrukcji zwyczajowego prawa międzynarodowego, z tą oczywistą różnicą, że praktykę i swoiste *opinio iuris* musiałby wykazać podmioty prywatne, a nie publiczne. Źródeł prawa dopełniały przyjęte formy kontraktów podobne do dzisiejszych ramowych warunków umów, na które można było się powołać.[361] Z czasem pojawiły się, szczególnie w miastach, wyspecjalizowane sądy, orzekające

[360] Reidenberg J.R.-*Lex informatica: The formulation of Information Polict Rules through technology*, Texas Law Review 76; (1998) ss.553 i n.

[361] Goldman B. *La lex mercatoria dans le contrats et l'arbitrage internationaux: realite et perspectives*, Journal du Droit International 106 (1979) ss.477-8, 487, 495-503

ex aequo et bono[362] na podstawie *lex mercatoria*. Z punktu widzenia dzisiejszej teorii prawa, *lex mercatoria* klasyfikowalibyśmy gdzieś pomiędzy alternatywnymi metodami rozwiązywania sporów - mediacjami i arbitrażami, a wewnętrznym prawem organizacji. Jednakże *lex mercatoria* stała się w średniowiecznej Europie prawem obowiązującym, ze względu na faktyczną siłę i zakres stosowania. O ile każda władza mogła normować dziedziny, które *lex mercatoria* regulowała, a prawo stanowione miałoby pierwszeństwo w razie rozstrzygania kolizji czy zbiegów takich norm, to egzekucja norm prawa państwowego nie byłaby realnie możliwa, głównie ze względu na charakter powiązań podmiotów wiążących się *lex mercatoria*. Dane państwo mogłoby bowiem normować wyłącznie albo zachowania własnych kupców, albo regulować handel na własnym terytorium, czyli wykonywać jurysdykcję w oparciu o narodowość lub zasadę terytorialności. Brak zgody pozostałych podmiotów, uczestniczących w obrocie opartym o *lex mercatoria*, musiałby więc prowadzić do wyłączenia państwa próbującego ów handel normować z sieci powiązań handlowych, a to z kolei musiałoby się wiązać ze stratami finansowymi, zmniejszeniem ruchu handlowego i wymiernymi konsekwencjami w zakresie wpływu na międzynarodową politykę handlową. W praktyce więc taka regulacja nie byłaby wykonalna. Wynika z tego, że ani zastrzeżeń teoretyków stojących na pozycjach pozytywizmu prawniczego, twierdzących, że *lex mercatoria* funkcjonowała wyłącznie dzięki prawom narodowym,[363] ani stanowiska zwolenników prawa naturalnego wskazujących, że *lex mercatoria* musi być wspólne dla całego świata (ponieważ „wychodząc od tych samych założeń, za pomocą sprawiedliwości i rozumu nie można dojść do innych norm"),[364] nie sposób uznać za zasadne. Obydwa te stanowiska obciążone są poważnymi błędami. Tak jak stanowisko pozytywistyczne nie bierze pod uwagę faktu, że to *lex mercatoria* często kreowało normy prawa

[362] Zachowały się nawet średniowieczne zapisy sądowe notujące orzeczenia *secundum lex mercatoriam*. zob. Elcin M. *Lex Mercatoria in Interational Arbiration. Theory and Practice*, European University Institute (2012) ss.12-4

[363] zob. Schmithoff C.M.- *Das neue Recht des Welthandels*- Rabel Journal of Comparative and International Law Private Law 28 wyd. Mohr & Siebeck(1964) ss.17

[364] Tak lord Mansfield w uzasadnienie do wyroku w sprawie *Pelly v. Royal Exchange Assurance Co.* , Burrow's Reports 341,347 (1757), w odniesieniu do *lex mercatoria* istniejącego w XVIII wieku, także Schmithoff *supra* str. 1

krajowego[365], tak naturaliści z kolei nie zauważają, że wewnętrzne regulacje handlowe są w poszczególnych krajach po prostu różne. Wobec tego oparte o nie pośrednio normy *lex mercatoria*, odwrotnie niż chciałby lord Mansfield, identycznych efektów dać nie mogą. Nie wchodząc w istotę sporów z zakresu filozofii prawa, należy jednak stwierdzić, że nie można po prostu wskazać jednoznacznie katalogu źródeł materialnych *lex mercatoria*.[366] Właśnie z tego też wynika skuteczność tego prawa, opartego na multicentryczności. Było ono bowiem powołane właśnie do uzgodnienia sprzecznych sytuacji prawnych podmiotów należących do różnych porządków prawnych. Do jego powstania logicznie konieczna więc jest wielość źródeł materialnych. Tylko bowiem w ten sposób może spełniać swoją rolę. *Lex mercatoria* stała się także rodzajem systemu tworzenia prawa, gdzie rolę ustawodawcy pełni *de facto* grupa podmiotów uczestnicząca w danym obrocie prawnym, a rolę promuglacji prawa pełni stan faktyczny dotyczący dziedziny, która regulacji podlega. Potwierdza to współczesna praktyka i próby stworzenia nowego *lex mercatoria*[367] i *ius commune*.[368] Przykładowo w preambule do Zasad Handlu Międzynarodowego[369] sporządzonych przez UNIDROIT, zakres przedmiotowy i podmiotowy stosowania Zasad jest unormowany w sposób otwarty. Preambuła wskazuje bowiem, że Zasady dotyczą kontraktów, w których strony się na nie powołują bezpośrednio, lub takich w których powołują *lex mercatoria* lub ogólne zasady prawa kontraktów międzynarodowych. Możliwe jest także subsydiarne stosowanie jego norm do umów międzynarodowych (prawa prywatnego), w których strony nie dokonały wyboru żadnego prawa.[370] Takie sformułowanie Zasad oznacza, że ustawodawcy krajowi stoją w obliczu konieczności brania pod uwaga istniejącego

---

[365] zob. Też Elcin M. *Lex Mercatoria...* s.15

[366] Możliwe jest wskazanie wyłącznie pewnych grup źródeł. Niemożliwe jest jednak stworzenie z nich katalogu źródeł prawa w klasycznym rozumieniu. Zasada ta utrzymała się w międzynarodowym prawie handlowym aż do współczesności. zob. Dalhuisen J.H. *The Sources of Modern Transnational Lex Mercatoria*, Opinio Juris (2012) par.3

[367] zob. Gucer S. *Lex Mercatoria in International Arbitration*, Ankara Bar Review (2009) s.33

[368] zob. Doris M.J. The Con*tinued Resonance and Challegne of the "Ius Commune" in Modern European Contract Law*, International Journal of Legal Information 34:2, art. 14 (2006) ss.3-8

[369] UNIDROIT Principles of International Commercial Contracts 2010, International Institute for Unification of Private Law (UNIDROIT), Rzym 2010

[370] zob. ibid. Pkt 8 Preambuły

prawa subsydiarnego, na które nie mają wpływu, nawet poprzez poddanych własnej jurysdykcji członków obrotu regulowanego przez *lex mercatoria*. Tym ostatnim bowiem wystarczy nie dokonać wyboru prawa, by "uciec" spod prawa własnej jurysdykcji. Wydaje się też, że nie istnieją żadne przekonujące reguły kolizyjne na wypadek różnicy unormowań pomiędzy *lex mercatoria* a prawem krajowym.[371] Z teoretyczno prawnego punktu widzenia, normą wyższego rzędu niewątpliwie powinno być uznane prawo krajowe, wynikające z jurysdykcji zwyczajnej. Z praktycznego punktu widzenia i z ususu wynika jednak odpowiedź przeciwna. To *lex mercatoria* reguluje prawo państw krajowych. Powołana wcześniej preambuła do Zasad UNIDROIT, zawiera unormowanie wskazujące, że Zasady mogą służyć do uzupełniania porządków prawa międzynarodowego i prawa krajowego. Takie unormowanie wynikające z prawa zwyczajowego, oznacza powstanie możliwości naruszenia jurysdykcji zwyczajnej jednego państwa poprzez stworzenie odpowiedniego stanu faktycznego przez pozostałych członków obrotu prawnego[372]. Rację ma więc Phillip C. Jessup, wskazujący że *lex mercatoria* to synonim ponadnarodowego prawa o bardzo specyficznych źródłach materialnych - swoistego *ius commune*, regulującego dużo szerszy zakres niż tylko konflikty umów prawa prywatnego, wynikające z różnic porządków prawnych w krajach pochodzenia sygnatariuszy.[373] Wspólną cechą wszystkich rodzajów prawa, które Jessup uznaje za spełniające desygnat nazwy *lex mercatoria* jest przyjęcie za materialne źródła prawa stanów faktycznych i konsenusu. Oczywiście, nie wyklucza to istnienia istnienia w tych systemach norm przedprawnych[374]. Co więcej, najczęściej właśnie taka sytuacja będzie w nich zachodzić (jak choćby wspomniane powyżej rozstrzyganie sporów w historycznym *lex mercatoria* zgodnie z zasadą *ex aequo et bono*). Zwyczaj

---

[371] zob. też Klabbers J., Piiparinen T. *Normative Pluralism and International Law: Exploring Global Governance*, Cambridge University Press (2013) ss.203-5

[372] Część doktryny wskazuje, że wynika to z faktu iż systemy prawne takie jak *lex mercatoria* czy UNIDROIT, stoją niejako poza systemem prawa międzynarodowego.zob. Goldman B. *The Applicable Law: General Principles of Law-Lex Mercatoria,*Kluwer Academic (1987)s.116[w: zbiorowa,red. Lew J.D.M. *Contemporary Problems in International Arbitration*, Boston: Kluwer Academic (1987)]

[373] [w:] Jessup Ph. C. - *Transnational Law*- Yale Univiersity Press (1956)

[374] por.Berger K.P. *The Lex Mercatoria (Old and New) and the TransLex-Principles*, Trans-Lex Law Research (2018) ss.13-8

spełnia w tych systemach rolę widocznego odniesienia podmiotów uczestniczących w obrocie do zastanych stanów faktycznych. W ten sposób ograniczenia pozaprawne stają się źródłami norm prawnych, a sam proces normowania staje się wyłącznie tłumaczeniem rzeczywistości na język prawny i prawniczy, nie będąc zakreślaniem granic możliwości działania w tej rzeczywistości. Modyfikuje to zasadę *consuetudo est tacitus consensus populi*. Istotnym elementem jest bowiem milcząca zgoda ale też na przykład możliwości technologiczne podmiotów, które *consuetudo* przyjmuje. Jeżeli bowiem, jak wskazano powyżej, normowanie jakiejś dziedziny życia oparte jest o zgodę osób daną działalność wykonujących, to zarówno indywidualne jak i ogólne możliwości techniczne w tej dziedzinie będą miały istotny wpływ na to, na co owe osoby się godzą. W ten sposób miejsce ustawodawców zajmujący twórcy architektury danego systemu (jak w przypadku l*ex mercatoria,* gdzie byli nimi ci, którzy faktycznie prowadzili działania tym prawem regulowane). Stają się *quasi-ustawodawcami* w tym sensie, że to od ich działań i decyzji będzie zależało jak ukształtowane zostaną stosunki prawne, z których z kolei z upływem czasu powstaną wiążące normy.[375] Faktycznemu ustawodawcy pozostaje więc tłumaczenie norm już istniejących i czynności techniczne, a więc dbanie o brak kolizji, zgodność z normami wyższego rzędu i pilnowanie stosowania zasad dobrej techniki prawodawczej.[376] Jeżeli natomiast tradycyjny ustawodawca będzie chciał wpłynąć na normy regulujące tę dziedzinę, będzie musiał w ramach własnej jurysdykcji tak operować prawodawstwem, by działanie to miało wpływ na ogół podmiotów uczestniczących w obrocie. Na identycznych zasadach opiera się też koncepcja *lex informatica*. Od *lex mercatoria* różni je tylko fakt rozwoju techniki w zakresie cyberprzestrzeni. Rozwój ten jeszcze bardziej zwiększa zakres normowania pozostający poza zasięgiem klasycznej jurysdykcji tradycyjnych podmiotów prawa międzynarodowego. Procedury legislacyjne państw są w samej swej istocie zbyt wolne, by nadążyć za możliwościami cyberprzestrzeni a klasyczne możliwości wykonywania jurysdykcji państwowej - nieomal żadne. Pokazują to choćby nieskuteczne próby zwalczania

[375] zob. Bonell M.J.*The law governing international commercial contracts and the actual role of the UNIDROIT Principles*,Uniform Law Review, 23:1,(2018), ss.17–21

[376] por. Bonell *The Law governing*...s.25

dostępu do nielegalnie kopiowanych plików filmowych czy muzycznych w drodze traktatów podejmowane przez WIPO (*World Intellectual Property Organization*), jedną z wyspecjalizowanych agend Organizacji Narodów Zjednoczonych zajmującą się zbiorową ochroną praw autorskich. WIPO podejmowało próby zwalczania rozprzestrzenia plików poprzez procedury traktatowe (jest depozytariuszem i sygnatariuszem 26 traktatów[377]) mających na celu zwalczanie nielegalnego obrotu materiałami chronionymi prawem autorskim). Postanowienia tych traktatów miały być później implementowane do prawnych porządków krajowych sygnatariuszy. Pomimo związania się owymi traktatami przez większość państw członkowskich ONZ, walka z nielegalnymi transferami okazała się być nieskuteczna[378]. Innym przykładem mogą być działania, mające na celu blokowania przepływu danych w przywołanej sprawie *Wikileaks.* Co więcej, możliwości kształtowania prawa po stronie samych uczestników obrotu, którym tradycyjna nauka prawa nie przyznaje kompetencji ustawodawczych są dużo większe. Przykładowo, kupcy stosujący *lex mercatoria* musieli korzystać z pieniądza, emitowanego przez państwa. Konsekwentna polityka pieniężna poszczególnych państw, obliczona na określony skutek była czynnikiem, który *lex mercatoria* modyfikował, a pozostawał poza zasięgiem jego użytkowników. Podmioty stosujące *lex informatica* mają w swojej dyspozycji kryptowaluty umożliwiające dokonywanie transakcji w sposób zdecentralizowany, do którego państwa i ich banki centralne nie mają dostępu. Nie oznacza to jednak, że państwa są zupełnie pozbawione wpływu na cyberprzestrzeń. Mają one bowiem wiele narzędzi realizowania własnej polityki pod warunkiem jednak przyjęcia nowych metod jej kształtowania, odpowiednich do istnienia cyberprzestrzeni. Państwa próbujące ingerować w prawo regulujące cyberprzestrzeń za pomocą tradycyjnych narzędzi normowania niewątpliwie poniosą porażkę. Przede wszystkim jurysdykcja zwyczajna skuteczna jest wyłącznie wtedy, gdy jest poparta skutecznym wykonywaniem prawa i ściganiem tych, którzy to prawo łamią przy

[377] zob. *Summaries of Conventions, Treaties and Agreements administered by WIPO*. Publikacja *WIPO* nr. 442E/13, Genewa (2013)

[378] Howarth R.J. *Lex Mercatoria: Can General Principles Of Law Govern International Commercial Contracts?* Canterbury Law Review 10:36 (2004) ss.17-9

jednoczesnym dokonaniu atrybucji. Państwo wyłącznie normujące cyberprzestrzeń musi przegrać, nie będzie w stanie swoich norm wykonać. Państwo przyjmujące do wiadomości istnienie *lex informatica* może jednak korzystać z własnej jurysdykcji zwyczajnej i nadzwyczajnej do sprawowania bardzo istotnego wpływu na normowanie *lex informatica* a tym samym - projekcji siły w cyberprzestrzeni. Przykładem takiego wykonywania jurysdykcji może być Chińska Republika Ludowo-Demokratyczna, umożliwiająca swoim obywatelom dostęp do sieci Internet *de facto* poprzez intranet (a więc zamkniętą sieć komputerową), połączony z internetem przy pomocy kilkudziesięciu strzeżonych łącz.[379] Jednakże to normowanie wpływa na cyberprzestrzeń wyłącznie pośrednio. Państwo stosujące podobne środki (zgodnie z zasadą terytorialności) wprowadza ograniczenia funkcjonalności, jakim ma podlegać infrastruktura położona na jego terytorium. Efekt tego ograniczenia oczywiście wpływa na funkcjonowanie cyberprzestrzeni w jej informatycznej części, ale wyłącznie w zakresie transferu opartego o tą infrastrukturę. Nie zmienia natomiast samej części informatycznej. Podmiot zdolny do ominięcia zabezpieczeń infrastrukturalnych (na przykład poprzez obejście zabezpieczeń lub uzyskanie połączenia przez inny niż poddany kontroli państwowej podmiot *ISP*), może uzyskać dostęp do informatycznej części cyberprzestrzeni w sposób nieskrępowany. Na tym bowiem poziomie państwo nie może skutecznie egzekwować podobnych ograniczeń (stanowionych wyłącznie w drodze własnej jurysdykcji zwyczajnej). W praktyce *lex informatica* jest w odróżnieniu od *lex mercatoria* poddana dwutorowemu normowaniu. Podmioty tworzące *lex informatica* mogą oczywiście tworzyć własne normy w systemie niezależnie od państw. Jednak te ostatnie nie mają wyłącznie ”kontrolować strat” (jak miało to miejsce w *lex mercatoria*) w wykonywaniu własnej suwerenności, ale mają one okazje aktywnie tym stratom przeciwdziałać, a nawet z powodzeniem realizować w cyberprzestrzeni własne interesy. Podsumowując powyższe rozważania powinno się wskazać na podstawowe elementy, stanowiące częściową definicję *lex informatica*. Należy

[379] zob. Sukosd M. *Policy and Marketing Strategies for Digital Media,* Routledge, Taylor and Francis (2014)s.172

odróżnić *lex informatica* od prawa międzynarodowego.[380] Jest ono prawem właściwym wyłącznie dla normowania cyberprzestrzeni (najczęściej w jej części informatycznej). Natomiast nie ma wątpliwości, że zbiór norm *lex informatica* jest wspólny z normami *ius gentium* i może istnieć wyłącznie w korelacji z prawem międzynarodowym publicznym.[381] Także określone zdarzenia prawne w jednym z tych systemów mogą tworzyć skutki prawne w drugim z nich (jak to ma miejsce w przypadku naruszeń suwerenności w cyberprzestrzeni). *Lex informatica* nie odnosi się natomiast do świata rzeczywistego (za wyjątkiem elementów fizycznej części cyberprzestrzeni, które podlegają *lex informatica* jedynie wtedy i w takim zakresie w jakim stanowią one element całości cyberprzestrzeni). Należy także zauważyć, że nie istnieją żadne normy *lex informatica*, które normują wprost. Wobec tego, nie mogą istnieć żadne normy konkretno-indywidualne tego prawa. *Lex informatica* tworzy bowiem architekturę systemu, bardziej przypominającego zjawisko naturalne niż przestrzeń normatywną. Podmiot podejmujący w niej działania musi liczyć się nie tyle z legalnością danego zachowania co z realną możliwością jego zaistnienia. Państwa nie mają więc możliwości prowadzenia określonej polityki przy pomocy stanowienia norm *lex informatica* w sposób bezpośredni. Mogą one natomiast wykonywać swoje polityki pośrednio, poprzez wpływanie (przy pomocy norm stanowionych w ramach własnej jurysdykcji zwyczajnej) na kształt *lex informatica* jako całości. Muszą się jednak liczyć z tym, że wpływ ten będzie ograniczony, ponieważ będzie także uzależniony od wpływu innych uczestników obrotu *lex informatica* na normowanie faktyczne cyberprzestrzeni, wynikające z podobnych działań. Należy także pamiętać, że normy te istnieją zupełnie poza podziałem na prawo stanowione czy zwyczajowe. Podział ten nie może mieć zastosowania,

---

[380] Podobnie jak w przypadku rozdzielenia *lex mercatoria* i klasycznego prawa międzynarodowego wspomnianego powyżej.

[381] Nie sposób się bowiem zgodzić z poglądami, często podnoszonymi w polskiej doktrynie prawa cyberprzestrzeni, według których *lex informatica* miałoby być systemem zupełnie oderwanym od prawodawstwa krajowego. Z faktycznego punktu widzenia nie ma żadnego powodu by uznać, że regulacje państwowe nie mogą wywierać wpływu na cyberprzestrzeń a przyznać taką rolę regulacjom faktycznym dokonywanym przez podmioty niepaństwowe (często mającym znacząco mniejszy wpływ techniczny na cyberprzestrzeń). cf. Dobrzeniecki K. *Lex informatica,* wydawnictwo "Dom Organizatora", (2008) s.143

ponieważ (a) normuje stan faktyczny, a nie ma żadnego znaczenia jakie prawo do określonego stanu doprowadziło (b) nie istnieje żaden ustawodawca *lex informatica*, więc nie może być postrzegane jako reprezentacja określonego systemu prawnego. Jest to skutek niematerialnego charakteru informatycznej części cyberprzestrzeni. Pogląd taki jest wyrażany przez wielu zwolenników teorii cyberprzestrzeni jako tworu organicznego.[382] Nawet przeciwnicy takiego pojmowania cyberprzestrzeni, wskazywali że jej konstrukcja, ze względu na swoje skomplikowanie, wymaga odpowiednich, odrębnych regulacji[383]. Regulacje takie mogłoby stworzyć właśnie konsekwentne stosowanie *lex informatica* i następcza kodyfikacja oparta o obserwacje praktyki międzynarodowej.[384] Logiczną, choć niekonieczną, konsekwencją przyjęcia koncepcji *lex informatica* w opisanym powyżej kształcie, byłoby stworzenie sądu lub trybunału międzynarodowego z zakresem jurysdykcji dotyczącym wyłącznie spraw cyberprzestrzeni i orzekającego *ex aequo et bono*.[385] Byłoby to rozwiązaniem opisanego powyżej problemu niewyspecjalizowanych sądów, pozwalającym na rozstrzyganie sporów niezależnie od funkcjonowania lub niefunkcjonowania zasady *non liquet* w prawie międzynarodowym publicznym. Sądy takie faktycznie pozbawione są możliwości wydawania prawidłowych orzeczeń. Oparcie prawa procesowego takiego sądu na zasadzie *ex aequo et bono*, leżacej u podstaw *lex informatica*, należałoby ocenić pozytywnie. Wynikające z takiej konstrukcji uproszczenia procedury umożliwiałyby orzecznictwu nadążenie za rozwojem cyberprzestrzeni i uwzględnienie jej specyfiki.[386] Jasno pokazały to dotychczasowe próby powołania krajowych sądów cyberprzestrzennych, działających

---

[382] Johnson D.R., Post D. *Law and Borders- The Rise of Law in Cyberprspace* 48 Stanford Law Review (1996) ss. 1367,1368

[383] por. Graham M. *Cyberspace* ZERO Geography, artykuł opublikowany 3 października 2011 roku.

[384] Ponieważ jakakolwiek inna metoda kodyfikacji byłaby skazana na porażkę, ze względu na otwartą architekturę systemu cyberprzestrzeni. zob.Reder M.E.K.,Darrow J.J.,Melvin S.P., Chang K. K. *Cyberlaw: Management and Entrepreneurship*,Wolters Kluwer (2015) r.1 s.9

[385] por. Zipporah B.W. *The Limits of Visionof Karl Llewelyn and the Merchant Rules*, 100 Harvard Law Review 465, (1987)ss. 503-19. Należy zauważyć, że koncepcja Llewelyna znalazła zastosowanie w art. 2 UNIDROIT.

[386] Wymagałoby to jednak stworzenia większej ilości norm wiążących *erga omnes* przyjmujących skutek danego zachowania za podstawę norm sankcjonujących

w oparciu o właściwą dla danego państwa procedurę sądową.[387] Opisywane problemy są z kolei skutkiem znaczącego zróżnicowania zasad rządzących prawem cyberprzestrzeni i tych obowiązujących w klasycznym prawie międzynarodowym publicznym. Można oczywiście wskazywać na normy tego ostatniego obecne w *lex informatica*, ich interpretacja jest jednak możliwa wyłącznie w korelacji z *lex informatica.* Normy *ius gentium* będą ulegać konkretyzacji jako afordancje *lex informatica* i to te ostatnie będą ostatecznie normować cyberprzestrzeń. Należy także zwrócić uwagę na szczególny zakres normowania *lex informatica*. W przypadku *lex mercatoria*, celem tworzonego systemu prawnego było usprawnienie i uzyskanie pewności obrotu i umożliwienie swobodnego przepływu towarów w ramach istniejących stosunków międzynarodowych. Wobec powyższego stanowiło ono wyłącznie zespół norm technicznych.[388] Tymczasem zakres przedmiotowy *lex informatica* nieomal pokrywa się z zakresem przedmiotowym prawa międzynarodowego publicznego.[389] Ma ono bowiem za zadanie normować szeroko rozumiane relacje międzypaństwowe z tym jednak zastrzeżeniem, że chodzi tu o relacje wyłącznie w informatycznej części cyberprzestrzeni. Wobec tego istnieje wiele punktów stycznych i wzajemnych oddziaływań tradycyjnego prawa międzynarodowego i *lex informatica,* a zdarzenia prawne występujące w jednym z tych porządków łatwo mogą wywoływać skutki prawne w drugim z nich. Nietrudno także zauważyć, że elementem tego wspólnego zakresu przedmiotowego jest także prawo konfliktów zbrojnych. W odróżnieniu więc od *lex mercatoria*, *lex informatica* nie może być tworzona w drodze wyłącznie konsensusu, ze względu na dużo dalej idącą sprzeczność interesów jego podmiotów.

Z tego też względu, nie jest możliwe wyprowadzanie norm *lex informatica* ze zwyczaju w takim sensie, w jakim zwyczaj rozumie współczesna teoria prawa międzynarodowego.[390] Praktyka międzynarodowa podlega bowiem ciągłym

---

[387] zob. Freeman E.H. *Cyber Courts* ... ss.5-6

[388] zob. Stemler A. *Regulation 2.0: The Marriage of New Governance and Lex Informatica*, Vanderbildt Journal of Entertainment and Technology 19:1 (2016) ss.101-5

[389] ibid. S. 108

[390] ibid. 101-5

zmianom. Zależą one od zmian w środkach technicznych leżących u podstaw cyberprzestrzeni a także od stopnia zależności danego państwa od środków informatycznych. Natomiast wysoki stopnień utajnienia zarówno systemów jak i operacji cyberprzestrzennych jak i anonimowość i wielość aktorów skutecznie uniemożliwia określenie *opinio iuris*.[391] Nie jest także pewne, czy wskutek oparcia *lex informatica* o afordancje *opinio iuris* miałoby w ogólne znaczenie normatywne. Wobec niemożliwości zachowania się inaczej niż umożliwiają określone afordancje - kwestia internalizacji danej normy przez podmiot wyraźnie traci na znaczeniu. Dotychczasowe doświadczenia z próbami regulacji cyberprzestrzeni wskazują także, że przywołane powyżej kwestie utrudniają także negocjowanie traktatów, które później mogłyby stać się źródłem prawa zwyczajowego.[392] Tym natomiast co łączy *lex informatica* i *lex mercatoria* jest natomiast strona formalnoprawna. W obydwu bowiem systemach dochodzenie ochrony prawnej możliwe jest w drodze jednorazowych rozstrzygnięć wiążących wyłącznie w określonej sytuacji i określone strony. O ile jednak *lex mercatoria* osiągało ten skutek przy pomocy orzekających *ex aequo* oddolnie powołanych niezawodowych arbitrów, co upodobniało ten system do rzymskiego sądownictwa obywatelskiego - *lex informatica* jest pozbawiona tej możliwości. W przeważającej części przypadków strony danego stosunku prawnego nigdy nie zidentyfikują się (lub wręcz tożsamość ta będzie sfałszowana).[393] Nie może więc być mowy o jakichkolwiek mechanizmach egzekwowania prawa czy rozstrzygania sporów w drodze innej niż transpozycja zakazów, nakazów i dozwoleń wynikających z tego prawa do architektury systemu. Nietrudno więc zauważyć, że *lex informatica* ma więcej różnic niż podobieństw w stosunku do *lex mercatoria*. Tym natomiast co łączy obydwie konstrukcje, jest subsydiarność wobec istniejących systemów prawnych, wobec niemożliwości innego normowania określonych stanów

---

[391] zob. Biller J., Schmitt M.N. *Un-Caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences*, EJIL:Talk! (2018) s.1

[392] zob. Arimateu L. *A Treaty for Governin Cyber-Weapons: Potential Benefits and Practical Limitations* [w: zbiorowa red. Czosseck C., Ottis R, Ziolkowski K. *4th International Conference on Cyber Conflict*, NATO CCD COE Publications, (2012) ss.91-5]

[393] zob. Także Zied T., Khemakhem M. *Sybil Nodes as a Mitigation Strategy against Sybil Attack*, Procedia Computer Science, wyd. 32 (2014) s. 1135 i n.

faktycznych.

4. Źródła i konkretyzacja norm Lex Informatica

Lex informatica jest niewątpliwie multicentrycznym systemem prawnym, zarówno w sensie formalnoprawnym jak i materialnoprawnym.[394] Wydaje się, że źródło jego prawa będą odpowiadać co do zasady koncepcji Jessupa dotyczacej *lex mercatoria* wskazanej powyżej. Jest więc *lex informatica* tworzone przez wiele podmiotów, co oznaczana, że spełnia przesłankę multicentryczności w sensie formalnym. *Lex informatica* jednak spełnia także warunek multicentryczności materialnej,[395] rozumianej jako zmienność tego prawa zależnie od *ratione temporis et loci* w cyberprzestrzeni, do którego akurat dana norma ma mieć zastosowanie. Z formalistycznego punktu widzenia mamy więc do czynienia ze zbieżnym do nieskończoności ciągiem *leges speciales*, z których większość nie jest w momencie ”konkretyzacji” znana żadnej ze stron danego stosunku prawnego.[396] Rolę takich *leges speciales* mogą pełnić nie tylko normy prawa (zarówno międzynarodowego jak i krajowego regulujące afordancje, ale też elementy normowania faktycznego szczegółowo omówionego w dalszej części wywodu. Nie oznacza to, że nie można szukać źródeł *lex informatica* wśród źródeł klasycznego prawa międzynarodowego publicznego.[397] Będą one jednak wpływały na cyberprzestrzeń pośrednio poprzez sam fakt wpływania zarówno na sytuację aktorów jak i zakresu przedmiotowego tego prawa. Niewątpliwie za źródła *lex informatica* należy więc (z powyższym zastrzeżeniem) uznać źródła wymienione w art. 38 statutu

---

[394] por. Buksiński T.*Monocentrism and Multicentrism as Legal Theories in the Global Era*, Archiwum Filozofii Prawa i Filozofii Społecznej wyd. Uniwersytetu Adama Mickewicza (2015) s.7

[395] A więc systemem prawnym “otwartym”, opartym mocno o pozatekstowe źródła prawa. zob. Też Morawski L.*Główne problemy współczesnej filozofii prawa*,*Prawo w toku przemian*,Wydawnictwa Prawnicze Lexis Nexis Warszawa (2003) s.25,

[396] zob. Stemmler A. *Regulation 2.0* ss.108-10

[397] ibid. 105-8

MTS.[398] Ich znaczenie będzie jednak inne niż w przypadku tradycyjnego prawa międzynarodowego. Głównym źródłem prawa cyberprzestrzeni jest zwyczaj i praktyka międzynarodowa.[399] W przeciwieństwie jednak do *lex mercatoria* współczesnego, mającego oparcie w regulacjach *UNIDROIT*, *lex informatica* traktuje zwyczaj w sposób bliższy temu, w jaki było on pojmowany w średniowiecznej wersji *lex mercatoria*. Nie jest więc istotne *opinio iuris*, a wyłącznie sama praktyka.[400] Wynika to z dwóch powodów. Po pierwsze, w prawie cyberprzestrzeni dużo większe znaczenia mają aktorzy niepaństwowi, w których przypadku określenie tego ostatniego jest w ogóle niemożliwe. Ewentualne wyrażenie przez któryś z tych podmiotów chęci związania się którąś z powstałych w ramach *lex informatica* norm zwyczajowych nie będzie w żaden sposób wpływać na pozostałe podmioty. Podmioty takie są też nietrwałe, w związku z czym ich uznanie danej normy za wiążącą ma mniejsze znaczenie niż podobny akt po stronie państwa. Drugi powód wynika z dużej roli normowania przy pomocy architektury systemowej. Jeżeli więc podstawowym sposobem stanowienia normy jest faktyczne uniemożliwienie lub umożliwienie danego działania - praktyka przewidująca stosowanie takich rozwiązań jest wystarczająca. Nie ma bowiem znaczenia, czy określony użytkownik internalizuje daną normę, skoro nie ma on faktycznej możliwości jej złamania.[401] *Opinio iuris* nie ma większego znaczenia w sytuacji, w której nie ma po prostu innej możliwości zachowania niż to, które jest przewidziane przez regulujące normy. Podobnie, skoro architektura systemu umożliwia tylko jedno określone zachowanie w danej sytuacji, nie ma możliwości rozważać, czy dany podmiot wyraża zgodę na związanie się daną

---

[398] zob. Patrikios A. *Resolution of Cross-Border E-Business Disputes by Arbitration Tribunals on the Basis of Transanational Substantive Rules of Law and E-Busienss Usages: The Emergence of Lex Informatica*. 21st BILETA Conference (2006) ss.2-4

[399] zob.Mefford. A. *Lex informatica: Foundations of Law on the Internet* Indiana Journal of Global Legal Studies 5:1 (1997) s.230

[400] zob. Harvey T. *The Proper Legal Regime for 'Cyberspace'*, 55 Pittsburgh Law Review 993 (1994) s.1021

[401] Pośrednim powodem, dla którego praktyka i architektura stają się tak istotne, jest także brak odpowiedniego dostosowania procedur (rozumianych jako zestawy norm regulujące postępowania sądowe) i merytorycznego przygotowania sądów do rozstrzygania sporów w cyberprzestrzeni. Szczegółowo opisuje ten problem D. Johnson [w: Johnson D., Post D. La*w and Borders*... s. 1367 i n.] zob także (w odniesieniu do *lex mercatoria*)Trakman L. *The Law Merchant: The Evolution of Commercial Law* (1983) s.17

normą. Teoretycznie można by wskazywać, że podmioty mają możliwość wyrażenia niezgody poprzez wykorzystanie własnego wpływu na informatyczną część cyberprzestrzeni, należy jednak zauważyć, że w takim przypadku doszłoby do zmiany określonej normy w drodze normowania faktycznego, nie zaś odrzucenia normy zwyczajowej. Podobne znaczenie będą miały dla prawa cyberprzestrzeni pozostałe źródła prawa wymieniane przez art. 38 Statutu MTS. Nie stanowią one źródeł bezpośrednio normujących cyberprzestrzeń, a wyłącznie wpływają na jej architekturę poprzez wpływ na prawodawstwo i praktykę podmiotów obrotu międzynarodowego.[402] Jednak, o ile w świecie rzeczywistym wpływ ten będzie miał na celu realizację określonych polityk prawnych, w przypadku norm prawa stanowionego przez państwa rozumianych jako element *lex informatica*, każda konkretyzacja tych obowiązków może potencjalnie dawać skutek inny od poprzedniej (i w związku z tym niekoniecznie musi wspomniane polityki realizować). Mechanizmy tej konkretyzacji będą natomiast leżeć bowiem poza zakresem normowania tego państwa.[403] Będą też one zmieniać się w miarę rozwoju technologicznego (a więc same będą poddane normowaniu faktycznemu przez *lex informatica*). Nie oznacza to oczywiście, że naruszona jest zasada stabilności prawa czy stosowania identycznych norm w identycznych sytuacjach prawnych.[404] Powodem takiego stanu rzeczy jest fakt, że w cyberprzestrzeni identyczne sytuacje prawne w zasadzie nie mogą się zdarzać, zwłaszcza na gruncie systemu prawnego inkorporującego technikalia jako element tego systemu.[405] Należy więc zadać pytanie, czy w ramach *lex informatica* mamy do czynienia ze źródłami prawa w klasycznym ich pojmowaniu, czy też wyłącznie ze źródłami norm, nie stanowiących całościowego

---

[402] zob.także Mačák K. *Is the International Law of Cyber Security in Crisis?* [w:zbiorowa,red. Pissanidis N., Rõigas H., Veenendaal M., *8th International Conference on Cyber Conflict,Cyber Power,*NATO CCD COE Publications, Tallinn(2016) ss. 131-3

[403] ibid.ss.133-4

[404] Podstawowym problemem faktycznie uniemożliwiającym rozstrzyganie sporów powstałych w cyberprzstrzeni wyboru prawa cyberprzestrzeni Symeonides S.C. *Choice of Law in the American Courts in 1995: A Year in Review* 44 American Journal of Competitive Law 181 (1996). ss.1-2

[405] Doktryna przyjmuje nawet rozróżnienie czynności prawnych dokonanych w całości w cyberprzestrzeni i identycznych czynności dokonanych poza nią lub wykorzystujących cyberprzestrzeń wyłącznie jako środek służący do przekazu informacji. Za przyczynę tego podziału przyjmowana jest właśnie niepowtarzalność sytuacji prawnych. zob. Lemley M. *Shrinkwraps in Cyberspace*, Jurimestrics wyd. 35, 311, (1994) s. 318 i 319

systemu prawnego. *Lex informatica* reinterpretuje bowiem wiele cech tradycyjnego systemu prawnego.[406] Jego normy nie są promulgowane ani publikowane, nie mają też cech przewidywalności w tradycyjnym pojmowaniu.[407] Istotną różnicą jest też sposób egzekwowania norm.[408] Normy *lex informatica* egzekwują się same, bowiem przepływ określonych danych, do którego sprowadza się każde działanie w cyberprzestrzeni, może dawać w danych okolicznościach jeden i wyłącznie jeden efekt, stanowiący sumę wszystkich regulujących go czynników.[409] Tym niemniej nie wolno ignorować faktu, że najistotniejszym z tych czynników jest oczywiście prawo - zarówno krajowe jak i międzynarodowe. Poglądy, które odmawiają *lex informatica* rangi prawa (lub też uznają, że jest ono niezależne od prawodawstw klasycznych), pomijają ów wpływ. Przede wszystkim samo istnienie cyberprzestrzeni i jej głównych elementów jest warunkowane prawem międzynarodowym i prawa krajowymi. Nietrudno bowiem zauważyć, że istnienie cyberprzestrzeni jest warunkowane prawnie. Dotyczy to zarówno elementów fizycznych (bezpośrednio poddanych jurysdykcji terytorialnej) jak i informatycznych (poddanych *lex informatica*). W teoretycznej sytuacji, kiedy wszystkie podmioty prawa międzynarodowego, na terytoriach których mogłyby być położone elementy infrastrukturalne cyberprzestrzeni zakazałyby a następnie skuteczne wyegzekwowały zakaz umieszczenia tych elementów na swoich terytoriach (kierując te normy wyłącznie do fizycznej części cyberprzestrzeni, a więc działając w ramach niezależnej od *lex informatica* jurysdykcji zwyczajnej) - cyberprzestrzeń nie mogłaby w ogóle istnieć. Oczywiście, taki wariant wydarzeń jest nieprawdopodobny, niemniej ilustruje mechanizm gwarantujący utrzymanie zasada kontroli państwowej nad cyberprzestrzenią *per se*. Rozpatrzmy stan faktyczny, w

---

[406] Część doktryny idzie nawet dalej. Reidenberg, twierdzi nawet, że *lex informatica* zastępuje w zasadzie prawo, ponieważ regulacje tworzą w tym zakresie nie ustawodawcy a technologowie [w: *lex informatica s. 569]*, Lessig w ogóle uznaje że *lex informatica* staje się czymś w podobnym do niepisanej konstytucji, gdzie pomimo braku wyraźnego ustawodawcy i ustawodawstwa, stają się jednak wiążące podobnie do nigdy nie spisanej konstytucji brytyjskiej [zob. Lessig L. *Code 2.0* Basic Books-Perseus Books Group, s.4 (2006).]

[407] Lindquist S.A, Cross F.C. *Stability, Predictability And The Rule Of Law* [w: zbiorowa, red. Cross F.C., Lindquist S.A. *Stare Decisis As Reciprocity Norm* University of Texas Law School Press (2007)ss.50-5]

[408] ibid. s. 51

[409] zob. Nuth M.S. *Lex Informatica and Cyberspace*, University of Oslo,(2017) s.4

którym państwo ogranicza wszystkim użytkownikom cyberprzestrzeni dostęp do elementów cyberprzestrzeni opartych o serwery położone na swoim terytorium. Następnie państwo to ogranicza dostęp do części danych położonych na tych serwerach dla wszystkich komputerów znajdujących się poza granicami tego państwa, próbujących uzyskać do tych danych dostęp. W takim przypadku łatwo zauważyć, że nie ma większych różnic pomiędzy *lex informatica* a klasycznym prawem międzynarodowym. Państwo ma bowiem suwerenne prawo kontrolowania dostępu do określonych dóbr położonych na własnym terytorium. Powstaje jednak pytanie, czy w przypadku cyberprzestrzeni, dobra te w ogóle mogą być chronione w sensie czysto prawnym. Przyjęcie bowiem koncepcji, według której cyberprzestrzeń należy do *commons* musi oznaczać, że umieszczenie co do zasady jakiegoś elementu w tej cyberprzestrzeni także czyni go elementem *commons*, a wyjątki od tej zasady winny być, zgodnie z ogólnymi zasadami prawa, skonstruowane jasno i nie podlegać rozszerzeniom. Fakt, że w istniejącym stanie prawnym brak podobnych regulacji[410] nie może być interpretowany inaczej niż jako wyraz woli państw.

Państwa muszą jednak mieć na uwadze, że skoro wyraziły (choćby dorozumianą) zgodę na istnienie cyberprzestrzeni, to *lex informatica* obowiązuje w opisywanym tu kształcie. Ochrona własnych ”terytoriów” cybernetycznych tych państw nie może więc być wykonywana przy pomocy standardowych narzędzi prawnych.[411] Choć precyzyjne przewidywanie możliwości konkretyzacji nie jest możliwe, byłoby błędem uznanie, że prawo cyberprzestrzenne nie posiada cechy stabilności, a w związku z tym prawa stanowione państw nie są źródłem prawa cyberprzestrzeni. Stabilność ta wynika z faktu, że przymiot ten mają prawa, które umożliwiają samo istnienie cyberprzestrzeni.

Należy więc postrzegać *lex informatica* jako multicentryczny system prawny,

---

[410] zob. także Abramson R. *Trademarks and the Internet*, Advanced Seminar on Trademark Law, par. 299 [w: PLI Patents, Copyright,Trademarks and Literary Course Handbook Series G4-965(1996)s. 303-10] Abramson wskazuje wręcz, że nie ma możliwości stosowania starych regulacji dotyczących własności do kwestii umieszczania danych w cyberprzestrzeni. *[...] cyberspace is another world and none of the old rules apply[...]*

[411] Reidenberg rozróżnia możliwość wykonywania jurysdykcji zwyczajnej w tradycyjnym prawie i w *lex informatica.*zob. Reidenberg J.R. *Lex informatica...* s. 567

uzależniony od technologii, a konstruowany w oparciu o specyficznie pojmowany zwyczaj i praktykę międzynarodową. Normy tego prawa będą przede wszystkim chronić dobra prawne określane na mocy zasady *ex aequo et bono.* Prawo to jest ze swej natury ponadnarodowe, a podmioty prawa międzynarodowego (w tym także niestandardowe, jak na przykład *non-state actors*) mogą co prawda na nie wpływać, ale jako uczestnicy. A uczestnicy, pozbawieni władzy *imperium,* siłą rzeczy będą pozbawieni pośredniego (poprzez własne prawodawstwo) wpływu na *lex informatica* i ograniczeni do wpływu bezpośredniego (poprzez własne możliwości faktycznego modyfikowania kodu cyberprzestrzeni).

5. Normowanie granic w informatycznej części cyberprzestrzeni przez lex informatica .

Na gruncie powyższych rozważań i opisanej powyżej współzależności jurysdykcji i suwerenności państwowej należy przyjąć, że jurysdykcja zwykła może być wykonywana także co do informatycznej części cyberprzestrzeni. Jedyną dostępną państwom możliwością skutecznego stanowienia własnych norm prawnych w cyberprzestrzeni jest normowanie faktyczne w ramach *lex informatica.* Jak już wskazano powyżej, konieczną przesłanką istnienia terytorium cyfrowego jest oparcie jego elementów informatycznych o urządzenia części fizycznej zlokalizowane na terytorium państwa. Pozwala to na wykonywanie wobec tego „cyberterytorium" pełnej jurysdykcji wynikającej z normowania faktycznego, ponieważ wyłącznie normy prawa stanowione przez dane państwo będą określać kod finalnie normujący ową część cyberprzestrzeni. Mechanizm normowania pozostanie więc identyczny jak w przypadku *lex informatica* i normowania multicentrycznego całości cyberprzestrzeni - jedyną różnicą będzie fakt, że na daną część będą wpływać wyłącznie normy stanowione w ramach jurysdykcji preskryptywnej jednego państwa (zamiast wielu- jak w przypadku całej, stanowiącej *commons*, części informatycznej cyberprzestrzeni). Istotą jurysdykcji jest prawo do normowania określonych dziedzin życia i egzekwowania tych norm, a istotą suwerenności - prawo wykonywania jurysdykcji. Łatwo więc zauważyć, że panstwo, stosując opisany mechanizm

normowania: (1) będzie mogło uznać owe elementy cyberprzestrzeni za własne suwerenne terytorium; (2) będzie w stanie wykonywać w stosunku do niego swoją jurysdykcję zwyczajną. Należy teraz rozważyć, jak miałoby wyglądać faktyczne rozgraniczenie części informatycznej cyberprzestrzeni stanowiącej *commons* od jej terytorialnych elementów. Doktryna prawa międzynarodowego zauważa, że pojęcie granicy podlega ewolucji i zyskuje współcześnie nowe znaczenie. Obok oczywistego - oznaczającego rozdzielenie poszczególnych terytoriów państwowych, doktryna zaczyna coraz częściej wskazywać istnienie tzw. granic funkcjonalnych,[412] służących bardziej rozgraniczeniu interesów państw niż ich terytoriów i co najbardziej istotne - niezależnych od zasady terytorialności.[413] Takie rozumienie granic musi leżeć u podstaw konstruowania granic cyberprzestrzennych. Skoro więc każde państwo może takie normowanie wykonywać co do informatycznej części cyberprzestrzeni, musi to oznaczać że istnieje jurysdykcja cyberprzestrzenna, a co za tym idzie - państwa wykonują w cyberprzestrzeni własną suwerenność. Fakt, iż państwa nie mają ani monopolu ani możliwości normowania w pełnym zakresie przedmiotowym nie powinien być uznany za przesłankę odmowy istnienia tego rodzaju jurysdykcji. Niewątpliwie będzie natomiast oznaczać redefinicję tych pojęć. Należy jednak zauważyć, że w podobny sposób ograniczona staje się jurysdykcja państw w świecie rzeczywistym. Procesowi temu towarzyszy znaczący wzrost znaczenia norm prawa międzynarodowego wiążących *erga omnes* a także organizacji ponadnarodowych, mających wpływ na prawa krajowe, co często mocno zmienia praktykę państw - nieprzystosowaną do funkcjonowania w podobnym systemie.[414] Podobnie zresztą jak w tym ostatnim przypadku, to państwo właśnie wyraża zgodę na częściowe ograniczenie własnej suwerenności w zamian za możliwość uczestniczenia w pewnym określonym obrocie prawnym. Można więc argumentować, że nawet

---

[412] zob. Riccardi A., Natoli T. *Borders and International Law: Setting the Stage*[w: zbiorowa, red Natoli T., Riccardi A. *Borders, Legal Spaces and Territories in Contemporary International Law*, Springer (2019) ss.8-15]

[413] zob. także Bethlehem D. *The End of Geography: The Changing Nature of the International System and the Challenge to the International Law*, European Journal of International Law 25:1 (2014) s.23

[414] por. Camilieri J., Falk J. End of Sovereignty? The Politics of Shrinking and Fragmenting World Edward Elgar Publishers (1992) ss. 250-7

domniemana zgoda na uczestniczenie w cyberprzestrzeni jest w istocie *sui generis* delegacją kompetencji. Oczywiście, ochrona własnej suwerenności w informatycznej części cyberprzestrzeni może wymagać użycia siły, podobnie zresztą jak każda inna okoliczność dotycząca suwerenności. Skoro, jak wykazano powyżej, nie sposób dokonać w jasny sposób delimitacji granic cyberprzestrzeni w świecie fizycznym, konieczne jest wypracowanie sposobu określania naruszeń suwerenności w inny sposób - w oparciu o kryterium inne niż terytorialność. Zasadniczo praktyka w obrocie międzynarodowym i *opinio iuris* poszczególnych uczestników tego obrotu określa trzy możliwości (ponieważ chodzi tu wyłącznie o skutki w klasycznym prawie międzynarodowym, choć wynikłe z działań w cyberprzestrzeni - tak więc *opinio iuris* należy uznać, w przeciwieństwie do czystego *lex informatica,* za istotny czynnik). Należy tu wskazać, że praktyka ta jest jeszcze zbyt płynna a *opinio iuris* zbyt niejednolite, by można było mówić o wiążących normach prawa międzynarodowego zwyczajowego, zwłaszcza że brak jednoznacznych wskazań sądownictwa międzynarodowego czy doktryny, które mogłyby tę kwestię ostatecznie przesądzić.

Pierwsza z tych możliwości zakłada podejście praktyczne oparte na opisanej w rozdziale teorii ekwiwalencji kinetycznej i odpowiednim stosowaniu art. 51 Karty Narodów Zjednoczonych. Zwolenników tej doktryny w zasadzie nie interesuje rozgraniczenie normowania, przyjmują wyłącznie stan faktyczny w rozumieniu *lex informatica.* Suwerenność rozumieją oni wyłącznie w jej negatywnym sensie - jako prawo każdego państwa do niepodlegania atakom, interwencjom i interferencjom – niezależnie od ich źródeł. Podstawową słabością tej koncepcji jest właśnie sama doktryna ekwiwalencji kinetycznej. Z samej swej natury obejmuje ona wyłącznie zniszczenia fizyczne, takie jak dokonałyby się w wyniku ataku zbrojnego. Tymczasem takie ataki, chociaż oczywiście stanowiące rzeczywiste zagrożenie, stanowią wyłącznie jeden i niekoniecznie najważniejszy (pomimo niewątpliwie najdalej idących skutków) z typów naruszeń suwerenności w cyberprzestrzeni. Należy także wspomnieć, że atak powodujący zniszczenia w sferze materialnej, daje prawo do daleko posuniętej odpowiedzi kientycznej, uruchamiając prawo do samoobrony,

w tym uderzenia militarnego. Natomiast przyjęcie wyłącznie takiej koncepcji naruszeń jurysdykcji zostawia państwo całkowicie bezbronne wobec każdej operacji cybernetycznej, która nie powoduje zniszczeń materialnych Państwo pozostanie bezbronne nawet wobec takiego ataku, który co prawda zniszczenia zgodnie z doktryną ekwiwalencji kinetycznej powoduje, ale są one zbyt małe lub na tyle nieistotne, by zostać uznane za atak zbrojny lub użycie siły w rozumieniu Karty Narodów Zjednoczonych.[415] Należy bowiem pamiętać, że nawet cyberoperacja prowadząca do strat materialnych analogicznych do tych wynikłych z działań zbrojnych, może zostać uznana za niewystarczający powód do uzasadnienia obrony kinetycznej, jeżeli jej intensywność nie przekracza stopnia starć (*border clashes*).

Druga koncepcja zakłada dokonanie swoistej analogii z zasady terytorialności i wskazuje, że państwo, pomimo stałej zmienności cyberprzestrzeni, jako swoje *sui generis* terytorium może traktować te elementy cyberprzestrzeni, które dotyczą infrastruktury materialnej podlegającej jurysdykcji tego państwa na mocy zasady terytorialności rozumianej ściśle, albo też w jakiś sposób wpływają na istniejące w materialnym świecie podmioty i przedmioty prawa poddane jurysdykcji tego państwa. Ta z kolei konstrukcja wydaje się być wyprowadzana z analogii z zasadą represji wszechświatowej stosowanej powszechnie przyjmowanej w międzynarodowym prawie karnym. Państwo ma jurysdykcję nad danym zdarzeniem w cyberprzestrzeni wtedy, gdy dotyczy jakichś jego interesów. Taką konstrukcję przyjęła na przykład Unia Europejska w GDPR (a także w poprzedzających jego wejście w życie aktach prawnych o ochronie danych osobowych).[416] Wskazywała ona tam bowiem, że akty owe stosują się do wszystkich transferów danych, które choćby przechodzą przez łącza należące do UE albo dotyczą któregokolwiek z podmiotów poddanych jurysdykcji zwyczajnej Unii. Niewątpliwie niewłaściwe są poglądy, według których jest to wykonywanie jurysdykcji

[415] Kwestia podobnych ataków (na przykład *border clashes* zdefiniowane przez MTS w *Nicaragua*) zostanie omówione w rozdziale dotyczącym prawa konfliktów cyberprzestrzennych.

[416] zob. art.art. 1-6 RODO

nadzwyczajnej. Z samej z swej istoty bowiem, jurysdykcja nadzwyczajna opiera się o wyłącznie wykonywanie skutków jurysdykcji zwyczajnej poza jej granicami. Innymi słowy, w ramach jurysdykcji nadzwyczajnej nie może być mowy o jakimkolwiek elemencie normatywnym o charakterze generalnym czy abstrakcyjnym a wyłącznie o wykonywaniu praw (lub prawa międzynarodowego czy innych norm wiążących *erga omnes*).

Trzecia koncepcja stanowi połączenie obydwu powyższych. Zakłada ona jednoczesne stosowanie koncepcji terytorialności cyberprzestrzennej w rozumieniu opisanym powyżej wobec wszystkich cyberoperacji, z jednoczesnym przyjęciem koncepcji ekwiwalencji kinetycznych, jeżeli operacje te przekraczają poziom użycia siły. Wydaje się, że ta koncepcja jest najsłuszniejsza, choć także niepozbawiona wad. Przede wszystkim stosować się będzie do niej wątpliwość dotycząca ataków niekinetycznych i wszystkich operacji, które naruszają suwerenność, nie posiadając ekwiwalencji kinetycznej. Za słuszne należy więc uznać jej rozszerzenie, przyjmujące, że suwerenność państwa w cyberprzestrzeni jest naruszana nie tylko wtedy, gdy naruszone zostaną ”granice” jego cyfrowego terytorium, ale także zawsze wtedy, gdy zostaną naruszone jego nieterytorialne „granice funkcjonalne” w rozumieniu opisanym powyżej. Taka koncepcja naruszeń suwerenności zostanie przyjęta w dalszej części wywodu.

6. Zwyczaj w lex informatica a zwyczaj w prawie międzynarodowym.

Prawo zwyczajowe jest jednym z podstawowych źródeł prawa międzynarodowego publicznego. W ten sposób staje się też oczywiście elementem prawa cyberprzestrzeni, w taki sposób, w jaki każda norma tradycyjnego prawa międzynarodowego publicznego ma wpływ na cyberprzestrzeń. Nie ma też wątpliwości, że przypisywanie postępowaniu państw norm wiążących pozwala rozwiązywać wiele problemów interpretacji stanu faktycznego. Dzieje się tak zwłaszcza wtedy, kiedy pojawiają się zjawiska nowe, nieopisane, czy też o nie do końca jeszcze poznanych granicach. Byłoby więc niezwykle korzystne, gdyby można było wskazać choćby częściowe

normy prawa zwyczajowego, które wiązałyby państwa w cyberprzestrzeni, szczególnie że tak szybko zmieniająca się dziedzina życia jak cyberprzestrzeń musi ze swej natury wymykać się próbom klasycznych kodyfikacji. Wątpliwe jest jednak, czy możliwe jest dokonanie takiej konstrukcji. Międzynarodowy Trybunał Sprawiedliwości w art. 38(1)(b) Statutu uznaje prawo zwyczajowe za wiążące pod warunkiem łącznego spełnienia dwóch przesłanek. Musi więc, co oczywiste, istnieć *usus* - utarta praktyka państw posługiwania się lub oczekiwania od innych państw danego modelu zachowania w określonej sytuacji; musi także istnieć *opinio iuris*, subiektywna chęć danego państwa związania się ta normą. Próbą spełnienia pierwszej przesłanki jest powstanie Tallinn Manual i Tallinn Manual 2.0. Ujęcie najczęściej powtarzających się problemów prawnych w prawidła, choćby niewiążąco, może prowadzić do stworzenia *ususu* - zwłaszcza w razie powoływania się państwa na te źródła w codziennej praktyce.. Niemniej będzie on daleki od doskonałości. Po pierwsze, TM 2.0 reguluje najbardziej fundamentalne problemy, głównie prawa dotyczące naruszeń suwerenności ze szczególnym uwzględnieniem prawa konfliktów zbrojnych. Wiele kwestii dotyczących obrotu cyberprzestrzennego, nie naruszającego interesów państw trzecich w ogóle nie zostało w nim ujętych. Po drugie, większość działań cyberprzestrzennych jest przez państwa utrzymywana w ścisłej tajemnicy, co utrudnia obserwację praktyki w stosunku do wielu zakresów prawa cyberprzestrzeni, a *opinio iuris* w cyberprzestrzeni jest, jak wskazano powyżej, praktycznie nieobecne. Niekoniecznie więc fakt, że państwa w określonej sytuacji przyjmują dany model zachowania, musi konstytuować praktykę. Może bowiem wynikać z innych czynników, niewidocznych z powodu wspomnianego utajnienia. Ostatni problem stanowi okoliczność, że przypisanie odpowiedzialności w cyberprzestrzeni jest ciągle niezmiernie trudne. Szacuje się, że w przypadku działań państwowych prawdopodobieństwo błędu w przypisaniu odpowiedzialności wynosi około 30 procent.[417] W przypadku działań dokonywanych przez *non-state actors,* staje się ono jeszcze trudniejsze, a jak wskazano powyżej w rozdziale dotyczącym testów przypisania - nawet prawidłowa atrybucja nie gwarantuje przypisania. Skoro nie

[417] zob. Klimburg A. *The Darkening Web... s.187*

można więc mówić o przypisaniu, nie sposób też wykazywać, jakie są dalsze działania państw. Pewną podstawą dla opisania prawa zwyczajowego mogłaby być historia kryzysu w relacjach amerykańsko-chińskich w związku z licznymi przypadkami szpiegostwa przemysłowego w USA, dokonywanymi przez chińskie rządowe grupy hakerskie, a także trzy kanoniczne już stany faktyczne dla prawa cyberprzestrzeni. Chodzi o kazus *Stuxnetu* i uderzenie na irańskie wirówki atomowe, a także dwa ataki przeprowadzone przez wojska informatyczne Federacji Rosyjskiej przeciwko Estonii i Gruzji Warto zaznaczyć, że w żadnym z tych, powszechnie uznawanych za największe i najważniejsze, przypadków operacji cyberprzestrzennych, nie udało się określić jednoznacznie praktyki państw zaatakowanych jak i aktorów, którzy operacje przeprowadzali. Spowodował to zarówno wysoki stopień utajnienia samych operacji, ich celów oraz skutków, jak i niemożliwość jednoznacznej atrybucji. Uzasadniony więc wydaje się wniosek, że prawo zwyczajowe cyberprzestrzeni, w tradycyjnym rozumieniu jako suma *opinio iuris* i praktyki międzynarodowej, wydaje się nieosiągalne. Wszystkim podmiotom prawa międzynarodowego brak bowiem wystarczających informacji do zbudowania jasnego obrazu sytuacji, a także do pełnego zrozumienia przyczyn zachowania innych uczestników obrotu. W związku z tym nie ma także możliwości skonstruowania *opinio iuris*. Drugim znaczeniem w jakim zwyczaj kształtuje prawo cyberprzestrzeni jest oczywiście jego rola w powstawaniu i aktualizowaniu *lex informatica*. Jak wskazano powyżej, w tym zakresie istotna jest wyłącznie praktyka państw, a rola *opinio iuris* pozostaje marginalna. W tym sensie zwyczaj jest jednak obecny wyłącznie w *lex informatica* a co za tym idzie, w informatycznej części cyberprzestrzeni.

7. Normowanie faktyczne.

Dla precyzyjnego zrozumienia zasady działania *lex informatica* należy także rozważyć dokładnie sposób normowania istniejący w tym systemie. Ze względu na opisaną powyżej zasadę tworzenia tych norm, w pracy niniejszej przyjęto określenie

normowania faktycznego. O ile bowiem, klasyczne systemy prawne tworzą normy, które ulegają konkretyzacji w sytuacji spełnienia odpowiednich przesłanek a następnie dzięki wykonywaniu prawa wpływają na zachowania podmiotów tego prawa, *lex informatica* pomija ów krok. Normy tego prawa nie tyle konkretyzują się w danej sytuacji, co umożliwiają lub uniemożliwiają określone zachowania. Zamiast klasycznych nakazów, zakazów i dozwoleń[418]*, lex informatica* zna wyłącznie stany kwantowe.[419] Oczywiście, zastosowanie niektórych z możliwych rozwiązań może naruszać normy tradycyjnego prawa narodów, jednakże naruszenia takie odbywają się na metapoziomie prawa cyberprzestrzeni. Ma to znaczenie o tyle, o ile jest możliwe następcze wskazanie normy prawa międzynarodowego odnoszącej się do określonego zachowania lub skutku.[420] Skuteczna ochrona podstawowych interesów prawnych państw, takich jak suwerenność, może odbywać się nieomal wyłącznie na poziomie *lex informatica*.[421]

Staje się więc jasne, że cyberprzestrzeń i jej natywne prawo łamie monopol tradycyjnie pojmowanego prawa na normowanie. Zastępuje go takie normowanie, w którym prawo staje się tylko jednym z narzędzi i jednym ze źródeł norm. Pozostałymi stają się przede wszystkim możliwości technologiczne. Zyskują natomiast na znaczeniu normy rozproszone,[422] czy odwołania do pozaprawnej i pozaprawniczej struktury świata rzeczywistego.[423] Pogląd ten, zyskując na

---

[418] zob. Nieznański E. Logika Deontyczna w systemie S5,Studia Philosophiae Christianae 43 ,Uniwersytet kardynała Stefana Wyszyńskiego (2007) s.8

[419] Nielsen M.A, Chang I.L.*Quantum Computation and Quantum Information*, Cambrdge Univeristy Press (2000) ss.53-9

[420] Przykładem może być stosowanie technologii *blockchain* do kodowania informacji. Jest to system oparty o sieć komputerów z dostępem do pewnego ciągu danych, zabezpieczonych nieomal niemożliwym do złamania szyfrem. Zarówno wprowadzanie jak i przetwarzanie danych w tym systemie jest poza kontrolą państw, zakaz stosowania podobnych technologii nie byłby możliwy do wyegzekwowania a decentralizacja systemu uniemożliwia znalezienie wszystkich kopii danej informacji. Tym samym *blockchain* pozostaje wyłącznie w domenie *lex informatica*. Nie oznacza to jednak, że nie może zostać użyty do działania międzynarodowo zakazanego - jak zakazana interwencja w sprawy państwa trzeciego a tym samym - powodując skutki w prawie międzynarodowym publicznym. zob. Też Wright A., de Flippi P. *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*,SSRN,(2015) ss.1-7

[421] zob. na przykładRussel S.Dewey D. Tegmark M.*Research Priorities for Robust and Beneficial Artificial Intelligence,*AI Magazine 36, No 4 (2015),s.3*:*

[422] zob. Durkheim E. *Zasady Metody Socjologicznej* Biblioteka Socjologiczna PWN (2016)

[423] Goldoni M. *The Normativity of Code as Law: Toward Input Legitimacy* Globalisation Constitution Project FWO Foundation (2011) ss.6-7

popularności, został w końcu wyrażony w używanym przez jurysprudencję przychylną koncepcji normowania prawa cyberprzestrzeni w sposób faktyczny, w określeniu *Code is Law*.[424] Z zaakceptowania kodu jako czynnika normatywnego wynika nie tylko, że podmioty działające w cyberprzestrzeni zyskują *sui generis* autonomię, ponieważ tworzą prawa same dla siebie, ale też - że czynią to nie za pomocą jakiejś autonomicznej legislatywy, lecz za pomocą faktycznego wyznaczania granic możliwości postępowania.[425] Dyskusje na temat sposobu w jaki dochodzi do owego normowania jakiejś *sui generis* procedury tworzenia faktycznego prawa cyberprzestrzeni nie doczekały się rozstrzygnięcia. Najbliższa prawdy wydaje się przyjmowana przez amerykańskich teoretyków prawa cyberprzestrzeni analogia do lobbystów; wpływających na klasyczny proces legislacyjny.[426] W porównaniu tym chodzi o podkreślenie faktu, że to podmioty mające interes w określonym rozstrzygnięciu normatywnym podejmują pewne działania faktyczne, zmierzające do wprowadzenia określonej normy do systemu. Oczywiście analogia ta jest wyłącznie poglądowa i pomija dwa najważniejsze dla normowania faktycznego aspekty. Pierwszym jest fakt, że działalność lobbystyczna odbywa się w ramach ustalonej legislacji i może być wykonywana wyłącznie pośrednio, poprzez wpływ na podmioty prawo stanowiące w sposób bezpośredni. W przypadku normowania faktycznego cyberprzestrzeni, podmioty, działające w celu uzyskania określonego efektu normatywnego wpływają bezpośrednio na architekturę systemu (jak to mam miejsce w przypadku normowania faktycznego). Działania te stoją *per se* poza klasycznym systemem prawa międzynarodowego i same w sobie nie są w żaden sposób normowane, lub normowane pośrednio, o ile leżą w zakresie jurysdykcji zwyczajnej państw. Drugą kwestią jest brak jakiegokolwiek procesu legislacyjnego, na który można byłoby wspomniany wpływ wywierać. Ewentualne dążenie do zmiany

---

[424] Określenie to pochodzi od tytułu artykułu Lawrence'a Lessiga, w którym wprowadził on do doktryny koncepcję normowania faktycznego. zob. Także Lessig L. *Code is Law* Harvard Magazine 1/2001 (2001) s.2

[425] por.Dommering E.Asscher L.F. *Coding regulation- Essays on the Normative Role of Information Technology* Information Technology and Law Series T.M.C. ASSER Press/ Springer (2006); autorzy analizują wręcz konsekwencje przyjęcia istnienia technologii jako alternatywy dla klasycznego procesu legislacyjnego.

[426] zob. Wu, T. *When Code Isn't Law* Virginia Law Review 89 (2003) s.7;

normowania kodem, musi zakładać po prostu zmianę tego ostatniego.

Nie oznacza to jednak, że samo *lex informatica* jest w całości od prawa odrębne. Należy bowiem zauważyć, że istnienie normowania faktycznego nie wyłącza istnienia wspólnych z normami prawa międzynarodowego publicznego zakresów normowania. Staje się więc *lex informatica* także zespołem *leges speciales*, prawa międzynarodowego publicznego. Ta cecha *lex informatica* pozwala podmiotom obrotu międzynarodowego na interpretację zdarzeń faktycznych w cyberprzestrzeni w ramach prawa międzynarodowego, a także na wpływanie na cyberprzestrzeń przy pomocy tradycyjnych metod wykonywania jurysdykcji.

Istotny problem z ostatnią wskazaną cechą tworzy z punktu widzenia prawa międzynarodowego kwestia wskazania momentu, w którym określone normy "kodu" stają się prawem w rozumieniu prawa tradycyjnego. Wydaje się, że najlepszym rozwiązaniem jest proponowane w europejskiej doktrynie prawa cyberprzestrzeni[427] przyjęcie, że za moment ten należy przyjąć chwilę, kiedy normy te spełnią kryteria Fullera.[428] Nietrudno zauważyć, że normy *lex informatica* spełniają wszystkie z tych ośmiu kryteriów.[429]

1. Generalna obowiązywalność (*Generality*)

Fuller wskazuje, że norma prawa musi być generalna, a więc odnosić się do każdego podmiotu, który znajduje się w określonej sytuacji prawnej. Dowolna norma *lex informatica* oparta jest o architekturę systemu, nie ma więc możliwości, by działanie tego kodu zmieniało się zależnie od czynników leżących poza tą architekturą, a więc w ujęciu prawnym - poza samym systemem normatywnym.

2. Promulgacja(*Promulgation*)

W rozumieniu ścisłym, ten warunek wydaje się nie być spełniony przez normowanie faktyczne cyberprzestrzeni. Jednakże Fuller uznaje warunek promulgacji za spełniony także w szerszym sensie, a więc pod warunkiem spełnienia przesłanki powszechnego

---

[427] Asscher, L. *'Code' as Law. Using Fuller to Assess Code Rules.* [w:*Coding Regulation*,zbiorowa, red. E.J. Dommering and L. Asscher Asser Press ss.61-90]

[428] Fuller L.L. *The Morality of Law* Yale University Press (1969)s. 39.

[429] zob. Także komentarz L. Fullera do kryteriów. ibid. Ss.46-90

poinformowania uczestników obrotu o sposobie funkcjonowania tych norm.[430] Ponieważ każdy potencjalny uczestnik obrotu w ramach *lex informatica* ma możliwość wglądu w architekturę kodu, warunek ten należy uznać za spełniony.

3. Prospektywność *(Prospectivity)*

Kryterium prospektywności zakłada, że norma prawna je spełniająca normuje przyszłe zachowania. Ponieważ jakiekolwiek działania podejmowane w ramach cyberprzestrzeni z technicznych względów muszą być dostosowane do jej aktualnie obowiązującej konstrukcji, *lex informatica* ze swej natury wyklucza jakąkolwiek retroaktywność norm.

4. Jasność norm (*clarity*)

W swoim czwartym kryterium Fuller zawarł dwie przesłanki. Po pierwsze, norma musi dla swoich adresatów tak jasna jak to tylko możliwe. Po drugie, musi ona być interpretowana w sposób możliwe najbliższy jej powszechnemu pojmowaniu i w sposób wykluczający stosowanie interpretacji jako środka zmieniającego rzeczywiste znaczenie normy dekodowanej z danego przepisu. Łatwo zauważyć, że w przypadku *lex informatica* aktualny zbiór zachowań to ten, który jest możliwy do wykonania w ramach samej architektury systemu.[431] Przykładowo więc, przełamanie zabezpieczeń informatycznych będzie zachowaniem nielegalnym *ex aequo et bono*. Jego norma faktyczna będzie zakazywać będzie prowadzenia działań ze strony osób niepowołanych.[432] Zrozumienie funkcjonowania systemu implikuje więc zrozumienie norm faktycznych z niego wynikających a ich interpretacja rozszerzająca nie jest możliwa z samej istoty cyberprzestrzeni. Normy faktyczne są więc jasne i nie ma możliwości ich zmiany znaczenia w drodze interpretacji.

5. Niesprzeczność (*non-contradictory*)

6. Możliwość wykonania (*not ask the impossible*)

---

[430] por. Murphy C. *Lon Fuller and the Moral Value of the Rule of Law* 24 Law and Philosophy 239(2005) s. 4 i n.

[431] Niekoniecznie oznacza to oczywiście, że zachowania te będą legalne w rozumieniu prawa międzynarodowego publicznego.

[432] Należy oczywiście przyjąć istnienie kontratypów. Nie ma wątpliwości, że przykładowo służby prowadzące postępowanie będą miały prawo naruszyć zabezpieczenia serwera, na którym przechowywane są dane, które zostały wcześniej skradzione.

7. Stałość (*constant*)
8. Zgodność normy i sposobu jej egzekwowania (*congruence between statue and enforcement*)

Cztery ostatnie cechy wskazane przez Fullera, należy uznać za spełnione przez *lex informatica* z samej jego natury. Skoro normy faktyczne są skutkiem architektury systemu, nie ma możliwości by nie spełniały one któregoś z czterech ostatnich kryteriów. Taka sytuacja oznaczałaby bowiem, że dany fragment kodu stanowi jego błąd, a tym samym nie może być uważany za część tego systemu i w konsekwencji za normę *lex informatica*. Sam Fuller wskazywał, że w jego ujęciu prawo ma stanowić ”metodę dostosowywania ludzkiego zachowania do określonych zasad”.[433] Zestawienie tej ostatniej przesłanki z ośmioma wskazanymi powyżej kryteriami pozwala łatwo zauważyć, że *lex informatica* należy uznać za prawo w ścisłym sensie. Łatwo też dostrzec, że momentem, w którym dana jego norma spełni wskazane kryteria będzie moment jej technicznego wprowadzenia do systemu. Każda więc zmiana kodu w cyberprzestrzeni staje się prawem tej ostatniej w momencie, w którym zaczyna funkcjonować w sensie technicznym. Wtedy bowiem spełnia zarówno kryteria Fullera jak i staje się wspomnianą metodą dostosowywania zachowań podmiotów działających w cyberprzestrzeni do zasad nią rządzących. Należy zauważyć, że kryteria Fullera były już wcześniej wykorzystywane do analizy systemów prawnych opartych o zwyczaj[434] i uzasadnione wydaje się przeprowadzenie tego rozumowania także w kontekście prawa cyberprzestrzeni. Porównanie *lex informatica* z pozostałymi systemami o podobnej konstrukcji prowadzi także do wniosku, że pozytywnie należy ocenić powszechność możliwości tworzenia kodu, przynajmniej w jego najistotniejszych elementach. Stanowi ona bowiem czynnik przesądzający o zupełności normowania *lex informatica*. Owa powszechność wśród części doktryny jest uznawana za przesłankę zwiększenia demokratyzacji sporządzania kodu i w konsekwencji- demokratyzacji *lex*

[433] zob. Fuller *Morality*... s.106
[434] Asscher *Using Fuller...*, . s.2

informatica.[435]

Takie rozwiązanie, choć teoretycznie słuszne, jest oczywiście w praktyce niemożliwe do implementacji. Przede wszystkim, o konieczności jego odrzucenia musi przesądzać różnica w czasie, w którym dla własnej efektywności muszą powstawać elementy kodu w działającej w czasie rzeczywistym cyberprzestrzeni. Nie ma bowiem czasu na podejmowanie decyzji w drodze mechanizmów demokratycznych, tak, by wprowadzone tą drogą zmiany mogły zostać skutecznie zaimplementowane w sensie faktycznym. Nie zmienia to oczywiście słuszności odwołania się do kryteriów Fullera. Wskazują one bowiem jasno, że wyłącznie przy zastosowaniu koncepcji prawnonaturalnych możliwe jest ujęcie normowania faktycznego i szerzej, całego systemu prawa części informatycznej cyberprzestrzeni. Z samej natury tej dziedziny wynika bowiem niemożliwość istnienia takiej pozytywistycznej teorii, która umożliwiałaby stworzenie formalnoprawnych podstaw takiego normowania. Demokratyzacja, którą koncepcja Asschera przewiduje, ma jeszcze jeden aspekt. Jest próbą wprowadzenia mechanizmów ochronnych przez decentralizację normowania, oznaczającą w praktyce utratę monopolu państw na stanowienie prawa. Porównanie *lex informatica* z pozostałymi systemami o podobnej konstrukcji prowadzi także do wniosku, że należy pozytywnie ocenić powszechność możliwości tworzenia kodu, przynajmniej w zakresie najistotniejszych jego elementów. Stanowi ona bowiem czynnik przesądzający o dążeniu do zupełności normowania *lex informatica*. Owa powszechność jest uznawana przez cześć doktryny za przesłankę zwiększenia demokratyzacji sporządzania kodu, a w konsekwencji - demokratyzacji tej części prawa międzynarodowego publicznego, które pozostaje w ścisłym związku z *lex informatica.*[436]

Takie rozwiązanie, choć teoretycznie słusznie, jest oczywiście w praktycznie niemożliwe do implementacji. O konieczności jego odrzucenia musi przede wszystkim przesądzać różnica w czasie, w którym dla własnej efektywności muszą

[435] Asscher L. *'Code' as Law*...s.3 chodzi tu o elementy dotyczące życia większości obywateli państw.

[436] Asscher L. *'Code' as Law*... chodzi tu o elementy dotyczące życia większości obywateli państw.

powstawać elementy kodu w działającej w czasie rzeczywistym cyberprzestrzeni. Nie ma bowiem czasu na podejmowanie decyzji w drodze mechanizmów demokratycznych, tak, by wprowadzone tą drogą zmiany mogły zostać skutecznie zaimplementowane w sensie faktycznym. Nie zmienia to oczywiście słuszności odwołania do kryteriów Fullera. Wskazują one bowiem jasno, że wyłącznie przy zastosowaniu koncepcji prawnonaturalnych możliwe jest ujęcie normowania faktycznego, a szerzej - całego systemu prawa informatycznej części cyberprzestrzeni. Z samej natury tej dziedziny wynika bowiem niemożliwość istnienia takiej pozytywistycznej teorii, która umożliwiałaby stworzenie formalnoprawnych podstaw takiego normowania. Należy także zwrócić uwagę, że demokratyzacja, którą koncepcja Asschera przewiduje, ma jeszcze jeden aspekt. Jest próbą wprowadzenia mechanizmów ochronnych przez decentralizację normowania, która w praktyce oznacza utratę monopolu państw na stanowienie prawa, Przyczyną tej utraty jest właśnie zgodność kodu z kryteriami Fullera.[437] Kod mający cechy normatywne mogą bowiem tworzyć zarówno podmioty prywatne jak i państwa poprzez swoje organy. Prowadzi to oczywiście do rozszerzenia liczby podmiotów, będących *de facto* (a w pewnym sensie nawet - jeżeli widzieć *lex informatica* poprzez pryzmat ścisłej analogii z tradycyjnym *ius gentium - de iure*[438]) ośrodkami normowania.[439] Jednakże ośrodki państwowe mają, co oczywiste, przewagi wynikające właśnie ze stojącej za nimi siły państw. . Należy odróżnić ten stan rzeczy od istniejącego w doktrynie prawa międzynarodowego pojęcia multicentryczności[440], przyjmującego za punkt wyjścia tradycyjne pojmowanie jurysdykcji i opartego o koncepcję kompetencji przekazanych. W normowaniu faktycznym bowiem brak przekazywania jakichkolwiek kompetencji; te wskazane powyżej należą natomiast wyłącznie do podmiotów, które je wykonują. Podmioty te nie muszą (choć mogą, jeżeli są nimi państwa) wykonywać jakiejkolwiek

[437] Dommering E.Asscher L.F. *Coding regulation- Essays...* s.2-6

[438] Poglądy te są podobne, do koncepcji uznających globalne społeczeństwo jako autonomiczny podmiot, któremu przysługuje kompetencja ustawodawcza. zob. Scheinpflug Ch. *The Global Civic Society as normative entity?* GRIN Geistenwissenschaft (2012) ss.3-7

[439] Goldoni M. *The Normativity...*

[440] zob. Łętowska E. *Multicentryczność współczesnego systemu prawa i jej konsekwencje* Państwo i Prawo r.60 z. 4 (2005) s.3-10

jurysdykcji w rozumieniu prawa międzynarodowego, by tworzone przez nie normy faktyczne znajdowały się w systemie cyberprzestrzeń regulującym. W związku z tym normy tworzone przez podmioty, które mają możliwość normowania faktycznego (nie można tu bowiem użyć mającego jasne konotacje z *imperium* państwowym pojęcia 'kompetencja'), będą najczęściej kolidować z normami stanowionymi przez podmioty mające jurysdykcję w sensie tradycyjnym. Mamy więc do czynienia ze *sui generis* sporem kompetencyjnym, który jednak nie jest uregulowany w żadnych przepisach prawa i nie może być przez nie rozwiązany. Żadna bowiem próba skonstruowania takiego normowania nie będzie w stanie nadążyć za rozwojem technologii. Przykładem takiego "sporu kompetencyjnego" pomiędzy tradycyjną legislatywą a normowaniem faktycznym może być opisany poniżej spór Unii Europejskiej z ICANN dotyczący zastosowania przepisów *GDPR* do prowadzonego przez ICANN systemu WHOIS. Pomimo ostatecznego braku dostosowania przez ICANN swoich systemów do *GDPR*, oparte o systemy ICANN przypisania adresów internetowych funkcjonują w Unii Europejskiej bez przeszkód.[441] Wynika to oczywiście z faktu, że realna egzekucja *GDPR* w stosunku do ICANN musiałaby w praktyce prowadzić do odłączenia UE od sieci Internet, albo wręcz od całej cyberprzestrzeni. Należy bowiem pamiętać, że o ile spór sądowy z *EPAG* (będący w istocie zabiegiem prawnym, pozwalającemu *ICANN* na dotarcie w toku instancji do TSUE) dotyczy wyłącznie przyszłych rejestracji (chodzi o realizację obowiązku wynikającego z umowy *ICANN* i *EPAG*), *GDPR* wiąże także *ICANN* w odniesieniu do już posiadanych przezeń danych podmiotów, co do których przedmiotowe zastosowanie GDPR znajduje. Ten ostatni[442] ogłosił natomiast, że do wymogów GDPR swoich rejestrów nie dostosuje,

[441] 3 sierpnia 2018 roku, niemiecki sąd I instancji oddalił pozew skierowany przez ICANN przeciwko swojemu niemieckiemu rejestratorowi, EPAG o wydanie nakazu zbierania danych przewidzianych umową z ICANN, których EPAG przestał żądać od podmiotów chcących zarejestrować nowe domeny, uznając że nie ma do tego prawa zgodnie z regulacjami GDPR. Sąd odmówił wydania nakazu, nie rozstrzygając jednak w uzasadnieniu czy zbierania takich danych byłoby legalne pod rządami GDPR czy też nie. Po apelacji ICANN do Sądu Apelacyjnego w Kolonii, sąd pierwszej instancji (zgodnie z Zivillprozessordnung) uznał za konieczne powtórne rozpatrzenie sprawy, od której wniesiono apelację.

[442] Przykład ICANN, jako instytucji stosującej normowanie faktyczne poza jakąkolwiek kontrolą państw, pojawiał się w doktrynie już wcześniej. zob. Na przykład Froomkin M *Toward a critical Theory of Cyberspace* Harvard Law Review 116(2003) s.3-10

ponieważ nie ma takiej technicznej możliwości. W istocie więc, pomimo iż ICANN nie ma żadnej podstawy prawnej by wpływać na legislację unijną, nie ma wątpliwości, że GDPR w odniesieniu do niego nie zostanie wyegzekwowany. Pośrednio wskazuje na to przywołane powyżej orzeczenie sądu w *ICANN v. EPAG* z sierpnia 2018 roku, omijające istotę tego sporu. Niezależnie od rozstrzygnięć sądowych, *ICANN* ciągle nie wykonał obowiązku dostosowania się do *GDPR* (zarówno w sensie faktycznym jak i prawnym), podnosząc, że wyroki sądowe w sprawie nie nakładały na niego takich obowiązków (i pomijając zupełnie fakt, że obowiązek ten został już uprzednio nań nałożony przez obowiązujące w Unii prawo). Sprawa ta jest ściśle powiązana z wspomnianą powyżej kolizją kompetencyjną. Dochodzi tu bowiem do podobnej jak w *Yahoo! v. LICRA* sytuacji, w której jeden podmiot próbuje wykonywać swoją jurysdykcję preskryptywną wobec podmiotu tej jurysdykcji nie poddanemu. UE bowiem dąży do tego, by wyegzekwować stosowanie własnych norm od podmiotu prawa amerykańskiego. Spór ten różni się jednak od sprawy *Yahoo* dwoma istotnymi szczegółami. Po pierwsze, *ICANN* działa w UE poprzez swoje spółki-córki (*ICANN subsydiaries*), zakładane na prawach poszczególnych państw UE, a więc poddanych jej jurysdykcji. Po drugie zaś, należy pamiętać, że *GDPR* zawiera powołane wyżej uregulowania, które wymagają spełnienia tych uregulowań od każdego podmiotu, prowadzącego działalność związaną z przetwarzaniem danych w jurysdykcji UE, niezależnie od domicylu. Ponieważ zarówno EPAG jak i sam *ICANN* spełnia tę przesłankę, nie ma wątpliwości, że są one poddane jurysdykcji UE w tym zakresie. Unia Europejska jest jednak pozbawiona realnej możliwości egzekucji tych norm. Zakaz działalności *ICANN* w UE oznaczałby bowiem utratę możliwości dostępu do systemów IP i DNS dla wszystkich podmiotów w UE. Skutki takiego działania byłyby bardzo szerokie i trudne do oceny (także w jurysdykcjach trzecich - ze względu na wszechobecność części informatycznej cyberprzestrzeni). O ile więc UE ma możliwość związania swoim prawem *ICANN* w sensie tradycyjnego prawa międzynarodowego, nie jest ona w stanie egzekwować korespondujących z GDPR norm faktycznych w *lex informatica.* Brak tej możliwości prowadzi w konsekwencji do tego, że norma prawa tradycyjnego staje się prawem martwym.

Normowanie prawa cyberprzestrzeni przy pomocy tradycyjnego prawodawstwa, które w zamierzeniu ustawodawcy ma transponować dozwolenia, nakazy i zakazy do informatycznej części cyberprzestrzeni, odbywa się bowiem przez afordancje. Kreowanie norm prawnych poprzez afordancje zawiera w sobie znaną maksymę Lessiga, mówiącą o tym, że ”kod jest w cyberprzestrzeni prawem”, ale ma ono znaczenie szersze. Nie jest bowiem tak, że to wyłącznie kod jest źródłem tworzenia afordancji.[443] Możliwości tworzenia kodu, także podlegają pewnym normowaniom, przede wszystkim przez prawo tradycyjne (do nich także stosują się kryteria Fullera), ale także przez normy tradycyjnie uznawane za pozaprawne.[444] Wynika z tego, że *imperium* państwowe traci jakiekolwiek znaczenie prawne w procesie egzekucji prawa (choć nie, jak wskazano powyżej, w procesie jego stanowienia) . Skoro każdy z podmiotów może (przy założeniu, że ma takie możliwości faktyczne) skonstruować afordancje systemu w taki sposób, by osiągnąć zakładany cel, a afordancje te mogą być tworzone w ramach zbiorowo tworzonego, nigdzie nie kodyfikowanego prawa - wydaje się, że prawnie rozumiane *imperium* rozumiane jako monopol na egzekucję prawa staje się wyłącznie konstrukcją teoretyczną. W jego miejsce państwa mogą wykonywać *imperium* do tworzenia afordancji, które umożliwią im realizację własnych polityk. Przykładowo, Unia jest w stanie skorzystać z przysługującego jej *imperium* by wskazać *ICANN* i *EPAG* model zachowania. Jednak brak możliwości ukształtowania przez nią odpowiednich afordancji w ramach jej systemu informatycznego uniemożliwia jej skuteczne egzekwowanie tych norm na poziomie faktycznym. Wynika z tego oczywisty wniosek, że jurysdykcja zwyczajna ma w cyberprzestrzeni wyłącznie aspekt stanowienia prawa, traci natomiast swój aspekt

[443] zob. także. Cena F.,Rapp A., Marcengo A., Brizio A., Hilviu D., Tirassa M. *The Role of Affordance in Cyber-Physical Systems for Behavioral Change* Internet of Things - User-Centric IoT, Springer (2014) s.87

[444] Taką normą może być zarówno norma spełniająca kryteria materialnoprawne (jak na przykład stopień społecznej internalizacji norm dotyczących prawa regulującego ściąganie plików z internetu kształtującego wielkość służącej temu infrastruktury) jak i kryteria formalnoprawne (za takie należałoby uznać zwyczaje dotyczące korzystania z komputera, *de facto* regulujące ilość dostępnej w danym momencie mocy obliczeniowej). Niewątpliwie należy tu także ująć także sankcje rozproszone, które w przypadku sporu *ICANN* i UE, mogłyby na przykład oznaczać istnienie po stronie UE skutecznej możliwości nacisku politycznego lub ekonomicznego. zob. też. Morgan J. *Extra-legal norms: the irrelevance of the law (of contract)?*, Cambridge University Press (2013) s. 71 i n.

egzekucyjny. Konieczna jest wobec tego zmiana rozumienia *imperium* w *lex informatica; imperium* dotychczas zakorzenionego w tradycyjnych źródłach prawa - hierarchicznych, abstrakcyjnych i wynikających z określonych polityk, które ustawodawca za ich pomocą zamierza osiągnąć. Konkretyzacja norm *lex informatica* jest algorytmiczna i *per se* deterministyczna. Realizacja jakichkolwiek polityk za pomocą wyłącznie jej norm nie jest możliwa.[445] Jest bowiem *lex informatica* funkcją systemu afordancji, które dany podmiot zdołał dla realizacji własnych interesów skonstruować w informatycznej części cyberprzestrzeni. Nie sposób się zgodzić z poglądem, że podstawowa różnica między konkretyzacją norm prawa stanowionego a normowaniem faktycznym leży w tym, że ta pierwsza jest semantyczna, natomiast *lex informatica* podlega konkretyzacji wyłącznie syntaktycznej.[446] Nietrudno bowiem zauważyć, że konsekwentne przyjęcie tego poglądu jest co do istoty tożsame z teorią *das Reine Rechtslehre*, a jak wskazano powyżej, *lex informatica* może funkcjonować wyłącznie w obszarze koncepcji prawa naturalnego.

7. a. Podległość normom faktycznym

Należy zauważyć, że normy faktyczne w zupełnie inny sposób regulują zachowania adresatów norm. W tradycyjnie pojmowanym prawie norma (niezależnie od tego czy jest stosowana pośrednio czy bezpośrednio) wymaga dokonania subsumpcji do określonego stanu faktycznego i w ten sposób tworzy prawo, obowiązek lub zwolnienie od obowiązku danego zachowania. Taki proces nie dokonuje się w normowaniu faktycznym .Jak słusznie zauważa natomiast Lessig: *[...]one obeys these laws as code not beacuse one should; one obeys these laws as code beacuse one can do nothing else[...]-[...]prawa wynikającego z kodu nie przestrzega się dlatego, że istnieje taki obowiązek; przestrzega się go dlatego, że nie można zrobić niczego innego[...]*.[447] W istocie normowanie faktyczne z natury rzeczy nie operuje, jak

[445] zob.także Devin C., Fellin T., Kauffman S., Kopl R. *The Law and Big Data*, Cornell Journal of Law and Pulbic Policy 27:358, (2017) s.358

[446] cf.Devin et al. *The Big Data...* s. 359 i n.

[447] Lessig L. *The Zones of Cyberspace* Stanford Law Review 48 5/1996 (1996) ss.35-7

tradycyjne prawo nakazami, dozwoleniami i nakazami, ale tworzeniem i wyłączaniem możliwości zachowania się w określony sposób (a więc przywołanymi już wcześniej afordancjami). Różnica ta, pomimo iż *prima facie* wydaje się wyłącznie techniczna, ma doniosłe znaczenia prawne. Po pierwsze, wyłącza ona możliwość istnienia jakichkolwiek norm generalnych i programowych wyłączających zastosowanie danej normy w razie wystąpienia warunków szczególnych. Wobec normowania faktycznego nie sposób przykładowo uznać zastosować najczęściej przytaczanych przykładów takich norm jak Formuła Radbrucha[448], czy *rebus sic stantibus*. Afordancje w oczywisty sposób nie zmieniają bowiem swojego funkcjonowania zależnie od jakichkolwiek okoliczności. Po drugie, oznacza, że orzecznictwo i *jugde-made law* w ogólności (podobnie jak wszystkie normy tradycyjnego prawa międzynarodowego) stanowi w systemie normowania faktycznego wyłącznie jeden z elementów składowych, który może wpływać na końcową normę, ale nie może o niej przesądzać. Rozstrzygnięcie sporu na drodze orzeczenia sądu lub trybunału - wiążące dla prawa międzynarodowego publicznego, dla *lex informatica* będzie dopiero początkiem rozstrzygania. Sąd nie może bowiem orzec w sposób wiążący system afordancji. Ewentualne zmiany w tych ostatnich, mogą się dokonać wyłącznie w drodze zmian normowania przez państwa związane tym orzeczeniem i następczo wpłynąć na *lex informatica*. Zmiana taka nie będzie jednak bezpośrednim skutkiem wydanego orzeczenia.

Co do zasady, normowanie faktyczne łączy niejako pozytywistyczną i naturalistyczną teorię prawa. Tworzenie norm odbywa się w sposób koncepcyjnie bliski teoriom prawnonaturalnym, jednak ich skutek jest z kolei bliższy koncepcjom pozytywistycznym. Brak bowiem przy afordancjach określonych prawodawców, czy określonych norm pozwalających się stosować, niemniej skutkiem takiego procesu są normy niepodważalne i pozbawione w zasadzie jakichkolwiek klauzul generalnych czy wyjątków od stanowiących przez siebie reguł, a więc doskonale odpowiadające duchowi *das reine Rechtslehre.*

[448] Lex iniustissima non est lex- Prawo najbardziej niesprawiedliwe nie jest prawem [nie zasługuje na ochronę]. zob. Radbruch G.Gesetzliches Unrecht und Uebergesetzliches Recht, Sueddeutche Juristenzeitung (1946)

Najistotniejszym wnioskiem z istnienia normowania dla prawa międzynarodowego publicznego jest brak rozróżnienia przez normy faktyczne na podmioty publiczno- i prywatnoprawne. Konstrukcji kodu, opartego o opisane powyżej afordancje, podlegać będzie zarówno państwo i jak i każdy inny podmiot. Państwa będą miały w ramach swojej jurysdykcji większy wpływ na ostateczny kształt tych afordancji, ale nietrudno zauważyć, że sytuacja taka nie zawsze będzie miała miejsce i uzależniona będzie od wpływu faktycznego. Niektóre podmioty niepaństwowe, które z powodów faktycznych mają istotny wpływ na afordancje *lex informatica* (jak miało to przykładowo miejsce w przypadku działań Kaminsky'ego i Postela opisanych w tej rozprawie lub w przypadku podmiotów takich jak *ICANN*) mogą mieć na normowanie faktyczne wpływ równy państwom.

7. b. Bezzasadność arugmentów przeciw istnieniu normowania faktycznego.

Podstawowym argumentem przeciwko normowaniu faktycznemu jest oczywiście wysuwany przez pozytywistów zarzut, że w rzeczywistości nie jest ono prawem.[449] Podnoszą oni, że związek pomiędzy normowaniem wynikającym z prawa a stanami faktycznymi może istnieć wyłącznie w tym, że prawo normuje owe stany. Odrzucają więc przeciwnicy *lex informatica* pogląd, że stany te można interpretować jako element samego systemu mający znaczenie prawne.[450] Innym zarzutem jest, że zwolennicy prawa cyberprzestrzeni mówiąc o *lex informatica* tworzą sztuczny system prawa (wspomiane już *prawo konia*), podczas gdy cyberprzestrzeń należy po prostu regulować jak wszystkie inne dziedziny życia, zachowując prymat prawa stanowionego.[451] Argumenty te, nawet z pozytywistycznego punktu widzenia, nie są jednak przekonujące. Jak pokazuje praktyka, dotychczasowe tradycyjne prawo i sposoby normowania nie są wystarczające do unormowania cyberprzestrzeni.

---

[449] zob. Lambers R. *Code is not Law,* raport z konferencji *Code as Code* w Amsterdamie, INDICARE Team, Karlsruhe Institute of Technology (2004) par. 1 i 2

[450] Brownsword R. *Code, Control and Choice:Why West is West and East is East* Legal Studies 25:1 (2005) s.1-21

[451] Biegel S. *Beyond Our Control? Confronting the Limits of our Legal System in the Age of Cyberspace* MIT Press, Boston (2001)ss.

Konsekwentne przyjęcie koncepcji pozytywistycznej w odniesieniu do niej musiałoby prowadzić do niezliczonych luk prawnych, które z kolei musiałoby wypełniać normowanie faktyczne.[452] Łatwo także dostrzec, że niemożliwość normowania cyberprzestrzeni w drodze prawa stanowionego stoi w sprzeczności z podstawowym aksjomatem szkoły pozytywistycznej, a więc zasadą kompletności prawa.[453] Wydaje się więc, że pozytywistyczne postrzeganie prawa międzynarodowego w coraz większym stopniu się dezaktualizuje, a ono samo - wraz ze stopniowym przechodzeniem z porządku westfalskiego[454] do postwestfalskiego[455]- coraz bardziej ciąży w kierunku grocjańskiego pojmowania prawa naturalnego.[456]

Nie oznacza to jednak, że za trafne należy uznać argumenty przeciwko *lex informatica* proponowane przez szkołę prawnonaturalną.[457] Argumentacja ta opiera się o założenie przyjmujące, że *lex informatica* nie jest w ogóle potrzebne, ponieważ państwa mogą sprawować pełną kontrolę nad zdarzeniami w informatycznej części cyberprzestrzeni[458] za pomocą (koniecznych) pośredników, pomiędzy informatyczną częścią cyberprzestrzeni a jakimkolwiek podmiotem lub przedmiotem poddanym jurysdykcji zwyczajnej danego państwa. Wu i Goldsmith wskazują, że obywatel, który chciałby (korzystając z cyberprzestrzeni) wykonać działanie, którego zakazuje prawo tego kraju, nie może tego zrobić poprzez bezpośredni transfer danych

---

[452] przyznaje to też sam Easterbrook, twierdząc że w zakresie, w którym cyberprzestrzeni nie da się unormować za pomocą istniejących już norm, należy pozostawić ją samej sobie, wskazując *Then let the world of cyberspace evolve as it will and enjoy the benefits- a potem (po uregulowaniu tego co możliwe w drodze transpozycji istniejących norm) pozwólmy cyberprzestrzeni ewoluować jak chce i korzystajmy z tego rozwoju* [w: Easterbrook *Cyberspace and the Law... ss.23-5*] Należy więc z tego wnosić, że jego spór z Lessigiem dotyczy wyłącznie zakresu normowania faktycznego nie zaś samej zasady.

[453] zob. Hall S. *The Persistent Spectre: Natural Law, International Order and the Limits of Legal Positivism*, European Journal of International Law 12 (2001) s.297

[454] Fassbender B. *Peace of Westphalia (1648)* [w:*Max Planck Encyclopaedia of International Law*,zbiorowa red. Wolfrum R.] Max Planck Stiftung (2011) MPEPIL 739

[455] Termin został pierwszy raz użyty w przemówieniu brytyjskiego premiera Tony'ego Blaira, zob. Harris M. *Why is Tony Blair lending credibility to Kazkhstan's dictator?* Artykuł opublikowany w *The Telegraph* 2 lutego 2012 roku, zawierający transkrypcję z przemówienia.

[456] Parry J.T. *What is the Grotian tradition in international Law?* Univeristy of Pennsylvania Journal of International Law 35: 299 (2014) ss.315-318

[457] Chodzi tu o oczywiście o współczesną szkołę prawa naturalnego, opartą o poglądy R. Dworkina, nie zaś prawo naturalne w jego historycznym ujęciu.

[458] Niezależnie od tego czy nad mają kontrolę nad nią samą czy też nie. Co do tej kwestii poglądy są zróżnicowane, a wynik tego sporu dla zakresu pracy niniejszej nieistotny.

z jakimkolwiek serwerem położonym poza granicami jego kraju, a poprzez łącze umożliwiające mu ten transfer. Operator tych łącz, jak i samo łącze, stanowiąc elementy fizycznej części cyberprzestrzeni, są poddane jurysdykcji zwyczajnej tego państwa.[459] W związku z tym państwo to może, korzystając z własnej jurysdykcji preskryptywnej, zakazać pewnych zachowań owym pośrednikom, efektywnie uniemożliwiając dane działanie także użytkownikowi końcowemu.[460] Taka argumentacja (choć zasadna z punktu widzenia czysto prawnego), nie wytrzymuje jednak zetknięcia z rzeczywistością. Rozpowszechnienie się technologii *VPN*[461] umożliwia nie tylko omijanie ewentualnych mechanizmów wykrywania pakietów przez operatora sieci, ale wręcz przybranie przez użytkownika fałszywego adresu IP, w tym wskazującego fałszywie, jakoby przebywał on w innej jurysdykcji. Tzw maskowanie adresu IP[462] umożliwia przykładowo wskazanie operatorowi, że użytkownik wykonujący operację uznaną za nielegalną w jego jurysdykcji, przebywa i wykonuje tą operację w jurysdykcjach, w których są one dozwolone, a jego sieć wykorzystywana jest wyłącznie w celach przesyłowych. Ewentualne łamanie 'płaszcza' *VPN*, (jakkolwiek technicznie wykonalne) jest bardzo skomplikowane i wymaga ukierunkowanych działań. Nie mogą być więc prowadzone *in abstracto*. Mogą więc być skuteczne w przypadkach najistotniejszych, jednak nie można ich stosować do kontrolowania całości przesyłu danych we współczesnym państwie z choćby przeciętnym wolumenem ruchu sieciowego. O ile więc możliwe jest preskrypytywne wykonywanie jurysdykcji w ten sposób na poziomie prawnym, jej wykonywanie będzie nieomal niemożliwe w praktyce.[463] Nadto należy zauważyć, że

---

[459] cf. Wu.T., Goldsmith J. *Who controls...* ss. 69-72

[460] zob. Goldsmith J. *Against Cyberanarchy,* University of Chicago Law Review t. 65, s. 1198 (1998), także Wu T. *Cyberspace Sovereignty? The Internet and International System*, Harvard Journal of Law and Technologyt. 10 s. 679 (1997)

[461] *Virtual Private Network*. Technologia umożliwiająca przesył tzw. przezroczystych pakietów danych. Numery IP, są owym pakietom przypisywane przez wewnętrzną w stosunku do całej cyberprzestrzeni, sieć prywatną.

[462] zob. Baker F., Montgomery D., Luckie M. et al. *Addressing the challenge of IP spoofing*, Internet Society (2015) ss.3-6

[463] Za przykład nieskuteczności normowania działań pośredników, może służyć brak realnych sukcesów w prawnym zwalczaniu możliwości nielegalnego przesyłu i pobierania muzyki, filmów i skanów książek. zob. Raport *Global Online Piracy Study* sporządzony przez Instytut Prawa Informatycznego Uniwersytetu w Amsterdamie, s.27-31 (2018)

zdecydowana większość istotnych naruszeń cyberprzestrzennych (a więc stanowiących zagrożenie dla interesów państwa, a nie działania kryminalne) nie wykorzystuje podmiotów *ISP*. Opisywana tu kontrola jest więc bardzo ograniczona zakresowo.

7. c. Relacje prawa stanowionego i normowania faktycznego

Nie ma wątpliwości, że opisane wyżej mechanizmy powodują wzajemne przenikanie się *lex informatica* i tradycyjnego prawa międzynarodowego publicznego. Należy więc postawić pytanie czy są one dwoma konkurencyjnymi systemami czy też może dwiema częściami większego systemu normatywnego? Wydaje się, że jednak właściwa jest druga odpowiedź. Pomimo wielu wskazanych powyżej niedoskonałości, przywołane już odwołanie do kryteriów Fullera, oraz uznanie wynikającej z nich koncepcji „globalnego podmiotu normującego" proponowanej m.in. przez Asschera[464] wydaje się być słusznym kierunkiem. Normowanie faktyczne więc staje się po prostu prawem. Dzieje się to w momencie zaistnienia danej normy w architekturze systemu i w zakresie w jakim na ową architekturę wpływa - a więc w czasie i w zakresie w jakim spełni ona kryteria Fullera. Ponieważ, jak wskazano powyżej, zakresy normowania *lex informatica* i prawa międzynarodowego regulującego cyberprzestrzeń są różne (choć nie rozłączne) - musimy uznać, że stanowią one dwa filary regulacji cyberprzestrzeni. Ważne jest też, że tradycyjne prawo jak i normowanie faktyczne wzajemnie na siebie wpływają. Wobec tego, logiczną niemożliwością staje się przyjęcie koncepcji zakładającej konkurencyjność tych porządków.

7. c. 1. Wpływ prawa stanowionego na lex informatica i normowanie faktyczne

Niezależnie od głosów wskazujących na oderwanie normowania cyberprzestrzeni od państw i wykonywanej przez nie jurysdykcji, oczywiste jest, że wpływ tworzonych przez nie norm na cyberprzestrzeń jest przemożny. Dane mogą być udostępniane, zwielokrotnianie i w inny sposób przetwarzane w cyberprzestrzeni (rzeczywiście poza

[464] Asscher, L. *'Code' as Law. Using Fuller...*

kontrolą państw), ale sama cyberprzestrzeń niczego nie tworzy, jest wyłącznie sumą danych do niej wprowadzonych. Przykładowo, Federacja Rosyjska ograniczyła możliwość dostępu do danych wrażliwych jej służb kontrwywiadowczych w cyberprzestrzeni wprowadzając w części z nich zakaz prowadzenia akt w postaci cyfrowej. W ten sposób norma prawa administracyjnego, nakazująca sporządzanie maszynopisów, a więc w ogóle nie dotycząca cyberprzestrzeni, normuje faktycznie możliwość działania cybernetyczne. Klauzule generalne prawa krajowego, takie jak na przykład nakaz transparentności i ścisłej celowości zbierania danych przez organy administracyjne od obywatela normują wtórnie kod użyty do budowania określonych stron internetowych. Na mocy prawa UE[465], strony internetowe dostępne w Unii Europejskiej, wymagają zatwierdzenia przez użytkownika regulaminu przetwarzania jego danych osobowych, zanim rozpoczęte zostanie oferowanie usługi, jednocześnie definiując moment tego rozpoczęcia w innych przepisach jako samo otwarcie strony. W efekcie jedynym środkiem w pełni legalnej konstrukcji strony jest uniemożliwienie nawet oglądania zawartości strony zanim regulamin i polityki przetwarzania danych nie zostaną potwierdzone. Jednakże potwierdzenie wymaga zidentyfikowania komputera, z którego zgoda zostaje wyrażona za pomocą tzw. plików *cookies*. Te zaś na mocy samego GDPR[466] są uznane za dane osobowe. Z punktu widzenia prawa stanowionego, udostępnienie niewielkiej ilości danych (zidentyfikowanie komputera w celu wyrażenia zgody) zanim owa zgoda zostanie wyrażona jest koniecznym technicznym wyjątkiem. Z punktu widzenia *ratio legis* normy jest on nieistotny ze względu na brak pozaprawnego znaczenia faktycznych czynności, w drodze których obowiązek ów jest wykonywany. Spróbujmy porównać sytuację opisaną powyżej z pozornie podobną sytuacją zapłaty za przejazd pociągiem. Z punktu widzenia prawa stanowionego oczywiste jest, że pasażer pociągu, zobowiązany po wejściu do tego pociągu do ”natychmiastowego” zgłoszenia konduktorowi braku biletu i kupienia go,

[465] zob. Art. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 roku w sprawie ochrony danych osób fizycznych w związku z przetwarzaniem danych osobowych prze instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylające rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE, Dz.Ur. UE L 295/39

[466] zob. Preambuła do GDPR (30)

przez pewien czas (aż do momentu znalezienia konduktora i faktycznego kupienia biletu) będzie pozostawał w owym pociągu nie opłaciwszy przejazdu. Nie ma jednak wątpliwości, że pasażer, który owe czynności faktyczne podejmuje, wykonuje obowiązek nałożony na niego przez normę prawną i nie powinien podlegać karze za brak biletu. Norma chroni określone dobro prawne, jakim jest uzyskanie przez przewoźnika należnej opłaty za przejazd. Zarówno czynności faktyczne jak i sam bilet nie tylko nie mają same w sobie znaczenia w oderwaniu od owej normy, ale nawet nie są do jej spełnienia konieczne, stanowiąc wyłącznie konwencjonalny dowód wniesienia opłaty za przejazd i zawarcia umowy przewozu. Zupełnie dopuszczalne byłoby na przykład zawieranie takiej umowy w formie ustnej. Podobnie bilet *per se* nie ma żadnego innego znaczenia niż to, które nadawane mu jest przez prawo. Ostatecznie więc normowanie prawem stanowionym jest w tym przypadku wyłączne i nie może istnieć żaden inny system normowania, który mógłby mieć wpływ na zarówno na dekodowaną normę jak i sposób wykonania wynikającego z niej obowiązku. Podobnie ustawodawca regulując sposób uiszczania opłaty za przejazd nie musi brać pod uwagę żadnych pozaprawnych okoliczności faktycznych. Jest to sytuacja diametralnie odmienna od przywołanego wyżej sposobu udostępniania regulaminów w ramach świadczenia usług drogą elektroniczną.

Norma nakazująca wyrażenie zgody normuje też faktycznie cyberprzestrzeń, z punktu widzenia której zbieranie tej zgody jest stosunkowo nieistotne. Prowadzi natomiast do istotnych zmian w samym kodzie. Konieczne jest bowiem takie stworzenie architektury witryn internetowych, by umożliwiały one zbieranie tych danych. Tworzy to dwie normy dotyczące samej cyberprzestrzeni. Po pierwsze, wymusza bardziej zamkniętą na interakcję sieć wymagającą większej ilości identyfikacji, przekazując w istocie część kompetencji państwowych na pozbawione jakichkolwiek kompetencji publicznoprawnych podmioty odpowiedzialne za prowadzenie tych stron.[467] Pod drugie, choć celem normy stanowionej przez państwo jest ochrona danych obywateli, faktycznie tworzy się norma wymuszająca na nich

[467] Do podobnych wniosków (choć analizując inny przykład zamknięcia dostępów do Internetu), dochodzi także Lessig [w: Lessig L. *The Law of The Horse: What Cyberlaw Might Teach* Harvard Law Review 113:501 3/99]

dokonanie identyfikacji. Żeby bowiem wyrazić zgodę na jakikolwiek regulamin, komputer użytkownika musi zostać zidentyfikowany po swoim numerze *IP*. A więc musi zostać przeprowadzana analiza fragmentów adresowych pakietów danych, która potwierdzi właściwość numeru. To z kolei umożliwia jego dalsze śledzenie, kojarzenie z innymi danymi przypisanymi do tego numeru, czy - wskazując już na najdalej idące konsekwencje - umożliwia dokonanie ataku cybernetycznego na tego użytkownika.[468] W istocie mamy więc do czynienia z dwiema, zupełnie odrębnymi normami. Jedna z nich wynika z wykładni przepisu prawa stanowionego, druga natomiast staje się normą *lex informatica*, nakazującą podmiotom w niej działającym skonstruowanie odpowiednich afordancji. Te ostatnie jednak są konieczne wyłącznie by spełnić normę prawa tradycyjnego, z punktu widzenia *lex informatica* nie tylko nie chronią tego samego dobra prawnego (a więc anonimowości użytkownika), ale przeciwnie - dobro to naruszają. Należy zauważyć, że normy te zawsze z natury swojej muszą być bezsprzeczne. Brak tej bezsprzeczności wynika z tego, że normowanie faktyczne musi odzwierciedlać wykonanie normy prawa stanowionego, a samo jego istnienie wynika ze specyfiki cyberprzestrzeni.[469] Konstatacja ta przeczy tezom zwolenników poglądu o zupełnej nieregulowalności części informatycznej cyberprzestrzeni[470], bowiem bezdyskusyjnie tworzy sytuację w której standardowe prawodawstwo normuje cyberprzestrzeń.[471] Ilustruje także, w jaki sposób mogą funkcjonować w cyberprzestrzeni kryteria Fullera (tu - kryterium niesprzeczności norm). Należy jednak także zauważyć, że normę faktyczną może stworzyć ten podmiot, który ma możliwość odpowiedniego wpływanie na kod. Nie jest więc potrzebne posiadanie przezeń jurysdykcji.[472]

---

[468] Dla uproszczenia wywodu, pominięte tu zostaną mogące potencjalnie modyfikować opisywany stan faktyczny kwestie dostępu z publicznych komputerów czy zmiennego lub fałszywego IP.

[469] Lessig L. *The Law of The Horse. What Cyberlaw...*

[470] D. Kushner *The Communications Decency Act and the Indecent Indecency Spectacle* 19 Hastings Communications and Entertainment LAw Journal 87, 131 (1996)

[471] por. Lessig L. *The Law...*

[472] Kang J. *Developments in the Law- The Law of Cyberspace* 112 Harvard Law Review 1574, 1643 (1993)

7. c. 2. Wpływ normowania faktycznego na prawo stanowione

Przyjęcie opisanych powyżej kierunków stanowienia prawa przez państwa nie musi być i częstokroć nie jest jednak wystarczające dla realizacji założonych przez to państwo celów czy też ochrony określonych dóbr prawnych.[473] Nietrudno zauważyć, że normy faktyczne wpływają nie tylko na wykonawcze normy ale także na same polityki, kierunki działania i normy abstrakcyjne promulgowane przez państwa. Styk prawa stanowionego i *lex informatica* staje się najbliższy Dworkinowskiej teorii *prawidłowej odpowiedzi*.[474] Dworkin twierdzi bowiem, że prawo (o ile zostanie prawidłowo zinterpretowane) zawsze daje prawidłową odpowiedź na określony problem. Nie znaczy to jednak, że wynik taki można uzyskać zawsze - prawidłowe odpowiedzi na pewne problemy prawne są po prostu niemożliwe.[475] W przypadku prawa regulującego cyberprzestrzeń, owa Dworkinowska odpowiedź istnieje zawsze, ponieważ tworzy ją architektura systemu. Wspomnianą 'najlepszą odpowiedzią' są bowiem określone afordancje. Mechanizm ten jest łatwo dostrzegalny we współczesnym prawie własności intelektualnej i prawie autorskim, jednocześnie pozostającym w domenie państwowej i regulującym liczne treści cyfrowe. Zabezpieczenia mające swoją podstawę prawną w ustawodawstwie realizowane są najczęściej przy pomocy kodu regulującego sposób, w jaki treści chronione przez to prawo mogą być wykorzystywane.[476] Ze względu jednak na fakt, że treści te mogą być zabezpieczane wyłącznie za pomocą określonych (kodem) środków - architektura systemów komputerowych i normowanie faktyczne wyznacza granice, które twórcy prawa muszą brać pod uwagę. Przykładem takich norm prawnych są regulacje

---

[473] cf. Pogląd Abbey Stemler opisującą działanie dwukierunkowości normatywnej na przykładzie systemu PayPal [w: Stemler A., *Regulation 2.0: The Marriage of New Governance and Lex Informatica*,Vanderberg Jorunal of Entertainment and Technology Law, t. XIX:1, (2016)s.110

[474] zob. Dworkin R. *No Right Answer*, Essays in Honor of H.L.A. Hart, zbiorowa, red. Hacker P.M.S., Raz J., Oxford Clarendon Press, (1977) ss. 58-84

[475] zob. ibid. Dworkin daje przykład

[476] Chodzi o tu na przykład o tzw.zabezpieczenia DRM (*Digital Rights Management*). Powstają wskutek umieszczenie w ciągu kodu pozwalającego użytkownikowi na odtworzenie pliku ciągu znaków, który identyfikuje odpowiedni plik a także zabezpiecza go przed niektórymi operacjami (np. kopiowaniem) zob. Miller M. *Is it Safe? Protecting Your Computer, Your Bussiness, and Yourself Online* Que Publishing (2008)

pozwalające uzależniać cenę książki lub programu komputerowego od ilości możliwych "otwarć" (a więc udzielać licencji na określoną ilość wykorzystań danego utworu) lub od istnienia lub nieistnienia możliwości wydruku tej treści. Ewentualne podobne regulacje bez istnienia odpowiednich zabepieczeń komputerowych musiałby być martwe, ponieważ brak narzędzi, by wyegzekwować podobne ograniczenia.[477] Z drugiej jednak strony, cyfryzacja dóbr chronionych prawem własności intelektualnej tworzy problemy nieznane w tradycyjnych systemach. Brak możliwości technicznych łatwego kopiowania treści umożliwiał uproszczenia ochrony praw autorskich przez faktyczne uczynienie z fizycznego egzemplarza dzieła i związanych z nim praw jednego przedmiotu obrotu.[478] Łatwo więc zauważyć, że granice przedmiotowe ochrony prawa własności intelektualnej wyznaczane są przez możliwości techniczne. Konsekwencją takiego stanu rzeczy jest jednak rozmycie kompetencji ustawodawcy.[479] O ile bowiem ustawa może wyznaczać granice generalno-abstrakcyjne, ich konkretyzacja w istocie należy do autorów kodu. Obydwa te działania są niemożliwe do osiągnięcia w sposób bezpośredni - tworzenie kodu pozostaje poza zakresem normowania jurysdykcją preskrypcyjną, natomiast stanowienie norm nie leży w kompetencjach twórców kodu. W istocie działania twórców kodu stają się *sui generis* przepisami wykonawczymi, gdyż działają oni na podstawie ustaw, ale końcowy użytkownik będzie poddany właśnie regulacjom kodu, nie zaś ustawy. Opisana tu korelacja będzie widoczna we wszystkich aspektach prawa cyberprzestrzeni, także w prawie konfliktów zbrojnych i innych, regulujących naruszenia suwerenności.

7. c. 3. Metanormy

Normy prawa stanowionego, mające swoje znaczenie w cyberprzestrzeni faktycznie

---

[477] zob. Stefik M. *Letting Loose the Light:Igniting Commerce in Electronic Publication* [w: *Internet Dreams: Archetypes, Myths and Metaphors* 219] (1996), tenże *Shifting the Possible: How trusted systems and Digital Property Challenge Us to Rethink Digital Publishing* Berkley Technical Law Journal 12 (1997) s.137

[478] por. Negroponte N. *Being Digital* wyd. A.Knopf Nowy Jork (1995)

[479] Lessig nazywa to zjawisko prywatyzacją prawa (*privatized law*).

mają podwójną dyspozycję; odnoszącą się do świata rzeczywistego jak i tą, która tworzy następczo afordancję. Istnieje jednak pewien rodzaj norm stanowiący szczególną odmianę norm prawa cyberprzestrzeni. Chodzi tu o metanormy. Obojętnie czy pierwotnie należą one do *lex informatica* czy do prawa stanowionego, nie tylko wzajemnie na siebie oddziałują w opisanym powyżej ujęciu podwójnej dyspozycji (co jest regułą w przypadku tych systemów), ale także bezpośrednio normują siebie nawzajem, poprzez pozostawanie nawzajem także w zakresach swoich hipotez. W tradycyjnym systemie prawa taka zasada działania jest często spotykana. Najprostszym przykładem są przepisy wskazujące przedmiotowy zakres normowania danego aktu prawnego. Należą do tego aktu jednocześnie go normując, w istocie więc normują między innymi same siebie. W przypadku cyberprzestrzeni, jak wskazano powyżej, każda norma ma podwójny skutek, ma bowiem odbicie w równoległym systemie. Metanormy stają się więc podstawom źródłem formalnoprawnym obydwu systemów.[480] Jednak podobnie jak we wszystkich pozostałych przypadkach, oddziaływanie na system z którego nie pochodzą odbywa się pośrednio.[481] Przykładem metanormy prawa cyberprzestrzeni może być wewnętrzna regulacja państwa, na którego terytorium znajduje się istotna dla funkcjonowania całej cyberprzestrzeni infrastruktura. Norma ta dotyczyłaby możliwości legalnego ograniczania dostępu do sieci opartej o infrastrukturę znajdującą się na terytorium tego państwa. Norma taka nie będzie *per se* wpływać na funkcjonowanie cyberprzestrzeni, ale utworzy ramy prawne dla takiego wpływu. Jednocześnie będzie tworzyć regulację ramową dla zmienionej pod jej wpływem architektury systemu, na przykład poprzez przygotowanie kopii przedmiotowego serwera znajdującej się poza jurysdykcją tego państwa. Przywoływanym w doktrynie przykładem metanorm są często normy określające stopień tolerancji dla naruszeń danego systemu

[480] Część doktryny wskazuje, nawet że system będzie miał jeszcze więcej źródeł, przykładowo Lessig dodaje jeszcze normy rozproszone. Dla jasności wywodu, pominięte zostaną wszystkie pozaprawne źródła normowania.

[481] zob. także Lessig L. *The Limits in Open Code : Regulatory Standards and the Future of the Net,* 14 Berkeley Tech Law Journal (1999) s. 759. Autor wyróżnia tam, w ramach architektury systemów, dwa rodzaje kodu zamknięty i otwarty. Kod zamknięty jest w praktyce nie do usunięcia dla użytkownika końcowego. Kod otwarty pozwala na dowolne modyfikacje. W odniesieniu do normowania należałoby wskazać analogię z normami odpowiednio *ius cogens* i *dispositivum*.

normatywnego.[482] Norma taka będzie jednocześnie tworzyć określone afordancje dotyczące regulacji ruchu w terytorialnej strefie informatycznej części cyberprzestrzeni jak i w ramach tradycyjnego prawa tworzyć normy określające polityki sekurytyzacyjne danego państwa (kwestia sekurytyzacji zostanie szczegółowo omówiona w dalszej części wywodu). Oczywiście normy te będą na siebie wzajemnie wpływać. Ponieważ afordancje mogą działać wyłącznie w jeden określony sposób - rozmaite normowania tego samego zakresu przy pomocy norm będą prowadzić do kolejnego, tym razem nierozwiązywalnego, konfliktu jurysdykcyjnego.[483] Brak możliwości rozwiązania tego konfliktu wynika z oparcia metanorm o afordancje i podwójny ich skutek (zarówno wobec prawa międzynarodowego jak i wobec *lex informatica*). Ze względu na brak możliwości normowania tych pierwszych bezpośrednio- nie ma możliwości wypracowania mechanizmu określającego reguły kolizyjne. Podwójny skutek tych norm wpływa natomiast na możliwość wpływania za pomocą afordancji wytwarzanych przez metanormy na jurysdykcje trzecie.

7. d. Podsumowanie

Cyberprzestrzeń jest normowana przez *lex informatica* - skomplikowany system prawny, łączący tradycyjne prawo międzynarodowe, prawodawstwa krajowe, zwyczaj (rozumiany jednak inaczej niż przez tradycyjne prawo międzynarodowe) i technologię. Normy *lex informatica* stają się prawem po spełnieniu kryteriów Fullera (prawnie) i inkorporacją do architektury cyberprzestrzeni (faktycznie). Ponieważ jednak kryteria jasności i promulgacji, które w ujęciu Fullerowskim pełnią niezwykle istotną rolę - podlegają w *lex informatica* istotnym redefinicjom, mamy więc do w przypadku cyberprzestrzeni do czynienia ze swoistą fuzją wspomnianych kryteriów

[482] zob. Axelrod R. *An Evolutionary Approach to Norms* American Political Science Review 80 (1986) ss.1095-111

[483] Nazywanego w doktrynie 'kakofonią jurysdykcyjną' zob. Też *Hollis D.* Cacophony or Concert? Minor notes on Metanorms in Cyberspace, Prezi.com (2014) ss.1-7

Fullera z zasadą *żywego prawa (lebendes Recht)* sformułowaną przez Ehrlicha.[484] Ten ostatni wskazywał bowiem podobny do normowania faktycznego mechanizm w tradycyjnie ujmowanym prawie dowodząc, że żaden system prawny nie jest w pełni odporny na oddziaływanie ze strony społeczności, której postępowanie ma normować.[485] Istnieje jednak podstawowa różnica między koncepcją Ehrlicha a sytuacją istniejącą w cyberprzestrzeni. Chodzi mianowicie o fakt, że *żywe prawo* jest suwerenne uwzględnianie wpływu norm rozproszonych nań jest wyłącznie środkiem technicznym, mającym zwiększyć jego skuteczność i wpłynąć na jego dobrowolne przestrzeganie. Normowanie faktyczne w cyberprzestrzeni natomiast normuje bezpośrednio i nie istnieje żadna możliwość by go nie uwzględnić (tak jak ma to miejsce w *żywym prawie*). Funkcją tych dwóch aspektów *lex informatica* - jest normowania faktyczne, przy pomocy afordancji będących w istocie tym normami w systemie, który uwzględnia także istnienie technologii. Ze względu jednak na oparcia *lex informatica* na afordancjach, jego bezpośrednie normowanie nie jest wykonalne. Zmniejsza to oczywiście rolę jurysdykcji preskryptywnej i powoduje, że wpływ na normowanie cyberprzestrzeni zyskują także podmioty niepaństwowe jak *non-state actors* czy podmioty prawa prywatnego jak *ICANN*. Proces ten skutkuje postępującą redefinicją suwerenności ponieważ państwa muszą sięgać po zupełnie inne środki w celu jej ochrony. Dodatkowo, uznanie cyberprzestrzeni za *commons* wyłącza wiele elementów cyberprzestrzeni - jednocześnie implikując konieczność stosowania afordancji do stworzenia granic funkcjonalnych, wyróżniających "terytorialne" strefy informatycznej części cyberprzestrzeni z jej 'nieterytorialnej' części (stanowiącej *res communis omnium*).

[484] zob. Ehrlich E. *Grundlegung der Soziologie der Recht* Dunker & Humblodt Verlag (1913) ss.2-5

[485] por.Nelken D. *Eugen Ehrlich, Living Law, and Plural Legalities* Theoretical Inquiries in Law 9.2/2008 (2008) s. 443

III. Cyberprzestrzenne zagrożenia dla suwerenności

1. Suwerenność

Podstawowym i centralnym dla przedstawionych tu rozważań pojęciem jest suwerenność państwa. Suwerenność ma też kluczowe znaczenie dla prawa międzynarodowego publicznego, ponieważ to właśnie suwerenne państwa uczestniczą w obrocie tego prawa. Istnieje wiele koncepcji suwerenności, jednak wszystkie one w gruncie rzeczy różnią się wyłącznie sposobem technicznego osiągnięcia tego samego skutku. Nie ma bowiem sporu, że suwerenność to zwierzchność określonego państwa nad określonym terytorium.[486] Koncepcja ta ugruntowała się w porządku westfalskim prawa międzynarodowego.[487] Wobec tego, w klasycznej, pozytywistycznej interpretacji[488], to z suwerenności właśnie wypływa całe prawo międzynarodowe, w gruncie rzeczy rozumiane jako umowa suwerennych podmiotów, analogiczna do umowy w prawie cywilnym.[489] John Austin wyciągnął z tego założenia wniosek, że prawo międzynarodowe w istocie nie jest prawem, tak jak nie jest prawem zbiór umów w funkcjonujących w obrocie cywilnym czy też statut spółki, chociaż zarówno umowy jak i statuty są źródłem praw i obowiązków. O ile taka koncepcja prawa międzynarodowego wydaje się jednak iść zbyt daleko, jasno wskazuje ona na prymat suwerenności państwowej i jej niezwykle istotną rolę w kształtowaniu stosunków międzynarodowych.[490] Często przywoływanym przykładem takiej roli jest fakt, iż agendy międzynarodowe (takie jak Rada

[486] zob. Besson S. *Sovereignty* [w: Max Planck Encyclopaedia of International Law], Max Planck Stiftung (2011)

[487] Nazywanego tak od kończącego wojnę trzydziestoletnią pokoju w Westfalii w 1648 roku. Postanowienia pokojowe przenosiły akcent wykonywania suwerenności na państwa narodowe, likwidując istniejącą w Średniowieczu sieć powiązań międzynarodowych. zob.Hayman P.A., Williams J. *Westpahalian Sovereignty:Rights, Intervention,Meaning and Context* Global Society (2011) ss.521-3

[488] zob Janis M.W. *Jeremy Bentham and the Fashioning of 'International Law'* 78 American Jorunal of International Law 405.(1984)

[489] Austin J. *The Province of Jurisprudence Determined* (1832) cyt. za reprintem z 1998 roku, Hackett Publishing s.201

[490] zob. James A. *Sovereign Statehood. The Basis of International Society*, Allen and Uwin (1986) ss.39-40

Bezpieczeństwa ONZ) uzyskują prawo do bezpośredniej ingerencji w *domaine réservé* państw (na przykład poprzez uzyskanie prawa do ingerencji już nie tylko w konflikty międzynarodowe ale także w niemiędzynarodowe).[491] Ta rola jednak uległa redefinicji w miarę przenoszenia coraz szerszych kompetencji państwowych na organizacje międynarodowe i ponadnarodowe.[492] Porządek taki doktryna określa jako post-westfalski, przewidując w nim rolę państw jako partycypantów procesu decyzyjnego, a więc tworząc sytuację, w której suwerenność staje się *sui generis* prawem głosu.[493] Wydaje się jednak, że kierunek ten został zatrzymany i państwa nie są skłonne wyrzec się swojej suwerenności w całości.[494] Niewątpliwie natomiast trwałym skutkiem post-westfalskiego przełomu w suwerenności jest przyjęcie zasady równości państw, wynikającej właśnie z powstania owych ciał ponadnarodowych. Umożliwiając one wyrównanie potencjałów dawniej definiujących pozycję międzynarodową danego państwa.[495]

1. a. Koncepcje suwerenności we współczesnym prawie międzynarodowym.

Podstawową osią sporu o funkcjonowanie suwerenności w dzisiejszym prawie międzynarodowym, jest spór pomiędzy jej pozytywistycznym traktowaniem jako normy przedprawnej[496] a współczesnym nurtem traktującym suwerenność jako jeden z wielu atrybutów państwowości, coraz bardziej poddanych normom prawa międzynarodowego, w tym jego normom przedprawnym i coraz szerszemu

[491] tak na przykład profesor Elżbieta Karska [w: zbiorowa, red. Karska E. *Wpływ Europejskiej Konwencji Praw Człowieka na systemy ochrony praw człowieka oraz międzynarodowe prawo karne i humanitarne*. Uniwersytet Kardynała Stefana Wyszyńskiego (2013) s.13]

[492] Powszechnym poglądem doktryny jest, że przekazywanie kompetencji na organizacje ponadnarodowe nie stanowi rezygnacji z suwerenności rozumianej jako niezależność państwa, analogicznie jak związanie się umową nie oznacza utraty wolności a przeciwnie - stanowi jej przejaw. zob. Kranz J. *Suwerenność państwa i prawo międzynarodowe* [w: zbiorowa, red. Wołpiuk W.J. *Spór o suwerenność*, Wydawnictwo Sejmowe (2001) s. 108]

[493] zob.Cox R.W.*Approaches to World Order,* Cambridge University Press(1989) s.251

[494] zob.Jennings R. *Sovereignty and International Law* [w: zbiorowa, red.Kreijen G., Brus M., Duursma J., De Vos E.,Dugard J. *State, Sovereignty and International Governance* (2002) Oxford Scholarship (2002)]

[495] zob. Philpott D. *Revolutions in Sovereignty: How Ideas shaped Modern International Relations*,Princeton University Press (2001)

[496] zob. Ehrlich L. *Prawo międzynarodowe*, Wydawnictwo Prawnicze, wyd.4 (1958) ss.123-4

katalogowi norm obowiązujących *erga omnes*.[497] Praktyka międzynarodowa wydaje się, wraz z przechodzeniem od porządku westfalskiego do post-westfalskiego, coraz bardziej przychylać się do drugiej ze wspomnianych koncepcji.

Niemniej większość podstawowych elementów suwerenności jest wspólna dla wszystkich tych ujęć. Przede wszystkim można tu zaliczyć sprawowanie władzy najwyższej na danym terytorium[498] i prawo do uczestniczenia w obrocie prawnym wśród innych suwerennych i równych podmiotów.[499] Pomimo zachwiania równowagi podmiotów prawa międzynarodowego nigdzie nie jest kwestionowana zasada równości samych państw. Chociaż bezwzględnie wiążąca zasada, głosząca tę równość została sformułowana stosunkowo niedawno,[500] bo niewiele ponad wiek wcześniej, wrosła bardzo szybko we współczesne stosunki międzynarodowe i stała się jedną z fundamentalnych zasad funkcjonowania tych stosunków, nie podlegającą dyskusjom we współczesnej doktrynie prawa międzynarodowego. W dalszej części rozważań przyjęto więc brzmienie zasady regulującej równości wszystkich suwerennych państw[501], w kształcie nadanym im przez Kartę Narodów Zjednoczonych.[502] Należy zauważyć, że norma ta sama w sobie potwierdza istotność zasady suwerenności w obrocie międzynarodowym.[503] Jednakże ta sama Karta znacząco ogranicza na suwerenność wewnętrzną[504] wprowadzając tzw. Klauzulę

---

[497] zob. Worster W.Th. *Law, Politics and the Conception of the State in State Recognition Theory*, Boston University International Law Journal 27:115 (2009) ss. 116-20

[498] zob. Aron R. *Peace and War. A Theory of International Relations*, Praeger (1967) s.739

[499] Ten aspekt suwerenności wydaje się tracić na znaczeniu wobec rozwoju licznych i decydujących o coraz szerszym zakresie organizacji ponadnarodowych. zob.też Brand R.A. *External Sovereignty and International Law* Fordham International Law Journal 18:5 (1995) ss.1695-6

[500] por. Armstrong S.W. *The doctrine of Equality of Nations in the International Law and the relation of the doctrine to the Treaty of Versailles* American Journal of International Law nr. 4 tom 14 (październik 1920) s. 540-64

[501] Ansong A. *The Concept of Sovereign Equality of the States in International Law*,GIMPA Law Review 2-1 (2016) ss.14-34

[502] por. Art. 2 (1) Karty Narodów Zjednoczonych

[503] ibid. Karta wskazuje bowiem, że podstawą funkcjonowania Narodów Zjednoczonych jest ”suwerenna równość”. zob także Makinda S.M. *The United Nations and State Sovereignty: Mechanism for Managing International Security*, Australian Journal of Political Science 33 (1998) ss.105-110

[504] A więc suwerenności dotyczącej niezakłóconego wykonywania jurysdykcji na własnym terytorium. zob.Besson S. *Sovereignty* [w: *MPEPIL*...par.26]

Supremacyjną.[505] Zakłada ona, że w razie konfliktu obowiązków wynikających z Karty ze zobowiązaniami wynikłymi z innego źródła - decydujące są normy wynikające z Karty.[506] Część komentatorów Karty uznała wręcz, że art. 103 w związku z art. 2(6) Karty[507], nadają jej charakter *stricte* konstytucyjny (dla społeczności międzynarodowej).[508] Stanowisko to ciągle jednak nie wydaje się być uznawane za znaczące. Należy też przypomnieć, że w orzecznictwie Międzynarodowego Trybunału Sprawiedliwości, normy KNZ są uznawane za normy mające charakter norm *erga omnes*.[509] Nie jest jasne jak precyzyjnie interpretować owo określenie (ponieważ niewątpliwie nie oznacza ono, że wszystkie normy Karty mają charakter e*rga omnes*), niemniej łatwo zauważyć, że Trybunał podkreśla szczególną rolę zarówno Karty jak i praktyki ONZ. Kolejnym elementem suwerenności jest wiązanie się faktu jej istnienia z prawami tradycyjnie przypisywanymi państwom jak prawo legacji i przyjmowania poselstw, zawierania umów, etc.[510] O ile materialnie kwestie te pozostają poza zakresem niniejszego opracowania, ich formalny status jest niezmiernie istotny. Z kwestią owych praw, a szczególnie z obowiązkami po stronie państw trzecich , pozostającymi ich korelatami, wiąże się bowiem podstawowy spór o definicję suwerenności, kluczowy dla jej pojmowania w cyberprzestrzeni. Chodzi tu mianowicie o kwestię tego, czy suwerenność ma charakter konstytutywny czy deklaratoryjny.[511] Znaczenie tego

---

[505] zob. Art. 103 Karty Narodów Zjednoczonych.

[506] zob.Liivoja R. *The scope of the Supremacy Clause of The United Nations*, International and Comparative Law Quaterly 578 (2016) ss.587-92

[507] Nakazującym ONZ zapewnić nawet wobec państw nie będących członkami ONZ wykonywanie zapisów Karty, o ile jest to niezbędne do utrzymania ładu światowego i pokoju.

[508] zob. Fassbender B. *The United Nations Charter as Constitution of International Community*, Columbia Journal of Transnational Law 36 (1997) s.594

[509] Pogląd taki wyraził Międzynarodowy Trybunał Sprawiedliwości, uznając źródło zasady prawnej w Karcie Narodów Zjednoczonych za przesłankę obowiązywania tej zasady jako "mającej charakter normy *erga omnes*", przypisując zasadzie samostanowienia narodów taką rangę wyłącznie na podstawie zawarcia je w KNZ. Trybunał wskazał, że *[that self-determination] as it evolved from the Charter of the United Nations and from United Nations Practice, has an erga omnes character, is irreproachable*-[*skoro zasada samostanowienia narodów] wyewoluowała z Karty Narodów Zjednoczonych i ich praktyki, przypisanie jej charakteru erga omnes jest bezdyskusyjne*[w: *Case Concerning East Timor* (*Portugalia v. Australia),* orzeczenie z dnia 30 czerwca 1995, ICJ Reports 1995 par. 29]

[510] por. Fowler M.R., Bunck J.M. *What constitues the sovereign state*, Review of International Studies 22-4 Camridge University Press (1996) ss.381-404

[511] Worster William *Sovereignty Theories of State Recognition*, artykuł publikowany w

zagadnienia dla prawa cyberprzestrzeni. wynika z faktu, że choć dla tradycyjnie pojmowanych stosunków międzynarodowych kwestia ta wydaje się mieć znaczenie techniczne, jej rozstrzygnięcie będzie determinować wszelkie próby definiowania cybersuwerenności. Teoria konstytutywna, uważana obecnie za słabszą, ale zyskująca coraz szersze poparcie, [512] zakłada, że to tylko i wyłącznie uznanie decyduje o istnieniu państwa.[513] Hersch Lauterpacht przyjmuje nawet koncepcję, że powstanie nowego państwa jest swoistym oświadczeniem woli państw już istniejących.[514] Na gruncie tej teorii powstaje kilka istotnych pytań. Na przykład; czy konieczne jest wyznaczenie zakresu dyskrecjonalności państw w uznaniu nowych?[515] Czy możliwe jest wskazanie momentu, w którym uznanie jest możliwe lub wręcz konieczne, a także przesłanek takiej konieczności? Ze względu na brak wiążących *erga omnes* kryteriów państwowości,[516] brak jasności co do momentu, kiedy spełniona byłaby przesłanka, w którym momencie należałoby podejmować test wspomnianej dyskrecjonalności, lub w którym momencie miałby powstawać ów ewentualny obowiązek uznania. Powstaje jednakże pytanie: jak istnienie hipotetycznego obowiązku uznania pogodzić z niekwestionowaną nigdy praktyką częściowego uznania państw?[517] Można bowiem wskazać wiele przypadków państw, które zostały uznane przez tylko jedną grupę państw. W żadnym takim przypadku nie nastąpiło kwestionowanie legalności owego uznania (lub też odmowy uznania) tylko i wyłącznie na podstawie decyzji państw, które zachowały się inaczej. Trudno też kwestionować, że uznanie państwa jest częstokroć elementem polityki międzynarodowej, a racje państw, które decydują się na przyjęcie określonej postawy wobec aspiracji nowego państwa częstokroć są oparte o przesłanki polityczne właśnie,

---

Exploring Geopolitics wyd. I/2015.

[512] zob. Np. Oppenheim Lassa *International Law* (Lauterpacht edition) par. 71 s. 125 wyd. 8 1995 Longmans, Green and Co.

[514] Lauterpacht Hersch *Recognition of States in International Law*, 53 Yale Legal Journal 385(1944) s.419.

[515] Worster William *Law, Politics, and the Conception of the State in State Recognition Theory* Boston University Law Journal wyd. 27:115 (1990) s.116

[516] Nie jest możliwe przyjęcie Konwencji z Motenvideo jako powszechnie wiążącej. por. Grant Thomas *Defining Statehood: The Montevieo Convention and its discontents*. Columbia Journal of Transitional Law 37:403 (2003) str. 434

[517] zob. Geldenhuys D. *Origins of Contested Statehood* [w: Contested States in World Politics] Palgrave Macmillan(2009] s. 2

nie zaś czysto prawne. Nie jest także jasne, jak szerokie musiałoby być uznanie, by gwarantować podmiotowi status państwa. Najczęściej wskazuje się na konieczność uznania przez co najmniej jedno państwo.[518] Wydaje się jednak, że istnienia samego pojęcia państwa częściowo uznanego (a więc państwa uznawanego przez jedne a nieuznawanego przez inne kraje) jest nie do pogodzenia z tym progiem.

Koncepcja deklaratoryjna[519] zakłada natomiast, że państwo staje się nim w momencie spełnienia określonego zespołu przesłanek. Interpretowana więc ściśle koncepcja deklaratoryjna pozwala na uznanie państwa nawet nie istniejącego fizycznie.[520] Uznanie innych państw jest według tej koncepcji wyłącznie przyjęciem pod wiadomości powstania nowego podmiotu prawa międzynarodowego i samo w sobie jest pozbawione znaczenia. Istotną wadą tej koncepcji jest brak jasności co do kształtu przesłanek państwowości.[521] Koncepcja deklaratoryjna wydaje się jednak (w przeciwieństwie do konstytutywnej) dawać pewną odpowiedź na pytanie o moment powstania państwowości. Przyjmuje się, że skoro istnienie państwa ma być inferowane z faktu podjęcia przezeń swoich funkcji, to wystarczy wskazać moment, w którym państwo to wykonuje własną suwerenność, by uznać je za państwo właśnie.[522] Dla komplementarności wywodu należy wskazać, że dochodziło też do prób połączenia obydwu teorii (podejmował je na przykład Lauterpacht).[523] Wydają się one jednak z góry skazane na niepowodzenie ze względu na niewspółmożliwość obydwu teorii.

Dodatkową komplikację stanowi brak jednolitego sposobu uznania.[524] Nie istnieje bowiem określona procedura, którą dane państwo musi przejść aby zostać uznane.

---

[518] zob. Hillier T. *Sourcebook* ss.201-2

[519] Worster W. *Law, Politics....* s . 119

[520] zob. art.art. 3 i 6 Konwencji z Montevideo. Także Worster W. Sovereignty Two Competing Theories of State Recognition Exploring Geopolitics 2/10 (2010) par.3

[521] Powszechnie przyjmowana jest Konwencja z Montevideo. Brak jednak jasnej normy lub prawa zwyczajowego w zakresie uznania kryteriów zawartych w tej konwencji za wiążące kryteria państwowości.

[522] Wynika to z uznania suwerenności za możliwość i prawo działania w braku innego prawa dane działanie regulującego. zob. Czaputowicz J. *Suwerenność*, Polski Instytut Spraw Międzynarodowych (2013) ss.51-2

[523] por. Lauterpacht H. *Recognition in International Law* (1947)

[524] zob. Daniluk M.*Problem uznania rządu w prawie międzynarodowym na przykładzie uznania libijskiej Narodowej Rady Tymczasowej*, Studia Iuridica Lublinensia 20, 2013 s 121

Oczywiście, można wskazywać, że przykładowo przyjęcie do Organizacji Narodów Zjednoczonych oznacza spełnienie warunku międzynarodowego uznania, ale błędne byłoby wskazywanie *a contrario*, że brak tego członkostwa oznacza także brak uznania międzynarodowego.[525] O ile bowiem nie sprawia problemów interpretacyjnych uznanie wyraźne, doktryna przyjmuje także możliwość uznania dorozumianego. Shaw dodatkowo wyróżnia kwestię uznania kolektywnego i jednostkowego.[526] O ile jednostkowe uznania przez poszczególne państwa nie wymagają wyjaśnienia, idea uznania kolektywnego polega na wydaniu wiążącego *erga omnes* (przy założeniu teorii konstytutywnej) oświadczenia woli, wiążącego dla całej społeczności międzynarodowej lub stwierdzenia spełnienia warunków uznania (dla teorii deklaratoryjnej) przez określoną instytucję międzynarodową, uznawaną za emanację[527] całej społeczności międzynarodowej. Do cyberprzestrzeni regulowanej przez afordancje i nienormowanej bezpośrednio będzie więc możliwa do zastosowania wyłącznie koncepcja deklaratoryjna. Będzie ona także pozwalała na analizę suwerenności cyberprzestrzennej w oparciu o przyznanie przymiotu suwerenności działaniom w razie braku innego prawa - w tym wypadku, będzie chodziło o *lex informatica* i suwerenność mającą swoje źródła w wykonywaniu normowania faktycznego. Suwerenność służy też do funkcjonalnego rozdzielenia systemów prawnych, wyznaczonych przez przywołane powyżej granice funkcjonalne. Jak słusznie wskazuje się w doktrynie - suwerenność jest pojęciem binarnym, państwo o ograniczonej suwerenności to tyle co państwo niesuwerenne. Przeważająca część doktryny uznaje, że ograniczenie suwerenności ze względu na prawo międzynarodowe - nie może być uznanie za jej naruszenie (a tym samym likwidację), a raczej stanowi uzasadnienie celu istnienia suwerenności.[528] Nie brak jednak głosów

---

[525] por. Lloyd D.O. *Sucession, Secession and State Membership in the United Nations,* New York University Journal of International Law and Politics 761(1993)

[526] Shaw Malcolm *International Law* Cambrigde University Press wyd. 6 s. 465

[527] Shaw w swojej książce podaje przykłady Organizacji Narodów Zjednoczonych i Ligi Narodów.

[528] Wynika to z zasady wynikłej z *case-law* Stałego Trybunału Arbitrażowego. zob. *Island of Palmas Case* (Holandia v. USA) STSM, 2 AIAA 829 (1928), UN Reports of International Arbitral Awards (2006) ss.839-40, także Bennoune K. *'Sovereignty vs. Suffering'? Re-examining Sovereignty and Human Rights through Lens of Iraq* 13 European Journal of International Law (2002)ss.245-60

przeciwnych, wskazujących, że niektóre elementy prawa międzynarodowego (takie jak wykonywane ponadnarodowo prawa człowieka), wzrost znaczenia organizacji ponadnarodowych i wzrost znaczenia aktorów niepaństwowych suwerenność redefiniują albo wręcz likwidują.[529] Poglądy te oparte są na założeniu, że o ile państwa tracą możliwość konstruowania owych granic funkcjonalnych - ich suwerenność traci swoją treść i w konsekwencji przestaje istnieć. Uwagi te w oczywisty sposób będą się także odnosić do cyberprzestrzeni, w której granice funkcjonalne, konstruowane przy pomocy *lex informatica*, stanowią podstawę ochrony suwerenności państwowej. Wobec wspomnianej konieczności redefinicji suwerenności i zmiany jej desygnatu, doktryna zaczęła wyróżniać trzy pola, na których jest ona wykonywana w zglobalizowanym świecie:[530] kontrolę (*control*), władzę (*authority*) i legitymację (*legitimacy*). Władza jest odbiciem tradycyjnego, prawnego pojmowania suwerenności i oznacza możliwość wykonywania niekwestionowanej władzy nad określonym terytorium. Kontrola dotyczy tej samej kwestii, jednak w ujęciu faktycznego jej wykonywania. Nie jest więc kategorią prawną a określonym stanem faktycznym. Legitymacja natomiast stanowi zasadność sprawowania zarówno władzy, jak i kontroli w sensie prawnym. Takie ujęcie suwerenności stanie się podstawą dla zrozumienia jej roli w cyberprzestrzeni, szczególnie w jej części stanowiącej *res communis omnium.*[531] Ma ono swoje źródło oczywiście w nieprzystawalności porządku westfalskiego do świata, w którym państwa coraz częściej podlegają wpływom zewnętrznym,[532] który według części doktryny prowadzi do uznania suwerenności za kwestię nie tylko ponadterytorialną ale też ponadpaństwową.[533] Oznacza to, że państwa są zmuszone do określania własnej polityki (a więc wykonywania wspomnianych wcześniej ‘kontroli’ i ‘władzy’)

---

[529] zob. Schreuer Ch. *The Waning of the Sovereign State: Towards a New Paradigm for International Law?* European Journal of International Law 4 (1993) ss. 450-61

[530] zob. Litfin K.T. *Sovereginty in World Ecopolitics*, Mershon International Studies Review 41 (1997) ss.169 i n.

[531] zob. Rossi Ch. R. *Conclusions on the Future of the Global Commons* [w:zbiorowa, red. Rossi Ch.R. *Sovereignty and Territorial Tempation: The Grotian Tendency,* Cambridge Univeristy Press (2017) ss.285-92]

[532] zob. Strange S. *The Westfailure System* [w:zbiorowa red. Cox M. *20th Century International Relations* SAGE, (2007) s.249]

[533] zob. Czaputowicz J. *Suwerenność* ...s.315

w sposób zakładający istnienie pozostałych podmiotów prawa międzynarodowego (a więc organizacji ponadnarodowych i pozostałych państw, przynajmniej w takim zakresie, w jakim mają one wpływ na te organizacje). Bez zmian natomiast pozostaje aspekt 'legitymacji' przyznawanej niezależnie od ujęć suwerenności - wyłącznie państwom.

1. b. Suwerenność w cyberprzestrzeni

Konstrukcja cyberprzestrzeni z punktu widzenia suwerenności jest niezwykle skomplikowana. Infrastruktura stanowiąca podstawę części fizycznej jest zlokalizowana terytorialnie. Część informatyczna dzieli się na *commons* i wyznaczane granicami funkcjonalnymi strefy terytorialne. Jednak zgodnie z definicją cyberprzestrzeni, należy ją postrzegać jako całość. Próba określenia sposobu wykonywania suwerenności państwowej w stosunku do niej musi oczywiście obejmować wszystkie te trzy elementy. Największą komplikację dla wykonywania suwerenności stanowi fakt, że co do zasady całościowo pojmowana cyberprzestrzeń uznawana jest *res communis omnium*. Implikuje to liczne ograniczenia w zakresie suwerenności państw w niej uczestniczących.[534] W istocie, państwa będą musiały ograniczyć się w tym zakresie do suwerenności pojmowanej negatywnie - jako przeciwdziałanie naruszeniom. Za element własnej suwerenności będą natomiast mogły one uznać wykonywanie własnych norm faktycznych w odniesieniu do części fizycznej i stref terytorialnych. Dodatkową komplikacją jest wyjęcie danych spod jurysdykcji państwowej, a zatem uniemożliwienie wykonywania suwerenności bezpośrednio w stosunku do nich. Odnosząc zatem do cyberprzestrzeni poprzednio przywołany funkcjonalny podział suwerenności, łatwo zauważyć, że wpływa ona przede wszystkim na legitymację państw do wykonywania suwerenności. Wobec oparcia prawa cyberprzestrzeni na *lex informatica* i normowaniu faktycznym, państwa tracą monopol na jej wykonywanie. Natomiast atrybuty władzy i kontroli podlegają

[534] zob. Clancy E.A. *The tragedy of Global Commons*, Indiana Journal of Global Legal Studies, 5:2 (1998) ss.682-5

redefinicji zgodnie z opisanym powyżej mechanizmem. Państwa wykonują kontrolę w informatycznej części cyberprzestrzeni w takim stopniu, w jakim umożliwia im to ich wpływ na normowanie faktyczne natomiast wobec części fizycznej zachowują one takie stopień kontroli jaki wynika z ich jurysdykcji zwyczajnej.

Nie ma wątpliwości, że głównym aspektem działań państw w cyberprzestrzeni jest przeciwdziałanie naruszeniom własnych interesów, które byłyby naruszane zarówno w obrębie samej cyberprzestrzeni, jak w świecie rzeczywistym (choć poprzez cyberprzestrzeń dokonanych).[535] Musi więc istnieć zasada ich rozgraniczenia.[536] Chodzi tu o konstrukcje granic funkcjonalnych, spełniających jednak możliwość ochrony suwerenności rozumianej jako wolność od wpływów. Granice takie muszą być konstruowane technicznie i przede wszystkim uniemożliwiać dostęp do stref terytorialnych informatycznej części cyberprzestrzeni jak i do elementów jej części fizycznej. Wydaje się, że istnieją dwie takie zasady. Po pierwsze, państwa mogą wykonywać lokalizacje pakietów danych i odnosić te lokalizacje do geografii politycznej świata rzeczywistego.[537] Pakiety te w systemie opartym o numery IP mogą być więc precyzyjnie lokalizowane.[538] Z tej technicznej możliwości wynika zdolność systemów komputerowych do lokalizowania określonych użytkowników cyberprzestrzeni.[539] Umożliwia to z kolei wykonywanie prawa danego kraju wobec użytkowników cyberprzestrzeni, którzy operują w oparciu o dane wprowadzone do niej. Wobec tego państwa mogą nakładać na użytkowników cyberprzestrzeni wymóg dostosowania się do nakazów własnej jurysdykcji i w ten sposób chronić własną suwerenność, w oparciu o terytorium. Serwer rozpoznaje bowiem zarówno z jakiego terytorium łączy się dany użytkownik i może regulować w drodze normowania faktycznego jego zachowania, na przykład zakazując dokonania określonej transakcji

---

[535] zob. Schmitt M.N., Vihuul L. *Respect for Sovereignty in Cyberspace*, Texas Law Review 95 (2017) ss.1059 i n.

[536] zob. Tarjanne *Internet Governance: Towards Voluntary Mulilateralism,* Internet Domain Names: Informations Session, Meeting of Signatories and Potential Signatories of the Generic Top Level Domain Memorandum of Understanding (1997)

[537] zob. Valdar A. *Understanding Telecommunications Networks,* London Institute of Enigineering and Technology (2006) s.194

[538] por. Lipke D.J. *You Are Here:The race to bring Geography to the Borderless Web*, American Demographics (2001) s.65

[539] zob. Wu. T., GoldsmithJ. *Who Controls...* s.54

czy też pobrania określonej treści, o ile prawo kraju z którego połączenie pochodzi tego zabrania. Jednakże tak skonstruowana ‘granica’ cyfrowa dotyczy wyłącznie internetu (a więc wyłącznie jednej z warstw informatycznej części cyberprzestrzeni), a nawet tam może być łatwo przekroczona.[540] Jest ona więc wystarczająca dla prostych czynności, takich jak ograniczenia nakładane na sprzedaż koncesjonowanych wyrobów czy udostępnianie plików medialnych. Nie jest jednak w stanie ochronić suwerenności przed naruszeniami poważniejszymi. Ponadto, jej wykonywanie zależne jest od jurysdykcji, w której znajduje się serwer. Jeżeli bowiem usługa zakazana w jednym państwie, będzie oferowana z serwerów znajdującej się w innej lub wręcz “sztucznej” jurysdykcji,[541] przez podmiot który nie będzie przestrzegał zakazów lokalizacyjnych lub wręcz pozwalał na łamanie ich przy pomocy narzędzi spoofingowych[542], w efekcie nie będzie możliwości zakazania w określonej jurysdykcji danego zachowania. Dodatkowo, państwo będzie mogło ścigać wyłącznie własnych obywateli (jak miało to miejsce w przypadku sprawy *LICRA v. YAHOO!*), natomiast źródła udostępnienia pozostają poza zasięgiem jurysdykcji tego państwa, jako zlokalizowane na innym, suwerennym terytorium. Klasycznym przykładem takich serwerów, opisywanym w doktrynie, są serwery umożliwiające hazard on-line[543], omijając przepisy jurysdykcji krajowych i wykorzystując przykładowo konta typu pre-paid do dokonywania zakładów. Państwa oczywiście mają możliwość przeciwdziałania takiemu zachowaniu w drodze normowania faktycznego, konkretnie poprzez nakazywanie własnym (poddanym zwyczajnej jurysdykcji) dostawcom usług internetowych blokowania określonych połączeń (na przykład z serwerów znajdujących się w takiej jurysdykcji, lub powiązanych ze znanym serwerem naruszającym prawo krajowe).[544] Jak jednak wskazano powyżej,

---

[540] por. Hovanesian M.D. *Hackers and Pishers and Frauds,OhMy!*, Business Week 6/2005

[541] Jednym z najbardziej rozpoznawalnych przypadków takiej konstrukcji były serwery firmy *Havenco*, funkcjonujące w tzw. Księstwie Sealandii. Szerzej kwestia ta została omówiona w rodziale dotyczącym *cyberlawfare*.

[542] zob. Hovanesian *Hackers...*

[543] zob.na przykład Walters L.G. *Online Casino Risk. A safe bet or risky business?* Walters Law Group (2019)

[544] zob. Katsh M.E. *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace* University of Chicago Legal Forum 335(1996), także Wu T., *Cyberspace*

takie działania mogą być skuteczne wyłącznie w najprostszych sprawach, a nie przeciwko zaplanowanym naruszeniom suwerenności danego państwa. Te ostatnie bowiem z samego założenia obliczone są na obejście rutynowych zabezpieczeń cybernetycznych na samym początku operacji Ten typ suwerenności cyberprzestrzennej, ze względu na liczne ograniczenia techniczne jest więc bardzo niedoskonały. Za trafną należy więc uznać generalizację poglądów , dokonaną przez doktrynę amerykańską - *If the King's writ reaches as far as the King's sword then much of the content of the Internet might be perceived to be free from the regulations of any particular sovereign- Jeżeli więc prawo króla sięga tam dokąd sięga jego miecz, wiele elementów Internetu należy uznawać za niepodlegające regulacjom jakiegoś określonego suwerena*.[545] Koresponduje to z pojmowaniem suwerenności jako "wolności od wpływów innych"[546] Kluczowym problemem wydaje się tu swoiście pojmowana kwestia terytorium. Owe techniczne trudności z wykonywaniem suwerenności wiążą się właśnie z faktem, że państwa nie mogą wykonywać swojej jurysdykcji w stosunku do całego połączenia[547], które prowadzi do wykonania określonej czynności. Taka forma zachowywania suwerenności jest wykonalna w kwestiach, w których wystarczająca jest adekwatna, a nie absolutna szczelność ochrony prawnej określonego dobra. Jednakże w przypadkach, w których konieczna jest ochrona absolutna, a więc w przypadku dóbr prawnych decydujących o racji stanu, konieczne jest wykonywanie suwerenności według drugiej z wymienionych koncepcji. Zakłada ona tworzenie quasi-terytoriów cyfrowych *sensu stricto*, a więc terytoriów, które pomimo iż znajdują się w informatycznej części cyberprzestrzeni, stanowią przedłużenie terytorium państwa (tym samym pozostając wyłączone z *commons*). Koncepcja państwowych elementów *commons* (wyłączając przywołaną

Sovereignty? The Internet and the International System, Harvard Journal of Law and Technology 10:647 (1997) i Posner E.A., Lichtman D. Holding Internet Service Providers Accountable, John M. Olin Law & Economics Working Paper 217 (2004)ss.5-8

[545]zob. Boyle J. *Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors* University of Cincinnati Law Review 66 (1997)

[546] zob. Czaputowicz *Suwerenność*... s.53

[547] Z przyczyn technicznych kontrolę nad danym działaniem cyberprzestrzennym, można wykonywać w pełni wyłącznie kontrolując zarówno punkt wejścia jak i wyjścia, a więc pierwsze i ostatnie urządzenie części fizycznej, biorące udział w przesyle danych. zob. Choucri N. *Modeling cyberspace control worldwide*, MIT Industrial Liason Program

powyżej kwestię wód terytorialnych wydzielonych z morza otwartego), po raz pierwszy pojawiła się w doktrynie prawie międzynarodowego w zakresie dotyczącym przestrzeni kosmicznej.[548] Chodzi tu o tzw. Deklarację Bogotańską[549], traktat sygnowany przez państwa, których terytoria znajdują się na linii równika. Deklaracja przyjmowała, że odpowiadająca równikowi orbita geostacjonarna Ziemi, wraz z jej właściwościami (wynikłymi z grawitacji ziemskiej) nie należy do elementów kosmosu,[550]ale jest surowcem naturalnym podobnym do pierwiastków czy paliw. Niezależnie od zapisów prawa kosmicznego[551], które nie mają tu zastosowania, jest to element terytorium państw równikowych właśnie. Tym samym, państwa umawiające się przyznały sobie prawo do rozszerzenia własnej suwerenności poza atmosferę ziemską, powszechnie uznaną w doktrynie prawa kosmicznego za granicę jurysdykcji terytorialnej.[552] Deklaracja Bogotańska nigdy nie zyskała szerszego znaczenia, jednak argumentacja w niej zawarta w swoich podstawowych założeniach może być łatwo zastosowana do cyberprzestrzeni oraz jej fragmentów stanowiących 'bańki' elementów cyberprzestrzeni, będących bezpośrednio sui generis cyberterytorium państwa. Należałoby więc znaleźć swoisty odpowiednik zasady *cuius est solum, eius est usque ad coelum et ad inferos*[553], funkcjonujący w informatycznej części cyberprzestrzeni. Intuicyjnie mogłoby się wydawać, że tak będą określane te elementy informatycznej części cyberprzestrzeni, istniejące w niej w oparciu o elementy części fizycznej położnej na danym terytorium. To oczywiście warunek konieczny. Tylko wtedy w stosunku do owego „cyberterytorium" państwo będzie mogło wykonywać

---

[548] zob. Durrani H.A. *The Bogota Declaration: A case Study on Sovereignty, Empire and the Commons in Outer Space*. Columbia Journal of Transnational Law (2016)

[549] Deklaracja Pierwszego Szczytu Państw Równikowych, przyjęta 3 grudnia 1976 roku w Bogocie.

[550] por. St.John D.The Bogota Declaration and the Curious Case of Geostationary Orbit Denver Journal of International Law and Policy 1/13(2013) s.2

[551] Chodzi tu szczególnie o art. II Traktatu o Przestrzeni Kosmicznej zdnia 17 stycznia 1967 roku, sygnowanego przez Zjednoczone Królestwo, Stany Zjednoczone i Związek Sowiecki (obecnie sygnowany przez 108 państw) potwierdzający zasadę niezawłaszczalności kosmosu.

[552] zob. Neocleous M. *Police Power, all the way to heaven. Cujus est solum and the no-fly zone,* Radical Philopsophy 182 5:14 (2013) ss.6 i n.

[553] Zasada prawa rzymskiego, mówiąca że ten kto posiada ziemię (terytorium) posiada je od środka Ziemi do nieba. zob. *Harvard Legal Essays, Written in Honor of and Presented to John Henry Bale and Samuel Williston*, Ayer Company Publishers (1997) s.522

zarówno jurysdykcję zwyczajną w stosunku do jego części fizycznej jak i mogło będzie sprawować kontrolę nad częścią informatyczną. W taki właśnie sposób, w okresie kontrolowania *DNS* przez *IANA*, rząd Stanów Zjednoczonych powstrzymał kryzys po opisanym powyżej przekierowaniu ruchu w serwerach DNS przez Jona Postela. Nieautoryzowane zmiany w serwerach *IANA* uznane zostały za przestępstwo.[554] Oczywiście było to możliwe wyłącznie dzięki możliwości kontrolowania i wykonywania jurysdykcji zwyczajnej w stosunku do serwerów organizacji. Jednak samo spełnienie tej przesłanki nie jest wystarczające. Poza granicami USA pozostawały inne serwery należące do *IANA*, ze względu więc na wszechobecność cyberprzestrzeni nie można mówić o spełnieniu przesłanki ochrony własnych kluczowych danych (jak dostęp do serwerów rządowych za pomocą kopiowania połączeń DNS) już na tym etapie.[555] Konieczna jest dodatkowo ochrona własnych danych konstytuujących owe rządowe witryny (tu w rozumieniu nośników informacji czytelnych dla człowieka, stanowiących techniczne przekazy szeregów bitów pomiędzy urządzeniami działającymi w cyberprzestrzeni), a także ochrona fizycznej części cyberprzestrzeni, w oparciu o którą dane te funkcjonują. O ile pierwsza z przesłanek wskazanych powyżej konstytuuje cyfrowy odpowiednik miejsca, druga jest analogią obowiązku utrzymywania przez dane państwo zdolności do wykonywania jurysdykcji na obszarze, które uważa ono za element własnego, suwerennego terytorium.[556] Trzecią przesłanką, którą musi spełniać opisywane quasi terytorium musi być kryterium istotności informacji przechowywanych w owej terytorialnej przestrzeni dla racji stanu państwa, które deklaruje suwerenność nad tym wycinkiem cyberprzestrzeni. Pewien problem w powyższej konstrukcji stanowi fakt, że cyberprzestrzeń nie jest miejscem w fizycznym rozumieniu.[557] Wskazuje na to zarówno atrybut wszechobecności jak i niemożliwości fizycznego zlokalizowania.

---

[554] zob. Simon C. *The technical Construction of Globalism*Ł *Internet Governance and DNS Crisis*, rkey.com (2005) ss.1-3

[555] zob.Feld H.*Structured to Fail: ICANN and the 'Privatization' Experiment* [w:zbiorowa, red. Thierer A.D., Wayne C. *Who Rules the Net?:Internet Governance and Jurisdiction*, Cato Institute, Waszyngton (2003) s.345]

[556] zob. Na przykład Beale J.H. *The Jurisdiction of a Soveregin State*, Harvard Law Rebiew 36:6 (1923) ss.145 i n.

[557] por. Hunter D. *Cyberspace As Place, and the Tragedy of the Digital Anticommons* Calfornia Law Review (2002)

Wydaje się jednak, że nie oznacza to, że nie można przypisać jej pewnych cech terytorium państwowego.[558] Estonia, państwo od dawna koncentrujące się na budowaniu silnej obecności w cyberprzestrzeni, wprowadziła wprowadziła e-rezydencję. W ten sposób rząd estoński oferuje "prawo pobytu" w estońskiej cyberprzestrzeni każdemu kto złoży odpowiedni wniosek.[559] Około 500 osób ze 150 krajów otrzymało prawo takiej e-rezydencji[560]. Z konstrukcji tej wynikają doniosłe skutki dla prawa jurysdykcji w cyberprzestrzeni. Nie ma wątpliwości, że przyznawanie praw rezydencji i szerzej, wszystkie prawa związane z prawem pobytu muszą być uznane za wykonywanie jurysdykcji zwyczajnej. Tylko bowiem podmiot wykonujący jurysdykcję nad danym terytorium, może oferować określonym innym podmiotom zwolnienie z ograniczeń korzystania z tego terytorium. Specyfiką e-rezydencji w estońskim ustawodawstwie jest fakt rozdzielenia jej od prawa rezydencji fizycznej, pozwalającej na przebywanie na terytorium Estonii - a przez to na terenie UE. W jej dzisiejszym kształcie, e-rezydencja jest wyłącznie udostępnieniem pewnych funkcji estońskiego aparatu publicznego w wersji cyfrowej, umożliwiając (dodatkowo po weryfikacji przez estońskie służby) działania takie jak zdalne założenie spółki prawa estońskiego. Jednakże sam fakt istnienia takiej formy rezydencji, może być wstępem do stworzenia jurysdykcji nad suwerennym terytorium wyłącznie cyberprzestrzennym. E-rezydencja jest regulowana wyłącznie wewnętrznymi przepisami państwa estońskiego. Czysto teoretycznie rozszerzenie praw przyznawanych w takiej drodze nie jest w żaden sposób ograniczone (poza ograniczeniami wiążącymi rząd Estonii jako taki). W praktyce więc samo więc rozszerzenie zakresu tych praw i obowiązków oznacza, że Estonia wykonuje swoją suwerenność w określonym odcinku cyberprzestrzeni, a inne państwa milcząco uznają ten fakt. Łatwo też zauważyć, że e-rezydencja jest czymś diametralnie innym niż rozpowszechnione udostępnienie możliwości dokonywania czynności administracyjnych przez internet. Takie działanie jest wyłącznie zmianą sposobu

[558] zob. Lastowka G., Hunter D. *The Laws of the Virtual World*, California Law Review 92:1 (2004)

[559] Schmurer E.B. *E-stonia and the Future of the Cyberstate: virtual governments come online*. Snapshot 28 stycznia 2015

[560] Stan na lipiec 2018. por. www.e-resident.gov.ee

składania dokumentów. W opisywanym przypadku Estonia wykonuje swoją suwerenność w informatycznej części cyberprzestrzeni. Co istotne, rezydencja ta jest ograniczona do cyberprzestrzeni i poza nią niedostępna. Jej przyjęcie przez dany podmiot wywiera jednak skutki prawne w jurysdykcjach obcych. E-rezydencja pozwala uzyskać dostęp do rynku wewnętrznego Unii Europejskiej.[561] Podobnie, daje ona dostęp do przeprowadzania procesów administracyjnych w Estonii. Nie ma więc wątpliwości, że to państwo wykonuje własną suwerenność (choćby poprzez zezwalanie na działanie na własnym rynku określonym podmiotom gospodarczym) w cyberprzestrzeni.

.

2. Jurysdykcja zwyczajna i nadzwyczajna jako podstawowe narzędzia wykonywania suwerenności w cyberprzestrzeni

Podstawowym narzędziem (jak wykazano powyżej - zarówno pośrednio jak i bezpośrednio) ochrony suwerenności jest wykonywanie jurysdykcji. Dotyczy to zarówno części fizycznej jak i 'terytorialnych' fragmentów części informatycznej cyberprzestrzeni (normowanych co do zasady przez jurysdykcję zwyczajną) jak i części informatycznej stanowiącej *commons* (normowanej co do zasady przez jurysdykcję nadzwyczajną). Zgodnie z ogólną zasadą prawa międzynarodowego, jurysdykcja zwyczajna może być jednak wykonywana, o ile nie istnieje norma przeciwna.[562] Będą one więc miały zdecydowanie mniejszy wpływ na cyberprzestrzeń.

Prawo cyberprzestrzeni staje się więc gałęzią prawa międzynarodowego, w którym jurysdykcja zwyczajna i nadzwyczajna istnieją wspólnie - co oznacza dalsze oderwanie od zasady terytorialności. Całość tak wykonywanej suwerenności będzie bowiem wykonywana eksterytorialnie.[563] Ilustracją takiego mechanizmu może być

---

[561] zob. Heshmaty A. *E-Residency- how does it work?* LexisNexis PSL (2017) s.2

[562] zob. Phillipe X. *The principles of universal jurisdiction and complementarity: how do the two principles intermesh?,* International Review of the Red Cross 88:862 6/06(2006), s.389

[563] por.Colangelo A.J. *What is Extraterritorial Jurisdiction* 99 Cornell Law Review

ochrona danych przed naruszeniami poniżej użycia siły, wywołujących skutek na terytorium państwa. Państwo wykorzystujące cyberprzestrzeń do wsparcia wykonywania własnej suwerenności (w tym do realizacji własnych kluczowych dla suwerenności interesów) w świecie rzeczywistym, będzie musiało owe działania chronić we wszystkich trzech zakresach cyberprzestrzeni. Przykładowo, umożliwienie przez dane państwo swoim obywatelom oddawania głosów w wyborach przy użyciu Internetu- będzie wymagało od tego państwa ochrony swojej *domaine réservé* we wszystkich trzech zakresach. Po pierwsze, konieczne jest więc ochrona własnej infrastruktury terytorialnej (serwerów), wykonywana przy pomocy norm jurysdykcji zwyczajnej. Nadto, dane tak istotne dla interesów państwa, umieszczane są w domenach odgraniczonych od ruchu cyberprzestrzennego (a więc na przykład w domenie *.gov*). Spełniają więc wskazane powyżej przesłanki znajdowania się w strefie informatycznej części cyberprzestrzeni, którą państwo to uznaje za swoje cyfrowe ”terytorium”. Oczywiście, ewentualne naruszenie owych danych, musiałoby być wykonane z zewnątrz, a w konsekwencji ściganie sprawców lub podejmowanie środków przekraczających cybernetyczną obronę pasywną (stosowaną do ochrony ‘terytorialnej’ części cyberprzestrzeni) musiałoby się dokonać za pomocą jurysdykcji nadzwyczajnej. Skuteczna ochrona owych danych będzie więc wymagała skutecznego działania państwa we wszystkich trzech porządkach: za pomocą działań legislacyjnych - zapewniających bezpieczeństwo własnej infrastrukturze; za pomocą skutecznych decyzji sekurytyzacyjnych tworzących odpowiednie afordancje w ramach *lex informatica* i chroniących własne terytorium cyfrowe, a także za pomocą własnej jurysdykcji nadzwyczajnej wykonywanej w ramach tradycyjnego prawa międzynarodowego publicznego. Należy także dostrzec, że warunkiem skutecznej ochrony własnej suwerenności jest łączne spełnienie wszystkich tych warunków. Jednym wyjątkiem od tej zasady będzie wykonywanie przez państwo prawa samoobrony i użycie do niej środków kinetycznych lub mających skutek kinetyczny, dla których zastosowania może być wystarczające wykonywanie własnej, tradycyjnie pojmowanej, jurysdykcji w ramach prawa międzynarodowego

(6/2014)s.1303

publicznego. Wyjątek ten wynika z pełnej dopuszczalności odpowiedzi kinetycznej na atak cybernetyczny, który w świecie fizycznym miałby konsekwencje porównywalne z konsekwencjami ataku konwencjonalnego.[564] Skoro więc państwo może dokonać odpowiedzi w świecie rzeczywistym - może także skutecznie chronić własną suwerenność wyłącznie w drodze wykonania norm tradycyjnego prawa międzynarodowego (niekoniecznie chroniąc skutecznie własne interesy w ramach *lex informatica*). Taka sytuacja zostanie jednak szerzej omówiona w rozdziałach dotyczących konfliktów cyberprzestrzennych.

Należy także rozważyć w jaki sposób państwa mogą wykonywać swoją suwerenność w eksterytorialnej części cyberprzestrzeni za wyjątkiem jurysdykcji nadzwyczajnej. Pierwszą z koncepcji jest przeprowadzanie analogii z prawa morza.[565] Zakładała by ona przypisanie strefom ”terytorialnym” cyberprzestrzeni roli podobnej jaką mają okręty danego państwa, poddane prawu państwa bandery noszonej przez daną jednostkę i tym samym stanowiąc *sui generis* tegoż państwa suwerenne terytorium.[566] W oczywisty sposób wymagane byłoby więc wskazanie bezpośredniego naruszenia tego ostatniego co, jak już wskazano, jest nieomal niewykonalne z powodu problemów z dokonaniem atrybucji.

Drugą natomiast (i jak się wydaje praktycznie słuszniejszą) koncepcją jest koncepcja konsekwentnego stosowania do tychże stref prawa naturalnego, w oparciu o analogię do związku prawa cyberprzestrzeni z *lex informatica*.[567] Ponieważ fundamentalną rolę odgrywa tu zasada *ex aqueo et bono*, konsekwentne przyjmowanie tej zasady dawałoby państwom prawo do ochrony własnej suwerenności za pomocą środków proporcjonalnych i wynikających z *lex informatica*

---

[564] zob.Rundle A. *International Acceptance of Kinetic Operations in Response to a Cyber Attack* US Marine Corps Univeristy (2011) ss.11-4

[565]zob. Hildebrandt M. *Extraterritorial Jurisdiction to Enforce in Cyberspace? Codin, Schmitt, Grotius in Cyberspace*. University of Toronto Law Journal wyd. 63/2 (2013) Autorka proponuje analizę jurysdykcji nadzwyczajnej w oparciu nie tylko o współczesne prawo morza, ale cofnięcie się do *Mare Liberum* Grotiusa.

[566] zob. Art. 92 Konwencji z Montego Bay. Także Honniball A.N. *The exclusive Jurisdiciton of Flag States: A Limitation on Pro-active Port States?* The International Journal of Marine and Coastal Law 31 (2016) ss.500-10

[567]cf. Thumfart J. *Francisco de Vitoria and the Nomos of the Code: The Digital Commons and Natural Law, Digital Communication as a Human Right Just Cyberwarfare*[w:Beneyto M., Varela J., Varela C., *At the Origins of Modernity:Francisco de Vitoria and the Discovery of International Law*(2017) ss.197 i n.]

(co wyłączałoby środki kinetyczne używane w świecie fizycznym). Przyjęcie tej zasady, jakkolwiek stanowiłoby rozwiązanie problemów, wskazanych przy omawianiu poprzedniej koncepcji- dawałoby (w połączeniu z brakiem poddania informatycznej części cyberprzestrzeni kontroli sądowej) zbyt daleko idącą swobodę w doborze środków. To swoiste odwrócenie hierarchii jest funkcją utraty przez zasadę terytorialności znaczenia w we współczesnym prawie międzynarodowym a także nieistnienia jakiejś *sui generis* "cyberjurysdykcji zwyczajnej", a więc konstrukcji prawnej, chroniącej te same dobra prawne z uwzględnieniem specyfiki technicznej cyberprzestrzeni. O ile w świecie rzeczywistym bowiem zjawisko odrywania jurysdykcji od terytorium postępuje ewolucyjnie,[568] powstanie cyberprzestrzeni dokonało w ramach tego stosunku zakresowego jednoznacznej redefincji cyberprzestrzeni. Nie oznacza to oczywiście całkowitej likwidacji zasady terytorialności, która jest ciągle obecna w jurysdykcji wykonywanej w cyberprzestrzeni. Stanowi jednak wyłącznie techniczną przesłankę wykonywania tej jurysdykcji, nie zaś jej podstawę i normę generalną.

3. Cyberprzestrzenne naruszenia suwerenności nie stanowiące cyberataku.

Ze względu na fakt, iż najdalej idącym i z tego względu najbardziej doniosłym prawnie naruszeniem suwerenności jest atak w rozumieniu prawa konfliktów zbrojnych, kwestia takich ataków zostanie omówiona w osobnym rozdziale w dalszej części wywodu.

Jednak fakt, iż dana operacja nie stanowi ataku, nie nie oznacza, że nie powoduje ona naruszenia suwerenności. Należy pamiętać, że cyberoperacjom poniżej poziomu użycia siły przysługuje domniemanie legalności w świetle prawa międzynarodowego. Wynika to przede wszystkim z opisanych powyżej kwestii prohibitywności. Każda operacja cybernetyczna przeprowadzana przez państwo w części cyberprzestrzeni stanowiącej *commons* jest więc uznawana za legalną, o ile nie istnieje norma prawa

[568] cf. Rivkin D.W. *The importance of extraterritorial jurisdiction*[w: *Report of the Task Force on Extraterritorial Jurisdiction, International Bar Association*] s.33 in.

międzynarodowego, która by tej operacji zakazywała.[569] Jest to istotna i mająca doniosłe skutki różnica w stosunku do przywołanych wcześniej operacji zakładających użycie siły i siły zbrojnej, które co do zasady są nielegalne[570] a w ograniczonych przypadkach mogą być wtórnie legalizowane. Powstaje jednak pytanie o legalność operacji mających na celu pozyskanie informacji, nie będących jednak działaniami szpiegowskimi. Zarówno doktryna jak i praktyka państw przyjmuje, że te dwa pojęcia nie są znaczeniowo podobne.[571] Ponieważ wskazuje się, że głównym czynnikiem rozróżniającym te pojęcia jest bezpośredni udział agenta, czynnika ludzkiego w przeciwieństwie do analizowania danych, można przyjąć że rozróżnienie to pokrywa się z tradycyjnym podziałem źródeł wywiadowczych na *HUMINT*[572] i *SIGINT*[573]. Działania z tego pierwszego zakresu będą więc w rozumieniu regulacji z Protokołu[574] uznane za szpiegostwo, jako spełniające kryterium prowadzenia ich bezpośrednio przez ludzi (z wyłączeniem sprzętu elektronicznego). Mieszczą się one co do zasady w pojęciu niezakazanego międzynarodowo szpiegostwa. Brak jednak podobnej praktyki w zakresie traktowania działań z zakresu SIGINT, które naruszają suwerenność[575] państwa trzeciego w cyberprzestrzeni. Doktryna wyróżnia dwie główne grupy operacji cyberprzestrzennych stanowiących naruszenia suwerenności, nie przekraczających jednak poziomu użycia siły. Chodzi tu o tzw. operacje *CNE*[576], a więc naruszenie integralności systemów informatycznych państwa, które stanowi cel

---

[569] zob. Prawidło 3 Tallin Manual wraz z komentarzem,par. 3 [w: *Tallin Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press,zbiorowa,red. Schmitt M.N.(2017)]

[570] Co wynika z ogólnego zakazu interferencji i interwencji a także z wiążącej *erga omnes* normy dekodowanej z art. 51 Karty Narodów Zjednoczonych.

[571] por. *Komentarz do art. 46 I Protokołu Dodatkowego* [w:*Commentary on the Additional Protocols, Sandoz Swinarski, Zimmermann* par. 1765

[572] Akronim słów HUMan INTelligence- ludzkie źródła, zob. Także *Human Intelligence Collector Operations* US DoA FM2-23.3)FM 34-52 Waszygnton wrzesień 2006 par. 1-1

[573] SIGINT (Signals Intelligence), zob także *SIGINT for Anyone. The Growing Availability of Signals Intelligence in the Public Domain*

[574] co nie jest warunkiem koniecznym, możliwe są bowiem operacje SIGINT polegające przykładowo na przechwytywaniu sygnałów radiowych we własnej jurysdykcji, które w oczywisty sposób nie narusza suwerenności państwa, które te sygnały nadaje.

[575] por. I Protokół Dodatkowy do Konwencji Genewskich z Komentarzem.

[576] Skrót od *Computer Network Exploitation(Naruszenie Sieci Komputerowej)*, zob. *Cyberspace and Electronic Warfare Operations*, USA Departament of the Army Field Manual,FM, 3-12, roz. 2 (2-1) (2017). Niewielka część doktryny przyjmuje skrót *CNO (Computer Network Operations).* Skrót ten opisuje to samo zjawisko. W dalszej części wywodu, dla zachowania jednolitej terminologii stosowany będzie wyłącznie częściej stosowany termin *CNE.*

sam w sobie. Celem takiej operacji może oczywiście być następczo interferencja lub interwencja skierowana przeciwko państwu zaatakowanemu, choć nie jest to warunek konieczny. Drugim rodzajem operacji poniżej poziomu ataku są operacje zbiorczo określane jako *ISR*.[577] Obydwa te rodzaje operacji zostaną omówione szczegółowo poniżej.

3. a. Computer Network Exploitiation

Operacje *CNE* należy uznać za cyberprzestrzenny odpowiednik instalacji środków wywiadowczych na terytorium innego państwa. Cel ostateczny tego naruszenia może nawet nie być nakreślony w momencie przeprowadzania określonej operacji. Potencjalnie operacja *CNE* może być elementem każdej innej operacji cyberprzestrzennej. Ponieważ jednak skutek takiej operacji może być oddalony w czasie od jej przeprowadzenia, zaś okres pomiędzy jej przeprowadzeniem a wystąpieniem skutku jest potencjalnie nieograniczony - nie jest możliwe przeprowadzenie oceny takiego działania *in abstracto.* W związku z tym istnieją znaczące problemy zarówno z oceną legalności takiej operacji jak i stopnia ewentualnego naruszenia, które, jak wskazano powyżej, dokonywane są najczęściej następczo. Prowadzi to do sytuacji, w której nawet istnienie odpowiedniego prawa nie gwarantuje możliwości dokonania właściwej jego subsumpcji i w efekcie znalezienia właściwej odpowiedzi po stronie państwa, które stało się celem takiej operacji. W zasadzie możliwe jest przyjęcie dwóch koncepcji odpowiedzi na *CNE*. Pierwsza z nich zakłada możliwość domniemania przez państwo celów, które tą operacją miałyby być osiągnięte i uzasadnienie poziomu zastosowanej obrony do owego domniemania. Niewątpliwie jednak taki zakres należy uznać za zbyt szeroki i prowadzący do nadużycia prawa. Z kolei zawężająca interpretacja prawa do przeciwdziałania operacjom *CNE* stanowi potencjalnie znaczące ograniczenie prawa państw do obrony, szczególnie w przypadku operacji stanowiących wstęp do dalszych

[577] Akronym od angielskich terminów *Intelligence,Surveillance,Reconaissance(Wywiad, Śledzenie, Rozpoznanie)* zob. Także Williams B.T. *The Joint Force Commander's Guide to Cyberspace Operations,* Joint Forces Quaterly nr 23, 2/2014, s. 5 (2014)

działań, których ostateczny skutek może mieć ekwiwalencję kinetyczną.

3. a. i. Legalność

Z powyższego wynika więc, że legalność *CNE*, może być więc oceniana wyłącznie *ex post.* Jednakże ze swej natury, operacje tego typu są trwałe i rozwojowe.[578] Wykonanie jednego etapu pozwala rozpocząć następny zarówno dzięki pozyskanym informacjom jak i dzięki zwiększeniu zakresu dostępu do dalszych elementów systemu.[579] Co więcej, nikt poza stroną przeprowadzającą daną operację nie ma możliwości wyraźnego wskazania momentu jej zakończenia. Pozyskiwanie informacji przy pomocy *CNE* wymaga działania podobnego do przeprowadzenia ataku cybernetycznego; a więc zidentyfikowania elementów systemu komputerowego, przełamania systemów obrony (czyli naruszenia suwerenności). Jednakże taka operacja nie kończy się wywołaniem żadnych strat w systemie, nie można jej więc uznać za atak (zwłaszcza wobec podniesionych standardów testu ataku wobec operacji wyłącznie cyberprzestrzennych.[580] W dzisiejszym stanie prawnym *CNE* nigdy nie jest uważane za użycie siły w rozumieniu art. 2(3)(4) KNZ.[581] Taka interpretacja jest zrozumiała z punktu widzenia formalnoprawnych kryteriów, jednakże budzi wątpliwości z punktu widzenia interpretacyjnego i prawnonaturalnego.

---

[578] zob.Cartwright J.E. *Joint Terminology for Cyberspace Operations* Memorandum of Chiefs of Militrary Services Commanders of the Combatant Commands Directors of The Joint Staff Directorates. Par. 5 (2010)

[579] Najczęściej wykonywane przez specjalne elementy kodu użytego do przeprowadzenia całej operacji pozwalającego na wykonywanie zdalnego dostępu do określonych funkcji zainfekowanych komputerów. zob. *Tracking GhostNet:Investigating a Cyber Espionage Network* Information Warfare Monitor, Munk Centre for International Studies, Univeristy of Toronto s. 48 (2009)

[580] zob. Ziolkowski *Ius...*

[581] zob. Także Wortham A. *Should Cyber Exploitation Ever Consitute a Demonstration of Hostile Intent That May VIolate UN Charter Provisiones Prohibiting the Threat or Use of Force* Federeal Communications Law Journal t.64, wyd.3 s 656 Maurer School of Law:Indiana University (2012)

Samo przełamanie obrony cybernetycznej (chroniącej ze swej natury strefy terytorialne) musi zostać jednak uznane za naruszenie suwerenności, poprzez sam fakt jego dokonania. Wydaje się, że analogicznie do operacji wywiadowczych, *CNE* są uznawane za legalne (z identycznego powodu - braku możliwości realnego wyegzekwowania zakazu), dopóki nie przekroczą uznawanych przez praktykę międzynarodową granic *CNE* (a więc dopóki raz dokonane CNE nie stanie się podstawą do dalej idących działań).[582] Praktyka ta jednak nie jest jasna, w związku z czym wspomnianą granicę jest niezmiernie trudno wyznaczyć w sposób pewny.[583] Co więcej, samo uzyskanie dostępu do danych wrażliwych może prowadzić do wystąpienia strat po stronie państwa będącego celem operacji.[584]

Drugim istotnym kryterium utrudniającym konstrukcję jasnych granic legalności *CNE* jest fakt istnienia luki prawnej w zakresie ich przeprowadzania przy nieautoryzowanym wykorzystaniu symboli chronionych międzynarodowo. Dotychczasowe prawo cyberprzestrzeni ogranicza normy zakazujące stosowania wiarołomstwa czy nielegalnego wykorzystania symboliki organizacji międzynarodowych takich jak ONZ wyłącznie do konfliktu zbrojnego.[585] Jeżeli natomiast *CNE* rozpoczyna od wyłudzonego w drodze legalnej operacji wywiadowczej[586] dostępu do sieci państwowej, z punktu widzenia prawa międzynarodowego nie będzie można wskazać normy penalizującej owo działanie (o ile operacja ta nie przekroczy poziomu ataku kinetycznego lub niekinetycznego).

---

[582] Przykładowo operacje *CNE* prowadzone przez brytyjski wywiad prowadzone dla operacyjnego rozpracowania celów zarówno w Zjednoczonym Królestwie jak i poza jego granicami, prowadzonymi bez wyraźnego upoważnienia prawnego, zostały określone wyłącznie jako *nieproporcjonalne* a ich legalność kwestionowana wyłącznie ze względu na przekroczenie zakresu przedmiotowego zbierania informacji. zob. Paganini P. *GCHQ accused of illegal Computer Network Exploitation activities*, Security Affairs (2015)

[583] zob. Cebrowski A.K. *CNE and CNA in the Network-Centric Battlespace: Challenges for Operators and Lawyers* International Law Studies 76 (2012) s.2

[584] zob. Lin H.S. *Offensive Cyber Operations and the Use of Force*, Journal of National Security wyd.4 t.63 s.68 i n. (2010).

[585] Tak na przykład Tallinn Manual 2.0. IGoE umieszcza normy zakazujące podobnych zachowań w częsci czwartej dotyczącej konfliktu zbrojnego(z użyciem siły zbrojnej). Identycznie traktowane są podobne zachowania dokonywane poza cyberprzestrzenią; Konwencje Genewskie zakazują zachowań w czasie wojny a Statut Rzymski *explicite* umieszcza nielegalne zastosowanie symboliki międzynarodowej w części dotyczącej przestępstw wojennych. zob. także art.8(2)(b)(iii) Statutu Rzymskiego.

[586] może to być na przykład uzyskanie w wyniku operacji szpiegowskiej. zob także Honan M. *Kill the password: A string of characters won't protect you* Wired (2012)

Nie jest więc oczywiste, jak traktować wysłanie fałszywej wiadomości e-mail udającej przykładowo informację sporządzoną przez Międzynarodowy Komitet Czerwonego Krzyża, w istocie służącej instalacji w terytorialnej sieci państwa trzeciego oprogramowania malware.[587] Powstaje pytanie, czy można uznać takie działanie za nielegalne na gruncie obejmującego najszerszy katalog zachowań art. 1 ARSIWA. Przyjmuje się, że norma ta ma charakter niejako subsydiarny, inkorporując do wiążącego *erga omnes* prawa zwyczajowego przesłankę naruszenia wspomnianą przez Trybunał Arbitrażowy w sprawie *Rainbow Warrior.* Trybunał wskazał wówczas, że każde naruszenie przez państwo jakiegokolwiek obowiązku należy uznać za akt zabroniony.[588] Jednakże nawet ta norma (którą należy tu uznać za normę sankcjonującą) wskazuje, że jakaś norma sankcjonowana (w tym wypadku zakaz użycia symboli chronionych w operacjach *CNE*) musi wcześniej istnieć. Brak jednak takiej wyraźnej normy. Na legalność *CNE* (nawet przeprowadzanej w taki sposób) jako takiej wskazuje też dotychczasowa praktyka i *opinio iuris* państw. W aktualnym stanie prawnym ani razu nie doszło bowiem do próby uruchomienia jakiejkolwiek podstawy odpowiedzialności międzynarodowej przeciwko państwu, które jakąkolwiek *CNE* przeprowadziło, o ile nie przekroczyła ona progu ataku.[589] Innym istotnym problemem jest kryterium czasowe. Czy czas trwania operacji może wpływać na legalność trwania *CNE,* a także o przesłanki jego delegalizacji takiej operacji ze względu na czas jej trwania. Nie można wskazać wyraźnie (jakby się to intuicyjnie wydawało - niewątpliwie istniejącego) momentu, w którym *CNE* staje się operacją mającą już na celu wywołanie szkód (ale jeszcze zanim one powstaną - co pozwoliłoby na obronę), ponieważ jak przyjmuje się w doktrynie, zamiar taki lub jego

---

[587] Identyczny mechanizm wykorzystał chiński wywiad w operacji, której eksperci cyberbezpieczeństwa z państw zachodnich przypisali kryptonim *GhostNet*, wykorzystując do instalowania oprogramowania malware fikcyjne wiadomości e-mail rzekomo pochodząca z biura Dalaj Lamy,zob. Także Nagraja Sh.,Anderson R. *The snooping dragon: social-malware surveillance of the Tibetan movement.* University of Cambrigde Computer Laboratory nr 749 (2009).

[588] zob.Orzeczenie w sprawie *Case Concerning the difference between France and New Zeland...* par. 75. Także, komentarz ILC do ARSIWA, art. 1 par.2 i n.

[589] Błędnym poglądem jest wskazywanie, jako dowodu na tezę przeciwną, działań Stanów Zjednoczonych mających na celu przeciwdziałanie prowadzeniu przez ChRLD wykradania technologii. Wszystkie zastosowane, a także proponowane działania miały bowiem charakter retorsji, a więc w odróżnieniu od represaliów środków odwetowych dopuszczonych przeciwko działaniom legalnym.

brak nie przesądzają o legalności operacji.[590] Dodatkowo ocenę sytuacji prawnej utrudnia fakt, że uzyskanie dostępu do sieci nie musi mieć jednoznacznie sprecyzowanego celu,[591] a także, że przy rozpatrywaniu legalności *CNE* w ogóle nie jest brane pod uwagę kryterium celowości. W efekcie praktyka międzynarodowa dopuszcza więc naruszenie suwerenności w cyberprzestrzeni (noszące przynajmniej znamiona interferencji a potencjalnie interwencji), którego legalność opiera się na zupełnie niejasnym kryterium. Państwo, którego suwerenność zostaje naruszona, nie tylko nie ma możliwości określenia czy kryterium to zostało spełnione ale nawet nie jest w stanie stwierdzić czy dokonana interferencja nie stanowi wstępu do użycia siły zbrojnej. Co istotne, w przypadku operacji *CNE* dopuszczalna jest dużo większa swoboda w wyborze celów (brak bowiem pozytywnej normy wynikającej z prawa konfliktów zbrojnych, nakazującej wybieranie celów, których zaatakowanie ma cel militarny).[592] Jest też jasne, że ze względu na sieciowość systemów informatycznych nie jest możliwe zupełne ominięcie plików, które nie spełniają w pełni kryteriów celu militarnego.[593] Wydaje się więc, że naruszenie sieci należy uznać za *per se* legalne do momentu, w którym *CNE* nie staną się środkiem do złamania innej normy prawnej, zakazującej interferencji lub interwencji idącej dalej niż samo *CNE*. O ile w sensie prawnym opinię taką można uznać za uzasadnioną, praktycznie wskutek legalności *CNE per se* - zezwala się państwom na dowolne przeprowadzanie cyberoperacji (ze względu na ich domniemany niski stopień naruszenia suwerenności), które mogą być początkiem bardzo daleko idących naruszeń tej suwerenności. Taka konstrukcja norm zwyczajowych dotyczących *CNE*, mająca swoje źródło w analogii przeprowadzonej z normy uznającej za legalne operacje szpiegowskie (niewątpliwie obecna w praktyce

---

[590] zob. Prawidło 14 TM 2.0, wraz z komentarzem IGoE do tego artykułu, par. 8

[591] W którym to przypadku, operację należałoby zakwalifikować jako *ISR*. Szczegółowo ten typ operacji zostanie omówiony poniżej.

[592] Tak na przykład Schmitt M.N. [w:*Cyber Operations and the Jus in Bello: Key Issues* Naval War College International Law Studies, (2011). s.93-8]. Należy jednak wskazać także na istniejące głosy przeciwne wskazujące, że zasady dotyczące wyborów celów jakiejkolwiek operacji muszą być równie rygorystyczne co podczas konfliktu zbrojnego. zob. Na przykład Melzer N. *Cyberlawfare and International Law* UNIDIR Resources, Ideas for Peace and Security (2011)s. 36 i n.. Nie sposób się jednak zgodzić z takim poglądem, choćby dlatego, że jego ścisłe stosowanie oznaczałoby prawnomiędzynarodową delegalizację szpiegostwa.

[593] Schmitt przyjmuje nawet, że niektórych danych w ogóle nie należy brać pod uwagę

międzynarodowej),[594] znacząco ogranicza możliwość ochrony suwerenności państwowej w cyberprzestrzeni.

3. a. ii. Remedia przeciwko naruszeniom suwerenności natywne dla CNE

Kwestia dopuszczalności remediów przeciwko operacjom cybernetycznym poniżej poziomu użycia siły zostanie omówiona poniżej. Łatwo jednak zauważyć, że ze względu na swoją specyfikę, operacje *CNE* wymagają odrębnego porządku ochrony. Stosowanie remediów na tym poziomie stanowiło nierozwiązany problem prawny już w przypadku pokrewnych zakresowo operacji przeprowadzanych poza cyberprzestrzenią.[595] Natura *CNE* i jej nieokreślony charakter oznacza, że za niewystarczający należy uznać podstawowy środek obrony suwerenności przeciwko naruszeniom poniżej poziomu użycia siły czyli obronę pasywną (omówioną w dalszej części tego rozdziału). Same bierne zabezpieczenia mogą bowiem w dużym stopniu utrudnić prowadzenie operacji jednocześnie podwyższając ich koszty i zmniejszając szanse powodzenia. Taki skutek jest generalnie wystarczający w przypadku działań poniżej użycia siły, stanowiąc optimum z punktu widzenia ekonomiki sekurytyzacyjnej - ze względu na możliwy dalszy rozwój tych operacji. Zgodnie z zasadami ogólnymi prawa międzynarodowego, za podstawową regulację dotyczącą przeciwdziałania naruszeniom suwerenności (niezależnie od poziomu tego naruszenia) przyjmuje się cztery przesłanki wskazane przez Międzynarodowy Trybunał Sprawiedliwości. Aby środek taki był legalny, musi on być:(1) skierowany przeciwko sprawcy naruszenia i podjęty bezpośrednio w odpowiedzi na to naruszenie, (2)poprzedzony żądaniem wstrzymania nielegalnych działań, (3)proporcjonalny i pozostający w związku z pierwotnym naruszeniem, (4) nakierowany na

[594] Chodzi tu o przyczynę praktyczną. Ponieważ państwa prowadzą działalność szpiegowską zob. Na przykład Radsan A.J. *The Unresolved Equation of Espionage and International Law*, Michigan Journal of International Law 28:3(2007) ss. 597-600

[595] Jak słusznie wskazywał Thomas Franck, współczesne działania ukierunkowane na osiąganie celów wewnątrz jurysdykcji innych państw przebiegają z reguły po ekstremach, albo uniemożliwiając *ex post* skuteczne przeciwdziałanie, albo stanowiąc zbyt małe zagrożenie by uzasadniać prawnie skuteczną odpowiedź. [w: Franck Th. M. *Who Killed Article 2(4)?: Changing Norms Governing the Use of Force by States*, American Journal of International Law, wyd. 64, (1970) s .812

powstrzymanie pierwotnych naruszeń i, w przypadku, gdy nie stanowi samoobrony przeciwko atakowi, odwracalny.[596] Kryteria te, choć wynikają z orzeczenia w sprawie nie związanej z cyberprzestrzenią, przeważająca część doktryny skłonna jest uznawać za stosowalne do remediów służących obronie przed operacjami cyberprzestrzennymi poniżej poziomu ataku.[597] Jak jednak wskazano powyżej, na etapie naruszania biernych środków obronnych nie można w odniesieniu do operacji *CNE* określić ani jej celów[598] ani stopnia intensywności.[599] Stanowi to o pierwotnej niemożliwości zrealizowania trzeciego kryterium i znaczącym utrudnieniu stosowania czwartego z nich. Wobec tego nie sposób ustalić ani proporcjonalności ewentualnych remediów, ani też nakierować działania na powstrzymanie operacji, skoro cele jej nie są znane stronie, która remedia ma zastosować. Nadto, jak wskazuje praktyka międzynarodowa, ze względu na wysoki stopień utajnienia[600] i szybkość przeprowadzania operacji cybernetycznych, rzadkością jest bezpośrednia reakcja w drodze aktywnej obrony nawet na atak cybernetyczny. Tym mniej prawdopodobna jest taka reakcja w odpowiedzi na mniej znaczące naruszenie suwerenności. W związku z tym państwo będące celem operacji *CNE* ma znacząco ograniczone możliwości wykonywania ochrony przed możliwym atakiem, ze szczególnym uwzględnieniem uderzenia prewencyjnego, właśnie ze względu na niemożliwość rozróżnienia *CNE per se* od podobnej operacji stanowiącej wyłącznie wstęp do szerszej operacji lub cyberataku. Stanowi to znaczący argument za przyjęciem *de lege ferenda* w odniesieniu do *CNE* koncepcji domniemania opisanej powyżej, jako

---

[596] zob. Orzeczenie MTS z dnia 25 września 1997 roku [w:*Case concerning the Gabcikovo-Nagymaros Project* (Hun. v. Slo.),ICJ Reports 1997,(7) (1997) par. 83-8.].

[597] tak na przykład Mary O'Connell [w:O'Conell M.E., Arimatsu L.,Wilmshurst E. *Cyber Security and International Law:Meeting Summary*, Chatam House, (2012) s.8 ,także Michael Schmitt [w:Cy*ber Operations...* s. 160]

[598] Ponieważ tylko określenie celu cyberoperacji pozwala rozstrzygnąć czy jest ona atakiem. Tymczasem jak wynika z ustalonej linii orzeczniczej, przeciwko operacji nie stanowiącej użycia siły (a nie tylko siły zbrojnej) nie są dopuszczalne remedia siłowe. Tak MTS [w: *Niacargua...* par. 249] także EECC (Ethiopia-Eritrea Claims Commission) [w: Partial Award 2004 *Jus ad Bellum*, par. 12, UN Reports of International Arbitral Awards 26, (2014)s. 155 i n.]

[599] zob. także Molnar A.,Parsons Ch., Zouave E.,*Computer network operations and'rule-with-law' in Australia*, Internet Policy Review Journal on Internet Regulation 6:1 (2017) ss.4-9

[600] Dyskusyjne jest, czy w ogóle w tych warunkach możliwe jest wynikającego z art.52(1)(a) ARSIWAspełnienie obowiązku notyfikowania o planowanych środkach odwetowych państwa, przeciwko któremu będą one skierowane. Tak na przykład Roscini M. [w:*Cyber Operations...* s.121]

gwarancji realizacji prawa do obrony przewidzianego przez art. 51 Karty Narodów Zjednoczonych. Należy jednak zauważyć, że w aktualnym stanie prawnym brak w tym zakresie wyraźnych regulacji. Wydaje się jednak, że w tym kierunku zmierza praktyka międzynarodowa.

3. a. iii. Wykorzystanie CNE jako groźba użycia siły zbrojnej

Jak już wspomniano, *CNE,* do momentu konkretyzacji jego rzeczywistych celów nie sposób zdefiniować. Jeżeli więc strona, która dokonała *CNE* ujawni fakt przeprowadzenia takiego ataku - informuje praktycznie stronę, której systemy zostały naruszone o możliwości przekształcenia jej zarówno w atak o nieokreślonym zakresie.[601] Ponieważ nie ma żadnej możliwości oceny stopnia zagrożenia *in abstracto*, praktyka międzynarodowa wypracowała odrębne kryteria służące wyłącznie do oceny stopnia zagrożenia.[602] Pierwsze kryterium to potencjał naruszenia przez potencjalną operację jednej z czterech cech systemu komputerowego: bezpieczeństwa danych, integralności systemowej, prawidłowości certyfikatów bezpieczeństwa oraz dostępności systemu dla osób uprawnionych.[603] Drugim jest zestaw kryteriów, pozwalających na ocenę skutków spełnienia zagrożenia a więc czas, skala potencjalnej operacji i efekt.[604] Wydaje się więc, że wobec tych kryteriów, można oznaczyć te operacje *CNE*, które potencjalnie mogą przekształcić się w atak cybernetyczny .[605] Jednakże z prawnego punktu widzenia klasyfikowanie operacji

---

[601] Potwierdza to na przykład niezwykłe podobieństwo wirusa *Stuxnet*, kodu użytego na ataku na irańskie centra wzbogacania uranu i *DuQu*, kodu nieznanego pochodzenia, używanego w operacjach *CNE*.
zob.także Bencsáth B.,Pék G.,Buttyán L., Félegyházi M. *DuQu: A Stuxnet like malware found in the wild* CrySyS Laboratory of Cryptography and System Security, Budapest University of Economics and Technology (2011) s.2

[602] por. Erickson J. *Hacking : The Art of Exploitation* 2 No Starch Press (2008) s.35

[603] zob. Także Hollis D.B. *An e-SOS for Cyberspace* Harvard International Law Journal,52:2 (2011) s.380

[604] W przypadku zagrożenia *CNE,* chodzi o skutek pośredni. Gdyby operacja miała nawet potencjalne skutki bezpośrednie, należałoby ją uznać za cyberatak i w związku z tym podlegałaby regulacjom związnych z prawem konfliktów. zob. też.Monte M. *Network Attacks and Exploitation*: *A Framework*, Wiley (2015) ss.10-5

[605] Podobnego zdania są także specjaliści od zabezpieczeń komputerowych. zob. na

spełniających takie kryteria zagrożenia jako *CNE*, prowadziłoby do znaczącego ograniczenia prawa do samoobrony. Za uzasadnione należy więc uznać podejście, według którego każdą (nawet potencjalnie) zaawansowaną operację należy uznać za groźbę lub początek ataku cybernetycznego i zastosować do niej normy prawa międzynarodowego mające za przesłankę zagrożenie użyciem siły. Tak daleko idące prawo do obrony wobec potencjalnie niegroźnej operacji może wydawać się zakreślone zbyt szeroko. Zgodnie jednak z przywołaną już w rozprawie niniejszej opinią sędziego Simmy - żadna norma prawa międzynarodowego nie może pozbawiać państwa prawa do obrony własnej suwerenności. Ze względu na brak innych możliwości obrony przed atakami wynikłymi z rozwinięcia operacji *CNE* - taki zakres obrony należy uznać za uzasadniony.

3. b. Operacje ISR

Nazwa, powszechnie stosowana w literaturze, stanowi akronim słów *Intelligence, Surveillance, Recon(aissance)-wywiad, śledzenie, rozpoznanie*. Podstawową cechą rozróżniającą takie działania od operacji szpiegowskich jest fakt, że nie są one prowadzone przez służby wywiadowcze, a przez regularne oficjalne agendy, najczęściej stanowiące rodzaje sił zbrojnych (chodzi tu o tzw. wojska cyberprzestrzenne - powoływane przez znaczącą ilość państw). Z tego powodu często (w odróżnieniu od działań szpiegowskich) wykonywane są jawnie. Operacje tego typu stanowią najczęściej przeprowadzany typ operacji w cyberprzestrzeni.[606] Jednym z podstawowych celów, które takie działania mają osiągać jest „mapowanie" cyberprzestrzeni potencjalnego przeciwnika.[607] Nie sposób jednak uznać takich operacji co do zasady za odmianę legalnych *CNE* czy wprost działań szpiegowskich (co nie znaczy, że pewnych operacji *ISR* nie zakwalifikujemy do jednej z tych

przykład Winterfeld S. i Andress J.W. *Computer Network Exploitation* [w: Winterfeld S. Andress J.A. *Cyberwarfare,* Safari Books (2019)s.75]

[606] zob. Pomerleau M. *What is ISR in non-physical domains,* C4ISRNET(2016) s.1-3

[607] zob. Definicja *Cyber ISR*[w:*Cyberspace Operations,* Joint Chiefs of Staff Joint Pulbications 3-21(R)], także Jarmon J.A., Yannakogeorgeos P. *The Cyber Threat and Globaliation: The Impact on U.S. National and International Security*, Rowman and Litfield, (2018) s.5.

kategorii). Co więcej, operacje *ISR* mogą w ogóle nie posiadać określonych celów, a zbierać wszystkie możliwe informacje o pewnej kategorii celów.[608] Wydaje się uzasadnione z prawnego punktu widzenia, że normy regulujące operacje *ISR* należy uznać za *leges speciales* w stosunku do norm regulujących operacje na poziomie *CNE.* Wobec tego stosują się do nich odpowiednio powyższe rozważania na temat tego ostatniego.

Celem wszystkich operacji ISR jest zbieranie informacji bez bezpośredniego wpływania na systemy, do których uzyskano dostęp przy pomocy tej operacji. Z tego względu, jako działalność szpiegowska, jest to zachowanie uznawane za międzynarodowo legalne. Jako takie - podlega wyłącznie zakazom wynikającym z prawa wewnętrznego. W przypadku ISR nie jest jednak możliwe określenie granic jurysdykcji, które zostały naruszone. Wynika to z zasady wszechobecności cyberprzestrzeni. Jeżeli bowiem celem jest uzyskanie wglądu w określone dane, to możliwe jest wykonanie tego w niejako dowolnym ”miejscu” informatycznej części cyberprzestrzeni (wyjątek stanowi konieczność naruszenia wspomnianych wyżej *quasi* terytoriów cyfrowych, do których jednak włamanie jest jednoznaczne z zakazaną innymi normami interwencją- stając się w istocie operacją *CNE*), a więc bez konieczności naruszenia suwerenności jakiegokolwiek państwa. Powstaje więc pytanie, jakie normy prawne należałoby stosować do operacji z zakresu ISR. W przypadku konwencjonalnych działań wywiadowczych naruszenie suwerenności jest oczywistością, nie można więc stosować praktyki międzynarodowej wykształconej w tym zakresie do cyberprzestrzeni. Nie ma wątpliwości, że podmiot, przeciwko któremu działania takie są prowadzone, ma prawo stosować własną jurysdykcję zwyczajną i nadzwyczajną w celu przeciwdziałania takim operacjom i ścigania jej sprawców. W przypadku operacji wyłącznie cyberprzestrzennych zasada ta nie będzie miała zastosowania praktycznego. Konieczne jest więc stosowanie

[608] Tak została przeprowadzona przykładowo rosyjska cyberoperacja z zakresu ISR *Havex*, mająca na celu zbieranie informacji o szeroko pojmowanym europejskim przemyśle ciężkim. Dane te później były wykorzystywane w celowych operacjach szpiegowskich i cyberatakach. cf. Paganini P. *Cyber espionage campaign based on Havex RAT hit ICS/SCADA systems,* artykuł opublikowany w *Security Affairs*, 6/14(2014) ss.3-4. zob. także Klimburg A.*The Darkening...* s. 249

samego *lex informatica,* a normy wynikłe z jurysdykcji mogą być stosowane wyłącznie następczo. Wynika to zarówno z zasady wszechobecności cyberprzestrzeni jak i z zasady niemożliwości jej fizycznego zlokalizowania. Odróżnia to przeciwdziałanie operacjom *ISR* od operacji *CNE* lub ataków cyberprzestrzennych. Te bowiem muszą mieć fizyczne cele (choćby były nimi elementy fizycznej części infrastruktury), które wskazują jurysdykcję zgodnie z zasadami ogólnymi. W przypadku ISR taka sytuacja nie występuje. Rozpatrzmy operację, w której państwo wprowadza do cyberprzestrzeni bota,[609] którego celem jest lokalizowanie w czasie rzeczywistym telefonów należących do urzędników państwowych innego państwa, a następnie przekazywanie tych lokalizacji do satelitów szpiegowskich w celu podsłuchiwania komunikacji prowadzonej przez te telefony. Operacja ta w ogóle nie ma fizycznych aspektów, w związku z czym naruszenie suwerenności mogłoby dotyczyć wyłącznie części informatycznej cyberprzestrzeni. Obydwie strony mogą być zainteresowane zarówno eskalacją jak też deeskalacją. Pierwsza nastąpiłaby poprzez wskazanie, że wykonują jurysdykcję nad częścią informatyczną i w związku z tym opisana operacja została przeprowadzona na poziomie *CNE* lub nawet ataku cybernetycznego, jeżeli skutkiem podsłuchu były straty fizyczne. Drugą łatwo mogą osiągnąć poprzez uznanie, że operacja została przeprowadzona poza jakimkolwiek zakresem ich jurysdykcji (co uzasadniałoby niestosowanie zarówno jurysdykcji zwyczajnej jak i nadzwyczajnej) lub poprzez potraktowanie operacji jako *stricte* szpiegowskiej i przeciwdziałanie jej wyłącznie za pomocą środków politycznych. Obydwa państwa mają więc *de facto* możliwość wyboru skutków prawnych tej samej operacji. W przypadku operacji fizycznej podejmowane są działania kontrwywiadowcze, a praktyka międzynarodowa często bardzo luźno interpretuje granice, którymi związane jest państwo przeciwko któremu prowadzona jest operacja. Przykładem tego może być zachowanie Stanów Zjednoczonych w tzw. Kryzysie Pueblo. Okręt nasłuchu elektronicznego USS Pueblo, zamaskowany jako statek badawczy prowadził nasłuch łączności północnokoreańskiej, pozostając na wodach

[609] Nie chodzi tu o urządzenie a o kod wykonujący określone zadania. Kod taki ma swobodę 'poruszania się' po cyberprzestrzeni. Rozpoznaje on wskazane mu przez twórców sygnały lub inne elementy kodu i wykonuje wobec nich określone działania.

międzynarodowych. Został jednak zidentyfikowany i zajęty, a jego załoga uwięziona. USA podejmując działania dyplomatyczne na rzecz powrotu załogi do kraju nie podnosiły w ogóle argumentu bezprawności zatrzymania, zarówno w stosunkach dwustronnych jak i na szerszym forum międzynarodowym. Powodem tego była właśnie prowadzona przez jednostkę działalność szpiegowska.[610] Korea Północna natomiast ograniczyła się do aresztowania załogi statku pod zarzutami działalności szpiegowskiej opartej na prawie krajowym i nie podnosiła żadnych roszczeń międzynarodowych.[611] Wydaje się, że w cyberprzestrzeni, gdzie praktyka międzynarodowa wskazuje na duży szerszy zakres pozwoleń operacje ISR należy uznać za legalne w rozumieniu prawa międzynarodowego, podobnie jak klasyczne operacje szpiegowskie,.[612]

4. Mieszane naruszenia suwerenności poniżej poziomu konfliktu

Możliwa jest sytuacja, w której naruszenie suwerenności w cyberprzestrzeni, powoduje także jej jednoczesne naruszenie w świecie fizycznym. Należy zauważyć, że do sytuacji takiej może dojść w ramach działania umyślnego lub nieumyślnego, albo też na skutek zaniechania. Dla oceny prawnej kluczowe będzie ustalenie, w której ze sfer naruszenie jest dalej idące. Przykładem takiej sytuacji może być użycie drona, naruszającego fizyczną przestrzeń powietrzną danego państwa i zakłócającego przy pomocy przenoszonych środków walki elektronicznej pracę serwerów, na których opiera się obrona terytorialnej części cyberprzestrzeni zaatakowanego państwa. Jeżeli przyjmiemy, że do obydwu naruszeń doszło przez fakt, że kontrola nad owym dronem była sprawowana w drodze operacji

---

[610] zob.Finch,jr. St.B. *Pueblo and Mayaguez: Legal Analysis* Case Western Journal of International Law 9:1 (1977) s. 83-7

[611] Doktryna prawa cyberprzestrzeni przyjmuje, że praktyka braku istotnych reakcji na poziomie międzynarodowym na incydenty podobne jak ten związany z zatrzymaniem USS Pueblo, ukształtowała się zasadniczo podczas okresu Zimnej Wojny. Amerykańscy analitycy wskazują na szereg kolejnych sytuacji, w których zarówno Stany Zjednoczone jak i Związek Sowiecki ograniczały reakcję w podobnych sytuacjach do sfery politycznej. cf. Libicki M. C. *Cyberspace in Peace and War*, Naval Institute Press (2016) ss.282 i n.

[612] W pewnym sensie stanowią one odmianę operacji SIGINT, których legalność doktryna prawa międzynarodowego wyraźnie uznaje. Choć *per se* operacje te nie należą do domeny cyberprzestrzeni, funkcjonują one w oparciu o sygnały identyczne z tymi, o które oparte jest funkcjonowanie cyberprzestrzeni. zob. także Sulmasy G. *Counterintuitive: Intelligence Operations and International Law*, Berkeley Law Scholarship Repository 1:1(2006) s.10

cyberprzestrzennej dokonanej przez państwo trzecie, musimy zauważyć, że dojdzie do interferencji zarówno w świecie fizycznym (także wobec fizycznej części cyberprzestrzeni), jak i informatycznej części cyberprzestrzeni dwóch niezależnych państw - tego, które jest właścicielem drona i tego, którego suwerenność ostatecznie została naruszona. Ewentualne działania kinetyczne podjęte przez to ostatnie państwo w obronie własnej przestrzeni powietrznej i zestrzelenie drona będzie skutkowało użyciem siły kinetycznej do odparcia operacji *CNE.* Legalność takiego działania wydaje się być kwestionowana (podczas gdy zakłócania - o ile nie prowadzi do trwałych zniszczeń infrastrukturalnych - nie można uznać za operację mającą ekwiwalent kinetyczny). Drugim istotnym problemem będzie także fakt użycia siły wobec jednostki państwa, które *de facto* danego naruszenia nie dokonało. Ewentualne natomiast roszczenia wobec tego państwa wynikłe z braku należytej ochrony własnej suwerenności (tu - niedopuszczenia do przejęcia kontroli nad dronem), wymagałyby pełnego procesu atrybucyjnego. Podmiot, który przejmujący kontrolę nad dronem - czyni to w drodze naruszenia integralności systemów o nieokreślonym w momencie jego dokonania skutku, co dokładnie odpowiada przedstawionej powyżej definicji operacji *CNE.*[613] Natomiast samo zestrzelenie zostaje dokonane przez inne państwo Sytuacje takie wynikają z nakładania się na siebie porządków cyberprzestrzeni i prawa międzynarodowego publicznego.[614] Wskutek mieszanych naruszeń suwerenności brak możliwości jasnego określenia podmiotów odpowiedzialnych za określone działanie a także jasnego wyboru prawa (pomiędzy *lex informatica* a tradycyjnym prawem międzynarodowym). Więcej - brak nawet pewnych przesłanek, pozwalających na określenie sytuacji, w których zasadny jest wybór dalej idących środków obrony własnej suwerenności, niezależnie od tego, z którego ze wspomnianych systemów wynikają. Pod tym względem mieszane naruszenia suwerenności poniżej poziomu siły stanowią sytuacje dużo bardziej skomplikowane

[613] Samo przejęcie tej kontroli nie powoduje bowiem żadnych skutków w świecie fizycznym. zob. Stroheimer M., Schafer M., Lenders V., Martinovic I. *Realities and challenges of nextgen air traffic management: the caseo f ADS-B*, IEEE Communications Magazine 52:5(2014) ss.111-8

[614] zob. Hartmann A., Giles K. *UAV Exploitation: A New Domain for Cyber Power*, 8th International Conference on Cyber Conflict [w: zbiorowa, red. Pissanidis N., Roigas H., Veenendaal M. *Cyber Power* NATO CCDCOE Publications (2016) s.206]

prawnie niż podobne naruszenia rozstrzygane przez prawo konfliktów zbrojnych, gdzie nie zachodzi wspomniany problem zmieszania porządków prawnych. Z tego względu właśnie ten rodzaj naruszeń mieszanych (zwłaszcza omówione poniżej cyberoperacje wykonywane jednocześnie w cyberprzestrzeni i świecie rzeczywistym) pozwalają na regulację stopnia odpowiedzi przez stronę ją przeprowadzającą.[615] Łatwo zauważyć, że cyberoperacje poniżej poziomu użycia siły funkcjonują w obecnym stanie prawnym w luce prawnej, regulowane wyłącznie normami partykularnymi, bez regulacji kompleksowej (jak ma to miejsce w przypadku cyberataków – gdzie stosuje się odpowiednio prawo konfliktów zbrojnych) Brak też możliwości zastosowania do cyberoperacji ogólnych zasad odpowiedzialności międzynarodowej opartej o ARSIWA, czy zasad wypracowanych w *case-law*. Reżimy te bowiem opierają się o zasadę generalną należytej staranności (*due-dilligence*) w wykonywaniu obowiązków państwa wobec społeczności międzynarodowej.[616] Po pierwsze w cyberprzestrzeni naruszenia takie mogą dokonywać podmioty niepaństwowe, do których zasada ta się nie ma zastosowania. Po drugie, ze względu na legalność operacji szpiegowskich, w których zakresie mieszczą się operacje *ISR* - nie jest jasne, czy w ogóle możliwe jest przypisanie państwu winy za ich przeprowadzenie na gruncie odpowiedzialności za czyny międzynarodowo zabronione. Wynika to także z braku jasnych kryteriów możliwości określenia rozmiarów szkody, jeżeli szkoda ta nie ma ekwiwalentu kinetycznego. Ostatnim powodem jest wspólna dla wszystkich rodzajów naruszeń suwerenności w cyberprzestrzeni praktyczna niemożliwość dokonania atrybucji. Nawet jednak w razie dokonania tej ostatniej, cyberprzestrzeń tworzy nowy problem w zakresie odpowiedzialności międzynarodowoprawnej. Dotychczas czyny zabronione międzynarodowo w rozumieniu ARSIWA dokonywane były przez państwa, od których dochodzenie odpowiedzialności było stosunkowo łatwe. Były one bowiem

---

[615] Kwestia ta zostanie przealizowana szczegółowo w rozdziale piątym niniejszej rozprawy.

[616] zob. Stockburger P.Z. *From Grey Zone to Customary International Law: How adopting the Precautionary Principle may help crystalize the due dilligence principle in Cyberspace* 10th International Conference on Cyber Conflict [w: zbiorowa,red. Minarik T., Jakschis R., Lindstroem L. CyCon X Maximising Effects, NATO CCD COE Publications (2018) ss.245-50]

związane traktatami czy też poddane jurysdykcji sądów i trybunałów międzynarodowych. Z kolei naruszenia dokonywane przez aktorów niepaństwowych, miały charakter marginalny ze swej natury. Inaczej jednak ta kwestia wygląda w cyberprzestrzeni. O ile przeprowadzenie cyberataku wymaga dostępu do możliwości technicznych i wiedzy specjalistycznej znacząco ograniczającej ilość podmiotów, które mogą taką operację przeprowadzić - działanie poniżej tego poziomu może przeprowadzić dużo szerszy katalog podmiotów, z których część w ogóle nie jest związana prawem międzynarodowym. Wobec pozostałych aktorów niepaństwowych stosowanie zasad odpowiedzialności przewidzianych w prawie międzynarodowym byłoby obarczone pierwotną niemożliwością ich wykonania.[617] Ostatnim powodem jest fakt, że bardzo często nie da się ocenić czy szkody w ogóle wystąpiły i wskazać na związek przyczynowo-skutkowy. W dalszej części wywodu jako ilustracja opisanych powyżej przyczyn, zostanie omówiony jeden z takich właśnie przypadków, jak się wydaje- najbardziej reprezentatywny. Chodzi tu o naruszenia suwerenności przy pomocy używania tzw. *Big Data*[618] i możliwości ich zastosowania w operacjach poniżej poziomu użycia siły. Istotą tego rodzaju danych jest umożliwienie ich posiadaczowi uzyskiwania właściwie dowolnych informacji o dowolnie wybranej grupie użytkowników cyberprzestrzeni na podstawie metadanych możliwych do określenia na podstawie dokonywanych przez nich transferów danych.[619] Wykorzystanie metadanych ma swoje źródło w reklamie i do niej było pierwotnie wykorzystywane. Posiadanie odpowiedniej mocy obliczeniowej pozwala jednak także pozyskiwać informacje natury państwowej lub profilować komunikaty,

---

[617] zob.Plakokefalos I. *The Use of Force by Non-States Actors and the Limits of Attribution of Conduct: A Reply to Vladyslav Lanovoy*, European Journal of International Law 28:2 (2017) ss. 590 i n.

[618] Zgodnie z przyjmowaną ogólnie tzw. Definicją Gartnera(tzw. 3 V; *Velocity, Volume, Variety-Szybkość, Rozmiar, Zróżnicowanie*), są to dane zbierane z bardzo szerokiego zakresu transferów danych dokonywanych w cyberprzestrzeni a następnie przypisywane do numerów IP, urządzeń które w tych transferach uczestniczyły. zob. Douglas L. *The importance of 'Big Data'*, Gartner IT Glossary (2012)s.1 Definicja ta została rozszerzeona o dwa kolejne punkty; mianowicie *Value i Veracity-Wartość i Wiarygodność*. zob. *The Value-and Truth- of Big Data* [w: *Oracle Big Data,Integrated Cloud Applications* raport firmy Oracle na temat tworzenia zapisów z danych przechowywanych w chumrach.]

[619] Matza C., Kosinski M., Navec G., Stillwell D.J. Psychological targeting as an effective approach to digital mass persuasion [w: zbiorowa, red. Fiske T. Proceedings of National Academy of Science 117:48 (2017) ss.1274 i n.]

skierowane do społeczeństw państw trzecich. Umożliwia to daleko idące ingerowanie w wyniki wyborów, za pomocą odpowiednio spreparowanych komunikatów. Co istotne, działanie takie nie łamie pozytywistycznie pojmowanych zasad nieinterwencji i nieinterferencji. Dyskusyjne byłoby nawet przyjęcie, że łamie je w ujęciu materialnoprawnym. Jest bowiem przeprowadzane w informatycznej części cyberprzestrzeni (czyli *res communis omnium*). Nie może więc być mowy o naruszeniu suwerenności. Należy także zauważyć, że najczęściej operacje takie są regulowane poprzez podmioty prywatne, działające często w wielu jurysdykcjach. Podmioty takie, właśnie dzięki swojej globalnej obecności, są w stanie funkcjonować w praktyce wyłączenie w *commons* informatycznej części cyberprzestrzeni, a w związku z tym zupełnie omijać jurysdykcję w oparciu o terytorialność. Na podobnej zasadzie firmy takie są w stanie unikać niekorzystnych regulacji prawnych promulgowanych w krajach, na prawach którego są one rejestrowane. Wystarczy bowiem, aby podmiot taki rejestrował swoje struktury w innych jurysdykcjach, a następnie na mocy własnych wewnętrznych regulacji, przekazywał kompetencje (a w związku z nimi dostęp do określonych danych) owym strukturom. Wskutek takich działań, dowolny z takich podmiotów zależnych może w każdym momencie uzyskać pełne kompetencje i możliwości dostępu do danych posiadanych przez podmiot dominujący. W istocie, ten ostatni może w czasie rzeczywistym przenosić się w całości z dowolnej jurysdykcji terytorialnej, wyłącznie poprzez zmianę reprezentacji do określonej czynności. Łatwo zauważyć, że w praktyce dla podmiotu dominującego zmiana ta jest pomijalna, natomiast wyłącza stosowalność jurysdykcji opartej na zasadzie terytorialności.[620] Do dzisiaj brak regulacji rozwiązujących ten problem po stronie klasycznych podmiotów prawa międzynarodowego.[621] Nie jest także jasne, czy regulacje takie w ogóle są możliwe. Podmioty te bowiem pozostają najczęściej pod kontrolą innych zdecentralizowanych podmiotów, najczęściej podmiotów prawa

[620] Przykładem takiego działania, może być wyłącznie milionów użytkowników portalu Facebook z zakresu przedmiotowego działania (GDPR)RODO, poprzez przeniesienie ich poza serwery położone w Unii.zob Kostaki I. *Mr. GDPR: Interview with Giovanni Buttarelli,*New Europe wyd. Z 28 maja 2018 roku. (2018) s.2

[621] zob. Lietzen I. *Third Facebook-Cambride Analytica Hearing: data breach prevention and cures*, komunikat prasowy Parlamentu Europejskiego z 4 czerwca 2018 roku

międzynarodowego *sui generis*. Przykładowo kontrolę (powszechnie akceptowaną przez organa państw), nad prawdziwością transferów danych do Facebooka[622] sprawował IFCN.[623] Wynika z tego, że kontrola nad jednym z podstawowych aspektów zgodności prawa ochrony danych osobowych ze stanem faktycznym nie tylko jest wykonywana poza jurysdykcją państw (lub innych podobnych organizacji, jak na przykład Unii Europejskiej), ale wręcz, że wykonuje ją podmiot trzeci. Nie sposób wskazać także, jakkolwiek sam pogląd taki wydaje się mieć daleko idące konsekwencje, dlaczego niewłaściwe byłoby uznanie takiej sytuacji za prawo zwyczajowe. Można bowiem wskazać zarówno istnienie praktyki międzynarodowej jak i *opinio iuris,* uznające za legalne sprawowanie nadzoru nad *big data* przez podmioty prawa prywatnego. Spróbujmy jednak porównać prawo pierwotne i wtórne Unii Europejskiej z jej opisaną powyżej praktyką w zakresie regulacji *big data*. Przede wszystkim już samo zestawienie postanowień Karty Praw Podstawowych UE z wykorzystywaniem tego typu danych stwarza poważne trudności interpretacyjne. Karta wymaga bowiem, aby jakiekolwiek dane były przetwarzane w oparciu o zgodę podmiotów, których one dotyczą lub o inne podstawy prawne, legalizujące takie przetwarzanie.[624] Podobne regulacje zostały powtórzone w *GDPR*, obowiązującym w przeciwieństwie do Karty w całej UE, oraz w pewnym zakresie także podmioty spoza UE, a prowadzące w niej swoje interesy.[625] Pomimo istnienia tych regulacji, w UE działają podmioty, których działania pozostają do nich faktycznie w relacji *praeter legem* lub nawet *contra legem*[626]. Z braku jakichkolwiek działań organów UE w tym zakresie, a nawet faktycznego wprowadzania wyjątków do stosowania tych przepisów, należy inferować milczącą zgodę na takie działania (i w konsekwencji- milczącą

---

[622] zob. Zuckerberg M. *Anwers from Facebook to questions asked during Mark Zuckerberg meeting*, odpowiedzi dla komisji Parlamentu Europejskiego,(2018) par. 18

[623] *International Fact-Checking Network*. Jest to zarejestrowany na prawie amerykańskim, podmiot zależny międzynarodowej organizacji dziennikarskiej, pozbawiony jakichkolwiek, jasno zdefiniowanych, obowiązków prawnomiędzynarodowych.

[624] zob. art. 8(2) Karty Praw Podstawowych Unii Europejskiej, ogłoszonej przez Parlament Europejski, Radę i Komisję 30 marca 2010 roku,opublikowanej w Dzienniku Urzędowym UE pod sygnaturą 2010/C 83/02 (2010), dalej jako Karta Praw Podstawowych UE.

[625] zob. Art. 5 i 6 RODO.

[626] Jak choćby wspomniany powyżej spór ICANN z Komisją Europejską i Radą.

delegację kompetencji na owe organizacje międzynarodowe jak IFCN).[627] Na podstawie powyższych rozważań, jeżeli przyjmiemy istnienie takiej normy prawa zwyczajowego, jedynym logicznym wnioskiem musi być konstatacja, że same *Big Data* (które należy tu odróżnić od pozostających z innych przesłanek poza jurysdykcjami danych tworzących cyberprzestrzeń) są elementem *commons* czyli informatycznej części cyberprzestrzeni. Zgodę państw na uznanie pojmowanych *in abstracto Big Data* za element *commons* należy z kolei uznać za zrzeczenie się jurysdykcji w tym zakresie. Nie ma więc możliwości analizowania ich w kontekście interwencji czy interferencji. Jeżeli bowiem przyjmiemy, że interferencja (a jako pojęcie mieszczące się w interwencji, jej zaistnienie implikuje tę ostatnią) może być dokonana z użyciem legalnych środków, otrzymujemy sprzeczność. Obydwa możliwe jej wyjaśnienia: primo, koncepcja że zachowanie stanowiące *malum per se* jest wtórnie legalizowane, oraz secundo, założenie że w razie użycia *Big Data* do interwencji interwencja ta nie jest nielegalna - nie są do utrzymania. Jedynym możliwym z logicznego punktu widzenia wyjściem jest przyjęcie, że ze względu na fakt, że *Big Data* stanowią element *res communis ominum*, nie zostaje spełniona przesłanka przedmiotowa interferencji, ponieważ żadnej suwerenności nie można tu wskazać, a tym samym naruszyć. Łatwo jednak zauważyć, że w świecie fizycznym nie będzie żadnej możliwości rozróżnienia pomiędzy interferencją dokonaną w taki sposób, a interferencją spełniającą przesłankę przedmiotową czynu zabronionego międzynarodowoprawnie. Stosowanie *Big Data* daje więc możliwość zastosowania normowania faktycznego do naruszenia suwerenności państwowej, w sposób nie tylko nie stanowiący ataku, ale nawet uniemożliwiający podniesienie złamania zasady nieintereferencji[628] przez stronę poszkodowaną. To z kolei prowadzi nawet już nie

---

[627] zob.Orzeczenia Sądu Rejonowego w Bonn (syg. 10 O 171/18) i Wyższego Sądu Kolonii (syg. 19 W 32/18) we wspomnianej powyżej sprawie ICANN v. EPAG, w sprawie wydania środka zabezpieczającego w sprawie stosowania RODO do serwisu *WHOIS.* Powszechna opinia wyrażona w doktrynie, wskazująca na przegraną ICANN, nie bierze pod uwagę, że orzeczenia niemieckich sądów dotyczyły wyłącznie środków *ad interim*, których przyznania odmówiono z powodów formalnych. Obydwie instancje wyraźnie odmówiły orzeczenia *in meritii*.

[628] Należy zauważyć, że nie istnieje (a nawet nie wydaje się możliwy do skonstruowania) odpowiednik Testu Schmitta odnoszący się do naruszenia zasady interwencji i interferencji, która nie stanowi użycia siły.

tyle do skonstruowania narzędzia umożliwiającego legalne naruszenia suwerenności państwowej w cyberprzestrzeni, ale faktyczne rozmywanie owej suwerenności - jeszcze na gruncie teoretycznoprawnym. Dzieje się to przede wszystkim na drodze wspomnianych wcześniej afordancji, czyli w sensie prawnym normowania faktycznego cyberprzestrzeni, poprzez ograniczanie lub zwiększanie możliwości wykorzystywania danego systemu przez jego użytkowników. W przypadku normowanej kodem informatycznej części cyberprzestrzeni działanie takie jest praktycznym wykonywaniem jurysdykcji preskrypcyjnej. Należy jednak zauważyć,że wpływ na możliwy zakres afordancji dostępny jest nie tylko podmiotom nieuprawnionym do wykonywania jurysdykcji zwyczajnej w odniesieniu do jakiegoś określonego terytorium, ale także podmiotom, w przypadku których nie ma mowy o suwerenności - w ogóle nie posiadającym przymiotu suwerenności, jak w przypadku podmiotów prawa prywatnego lub osób prawnych w opisywanych powyżej przypadkach.

5. Remedia przeciwko operacjom nie stanowiących użycia siły.

Ze względu na opisane powyżej komplikacje prawne dotyczące przeciwdziałania cyberoperacjom poniżej poziomu użycia siły wydaje się, że podstawowym środkiem ochrony suwerenności w tym zakresie jest odpowiednia polityka sekurytyzacyjna. Jej celem jest uniemożliwienie lub przynajmniej jak najdalej idące utrudnienie naruszenia przy jednoczesnym braku aktywnej (a więc aktywnie szkodzącej podmiotowi, który operację przeprowadza) odpowiedzi. Taka konstrukcja umożliwia działania nawet w warunkach trudności prawnych opisanych powyżej - ze względu na brak konieczności rozwiązywania opisanych tam problemów interpretacyjnych dla skuteczności tego przeciwdziałania.

Przyjmuje się, że taka koncepcja bezpieczeństwa została skonstruowana przez tzw. Szkołę Kopenhaską (termin ów został użyty przez Billa McSweeney'a na określenie grupy politologów zajmujących się teorią bezpieczeństwa międznynarodowego na

Uniwerystecie w Kopenhadze).[629] Pod tym terminem autorzy związani ze Szkołą rozumieją decyzję danego państwa o uznaniu określonego zakresu własnych interesów za wymagający szczególnej ochrony.[630] Ochronę tę podmioty prawa międzynarodowego wykonują poprzez działania prawne i polityczne w pięciu podstawowych sektorach: politycznym, ekonomicznym, militarnym, środowiskowym i społecznym.[631] Ponieważ nieomal każde państwo uznaje cyberprzestrzeń za mającą znaczenie kluczowe dla jego suwerenności, a sposoby realizowania jej ochrony oraz kolejność priorytetów mogą oczywiście być zróżnicowane, istnieje wiele koncepcji sekurytyzacji cyberprzestrzeni. Analiza większości z nich wskazuje jednak, że wspólne dla wszystkich państw będzie oparcie przeciwdziałania naruszeniom suwerenności na opisywanym poziomie na tzw. cybernetycznej obronie pasywnej. Należy tu przywołać tzw. model Libickiego[632], wyróżniający w ramach sieci krajowej trzy warstwy: fizyczną - urządzenia komputerowe jako takie, syntaktyczną - obejmującą oprogramowanie i systemy sterujące częścią fizyczną cyberprzestrzeni oraz semantyczną - czyli wyłącznie informacje w cyberprzestrzeni przechowywane. Zgodnie z tym modelem sieć danego państwa jest wielopłaszczyznowa, a skierowanie operacji do jednej z tych warstw pozwala pośrednio wpływać na następne. Współczesne sieci, w przypadku blisko współpracujących podmiotów, muszą być ze sobą blisko powiązane dla skutecznego działania. Wystarczające byłoby więc skierowanie operacji przeciwko najsłabszemu w danym zakresie modelu Libickiego elementowi tej sieci, by później, już ominąwszy jej obronę, wpływać na inne jej poziomy (także te w innych częściach sieci stanowiącej terytorialną część cyberprzestrzeni). W praktyce oznacza to, że zróżnicowanie wartości przypisywanej poszczególnym elementom jest pozbawione znaczenia, ponieważ odporność całego systemu na naruszenia będzie taka, jak jej najsłabszego elementu według modelu

[629] McSweeney B. *Identity and Security: Buzan and the Copenhagen School*, Review of International Studies 22:1 (1996), s. 88 i n.

[630] zob. Buzan B., Waever O., de Wilde J. Security: A new framework for Analysis, Lynne Rienner Publishers (1998), s. 24

[631] ibid.. s. 27-30

[632] zob. Libicki M.C., Conquest in Cyberspace: National Security and Information Warfare, publikacja Rand Corporation, Cambridge University Press(2007), ss. 24-27

Libickiego.[633] Przykładem takiego funkcjonowania obrony pasywnej może być opisywana w literaturze przedmiotu potencjalna operacja skierowana przeciwko superkomputerowi, dokonana wyłącznie poprzez uzyskanie wpływu na system chłodzenia tego komputera. Przekroczenie pewnego poziomu temperatury w wyniku manipulacji systemem może prowadzić do samoczynnego wyłączenia komputera lub utraty danych na nim zawartych, chociaż integralność samego komputera i jego systemów nie zostaje w żaden sposób naruszona.[634] Łatwo zauważyć, że implikuje to konieczność integracji do systemów prawnych dotyczących bezpieczeństwa cybernetycznego - także regulacji dotyczących innych zakresów przedmiotowych prawa, które same z kolei mogłyby mieć wpływ na bezpieczeństwo cybernetyczne. Elementy części fizycznej są także ruchomościami, i jako takie podlegają odpowiednim regulacjom, zupełnie niezależnym od prawa cyberprzestrzeni. Regulacje kwestii pokrewnych ściśle rozumianemu bezpieczeństwu (takich jak dostęp do urządzeń czy określenie norm wytrzymałości materiałów stosowanych w infrastrukturze fizycznej cyberprzestrzeni) będzie dokonywane w drodze jurysdykcji preskrypcyjnej. Podstawowym narzędziem prawnym dla obrony pasywnej będzie więc stanowienie norm w ramach jurysdykcji zwyczajnej. Normy te muszą być jednak stanowione zgodnie z odpowiednim stanem wiedzy o procesach zachodzących w informatycznej części cyberprzestrzeni. W ten sposób powstaje odpowiednia norma *lex informatica,* pośrednio tworząca afordancje funkcjonujące w cyberprzestrzeni rozumianej jako całość. Afordancje te nie są w stanie przeszkodzić aktorom przeprowadzającym cyberoperację (co uzasadnia brak konieczności przeprowadzenia atrybucji działania i gwarantuje legalność takiej obrony), natomiast pozwala na zniweczenie lub przynajmniej znaczące ograniczenie szkód przez tę operację

[633] zob. Chung, K., Kalbarczyk, Z. T., & Iyer, R. K. *Indirect cyber attacks by perturbation of environment control: A data driven attack model*, wykład w ramach konferencji HotSoS 2018 [w: wydawnictwo pokonferencyjne z Annual Symposium and Bootcamp on Hot Topics in the Science of Security Raleigh, USA (2018) ss.5-7]

[634] zob.Chung K., Formicola V., Kalbarczyk Z.T., Iyer R.K.*Attacking Supercomputers Through Tergeted Alteration of Evnironmental Control: A data driven case study*, University of Illinois, IEEE Conference on Communications and Network Security (CNS)(2016) par. 1i 2

poczynionych.[635] O ile brak tu klasycznego odstraszania (opartego o konieczność wkalkulowania u ewentualnego aktora przeprowadzającego operację własnych strat) zastosowanie pasywnych środków gwarantuje, że afordancje chroniące suwerenność państwa zyskują na skuteczności w dwóch kluczowych w cyberprzestrzeni aspektach: szybkości reakcji i likwidacji trudności atrybucyjnych. Ponieważ pierwszorzędnym celem każdego systemu ochrony państwa jest niedopuszczenie do strat po jego stronie, a ewentualne retorsje wobec podmiotów dokonujących naruszeń muszą pozostawać drugorzędne - obrona pasywna, jako znacząco bardziej skuteczna, staje się standardem w praktyce ochrony własnych interesów przez podmioty prawa międzynarodowego. Natomiast rolę odstraszania w przypadku obrony pasywnej[636], pełni maksymalne zwiększenie kosztów ewentualnej operacji przy jednoczesnej minimalizacji korzyści, możliwych do osiągnięcia przez jej wykonawcę[637] Należy pamiętać, że w przeważającej części połączenia cyberprzestrzenne podlegają kontroli prywatnych podmiotów *ISP*. Kontrola nad tymi podmiotami to kolejny zakres przedmiotowy, w którym wykonywanie przez państwa ich jurysdykcji preskryptywnej musi odbywać się z uwzględnieniem całości cyberprzestrzeni.[638] Oznacza to więc, że pierwszym elementem skutecznej obrony pasywnej musi być prawne uregulowanie kwestii prywatnych podmiotów *ISP*, dążące do zabezpieczenia fizycznej i syntaktycznej strefy sieci wewnętrznych według klasyfikacji Libickiego. Niezmiernie bowiem często do operacji lub nawet ataków przeciwko serwerom rządowym dochodzi za pośrednictwem sieci prywatnych i ogólnodostępnych.[639]

---

635 zob. także Shackelford S. *When it comes to Cyber Security, Passive Defence is Best*, Indiana University, The Conversation (2019) par.2 i 3

636 Dalej jako PCD (*Passive Cyber Defence*)

637 Chodzi tu o tzw. *Detterence by denial*, a więc odstraszanie nie tyle oparte o pewność odpowiedzi ale o niewielką skuteczność cyberoperacji w stosunku do poniesionych na nią nakładów. zob. także Snyder G.H. *Deterrence and Defense: Toward a Theory of National Security*, Priceton Legacy Library (1961) s.1

638 zob. także Raport amerykańskiego DHS (Department of Homeland Security)*Recommended Practice: Improving Industrial Control System Cybersecurity with Defense - in - Depth Strategies. Industrial Contorol Systems Cyber Emergency Response Teams* (2016)ss.33-7

639 W taki sposób działały przykładowo wirusy *NotPyetya* i *WannaCry*. Wykorzystywały one prywatne komputery do wykonywania operacji przeciwko określonym, wpisanym w swój własny kod serwerom rządowym. zob. także Schmitt M., Biller J. *The NotPetya Cyber Operation as a Case Study of International Law,* European Journal of International Law, EJIL:Talk! 2/17 (2017) s.2

Drugim etapem obrony pasywnej jest natomiast zwiększanie poziomu trudności i zmniejszanie korzyści z przeprowadzonej operacji. Wymaga to monitorowania w czasie rzeczywistym zakresów sieci, do której ma dostęp każdy z podłączonych do niej użytkowników (a więc także tych legalnie w niej przebywających). Stopień tego monitorowania jest oczywiście decyzją z zakresu sekurytyzacji. Najczęściej prowadzona jest ona przy pomocy kontroli punktów docelowych pakietów danych wysyłanych przez system poruszający się po sieci, czyli tzw. *Deep Packet Inspection.*[640] Oczywiście kontrola ta będzie bezpośrednio wpływać na wolność ruchu w danej sieci - co ma szczególne znaczenie w przypadku kolektywnej obrony cybernetycznej[641] i uzależniona będzie będzie od zarówno prawnej jak i faktycznej integracji odpowiednich afordancji. Trzecim etapem obrony pasywnej, będzie natomiast minimalizacja poniesionych strat, w przypadku wielu podmiotów uzależniona od skutecznego informowania się wzajemnego przez te podmioty o dokonanych naruszeniach. Sytuacja ta komplikuje się w przypadku działań kolektywnych, gdzie grupy podmiotów wymagają ścisłej współpracy.[642]

Innym czynnikiem, wpływającym na ograniczanie obrony poniżej poziomu użycia siły do *detterence by denial* jest (również zresztą powiązany z trudnością atrybucji), zakaz prowadzenia cybernetycznych operacji obronnych (nawet nie stanowiących użycia siły) przez podmioty prywatne podległe ich jurysdykcjom.[643] Zakaz taki jest przyjmowany do praktyki międzynarodowej w coraz szerszym stopniu i już usankcjonowany w wielu krajowych porządkach prawnych Ze względu na to, że przeważająca ilość naruszeń suwerenności poniżej poziomu użycia skierowana jest przeciwko elementom sieci należącym do podmiotów prywatnych (na przykład podmiotów *ISP*) i są one praktycznie wystarczające (co wynika z modelu Libickiego),

---

[640] zob. Fuchs. Ch. *Implications of Deep Packet Inspection (DPI) Surveillance for Society*, publikacja Uniwersytetu w Uppsali w ramach projektu *"PACT-Public Perception of Security and Privacy:Assessing Knowledge, Collecting Evidence, Translating Research into Action"* finansowanego przez Komisję Europejską

[641] zob. Thompson L. *Cyber Alliances: Collective Defense Becomes Central To Securing Networks, Data*, Forbes (2014). par.par.4-6

[642] zob.Arquilla J., Ronfeldt D. *The Advent of Netwar*,RAND Corporation Santa Monica, (1996) s.94

[643] Przykładem powstawania norm prawa zwyczajowego w tym zakresie może być deklaracja podpisaną przez ponad stu sygnatariuszy z inicjatywy prezydenta Republiki Francuskiej E. Macrona, tzw.. *Paris Call for Trust and Security in Cyberspace* (2018), .

norma ta stanowi także ograniczenie możliwości ochrony suwerenności. Państwa stają bowiem przed wyborem reagowania na każde naruszenie, lub rezygnacji z obrony w zakresie, w jakim naruszony został element sieci należący do podmiotu prawnego. Możliwe są różne metody prowadzenia obrony pasywnej, jednak wszystkie one zamykają się w dwóch doktrynach sekurytyzacyjnych: sieci otwartej (kładącej nacisk na swobodę przesyłania danych) i sieci zamkniętej, zakładającej maksymalną możliwą kontrolę ruchu cyberprzestrzennego. Ta pierwsza koncepcja przyjmowana jest w Unii Europejskiej, druga natomiast w Stanach Zjednoczonych.

W grudniu 2018 roku, Parlament Europejski przyjął tekst propozycji unijnej regulacji cyberprzestrzennej[644]. czyli tzw. *Cybersecurity Act*. Należy zauważyć, że pomimo braku oficjalnej promulgacji przywołanego aktu prawnego, jest on uzgodniony przez Komisję Europejską oraz Parlament Europejski i Radę.[645] Celem tej regulacji ma być przede wszystkim uregulowanie bezpieczeństwa cyberprzestrzennego UE oraz doprecyzowanie podstaw prawnych funkcjonowania ENISA - unijnej agencji bezpieczeństwa wewnętrznego. Podstawowym celem promulgacji *Cybersecurity Act* jest uszczegółowienie obowiązującej już Dyrektywy w sprawie środków na rzecz bezpieczeństwa sieci.[646] Dyrektywa ta zakłada bowiem istnienie centralnej dla całej Wspólnoty agencji, mającej na celu obronę integralności sieci cybernetycznych UE. ENISA, powołana do życia w 2013 roku była dotychczas agendą o charakterze bliższym doradczemu, bez realnie określonego zakresu kompetencji.[647] *Cybersecurity Act* utrzymuje doradzanie organom UE jako jedno z podstawowych zadań ENISA[648], rozszerza jednak jej kompetencje na faktyczne działania na rzecz zwiększenia bezpieczeństwa sieci. Ta ostania kompetencja musi natrafić jednak na liczne problemy interpretacyjne. System bezpieczeństwa cybernetycznego UE budowany jest w oparciu o pośrednie regulacje i zasadę

[644] zob. IntrIs. File 2017/0225(COD), 15786/18 przyjęty 20 grudnia 2018 roku.Odpowiednie spotkanie COERPER odbyło się 19 grudnia 2018 roku

[645] zob. Komunikat prasowy Komisji Europejskiej EU Cybersecurity Act agreed! z 11 grudnia 2018 roku.

[646] Dyrektywa Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2018 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

[647] zob. Dyrektywa Parlamentu Europejskiego i Rady 460/2004

[648] zob. Art. 5 Cybersecurity Act

subsydiarności. Oznacza to, że państwa członkowskie powołane są do zorganizowania własnych zespołów CSIRT *(Computer Security Incident Response Team-Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego)*[649], które zobowiązane są do spełniania określonych w dyrektywie standardów.[650] Zawarcie tych regulacji w dyrektywie a więc w akcie prawa unijnego wiążącego państwa członkowskie pośrednio, ujmuje regulację standaryzacji *CSIRT* wyłącznie w sferze programowej. Regulacje zawarte w przywołanych powyżej załącznikach do dyrektywy powodują, że unifikacja dokonywana jest wyłącznie na najniższym możliwym poziomie. W istocie bowiem, każdy z *CSIRT* podlega prawom krajów członkowskich, brak też jakiejkolwiek regulacji ramowej, umożliwiającej *ENISA* samodzielne prowadzenie obrony unijnej cyberprzestrzeni (regulacje ramowe zawarte w prawie konstytuującym europejskie *CSIRT* określają rolę koordynacyjną w implementowaniu regulacji, zgłaszaniu incydentów i moderowanie wymiany doświadczeń pomiędzy poszczególnymi *CSIRT*). *ENISA* ma też wyłącznie pośredni, w istocie doradczy wpływ na legislację cyberprzestrzenną na szczeblu wspólnotowym.[651] Podobny kompetencje przyznawały też Agencji poprzednie regulacje unijne w tym zakresie. Należy także wskazać, że zwyczajowo rekomendacje ENISA były przyjmowane przez unijnych legislatorów. Poza tym uczestniczy ona w tworzeniu prawa unijnego (poprzez certyfikację systemów, jako zgodnych z minimalnym standardem bezpieczeństwa) a także wspomaganiu krajowych zespołów CSIRT.[652]

5. a. Struktura obrony pasywnej UE

Na poziomie unijnym nie istnieją uregulowania prawne dotyczące sprawowania kontroli nad podmiotami z sektora ISP. Nie promulgowano także żadnych wiążących bezpośrednio lub pośrednio państwa członkowskie przepisów, nakazujących

[649] zob. Art 9(1) Dyrektywy 2016/1148
[650] zob. Zał I (1) ,zał. II i zał. III do Dyrektywy 2016/1148
[651] zob. Art 4(3) Cybersecurity Act
[652] Zgodnie z normą art. 9(5) Dyrektywy 2016/1148 w związku z art.6(1)(c) Cybersecurity Act.

wprowadzenie podobnych przepisów do porządków krajowych. Przeciwnie, Dyrektywa Parlamentu Europejskiego i Rady regulująca unijny rynek usług elektronicznych zdejmuje implicite obowiązek wprowadzenia jakichkolwiek przepisów monitorujących działalność ISP w ich jurysdykcjach.[653] Nietrudno więc zauważyć, że sytuacja ISP nie jest w zakresie obrony cybernetycznej uregulowana na poziomie unijnym w sposób faktyczny. Do ISP odnoszą się wyłącznie normy programowe, takie jak przewidziana przez pkt (12) *Cybersecurity Act*[654] nakazujący zachęcanie[655] tych podmiotów do konstruowania swoich systemów w sposób bezpieczny i zakładający możliwość przeprowadzenia cyberataków. Wraz z przywołaną powyżej normą nie ustalono żadnych wytycznych czy standardów unijnych wskazujących, jakie systemy należałoby uznać za bezpieczne. Dodatkowo, pozytywnym przepisem wyłączone z jurysdykcji unijnej są także podmioty mające siedzibę w krajach nie będących członkami Unii[656], co należy uznać za niezrozumiałe, zwłaszcza wobec odwrotnego uregulowania sytuacji tych podmiotów w *GDPR*. Opisany powyżej stan prawny *de facto* oznacza, że zarówno przyznane *ENISA* przez *Cybersecurity Act* kompetencje kontrolne jak i ewentualne uprawnienia krajowych agencji tego typu nie mają zastosowania do prywatnych podmiotów, którymi są ISP. Brak bowiem możliwości prawnej (zarówno w prawie wspólnotowym jak w porządkach krajowych) zakazania lub ograniczenia zakresu działalności określonemu ISP, którego zabezpieczenia są nie wystarczające dla skutecznego wykonywania pasywnej obrony cybernetycznej.

5. b. Ograniczanie strat

Unia Europejska przyjmuje w swoim prawodawstwie uregulowaną rozporządzeniem Parlamentu i Rady zasadę "sieci otwartej", zwaną też "zasadą sieciowej

---

653 zob. Art. 15 Dyrektywy Parlamentu Europejskiego i Rady z 8 czerwca 2000 o niektórych aspektach... 2000/31/EC

654 (12) preambuły do *Cybersecurity Act*

655 *Should be encouraged*

656 ibid. Dyrektywa 2000/31/EC

neutralności".[657] Dla opracowania niniejszego istotne są dwie regulacje wynikające ze wspomnianego rozporządzenia. Pierwsza z nich gwarantuje tzw. użytkownikom końcowym prawo do swobodnego korzystania[658] z dowolnych usług i aplikacji niezależnie od miejsca docelowego położenia informacji, treści czy usługi. Druga wyłącza prawo prywatnych podmiotów (w tym *ISP*) do jakiejkolwiek ingerencji w transmisję, lub wyróżniania jakiegokolwiek przesyłu danych w jakikolwiek sposób.[659] Same te regulacje wystarczają, by uniemożliwić śledzenie pakietów danych na poziomie ISP. Należy zauważyć, że ze względu na rangę aktu, w jakim została ona sformułowana, także kraje członkowskie UE muszą dostosować do niej swoje krajowe porządki prawne. Wynika z tego, że aktualne uwarunkowania prawne wyłączają możliwość jakiegokolwiek analizowania kierunków przepływu pakietów danych w ramach elementów sieci terytorialnie poddanych jurysdykcji państw członkowskich UE, nawet jeżeli ruch ten pochodzi spoza granic tych jurysdykcji. Należy zauważyć, że nowelizacja rozporządzenia o dostępie do sieci zakładająca powstanie unijnego urzędu certyfikacji cybernetycznej, nie zmienia zasadniczo tej sytuacji ze względu na, określony w powołującym go rozporządzeniu, zakres uprawnień.

Podobnie państwa członkowskie UE nie mają żadnej możliwości wykonywania prewencyjnej kontroli ruchu we własnych sieciach krajowych. O ile nie stoi to oczywiście na przeszkodzie wykonywaniu kontroli pakietów (przykładowo w trakcie śledztwa policyjnego), kontrola ta nie może być wykonywana w żaden sposób w ramach obrony pasywnej. Europejskie *CSIRT* mają więc możliwość reagowania dopiero w momencie rozpoczęcia operacji przeciwko właściwemu celowi. Należy także pamiętać, że wczesne przeprowadzenie DPI pozwala na zmianę pakietu adresowego przesyłanych danych, a więc umożliwia *CSIRT* państwa będącego celem cyberoperacji na przekierowanie jej na serwery, w których nie będzie ona w stanie wyrządzić szkód.

---

[657] zob.art. 1 i Preambuła do Rozporządzenia Parlamentu Europejskiego i Rady 2015/2120 z dnia 25 listopada 2015 r. opublikowanego w Dzienniku Urzędowym UE, Dz.U. L 310 z dnia 26 listopada 2015, ss.1-18, nr CELEX:32015R2120

[658] ibid. Art. 3(1)

[659] ibid. Art. 3(3)

5. c. Struktura obrony pasywnej USA

Federalna obrona cyberprzestrzeni[660] opiera się na czterech podstawowych aktach prawnych[661]:

1. FISMA, czyli *Federal Information Security Management Act* z 2002 roku wraz z jego kompleksową nowelizacją dokonaną 12 lat później, tzw. *FISMA Act of 2014*[662]. Uzupełnieniem tego aktu prawnego jest sporządzona przez NIST[663] *Framework for Improving Critical Infrastructure in Cyberspace*.
2. *National Cybersecurity Protection Act of 2014(NCPA)*[664]- służący koordynacji sektora prywatnego i publicznego w zakresie cyberbezpieczeństwa;
3. *NCCIP-National Cybersecurity and Critical Infrastructure Protection (NCCIP)*[665]-precyzująca role współpracy sektorów publicznego i prywatnego w zakresie zgłaszania ataków na systemy prywatne sektorowi publicznemu i udoskonalanie polityk służących przeciwdziałaniu taki naruszeniom;
4. *Cybersecurity Enhancement Act of 2014*[666], regulujący promulgowania standardów obrony sieci przez Narodowy Instytut Standardów i Technologii, podlegających dobrowolnemu wdrożeniu w sektorze prywatnym

Poza regulacjami wskazanymi powyżej, podstawową rolę koordynacyjną pełni *Comprehensive National Cybersecurity Initiatve.*[667] Pełna lista zadań i zespołów

---

[660] Artykuł niniejszy, koncentruje się wyłącznie na cywilnej obronie cybernetycznej, pomijając kwestię związane z istnieniem amerykańskich wojsk cybernetycznych ze względu na brak ich unijnego odpowiednika.

[661] zob. także Pernik P., Wojtkowiak J., Verschoor-Kirss A.*National Cyber Security Organisation: United States* NATO Cooperative Cyber Defence of Excellence Tallinn, Estonia, (2015) s. 11-3

[662] Przyjęta 13 grudnia 2014 roku przez 113 Kongres P.L. 113-283, zmieniająca FISMA 2002, U.S.C. ch.35 t. 44

[663] National Institute of Standards and Technology.

[664] *National Cybersecurity and Communications Integration Centre Act of 2014* S.2519,(2014)

[665] *NCCIP ACT* z 27 czerwca 2014 roku. H.R. 3696, (2013)

[666] *Federal Cybersecurity Enhancement Act of 2015*, S.1869,(2015)

[667] Dalej powoływana jako CNCI. Powołana do życia w styczniu 2008 roku, dwiema tajnymi rozporządzeniami. National Security Presidential Directive-54 i Homeland Security Presidential Directive-23. Pomimo odtajnienia powołanych powyżej aktów założycielskich CNCI, większość informacji jej dotycząca pozostaje utajniona, w

działających wewnątrz CNCI podlega utajnieniu,[668] jednakże ujawnione treści dotyczące tej instytucji[669] wskazują, że jej podstawowym zadaniem jest bezpośrednie wpływanie na zdolności obronne infrastruktury cyberprzestrzennej USA i koordynowanie pozostałych podmiotów służących temu celowi, w tym pozostałych agend rządowych.[670] CNCI ma więc realne możliwości działania, na przykład poprzez koordynowanie i stawianie zadań cywilnym agencjom kontrwywiadowczym, zarówno w sensie programowym jak i w zwalczaniu określonych, istniejących już zagrożeń, w tym dla sektora prywatnego. Drugim z sieciowych zespołów, tym razem podległym DHS[671], a służącym do koordynacji działania na poziomie łączącym kontrwywiad, działania policyjne i sektor prywatny, jest *National Cybersecurity and Communications Integration Center*.[672]

Rynek ISP został otwarty dla podmiotów prywatnych dopiero w 1991 roku.[673] Podmioty te wraz z otwarciem rynku dostawców internetowych uzyskały względną swobodę. Podobnie jak w Unii Europejskiej, nie są one w żaden sposób uregulowane w zakresie minimalnego wymaganego stopnia zapewnianego bezpieczeństwa. Jednakże NCPA wymaga od podmiotów ISP, zarówno prywatnych jak i państwowych, dostosowywania się do wytycznych dotyczących bezpieczeństwa sieci opracowanych przez wyspecjalizowane agendy DHS, zajmujące się koordynacją bezpieczeństwa cybernetycznego. W przeciwieństwie do rekomendacji czy nadzoru *ENISA*, rządowe wytyczne dotyczące obrony cybernetycznej są wiążące także dla podmiotów prywatnych. Dodatkowo, w przeciwieństwie do regulacji europejskich, zasoby prywatnych ISP mogą być wykorzystane przez agencje rządowe w dowolnym

związku z czym nie ma możliwości przeprowadzenia pełnej analizy prawnej tej instytucji.

668 zob. także Rollins J., Henning A.C. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, Congressional Research Service,(2009) s.5

669 Transkrypcje dyrektyw NSPD-54 i HSPD-23, zostały odtajnione decyzją prezydenta Baracka Obamy w 2014 roku.

670 zob. Pernik,Wojtkowiak,Verschoor-Kirss *A National...* s.10

671 Department of Homeland Security

672 Powstały na mocy Dyrektywy Prezydenta NSC-63,cytowanej w wydawnictwie Białego Domu *Cyberspace Policy Review:Assuring a Trusted and Resilient Information and Communications Infrastructure* z 2009 roku.

673 por. Lewis P.H. *U.S. Beigns Privatizing Internet's Operations,* The New York Times z 24 października 1994 roku.

czasie, bez dodatkowych wymogów prawnych.[674] W Kongresie Stanów Zjednoczonych natomiast trwają dyskusje nad nałożeniem na wszelkie podmioty prowadzące działalność jako ISP prawnego obowiązku prowadzenia analiz pozwalających na przeciwdziałanie tak zwanym *spoof addresses*.[675]

5. d. Ograniczanie strat

Agencje powołane do kontroli bezpieczeństwa amerykańskich sieci mają uprawnienia do prowadzenia prewencyjnej *DPI*. *CIO* aktualnie jest w trakcie wprowadzania obejmującego cały ruch sieciowy programu *EINSTEIN*, pozwalającego na prowadzenie *DPI* i łączenie adresów użytkowników końcowych z bazami danych prowadzonymi przez federalne agencje bezpieczeństwa.[676] Umożliwia to zarówno monitorowanie jak i przekierowywanie nieautoryzowanych wejść do systemu, śledzonych od samego wejścia do systemu na mocy *Trusted Internet Connection Initiative*. Istniejące regulacje cyberprzestrzenne nakładają prawny nakaz wymiany informacji o atakach przeprowadzanych przeciwko sieciom znajdującym się na terytorium USA, nie tylko między sobą, ale także, co najbardziej istotne, z odpowiednimi organami federalnymi powołanymi do zwalczania cyberprzestępczości, nawet tej która nie narusza poziomu użycia siły i nie stanowi ataku. Pozwala to na użycie zespołów *CSIRT* do ochrony cywilnych sieci, które mogą zawierać informacje lub odgrywać kluczową rolę w działaniu infrastruktury niestrategicznej.

---

[674] Chodzi tu o tzw. *Trusted Internet Connections Initiative*, działającą w oparciu o sekcję 702 *FISA Amendment ACT* z 2008 roku. zob. także Rowe B., Wood D., Reeves D.,Braun F. *The Role of Internet Service Providers in Cyber Security*, publikacja *Institute for Homeland Security Solutions,* San Francisco (2011)

[675] A więc o sfałszowane dane lokalizacyjne, służace ukryciu tożsamości użytkownika.

[676] zob. Raport *Deep Packet Inspection (DPI): U.S. Governement Market Foreast 2019-2024, Tabular Analysis,* Market Research Media (2018) s.12

5. e. Podsumowanie

Podstawowym wnioskiem płynącym z porównania systemów cybernetycznej obrony pasywnej UE i USA jest różnica w decyzjach sekurytyzacyjnych obydwu podmiotów. USA niewątpliwie konstruują swoje działania w sposób gwarantujący dużo dalej idące bezpieczeństwo własnych sieci, nawet za cenę zwiększenia kontroli nad cywilnym ruchem w Internecie i pozostałych globalnych sieciach wymiany danych. Co istotne, USA konsekwentnie wykonują swoją jurysdykcję w zakresie cyberbezpieczeństwa wobec podmiotów fizycznie znajdujących się poza ich jurysdykcją, nawet w sytuacjach które nie uzasadniają zastosowania jurysdykcji nadzwyczajnej. UE podobne mechanizmy stosuje niekonsekwentnie, nakładając podobne obowiązki w ramach ochrony danych i *GDPR*, natomiast w żaden sposób nie kontrolując *ISP*, które jednocześnie pozostają poza granicami Unii i umożliwiają przesył pakietów danych do jej sieci. Nie może być wątpliwości, że wobec istotności naruszeń suwerenności na poziomie poniżej użycia siły i wskazanego przez Libickiego ograniczenia siły cybernetycznej obrony pasywnej do siły najsłabszego elementu sieci, z punktu widzenia suwerenności państwowej słuszniejsza jest koncepcja sieci zamkniętej.

Niezależnie jednak od przyjętej koncepcji obrony, obrona pasywna i *detterence by denial* stanowić będzie podstawowy środek ochrony suwerenności przed jej naruszeniami operacjami *ISR* i *CNE.* Wynika to z faktu, że zastosowanie któregokolwiek z remediów aktywnych dotyczących naruszenia suwerenności wymaga wykrycia źródła ataku i dokonania precyzyjnej atrybucji, która w cyberprzestrzeni może zostać łatwo dokonana błędnie. Nie ma wątpliwości, że odpowiedź skierowana przeciwko stronie, która nie dokonała operacji jest uznawana za czyn bezprawny. Należy także wspomnieć, że wymaganie identycznych stopni pewności dla wykonania odpowiedzi na atak w cyberprzestrzeni wyłączałoby w praktyce możliwość jej dokonania.[677] Analizy wskazują, że około 1/3

[677] Szacuje się , że prawidłowość przypisania operacji dokonywanej w cyberprzestrzeni to około 70-80 procent. Dla porównania ataki przy pomocy rakiet, przypisywane są

użytkowników potrafi sfałszować swoją tożsamość internetową w sposób uniemożliwiający jej ostateczne rozpracowanie.[678] Jest oczywiste, że rozkład grup posiadających podobne możliwości nie jest równy w populacji. Istnieje bowiem potencjalna możliwość wystąpienia dwóch sytuacji. Pierwsza to możliwość wykonania odpowiedzi wobec podmiotu, którego tożsamość została skradziona. Druga, to kwestia statusu podmiotu, którego tożsamość została skradziona. Dodatkowym problemem jest podział atrybucji na przypisania czysto techniczne - określonych działań do określonych urządzeń komputerowych i atrybucję osobową, polegającą na przypisaniu określonym osobom (a co za tym idzie podmiotom prawa międzynarodowego) określonego działania lub zaniechania.[679] Co do obydwu opisanych powyżej wątpliwości, brak zarówno wyraźnej praktyki międzynarodowej jak i *opinio iuris*[680] Pewnym rozwiązaniem tej kwestii mogłoby być powołanie postulowanego przez część doktryny specjalnego organu międzynarodowego wyspecjalizowanego w dokonywaniu atrybucji czynów zabronionych międzynarodowo w cyberprzestrzeni.[681]

Doktryna prawa międzynarodowego stoi na stanowisku, że w przypadku działań cyberprzestrzennych o zakresie niższym niż użycie siły, należy przyjąć odpowiedzialność państwa za czyn zabroniony, *internationally wrongful act* w rozumieniu ARSIWA.[682] Taką interpretację przyjął także Departament Obrony USA.[683] Rząd tego państwa identyczne stanowisko skierował następnie do

właściwym wykonawcom w więcej niż 98 przypadkach na 100. por. Klimburg. A. *The Darkening Web*... s.142

[678] zob. Beverly R., Berger A., Hyun Y., Claffy K. *Understaning the efficacy of deployed Internet source address caldation filtering*[w: *Proceedings of the 9th ACM SIGCOMM Conference on internet Measurement Conference,* Chicago (2009) ss.20-5]

[679] zob. Także Corn P.G., Talyor R., *Soveregnity in the Age of Cyber* [w: zbiorowa, red. Corn P.G., Taylor R. *Symposium on Sovereignty, Cyberspace and Tallin Manual 2.0*The American Society of International Law, American Journal of International Law Unbound 111 (2017)] ss.208-11

[680] Egan B. *International Law and Stablity in Cyberspace* raport doradcy prawnego Departamentu Stanu USA.

[681] zob. Klimburg *Darkening...* s.332

[682] International Law Commision Articles on Responsiblity of States for Internationally Wrongful Acts, przyjęte na 53 sesji Komisji w 2001 roku, publikowane jako aneks do rezolucji Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych 56/83, (2001)

[683] por. Department of Defense, Office of Gen. Counsel *An Assesment of International Legal Issues in Information Operations* wyd. 2 ,(1999).

eksperckiej grupy rządowej Narodów Zjednoczonych do spraw telekomunikacji.[684] Wskazano tam, że o ile większość działań w cyberprzestrzeni podejmowanych przez państwa nie ma wystarczających skutków by uznać je za użycie siły, nie oznacza to, że nie podlegają one rządom *inter alia* ogólnych zasad prawa międzynarodowego dotyczących suwerenności, praw człowieka czy właśnie normom regulującym odpowiedzialność państw za działania bezprawne, w szczególności ARSIWA. Stanowisko takie podtrzymuje także Komisja Ekspertów stanowiąca zespół tworzący TM, jak i sam kierownik Komisji.[685] Michael Schmitt wskazuje wprost, że w jego opinii nie ma możliwości, by społeczność międzynarodowa tolerowała "Dziki Zachód", którym *de facto* jest regulacja prawnomiędzynarodowa wszystkich operacji cybernetycznych, naruszających suwerenność państwa, a nie wywołujących skutków, które uzasadniałyby uznanie danej operacji za użycie siły.[686] Z teoretyczno-prawnego punktu widzenia, stanowisko takie stwarza wrażenie oczywistego. Argumentacja ta wynika bowiem z ugruntowanego pojmowania zasady zakazu interferencji (*non-interference prinicple*)[687] w związku z przyjmowaną w ARSIWA definicją czynu zabronionego (*internationally wrongful act)*[688], według której każde możliwe do przypisania danemu państwu naruszenie jego zobowiązań międzynarodowych, należy uznać za czyn zabroniony.[689] Jednak nawet na gruncie czysto teoretycznym, powyższa argumentacja nie może być uznana za niekwestionowaną. Należy tu przede wszystkim wskazać na deklarację sędziego MTS, Bruno Simmy dotyczącą zasady *Lotus*.[690] Wskazał on, że zasada wynikająca z orzeczenia *Lotus*, mówiąca że nie

---

[684] UN Group of Governmental Experts on Developments in the Field of Informations and Telecommunications in the Context of International Security (GDE).

[685] zob. Schmitt M., Vihul L. *Respect for Sovereignty in Cyberspace* Texas Law Review 7:95 (2018) ss.1640-5

[686] ibid.

[687] Zakaz interferencji, pomimo rozpowszechnionego a błędnego użycia wymiennie z zasadą nie-interwencji (*non-intervention principle)* należy pojmować szerzej, jako całkowity zakaz (z wyjątkiem kontratypów) wpływania na wewnętrzne sprawy podmiotu prawa międzynarodowego, niezależnie od poziomu użytej siły.
zob. Ramcharan R. *ASEAN and Non-interference: A Principle Maintained* [w: Contemporary South Asia22:1, ISEAS- Yousof Ishak Institute(2000) s.60-88]; także Katsumata H. *Form "Non-interference" to "Open and Frank Discussions"* Asian Survey, 44:2 (2004) ss.240-5

[688] Art. 2 *ARSIWA*

[689] zob. Komentarz do art. 2 ARSIWA,ILC... ; par. 1 i 3.

[690] por. Simma B. *Unilateral Declaration on Lotus Principle [w: Accordance with*

wolno nakładać na państwa domniemanych ograniczeń suwerenności, oparta o zasadę konsensualności prawa międzynarodowego publicznego, jest zasadą przestarzałą i w gruncie rzeczy niemożliwą do stosowania w dzisiejszym świecie. Sędzia Simma wskazuje też, że możliwe jest milczenie prawa międzynarodowego o danej kwestii,[691] w przeciwieństwie do twierdzenia MTS w opinii dotyczącej Kosowa, podtrzymującego zasadę mówiącą, że to co nie jest wyraźnie zakazane musi być dozwolone w obrocie międzynarodowoprawnym. Przyjęcie tej argumentacji wyłączałoby konieczność uznania operacji *CNE* i *ISR* za czyny zabronione na gruncie ARSIWA. Możliwe byłoby bowiem przyjęcie, że prawo międzynarodowe o nich milczy. Coraz częściej pojawiają się w doktrynie głosy, wskazujące na konieczność uznania prowadzenia operacji wywiadowczych w czasie pokoju za normalne i uregulowane prawnomiędzynarodowo narzędzie dostępne państwom, ze względu właśnie na wyjątki od zasady nie-interwencji już obecne w prawie międzynarodowym, jak choćby konieczność zapobiegania aktom terroryzmu.[692]

Innym rozpowszechnionym poglądem doktryny jest założenie, że sam fakt zbierania informacji nie może być uznany za czyn zabroniony, tym samym więc nie może być uznany za naruszenie suwerenności danego państwa, o ile sposób tego zbierania fizycznie jej nie narusza (a więc na przykład jest dokonywany przy pomocy okrętów rozpoznania elektronicznego, pozostającego na wodach międzynarodowych).[693] Część doktryny ze sposobu traktowania szpiegostwa wywodzi jego "cichą legalność",[694] wywodząc to z rozbieżności pomiędzy prawem międzynarodowym publicznym i krajowym, które dopuszcza niekaranie państw za szpiegostwo, przy jednoczesnym wymierzaniu wyroków karnych jednostkom, które na zlecenie tych państw tego szpiegostwa dokonywały i wskazując że logiczną

International Law of the Unilateral Declaration of Indepedence by the Provisional Instituion of Self-Government of Kosovo, Advisory Opinion, 2010 ICJ nr 141], także zdanie odrębne sędziego Simmy [w: *Kosovo...* , ICJ Summary s.17]

[691] zob. Opinia *Kosovo...* par. 122

[692] zob. Demarest G.B. *Espionage in International Law* Denver Journal of International Law and Policy24:321 (1995-96)

[693] Tak na przykład McDougal M., Burke W. *The Public Order of the Oceans: A Contemporary International Law of the Sea* Yale University Press 54:1 (1965) ss.747-51

[694] zob. McDougal M.S. *The Intelligence Function and World Public Order* Temple Law Quaterly 46, Yale Law School Faculty Scholarship Series (1972) s. 2569

sprzecznością jest jednoczesne uznawania za legalne karanie za czyn w ramach krajowego prawa publicznego i ignorowanie braku uznania takiego samego albo wręcz tożsamego w sensie prawnym czynu za delikt prawa narodów.[695] Jak wskazano powyżej, konstrukcje prawne dotyczące szpiegostwa dają podstawę do przeprowadzenia analogii z operacjami cyberprzestrzennymi poniżej poziomu użycia siły. Co więcej, konieczne jest wskazanie jeszcze jednej wątpliwości co do wywodów wskazujących że naruszenia cyberprzestrzenne stanowią *delictum iuris gentium.* Art 2 ARSIWA mówi wyraźnie o możliwości przypisania jako przesłance koniecznej do stwierdzenia zaistnienia złamania prawa międzynarodowego. Co istotniejsze, interpretacja systemowa tego przepisu i umieszczenie tej przesłanki w przepisie określającej definicję legalną deliktu każe przyjąć, że zamysłem Komisji było nie tyle swoiste domniemanie niewinności w stosunku do podmiotów prawa międzynarodowego, a konstruowanie deliktu jako działania, które bez wątpliwości można przypisać państwu. Wobec praktycznej niemożliwości dokonania atrybucji w cyberprzestrzeni wątpliwe staje się, czy jakiekolwiek działania w cyberprzestrzeni można uznać za spełniające definicję legalną z *ARSIWA*. Nawet bowiem te działania, które przypisać się uda, najczęściej zostaną przypisane grupom indywidualnych osób, których związków z danym państwem będzie bardzo trudno dowieść. Pośrednio więc można założyć, że sama konstrukcja definicji deliktów międzynarodowych wyłącza z nich działania w cyberprzestrzeni. Nie zmienia tego stanu rzeczy nawet art. 8 *ARSIWA*, który przyjmuje możliwość przypisania państwu odpowiedzialności za działania czynników poza jego bezpośrednią kontrolą. Jak wskazuje bowiem ILC w komentarzu do *ARSIWA*, przypisanie państwu odpowiedzialności za działania osób nie pozostających pod bezpośrednią kontrolą tego państwa możliwe jest wyłącznie przy spełnieniu tych samych kryteriów, który do atrybucji odpowiedzialności przyjęły Międzynarodowy Trybunał Sprawiedliwości i Międzynarodowy Trybunał Karny do spraw byłej Jugosławii odpowiednio w sprawach *Nicarauga*[696] i *Prokurator v.*

[695] ibid.
[696] *Nicarauga...* par. 14

Tadic[697]. W odniesieniu do cyberprzestrzeni zasady te zostaną omówione poniżej, natomiast w tym miejscu wystarczy wskazać, że obydwa te orzeczenia przyjmują, że udział państwa w danej operacji musi być wyższy niż finansowanie i przygotowanie operacji[698], a kontrola musi być wykonywana bezpośrednio przez państwo i obejmować etap planowania i udziału w wykonywaniu.[699] Nawet w przypadku niewątpliwego zaangażowania państwa w operacje cyberprzestrzenne, sam charakter ich operacji a także wysoki stopień samodzielności osób faktycznie je przeprowadzających wyłącza możliwość spełnienia tych kryteriów, a co za tym idzie przypisanie na gruncie *ARSIWA*.[700] Niewątpliwie pogląd sędziego Simmy wyrażony w przywołanej wyżej opinii o możliwości milczenia prawa międzynarodowego publicznego można zastosować do zakresu operacji cyberprzestrzennych nie przekraczających progu użycia siły. Podobny pogląd wyrażało dwóch doradców prawnych Departamentu Obrony USA, przyjmujących, że dopiero dalszy rozwój *opinio iuris*, zwyczaju i praktyki pozwoli określić czy w ogóle i kiedy dokładnie takie operacje łamią suwerenność państwa.[701] Nie można więc przyjąć, że istnieje regulacja międzynarodowa - czy to zwyczajowa czy *black-letter law* regulująca cyberoperacje poniżej poziomu użycia siły. Możliwe jest oczywiście, że taka regulacja powstanie w przyszłości, choćby w drodze ukonstytuowania się jakiegoś jednorodnego zwyczaju pozwalającego na stworzenie prawa zwyczajowego w tym zakresie. Do tego momentu konieczne jest przyjęcie, że prawo międzynarodowe milczy w opisywanym tu zakresie. Nie oznacza to jednak, że ten nie podlega żadnym normowaniom. Podlega normowaniu faktycznemu, tak jak cała cyberprzestrzeń. Wyjątkiem od zakresu powyższych rozważań będą oczywiście operacje o intensywności poniżej granicy użycia siły, a przekraczające zakres dozwolonej interferencji w sprawy wewnętrzne państwa. Najczęstszym przykładem są ataki

---

[697] *Prosecutor v. Tadic* International Criminal Tribunal for the former Yugoslavia IT-94-1

[698] zob.*Nicaragua...* Awards. par.86

[699] zob.*Prosecutor v. Tadic...* Judgement par. 117

[700] por. Komentarz do art. 8 ARSIWA, sporządzony przez ILC par 3 i n.

[701] Corn P.G., Talyor R., *Soveregnity in the Age of Cyber* [w: zbiorowa, red. Corn P.G., Taylor R. *Symposium on Sovereignty, Cyberspace and Tallin Manual 2.0* The American Society of International Law American Journal of International Law Unbound 111 (2017)]str. 207-12

cybernetyczne na systemy zarządzania państwem, często dotyczące wyborów czy referendów.[702] Nie ma wątpliwości, że działania takie naruszają suwerenność i spełniają materialną przesłankę przewidzianą przez art. 8 ARSIWA.[703] Identyczny problem, jak w przypadku działań wojennych, będzie dotyczył przesłanki formalnej, czyli problemu atrybucji. Jednak ten zakres działań nie jest przedmiotem dotyczącym *ius in bello* i w tym rozdziale zostaje wyłącznie wskazany dla kompletności wywodu.

Jak wskazano powyżej, nie ma możliwości innego normowania *ius in bello* niż normowania systemowe.[704] W celu przeprowadzenia analizy takiego normowania, konieczne jest przeanalizowanie zasad prawnych dotyczących operacji militarnych poniżej i powyżej poziomu użycia siły przeprowadzanych przy pomocy środków kinetycznych a także przeanalizowanie, w jaki sposób mogą one funkcjonować w informatycznej części cyberprzestrzeni, oraz do jakiego stopnia, oparte o nie normowanie może wpływać na zmianę warunków w niej panujących.

---

[702] por.Ohlin J.D. *Did Russian CyberIntefererence in the 2016 Election Violate International Law?* Texas Law Review 15:79 (2017) ss.3-7

[703] Corn. G., Taylor, R. *Sovereignity in the Age...* ss.212-3

[704] por. Lessig L. *The Laws of Cyberspace* Jack N. and Lillian R. Berkman Center, Harvard Law School, Taiwan Net 98 (1998) ss.3-7.

IV. Prawo konfliktu cyberprzestrzennego

Prawo konfliktów zbrojnych co do zasady nie różnicuje naruszeń suwerenności ze względu na pole, na jakim zostało ono dokonane, uznając suwerenność za jednolitą. Niezależnie więc od tego, jakie interesy państwa zostały zaatakowane - działania te normuje właśnie ta dziedzina prawa. Cyberprzestrzeń stanowi jednak od tej zasady wyjątek. Wynika on z opisanych powyżej jej podziałów. Poszczególne pola prowadzenia konfliktu w cyberprzestrzeni będą regulowane przez różne systemy prawne - zależnie od tego, którą z części cyberprzestrzeni obejmą. Atak na części fizyczne będzie regulowany co do zasady normami prawa konfliktów zbrojnych (ponieważ celem ataku będzie infrastruktura zlokalizowana terytorialnie). Atak na terytorialne strefy cyberprzestrzeni będą regulowały także normy dotyczące prawa konfliktów zbrojnych, ale wraz z *lex informatica*. Elementy cyberataku wykonywane w części stanowiącej *commons* natomiast regulować będzie *lex informatica* w drodze afordancji (choć niektóre z tych działań będą mogły wywołać także skutki prawne znane tradycyjnemu prawu międzynarodowemu).

Z powyższych przesłanek wynika więc wniosek, że w drugim i trzecim ze wspomnianych przypadków *lex informatica* w zakresie dotyczącym cyberataków stanowić będzie zespół *leges speciales* do norm obowiązujących ogólnie. Wyjątkiem wydają się być wyłącznie instytucje prawa międzynarodowego dotyczącego konfliktów zbrojnych i wymagające uprzedniego wyrażenie woli przez państwa, jak przykładowo zastosowanie tzw. klauzuli *opt-out,*[705] pozwalającej państwom przystępującym do Międzynarodowego Trybunału Karnego na wyłączenie własnej zbrodni agresji spod jurysdykcji Trybunału.[706] Jej zastosowanie wymaga bowiem złożenia odpowiedniego oświadczenia przez dane państwo. Wydaje się, że instytucje takie nie mają zastosowania do elementów cyberataków dokonywanych w części cyberprzestrzeni stanowiącej *commons*, ze względu na brak możliwości złożenia

[705] zob. Art. 124 Statutu Rzymskiego

[706] zob. Hendry J. *Analysis: Activating the jurisdiction of the International Criminal Court over the Crime of Aggression*, Phillip Hirsch Institute (2018) s.1.

w tym zakresie wiążących oświadczeń woli z powodów formalnoprawnych, jak i ze względu na wyłączające jasny podział jurysdykcyjny zasady wszechobecności i niemożliwości fizycznego zlokalizowania cyberprzestrzeni. Ostatnią trudnością jest fakt, że wspomniane oświadczenie może być przez państwo, które je złożyło odwołane w dowolnym momencie.[707]Poniżej zostaną opisane główne instytucje prawa konfliktów zbrojnych istotne dla cyberprzestrzeni, wraz z odpowiadającymi im normami szczegółowymi, a także normami wynikającymi z normowania faktycznego i *lex informatica.*

1. Ius ad bellum - prawo do wojny w cyberprzestrzeni

Fundamentalną kwestią dla rozważań prowadzonych w pracy niniejszej jest znalezienie odpowiedzi na pytanie, czy istnieje pozytywne prawo podmiotów prawa międzynarodowego do prowadzenia wojny elektronicznej. Podobnie jak w wielu innych przypadkach tworzącego się prawa cyberprzestrzeni, zasada prawa do "wojny cyfrowej" przejęta została w drodze analogii z tradycyjnego prawa narodów. Łatwo zauważyć, że w prawie cyberprzestrzeni jej znaczenie znacznie zbliża się do roli, jaką odgrywała ona w *ius gentium* historycznie. *Ius ad bellum* w dawnych poglądach doktryny prawa międzynarodowego było jednym z przejawów suwerenności państwa. Władca w pełni suwerenny mógł decydować o prowadzeniu wojny; wasal mógł wyłącznie pomagać suwerenowi, który wojnę prowadził. Nie oznaczało to jednak, że prawo to nie było ograniczone. Historycznie, prawo międzynarodowe aż do XIX wieku, rozróżniało wojnę sprawiedliwą od wojny niesprawiedliwej, przyznając legalność wyłącznie tej pierwszej.[708] Wojna niesprawiedliwa była uważana za przestępstwo międzynarodowe.[709] Pierwszy proces za wojnę agresywną odbył się 26 października 1269 roku i zakończył skazaniem króla Conradina, który według

[707] zob. Karska E. *Dorobek Konferencji Rewizyjnej Statutu MTK ze szczególnym uwzględnieniem poprawki definiującej zbrodnię agresji*, Kwartalnik Prawa Publicznego 10-3 (2010) s.23

[708] zob.Simon H. *The Myth of Liberum Ius ad Bellum: Justifying War in 19th Century Legal Theory and Practice*, European Journal of International Law 29:1 (2018) ss.113-7

[709] ibid. s. 114

sentencji wyroku "bezprawnie podniósł broń" (*arma non licita induit)*.[710] Następnym istotnym historycznie przypadkiem skazania za prowadzenie wojny napastniczej był przypadek Napoleona Bonaparte, który w deklaracji Kongresu Wiedeńskiego[711] został uznany za "wichrzyciela i wroga pokoju światowego" który "zniszczył jedyny tytuł prawnego swojego istnienia[712]"a także został" wyjęty spod prawa",. Pomijając, że wspomniana deklaracja była wyłącznie polityczną i nieokreślone jest jej znaczenie prawne, należy zauważyć, że została ona wykonana, a jej zasadność nigdy nie była kwestionowana przez społeczność międzynarodową. Skazanie Napoleona na zesłanie na wyspę św. Heleny jest współcześnie interpretowane w taki sposób, że skazanie to było wyłącznie zachowaniem politycznym, swoistym środkiem zapobiegawczym przed wszczęciem przezeń kolejnej wojny europejskiej.[713]

Zwolennicy wspomnianej tezy wskazują, że skazanie na zesłanie nie było karą za prowadzenie wojny agresywnej, a wyłącznie za złamanie traktatu, według którego Napoleon miał pozostać w areszcie domowym na Elbie.[714] Nie sposób się zgodzić z tą tezą. Po pierwsze, złamanie konwencji nakazującej pozostawanie w określonym miejscu nie może być uznane za czyn zagrożony karą, można by sobie wyobrazić, choć raczej czysto teoretycznie, odpowiedzialność cywilną za tego typu naruszenia porządku prawnego. Po drugie, nie ma możliwości interpretowania wspomnianego traktatu, nakładającego na Napoleona obowiązek przebywania na Elbie, w oderwaniu od przyczyny nałożenia tego obowiązku, a taką przyczyną było właśnie prowadzenie wojen napastniczych. Zesłanie na św Helenę po ucieczce i wydarzeniach Stu Dni musi być w tym świetle interpretowane jako kontynuacja, w praktyce bliższa nadzwyczajnemu zaostrzeniu kary orzekanej recydywiście, niż ukształtowaniu

---

[710] zob. Rosario G.*Bibliotheca Scriptorum Qui Res in Sicila Gestas Sub Aragonum Imperio Retulere* wyd. Ex Regio Typogrpheo 9:27 (1873), digitalizacja Bayerische StaatsBibliothek

[711] *Deklaracja mocarstw uczestniczących w Kongresie Wiedeńskim z dnia 13 marca 1815 roku* British and Foreign State II. 663. Digitalizacja dokonana na Uniwersytecie Harvarda.

[712] *[...] thus violationg the Convention which established him in the Island of Elba[...]*(w ten sposób łamiąc postanowienia konwencji, które umieściła go na wyspie Elbie); chodzi tu o powrót do Francji podczas Stu Dni.

[713] por. Grzebyk P. *Criminal Responsibility for the Crime of Aggression* Routledge Taylor and Francis Group (2013) s. 132

[714] Hathaway O., Shapiro S.J., *How a radical plan to outlaw war remade the world,* Simon and Schuster Nowy Jork wyd 1 (2017) .s.251

stosunków prawnych w jakiś nowy sposób, jak chcieliby zwolennicy przywołanego wyżej poglądu. Przemawia za tym nie tylko fakt, że prawo do współcześnie pojmowanej obrony procesowej nie było w tamtych czasach oczywistością (co wyjaśniałoby brak procesu) ale też uznanie Napoleona za wyjętego spod prawa, pojmowanego zupełnie dosłownie. Należy też pamiętać, że doktryna prawa międzynarodowego dopuszczała w określonych wypadkach wymierzanie sprawiedliwości notorycznie łamiącym prawo międzynarodowe bez przeprowadzania procesu.[715]

Współczesne prawo międzynarodowe niewątpliwie *ius ad bellum* ogranicza. Zasada ta doznaje znaczących ograniczeń ze względu na przyjmowany nieomal bez wyjątków przez społeczność międzynarodową zakaz prowadzenia wojny i stosowania siły zbrojnej do rozstrzygania sporów międzynarodowych, wynikający choćby z Karty Narodów Zjednoczonych[716] i prawa zwyczajowego[717]. Niewątpliwie, ta zasada stosuje się do takich cyberoperacji, które stanowią ekwiwalent kinetyczny działań wojennych lub wspierania za pomocą środków cyberprzestrzennych nielegalnych działań wojennych. Powstaje jednak pytanie o istnienie prawa do wojny ściśle elektronicznej, rozumianej jako intencjonalne naruszenie suwerenności państwa trzeciego, w stopniu przekraczającym stopień użycia siły, jednakże bez ekwiwalencji kinetycznej. W tym zakresie, praktyka międzynarodowa zdaje się skłaniać ku opisanej powyżej koncepcji historycznej, z tą różnicą, że nie stanowi ona już wyłącznie przejawu suwerenności państwa, ale także staje się *sui generis* prawem także aktorów niepaństwowych. Wydaje się więc, że takie operacje mogą stanowić cyberprzestrzenne odpowiedniki *border clashes* w konfliktach fizycznych[718], które w rozumieniu prawa międzynarodowego publicznego nie kwalifikują się prawnie jako użycie siły zbrojnej (pomimo faktycznego charakteru działań zbrojnych) ze względu

[715] Tak na przykład Glueck Sh. *Crimes Against Humanity* [w: zbiorowa, red. Mettraux G. *Perspectives on Nuremberg Trials*,Oxford University Press (2008)] s. 72

[716] por. Art. 2(4) Karty, wskazujący, że wszyscy członkowie ONZ mają wyrzec się wojny jako środka prowadzenia spraw międzynarodowych.

[717] zob. Wright Q. *The Concept of Agression in International Law*, The American Journal of International Law 29:3 (1923) ss.373, także Sellars K. *Delegimitizing Aggression: First Steps and False Starts after the First World War,* Journal of International Criminal Justice 10:1 (2012) ss.7-13

[718] *Nicaragua...* par.117

na niewielką skalę działań. Ze względu na ogólne poddanie tego typu operacji *lex informatica* (wynikające z faktu ograniczenia jej zakresu do informatycznej części cyberprzestrzeni), opartej o zasadę *ex aequo...,* zasadne wydaje się przyjęcie do opisanego zakresu operacji wspomnianych analogii historycznych i w konsekwencji uznanie, że istotą uznania legalności wojny cybernetycznej są osiągane przez takie działanie cele.

Oczywiście normę taką należałoby uznać za *lex specialis* wobec regulacji generalnie zakazujących wojny w stosunkach międzynarodowych. Stosowałaby się ona wyłącznie do działań pozbawionych skutków kinetycznych. Takie rozumienie prawa do wojny (wyłącznie) cyberprzestrzennej zdaje się potwierdzać praktyka międzynarodowa Niekinetyczne ataki spotykają się najczęściej z podobną odpowiedzią ze strony państw, które podlegały takim operacjom, nie zaś odpowiedziom kinetycznym lub prawnym (jak na przykład skargom do trybunałów międzynarodowych, czy wnioskom o interwencje kierowanym do Rady Bezpieczeństwa ONZ).[719] Operacje niekinetyczne stają się także częstym środkiem ochrony interesów państwowych. Podstawowym problemem uznania takiej ograniczonej wojny cybernetycznej za legalną staje się atak, mogący mieć potencjalne konsekwencje kinetyczne, ale wyłącznie wobec określonego zachowania podmiotu zaatakowanego Znajduje się on pomiędzy etapami 2A i 2B według klasyfikacji konfliktów cybernetycznych CASCON[720]. Chodzi tu więc o etap cyberataku, który następuje po przełamaniu obrony systemu zaatakowanego (przy pomocy, ale przed wywołaniem jakichkolwiek skutków w świecie materialnym). Przykładem takiego ataku może być na przykład wirus *Stuxnet*, który doprowadził do wyłączenia irańskiego ośrodka wzbogacania uranu, stanowiącego część programu rozwoju broni nuklearnej tego państwa. Desynchronizacja wirówek mogła potencjalnie prowadzić do eksplozji - jednak skutki ataku cybernetycznego były widoczne dla operatorów

[719] por.Tanenbaum M. *Kinetic War vs. Cyber War: The Potential Battlefields Ahead*, MSSPALert, (2018) ss.2-3

[720] CASCON jest systemem oceny sytuacji podczas konfliktów, stworzonym przez profesora Lincolna Bloomfielda. zob. Także Bloomfield L.P. *Why Wars End: CASCON's Answers from History,* Millenium Journal of International Studies, London School of Economics,t.26 n.3 (1997) ss. 709-26

ośrodka wystarczająco wcześnie by wyłączyć wirówki zanim uszkodzenia stały się na tyle zaawansowane by doprowadzić do zniszczeń.[721] Dochodzi więc do sytuacji, w której skala skutków danego ataku (a tym samym skala naruszenia suwerenności) uzależniona jest wyłącznie od działań państwa zaatakowanego i w związku z tym - sytuacji, w której tak samo przeprowadzane ataki mogą dać różne skutki. Ponieważ wystąpienie lub brak skutków kinetycznych przesądzałby tu o pierwotnej legalności całej operacji, taki sposób prowadzenia konfliktów cyberprzestrzennych mieściłby się w założeniach *cyberlawfare*, umożliwiając obydwu stronom określenie stopnia eskalacji, a w konsekwencji znaczenia prawnego naruszeń i możliwej na nie własnej reakcji. Atak przy pomocy wirusa *Stuxnet* bowiem mógł, ale nie musiał wywołać skutki kinetyczne. Wydaje się, że fakt ten, w połączeniu z dużą łatwością z jaką uszkodzenia na etapie wyłącznie cyfrowym mogły zostać przez państwo zaatakowane wykryte (co z kolei oznaczało łatwość uniknięcia strat w świecie fizycznym), zmienił zdecydowanie zakres reakcji społeczności międzynarodowej na ów atak.

Była ona bowiem dużo łagodniejsza, niż reakcja na mające podobny cel, ale dokonywane w drodze ataków kinetycznych naloty izraelskich sił powietrznych skierowane przeciwko tym samym irańskim ośrodkom wzbogacania uranu.[722] Za uzasadnione należy więc uznać założenie, że wobec wojny cyberprzestrzennej o skutkach wyłącznie w jej informatycznej części, ograniczenie prawa do wojny jest znacząco mniej restrykcyjne niż w przypadku wojny konwencjonalnej, prowadzonej za pomocą środków kinetycznych lub wojny prowadzonej za pomocą środków cybernetycznych, ale prowadzących do skutków kinetycznych. *Ius ad bellum* w tym zakresie, podobnie jak w przypadku ogólnych norm *lex informatica* należałoby wyprowadzać z praktyki i normowania faktycznego. Zgodnie ze wskazanymi powyżej historycznymi przykładami - wykonywanie prawa do wojny cyfrowej byłoby uzależnione od przesłanek materialnych jej prowadzenia (a więc oznaczałoby to w praktyce przywrócenie opisanej powyżej historycznej instytucji wojny

[721] zob. Langner R. *To kill a centrifuge. A technical analysis of what Stuxnet's creators tried to achieve*, The Langner Group (2013) ss.4-5

[722] Które, pomimo nielegalności irańskiego programu nuklearnego(i potwierdzenia tego stanowisko przez Międzynarodową Agencję Energii Atomowej), wywołały reakcję nawet Rady Bezpieczeństwa ONZ. zob. Rezolucja RB ONZ 487 z dnia 19 czerwca 1981.

sprawiedliwej). Jak całe *lex informatica*, jest więc prawo do wojny elektronicznej oparte o zasady *ex aequo et bono*. Nie może natomiast być wątpliwości, że niesprowokowana agresja (nawet jeżeli wywiera ona skutki wyłącznie w cyberprzestrzeni i jest pozbawiona nawet pośredniego ekwiwalentu kinetycznego) nie może być uznana za zachowanie, które prawo powinno chronić. Należy też zauważyć, że rozwój działań cyberprzestrzennych, redefiniował jeszcze inny aspekt *jus ad bellum*. Prawo do wojny było dotychczas w sposób niekwestionowany wyłączną domeną państw.[723] Tymczasem aktorzy niepaństwowi nie tylko są technicznie zdolni do prowadzenia pełnoskalowych działań wojennych w cyberprzestrzeni, ale nawet mają w wielu zakresach przewagę na państwami - ze względu na możliwość dużo łatwiejszego ukrycia własnej tożsamości.[724] Działania aktorów niepaństwowych mogą mieć także skutki (zarówno kinetyczne jak niekinetyczne) równe operacjom państwowym - wkraczając tym w samym w domenę klasycznego *ius ad bellum,* bowiem zgodnie z doktryną ekwiwalencji kinetycznej atak taki stanowi o użyciu siły. Oznacza to także możliwość wykorzystywania aktorów niepaństwowych przez państwa do prowadzenia działań na tym poziomie.

[723] Pomijając Rewolucję Haitańską, do XX wieku w zasadzie nie zaistniał żaden przypadek długotrwałego prowadzenia działań wojennych przez aktora niepaństwowego. cf.Knight F.W. *The Haitan Revolution,* The American Historical Review 105 (1) (2000) ss.103-15

[724] cf. Pomerlau M. *State vs. Non-state hackers: Different tactics, equal threat?* Public Sectors 360, Defense Systems(2015) s.12

2. *Jus in bello.Prawo niekinetycznej wojny cyberprzestrzennej*

O ile do konfliktu prowadzonego w cyberprzestrzeni stosuje się prawo konfliktu zbrojnego, konieczne jest rozważenie możliwości istnienia odrębnego prawa cyberwojny, określającego sposób prowadzenia działań podczas opisanego powyżej konfliktu wyłącznie cyberprzestrzennego - a więc cyberwojny niekinetycznej. Oczywiście ponieważ konflikty te będą odbywać się wyłącznie w cyberprzestrzeni, regulować je będzie co do zasady *lex informatica*. Wydaje się więc, że rolę owego prawa wojny cyfrowej przejmuje normowanie faktyczne, które w drodze afordancji uniemożliwi prowadzenie określonych działań. Państwom brak bowiem realnych środków prawnych mogących chronić je w tym zakresie.[725] Istnienie prawa do wojny cybernetycznej wpływa ujemnie na zdolność do obrony tradycyjnych podmiotów prawa międzynarodowego w cyberprzestrzeni na drodze prawnej - ze względu na pozostawanie operacji o opisanym tu charakterze w luce prawnej. O ile klasyczne prawo konfliktu zbrojnego może być odpowiednio stosowane do standardowego konfliktu cybernetycznego[726], w przypadku działań niekinetycznych możliwość taka wydaje się być wyłączona. Należy tu zwrócić uwagę na standardowo przyjmowaną w prawie konfliktów zbrojnych jedną z definicji cząstkowych konfliktu zbrojnego - wskazującą, że samo użycie siły nie przesądza jeszcze o stanie konfliktu zbrojnego.[727] Skoro więc nawet użycie siły nie jest *per se* wystarczającą przesłanką by przesądzić o stanie konfliktu zbrojnego - tym bardziej nie mogą przesądzić o nim (a tym samym o stosowalności prawa konfliktów zbrojnych) cyberataki, które skutku kinetycznego nie mają (nawet jeżeli mają potencjał by go wywołać). Drugi problem interpretacyjny tworzy przyjęcie przez doktrynę prawa międzynarodowego za przesłankę pozytywną

---

[725] Cyberataki bez skutków kinetycznych stają się coraz bardziej rozpowszechnionym sposobem osiągania przez państwa własnych celów -często stając się w praktyce międzynarodowej środkiem zastępczym dla trudniejszych do wdrożenia czy utrzymania sankcji ekonomicznych i podobnych retorsji lub represaliów. zob. Także Flanigan E.R. *Integrated Non-Kinetic Operations: The Frontier of Warfare in Search of Doctrine*. School of Advanced Air and Space Studies Air University (2010) ss .12-6

[726] zob.Roscini M. *Cyber Operations ...* ss. 136-45

[727] cf. Wilson G.G. *Use of Force and War*, American Jorunal of International Law 26 (1932) s. 327

- konieczną do uznania określonych działań za konflikt zbrojny - istnienia tzw. *animus bellandi*[728], a więc zamiaru prowadzenia walki zbrojnej. O ile o istnieniu tego zamiaru w przypadku konwencjonalnych działań zbrojnych stosunkowo łatwo przesądzić[729] - w przypadku działań cybernetycznych, gdzie często brak nawet jasnej informacji kto je prowadzi i jaki jest dokładny zakres ataku, jest to prawie niewykonalne.[730] Podobny problem istnieje w odniesieniu do określania swojego zamiaru przez belligerenta poprzez dokonanie wypowiedzenia wojny. Obowiązek wyraźnego wypowiedzenia lub złożenia ultimatum grożącego wojną pod określonymi warunkami jest elementem pozytywnego prawa konfliktów zbrojnych a doktryna przyjmuje także, że obowiązek ów wynika z *black-letter law* i jest także obecny w prawie międzynarodowym zwyczajowym.[731] Potwierdza to także dotychczasowa praktyka międzynarodowa w tym zakresie. O ile więc generalnie do prawa konfliktów cyberprzestrzennych *ius in bello* stosować się będzie na zasadach ogólnych, nie sposób w rozważaniach tej instytucji pominąć wspomnianego natywnego dla cyberprzestrzeni prawa do wojny cybernetycznej pozbawionej skutków kinetycznych. Wydaje się ona być legalna pod warunkiem spełnienia przesłanki zasadności z punktu widzenia *lex informatica*. Działania takie będą następnie regulowane wyłącznie przez ten ostatni system prawny (co wynika ze wspomnianej powyżej prohibytywności prawa międzynarodowego). Podobnie przez *lex informatica* regulowane będą kwestie samoobrony, odpowiedzi i remediów. W razie spowodowania przez którekolwiek z działań w ramach wojny w cyberprzestrzeni skutków kinetycznych, działanie to będzie oceniane przez dużo bardziej restryktywne prawo konfliktów zbrojnych – a

---

[728] zob. McDonald A. *Declarations of War and Belligerent Parties: International Law Governing Hostilities Between States and Transnational Terrorist Networks* Netherlands International Law Review 54, (2007)s. 277, także Wright Q. *When does war exist?*, American Journal of International Law, t.26 nr 2 (1932) ss. 363-7

[729] zob. Barsotti R. *Armed Reprisals* [w: zbiorowa, red. Gazzini T., Tsagourias N. T*he Use of Force in International Law*, Routledge (2012) s.262]

[730] Doktryna prawa konfliktów zbrojnych utrzymuje, że *animus bellandi* można interpretować z określonych zachowań belligerentów, na przykład koncentrację jednostek wojskowych w określonym regionie, przygotowania logistyczne, etc. W cyberprzestrzeni żadne z zachowań z przyczyn technicznych nie może zostać zaobserwowane, w związku z tym brak możliwości określenia w ten sposób zamiaru belligerenta. zob. Także Eagleton C. *The Form and Function of the Declaration of War*, American Journal of International Law 32 (1938) s.25

[731] cf. Dinstein Y.War, Aggression and Self-Defence Cambridge University Press, 3rd ed. (2003) s.32

zauważyć należy, że zarówno legalność jak i bardzo wąska regulacja cyberprzestrzennej wojny niekinetycznej stanowi istotny problem dla ochrony suwerenności państw. Stają one w obliczu legalnego (choć ograniczonego zakresowo) sposobu, prowadzenia wojny przeciw któremu remediów mogą szukać wyłącznie w samych afordancjach *lex informatica*.

1. a. Konflikty sieciowe.

Dodatkowym utrudnieniem i tak już skomplikowanego prawa wojny cyberprzestrzennej jest fakt, że niektóre środki używane we współczesnych konfliktach funkcjonują zarówno w porządku operacji kinetycznych jak i w cyberprzestrzeni. Przykładem takich systemów mogą być rozmaite pojazdy bezzałogowe, podobnie jak w przypadkach opisywanych w rozważaniach poświęconych hybrydowych *CNE*. Jednakże w odróżnieniu od operacji poniżej poziomu użycia siły, cyberataki skierowane przeciwko nim i pozbawiające operatorów kontroli sprawowanej w informatycznej części cyberprzestrzeni potencjalnie dają natychmiastowy efekt kinetyczny w postaci możliwości zastosowania uzbrojenia przenoszonego przez dany dron. W rozdziale niniejszym, rozważone zostaną dwa przykłady takich pojazdów, mianowicie UAV[732] i UMS[733]. W pierwszym przypadku chodzi o latające drony, które w każdym aspekcie przypominają samoloty używane przez siły powietrzne do rozmaitych działań (także szpiegowskich[734] czy transportowych). W drugim chodzi o drony używane na akwenach. Podstawową kwestią, którą należy w kontekście dronów rozstrzygnąć jest kwestia ich traktowania przez prawo międzynarodowe publiczne. Kwestii tej nie

[732] Unmanned Aerial Vechicle- Bezzałogowy obiekt latający.

[733] Unamanned Maritime System- Bezzałogowy system morski. Ich elementem są UUV (Unmanned Underwater Vehicle), czyli systemy morskie operujące pod wodą.

[734] Niektórzy autorzy[zob. Raport Electronic Frontier Foundation o dronach szpiegowskich, dostępny pod www.eef.org/issues/surveillance-drones, dostęp na 1 września 2018 roku] wyróżniają szczególną kategorię dronów latających zwanych UAS- Unmanned Aerial Systems(bezzałogowe systemy powietrzne),wskazując, że od UAV odróżnia je możliwość używania także przez służby cywilne i brak regulacji w prawie konfliktów zbrojnych są szczególnym przypadkiem i podzbiorem UAV. Pojęcie UAS będzie więc dalej używane, wyłącznie w przypadku omawiania *leges speciales* dotyczących wyłącznie tej grupy dronów.

rozstrzyga *black-letter law*, brak też ustalonego prawa zwyczajowego. Istnieje jednak praktyka międzynarodowa, która prawdopodobnie takiemu prawu da początek. Opiera się ona o wewnętrzne regulacje największego operatora wojskowych systemów bezzałogowych - Stanów Zjednoczonych Ameryki Północnej. Departament Obrony tego państwa kwestię prawną dotyczącą systemów wojskowych systemów UAV rozstrzygnął w ten sposób, że zrównał ich status z samolotami używanymi przez wszystkie podległe mu rodzaje sił zbrojnych, pod warunkiem że operatorem drona jest członek personelu tych sił zbrojnych.[735] Podobnie jednoznacznego stanowiska nie zajęto jednak w odniesieniu do systemów morskich. Jednym ze sposobów odpowiedzi na pytanie o ich status jest przypisanie określonych UMS do tradycyjnych okrętów, na których są one przenoszone i uznanie ich za element tych okrętów.[736] Podobną koncepcję przyjmuje także marynarka wojenna Stanów Zjednoczonych.[737] Nie wyjaśnia to jednak kwestii statusu samych dronów. Tymczasem mogą one być używane jako odrębne jednostki, sterowane z brzegu podobnie jak UAV, lub też działać w innych warunkach prawnych niż okręt je przenoszący (na przykład dron może działać wewnątrz wód terytorialnych innego państwa, podczas gdy sam okręt pozostawać będzie i operować na wodach międzynarodowych). Sytuacja taka jest niemożliwa dla żadnego innego elementu wyposażenia okrętu, pozostającego w gotowości do działania.[738] Rozstrzygnięcie tej kwestii jest kluczowe dla prawa cyberprzestrzeni, wraz z kolejną kwestią, będącą niejako rozszerzeniem wskazanego problemu. Nie ulega wątpliwości, że morskie drony mają status jednostek pływających, ponieważ spełniają przesłanki przewidziane przez definicję uznawaną za wiążącą w ramach zwyczajowego prawa morza.[739] Powstaje pytanie czy może im

---

[735] zob. US *Departament of Defense Directive 4540.1 Use of International Airspace by U.S. Military Aircraft and for Missile and Projectile Firings,* (2015) par.3(a)

[736] Norris A.J. *Legal Issues Associated with Unamanned Mairitime Systems* [w: *Selected Wroks of Andrew J. Norris*]wyd. Bepress, U.S. Naval War College, (2013)

[737] *Commander's Handbook on the Law of Naval Operations* NWP 1-14M (2007) para. 2(3)(6)

[738] Pominięte tu zostają, nieistotne dla tematu niniejszej rozprawy sytuacje, w których ze względów uszkodzeń z jakichkolwiek powodów poniesionych przez okręt, niektóre elementy zostają przezeń utracone potencjalnie konstytuując czyn zabroniony w postaci szkód ekologicznych czy zablokowania szlaków wodnych.

[739] zob. *Międzynarodowe Przepisy o Zapobieganiu Zderzeniom na Morzu* Prawidło 3(a) [w: Konwencja w sprawie Międzynarodowych Przepisów o zapobieganiu zderzeniom na

być przypisany status okrętu[740]. Ta ostatnia definicja jest swoistym rozszerzeniem poprzedniej - zakłada, iż jednostka będąca okrętem, jest ujęta w odpowiednich rejestrach, nosi wyraźne oznaczenia przynależności państwowej i podlega dowództwu wojskowemu tego państwa, w szczególności jest bezpośrednio dowodzona przez oficera owego państwa i obsadzona załogą podlegającą dyscyplinie wojskowej. Wydaje się, że drony morskie mogą spełniać wszystkie te warunki, kwestia załogi mogłaby tu być rozwiązywana analogicznie do amerykańskiej interpretacji dotyczącej dronów lotniczych. Okręt bowiem uznawany jest w kontekście przenoszonych przezeń środków walki elektronicznej za element terytorium państwa przynależności. Wydaje się jednak że rozróżnienie dronów przyjęte przez USA nie jest zasadne (wobec faktu, że różnice pomiędzy lotniczymi a morskimi dronami dotyczą nie tyle ich samych co środowiska,w którym zostały wykorzystane) i zaciemnia dodatkowo i tak niejasną ich sytuację prawną. Dodatkowo brak ustalonej praktyki międzynarodowej (jak wskazano powyżej, w aktualnym stanie prawnym jakiekolwiek kompleksowe regulacje w tym zakresie przyjęło wyłącznie jedno państwo i przyjmuje ono niejasne kryteria), szczególnie w zakresie samego prowadzenia konfliktu jak i norm regulujących użycie dronów tworzy kolejną istotną lukę prawną w prawie konfliktów cyberprzestrzennych. Ponieważ cele działania drona mogą być zautomatyzowane[741] lub być określane w czasie rzeczywistym przez operatora, do ich zastosowania stosują się wszystkie problemy opisane powyżej przy operacjach *CNE* skierowanych przeciw dronom. W przypadku konfliktu cybernetycznego możliwe rozwinięcia samego cybernetycznego ataku na dron, mogą oznaczać nie tylko operację *CNE* ale także kinetyczny lub niekinetyczny cyberatak. Drony

morzu (COLREG), podpisana w Londynie w 1972 roku. Do polskiego porządku prawnego przyjęta po ratyfikacji 11 listopada 1976 roku (pub. Dz.U. 1977 nr 15 poz. 61).

[740] zob. Art. 29 Konwencji z Montego Bay

[741] Zautomatyzowane ustawienia drona podlegają ścisłym ograniczeniom. Zakazane jest samo programowanie drona w taki sposób by prowadział on działania, mogące naruszyć prawo międzynarodowe, zgodnie z zasadą minimalizacji strat i zakazem tzw. *Determined killing*. Raport dla Zgromadzenie Ogólnego Narodów Zjednoczonych wskazuje także, że samo używanie dronów powoduje lukę prawną w przypisywaniu odpowiedzialności(podobną do tej opisywanej w rozdziale niniejszej pracy poświęconym atrybucji w cyberprzestrzeni i wynikającej z identycznych przesłanek. zob. Emmerson B. *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Zgromadzenie Ogólne ONZ, A/HRC/25/59 (2014) s.5; także tegoż, Raport *interim* A/68/389

w oczywisty sposób należą do cyberprzestrzeni należąc zarówno do jej fizycznej (*per se*, stanowiąc i przenosząc urządzenia w oparciu o które może działać jej informatyczna część) jak i do informatycznej części (ponieważ sterowanie nimi odbywa się przy pomocy elementów tejże). Ewentualna cyberoperacja skierowana przeciwko dronom, nie tylko narusza jednocześnie suwerenność państwa, które jest drona właścicielem, ale może prowadzić do naruszeń państwa trzeciego, w przypadku przeprowadzenia przez tego drona ataku na cele owym trzecim państwie. W sensie czysto fizycznym jednak zarówno sygnały przekazane do drona jak i ich ciągi bitów określające dane "zachowanie" tegoż, są identyczne - niezależnie od tego, kto ów sygnał wysłał. Nie jest więc możliwe odróżnienie właściwego rozkazu do ataku od sygnału sfałszowanego w ramach cyberoperacji. To odróżnia cyberoperację przeciwko infrastrukturze krytycznej opisaną powyżej od takiej właśnie operacji. Ewentualne osiągnięcie takiego skutku cyberataku, którego ekwiwalencja kinetyczna byłaby równa atakowi w przypadku ataku na cyberprzestrzenne elementy infrastruktury krytycznej musi przebiegać dwustopniowo. Po pierwsze, konieczne jest dokonanie samego włamania, stanowiącego samo w sobie naruszenie suwerenności. Następnie musi zostać ona wykorzystana w określonym ataku powodującym straty potencjalnie mające ekwiwalent kinetyczny. W przypadku cyberataku na drona, rozdzielenie tych elementów nie jest konieczne.[742] Co więcej, możliwe jest prowadzenie cyberoperacji, za pomocą odpowiednich kodów (wykradzionych lub rozpracowanych kryptologicznie), identycznych z tymi, których używa państwo będące właścicielem drona.[743] Wobec niemożności uznania sygnału *in abstracto* za część cyberprzestrzeni (ponieważ stanowi on dane) nie sposób uznać jego wysłania za zachowanie w sensie prawnym, dopóki nie wywoła ono określonych skutków w rzeczywistości fizycznej (na przykład poprzez podanie dronowi fałszywych

[742] zob.także Hartmann K., Giles K.*UAV Exploitation:A new domain for cyberpower*.[w: 8th International Conference on Cyber Conflict Cyber Power,zbiorowa pod red. N.Pissanidis, H.Rõigas, M.Veenendaal NATO CCD COE Publications, Tallinn(2016) ss.210-14]

[743]zob.Seong-Hun S., Byung-Hyun L.,Sung-Hyuck I.Gyu-In JeeEffect of Spoofing on Unmanned Aerial Vehicle using Counterfeited GPS Signal,Journal of Postitioning Navigation and Timing 4(2),(2015) ss.57-65

współrzędnych, prowadzących do przeprowadzenia ataku na nielegalne cele), lub w samej informatycznej części cyberprzestrzeni (na przykład poprzez uniemożliwienie kontaktu z dronem jego właściwym operatorom). Prowadzi to do dwóch istotnych z punktu widzenia ochrony suwerenności konsekwencji. Po pierwsze, może w przypadku cyberataków na uzbrojone drony dojść do wyjątkowej sytuacji, w której określenie podmiotu, który dokonał naruszenia suwerenności jest niemożliwe do określenia dla strony zaatakowanej, ze względu na brak wglądu w zmiany kodu, który zostały dokonane przez podmiot, który dokonał operacji mającej na celu przejęcie kontroli nad dronem. Po drugie, operacje *CNE* wykonane przeciwko dronowi danego państwa mogą potencjalnie zostać przekształcone w atak (zarówno kinetyczny jak i niekinetyczny) jednakże skierowany przeciwko innemu państwu niż to przeciwko któremu została skierowana sama operacja *CNE*.

1. b. Stopniowanie użycia siły zbrojnej.

Orzecznictwo rozróżnia stopnia użycia siły zbrojnej.[744] Wydaje się, że w cyberprzestrzeni, podobne warunki będzie spełniać podział cyberoperacji na te mające ekwiwalent kinetyczny i te, które tego warunku nie spełniają, ale pomimo to wykonywanye są w ramach *ius ad bellum*. Rozróżnienie to mające oczywiście swój początek w prawie rzymskim i rozgraniczeniu pomiędzy *vis* a *vis armata.*[745] ma chronić przed przekroczeniem i nieuzasadnionym użyciem środków obrony przed agresją - w sposób rażąco nieproporcjonalny, czy wręcz stosowania operacji przeciwnika jako pretekstu do uzasadnienia własnej agresji. Z tego względu należy tą regulację oceniać pozytywnie. Rozróżnienie to nie jest pozbawione jednak słabych

[744] W orzeczeniu w sprawie *Nicaragua*[par.191, 210], MTS wskazał że konieczne jest rozróżnienie najcięższych przypadków użycia siły[*most grave forms*] od pozostałych przypadków [*other less grave forms*]. Rozróżnienie to była podtrzymane przez Trybunał w sprawie *Oil Case* (Islamic Republic of Iran v. USA), orzeczenie z dnia 6 listopada 2003 roku. ICJ Reports 2003 s.161 par. 51. Pomimo krytyki tego orzeczenia przez część doktryny, wiążącą normą prawa zwyczajowego jest uznawanie, że dla spełnienia przesłanki ataku zbrojnego, skala danego zachowania musi odpowiadać działaniom sił zbrojnych, nie zaś grup paramilitarnych. zob.też Brownlie I, Crawford J. *Brownlie's Principles of Public International Law*,Disputes,7 wyd. Oxford Univeristy Press (2012) ss.778-9

[745] zob. Berger A. *Encyclopaedic Dictionary of Roman Law,* American Philosophical Society (1953)

punktów, często podnoszonych przez głosy krytyczne wyrażane przez doktrynę. Podstawowym zarzutem wobec rozróżnienia określonego w *Nicaragua* jest stwierdzenie, że w istocie ułatwia ono użycie siły na ograniczonym poziomie - a więc może stanowić zachętę do ograniczonego użycia siły.[746] Rozróżnienie to jako pochodzące z prawa konfliktów zbrojnych jest też inkorporowane do prawa konfliktów cyberprzestrzeni na mocy ogólnej zasady stosowania klasycznego prawa konfliktów zbrojnych.[747] W prawie cyberprzestrzeni zauważalne są trzy podstawowe problemy interpretacyjne dotyczące zasady stopniowania siły. Po pierwsze, nie jest jasne czy rozróżnienie to w ogóle dotyczy cyberoperacji powyżej poziomu użycia siły jednak nie wywołujących skutków kinetycznych, a więc drugiego rodzaju konfliktu cyberprzestrzennego wspomnianego powyżej. Łatwo zauważyć także, że dodatkowe kryterium 'starć granicznych' wynikłe z orzecznictwa Międzynarodowego Trybunału Sprawiedliwości, nie jest możliwe do zastosowania w cyberprzestrzeni, w której nie istnieje możliwość jasnej delimitacji granic. Po drugie w przeciwieństwie do tradycyjnych środków prowadzenia wojny, gdzie rozróżnienie pomiędzy 'starciami' nie uruchamiających prawa do pełnoskalowej odpowiedzi a inwazją może zostać oparte na łatwo zauważalnych przesłankach, których interpretacja prawna jest solidnie ugruntowana w orzecznictwie i praktyce międzynarodowej. Trzecią kwestią jest problem z rozgraniczeniem sił zbrojnych w cyberprzestrzeni od grup nie mających tego przymiotu, istniejący na poziomie zarówno formalnoprawnym jak i materialnoprawnym. Formalnoprawnie nie sposób bowiem w oczywisty sposób rozgraniczyć grup hakerskich działających na zlecenie danego państwa, od jego cybernetycznych sił zbrojnych.[748] Zastosowanie w tym zakresie testu *Nicaragua* nie jest możliwe ze względu na brak możliwości stwierdzenia spełnienia przesłanki przynależności organizacyjnej tych grup - powodowanej anonimowością cyberprzestrzeni. Podobnych ograniczeń doznaje także test *Tadicia,* pomimo wynikających z niego szerszych możliwości przypisania odpowiedzialności państwu.

[746] zob. Brownlie, Crawford *Brownlie's Principles...* s.780

[747] zob. Rule 80 *Tallinn Manual 2.0* z komentarzem IGoE [w: *Tallinn Manual 2.0...* s.389]

[748] Holmberg E.J. *Armed Attacks in the Cyberspace. Do they exist and can they trigger the right to self-defense*, University of Stockholm (2015) ss.17 i n.

Wydaje się więc, że anonimowość cyberprzestrzeni skutecznie uniemożliwia przypisanie państwom odpowiedzialności za działania niewielkich grup hakerskich, które najczęściej podejmują w cyberprzestrzeni działania spełniające przesłanki 'mniej istotnych przypadków użycia siły'. Rozpatrywanie wątpliwości materialnoprawnych, należy rozpocząć od *ratio* rozróżnienia dokonanego w *Nicaragua*. MTS przyjął że niewielkie straty jakie mogą wywołać nieregularne oddziały uzasadniają ograniczenie odpowiedzi. Niewątpliwie, w przypadku konwencjonalnych działań należy uznać słuszność tej argumentacji - skutecznie przeciwdziałającej nadmiernej eskalacji konfliktu. Natomiast niewątpliwie traci ona na znaczeniu w cyberprzestrzeni, ponieważ nawet niewielkie, nieregularne grupy operujące w cyberprzestrzeni, mają zdolność dokonywania znaczących ataków, w tym także tych mających ekwiwalent kinetyczny. Jej utrzymanie w tym systemie prowadzi oczywiście do dalszego rozmycia norm regulujących prawo do ochrony suwerenności w cyberprzestrzeni ze względów identycznych jak ma to miejsce w przypadku operacji *CNE* i niekinetycznej wojny cyberprzestrzennej. Chodzi tu oczywiści o problem pierwotnej niemożliwości oceny stopnia zagrożenia na etapie, na którym skuteczna obrona (na przykład poprzez uderzenie prewencyjne) ciągle jest możliwa. Zachowanie normy stopniującej użycie siły w cyberprzestrzeni, niewątpliwie musi być z punktu widzenia ochrony suwerenności w cyberprzestrzeni ocenione negatywnie, niemniej w aktualnym stanie prawnym pozostaje ono częścią systemu prawa konfliktów cyberprzestrzennych.

1. c. Legalność użycia siły z punktu widzenia Karty Narodów Zjednoczonych

Jak wspomniano powyżej użycie siły nie jest już suwerennym prawem państw. Jednakże podstawa prawna tego zakazu nie jest w pełni określona. Najczęściej zarówno doktryna jak i orzecznictwo wskazują na wspomniany już art. 2(4) KNZ, zarówno *explicite* jak i jako źródło normy prawa zwyczajowego, wiążącej *erga omnes*. Praktyka narodowa nie jest jednak określona w tym zakresie. Przede wszystkim należy wskazać na pogląd konsekwentnie wyrażany przez Związek Sowiecki, który

w okresie od wejścia w życie Karty, do upadku tego państwa utrzymywał, że art. 2(4) nie jest normą bezwzględnie wiążącą państwa-sygnatariuszy Karty.[749] Co więcej, żadne z innych państw-sygnatariuszy Karty nie powołało się ani na same naruszenia, ani na deklarowany brak uznania związania się art 2(4) przez ZSRS, by uzasadnić wyłączenia własnych obowiązków wobec tego państwa, pomimo istniejącej normy która na takie zachowanie zezwala.[750] Należy jednak dodać, że argumentacja ta nie znalazła szerszego poparcia u pozostałych podmiotów prawa narodów.

KNZ jest źródłem pozytywnego zakazu stosowania prowadzenia wojny jako środka prowadzenia polityki międzynarodowej,[751] dekodowanego z norm nakazujących pokojowe działania na arenie międzynarodowej, zawartych w art. 2(3)[752]i art. 2(4)[753]. Norma zakazująca agresji, zyskała też status normy prawa zwyczajowego,[754] bezdyskusyjnie wiąże więc nawet państwa nie będące członkami ONZ. Należy więc zauważyć, że przedmiotowy zakres normowania wspomnianych artykułów Karty pozostaje w stosunku zawierania w stosunku do zasad nieinterwencji i nieinterferencji, choć niewątpliwie ma podobny cel - nakazanie powstrzymania się od naruszeń suwerenności państw trzecich w ramach realizacji własnych interesów. Natomiast zakres podmiotowy samej Karty jest oczywiście węższy, wskutek skierowania art. 2(3)(4) KNZ wyłącznie do członków Narodów Zjednoczonych przez same te przepisy. Tymczasem zasady nieinterwencji i nieintereferencji, pomimo ich bezspornego istnienia w porządku prawnym, nie są precyzyjnie zdefiniowane, czy to przez orzecznictwo czy praktykę.[755] Wydawałoby się więc, że ONZ mogłaby w art.2(3)(4) wyznaczyć (wraz z Międzynarodowym Trybunałem Sprawiedliwości, będącym

---

[749] zob. Rostow E.V. *The Legality of the International Use of Force by and from States* Yale Law School Faculty Scholarship Series Paper 2128 (1985) ss.287-30

[750] zob. Schachter O. *In Defense of International Rules on the Use of Force* University of Chicago Law Review 53:113(1986) ss.120-2

[751] Powszechnie przyjmowanego w doktrynie prawa międzynarodowego jeszcze w momencie prac nad kartą.

[752] *Wszyscy członkowie [ONZ] załatwiać będą swe spory międzynarodowe środkami pokojowymi[...]*

[753] *Wszyscy członkowie powstrzymają się w swych stosunkach międzynarodowych od groźby użycia siły lub użycia jej przeciwko integralności terytorialnej lub niezawisłości politycznej któregokolwiek państwa bądź w jakikolwiek inny sposób niezgodny z celami ONZ.*

[754] zob. Hassan K. *Jus Cogens and Obligations Under the U.N. Charter*, Santa Clara Journal of International Law 3 (2005) s.88

[755] zob.Denza E. *Diplomatic Law* Oxford University Press 3rd ed. (2008) ss.465-6

przecież elementem szeroko pojmowanego systemu Narodów Zjednoczonych) bardziej precyzyjne kryteria określania nieinterwencji i nieinterferencji przynajmniej w kluczowym zakresie konfliktu zbrojnego. Dla operacji cyberprzestrzennych precyzyjne bowiem określenie zakresu dozwolonej interferencji i interwencji ma znaczenie zasadnicze: zarówno ze względu na decyzje sekurytyzacyjne i kształt tworzonych afordancji, jak i ze względu na prawo wykonywania cyfrowego ataku prewencyjnego (wymierzonego w infrastrukturę i algorytmy, które inaczej miałyby zostać użyte do zaatakowania państwa, które atak prewencyjny wykonuje). W wielu przypadkach jest to jedyna możliwość skutecznej obrony przed atakami cyberprzestrzennymi.[756] Brak dokładnego zdefiniowana, zarówno na gruncie art.2(3)(4) KNZ, jak i na gruncie interpretacji przywołanych zasad, utrudnia lub wręcz uniemożliwia określenia proporcjonalności odpowiedzi obronnej lub ataku prewencyjnego, będących podstawową przesłanką legalności tychże.[757] Brak jasnych kryteriów uniemożliwia także częstokroć określenie samej legalności celów. Tymczasem część doktryny stoi na stanowisku, że sam fakt nielegalności osiąganych celów, *de iure* czyni nieomal każdy środek użyty w obronie nieproporcjonalnym.[758] Takie stanowisko, mające swoje korzenie w braku jasnej wykładni funkcjonalnej omawianych norm, prowadzi w konsekwencji do znaczącego rozszerzenia zakresu proporcjonalnej odpowiedzi na środki nielegalne. O ile w przypadku operacji kinetycznych istnieją inne, (poza proporcjonalnością) ograniczenia środków użytych do obrony suwerenności[759], w cyberprzestrzeni są one skuteczne wyłącznie w kontekście ataku o skutkach kinetycznych. Oparte są bowiem o kryterium, którego nie można brać pod uwagę przy ocenie operacji poniżej poziomu siły i ataków niekinetycznych. Należy jednak pamiętać, że - jak wskazał MTS w orzeczeniu w

---

[756] W rozprawie niniejszej celowo pominięto rozważania na temat definicji ataku zamieszczonej w art. 49(1) I Protokołu Dodatkowego ponieważ jako oparte na kryterium stosowania przemocy dotyczy ona *explicite* konfliktu kinetycznego i nie jest stosowalna do operacji cyberprzestrzennych.

[757] por. Dinstein Y.*War, Aggression and Self-Defence* Cambridge University Press 3rd ed.(2003) s. 184

[758] por. Kretzmer D. *The inherent Right to Self-Defence and Proportionality in Ius ad Bellum* European Journal of International Law, Oxford University Press,24:1 (2013) s.240

[759] zob. art. 51(5)(b) I Protokołu Dodatkowego. Także Rule 14 *Customary IHL*, International Committee of Red Cross

sprawie *Nicaragua*[760] - termin określając atak przekraczający przywołany powyżej wyższy stopień użycia siły - *armed attack* -nie jest elementem prawa traktatowego ani nie występuje w KNZ i nigdzie nie został zdefiniowany jednoznacznie. Natomiast jego użycie i zakres w orzeczeniu *Nicaragua* zostało przez sam Trybunał ograniczone wyłącznie do rozpoznawanej sprawy.[761] Pewne wskazówki można jednak odnaleźć w praktyce Narodów Zjednoczonych. Wskazują one, że *armed attack*, to tyle co naruszenie suwerenności za pomocą broni lub działań, mogących uzyskać podobny skutek.[762] Utrwalenie takiego rozumienia pojęcia *armed attack* i jego inkorporacja do prawa cyberprzestrzeni mogłyby być istotną pomocą w rozwiązaniu problemu z określeniem poziomu i momentu legalności odpowiedzi na cyberprzestrzenne naruszenie. Byłby to moment, w którym następuje spełnienie przesłanek *armed attack* ustalonych przez MTS w *Nuclear Tests*. Pozwalałoby to na prowadzenie obrony cybernetycznej przeciwko zarówno kinetycznym, jak i niekinetycznym atakom cybernetycznym, na mocy normy wynikającej z art.2(3)(4) Karty, a z pominięciem nieprecyzyjnych w tym zakresie i nieprzydatnych do prawa cyberprzestrzeni regulacji wyprowadzanych z zasad nieinterwencji i nieinterferencji. Regulacja taka mogłaby także dać początek normom zwyczajowym w podobny sposób regulującym naruszenia poniżej poziomu użycia siły w szczególności *CNE*. Należy także pamiętać, że normą nakazującą pokojowe rozwiązywanie sporów (a więc *de facto* inkorporującą do prawa cyberprzestrzeni dyspozycję art.2(3)(4) KNZ) jest *Rule 65* TM 2.0. Wprowadza ono także kryterium przedmiotowe naruszenia lub zagrożenia światowego pokoju lub bezpieczeństwa przez działania związane z cyberprzestrzenią. Wydaje się więc, że argumentacja ta koresponduje z przedstawioną powyżej, wskazując *de lege ferenda* na potencjalnie istotną rolę art. 2(3)(4) KNZ dla ochrony suwerenności w cyberprzestrzeni.

---

[760] *Armed Activities in and Against Nicaragua...* par.176

[761] zob. *Nicaragua...* par.205

[762] Tak MTS w sprawie *Nuclear Tests* par. 39, Rada Bezpieczeństwa ONZ w rezolucjach 1368/2001 i 1373/2001, dotyczących ataku na WTC, który uznano za atak zbrojny pomimo iż do jego przeprwoadzenia użyto samolotów cywilnych. Podobną koncepcję uznaje też doktryna. zob. Zemanek K. *Armed Attack* [w: Max Planck Encyclopedia of Public International Law t.1 (2012)s.599] także Roscini M. [w:*Cyber Operation and the Use of Force in International Law]*

1. d. Cyberataki

Przyjmuje się, że atakiem jest każda cyberoperacja, co do której można rozsądnie oczekiwać, że spowodują one straty w ludziach lub materialne.[763] Operacje te niekoniecznie muszą naruszać suwerenność państwa trzeciego, ponieważ definicja odnosi się także konfliktów wewnętrznych. Powszechnie za *Tallinn Manual 2.0* przyjmowana definicja ataku w cyberprzestrzeni została wyprowadzona z definicji ataku stosowanej w ogólnym prawie humanitarnym, na zasadach ogólnych inkorporowanej do prawa konfliktów cyberprzestrzennych. *A contrario* IGoE przyjmuje, że operacje nie spełniające owego kryterium[764] poziomu ataku nie osiągają.[765] Należy zauważyć, że przesłanką wystarczającą dla uznania danej operacji za atak, jest możliwość wyrządzenia przez daną operację strat (a nie samo ich wystąpienie). Oznacza to, że rozumienie ataku w cyberprzestrzeni jest szersze niż w prawie konfliktów zbrojnych prowadzonych w świecie fizycznym. Łatwo też zauważyć, że tak skonstruowana definicja obejmuje zarówno kinetyczne jak i niekinetyczne ataki cybernetyczne.

1. e. Charakterystyka cyberataku i sposób jego oceny.

Należy wskazać, że MTS przyjął, że artykuły 2(4), 51 i 42 Karty Narodów Zjednoczonych nie określają sposobu broni, która ma zostać użyta, a przesłanki określające wystąpienie *armed attack* określają wyłącznie poziomu natężenia użycia siły.[766] Przesłanka ta nie jest wystarczająco wyraźna w cyberprzestrzeni. Ataki cyberprzestrzenne mogą dawać bardzo zróżnicowane skutki z podobnych operacji. Brak więc w ich przypadku (istniejącej w świecie fizycznym) możliwości określenia na podstawie wiedzy pozaprawnej jakie potencjalne skutki może mieć atak

[763] zob.*Rule 30 TM* i Rule 92 *TM 2.0*.
[764] Dokładne kryterium przyjmowane przez IGoE to *brak zastosowania przemocy*.
[765] zob. Komentarz IGoE do *Rule30 TM*, par.2 *in fine*, także
[766] *Legality of the Threat or Use ...*,par. 39.

przeprowadzony określonymi siłami. Waxman wskazuje wręcz, że ze względu na konstrukcję systemów państwowych i infrastrukturalnych współczesnego świata, uderzenie cyberprzestrzenne może powodować większe konsekwencje niż atak konwencjonalny.[767] Roscini podkreśla, że takie podejście niekoniecznie musi oznaczać problem interpretacyjny - wskazując na orzeczenie MTS w sprawie *Nicaragua...*[768], i opinię Trybunału według której zarówno bezpośrednie jak pośrednie działanie, może oznaczać użycie siły.[769] Pogląd ten jest dyskusyjny. Przede wszystkim powszechnie akceptowany w doktrynie i praktyce międzynarodowej tzw. Test Schmitta (w oryginale *Schmitt Anaylsis*), przyjmuje bezpośredniość za jedno z podstawowych siedmiu kryteriów oceny czy doszło do zastosowania siły w rozumieniu art. 2(4) KNZ. Należy tu odnotować, że istnieją w doktrynie prawa międzynarodowego także głosy odrębne. Przede wszystkim, część doktryny stoi na stanowisku, że art. 2(4) KNZ w żaden sposób nie różnicuje "użycia siły", ani "groźby użycia siły" w szczególności ze względu na kryteria, które za decydujące w swoim teście przyjmuje Schmitt.[770] Należy jednak zauważyć, że Test Schmitta jest *explicite* oparty na normie wyprowadzonej z art. 2(4) KNZ.[771] W związku z tym z jego interpretacji funkcjonalnej należy wnosić, że podobnie jak ta norma - dotyczy on zarówno użycia siły jak i zagrożenia użyciem siły. Drugą osią sporu o interpretację jest koncepcja wyłączenie z zakresu użycia siły takiego ataku, który pomimo spowodowania strat w świecie fizycznym czyni to w drodze niszczenia rzeczy niematerialnych.[772] Oczywistym przykładem takiej operacji jest atak na systemy bankowe, połączony ze zniszczeniem danych na kontach lub atak na systemy giełdowe prowadzące do strat spółek notowanych, jednak niewpływających na ich

---

[767] Waxman M.C. *Cyberattacks and the Use of Force: Back to the future of article 2(4)* Yale Journal of International Law 36:2 (2011) ss.427-9

[768] zob. Orzeczenie MTS w sprawie *Nicaragua* par. 205

[769] Roscini M. *Cyber Operations and the Use of Force in International Law* Oxoford University Press (2016) s. 68 także Dinniss H. *CyberWarfare* par.27

[770] Tak na przykład Melzer N. *Cyberwarfare and International Law* United Nations Institute for Disarmament Research (2011) s.272

[771] zob. Silver D.B. *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter.*International Law Studies 76 (2014) ss.76 i n.

[772] Schmitt M. *Cyberoperations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts* [w:*Proceedings of a Workshop on Deterring Cyberattacks, Informing Strategies and Developing Options for U.S. Policy* (2010) ss.157-60]

sytuację w świecie fizycznym. Należy jednak zauważyć, że Test Schmitta rozróżnia ataki z użyciem siły (w rozumieniu tradycyjnego prawa konfliktów a więc mające ekwiwalencję kinetyczną) od cyberataków bez użycia siły (niekinetycznych).[773] Stanowisko to ma poparcie także w praktyce międzynarodowej.[774] Z punktu widzenia KNZ, to rozróżnienie ma istotne znaczenie dla uruchomienia wielu procedur, w tym najistotniejszej czyli uruchomienia prawa do samoobrony także poprzez uderzenie prewencyjne.[775] Doktryna wyróżnia trzy metody określania czy dany atak został dokonany z użyciem siły (należy pamiętać, że żadna z nich nie jest właściwa do oceny ataków niekinetycznych), które zostaną pokrótce omówione poniżej

1. e. 1. Doktryna ekwiwalencji kinetycznej

Podstawowym, jak przyjmuje się w praktyce międzynarodowej jak i doktrynie,[776] środkiem oceny czy operacja jest atakiem czy też naruszeniem suwerenności państwowej poniżej tego poziomu, jest test ekwiwalencji kinetycznej. Powszechność jego przyjmowania, wynika głównie z jego stosunkowej prostoty i niezawodności. Ocenie podlegają straty materialne wywołane atakiem, a następnie wysokość tych strat porównywana jest ze skutkami wywołanymi atakiem konwencjonalnym. Przyjmuje się, że strona odpowiada za operację cybernetyczną w identycznym zakresie, w jakim odpowiadałaby gdyby przeprowadziła odpowiadającą jej skutkami operację konwencjonalną. Model ten należy uznać za umożliwiający najszybszą i najmniej narażoną na błąd ocenę sytuacji. Szybkość, wobec tempa w jakim przeprowadzane są operacje cybernetyczne, jest niezwykle istotna. Przeciwnicy modelu wskazują natomiast, że nierzadko skutki operacji cybernetycznych są oddalone w czasie i przestrzeni lub wręcz w łańcuchu przyczynowo-skutkowym od

---

[773] zob. Schmitt M.N. *Computer Network Attack and the Use of Force in International Law: Thoughts on Normative Framework*, Columbia Journal of International Law 37 (1999) ss.860-70

[774] Flowers A., Zedally Sh. *Cyberwar: The What, When, Why, How,* IEEE Technology and Society Magazine (2014) ss.14-17

[775] zob. Keber T.O., Roguski N.P. *Ius ad bellum electronicum? Cyberangriffe in Lichte der UN-Charta und aktueller Staatenpraxis,* Archiv des Voelkerrechts wyd. Mohr Siebeck GmbH & Co. KG,49:4 (2011) s. 408

[776] zob. Schmitt M.N. *Normative Framework...* ss.905-8

powodujących te skutki operacji.[777] Jednak rozróżnienie pomiędzy bezpośrednimi a pośrednimi atakami jest problematyczne także w przypadku operacji kinetycznych, a wypracowana w tym względzie praktyka międzynarodowa może być stosowana odpowiednio.

1. e. 2. Doktryna ścisłej odpowiedzialności

Koncepcja ta jest podobna do opisanej powyżej koncepcji ekwiwalencji kinetycznej, jednakże inkorporuje ona jednak elementy reżimu odpowiedzialności międzynarodowej przewidzianego za czyny międzynarodowo zakazane.[778] Według tej koncepcji, państwo dokonujące naruszenia suwerenności odpowiada za wszystkie jego skutki - bezpośrednio z niego wynikające.[779] Koncepcja ta jednak zastępuje odpowiedzialność przewidzianą w *ARSIWA* odpowiedzialnością za przeprowadzenie ataku. Według tej doktryny atakiem jest więc jest każda operacja cyberprzestrzenna, która narusza suwerenność innego państwa i uderza w jego krytyczną infrastrukturę. W reżimie odpowiedzialności przewidywanym przez *ARSIWA*, zachowanie takie dawałoby podstawę do odszkodowania, jednakże w przypadku oceny legalności cyberoperacji będzie oznaczało przeprowadzenie ataku,[780] a wybór celu dla niej, będzie determinować, czy dany atak został czy nie został przeprowadzony z użyciem siły zbrojnej. Część doktryny przyjmującej zasadę ścisłej odpowiedzialności, rozszerza jej stosowanie przyjmując, że atakiem jest samo przygotowanie operacji – o ile jest ona wymierzona w infrastrukturę krytyczną państwa.[781]

---

[777] por. Gervais M. *Cyberattacks and the Laws of War* Berkeley Journal of International Law,30:2 (2012) s.539

[778] Chodzi o odpowiedzialność skodyfikowaną przez Komisję Prawa Międzynarodowego w *Draft Articles on Responsibility of States for Internationally Wrongful Acts,* przyjęte na 56 sesji plenarnej Zgromadzenia Ogólnego ONZ, rezolucją 56/83 z grudnia 2001 roku(z późniejszymi zmianami wprowadzonymi w dokumencie o syg. A/56/49. cyt za *Yearbook of International Law Commission* t.2 (2001), dalej jako *ARSIWA.*

[779] zob. także wynik arbitrażu w sprawie *Trail Smelter Case(USA, Canada)*, cyt. za Reports of International Arbitral Awards, United Nations, t.3 (2006) s.1919

[780] Należy zauważyć, że koncepcja tu opisana jest niewspółmożliwa z jakąkolwiek definicją cyberataku, opartą o kryterium skutku. W związku z tym, nie ma żadnej możliwości zastosowania do niej Testu Schmitta, którego kryteria wymagają wiedzy o skutku właśnie.

[781] zob. Gervais M. *Cyber Attacks and the Laws... s.19*

O ile takie założenie może się wydawać daleko idące, należy pamiętać że moment uruchomienia operacji cyberprzestrzennej może być w istocie identyczny z momentem rozpoczęcia występowania jej efektów. W związku z tym przyjęcie takiej przesłanki w reżimie prawnych opartym wyłącznie o ocenę skutków wydaje się zasadne. Istnieją jednak liczne problemy z faktycznym przypisaniem odpowiedzialności za atak, który jest dopiero w fazie przypisania.

1. e. 3. Doktryna oceny środków przenoszenia cyberbroni

Ostatnią i najmniej rozpowszechnioną koncepcją jest idea oceny stopnia naruszenia suwerenności na podstawie tego, w jaki sposób dana broń stosowana w cyberprzestrzeni została przeniesiona na teren podlegający jurysdykcji państwa, które jest celem operacji. Podstawową wadą tej koncepcji, w zasadzie czyniącą z niej wyłącznie teoretyczną konstrukcję, jest brak mającej status źródeł prawa, listy dozwolonych i zakazanych środków przenoszenia cyberbroni, jak i okoliczności w której zastosowanie tych środków można uznać za legalne. Praktyczne zastosowanie opisywanej koncepcji wymagałoby więc wielostronnych traktatów, podobnych do tych które regulowały użycie poszczególnych broni kinetycznych. Jak wskazano powyżej, w rozdziale dotyczącym *lex informatica*, wejście w życie takich traktatów jest mało prawdopodobne. Dodatkowo, w przypadku sieciowej cyberprzestrzeni, brak związania się traktatem, przez nawet mniejszość państw, oznaczałaby znaczącą przewagę osiąganą przez te państwa, nieporównanie większą niż w przypadku wypowiedzenia jednego z traktatów o broniach kinetycznych przez taką samą grupę państw. *Tallinn Manual 2.0* także wskazuje, że brak możliwości precyzyjnego rozdzielenia rodzajów broni cybernetycznych w stopniu wystarczającym do efektywnego stosowania opisywanej koncepcji.[782]

[782] zob. *Rule 103* i *Rule 110 Tallinn Manual 2.0*

1. e. 4. Podsumowanie

Nie ma wątpliwości, że doktryna oceny środków nie ma zastosowania praktycznego w dzisiejszym stanie prawnym. Pozostaje więc doktryna ścisłej odpowiedzi i ekwiwalencji kinetycznej. Na uznanie za obowiązującą tej ostatniej wskazuje aktualna praktyka międzynarodowa. Status ten jest też wzmacniany przez fakt szerokiej akceptacji w praktyce Testu Schmitta, który jak wskazano powyżej może być przeprowadzony wyłącznie przy założeniu doktryny ekwiwalencji kinetycznej. Kwestia statusu doktryny ścisłej odpowiedzi (która mogła by być stosowana subsydiarnie) jest skomplikowana. Za jej największą zaletę należałoby uznać możliwość odpowiedniego jej stosowania do oceny stopnia naruszeń wynikłych z cyberataków niekinetycznych. O ile jednak same przesłanki, jako wynikłe z odpowiedniego stosowania *ARSIWA* mają niewątpliwie statuts norm bezwzględnie obowiązujących w prawie międzynarodowym. Jednak ich transpozycja do prawa konfliktów cyberprzestrzennych wymagałaby niewątpliwie praktyki międzynarodowej i *opinio iuris*, których brak. Podobnie niejasna jest próba przypisania odpowiedzialności podmiotom międzynarodowym za przygotowywanie operacji cybernetycznych. Przyjęcie takiej koncepcji oznaczałoby prawo do zastosowania środków obrony przewidzianych przez art. 51 KNZ przeciwko państwu, które wyłącznie przygotowało operację. Tymczasem, praktyka międzynarodowa w zakresie cyberprzestrzeni wskazuje, że państwa przygotowują rozmaite operacje w ramach utrzymywania środków obrony. Uznanie ich za atak, stanowiłoby znaczące i nieuzasadnione różnicowanie operacji cyberprzestrzennych i przygotowywania planów operacji wojskowych, których prawo międzynarodowe w żaden sposób nie uznaje za nielegalne, czy spełniające przesłanki prawa do obrony jakiegokolwiek państwa trzeciego. Plan takiego cyberataku na infrastrukturę wrażliwą państwa trzeciego, może też być planem obronnym, przygotowywanym do wykonania w ramach obrony cybernetycznej lub sankcji w istocie zastępującej odpowiedź kinetyczną i w pełni legalnych. Przykładem takiej operacji może być niedawny cyberatak USA na irańskie cele wojskowe, stanowiący retorsję za zestrzelenie

amerykańskiego samolotu bezzałogowego. Przyjęcie, że istnienie takich planów może być uznane za atak, prowadziłoby do więc sprzeczności. Wobec tego, w dalszej części niniejszego opracowania, za kryterium oceny przyjęto kryterium ekwiwalencji kinetycznej wynikające z uznanego przez praktykę międzynarodową Testu Schmitta.

.

2. Test Schmitta

Według samego jego autora, celem konstrukcji Testu było stworzenie stosunkowo łatwego narzędzia służącego do oceny kiedy dana cyberoperacja przekracza próg użycia siły, narusza dyspozycję art. 2(4) KNZ i tym samym daje prawo do działań z zakresu samoobrony państwowej.[783] Został on oparty na katalogu kryteriów, których ocena pozwala stwierdzić zarówno fakt jak i stopień naruszenia suwerenności państwa trzeciego przy pomocy użycia siły (tu w rozumieniu *armed attack*, a więc tożsamym z tym, które przyjmowane jest w prawie konfliktów zbrojnych).[784] Łatwo więc zauważyć, że stosuje się on wyłącznie do kinetycznych ataków cybernetycznych. Poniżej zostaną omówione kryteria przyjmowane przez Test.

2. a. Dolegliwość(Severity)

Pierwszym z kryteriów wskazanych w teście jest kryterium dolegliwości *(severity)*. Różnica pomiędzy użyciem siły powyżej poziomu art. 2(4) a inną formą nacisku według tego kryterium polega na stopniu strat wywołanych atakiem. Podstawową formą oceny musi więc być kryterium ekwiwalencji kinetycznej. Zasady doświadczenia życiowego i analogii z innymi atakami przeprowadzanymi w historii pozwalają ocenić społeczności międzynarodowej stopień takiego uderzenia, a co za tym, idzie przyznać legalność także odpowiedzi na atak. Jako kryterium fizyczne, jest najmniej podatny na prowadzenie *cyberlawfare*, z reguły bowiem przyjmuje się że jakikolwiek atak kinetyczny (a więc operacja o stopniu naruszenia wyższym niż *border clashes* określone w *Nicaragua*) na terytorium państwa lub jego obywateli

[783] zob. Schmitt M.N.*Normative Framework...* s.885
[784] ibid. s.900

pozwala na użycie samoobrony.[785] Pierwszym krokiem do oceny dolegliwości ataku, jest więc stwierdzenia czy cele, w które został skierowany, są legalne.[786] Należy to odróżnić od legalności samego ataku, wyróżnionym jako odrębne kryterium. Drugim elementem badania dolegliwości, będzie rozróżnienie czy atak prowadzi do dokonania uszkodzeń fizycznych czy też wyłącznie strat informatycznych, rozumianych jako dokonanych wyłącznie w informatycznej części cyberprzestrzeni. Brak takich zniszczeń lub ich zamiaru, zgodnie z prawem zwyczajowym regulującym konflikty w cyberprzestrzeni, będzie oznaczał że mamy do czynienia z atakiem niekinetycznym (według afordancji umożliwiających daną operację) i w konsekwencji wyłączy możliwość zastosowania Testu.[787] Należy jednak pamiętać, że doktryna przyjmuje, że ochronie podlegają co do zasady także fizyczne dobra niematerialne.[788] Można więc przyjąć, że jeżeli atak spowoduje paraliż systemów państwowych, a tym samym uniemożliwi właściwe funkcjonowanie państwa i jego organów, to atak taki należy uznać za powodujący bezpośrednie skutki kinetyczne. Należy także go uznać także atak w rozumieniu czysto militarnym - choćby nawet nie doszło do trwałych zniszczeń czy uszkodzeń paraliżowanej infrastruktury.[789] Podobne skutki może też mieć grożenie atakiem cybernetycznym[790], którego dotkliwość należy mierzyć w oderwaniu od ewentualnych skutków, które mogłoby mieć wykonanie określonej operacji. Informacja lub groźba, przesłana oficjalnymi kanałami dyplomatycznymi i mająca wysokie prawdopodobieństwo spełnienia, o możliwości zdalnego wyłączenia radarów regulujących cywilny ruch lotniczy w danym państwie, musi prowadzić do zamknięcia ruch lotniczego, a co za tym idzie

---

[785] Z wyjątkiem wymogu zachowania proprorcjonalności obrony, wyprowadzonego z orzeczenia MTS w sprawie *Nicaragua*.

[786] Zgodnie z prawem konfliktów zbrojnych, legalny jest cel, którego zaatakowanie umożliwia wypracowanie istotnej przewagi przy braku nadmiernych strat ubocznych (*collateral damage*).zob. Art. 52 *I Protokołu Dodatkowego*

[787] zob. Rule 30 *Tallinn Manual*

[788] zob. Schmitt M.N. *Cyber Operations and the Jus Ad Bellum Revised*, 56 VIII Villanova Law Review Charles Widget School of Law Digital Resources 569 (2011)

[789] ibid. Schmitt wskazuje na cyberoperację przeciw Estonii w 2008 roku, którego elementem było paraliżowanie systemów państwowych, jednakże nie prowadzące do żadnych zniszczeń. Pomimo to, należy potraktować tą operację jako atak w rozumieniu Tallinn Manual.

[790] Samo takie działanie, co do zasady, zostanie uznane za zachodznie nielegalne. Dokładniejsze rozważania na ten temat zawarte zostaną w podrozdziale dotyczącym kryterium legalności.

strat materialnych. Nie ma przy tym znaczenia, czy atak miałby zostać rzeczywiście wykonany, tak jak nie ma znaczenia czy byłby potencjalnie możliwy.[791] Możliwa jest więc ocena ekwiwalencji kinetycznej także w odniesieniu do groźby użycia siły. Koresponduje to ze wspomnianym już wyprowadzeniem Testu z normy wynikłej z art. 2(4), który zakazuje także groźby użycia siły. Jednak analiza dolegliwości groźby wymaga oceny dwóch dodatkowych parametrów: prawdopodobieństwa[792] i dolegliwości ataku[793], który miałby być dokonany. Dopiero posiadanie obydwu tych informacji pozwala na ocenę dolegliwości samej zakazanej groźby, która będzie ich funkcją. Należy tu zauważyć, że możliwa jest sytuacja, w której, pomimo potencjalnej dolegliwości ewentualnego ataku, groźba nie będzie dolegliwa, ze względu na niskie prawdopodobieństwo przeprowadzenia jego przeprowadzenia. Dolegliwość - której ocena w przypadku ataku lub groźby ataku konwencjonalnego jest stosunkowo łatwa - w przypadku cyberprzestrzeni może być niezwykle trudna do oceny lub niewykonalna, szczególnie jeżeli atak lub groźba ataku będzie rozpoczęta przez operację *CNE*.

2. b. Legalność(Presumptive Legality)

Nie ma wątpliwości, że uderzenie w cele cywilne (nielegalne co do zasady) będzie bardziej dolegliwe niż uderzenie w cel legalny. Na tym etapie oceny zachowania, istnieje największa możliwość stosowania *cyberlawfare*. Normy prawa konfliktów zakazują bowiem ataku na infrastrukturę cywilną, nawet jeżeli jest ona połączona w jeden system komputerowy z infrastrukturą wojskową,[794] a nawet ataków, co do których nie istnieje pewność, który z celów (wojskowy czy cywilny) zostanie realnie uderzony.[795] W istocie, norma dekodowana z obydwu tych przepisów, wskazuje że

---

[791] zob. Opinia Międzynarodowego Trybunału Sprawiedliwości w sprawie *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*,wydana 8 lipca1996, ICJ Rep. 1996, par. 53

[792] Hathaway O.A., Crootof R. *The Law of CyberAttack,* Yale Law School Legal Scholarship Repository 3852 (2012) ss. 850-1

[793] ibid. S.849

[794] zob. Rule 43 *Tallinn Manual* wraz z jej rozwinięciem w *Tallinn Manual 2.0*

[795] zob. Rule 50 *Tallinn Manual 2.0*

istnieje zakaz przeprowadzania ataku cybernetycznego, czy szerzej - nawet użycia broni, o ile państwo przeprowadzające taką operację nie ma pewności, że celem jest system militarny. Tak pojmowana norma, stoi jednak w sprzeczności z normą prawa zwyczajowego dotyczącego konfliktu konwencjonalnego.[796] Ta bowiem, wyraźnie wskazuje że obiekty cywilne tracą swój immunitet w momencie, w którym są wykorzystywane dla celów wojskowych.[797] Różnica pomiędzy obiema normami sprowadza się do dwóch kluczowych punktów. Po pierwsze, istnieje istotna różnica w domniemaniu legalności działań, a co za tym idzie rozłożeniu ciężaru dowodów.[798] Po drugie istnieje różnica w zakresach przedmiotowych legalności ataku.

Norma wskazana w opracowaniu Czerwonego Krzyża, przyjmuje wyłącznie jedną przesłanką wyłączenie legalności- użycie obiektu dla celów militarnych. Według norm wskazanych w TM, sam fakt użycia sieci dla celów militarnych nie czyni z niej legalnego celu tak długo, jak połączona jest z nim sieć cywilna, a zastosowany środek przeprowadzenia operacji nie jest w stanie zaatakować wyłącznie sieci militarnej.[799] Ta różnica w normowaniu jest nierozwiązywalna na gruncie aktualnego stanu prawnego. Jedynym wnioskiem pozwalającym zachować niesprzeczność interpretacji jest przyjęcie, że norma wyrażona w *Tallinn Manual 2.0* dotyczy wyłącznie cyberprzestrzeni i jako taka stanowi *lex specialis* wobec normy wskazywanej przez Czerwony Krzyż. Brak jednak orzecznictwa lub praktyki międzynarodowej pozwalającej jednoznacznie potwierdzić zasadność takiej interpretacji. Dotychczasowa praktyka międzynarodowa, wskazuje raczej na szersze pojmowanie legalności celów, ponieważ mamy tu jednak do czynienia z metanormowaniem *lex informatica*, konieczna byłaby także zmiana normy zwyczajowej w prawie konfliktów

---

[796] zob. Rule 10 *Civilian Objects Loss of Protection from Attack*, *International Humanitarian Law Database* Międzynarodowy Komitet Czerwonego Krzyża, Oxford University Press, także art.art. 8(2)(b)(ii) i 8(2)(b)(v) Statut Międzynarodowego Trybunał Karnego *a contrario*

[797] *.Rule 10 Civilian Objects...*

[798] Kwestia problemu przeniesienia *onus probandi* na stronę atakującą, a więc pozbawioną kontroli nad obiektem będącym celem ze strony broniącej się, która obiekt kontroluje była już przedmiotem analiz prawnych. zob. *Conduct of the Persian Gulf War. Final Report to Congress* Departament Obrony Stanów Zjednoczonych (1992) par. 752

[799] Część IgoE przyjmuje wyjątek od opisywanej tu zasady w ten sposób, że o ile system wojskowy jest w jakikolwiek sposób odłączony od sieci cywilnej, możliwe jest stosowanie tam środków łamiących zasadę zakazu *indiscriminate attack*.

zbrojnych (a więc - normy prawa tradycyjnego: wymagającej nie tylko praktyki ale także *opinio iuris*). Wobec tego, nie jest możliwe ostateczne stwierdzenie która z norm jest właściwa. W istocie więc, takie rozróżnienie może stanowić podstawę dla działania *cyberlawfare*. O ile nie ma większego wpływu na sytuację prawną ataków prowadzących bezpośrednio do skutku kinetycznego - może mieć natomiast znaczenie kluczowe w ocenie prawnej ataku cybernetycznego poprzedzonego przez *CNE.* Jeżeli rozważymy sytuację, w której jedno państwa atakuje drugie w ten sposób, że instaluje *malware* rozstrajający działanie systemu dźwigów portowych w kraju zaatakowanym w ten sposób, żeby spowodować eksplozję amunicji ładowanej na okręty w tym porcie stojące. *Malware* ten według zamierzeń państwa wykonującego atak, ma doprowadzić do eksplozji, która może uszkodzić statki cywilne, a także zaatakuje całą sieć komputerową portu, w tym komputery sterujące dźwigami w części przeznaczonej dla marynarki handlowej, tak aby doprowadzić do wadliwego ich działania skutkującego uszkodzeniem zarówno ładunku jak i jednostek; a następnie dokonującego samoreplikacji w celu zainfekowania tych komputerów, nad którymi nie została przejęta kontrola podczas przeprowadzania właściwej operacji. Niewątpliwie tak skonstruowany atak, będzie spełniał przesłankę ataku, w rozumieniu Tallinn Manual.[800] Nie ma znaczenia czy atak zostanie skierowany w założeniu przeprowadzającej go strony przeciwko okrętom i magazynom wyłącznie wojskowym czy też także cywilnym (choć ta kwestia będzie istotna z punktu widzenia legalności). Istotny jest bowiem sam fakt możliwości wyrządzenia szkód materialnych. Sama kwestia legalności będzie podlegała dyskusji. Na mocy prawa zwyczajowego wyprowadzonego z norm konstruowanych przez *IGoE*, atak taki będzie nielegalny, ponieważ będzie przeprowadzony przeciwko obiektowi, który ma zastosowanie cywilne, a dodatkowo przy pomocy broni cybernetycznej o niepewnym efekcie. Według wskazanych powyżej norm Komitetu Czerwonego Krzyża, atak na wyłącznie wojskową część portu będzie legalny, niezależnie od ewentualnego cywilnego wykorzystania tej samej infrastruktury, ponieważ zgodnie z prawem humanitarnym,

[800] zob. Rule 30 *TM* zob.Rule 92 *także TM 2.0*

cel jest legalny, o ile 'jest wykorzystywany dla celów militarnych'.[801] Jego ewentualna następcza nielegalność może wyłącznie wynikać ze strat cywilnych przekraczających dopuszczalność w danej sytuacji poziom *collateral damage*. Dla obydwu stron różnica w normach będzie stanowić podstawę do konstrukcji odpowiedni strategii i taktyki ataku i obrony przed opisanym tu atakiem. Strona atakująca niewątpliwie wykona atak zgodnie z zapewniającymi jej szerszą legalność ogólnymi zasadami prawa humanitarnego. Paradoksalnie, oznacza to dla owej strony konieczność takiej konstrukcji ataku, który wyłączy z kodu użytego do przeprowadzenia ataku wszelkie ograniczenia dotyczące zakresu ataku. Zawarcie bowiem takich ograniczeń, *implicite* oznaczałoby stosowanie norm zawartych w *Tallinn Manual 2.0*, a w konsekwencji wyłączenie legalności całej operacji. Dla obrońcy natomiast konstruowanie systemów komputerowych w taki sposób, by atak na komputery militarne, był jednocześnie atakiem na systemy cywilne, jest legalnym sposobem ochrony własnych systemów za pomocą normowania faktycznego. Należy zauważyć, że istnieje zasadnicza różnica pomiędzy konstrukcją systemów komputerowych a zakazanym maskowaniem obiektów wojskowych jako cywilnych - zakazanym przez prawo międzynarodowego jako nielegalny podstęp wojenny,[802] łączący się z odmową spełnienia obowiązku informacyjnego o oznaczeniach sił zbrojnych.[803] Strona broniąca się, może powoływać się z bowiem z kolei na właściwe oznaczenie portu, a co za tym idzie na obowiązek takiego przeprowadzenia operacji przez stronę atakującą, by uniknąć zaatakowania systemów cywilnych. Nie istnieje bowiem żaden obowiązek rozdzielenia sieci, podobny do wskazanych wyżej norm zakazujących maskowania obiektów wojskowych jako cywilnych. Z samej zresztą istoty cyberprzestrzeni wynika, że byłoby to niewykonalne. Ochrona taka, byłaby

[801] zob. International Humanitarian Law Rule 10, także art. 52 Protokołu I do Konwencji Genewskich. Taką interpretację prawa zwyczajowego potwierdza także część doktryny, zob. na przykład Rado G. *Legitimate Military Targets* The Crimes of War Project (2001) s.1, także Petrovic J. *The Old Brigde of Mostar and Increasing Respect for Cultural Property in Armed Conflict* The humanitarian law series, Martinus Nijhoff Publishers (2013) ss.10-4

[802] zob. Art. 37(1)(c) i (1)(d)I Protokołu dodatkowego do Konwencji Genewskich z dnia 12 sierpnia 1949 r. dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych, Genewa 8 czerwca 1977 roku(Dz.U. 1992 nr 41 poz. 175)

[803] ibid. Art. 43(3)

nieskuteczna z punktu widzenia *lex informatica* lub nielegalna z punktu widzenia tradycyjnego prawa konfliktów zbrojnych. W przypadku operacji przechodzącej płynnie z *CNE* do cyberataku normowanie faktyczne umożliwia określanie stopnia legalności ataku, a także zakresu możliwej do wykonania obrony.

2. c. Natychmiastowość (Immediacy of Effect)

Czas który upłynął od przeprowadzenia ataku do wystąpienia jego skutków, może być sposobem oceny czy dana operacja jest atakiem. Kryterium to jednak jest jednostronne. O ile fakt wystąpienia skutków szybko ułatwia przypisanie skutków, ze względu na zmniejszenie liczy możliwych zmiennych, które miały wpływ na dany efekt, a więc ułatwia stwierdzenie dokonania ataku; upływ czasu, pomimo iż utrudnia rozpatrzenie sprawy, nie może wykluczać że do ataku jednak doszło. Dodatkową inferencją, którą z tego kryterium wyprowadza doktryna, jest założenie że niewielka odległość czasowa z reguły cechuje właśnie ataki z użyciem siły zbrojnej (*armed attack*)[804], natomiast rozdzielenie ich z reguły oznacza brak takiego ataku.[805]Jednak ani taka interpretacja tego kryterium ani nawet samo jego istnienie nie może być uznane za absolutne. Przede wszystkim - część ataków opiera się właśnie na rozdzieleniu lub wręcz warunkowości wystąpienia skutków. Jednym z przykładów takich operacji są ataki stanowiące drugi etap *CNE*. Innym przykładem rozdzielonego w czasie ataku może być zainstalowanie bomby logicznej, a więc kodu który wykonuje się w całości lub części zależnie od spełnienia się terminów lub warunków.[806] Sama bomba służy do uruchomienia dalszego etapu ataku, od którego konstrukcji zależne będą ostateczne skutki.[807] Szacuje się, że w systemach większości państw świata, znajdują się bomby logiczne umieszczone tam na wypadek pełnoskalowego konfliktu cybernetycznego.[808] Przykładem takich trudności, może

---

[804] zob. Ziółkowski K. *Ius ad bellum in Cyberspace*- Some Thoughts... ss.152-3
[805] zob.Schmitt M.N. *Cyberoperations and the Jus Ad Bellum Revisited...* ss.214-5
[806] zob.Robillard N. *Diffusing a Logic Bomb* SANS Institute (2004). s.7-11
[807] ibid. ss.12-4
[808] zob. Clarke R.A., Knake R.K. *Cyber War: The Next Threat to National Security and What to do About it* Ecco (2011) ss.15-9; 310-20

być opisany już wcześniej atak przy pomocy wirusa Stuxnet na Iran. Chociaż Stuxnet nie był *per se* bombą logiczną, sposób przeprowadzanie ataku miał pewne cechy podobieństwa. Przede wszystkim, istotny jest fakt, że Stuxnet został zainstalowany w systemach irańskich rok przed przeprowadzeniem ataku.[809] Stosowanie kryterium bezpośredniości do takiego ataku, nie jest wykonalne. Należałoby bowiem stosować je odrębnie najpierw dla naruszenia jurysdykcji Iranu poprzez zainstalowanie złośliwego kodu w jego systemach rządowych, a następnie analizować skutki kolejnych efektów. To jednak powodowałoby bezzasadne rozbicie logicznego ciągu na zjawiska, których nie można oceniać odrębnie. Podobne problemy mogą się także pojawić przy rozpatrywaniu ataków cybernetycznych przeprowadzanych w klasyczny sposób. Do takich wniosków musi doprowadzić choćby analiza ataku na systemy sterujące awaryjnym zrzutem wody na śluzach położonych na dużej rzece. Procedury takie atakowane są wyłącznie w sytuacji klęski żywiołowej. Zmiana elementu kodu, dokonana w drodze operacji cybernetycznej jest praktycznie niewykrywalna, nawet przy zachowaniu należytej ostrożności. Różni to atak cybernetyczny od porównywalnego konwencjonalnego. Ewentualny sabotaż kinetyczny, zostanie natomiast w analogicznej sytuacji zneutralizowany. Biorąc pod uwagę powyższe, należy przyjąć, że cele tego kryterium, które tak jak cały Test, ma na celu transpozycję kryteriów kinetycznych do cyberprzestrzeni, może mieć wyłącznie charakter subsydiarny.[810]

2. d. Bezpośredniość(Directness)

Kryterium podobne do natychmiastowości, jednak oparte na zastępującej odległość czasową, odległością kauzalną. Im dłuższy jest łańcuch przesłanek pomiędzy atakiem

---

[809] zob.Keizer G.*Stuxnet struck five targets in Iran, say researchers* artykuł opublikowany w. "Computerworld" 2/11 (2011)

[810] Tak na przykład K. Ziolkowski. Sam profesor Schmitt, powołując się na szkołę z *New Haven* (chodzi tu o sposób interpretacji prawa międzynarodowego mocno oparty o praktykę państw jako główne źródło interpretacji prawa, szczególnie wpływową na Uniwersytecie Harvarda) wskazuje, że cały opracowany przezeń test ma znaczenie wyłącznie pomocnicze, mając właśnie być pewnym zestawem kryteriów, według których państwa ocenią dane zachowanie, przyznając stronie zaatakowanej określone prawo do obrony. [w: Schmitt M.N. '*The Use of Force' in Cyberspace*... ss.313-6]

a skutkiem podlegającym mierzeniu, tym mniej prawdopodobne jest, że skutek ten nastąpił w wyniku ataku. Do kryterium bezpośredniości odnoszą się odpowiednio wszystkie wskazane powyżej zastrzeżenia, szczególnie kwestia bomb logicznych. Brak wiedzy jaki dokładnie kod został użyty w ataku uniemożliwia precyzyjne określenie, jakie są jego możliwe skutki, a więc także prześledzenie dokładnego łańcucha kauzalności.

2. e. Inwazyjność(Invasisveness)

Kryterium inwazyjności tyczy się naruszenia suwerenności państwa zaatakowanego w wąskim znaczeniu. Dla oceny istotny jest stopień w jakim naruszone zostały podstawowe przejawy suwerenności państwa (najczęściej chodzi tu o atak bezpośrednio na terytorium danego państwa lub cele znajdujące się pod ochroną jego jurysdykcji) w odróżnieniu od operacji skierowanych przeciwko jej mniej istotnym przejawom lub naruszającym suwerenność państwa wyłącznie pośrednio. Istotnym elementem oceny będzie tu także stopień w jakim naruszona została stabilność danego państwa. Dwie operacje; z których jedna będzie skierowana przeciwko infrastrukturze krytycznej państwa, druga natomiast będzie miała na celu zakłócenie kanałów łączności dyplomatycznej, skutkujące uniemożliwieniem zawarcia traktatu w określonych okolicznościach - będą naruszać suwerenność państwa w identycznym stopniu dopóki rozpatrywane będzie kryterium dotyczące suwerenności. Nie może jednak być wątpliwości, że atak na elementy gwarantujące stabilność państwa będzie wielokrotnie bardziej naruszał jego stabilność niż sabotaż uniemożliwiający zawarcie określonej umowy międzynarodowej. Część doktryny przyjmuje wprost, że przesłanki stabilności i bezpieczeństwa narodowego w odniesieniu do ataku, samoobrony czy uderzeń prewencyjnych muszą być rozumiane w najwęższy możliwy sposób, jako chroniące fizyczne bezpieczeństwo państwa i jego obywateli (a nie na przykład interesy ekonomiczne).[811] W oczywisty sposób, kryterium inwazyjności łączy się z kryterium bezpośredniości i dolegliwości. Należy pamiętać, że doktryna podkreśla,

[811] Ibid s.302.

że operacjom szpiegowskim (a tym samym operacjom *ISR*), należy przypisać zerowy stopień inwazyjności, a tym samym nie sposób uznać ich za atak.[812]

2. f. Mierzalność(Measurability)

Kryterium oparte o stopień możliwości oceny skutków ataku. Im bardziej widoczny i łatwiejszy do oceny skutek ataku, tym stopień mierzalności jest wyższy. Im większa siła ataku, tym bardziej wyraźny powinien być jego skutek. Atak polegający wyłącznie na niszczeniu danych w systemie, będzie miał niższą mierzalność niż atak polegający na komputerowym doprowadzeniu do uszkodzeń kinetycznych, które można łatwo skwantyfikować.[813] Kryterium to winno być stosowane w związku z kryterium bezpośredniości i opisanym poniżej kryterium inwazyjności, bowiem właściwy obraz ataku tworzy dopiero funkcja czasu wraz z jego inwazyjnością. Przyjmując argumentację przywołaną przy kryterium bezpośredniości, mierzalność należy także uznać za kryterium subsydiarne, mające mniejsze znaczenie.

2. g. Odpowiedzialność(Responsibility)

Kryterium odpowiedzialności sprowadza się do zaadaptowania wszystkich reżimów odpowiedzialności w prawie międzynarodowym do ataków cyberprzestrzennych i ocenie na jej podstawie stopnia zawinienia. Ze względu na obowiązki państwa, by nie umożliwiać łamania prawa z terytorium podległego własnej jurysdykcji w związku z ogólnym obowiązkiem naprawienia szkód,[814] musimy dojść do wniosku, że zgodnie z opisywanym kryterium, sam fakt dokonania ataku z terytorium danego państwa, będzie zachowaniem przez to państwo zawinionym. Jednak w cyberprzestrzeni (w przeciwieństwie do ataku kinetycznego) naruszenie jurysdykcji państwa z którego terytorium atak będzie przeprowadzony następuje w czasie,

[812] zob. Ziolkowski *Some Thoughts...* s. 298 i n.
[813] zob. Także Schmitt M.N. *Cyber Operations and the Jus...* ss.99-105
[814] zob. Art. 2 ARSIWA

w którym nie można rozsądnie oczekiwać reakcji na przejęcie takich systemów.[815] Przygotowanie do ataku przy pomocy środków militarnych wymaga czasu i przygotowań. Państwo na którego terytorium są one przeprowadzane, nawet jeżeli nie zdoła mu zapobiec, powinno mieć ich świadomość i ostrzec państwa, które ma zostać zaatakowane. W przypadku pośredniego ataku cybernetycznego (a więc mającego na celu wyłącznie uzyskanie dostępu do systemów danego państwa dla zamaskowania kierunku z którego przeprowadzany jest główny atak), od momentu naruszenia jurysdykcji do momentu,w którym atak jest prowadzony dalej (już poza tą jurysdykcją) upływają sekundy. Zgodnie z zasadą *impossibilium...*, nie można zasadnie oczekiwać żadnej reakcji. Samo więc przeniesienie ataku do cyberprzestrzeni, ogranicza faktycznie zakres przedmiotowy podmiotów mogących odpowiadać za czyn zabroniony do jego bezpośredniego sprawcy. Logiczną konsekwencją takiego określenia tego zakresu jest fakt, że także to kryterium może stosować się wyłączenie do bezpośredniego sprawcy.

2. h. Legalność ataku cybernetycznego i zagrożenia nim

Nie ma jednak wątpliwości, że skutkiem takiej konstrukcji prawa konfliktu cyberprzestrzennego stanowiącego funkcję tradycyjnego prawa konfliktów zbrojnych jak i normowania faktycznego *lex informatica* mamy do czynienia ze specyficznym systemem prawnym. Do ataku cybernetycznego, stosują się jednak ogólne zasady przeprowadzania ataków. Należą przede wszystkim dwie naruszalne zasady regulujące prawo każdego ataku. Należą do nich zasada programowa określająca ogólny cel legalnego ataku, którym może być wyłącznie ’ograniczenie zdolności działania wrogich sił zbrojnych’[816] i zasada unikania niepotrzebnego cierpienia.[817]

---

[815] zob. *Rule 61, 62, 64 Tallinn Manual 2.0* wraz z komentarzem IGoE ss. 290; 292-4 ; 298-300

[816] *Jedynym celem jaki państwa winny sobie stawiać w czasie wojny jest osłabienie sił nieprzyjaciela.*zob. Deklaracja w sprawie pocisków wybuchających małego kalibru, sygnowana w Petersburgu 11 grudnia 1868. cyt za. Gelberg I. *Prawo międzynarodowe i historia dyplomatyczna.* Polskie Wydawnictwo Naukowe t. 1 (1954)ss.253-7

[817] Pierwszy raz wyrażona w opinii Międzynarodowego Trybunału Sprawiedliwości w sprawie *Legality of the Threat or Use...* Powtórzona także przez IGoE w Prawidle 42

Obydwie te zasady nie są jednak w cyberprzestrzeni możliwe do wyegzekwowania. Po pierwsze, istnieją opisane powyżej problemy z atrybucją. Po drugie, brak możliwości określenia skutków wielu ataków cybernetycznych, uniemożliwia określenie poziomu 'nadmiernego cierpienia'. Ponieważ jest to przesłanka podmiotowa, możliwość określenia tych konsekwencji na poziomie planowania ataku jest konieczna dla przypisania odpowiedzialności podmiotowi, który atak przeprowadził. Atak powodujący przeciążanie reaktorów elektrowni atomowej będzie w oczywisty sposób takowe wywoływał, będąc w praktyce ekwiwalentem ataku atomowego. Natomiast atak służący kradzieży na dużą skalę materiałów objętych prawem autorskim, może jednocześnie spowodować duże straty, wystarczające do uznania go za atak, ale nie spowodować żadnego cierpienia.[818] Z powodu natomiast połączenia sieciowego komputerów, atak na cele militarne, może być jednocześnie atakiem na cele cywilne. Stan prawny komplikuje dodatkowo sformułowanie normy zakazującej użycia broni (w tym cybernetycznej), której natura może spowodować nadmierne cierpienia.[819] W pierwotnym zamyśle, norma ta miała ograniczać możliwość używania broni, których efekt mógłby rozszerzyć się poza cele militarne. Jednak regulacja ta, pochodząca z końca wieku XIX., w oczywisty sposób nie przewidywała problemów związanych z cyberprzestrzenią i prowadzeniem w niej wojny. Norma ta została rozszerzona tak, by obejmować swoim zakresem także środki prowadzenia wojny (a nie tylko broń) i o równorzędną przesłankę negatywną 'nadmiernych uszkodzeń'.[820]W cyberprzestrzeni każda broń i metoda prowadzenia wojny może spowodować wspomniane 'nadmiernie uszkodzenia', nawet w sytuacji,

---

Tallinn Manual. Zasada ta została uznana przez Trybunał za 'nienaruszalną, niezależnie od okoliczności' [w: opinii *Legality of the Threat...*]. zob. Także Prawidło 31 *TM*

[818] Podobną do opisywanej sytuacją była operacja hakerska przeprowadzona przez północnokoreańskich hakerów przeciwko serwerom należącym do koncernu Sony w celu wykradzenia i opublikowania w sieci filmu wyśmiewającego rząd tego państwa. O ile w tym przypadku cel operacji niewątpliwie wyłącza możliwość uznania operacji za atak, zmiana na spełniający kryterium ataku ciągle nie oznaczałby spełnienia przesłanki 'nieuzasadnionego cierpienia'. zob też Schmitt M.N. *International Law and Cyber Attacks: Sony v. North Korea,*artykuł opublikowany na justsecurity.org 17/14 (2014) ss.2-3

[819] zob. Art. 23(e) Konwencji dotyczącej praw i zwyczajów lądowej(II Konwencja Haska z 29 lipca 1899 roku) opublikowana w Dz. U.. 1927 nr 21 poz. 161. Norma ta została potwierdzona w art. 35(2) I Protokołu Dodatkowego.

[820] zob. Art. 35(2) I Protokołu Dodatkowego

w której uszkodzenia (w przewidywalnym zakresie) zostały wykluczone na etapie planowania operacji. W odróżnieniu od wspomnianej wcześniej odpowiedzialności podmiotu prawa międzynarodowego za spełnienie przesłanki planowania ataku w sposób powodujący nadmierne cierpienia lub uszkodzenia, dla określenia samej legalności ataku stopień zawinienia jest nieistotny. Atak taki byłaby bowiem nielegalny, brak zamiaru oznaczałby wyłącznie brak możliwości przypisania zawinienia podmiotowi prawa międzynarodowego, ale nie czyniłby ataku *per se* legalnym. Ponieważ konsekwentne stosowanie tej normy, oznaczałoby wyłączenie możliwości przeprowadzania jakichkolwiek ataków cybernetycznych (ponieważ każdy potencjalnie mógłby przekroczyć opisywaną granicę, a możliwość spełnia przesłankę nielegalności), w konsekwencji oznaczałby zakaz ich przeprowadzania. Jest jednak oczywiste, że praktyka międzynarodowa i cały system prawa międzynarodowego przeczy temu wnioskowi. Ponieważ zakaz ten nie został wyrażony *explicite*, a byłby wyłącznie interpretowany z innych norm dodatkowo sugerujących legalność takich ataków (ponieważ inaczej w ogóle nie podlegałyby jakimkolwiek regulacjom- jako *malum per se*), stałoby to w sprzeczności z wykładnią systemową i sugerowało sprzeczność w normach wynikających z traktatu. Ponieważ zasady wykładni zakładają eliminację sprzeczności, nie można też przyjąć że państwa-sygnatariusze dążyły do związania się niemożliwym, należy uznać że taka interpretacja nie jest prawidłowa. Dodatkowo, należy wskazać że w praktyce zakaz operacji cybernetycznych byłby silniejszy niż zakaz przeprowadzania ataków przy pomocy broni atomowej[821], co należałoby uznać za interpretację absurdalną. Skoro więc nie sposób uznać ataków cybernetycznych za nielegalne, normą, która w praktyce zakazuje ich przeprowadzania, należy uznać za niezgodną z zasadą *impossibilium nulla obligatio est*.

Jak wskazano powyżej prawo międzynarodowe zakazuje nie tylko samego użycia siły, ale także nielegalnej groźby jej użycia.[822] Orzecznictwo jako ogólną zasadę przyjmuje, że legalność zagrożenia użyciem siły należy zgodnie z zasadami

[821] Zarówno zagrożenie jak i nawet użycie broni atomowej nie zostało w sposób jednoznaczny wyłączone przez MTS[w: *Legality of Threat or Use of Nuclear...*par.17]
[822] Zakazana *explicite* przez art. 2(4) KNZ

przeprowadzania rozumowania *a fortiori* oceniać łącznie z oceną legalności samego użycia siły, uznając że skoro legalne w danym wypadku jest użycie siły, tym bardziej nie może być nielegalne zagrożenie tym użyciem, jako środek w mniejszym stopniu naruszający suwerenność państwa trzeciego. Międzynarodowy Trybunał Sprawiedliwości podobnie argumentując wskazywał dolną granicę legalności; jeżeli nielegalne jest użycie siły, nie może być legalne zagrożenie.[823] *Ratio legis* tej normy leży w nielegalności interferencji (a nie nieinterwencji), wyłączając możliwość wpływania na działania danego podmiotu prawa międzynarodowego. Znacząca część doktryny uważa, że zagrożenie użyciem siły może być użyte jako środek samoobrony,[824] o ile zgodnie z przedstawioną powyżej argumentacją samoobrona ta jest w danej sytuacji legalna.[825]

2. i. Samoobrona .

Karta zakłada także prawo każdego podmiotu prawa międzynarodowego do obrony własnej suwerenności.[826] Prawo konfliktu cyberprzestrzennego zakłada, że samoobronę uruchamia użycie siły, a więc operacja, która spełnia kryteria Testu Schmitta.[827] Musi także spełniać warunek istotności a więc przekraczać poziom *border clashes* określony w *Nicaragua*.[828] Tak zdefiniowane prawo do obrony (w tym obrony kinetycznej) pozostawia dwie istotne luki. Po pierwsze, w przypadku *CNE* przekształcających się następczo w atak kinetyczny - na obronę jest w momencie spełnienia opisanych tu przesłanek zbyt późno. W przypadku więc odrzucenia koncepcji domniemania, pozbawia to państw możliwości legalnej obrony własnej suwerenności przy pomocy środków innych niż obrona pasywna. Drugim

---

[823] zob. opinię MTS w sprawie *Legality of the Threat...* par.4 także sir Wood, M. *Use of Force, Prohibiton of Threat* zbiorowa, red. Wolfram R. Fundacja Maxa Plancka. (2013) par.1 in

[824] Groźba może być nawet wyrażona konkludentnie.zob. Orzeczenie MTS w sprawie *Corfu Channel* par.30 i n.

[825] zob. Williamson M. *Terrorism, Was and International Law: The Legality of Use of Force Against Afghanistan in 2001* Liverpool Law Review 31:3 (2010)s.317 .

[826] zob. Art. 51 KNZ *Nic w ninieszej Karcie,nie może uchybiać niepozbywalnemu prawu do samoobrony indywidualnej lub zbiorej w przypadku napaści zbrojnej[...]*

[827] zob. Rule 71 *Tallinn Manual 2.*, wraz z komentarzem.ss.339-40

[828] zob. *Nicaragua...* par 191 także *Tallinn 2.0 ...* ss.341-2

problemem, jest brak wystarczających regulacji dotyczących niekinetycznych konfliktów cybernetycznych. W oczywisty sposób, nie mogą być one uregulowane w tradycyjnym prawie konfliktów zbrojnych. Jedyne dostępne regulacje tego poziomu użycia siły wynikają więc z *lex informatica* i afordancji. Jednak afordancje w tym zakresie prowadzą w logicznej konsekwencji do uzależnienia skuteczności tych ataków wyłącznie od różnicy potencjałów - tworząc "legislacyjny dziki zachód".[829] Zakres odpowiedzi na niekinetyczny atak cybernetyczny należy uznać za zakres nieomal absolutnie nieunormowany.

Drugim aspektem osłabiającym możliwość ochrony suwerenności w cyberprzestrzeni jest fakt, że w tradycyjnym prawie konfliktów zbrojnych (a więc w konsekwencji, także w prawie regulującym kinetyczne konflikty cyberprzestrzenne) - prawo do samoobrony jest wyłącznie środkiem tymczasowym. Realne działania w celu zapewnienia pokoju podejmuje bowiem Rada Bezpieczeństwa ONZ i to ona ostatecznie decyduje o środkach, które zostaną podjęte dla przywrócenia pokoju.[830] Przeniesienie tego przepisu na grunt cyberprzestrzeni nie jest jednak łatwe. Operacje cyberprzestrzenne, najczęściej odbywają się w bardzo szybkim tempie, zawiadomienie Rady Bezpieczeństwa i uzyskanie jej stanowiska może wykraczać poza ramy czasowe ataku. Normy służące ocenie legalności ataku, jak Test Schmitta nie podlegają ocenie żadnego organu międzynarodowego, co wynika oczywiście z braku powołania jakiegokolwiek organu do oceny działań wyłącznie cyberprzestrzennych Teza autora Testu podnosząca, że to społeczność międzynarodowa oceni jak zastosować kryteria[831] jest oczywiście słuszna, ale nie wystarczająca. Należy więc *de lege ferenda* postulować przejęcie tej roli przez Radę Bezpieczeństwa ONZ. Należałoby jednak także rozważyć stworzenie osobnej

---

[829] Określenie używane przez amerykańską doktrynę prawa cyberprzestrzeni, które obrazowo oddaje skutek przekazywania coraz większych zakresów przedmiotowych prawa cyberprzestrzeni do normowania faktycznego *lex informatica*. zob. Singh P. *A Death Knell for the International Norms of Cyber Conflict*, Modern War Institute (2019) par.5

[830] ibid. *[...]Środki podjęte przez członków w wykonaniu tego prawa do samoobrony ędą natychmaist podane do wiadomości Radzie Bezpieczńęstwa i w niczym nie mogą uszczuplać władzy i odpowiedzialności Rady Bezpieczńestwa, wynikających z niniejszej Karty, do podejmowania w każdym czasie takiej akcji, jaką ona uzna za niezbędną do utrzymania lub przywrócenia międzynarodowego pokoju i bezpieczeństwa.*

[831] zob. Schmitt M.N. *'The Use of Force in Cyberspace', a Reply...*

procedury wydawania przez nią rezolucji w tym zakresie. RB może podejmować działania wyłącznie w wypadku wyrażenia zgody wszystkich jej stałych członków.[832] Ze względu na dotychczasowe problemy z taką konstrukcją, utrudniającą często podjęcie decyzji lub podporządkowującą ją procesom politycznym, model ten podlega częstym dyskusjom.[833] W sytuacji konfliktu cyberprzestrzennego ewentualne rezolucje byłyby (w razie zajęcia się tym zakresem konfliktów przez RB ONZ) podejmowane w identyczny sposób. Wobec opisanych powyżej problemów z dokonywaniem atrybucji i o ile ataku nie dokonały siły zbrojne danego państwa, kwestią sporną będzie na przykład kwestia nie tylko atrybucji, ale też przypisania odpowiedzialności państwu, któremu atak atrybuowano. Dodatkowo w przeciwieństwie do ataku kinetycznego regulowanego przez normy zwyczajowego prawa międzynarodowego - ataki cybernetyczne w dużej mierze regulowane są przez prawa krajowe, niekoniecznie kompatybilne. Brak identyczności norm uniemożliwia określenie praktyki międzynarodowej, która musiałaby wynikać ze spójnych działań w ramach *lex informatica*. O ile brak przypadku rozpatrywania przez Radę ataku cybernetycznego, pewien praktyczny obraz opisywanej powyżej komplikacji daje, załamanie się trwających 13 lat negocjacji na temat normowania ograniczeń możliwości prowadzenia cyberoperacji i ustalenia jednoznacznej zasady prawnej regulującej odpowiedzi kinetycznej na nie.[834] Fakt, że w zasadzie wszyscy stali członkowie RB ONZ nie mogli się porozumieć co do zasad stosowania prawa konfliktów w cyberprzestrzeni *in abstracto*, wskazuje jasno z jakimi trudnościami spotkałaby się próba rozpatrzenia rzeczywistego przypadku takiego ataku.[835] O ile więc niewątpliwie rezolucja RB ONZ byłaby środkiem pozwalającym na

---

[832] zob. art. 27(2) KNZ.

[833] zob.*Reforma ONZ* notatka MSZ RP

[834] zob. Bowcott O. *Dispute along cold war lines led to collapse of UN cyberwarfare talks*.artykuł opulibkowany 23 sierpnia w 2017 roku w 'The Guardian'.

[835] Chodzi tu o załamanie 23 czerwca 2017 roku obrad V GGE (Group of Governmental Experts) poprzez odrzucenie raportu końcowego, między innymi przez Federację Rosyjską i Chińską Republikę Ludowo-Demokratyczną. Raport dotyczył stosowania prawa o czynach zabronionych, prawa do samoobrony (w tym retorsji,represaliów i inferowanego z nich prawa do uderzeń prewencyjnych) i stosowalności międzynarodowego prawa humanitarnego do wojny w cyberprzestrzeni. Szczegółowa analiza prac 5 GGE, zob. *Schmitt M.N., Vihul L. International Cyber Law Politicized: The UN GGE's Failure to Advance Cybernorms, Just Security 30/06/17 (2017)*ss.8-11

bezdyskusyjne określenie zakresu i ram czasowych odpowiedzi legalnej obrony, nie wydaje się możliwe, by środek ten był możliwy do zastosowania z powodów faktycznych. Za dużo skuteczniejszy środek obrony suwerenności w odniesieniu do cyberprzestrzeni należałoby więc uznać opisany powyżej mechanizm oparty o art. 2(3)(4) Karty (w odniesieniu do kinetycznych cyberataków) i o koncepcję domniemania zakresu operacji (w przypadku *CNE* i cyberataków niekinetycznych).

3. Ograniczenia prowadzenia konfliktu w cyberprzestrzeni

Poniżej zostaną omówione dwa środki prowadzenia konfliktu zbrojnego, których cechą wspólną jest wprowadzenie w błąd przeciwnika lub wykorzystanie takiego błędu. Wiarołomstwo i podstęp, jako instytucje pochodzące z tradycyjnego prawa konfliktów kinetycznych, mają ustalone znaczenie, które jednak nie może być precyzyjnie transponowane do prawa konfliktu cyberprzestrzennego i jak pozostałe instytucje, umieszczone w tym systemie w drodze analogii, nabierają nowego znaczenia.

3. a. Wiarołomstwo(Perfidy)

Jest to sposób prowadzenia konfliktu, polegający na wykorzystaniu zaufania strony przeciwnej do określonych oznaczeń lub symboli chronionych międzynarodowo - Czerwonego Krzyża, Narodów Zjednoczonych lub oznaczeń państw neutralnych – w celu uzyskania nieuprawnionej przewagi militarnej. Co do zasady, można przyjąć że wiarołomstwem będzie każde celowe i bezpodstawne symulowanie przez jedną ze stron konfliktu stanu, w którym atak na nią byłby zbrodnią wojenną. W klasycznym prawie konfliktu jest ono zakazane przez Konwencje Genewskie[836] i ścigane jako zbrodnie wojenne[837]. Doktryna podtrzymuje, że wiarołomstwo jako takie jest także zabronione podczas konfliktu cyberprzestrzennego,[838] jednak istnieją daleko idące

[836] zob. Art. 37(1) I Protokołu Dodatkowego

[837] zob. Art. 8 Statutu Międzynarodowego Trybunału Karnego (Statutu Rzymskiego) z 17 czerwca 1998 wraz z późniejszymi zmianami.

[838] zob. Rule 123 *Tallinn Manual 2.0*wraz z komentarzem IGoE ss.495-6

spory co do tego jak należy je definiować. Dobrami prawnymi chronionymi przez zakaz wiarołomstwa jest życie i zdrowie belligerentów, którzy mogliby zostać zaatakowani w sposób opisany powyżej jak i zaufanie (determinujące ich skuteczność) do międzynarodowych oznaczeń zakazujących przeprowadzania uderzeń na określone obiekty lub osoby. Przesłanką pozytywną wiarołomstwa jest jakakolwiek szkoda na osobie.[839] 1 Protokół Dodatkowy, rozszerza ten zakres o zakaz pozbawiania wolności kogokolwiek w sytuacji wynikłej z wiarołomstwa. O ile w przypadku konfliktu kinetycznego, zakres ten wydaje się być wystarczający w przypadku cyberprzestrzeni, pomija wiele możliwych zachowań. Wiarołomstwo w konflikcie fizycznym, musi dotyczyć ataku na osoby, w cyberprzestrzeni nie jest to konieczne. Możliwy jest przykładowo scenariusz, w którym państwo zaatakuje swojego przeciwnika poprzez przeprowadzenie ataku polegającego na zainstalowaniu *malware* fizycznie uszkadzającego dyski twarde w systemach obrony cybernetycznej państwa zaatakowanego. Program taki jest bronią cybernetyczną zgodnie z podaną wyżej definicją, zostaje użyty w operacji cybernetycznej, która ma skutki kinetyczne przekraczające próg użycia siły, jednakże zostaje użyty w ataku, który nie wyrządza ani nie może wyrządzić szkód na osobie, ponieważ zostaje użyty wyłącznie przeciwko określonym dyskom, nie może także ze względu na swoją konstrukcję rozprzestrzenić się w sieci państwa zaatakowanego w taki sposób, by zakłócić działania sieci cywilnych. Tak skonstruowana broń cybernetyczna spełniałaby wszystkie kryteria legalności. Jednakże powstaje wątpliwość, jak traktować sytuację, w której rozpoczęcie ataku, a więc samo wprowadzenie *malware* do systemów państwa zaatakowanego dokonuje się w drodze przesłania wiadomości e-mail, zamaskowanej jako wysłanej przez Czerwony Krzyż. Na drodze wykładni językowej,[840] i jak się wydaje także systemowej- jedną możliwą interpretacją jest przyjęcie, że do wiarołomstwa nie doszło; nie została spełniona bowiem konieczna

[839] zob.Art. 23(b) IV Konwencji Haskiej zakazujący przede wszystkim 'zdradzieckiego zabijania lub ranienia osób służących w przeciwnych armiach lub obywateli przeciwnego narodu'.

[840] zob. Eberlin Ph. Gasser H.-P., Wenger Cl.F. [w: zbiorowa,*Komentarz do Protokołów Dodatkowych do Konwencji Genewskich* red. Sandoz Y., Swinarski Ch., Zimmermann B. International Committee of the Red Cross, wyd. Martinus Nijhoff Publishers, Genewa (1987)]par. 1493,

przesłanka pozytywna szkód na osobie. Z punktu widzenia czysto funkcjonalnego jednak, wiarołomostwo zostało popełnione. Brak szkód, nie ma też znaczenia dla ochrony drugiego z dóbr - zaufania do oznaczeń niekombatantów. Z punktu widzenia państwa zaatakowanego, istotny bowiem będzie fakt, że doszło do naruszenia suwerenności tego państwa przy pomocy symboli prawnie chronionych. Dodatkowo, należy zauważyć, że o ile za nielegalne uznawane jest każde wykorzystanie symboli neutralności,[841] penalizowane jest wyłącznie użycie ich w celu wiarołomstwa.[842] Grupa Ekspertów uznaje wspomnianą przesłankę za istotną - podając przykład sfałszowanej wiadomości *e-mail* udającej wiadomość od Czerwonego Krzyża w celu zwabienia określonej osoby na miejsce zasadzki lub ataku na rozrusznik serca przy pomocy fałszywej aktualizacji jego oprogramowania.[843] Wydaje się, że ta interpretacja, jakkolwiek zgodna z ogólną zasadą inkorporacji do prawa cyberprzestrzeni norm prawa konfliktów zbrojnych, wydaje się zbyt wąska. Zakres możliwych operacji przy pomocy wiarołomstwa jest w cyberprzestrzeni dużo szerszy i obejmuje cały zakres możliwych zastosowań nielegalnego dostępu do sieci (w tym przykładowo obejścia obrony pasywnej).

W 2017 roku, dokonano skutecznej cyberoperacji przeciwko internetowemu centrum zgłoszeniowemu FBI. Sprawcy wysyłali następnie do ofiar cyberprzestępstw e-maile będące dokładną kopią formularza informującego służby o przestępstwie używanego na zaatakowanej stronie, z dołączonym skryptem przekierowania, powodującym przesyłanie wypełnionych formularzy na nieznany adres i w konsekwencji kradzież dalszych danych.[844] Przeprowadzenie identycznej operacji, w identycznym celu wykonana przez aktorów niepaństwowych, będzie niemożliwa do przypisania jakiemukolwiek podmiotowi prawa międzynarodowego.[845]

---

[841] ibid. Komentarz do art. 37(1)

[842] por. Art. 85 I Protokołu Dodatkowego. Także art.8 Statutu Rzymskiego *a contrario*.

[843] zob.*TM2.0 ss.495 i n.*

[844] zob. Oświadczenie FBI z dnia 1 lutego 2018 roku, o sygnaturze I-020118-PSA.

[845] Możliwe byłoby oczywiście przypisania sprawcom winy na podstawie wewnętrznego prawa karnego poszczególnych państw, nie zmieniałoby to jednak stanu prawnego i faktycznego pomiędzy stronami w rozumieniu prawa międzynarodowego publicznego.

3. b. Podstęp(Ruse)

Podstęp jest zachowaniem podobnym do wiarołomstwa w tym, że także polega na takim prowadzeniu konfliktu, żeby wykorzystać nieświadomość strony przeciwnej. W odróżnieniu jednak od wiarołomstwa, podstęp nie opiera się na oszustwie dotyczącym chronionych dóbr, ale wykorzystuje dezinformację, mieszczącą się w normalnych kanonach prowadzenia działań zbrojnych. Jako taki jest normalnym elementem prowadzenia wojny i działań wywiadowczych, a każda strona konfliktu musi się liczyć z możliwością wprowadzenie jej w błąd przez stronę przeciwną.[846] Przykładem podstępu może być tworzenie sztucznego ruchu radiowego, lub rozstawienia makiet sprzętu wojskowego, sugerującego istnienie dodatkowych oddziałów w teatrze wojny. Przyjmuje się, że podstęp jest zachowaniem legalnym.[847]Nie jest to jednak legalność bezwzględna, chociaż trwają spory w doktrynie, gdzie przebiega granica pomiędzy wiarołomstwem a zabronionym podstępem. Dla zakresu pracy niniejszej ten spór nie jest jednak istotny, wystarczające jest przyjęcie mającej status prawa zwyczajowego zasady interpretacyjnej wskazującej, że żaden podstęp nie może legalizować zachowania inaczej zakazanego.[848] W cyberprzestrzeni podstępy stanowią głównie elementy obrony pasywnej (na przykład poprzez tworzenia fałszywych serwerów z nieistotnymi danymi, mającymi udawać dane, które mogą być celem *CNE*). Do podstępów należy stosować zasadę ograniczania narażania cywili.[849]

3. c. Obiekty cywilne i ich ochrona. Konieczność zachowania środków ostrożności

Konwencje chronią obiekty cywilne nie tylko przed bezpośrednim atakiem, ale także wymagają planowania operacji militarnych w sposób, który w jak największym stopniu wyłączy możliwość przypadkowego lub nieplanowanego uderzenia w te

[846] zob. art. 37(2) *I Protokołu Dodatkowego* wraz z komentarzem [w: *ICC Commentary... Sandoz, Swiniarski, Zimmermann...*] par. 1515 i n.
[847] ibid.par.1515
[848] ibid. par. 1515
[849] zob. Rule 93 w związku z Rule 123 *Tallinn Manual 2.0*

obiekty.[850] Nie ma wątpliwości, że te same wymogi stosuje się do operacji prowadzonych w cyberprzestrzeni a ich ewentualne naruszenie będzie jednym z podstawowych czynników dotyczących oceny stopnia naruszeń suwerenności i legalności danego ataku.[851] W cyberprzestrzeni z jej zasadą wszechobecnego dostępu, planowanie takich operacji napotyka jednak na problemy techniczne. Przede wszystkim, częstokroć nie ma możliwości określenia położenia infrastruktury (co stanowi jedną z przesłanek uznania celu za militarny lub cywilny) na poziomie planowania ataku. Prawo konfliktu cyberprzestrzennego wyłącza natomiast możliwość wykorzystanie wyłącznie numerów *IP* lub *DNS* do tego celu.[852] Ogólna norma prawa konfliktów zbrojnych mówi, że za cel militarny można przyjąć także obiekt, który ma co do zasady charakter cywilny, jednakże jest w danym momencie używany do celów militarnych.[853] W cyberprzestrzeni ta zasada stanowi istotny problem ponieważ sieciowość cyberprzestrzeni uniemożliwia rozróżnienie sieci militarnych i cywilnych. W praktyce więc, w cyberprzestrzeni możliwość rozgraniczenia cywilnych i militarnych celów może odbywać się wyłącznie w oparciu o kryterium funkcjonalne - efektywnego wpływu na działania (lub potencjał) militarny. Taka koncepcja wymaga przypisania podstawowej roli w tej ocenie *lex informatica.* Wyłącznie zrozumienie funkcjonowania odpowiednich norm faktycznych może pozwolić stronom na określenie przypisywanego im celu w architekturze systemu.

3. d. Ochrona dziennikarzy

Prawo do ochrony dziennikarzy relacjonujących konflikt zbrojny, ma swoje źródło w rezolucji Narodów Zjednoczonych, uznających że chronieni reporterzy stanowią dodatkowe zabezpieczenie przed łamaniem praw konfliktu zbrojnego.[854] Mogłoby się

---

[850] zob.Cz.IV, sek. I, Rozdział III (ochrona), IV (środki ostrożności) i V (strefy pod specjalną ochroną) *I Protokołu Dodatkowego do Konwencji Genewskiej z 1949...*

[851] Jeżeli bowiem naruszenie suwerenności jest legalne, państwo obowiązane jest je znosić.

[852] zob. Komentarz IGoE do Rule 100 *Tallinn Manual 2.0* par.9

[853] Komentarz do 1 Protokołu Dodatkowego par. 2020

[854] zob. Rezolucję Narodów Zjednoczonych 2673(XXV) z 9 grudnia 1970 roku, cyt. za

wydawać, że w konflikcie cyberprzestrzennym, prawo to nie ma zastosowania. Po pierwsze jednak, dziennikarze mogą znajdować się na polu konfliktu sieciowego. Ich obecność będzie wpływała na jego prowadzenie. Po drugie, ze względu na *ratio legis* ochrony dziennikarzy, nie ma żadnego powodu by kwestionować istnienie norm chroniących dziennikarzy w konflikcie cyberprzestrzennym. Po trzecie natomiast, ze względu na sieciowość, dziennikarze jak każdy inny podmiot ochronny mogą zostać wykorzystani według stosowania *cyberlawfare*. Brak jest legalnej definicji dziennikarza, poza przesłanką negatywną, wyłączającą z tego zakresu ochrony członków sił zbrojnych[855] i przesłanką pozytywną właściwego oznaczenia.[856] W środowisku wojny sieciowej, tradycyjnie pojmowane oznaczenie nie jest wystarczające. Systemy broni nie kierowane w czasie rzeczywistym przez człowieka, lub nie mające możliwości wizualnej identyfikacji oznaczeń, do realnego działania wymagałyby użycia specjalnych transponderów emitujących sygnał rozpoznawalny przez te systemy. Systemy prasowe niewątpliwie zawierają też dane wrażliwe w środowisku konwencjonalnego konfliktu. Ich przesyłanie przez sieci komputerowe, naraża je na przechwycenie i wykorzystania przez stronę konfliktu. Możliwość namierzenia przesyłanych zdjęć, czy też natychmiastowej reakcji na przejęte informacje, czyni z systemów dziennikarskich cel ewentualnych cyberoperacji.[857] Mamy w tym przypadku jednak do czynienia z podwójną luką prawną. Ewentualna operacja w celu uzyskania informacji z takiego źródła musiałby bowiem zostać uznana za szpiegostwo, a tym samym być (międzynarodowo) legalna. Do podobnych wniosków musi prowadzić literalna interpretacja normy nakazującej ochronę dziennikarzy.[858] Jednakże już jej interpretacja funkcjonalna, winna takich operacji zakazywać, ponieważ narażają one dobro prawne, jakim jest obecność dziennikarzy w miejscu konfliktu, w sposób porównywalny z bezpośrednio na nich dokonanym

IRRC (1971) s.3

[855] zob. *Komentarz do I Protokołu* par. 3261 i 3262

[856] ibid. Par. 3272

[857] Jedyną sankcją za podobną operacją byłaby, zgodnie z prawem zwyczajowym, utratę statusu członka sił zbrojnych. zob. Prawidło 66(b) TM. Jednakże samo naruszenie sieci prasowej, bez zamiaru pozyskania z niej danych, byłoby wyłącznie wykorzystaniem sieci (Computer Network Exploitation) i nie pozbawiałoby ochrony dokonującego jej podmiotu.

[858] zob.art. 79 I Protokołu Dodatkowego

atakiem. Drugą z luk prawnych, jest brak realnej możliwości obrony przez państwo, dla sił zbrojnych którego informacje przejęte z systemów prasowych mogą stanowić zagrożenie. Jeżeli bowiem dochodzi do opisywanej powyżej operacji, państwo takie nie może w żaden sposób przeciwdziałać, ponieważ jakakolwiek ingerencja mające na celu uniemożliwienie przesyłu danych, byłaby już co najmniej cyberoperacją albo wręcz cyberatakiem skierowanym albo przeciwko prasie bezpośrednio albo przeciwko częściom infrastruktury cyberprzestrzennej użytej do ich przesyłu – w każdym więc wypadku - czynem zabronionym międzynarodowo. Ewentualna zmiana praktyki międzynarodowej w tym zakresie mogłaby pozwolić na obronę(choć byłoby to niewątpliwie naruszanie zasady bezwzględnej ochrony niebeligerentów), jednakże nie rozwiązywałoby to problemu legalności wykonania cyberszpiegostwa w systemach prasowych. Co niezwykle istotne, dzisiejszy stan zwyczajowego prawa międzynarodowego, zarówno w zakresie praktyki międzynarodowej, jak i w zakresie *opinio iuris,* zakazuje ataków na dziennikarzy, natomiast nie wkłada na na podmioty prawa międzynarodowego obowiązku jakiejkolwiek ich ochrony w pozytywnym sensie.[859] Obowiązek nieatakowania natomiast ograniczony jest wyłącznie do osób dziennikarzy.[860] *A contrario* nie dotyczy więc zebranych danych materiałów, sprzętu wraz ze środkami zapisu i tym podobnych. Norma jest oczywiście zrozumiała w przypadku wojny fizycznej, natomiast w cyberprzestrzeni umożliwia legalność całego spektrum operacji, mogących mieć następczą, pośrednią ekwiwalencję kinetyczną. Podobnie, zdobywanie informacji poprzez cyberoperację skierowaną przeciwko systemom lub sprzętowi należy więc do czynów z punktu widzenia prawa międzynarodowego legalnych.[861]

[859] zob. Komentarz do art. 79 TM [w: *Kometnarz IGoE]* par. 2

[860] ibid. par.3

[861] Dla kompletności wywodu, należy odnotować, że sprzęt należący do prasy należy traktować jako obiekty cywilne. Operacja cybernetyczne prowadzące do zniszczenia lub uszkodzenia takiego sprzętu, będą co do zasady nielegalne na podstawie prawidła *38 TM.*

3. e. Ściganie łamania norm prawa konfliktu w cyberprzestrzeni.

Stanowienie norm wewnętrznych mających na celu powstrzymanie łamania norm[862] opisanych powyżej jak i ściganie sprawców czynów zabronionych jest zarówno obowiązkiem jak i prawem państw.[863] Nakaz ten stosuje się w takim samym stopniu do cyberprzestrzeni jak i do działań kinetycznych. Niewątpliwie z teoretycznego punktu widzenia jest on środkiem pozwalającym państwom chronić własną suwerenność. Otwarta jednak pozostaje kwestia, na ile normy są praktycznie stosowalne w cyberprzestrzeni. O ile nie ma wątpliwości, że nakaz ten ma charakter normy wiążącej *erga omnes* i nie istnieją przesłanki, by wyłączyć jego stosowalność do cyberprzestrzeni, otwarta pozostaje kwestia jego wykonalności. Niezależnie od tego jaką formą przyjmie naruszenie prawa humanitarnego w cyberprzestrzeni, zarówno ściganie jak i działania mające na celu zapobieganie zdarzeniom muszą obejmować analizę danych, które same pozostają poza zakresem jurysdykcji w jakimkolwiek jej rozumieniu. Jedyny możliwy wniosek wynikający z interpretacji funkcjonalnej wspomnianego nakazu, jest więc taki, że jest to metanorma wiążąca państwa by wykorzystały własną jurysdykcję do tworzenia afordancji utrudniających lub uniemożliwiających naruszenia. Wykonywanie jurysdykcji nadzwyczajnej jest możliwe wyłącznie w przypadku wykonania atrybucji, a więc faktycznie niezmiernie ograniczone, w tym także istniejącymi możliwościami przypisania winy podmiotowi prawa międzynarodowego. Dyskusyjna musi być także interpretacja zakładająca, że wspomniana norma musi być spełniona poprzez zawarcie odpowiednich traktatów ponieważ taka interpretacja łamałaby zasadę swobody wiązania się traktatami.[864] Nadto, musiałaby ona ulec zakwestionowaniu ze względu na praktykę

---

[862] zob. wspólny komentarz dla art. 49/50/129/146/50/51/130/147 Konwencji par.1 [w:*Komentarz I-IV Międzynarodowy Komitet Czerwonego Krzyża* par.1], tegoż *Respect of the Geneva Conventions-Measures taken to repress violations*, raporty na XX i XXI Międzynarodową Konferencję Czerownego Krzyża(par. 1965 i 69)

[863] zob. Rule 158 *Customary IHL*. Także Pasch J. *State Obligation to Punish Core International Crimes and the Proposed Crimes against Humanity Conventions* [w: zbiorowa, red. Bergsmo M., Tianying T. *On the proposed Crimes against Humanity Convention,* FICHL Publication Series 18 (2014) ss.202-7

[864] Prawo zwyczajowe traktatów, a także Konwencja Wiedeńska o Prawie Traktatów, uznaje przymus za przyczynę bezwzględnej nieważności wiązania się

międzynarodową. Państwa są więc niezdolne do jego spełnienia w cyberprzestrzeni w inny sposób niż poprzez stosowanie normowania faktycznego, które *de facto* w tym zakresie jest wykonywany w doktrynie *jurysdykcją sekretną.*[865] Termin ten określa sytuację, w którym cele przewidziane prawem są osiągane w drodze ustaw specjalnych, które wyłączają wiele z gwarancji przyznawanych jednostce przez dany system w celu zabezpieczenia bezpieczeństwa narodowego. Państwo wykonuje więc jurysdykcję, ale w sposób graniczący z łamaniem własnego prawa.[866] W cyberprzestrzeni, wydaje się to być jedyny sposób faktycznego, a co najistotniejsze legalnego wykonania tego obowiązku.

Wykonywanie jurysdykcji zwykłej możliwe jest wyłącznie w odniesieniu do części fizycznej cyberprzestrzeni. Tymczasem obowiązek ów wiąże, biorąc pod uwagę sieciowość i charakter *erga omnes* normy powstrzymywania, nie może być uznany za ograniczony do fizycznej części cyberprzestrzeni. Działające w cyberprzestrzeni służby danego państwa, mają obowiązek zwalczania łamania norm prawa konfliktu, nawet gdyby nie były tego konfliktu stroną. Jest to sytuacja podobna do obowiązku zwalczania piractwa na wodach międzynarodowych.[867] W cyberprzestrzeni nie ma jednak odpowiednika wód międzynarodowych, jakakolwiek reakcja musi się wiązać z naruszeniem jurysdykcji innych państw, choćby w zakresie dotyczącym fizycznej części cyberprzestrzeni. Wydaje się jednak, że te naruszenia, o ile państwo ich naruszające ograniczy się do celów przewidzianych prawem, należy uznać za legalne. Wskazują na to dwie przesłanki. Zgodnie z opisaną powyżej zasadą oparcia *lex informatica* opiera się o zasadę normowania *ex bono et aequo.* Skoro więc istnieje obowiązek ścigania, jego wykonywanie musi się w tym kryterium mieścić. Drugim istotnym argumentem, jest fakt zwyczajowego przyjmowania, że naruszenia

---

[865] Termin ten został wprowadzony do doktryny prawa międzynarodowego w odniesieniu do podobnego w sensie prawnym problemu list uniemożliwiających określonym osobom wchodzenie na pokłady samolotów pasażerskich ze względu na podejrzenia o powiązania z organizacjami terrorystycznymi. Listy takie były tworzone tajnie, bez wiedzy osób na nich umieszczonych a wpisanie na nią nie wiązało się dla osób w nich ujętych z żadnymi innymi konsekwencjami. zob. Manta I.D., Burke-Robertson C. *Secret Jurisdiction* Emory Law Journal t.65 (2016)s.1313

[866] Takie pojmowanie obowiązku ścigania naruszeń wynika z samego Protokołu Dodatkowego, który w art. 80 i 84 wskauzje, że powoływanie się na własne prawo wewnętrzne nie może być uznane za podstawę jakichkolwiek odstęp od tego obwiązku.

[867] zob. Art. 100-107 *Konwencji z Montego Bay*

suwerenności państwa dokonane dla wykonania norm *erga omnes*, są legalne.[868] Doktryna przyjmuje także, że państwo ścigające sprawców w jurysdykcji innego państwa nie może naruszać praw państw trzecich w tej jurysdykcji.[869] Rozpatrzmy przykładową sytuację, w której jedno państwo przygotowuje atak cybernetyczne na inne państwo. Zamierzony atak ma polegać na użyciu wykradzionego uprzednio numeru IP przypisanego Czerwonemu Krzyżowi, w celu nakłonienia przebywającego z misją humanitarną przedstawiciela państwa zaatakowanego do nawiązania łączności z rzeczywistą siedzibą Komitetu. Sygnał użyty w tej komunikacji ma następnie zostać namierzony i wykorzystany w naprowadzeniu dronów, które dokonają ataku kinetycznego. Tak zaplanowany atak niewątpliwie nosi znamiona wiarołomstwa w rozumieniu Protokołu. Zgodnie z opisywanym tu obowiązkiem - państwo, które powzięłoby o nim informację będzie zobowiązane do ścigania sprawców. W tym celu państwo to musi współdziałać z państwami trzecimi (jak choćby państwami, których infrastruktura została wykorzystana w celu wykonania operacji)[870] wykonać własną cyberoperację, która oznaczałaby zakazane naruszenie suwerenności państw trzecich. Tu jednak ujawnia się podstawowa słabość norm tworzonych dla świata fizycznego. Ewentualna pogoń za piratami, rozpoczyna się najczęściej na wodach międzynarodowych. Jeżeli w ogóle dochodzi do wejścia na wody terytorialne państwa trzeciego, okręt ścigający ma możliwość pełnego zidentyfikowania się i potwierdzenia własnej tożsamości, jak także przekazania państwu na wody którego wchodzi, wszelkich informacji o powodach tego naruszenia. Jego działania podlegają ciągłemu monitorowaniu. Mająca identyczny cel operacja cyberprzestrzenna, będzie miała jednak zupełnie inny przebieg. Dane, konieczne do uprawdopodobnienia istnienia planów wskazanego ataku, będą musiały zostać wyszukane na serwerach, na których prawdopodobnie będą znajdować się także inne dane, które będą musiały być sprawdzone w celu znalezienia tych, które są wymagane do przeciwdziałania wiarołomstwu. Nie istnieje żadna możliwość zagwarantowania, że dane w ten sposób

[868] Tak na przykład Rada Bezpieczeństwa ONZ w Rezolucji S/RES/1816 z dnia 2 czerwca 2008 roku,par.8(a)(b) dotyczącym piractwa w Somalii.

[869] por. Treves T. *Piracy,Law of the Sea, and Use of Force: Developments off the Coast of Somalia* European Jorunal of International Law 20:2(2009)s.403

[870] zob.Rule 18 *Tallinn Manual 2.0.*

zdobyte nie zostaną użyte w inny sposób. Oczywiście, norma *erga omnes* daje prawo wyłącznie do naruszenia suwerenności, wymaganego i ograniczonego do ścigania naruszeń prawa humanitarnego i jako takie musi być znoszone przez państwo. W sytuacji jednak, w której państwo poszukujące danych w celu powstrzymania ataku, jednocześnie wykorzysta legalne wejście do systemu w celu przeszukania innych plików na serwerach, do których dostęp uzyskało, dopuści się wyłącznie legalnego szpiegostwa. Co więcej, operacje, w sytuacji istnienia zamiaru przeprowadzenia działań szpiegowskich mogą i prawdopodobnie będą przeprowadzane bez informowania innych państw. Z tego z kolei wynika fakt, że państwo, które jest właścicielem serwerów będzie naruszeniu swojej suwerenności przeciwdziałać, pomimo jego pierwotnej legalności (na etapie wejścia do systemu, naruszenie suwerenności jest wtórnie legalizowane, traci tę legitymację w razie podjęcia działań wywiadowczych, a więc następczo. W cyberprzestrzeni nie ma możliwości oceny ani zamiarów, ani nawet sił użytych do operacji cyberprzestrzennej, bowiem na etapie dokonywania wejścia do serwerów czy sieci rozróżnienia te są niewykonalne. Należy pamiętać, że odpowiedzialność podmiotu prawa międzynarodowego za brak ścigania lub zapobiegania nadużyciu prawa humanitarnego idzie tak daleko, że obowiązuje w przypadku, gdy tylko podmiot ten mógł zapobiec lub ścigać te naruszenia.[871] Istnienie takiej normy jest wystarczającym powodem, z punktu widzenia państwa, którego suwerenność będzie naruszana, żeby przyjąć zasadność takiej operacji.

3. f. Odstraszanie

Tradycyjnie pierwszą linią obrony suwerenności jest uzyskanie przez państwo zdolności odstraszania ataku. Odstraszanie może przebiegać dwutorowo[872]. Pierwszym jest uzyskanie zdolności do wykonania kontrataku, nawet nielegalnego, atakże najczęściej publikacja zakładającej takie działanie doktryny. Drugim,

[871] zob. Art. 86 *Protokołu Dodatkowego* I *w* zw. z art. 1 *Convention on the Non-Applicability of Statutory Limitaions to War Crimes and Crimes against Humanity*. Otwarta do ratyfikacji rezolucją Zgromadzenia Ogólnego 2391 z 26 listopada 1968 roku.

[872] zob. Także Schelling Th. C. *Arms and Influence*, Praeger, (1977) par. 36-43

konstrukcja istotnych przeszkód w dokonaniu cyberoperacji w drodze *detterence - by - denial* Nietrudno zauważyć, że podstawowym elementem takiej konstrukcji odstraszania jest poinformowanie ewentualnego napastnika o podejmowanych działaniach. Szczególnie prawdopodobne jest to właśnie w cyberprzestrzeni[873], gdzie sam fakt przeprowadzenia operacji ułatwia kontratak[874] stronie przeciwnej. Należy zauważyć, że o ile odstraszanie w przypadku ataków dopuszcza użycie środków aktywnych, nie wyklucza to oczywiście stosowania opisanego powyżej odstraszania pasywnego, jako dodatkowego elementu obrony przed cyberatakami.

3. g. Prawo do uderzenie prewencyjnego

Uderzenie prewencyjne nie zostało nigdy precyzyjnie zdefiniowane. Samo określenie jego miejsca w systemie prawa międzynarodowego stanowi problem. Nie jest bowiem pewne, czy należy uznać je za element samoobrony. Normy regulujące tękwestię wydają się sprzeczne, nie sposób więc też oczekiwać jednolitej praktyki międzynarodowej. Doktryna wskazuje na trzy możliwości rozwiązania kwestii uderzeń prewencyjnych. Pierwsza z tych koncepcji zakłada absolutny zakaz wykonywania takich ataków. Druga, uznaje że co do zasady zakazane uderzenia prewencyjne mogą być wykonywane w bardzo nielicznych okolicznościach na zasadzie wtórnej legalizacji. Trzecia koncepcja, bez wątpienia mająca najmniejszą popularność, zakłada że uderzenie prewencyjne jest formą wykonywania prawa do samoobrony i może być wykonywane dowolnie, tak długo jak spełnione są przesłanki legalności defensywnego użycia siły przez określone państwo, i o ile uderzenie to wykonywane jest w istocie do zlikwidowania zagrożenia dla państwa je wykonującego. Wszystkie te trzy koncepcje zostaną omówione w dalszej części

---

[873] Należy zauważyć, że sam fakt cyberprzestrsennej odpowiedzi nie pozbawia państwa prawa do podjęcia działań w świecie fizycznym. zob. Także Derian J.D. *Cyber-Deterrence* Wired Magzine 9/94 (1994) s.1

[874] Część doktryny przyjmuje, że prawo do wykonywania odpowiedzi (w tym retorsji i represaliów) na operacje cyberprzestrzenne nie jest ograniczone w czasie, ze względu na ograniczoną (w stosunku do pełnoskalowego użycia broni kinetycznych lub broni ABC) możliwość dokonania zniszczeń w infrastrukturze obronnej. zob. Goodman W. *Cyber Deterrence: Tougher in Theory than in Practice?* Strategic Studies Quaterly 3/2010, (2010) s.108

wywodu. Podjęta zostanie też próba określenia, czy prawo do wykonania uderzenia prewencyjnego może zostać wykonane w cyberprzestrzeni i w jaki sposób może być przeprowadzone. Jest to kwestia tym bardziej istotna, że ze względu na naturę cyberprzestrzeni uderzenie prewencyjne w wielu wypadkach jest nie tyle najlepszym, co jedynym środkiem aktywnej obrony własnych systemów, bowiem skuteczne wykonanie ataku cybernetycznego może pozbawiać państwo zaatakowane realnej możliwości obrony własnej suwerenności.[875] Niezależnie od przyjętej teorii, niewątpliwie nielegalne jest wykonanie uderzenia prewencyjnego przeciwko atakowi, który nie spełnia kryteriów użycia siły. O ile siłę nadchodzącego uderzenia konwencjonalnego można ocenić przed podjęciem decyzji o przeprowadzeniu uderzenia prewencyjnego, sama próba nieautoryzowanego wejścia do systemów państwa będącego celem ataku, jest przeprowadzana w identyczny sposób, niezależnie od planowanego zakresu ataku. Historycznie, koncepcja prawa do wykonywania uderzenia prewencyjnego pochodzi od tzw. *Incydentu Caroline*. W roku 1837 roku, podczas kanadyjskiego powstania skierowanego przeciwko Brytyjczykom, grupa obywateli Stanów Zjednoczonych, państwa deklarującego neutralność w tym konflikcie, postanowiła wesprzeć Kanadyjczyków. Po zebraniu oddziału liczącego około 1000 osób i uzbrojeniu go, na pokładzie prywatnego parowca *Caroline*, zarejestrowanego w Stanach Zjednoczonych, postanowili oni zająć wyspę Navy. Statek został jednak zaatakowany przez oddział Royal Navy, zajęty po abordażu i spalony. Atak na *Caroline* został oprotestowany przez Stany Zjednoczone jako niesprowokowany.

Wskazywano, że żaden atak na wojska brytyjskie nie został przeprowadzony, zajęto wyłącznie nieistotne terytorium, które znajdowało się w międzyczasie pod kontrolą kanadyjską. Brytyjczycy zignorowali protesty, wskazując, że atak i zajęcie *Caroline* było konieczne, ponieważ służyła ona do przewozu wojsk i broni, które w oczywisty sposób miały zostać użyte przeciw nim. Atak doprowadził do kryzysu dyplomatycznego pomiędzy Stanami Zjednoczonymi i Zjednoczonym Królestwem,

[875] zob. Schneier B. *Data and Goliath: The Hidden Battles to Collect Your Data and control Your World.*W. W. Norton & Company (2018) ss.435-440

który został jednak rozwiązany na drodze dyplomatycznej korespondencji pomiędzy Danielem Websterem, Sekretarzem Stanu USA i Alexandrem Barringiem, baronem Ashburton, brytyjskim dyplomatą. Porozumienie, uznające incydent za zawiniony przez obie strony, stało się jednym z punktów traktatu pomiędzy obydwoma państwami podpisanego w roku 1842.[876] Doktryna prawa międzynarodowego, analizując wspomniane porozumienia, a także prowadzącą do porozumienia korespondencję, uznała całą sytuację za precedens określający praktykę międzynarodową w zakresie uderzeń prewencyjnych, wyprowadzając tzw. Test Caroline.[877] Test zakłada, że uderzenie prewencyjne musi być proporcjonalne i konieczne, uznawane jest bowiem za środek subsydiarny.[878] Założenie wynikające z testu było niekwestionowane; zarówno w kontekście praktyki międzynarodowej jak i *opinio iuris,* aż do wejścia w życie Karty Narodów Zjednoczonych. Ta bowiem uznaje jakiekolwiek prawo do obrony za dopuszczalne dopiero od momentu dokonania ataku.[879] Dla części doktryny, jest to dowód nielegalności jakiegokolwiek uderzenia prewencyjnego. Nie jest to jednak interpretacja jednoznaczna. W *Nicaragua* sędzia Schwebel wskazał, że redakcja art. 51 stosuje implikację nie równoważność. Wyprowadza on z tego wniosek, że prawo do samoobrony może więc być stosowane gdy dojdzie do ataku, natomiast nie jest ściśle do tego momentu ograniczone.[880] Należy także zauważyć, że sam Trybunał w orzeczeniu w tej samej sprawie odmówił zajęcia stanowiska co do kwestii legalności uderzeń prewencyjnych (sędzia Schwebel przywołaną argumentację zawarł w zdaniu odrębnym).[881]

---

[876] Chodzi o tzw. Traktat *Webster-Ashburton*, dotyczący statusu kolonii brytyjskich w Ameryce Północnej.

[877] Jego pierwotne brzmienie wynikało z wypracowanego przez obydwu dyplomatów wspólnego stanowiska. Strony przyjęły, że atak jest dopuszczalny w sytuacji, w której atak jest natychmiastowy i mający wystarczającą siłę, by przełamać obronę, celu ataku (*instant and overwhelming*), nie pozostawiający czasu do namysłu i zaistniały przy braku innych, możliwych do zastosowania środków. (*leaving no choice of means and no moment for deliberation*). por. List Sekretarza Stanu Daniela Webstera do lord Batinga, barona Ashburn z 6 września 1842. cyt. za archiwum *Avalon Project* prowadzonym przez Uniwersytet Yale (2019).

[878] por. Clark Arend A. *International Law and the Preemptive Use of Military Force* The Center for Strategic and International Studies and the Massachusetts Institute of Technology, The Washington Quaterly 26:2 (2003) ss.93-7

[879] zob. Art. 51 KNZ

[880] zob. *Nicaragua*, zdanie odrębne sędziego Stephena Schwebela (1986)

[881] *Nicaragua* Orzeczenie, par. 194

3. g. 1. Zastosowanie prawa do uderzenia prewencyjnego w cyberprzestrzeni.

Według powszechnej opinii ośrodków analizujących obronność, główną możliwością obrony przed atakiem w cyberprzestrzeni jest atak prewencyjny, zarówno militarny jak i cyberprzestrzenny. Zgodnie ze opisanymi powyżej normami, wymogiem do wykonania prawa do uderzenia prewencyjnego jest spełnienie określonych pozytywnych przesłanek; między innymi przesłanki proporcjonalności, konieczności i skierowany może być wyłącznie przeciwko atakowi, który jest nieunikniony i ma nastąpić natychmiast. Tymczasem w cyberprzestrzeni, ustalenie momentu, w którym atak staje się nieunikniony, jest z faktycznego punktu widzenia niewykonalne. Zupełnie inaczej jest w przypadku ataku konwencjonalnego, gdzie istnieje możliwość stwierdzenia kiedy ten wchodzi w fazę uderzenia. Część doktryny prawa międzynarodowego, uznająca generalny zakaz stosowania uderzeń prewencyjnych, stoi na stanowisku, że to właśnie moment, w którym atak staje się nieunikniony, określa moment, w którym państwo będące celem ataku, ma możliwość wykonania prawa do samoobrony, pomimo faktu że samo uderzenie nie zostało jeszcze wykonane. Jednocześnie ze skali ataku, możliwe jest określenie proporcjonalności.[882] W cyberprzestrzeni nie da się wskazać momentu, w którym atak wchodzi w ową fazę, systemy obrony zaczynają bowiem wykrywać atak dopiero w momencie, w którym integralność tych systemów została naruszona, a więc atak został już wykonany. Z opisanych powyżej powodów, nie da się określić proporcjonalności odpowiedzi. W momencie naruszenia systemów bezpieczeństwa informatycznego danego państwa, nie sposób stwierdzić, jaka jest planowana siła ataku, w szczególności czy przekracza on próg użycia siły, jak i tego czy ewentualny

[882] zob. Maggs G.E. *How United States Might Justify a Preemptive Strike on a Rouge Nationas Nuclear Weapon Development Facilities Under the U.N. Charter.* 57 Syracuse Law Review 465 (2007)

skutek będzie miał efekt kinetyczny czy nie. Podobnie, na poziomie początkowym, nie ma możliwości stwierdzenia, jaka będzie lub jest zamierzona jego siła, co wyłącza możliwość określenia odpowiedzi proporcjonalnej. Nie ma więc możliwości bezpośredniego zastosowania testu *Caroline* do cyberprzestrzeni. Może on jednak być do niej stosowany odpowiednio. Przede wszystkim należy przyjąć, że prawo cyberprzestrzeni przyjmuje wynikły zeń nakaz zachowania subsydiarności i proporcjonalności ataku prewencyjnego.[883] Proporcjonalności jednak w przypadku ataku kinetycznego nie sposób określić. Samo bowiem prawo do ataku i obrony nie jest bowiem różnicowane pomiędzy cyberprzestrzenią a konfliktem konwencjonalnym.[884] Niemniej na legalność uderzenia prewencyjnego w cyberprzestrzeni może wpływać istniejące w sprawie *case-law*. Zgodnie z przełomowym orzeczeniem MTS w sprawie *Nicaragua*, w wypadku ataku o niewielkiej skali, dozwolona jest wyłącznie odpowiedź poniżej poziomu użycia siły.[885] Należy jednak wskazać, że sam Trybunał nie orzekał w tej w kwestii jednoznacznie. Sędzia Bruno Simma przedstawił przekonującą interpretację zasady wyrażonej przez Trybunał w sprawie *Nicaragua.* Wskazywał on, że ponieważ zasadą ogólną samoobrony w rozumieniu art. 51 KNZ jest proporcjonalność, nie ma możliwości ograniczenia tego prawa w taki sposób, żeby strona zaatakowana miała mniejsze prawa niż strona atakująca. Twierdzi on, że orzeczenie MTS należy zinterpretować w ten sposób, że o ile brak pełnoskalowej agresji istotnie wyłącza prawo do prowadzenia pełnoskalowej obrony ze względu na zasadę proporcjonalności, ta sama zasada oznacza, że strona zaatakowana nie może zostać pozbawiona prawa do obrony, o sile odpowiadającej sile ataku (z zachowaniem wspomnianego powyżej wyjątku).[886]

Należy także zauważyć, że prawo dopuszcza ewentualne straty (w tym mające

---

[883] zob. Rule 72 *Tallinn Manual 2.0*

[884] Tak na przykład pr.30 *Tallinn Manual 'Definition of cyber attack'*, także par. 4 komentarza do tetego artykułu sporządzonego przez International Group of Experts

[885] zob. Orzeczenie *Nicaragua* par. 249. Także Orzeczenie dotyczące *Jus ad Bellum* wydane przez Ethiopia-Eritreia Claims Commission par. 12, który powołuje i podtrzymuje wskazane orzeczenie MTS.

[886] zob. Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America) International Court of Justice, Jugdement, ICJ Reports 1986, zdanie odrębne sędziego Bruno Simmy.

nawet ekwiwalencję kinetyczną), spowodowane uszkodzeniem lub czasowym wyłączeniem systemów informatycznych strony będącej celem operacji, w tym wśród infrastruktury cywilnej, o ile ich osiągnięcie nie było celem ataku *per se*.[887] Podobnie, odpowiedź cyberprzestrzenna dokonywana w jej informatycznej części musi być odpowiedzią na atak, który ma cechy natychmiastowości i być nie do uniknięcia, bowiem jak wskazano - jego wykrycie możliwe jest dopiero w momencie jego rozpoczęcia. Z powyższych przesłanek wynika fakt, że operacja cybernetyczna, wykonana jako atak prewencyjny, bez zaplanowanych efektów kinetycznych skierowanych przeciwko cywilnej infrastrukturze państwa atakującego, będzie zawsze legalnym środkiem (zarówno według prawa dotyczącego cyberprzestrzeni jak i norm ógólnych prawa konfliktów zbrojnych dotyczących ataku prewencyjnego), ponieważ z samej swej natury nie może nie spełniać przesłanek tejże legalności.

Z powyższego wynika, że państwa mają prawo do zastosowania niekinetycznego ataku cyberprzestrzennego w wykonaniu swojego prawa do uderzenia prewencyjnego. Przyjmując argumentację sędziego Simmy wskazującą, że strona broniąca się nie może mieć mniejszych praw niż napastnik i biorąc pod uwagę, że naruszenie suwerenności jest co do zasady działaniem nielegalnym - taką odpowiedź należy uznać za proporcjonalną w rozumieniu prawa międzynarodowego. Należy także zauważyć, że brak kinetycznej ekwiwalencji, pozwala spełnić przywołany powyżej wyjątek - braku pełnoskalowej odpowiedzi - w każdym przypadku, ponieważ atak niekinetyczny nigdy nie jest atakiem pełnoskalowym. *De lege ferenda* należy także postulować odpowiednie stosowanie koncepcji domniemania, stosowanej do oceny stopnia naruszeń przez *CNE,* do określenia momentu,w którym cyberatak staje się nieunikniony, co pozwoliłoby na skuteczne wykonywanie obrony własnej suwerenności w cyberprzestrzeni, przy jednoczesnym stworzeniu normy gwarantującej uniknięcie przekroczeń tejże.

---

[887] zob. Rule 51 *Tallin Manual i Rule 113 Tallinn Manual 2.0,* wraz z komentarzem IGoE Należy jednak zauważyć, że IGoE nie wyróżnia odrębnego prawa do ataku prewencyjnego - stosując wspomniane zasady do ogólnie do samoobrony wykonywanej w cyberprzestrzeni.

V. Cyberlawfare

1. Geneza i pojęcia 'lawfare'

Pojęcie *lawfare* pochodzi z połączenie angielskich słów *law* i *warfare*. Pierwszy raz został on zastosowany przez australijskich teoretyków prawa Carlsona i Yeomansa.[888] W powołanej wyżej pracy autorzy wskazują, że prawo (zwłaszcza międzynarodowe), przestaje być narzędziem rozwiązywania konfliktów a staje się narzędziem ich prowadzenia.[889] Pojęcie *lawfare* przyjęte zostało do doktryny prawa międzynarodowego i rozwinięte, zyskując drugie znaczenie. Drugim aspektem *lawfare* stało się ocenianie sytuacji militarnej konfliktu przez pryzmat prawa międzynarodowego.[890] Amerykańska doktryna wskazuje, że stosowanie prawa międzynarodowego staje się czynnikiem, który może znacząco wpływać na możliwość projekcji siły. Najdalej idący pogląd, wskazuje że prawo staje się *de facto* bronią konfliktu asymetrycznego.[891] Doktryna prawa międzynarodowego wskazuje, że dowodzenie w konfliktach zbrojnych staje się poddane w coraz większym stopniu, coraz szerzej zakreślanym kryteriom prawa międzynarodowego, natomiast coraz mniej jest poddane realizacji celów militarnych.[892]

Część doktryny wyraża wprost opinię, że rozwój prawa międzynarodowego konfliktów zbrojnych może prowadzić bezpośrednio do przedefiniowana balansu siły militarnej na świecie.[893] Obydwa wskazane aspekty *lawfare* w zasadzie dotyczą jednego problemu. Prawo i jego stanowienie staje się narzędziem budowania własnej

---

[888] zob. Carlson J., Yeomans N.-*Whither Goeth the Law- Humanity or Barbarity,* The Way Out- Radical alternatives in Australia, Smith and Crossley ed. Melbourne Lansdowne Press (1975) ss.2-5

[889] Dosłowanie autorzy piszą *Lawfare replaces warfare and the duel is with words rather than swords...*- ibid. s.2

[890] por. Dunlap Ch. J.- *Law and Military Interventions: Preserving Humanitarian Values in 21st Conlifcts*- Humanitarian Challenges in Military Intervention Conference Carr Center for Human Rights Policy, Kennedy School of Government Harvard University, Washington D.C. (2001) ss.2-7

[891] zob. Dunlap *Law and Military... ss.4-5*

[892] *NATO lawyers... became in effect... its tactical commanders* [w: Betts R.K. *Compromised Command*- opublikowane w Foreign Affairs nr 126 Lipiec/Sierpień 2001

[893] *International Law may become one of the most potent weapons ever deployed against United States* [w: Rivkin Jr. D.B. i Casey L.A.-*The rocky shoals of international law*- The National Interest 35 (2000/01) s.1

(a tym samym ograniczania po stronie innych podmiotów) możliwości projekcji siły. Wpływ danego państwa na proces stanowienia prawa międzynarodowego publicznego jest wprost proporcjonalny do możliwości tej projekcji. Sama konstrukcja współczesnego *ius gentium* pozwala stosowanie podobnego mechanizmu nawet poza domeną konfliktów zbrojnych. Przykładowo zasada równości podmiotów prawa międzynarodowego pozwala na osiąganie przez państwa niemające realnej siły militarnej celów tradycyjnie osiąganych przez państwa poprzez projekcję siły, poprzez działania prawne na forach takich jak Organizacja Narodów Zjednoczonych.

Należy rozważyć w jaki sposób koncept *lawfare* może być i jest realizowany w cyberprzestrzeni. Podstawową różnicą pomiędzy prawem konfliktu zbrojnego a prawem konfliktu cyberprzestrzennego jest to, że normy prawa wojny obowiązują nieomal każde państwo w tym samym zakresie. Normy te najczęściej obowiązują *erga omnes*, ewentualne traktaty w tym zakresie dla swojej skuteczności wymagają związania się nimi przez większość państw (przykładowo - traktaty rozbrojeniowe). Tymczasem *lex informatica* jest bardzo wrażliwa na działania wynikłe z *cyberlawfare*. Co najbardziej istotne, w systemie prawnym opartym na afordancjach i normowaniu faktycznym, możliwe jest konstruowanie kodu, w sposób umożliwiający określone naruszenia suwerenności państw trzecich przy pomocy działań legalnych z punktu widzenia prawa międzynarodowego. Przykładowo, państwo może w ramach własnej jurysdykcji preskryptywnej tworzyć narzędzia, które poprzez pośredni wpływ na kod i architekturę cyberprzestrzeni, ułatwi mu operacje cybernetyczne naruszające suwerenność państw trzecich poprzez normowanie sposobu transferów opartych o własną infrastrukturę cyberprzestrzenną. Podobnie działania mogą też podjąć państwa, na terytorium których zlokalizowane są elementy infrastruktury należące do organizacji ponadnarodowych pełniących istotną rolę w cyberprzestrzeni jak *ICANN*. Skuteczne normowanie takich podmiotów pozwala w oczywisty sposób na realizację własnych polityk w całej informatycznej części cyberprzestrzeni. Przykładowo w razie korzystnego rozstrzygnięcia dla siebie sporu z *ICANN*, Unia uzyskała by *de facto* możliwość narzucenia norm *GDPR* wobec wszystkich podmiotów funkcjonujących w cyberprzestrzeni. Oczywiście nie wynikałoby to z rozszerzenia

zakresu jej jurysdykcji preskryptywnej. Byłoby skutkiem wyłącznie łańcucha faktycznych zależności i ich wpływu na cyberprzestrzeń. *ICANN* musi przyjąć, że będzie musiał dostosować się do wymogów jurysdykcji tak istotnej z punktu widzenia cyberprzestrzeni jak unijna - natomiast pozostałe podmioty w cyberprzestrzeni obecne (w tym także sama UE) są faktycznie zobowiązane do stosowania się do *bylaws ICANN*, ponieważ inaczej nie mogłyby partycypować w systemie *IP*.

Drugą możliwością wykorzystania *lawfare* w cyberprzestrzeni jest realizacja wpływania na normy pośrednio tworzące *lex informatica* - tworząc jego warstwę prawna. Przykładem takiego działania mogą być dążenia Chin do usunięcia konfliktów cyberprzestrzennych z zakresu przedmiotowego tradycyjnego prawa konfliktów zbrojnych.[894] Zmiana taka (chociaż wykonana wyłącznie w zakresie prawa międzynarodowego publicznego) miałaby skutki nie tylko w nim i w konsekwencji w *lex informatica,* ale także oznaczała znaczące przesunięcie faktycznej i politycznej możliwości projekcji siły. Zniesienie zasady inkorporującej normy prawa konfliktów zbrojnych do konfliktu cyberprzestrzennego - oznaczałyby znaczące zwiększenie zakresu możliwych do skonstruowania afordancji służących do przeprowadzania cyberataków. Były one bowiem ograniczone wyłącznie przez normowania faktyczne - bez ram prawnych wyznaczanych przez prawo międzynarodowe publiczne. Podobny skutek miałyby też zmiany w regulacjach (szczególnie ponadnarodowych) dotyczących sposobu samego transferu danych - mające istotny wpływ na samo konstruowanie obrony pasywnej. Ponieważ ta ostatnia stanowi podstawowy środek ochrony suwerenności w cyberprzestrzeni, wszelkie zmiany w tym zakresie *de facto* pozwalają państwom mającym największy wpływ na konstrukcję prawa międzynarodowego uzyskać zdecydowaną przewagę w ewentualnych operacjach cyberprzestrzennych. Należy tu zauważyć, że kluczowe w tym zakresie elementy normowania faktycznego zostały przekazano organom niepaństwowym, mającym faktyczny status podobny do eksterytorialności. Częściowy wpływ na te organizacje, który mogą wywrzeć wyłącznie niektóre

[894] zob. Kittrie O.F. *Lawfare: Law as a Weapon of War,* Oxford University Press (2016) s.170

państwa - daje im istotną przewagę w ewentualnym stosowaniu *cyberlawfare*. Wpływ na normy *lex informatica* nie jest więc równy. Obserwacja ta stanowi jednoznaczny argument przeciwko wskazanej we wcześniejszej części wywodu koncepcji demokratyzacji tworzenia kodu proponowanej przez Asschera. Istotą bowiem *cyberlawfare* jest właśnie mechanizm odwrotny - a praktyka międzynarodowa niewątpliwie wskazuje na ten kierunek rozwoju cyberprzestrzeni.. Ze względu więc na samo istnienie *cyberlawfare* państwa o większych możliwościach faktycznych, zyskują silniejszą pozycję w ramach *lex informatica*.[895] W cyberprzestrzeni zostaje więc zakwestionowana sama zasada równości państw. O ile bowiem w świecie fizycznym nierówności siły poszczególnych państw są wyrównywane przez normy prawa ponadnarodowego – w *lex informatica* mechanizm ten jest obecny wyłącznie w tak ograniczonym zakresie w jakim wpływa na jego normy prawo międzynarodowe publiczne. Natomiast wpływ, który na to ostatnie mogą zyskać państwa w ramach prawa narodów jest na tyle niewielki, że nie równoważy możliwości wpływu na *lex informatica* wykonywanego faktycznie przez *non-state actors* - poza kontrolą któregokolwiek z systemów prawnych i przez żaden z nich nie normowane.[896] Zastosowanie norm jednego z tych systemów prawnych do jak najdalej idącego wykorzystania luki lub słabości drugiego z nich w cyberprzestrzeni, daje skutek w postaci normy lub bezpośrednio afordancji w najdalszym możliwym stopniu, umożliwiającym danej stronie wykonanie swoich zamiarów. Przykładowo, zasada wszechobecności (i wynikające z niej afordancje *lex informatica*), mogą być zastosowane do faktycznego zniweczenia norm prawa danego państwa dotyczącego kontroli publikacji danych (jak miało to miejsce w *Baer v. Wikileaks*). Jeżeli dodatkowo strona, która dąży do publikacji, wzmocni efekt *cyberlawfare*, przy pomocy włączenia norm tradycyjnego prawa międzynarodowego (na przykład, poprzez umieszczenie serwerów publikujących kopie danych w jurysdykcjach sztucznych lub na terytoriach spornych) - uzyska faktyczną niemożliwość ochrony

[895] zob. Kittrie *Lawfare...* ss.45-8

[896] Decentralizacja cyberprzestrzeni jako jedna z przyczyn skuteczności *cyberlawfare*, jest zauważana przez coraz więcej państw i jednoznaczenie postrzegana jako zagrożenie dla suwerenności. zob. Ferguson A.T. *Closing the Gaps: Cybersecurity for U.S. Forces and Commands,* Joint Forces Staff College (2016) s.6

suwerenności państwa, które w drodze własnego prawodawstwa chciało zapobiec publikacji.[897]

Należy pamiętać także, że *cyberlawfare* (w przeciwieństwie do *lawfare)* dotyczy nie tylko środków możliwych naruszeń suwerenności, ale także pola na jakim jest ono dokonywane. Przykładem takiego działania może być (wykonane w drodze ustawodawstwa krajowego) promulgowanie przez USA prawa nakazującego każdemu producentowi systemów operacyjnych dostępnych w tym państwie umieszczanie w nich tzw. *backdoor*, pozwalających obejść zabezpieczenia danego systemu i bez wiedzy administratora czy użytkownika urządzenia pobierać z niego dane.[898] W ten sposób, w drodze jurysdykcji zwyczajnej Stany Zjednoczone tworzą pośrednio afordancję stanowiącą niejako odpowiednik przeprowadzanie operacji *CNE* wobec każdego (faktycznie) systemu operacyjnego na świecie. Oczywiście, zarówno sama możliwość jak i skuteczność takiej normy zależy wyłącznie od faktycznej i politycznej zdolności danego państwa do projekcji siły.[899] Działanie takie stanowi jednak przykład uczynienia z prawa *de facto* broni pozwalającej na osiągnięcie określonych celów politycznych. Nie sposób pozostając na gruncie rozważań wyłącznie prawnych wskazać *ratio legis* takiego normowania. Służby pewnego państwa uzyskują swobodny dostęp do systemów operacyjnych, *de facto* także dostęp do danych osób, w żaden sposób nie poddanych ich jurysdykcji. W oparciu o wszechobecność cyberprzestrzeni, zakres przedmiotowy afordancji stworzonych w drodze podobnego przepisu jest potencjalnie nieograniczony. Ustanowienie takiej normy, o ile niewątpliwie legalne z punktu widzenia formalnoprawnego punktu widzenia, materialnie (i faktycznie) oznacza rozszerzenie normowania bez żadnej podstawy prawnej. Należy także zauważyć, że państwa, których jurysdykcjom poddane są osoby i systemy, z których dane będą analizowane - nie mogą powołać się na naruszenie własnej suwerenności. Z prawnego punktu widzenia, dostęp do systemów będzie wynikał ze stanu faktycznego i prawa, którego literalnie pojmowany

[897] zob. Fergusson *Closing the Gaps...* s.11

[898] zob. Toomey P. *The NSA continues to violate Americans' Internet Privacy Rights,* ACLU National Security Project (2018) par.1

[899] zob. także Mačak K.*From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers* Leiden Journal of International Law 30 (2017) ss.882-4

zakres nie wykracza poza terytorium państwa, które je promulgowało.[900]

Odrębną kwestią staje się pytanie, czy tak pojmowane prawo w ogóle jeszcze może być uważane za prawo. Na problem ten wskazywał już w 1978 roku dziekan *Cornell Law School*, Roger Cramton, który twierdził, że *legalistyczny instrumentalizm staje się religią sal wykładowych szkół prawniczych* a zadaniem współczesnego prawnika staje się *takie manipulowanie wykładnią i procesem by w najszerszym zakresie bronić interesu klienta.*[901] Jeszcze dalej poszedł profesor Tamanaha, który wskazywał, że skutkiem legalistycznego instrumentalizmu jest *upadek prawa wyższego rzędu, rozkład idei dobra wspólnego*[902]. W przypadku *lawfare* (choć przywołane uwagi mają niewątpliwie znaczenie) z formalnoprawnego mamy ciągle niewątpliwie do czynienia z prawem, które ewentualnie może być nadużywane. *Cyberlawfare* natomiast - ze względu na anonimowość, wszechobecność cyberprzestrzeni i samą konstrukcję *lex informatica* - oznacza tworzenie stanów faktycznych przy pomocy norm prawnych często wyłącznie formalnie będących prawem.

Istotnym zagrożeniem dla suwerenności stwarzanym przez *cyberlawfare* jest także redefinicja tego, co doktryna prawa konfliktów zbrojnych zwykła określać konfliktem asymetrycznym. W tradycyjnym rozumieniu oznaczało to konflikt zbrojny lub z użyciem innych środków odpowiadających poziomowi użycia siły, w którym jedna ze strony jest wyraźnie słabsza, a co za tym idzie podlega prawnie i faktycznie dalej idącej ochronie społeczności międzynarodowej.[903] Ze względu na brak ustalonej praktyki w zakresie cyberprzestrzeni, asymetria konfliktu *cyberlawfare* sprowadza się do tego, że strony nie mają możliwości legalnej odpowiedzi na naruszenia własnej suwerenności, ponieważ dysponują albo zbyt silnymi środkami odpowiedzi albo zbyt słabymi. Jak napisał o programie cyberprzestrzennym Korei Północnej, były zastępca dyrektora NSA, Chris Inglis *Cyber is a tailor-made instrument of power for [North Korea].There's a low cost of entry, it's largely asymmetrical, there's some degree*

[900] cf. Kittrie *Lawfare...* ss.333-5

[901] Cramton R. C. *The Ordinary Religion of the Law School Classroom*, 29 Journal od Legal Education 247 (1978) s.247

[902] Tamanaha B. Z. *How an Instrumental View of Law Corrodes the Rule of Law*, 56 DePaul University Law Review (2007) s.469

[903] zob. Geiss R. *Asymmetric conflict structures*, International Review of the Red Cross 88:864(2006) ss.757-9

of anonymity and stealth in its use. It can hold large swaths of nation state infrastructure and private-sector infrastructure at risk. It's a source of income. You could argue that they have one of the most successful cyberprograms on the planet, not because it's technically sophisticated, but because it has achieved all of their aims at very low cost.[Narzędzia cyberprzestrzenne są idealnym środkiem projekcji siły dla Korei Północnej. Niski koszt wejścia, wysoka asymetryczność, spora anonimowość i możliwość niewykrywalnego działania. Możliwość zaatakowania bardzo dużych partii infrastruktury sektorów publicznego i prywatnego. Źródło zysku. Prawdopodobnie Koreańczycy rozwinęli najbardziej udany program cybernetyczny na świecie. Nie dlatego, że jest on tak zaawansowany technicznie, ale dlatego że osiągają wszystkie swoje cele przy bardzo niskich kosztach własnych.[904]

Asymetria konfliktu *cyberlawfare* opiera się więc nie tyle na nierówności siły stron (ponieważ skutki różnicy potencjałów zostają znacząco spłaszczone w porównaniu do skutków tych w świecie rzeczywistym), co na użyciu do naruszenia suwerenności państwa trzeciego środków, co do których brak (zarówno w prawie międzynarodowym jak i w *lex informatica*) określonych norm. Brak tych norm implikuje utrudnia lub wręcz często uniemożliwia odpowiedź lub obronę suwerenności przez państwo będące celem operacji, przy jednoczesnym osiągnięciu własnych celów przez państwo naruszające.

Doktryna prawa cyberprzestrzeni wskazuje, że przykładem takiej sytuacji jest brak natychmiastowej odpowiedzi prawnomiędzynarodowej na ataki na infrastrukturę państwową (jak przywołany powyżej casus wirusa *Stuxnet*). Może on nawet wskazywać na tworzenie się prawa zwyczajowego znacząco ograniczające możliwość odpowiedzi prawnej państwa na cyberataki niekinetyczne i operacje poniżej poziomu użycia siły (w tym także z potencjałem do przekształcenia się w atak o ekwiwalencji kinetycznej).[905] Sami prawnicy rządu USA, w tym pułkownik Gary Brown, doradca prawny Dowództwa Operacji Cybernetycznych USA wskazywał, że do ataku na Iran niewątpliwie doszło i że milczenie Iranu jest groźne z punktu widzenia zwyczajowego

[904] Cyt. za Sanger E., Kickpatrick D., Perlroth N. *The World Once Laughed at North Korean Cyberpower. No More.* New York Times z 15 października 2017
[905] ibid.

prawa cyberprzestrzeni.[906] Dochodzi więc do sytuacji, w której na gruncie prawnym, państwa tracą możliwość skutecznej ochrony własnej cyberprzestrzennej suwerenności, nie tylko ze względu na możliwości faktyczne, które umożliwiłyby im tej suwerenności ochronę, ale przede wszystkim ze względu na brak odpowiednich norm prawa, które tę odpowiedź by regulowały lub uzasadniały. Nawet *Tallin Manual 2.0* - uznawany za najdokładniejsze i najszersze w aktualnym stanie prawnym opracowanie dotyczące prawa konfliktu cyberprzestrzennego - nie wskazuje środków, za pomocą których podmioty prawa międzynarodowego mogą bronić swojej suwerenności przed naruszeniami, które nie są wystarczające do uruchomienia art. 51 KNZ. Zwracał na to uwagę sam Michael Schmitt, który stwierdził *The advent of cyber operations threw the instrument-based approach into disarray by creating the possibility of dramatically destabilizing effects caused by other than kinetic actions- Wynalezienie cyberoperacji rozbiło analizy oparte na tradydcyjnych instrumentach prawnych, ponieważ możliwe stało się wywoływanie efektów kolosalnej destabilizacji, nieopartej o działania kinetyczne.*[907] W praktyce, w połączeniu z problemami atrybucyjnymi, doprowadziło to do sytuacji, w której asymetria konfliktu jest nie tyle wynikiem dysproporcji w układzie sił, co świadomym wyborem sposobu prowadzenia działań przez stronę słabszą, które (przynajmniej w samej cyberprzestrzeni) mogłaby działać wykorzystując dużo większą siłę, a nie czyni tego właśnie po to, by wyłączyć ewentualną odpowiedź kinetyczną, której z kolei nie mogłaby powstrzymać.[908] To czyni cyberprzestrzeń idealnym polem dla działań mających na celu naruszenia suwerenności państw trzecich. dla działań opartych o *lawfare.* Strona planująca dane działanie faktycznie zyskuje możliwość ‘wyboru’ skali i miejsca konfliktu. Dodać do tego należy wzrost znaczenia *non-state actors*[909], którzy w cyberprzestrzeni faktycznie zostają zrównane z tradycyjnymi. Należy także wskazać, że w cyberprzestrzeni działania państw i *non-state actors* są częstokroć powiązane. Wobec

---

[906] Brown G.*Why Iran Didn't Admit Stuxnet Was an Attack* Joint Forces Quaterly nr 63 4/2011

[907] Schmitt M.N. *Computer Network Attack and the Use of Force...* s.917

[908] zob. także Nguyen R. *Navigating "Jus ad Bellum" in the Age of Cyber Warfare*, California Law Review 101:4 (2013) ss.1080-5

[909] zob. Kittrie *Lawfare...* s.338

wskazanej powyżej znikomej skuteczności testów przypisania (zarówno *Tadić* jak i *Nicaragua*), podmioty te częstokroć są wykorzystywane do wykonywania operacji przeciwko sieciom państw trzecich wyłączających możliwość odpowiedzi przeciwko państwu, które łatwo może uniknąć spełnienia przesłanek któregokolwiek z testów przypisania odpowiedzialności, jednocześnie korzystając z własnych środków by anonimizować grupę, która faktycznie naruszeń dokonała.[910] W praktyce, *cyberlawfare* stanowi dalsze ograniczenie tradycyjnej jurysdykcji i suwerenności państw w cyberprzestrzeni i przeniesienie ich ciężaru na normowanie faktyczne.[911] Podobnie podstawowe narzędzie państw, które mogłoby pozwolić na wyłączenie a przynajmniej ograniczenie roli *cyberlawfare*, a więc zawieranie traktatów i wprowadzanie w życie ich postanowień, okazuje się niewykonalne.[912] *Cyberlawfare* oznacza więc, że faktyczny wybór poziomu, na którym odbywa się starcie, leży po stronie tego, kto ów konflikt inicjuje, a wyboru owego dokonuje poprzez faktyczne dorozumiane "oświadczenie woli".

Z czysto prawnego punktu widzenia , wydaje się, że ciężko o dokładne określenia granic zjawiska *lawfare* i w konsekwencji *cyberlawfare*. Jedyną definicją tego zjawiska jest ta zaproponowana przez Ch. Dunlapa "*lawfare* to wykorzystanie prawa jako broni".[913] Przeważająca część doktryny wskazuje także, że głównym (albo wręcz jedynym) środkiem prowadzenia *lawfare* jest prawo międzynarodowe, ze szczególnym uwzględnieniem jurysdykcji uniwersalnej i norm *ius cogens*.[914] Jeżeli

---

[910] zob. Tez Sander B.*The Sound of Silence: International Law and the Governance of Peacetime Cyber Operations*, 11th International Conference on Cyber Conflict, [w: zbiorowa, red. Minarik T., Alatalu S., Biondi S., Signoretti M., Tolga I., Visky G. *Silent Battle* NATO CCD COE Publications (2019)ss.5-8

[911] Kang C., Nakashima E. *Tech Executives to Obama: NSA Spying Revelations Are Threatening Business* Washington Post 17 grudzień 2013 s.1.

[912] [...]*Internet treaties in particular has proven elusive...-[...]traktaty internetowe, szczególnie okazały się wymykać praktycznym możliwościom konstrukcji...*[w:Goldsmith J.L., Wu T.*Who controls the Internet?...* s.165]

[913] Dunlap *Preserving Humanitarian Values...*s.3

[914]por. Goldsmith J. *The Terror Presidency: Law and Jugdement inside the Bush administration* NYC W.W. Norton (2007) r.1; teoretycznie można sobie wyobrazić *lawfare* prowadzony na mocy prawa wewnętrznegopaństwa z którym prowadzi się wojnę, najczęściej jednak te normy podlegają łatwej zmianie w ramach legislatur tych państw, z prawnego punktu widzenia nie mogą więc być wykorzystywane do prowadzenia konfliktu zbrojnego. Należy także zwrócić uwagę na fakt, że ewentualne argumenty z prawa krajowego w tym ujęciu, w istocie byłyby i tak rozstrzygane w oparciu o prawo międzynarodowe i to jego stan prawny byłby ostatecznie decydujący.

zestawimy obydwa te opisy, to musimy dostrzec, że niosą one w istocie treści o znaczeniu z punktu widzenia prawa międzynarodowego materialnoprawne. Po pierwsze więc *lawfare* należy uznać za metodę prowadzenia konfliktu zbrojnego. Po drugie, zakresem przedmiotowym normowania jest określony sposób wykorzystania prawa międzynarodowego. Po trzecie, sposób ów oparty jest o aktualny stan prawny norm wiążących *erga omnes*.

Pierwszą poważnym problemem interpretacyjnym, który wynika z takiego definiowania *lawfare* jest fakt, że przy próbie dokonania subsumpcji wspomnianego zakresu normowania, musimy dostrzec, iż w istocie oznacza on że mamy do czynienia z pojęciem należącym do metazakresu języka prawnego. Normuje ono bowiem samo siebie. Jeżeli *lawfare* polega na wykorzystaniu prawa konfliktu jako broni, opierając się na normach *erga omnes*, należy najpierw odpowiedzieć na pytanie, czy takie wykorzystanie tego prawa można uznać w ogóle za legalne. Niewątpliwie, zgodnie z zasadą *male nostro iure uti non debemus*, *lawfare* należałoby uznać za nielegalne, właśnie na mocy wiążących *erga omnes* norm prawa konfliktu. Prawa konfliktów istnieją bowiem właśnie w celu ochrony najbardziej zagrożonych dóbr prawnych, a wykorzystywanie tej ochrony do prowadzenia tego konfliktu, musi w praktyce prowadzić do jej osłabienia. Ponadto, to właśnie prawo konfliktów określa, które dobra, i w jaki sposób, są chronione.[915]

Nadto *lawfare* może być prowadzony nawet po przeprowadzeniu ataku, na przykład poprzez próbę wtórną delegalizacji ataku, przeprowadzanego zgodnego z prawem międzynarodowym. Często przywoływanym w doktrynie przykładem takiej sytuacji, był nalot NATO na siedzibę serbskiego radia państwowego w Belgradzie podczas interwencji w 1999 roku. Pomimo oczywistego faktu, że radio to mieściło ośrodki propagandy rządowej dodatkowo wykorzystywane przez własny rząd do podżegania do zbrodni wojennych.[916] Dodatkowo, należy wskazać, że prawo międzynarodowe

[915] zob. Dunlap *Preserving...* s. 7 i n.

[916] Finninn S. *Elements of accessorial modes of liability:Article25(3)(b) and (c) of the Rome Statue of the International Criminal Court* Martnus Nijhoff Publishers,Boston, International Humanitarian Law Series 38 (2012) ss.220-8 ;podstawowym predcedensem określającym taką możliwość kwalifikacji jest wyrok Międzynarodowego Trybunału Wojskowego w Norymberdze w sprawie przeciwko Juliusowi Streicherowi.

każdej radiostacji przyznaje status legalnego celu militarnego.[917] W przywołanej sytuacji nie doszło też do udzielenia rozgłośni wtórnej ochrony, mogącej (choć niekoniecznie) wynikać z prawa konfliktów zbrojnych.[918] Pomimo to, międzynarodowe organizacje humanitarne wskazywały na bezprawność ataku.[919] W pewnym zakresie, przychyliły się do tej opinii także trybunały międzynarodowe, ostatecznie przyznając przymiot legalności atakowi na siedzibę radia, jednakże uzasadniając ją włączeniem jej mocy nadawczej do systemu wojskowych radiostacji serbskich.[920] W tym przypadku, *lawfare* zostało wykorzystane właśnie jako środek wtórnej delegalizacji ataku, wystarczająco skutecznie (na co wskazuje wskazane powyżej uzasadnienie Trybunału) by umożliwić stronie militarnie słabszej - asymetryczną obronę przy pomocy prawa stosowanego jako broni, zgodnie z wskazaną wyżej definicją. Co istotne, wszystkie wyraźne normy prawne, dostępne w momencie podejmowania decyzji o ataku wskazywały nie tylko, że atak ów nie jest zabroniony (co byłoby wystarczające na gruncie zasady prohibitywności), ale też wyraźnie dozwolony. Pomimo to działania organizacji humanitarnych i mediów zupełnie nie regulowane prawnie (ani na prawie nie oparte) spowodowały w sądowym rozstrzygnięciu ominięcie zupełnie kwestii legalności ataku. Ponieważ orzeczenie to nigdy nie było kwestionowane, podobnie jak sposób jego wydania, należy przyjąć, zgodnie z normą art. 38 Statutu MTS, że *lawfare* jest legalnym, a przynajmniej niezakazanym środkiem prowadzenia konfliktu. Należy także zauważyć,że zasada odmówienia ochrony określonemu sposobowi wykonywania prawa, na mocy zasady *male nostro iure...* możliwa jest wyłącznie po dokładnym zbadaniu sprawy przez odpowiedni sąd lub trybunał. Sam ten fakt, a więc możliwość,

---

[917] zob. Art 8(1)(a) Konwencji Haskiej o ochronie dóbr kultury w razie konfliktu zbrojnego wraz z załącznikami podpisanej 14 maja 1954 (Dz.U. z 1957 nr 46 poz. 212 zał.)

[918] zob. Y. Dinstein *Legitimate Military Objective Under The Current Jus In Bello. The principle of distinction and military objectives* [w:zbiorowa, red. A.E. Wall *Legal and Ethical Lessons of NATO Kosovo's campaign* International Law Studies 78 (2016) ss.145-52]

[919] Arkin W.M., Ivansevic B. Civilian Deaths in the NATO Air Campaign RaportHuman Rights Watch (2000) ss.5-7

[920] International Criminal Tribunal for the Former Yugoslavia, *Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against theFederal Republic of Yugoslavia,* Publikacja MTKBJ, (2000) par.4

że legalny, zgodnie z *black-letter law,* atak może być kwestionowany przed sądem, musi wpływać na podejmowanie decyzji o nim - stając się z kolei tym samym elementem *lawfare*. Nie jest też wykluczone, że poza samą oceną strat i zysków wizerunków czy ewentualnych kosztów procesowych, samo istnienie konieczności wykazania zasadności własnego działania - czy to przed sądami lub trybunałami międzynarodowymi, czy też przed samą opinią publiczną może prowadzić do ujawnienia źródeł (najczęściej utajnionych), co samo w sobie grozi państwu ujawniającemu takie informacje poważnymi konsekwencjami. Na taką interpretację, wskazuje też istniejąca praktyka międzynarodowa, *opinio iuris* państw i orzecznictwo trybunałów i sądów międzynarodowych, jednomyślnie odrzucająca delegalizację *lawfare* na mocy wspomnianej zasady *male nostro iure...*

Problemy te oczywiście wynikają z braku regulacji prawnej dotyczącej *lawfare* i *cyberlawfare*, które ze względu na samo istnienie *lawfare*, są jednak niewykonalne.[921] Norma taka (skonstruowana na podobieństwo norm programowych w porządkach krajowych) musiałaby być sama elementem prawa międzynarodowego i jako taka - także podlegałaby *lawfare*.

Zjawisko c*yberlawfare* jest funkcją opisanego wyżej zjawiska *lawfare* i możliwości technicznych wynikających z samej istoty cyberprzestrzeni, prowadzone za pomocą normowania faktycznego. O ile bowiem w klasycznym pojęciu, *lawfare* może być stosowane do wpływania na sytuację stron podczas konfliktu, należy pamiętać że jest on wyłącznie jednym z elementów tą sytuację kształtujących. Strona przeciw której *lawfare* jest stosowane, może jednak przyjąć straty z niego wynikające by zachować przewagę wynikającą z innych okoliczności. Przykładowo, może ona przyjąć straty prawne wynikające z nieujawnienia okoliczności, które mogłyby zdjąć z niej określone oskarżenie, jednakże dzięki temu zachować przewagę faktyczną, gwarantowaną przez zachowanie tajemnic. W cyberprzestrzeni zachowanie takie jest niemożliwe, ze względu na normowania faktyczne. *Cyberlawfare* bowiem nie tyle tworzy normy, które wiążą strony konfliktu - co zmienia w określony sposób

[921] zob. Yoo J. *War by other means: an insider account on war on terror* Atlantic Mth. Press 1st ed. (2006) s.5

architekturę systemu, w którym konflikt ów jest prowadzony. Tworzy natomiast zaplanowane afordancje: albo bezpośrednio umożliwiające określone naruszenie albo modyfikujące sposób inkorporacji norm prawa międzynarodowego do prawa cyberprzestrzeni. Ponieważ te ostatnie wynikają najczęściej z prawa zwyczajowego,[922] bardzo często oparte są o działania mające na celu realizację interesów państw(z powodu ich dostosowania do praktyki międzynarodowej).[923]

Zgodnie z opisaną wyżej doktryną normowania faktycznego cyberprzestrzeni, to architektura systemu, zarówno zaatakowanego, jak i tego, z którego atak jest przeprowadzany, będzie decydowała o parametrach ataku. W istocie bowiem, w przeciwieństwie do ataku (zarówno kinetycznego jak i niekinetycznego), kontrola nad raz uruchomionym działaniem, prowadzącym do naruszenia suwerenności innego podmiotu jest znacząco ograniczona, podobnie jak ograniczona jest kontrola nad raz uruchomionym kodem, który wykonuje określone zadania. Wskazuje się, że *cyberlawfare* tym skuteczniejsze im więcej obszarów prawa obejmuje - wliczając w to nie tylko *lex informatica* i obszar prawa międzynarodowego publicznego ale także obszary prawa krajowego i prawa międzynarodowego prywatnego.[924] Ponieważ wpływ, który cyberprzestrzeń wywiera na świat rzeczywisty obejmuje wszystkie te zakresy - normowanie ich wszystkich wpływa na afordancje istniejące w informatycznej części cyberprzestrzeni. *Cyberlawfare* należy więc uznać za zespół zachowań, wykorzystujący zarówno normy prawa międzynarodowego, praw krajowych poszczególnych państw jak i *lex informatica* (w ramach normowania faktycznego) w celu osiągania przez podmioty prawa międzynarodowego (w tym

---

[922] Michael Schmitt odnosząc się do prawa zwyczajowego dotyczącego konfliktów w cyberprzestrzeni stwierdził wręcz, że nie sposób danego zachowania oceniać *in abstracto*, właśnie ze względu na płynność regulacji prawnych konstruowanych w opisywany sposób. zob. Schmitt M. N. *The 'Use of Force' in Cyberspace: A reply to Dr Ziolkowski* [w: zbiorowa,red. Czosseck Z., Ottis R.,Ziolkowki K. *4th International Conference on Cyber Conflict*, NATO Cooperative Cyber Defence Centre Of Excellence Publications Tallinn (2012) s.125] O ile sam pogląd jest dyskusyjny z logicznego punktu widzenia, ponieważ niezależnie od przyjętych kryteriów, żadne zachowanie nie może być jednocześnie legalne i nielegalne, argumentacja doskonale ilustruje problemy z precyzyjnym określeniem norm prawa międzynarodowego i dokonania ich subsumpcji.

[923] ibid.

[924] zob. Canuel E. *The Four Arctic Law Pillars: A Legal Framework* Georgetown Journal of International Law 46:735 (2016) s. 737

non-state actors[925]) założonych celów faktycznych i prawnych. Celami faktycznymi *cyberlawfare* może być stworzenie określonych afordancji - pozwalających na przeprowadzanie danej cyberoperacji w tym naruszeń suwerenności. Celami prawnymi może być zmiana kwalifikacji danego zachowania w cyberprzestrzeni w sposób gwarantujący ograniczenie możliwej odpowiedzi lub prawa do obrony przez podmiot, którego suwerenność ma zostać naruszona. W obydwu więc przypadkach, prawo staje się nie tyle normą broniącą określonego porządku, co narzędziem służącym do tego porządku naruszania lub przynajmniej jego modyfikowania. Należy także zauważyć, że brak jednoznacznej definicji zarówno *lawfare* jak i *cyberlawfare*. Należy także pamiętać, że, jak już wskazano powyżej, w odniesieniu do *lawfare* także *cyberlawfare* jest zjawiskiem ciągle zmieniającym się - definicja taka jest niemożliwa. Ponadto, ponieważ definicja taka musiałaby być ujęta w akcie prawnym, sama mogłaby być użyta do prowadzenia tegoż.[926]

2. Zastosowanie Cyberlawfare w operacjach cyberprzestrzennych

Prawo zwyczajowe dotyczące cyberprzestrzeni przyjmuje, że bronią w rozumieniu prawa cyberprzestrzeni jest każda metoda prowadzenia operacji cybernetycznych w sposób mogący prowadzić do strat w ludziach lub zniszczenia określonych obiektów fizycznych.[927] Cytowany przepis rozróżnia też pomiędzy bronią w cyberprzestrzeni - środkami prowadzenia wojny w cyberprzestrzeni, przez które rozumie broń a także wszystkie systemy rozprzestrzeniania kodu, który może zostać wykorzystany do przeprowadzanie operacji[928]. Oczywista jest analogia z istniejącego w prawie konwencjonalnego konfliktu zbrojnego rozróżnienia na broń, i środki jej

[925] zob. też Tanyildzi M.E. *State Responsibility in Cyberspace: The Problem of Attribution of Cyberattacks conducted by non-state actors,* Law and Justice Review 8:14 (2017) ss.120-5

[926] zob.Raport z sympozjum Case Western Reserve University School of Law [w: zbiorowa, red. Scharf M., Andersen E. *Is Lawfare Worth Defining?*, Case Western Reserve Journal of International Law 43:11 (2011) ss. 12-7

[927] zob.Rule 41 *Tallin Manual*

[928] Ibid, wraz z komentarzem IGoE par. 2

przenoszenia. Już z samej natomiast definicji cyberataku,[929] zarówno kinetycznego jak i niekinetycznego, łatwo można zauważyć, że definicja broni cybernetycznej nie jest wystarczająco ostra.[930] Wiele operacji cybernetycznych ma potencjał do wywołania skutków kinetycznych, jednak pomimo to ostatecznie nie wywołują one skutków w świecie fizycznym. Nie sposób więc przypisać narzędziom ich wykonywania *in abstracto* statusu broni i podobnie nie da się określić czy dana operacja powinna być uznana za atak. Mechanizm ten został już opisany powyżej. Jednakże ma on istotną konsekwencję w związku ze zjawiskiem *cyberlawfare*. Strona, która operację przeprowadza, może dowolnie, na każdym z etapów jej prowadzenia - eskalować lub deeskalować jej zakres i w konsekwencji wybierać pomiędzy rozmaitymi stopniami prawnej doniosłości własnej operacji. Sama ta możliwość odróżnia cyberatak (a więc i *cyberlawfare*) od odpowiedniej fazy ataku konwencjonalnego. Po pierwsze, nawet samo zbliżanie się samolotów czy okrętów do granicy przestrzeni powietrznej czy wód terytorialnych jest uważane za zachowanie ryzykowne, uruchamiające protokoły obrony. Po drugie, możliwości modyfikacji ataku kinetycznego są znacząco ograniczone. Po trzecie, nawet te ograniczone modyfikacje mieszczą się w ramach pierwotnej siły użytej do wykonania ataku. Możliwa jest bowiem zmiana celów nalotu - jednak jego całościowa intensywność pozostanie niezmieniona. W cyberprzestrzeni te ograniczenia nie obowiązują. Nietrudno więc zauważyć, że przeprowadzenie hipotetycznego uderzenia prewencyjnego wymagające stwierdzenia ataku, dokonania jego atrybucji, określenia celów, opracowania proporcjonalnego uderzenia prewencyjnego, a następnie jego przeprowadzenie, będzie niezmiernie ciężkie a jeżeli wziąć pod uwagę potencjalne konsekwencje błędu- bliskie niemożliwości.[931] Spróbujmy rozważyć sytuację,

---

[929] zob. Rule 92 *TM 2.0.* Powołany przepis uznaje za cyberatak każdą cyberoperację, która może rozsądnie oceniając, powodować straty w ludziach lub w mieniu.

[930] zob. także Foltz A.C. *Stuxnet, Schmitt Analysis and the Cyber 'Use of Force' Debate.*Joint Forces Quaterly 67:4 (2012) s. 47

[931] I to pomimo dokonania natychmiastowej analizy prawnej. Nie rozwiązuje więc tej kwestii, przejęcie rozpowszechnionej w konfliktach kinetycznych praktyki,polegającej na włączaniu oficerów prawnych, których wyłącznym zadaniem jest dostarczenie dowodzącym operacją analizy o skutkach prawnym planowanych przez nich działań w czasie rzeczywistym. zob. Także Dunlop Ch. J. *Law and Military Intervention...* s.8

w której dokonano cyberataku, przy użyciu tzw. *BotNetu*,[932] zaprogramowanego w taki sposób by w jednym czasie wszystkie komputery do niego podłączone wykonały atak niekinetyczny na sieć państwa, przeciwko któremu atak jest prowadzony i doprowadziły do wyłączenia jego systemów wrażliwych. Atak taki został przygotowany wcześniej, ponieważ prosty kod, zawierający koordynaty celu i precyzyjny moment ataku został umieszczony na etapie włączania danego komputera do *BotNetu*, na podobieństwo bomby logicznej. Naruszenie jurysdykcji następuje dopiero na etapie pojawienia się pierwszych skutków ataku, który już powoduje straty w infrastrukturze wrażliwej. Dochodzi w tym momencie do powstania po stronie państwa zaatakowanego prawa do uderzenia prewencyjnego lub obrony. Zgodnie z mechanizmami opisanymi powyżej. Jednak, nawet wobec przyjęcia doktryny domniemania nie istnieje odpowiedź kinetyczna, która mogłaby zostać uznana za proporcjonalną.[933] Nie będzie tu miał znaczenia fakt, że da się łatwo ustalić spełnienie przesłanki bezpośredniości ataku. Co więcej, w razie ewentualnego wstrzymania ataku, państwo, które wykonało uderzenie prewencyjne (nawet niekinetyczne), może zostać oskarżone o niesprowokowaną akcję także przeciwko jurysdykcjom trzecim (istotą tworzenia BotNetu jest przejmowanie komputerów znajdujących się w różnych częściach świata - zgodnie z zasadą wszechobecności cyberprzestrzeni), a więc zabronioną interwencję wobec państw w daną operację niezaangażowanych. Istotną rolę pełnić będzie także tzw. Zasada Webstera,[934] powszechnie przyjmowana do oceny legalności operacji wykonywanych w ramach wykonywania prawa obrony własnej suwerenności. Wskazuje ona, że siła użyta do legalnej obrony wymaga dla swojej legalności spełnienia pozytywnej przesłanki skuteczności (w zakresie obrony przed atakiem).[935] W przypadku opisywanego tu

---

[932] Chodzi o sieć uprzednio zaatakowanych komputerów, które sterowane zdalnie, przekazują część swojej mocy obliczeniowej podmiotowi, który atak przeprowadza. zob. Sabanal P. *Thingbots: The future of Botnets in the Internet of Things,* artykuł opublikowany w IBM Security Intelligence (2016) s.1

[933] Taki atak nie mógłby być przypisany rozsądnie państwu, na terytorium którego znajdują się zainfekowane kodem malware komputery, przekraczałoby to poziom nawet najostrzejszego testu odpowiedzialności państwa za działania prowadzone z jego terytorium,przyjętego w sprawie *Tadić.*

[934] Cyt za *British Foreign and State Papers 1840-41* 29 s.1138

[935] Zwyczajowe prawo międzynarodowe nie przewiduje jakiegokolwiek złagodzenia

przypadku, legalna obrona zostaje ograniczona do uderzenia prewencyjnego (ponieważ państwo stanowiące cel musi się liczyć z utratą własnego potencjału cyberprzestrzennego w związku ze skutecznym przeprowadzeniem operacji) Skoro więc możliwa jest taka konstrukcja BotNetu, by był on przeprowadzany jednocześnie z wielu jurysdykcji,[936]przeprowadzenie odpowiedzi cyberprzestrzennej wymagałoby spełnienie wszystkich wspomnianych przesłanek legalności odpowiedzi przeciwko każdej z tych jurysdykcji. Należy także pamiętać, że taki atak prewencyjny musiałby być, z natury operacji zakładających użycie BotNetów (najczęściej wykorzystujących elementy sieci cywilnej, jako najprostsze do przejęcia), skierowany przeciwko systemom cywilnym, będzie więc łamać normę regulującą kwestię legalnego atakowania celów cywilnych.[937] Oczywiście, należy rozpatrzyć, czy wobec tego sam atak przy pomocy *BotNet* nie powinien być uznany, z przytoczonych wyżej powodów za atak przy wykorzystaniu infrastruktury cywilnej. Wydaje się, że ze względu na brak jasnej normy regulującej tę kwestię, winna rozstrzygać praktyka międzynarodowa, a ta jednoznacznie odmawia uznania ataków tego typu za nielegalne ze względu na wykorzystanie infrastruktury cywilnej. Należy także pamiętać o wskazanej już zasadzie przyjmowanej między innymi przez *Tallinn Manual 2.0* - dotyczącej rozróżniania cyberprzestrzennej infrastruktury cywilnej i militarnej na podstawie kryterium funkcjonalności. Ponadto, w przeważającej większości - operacje cyberprzestrzenne wykorzystują infrastrukturę cywilną - co wynika z samej konstrukcji cyberprzestrzeni- zakres delegalizacji musiałby być więc dużo szerszy i zasadnie można twierdzić, że norma taka nie znalazłaby potwierdzenia w praktyce międzynarodowej i *lex informatica*.[938] Co więcej, nawet świadome

---

rygoru testu w przypadku ataku terrorystycznego, tak więc ewetnualna kwalifkacja ataku jako terrorystyczny nie zmienia możliwości państwa zaatakowanego, co do stosowania samooborony. zob.*Frequently Asked Questions on International Law Aspects of Countering Terrorism* UNODC(United Nations Office on Drugs and Crime) (2009) s.64

[936] Chodzi tu wyłącznie o fizyczną część cyberprzestrzeni. W kontekście ataku przez BotNet, granice jurysdykcji w informatycznej części cyberprzestrzeni nie będą miały istotnego wpływu na stan prawny.

[937] zob. Rule 102 w związku z Rule 111 w zw. z Rule 115 *Tallinn Manual 2.0*

[938] zob. Kittrie *Lawfare...* s.172

i dobrowolne udostępnienie własnych komputerów cywilnych[939] w celu przeprowadzenia ataku opartego o BotNet nie zostało uznane za przesłankę utraty przez ochotników statusu cywilów.[940] Zgodnie z argumentacją *a fortiori* należy więc przyjąć, że tym bardziej ochronie podlegają elementy sieci przejęte bez zgody ich użytkowników.

Opisywany powyżej przykład operacji wskazuje, że odpowiednie wykorzystanie natywnych dla cyberprzestrzeni możliwości (jak choćby wynikających z jej anonimowości i wszechobecności), a także odpowiedniej konstrukcji afordancji pozwala osiągnąć sytuację, w której zarówno prawo międzynarodowe jak i *lex informatica* mogą zostać wykorzystane do ograniczenia możliwego zakresu odpowiedzi i utrudnienia obrony państwu przeciwko, któremu dana operacja jest przeprowadzana.

3. Cyberlawfare a zasada nieintereferencji.

Związek *cyberlawfare* i zasady nieinterferencji należy rozpatrywać na dwóch płaszczyznach. Pierwszą z nich jest normowanie faktyczne, drugą wpływ na normatywne postrzeganie tej zasady. Nietrudno zauważyć, że ostateczny kształt tej zasady w cyberprzestrzeni będzie metanormą, funkcją obydwu wspomnianych elementów. Jest oczywiste, że cyberprzestrzeń umożliwia dokonywanie interferencji na dużo większą skalę i w o wiele prostszy sposób niż w przypadku naruszeń poza cyberprzestrzenią. Jakiekolwiek działania mające na celu dokonanie interferencji musiały być przeprowadzane w sposób, który wymagał czynnego działania przez

[939] Mowa tu o przypadku, w którym Izrael udostępnił do pobierania program *Patriotinstaller*, umożliwiający przekazywanie mocy obliczeniowej cywilnych komputerów osób, które zdecydowały się zainstalować kod, izraelskiej armii w celu zastosowania do wykonywania operacji BotNet skierowanych przeciwko Hamasowi. zob. Także Zdrnja B. *An Israeli patriot program or a trojan?* InfoSec Diary Handlers Blog (2009). ss.1-2 Żaden z członków społeczności międzynarodowej nie zgłaszał obiekcji do takiego zastosowania cywilnej infrastruktury cyberprzestrzennej.

[940] Zgodnie z regulacjami prawa zwyczajowego, cywile tracą swój statut wyłącznie w przypadku bezpośredniego udziału w konflikcie. Samo udostępnienie prywatnych komputerów należy uznać za udział wyłącznie pośredni. Duże poparcie ma w doktrynie teza, że w razie wątpliwości co do stopnia udziału cywilów w konflikcie zbrojnym, należy domniemywać że jest on pośredni dopóki nie zostanie ponad wszelką wątpliwość udowodniona teza przeciwna. zob. Rule 97 *Tallinn Manual 2.0* wraz z komentarzem IGoE do tegoż - par. 12 i 13.

państwo naruszające a w związku z tym pozostawienia przez to państwo śladów. Tradycyjnie wskazywanymi przykładami takich działań było prowadzenie działań propagandowych, mających na celu wpłynięcie na opinie publiczną w danej sprawie. Jednakże działania takie mogłyby być prowadzone wyłącznie na ograniczoną skalę, na przykład poprzez nadawanie audycji radiowych, z nadajników radiowych umieszczonych poza granicami jurysdykcji danego państwa. Takie środki jednak nie mogły mieć daleko idących skutków, jak i stosunkowo łatwo było je zneutralizować. Tymczasem cyberprzestrzeń pozwala na interferencję w *domaine reserve* przy pomocy analizy tzw. *Big Data*.[941] W stanie prawnym obowiązującym w okresie powstawania niniejszej rozprawy, *Big Data* nie jest regulowane przez żadne ze źródeł prawa międzynarodowego.[942] Tymczasem, o ile bierne ich zbieranie i analizowanie należy uznać raczej za legalny biały wywiad,[943] stwarzane przez analizę *Big Data* możliwości istotnie zwiększają skuteczność działań interferencyjnych. Wydaje się, że zbierania i analiza danych w tym zakresie mieści się w zakresie dozwolonego prawem międzynarodowym zbierania informacji, zdaje się to też potwierdzać praktyka międzynarodowa.[944] Co więcej, stosując *cyberlawfare*, państwo może przeprowadzić operację mającą na celu dokonanie interferencji, w taki sposób, by osiągnąć wszystkie założone skutki takiej operacji, nie naruszając istniejącego w swoim obecnym kształcie ani prawa międzynarodowego publicznego, samego *lex informatica*, a także, co łatwo już dostrzec, żadnej z metanorm. Rozpatrzmy operację mającą na celu wpływ na referendum w sprawie przyjęcia pewnej umowy międzynarodowej - a więc na istotny proces polityczny, przy pomocy ówcześnie zebranego z legalnych źródeł

---

[941] Chodzi o dane zbierane przy pomocy mediów społecznościowych, danych handlowych i wielu innych dających możliwość opracowania modelu zainteresowań poszczególnej osoby i przypisywania go do numerów IP urządzenia, co pozwala później na celowanie określoneych przekazów, już nie tyle do grup społecznych co do określonych jednostek. zob. Także Sagliocca A. *Cambrigde Analytica and Big Data: where are we now? Some post-scandal reflection on the Data Analytics and Political Consulting Gain.* Ingenium 5/18 (2018) s.2-3.

[942] Nie sposób nwet uznać braku sprzeciwu wobec stosowania go za prawo zwyczajowe, ponieważ nie ma pewności co do istnienia *opinio iuris*.

[943] Tzw. OS INT (Open-Souce Intelligence),czyli zbieranie informacji z jawnych i powszechnie dostępnych źrodeł. zob. Także Hulnick A.S. *The Dilemma of Open Source Intelligence:Is OSINT Really Intelligence?* The Oxford Handbook of National Securitz Intelligence (2010)s.229 i n.

[944] Choć nie sposób mówić na razie o wykształceniu się w tym zakresie jakiegokolwiek prawa zwyczajowego.

Big Data, bez naruszenia suwerenności w cyberprzestrzeni. *Prima facie*, działania takie będzie interferencją, lub gdyby przekroczony został próg *coercion* (przymusu)[945], nawet interwencją w wewnętrzne sprawy suwerennego państwa.

Rozpatrzenie ewentualności przeprowadzenia ataku DDoS na systemy wyborcze w taki sposób, by uniemożliwiły odczytywanie właściwych komunikatów wyborczych, jednocześnie wyświetlając ciągle na komputerach użytkowników grafikę sugerującą jedną z odpowiedzi w referendum, niewątpliwie należy uznać przynajmniej za interferencję. Możliwy jest jednak zupełnie inny scenariusz przeprowadzenie podobnej operacji. Może się ona opierać na utworzonej specjalnie na ten cel platformy propagandowej a następnie udostępnionej członkom sił politycznych w kraju stanowiącym cel, a mającym na owo przykładowe referendum pogląd zbieżny z interesem państwa przeprowadzającego operację. O ile celem, tak jak poprzednio, będzie ingerencja w proces polityczny i, jak poprzednio, spełniona będzie przesłanka przedmiotowa, wskazanie naruszenia jurysdykcji będzie w zasadzie niemożliwe. Operacja będzie bowiem przeprowadzana w jurysdykcji państwa je przeprowadzającego. Państwo, które więc chciałoby realnie przeciwdziałać faktycznemu wpływowi strony trzeciej na własne procesy polityczne musiałoby samo naruszyć suwerenność państwa ten wpływ mającego. Należy tu zwrócić uwagę na fakt, że zakaz interferencji jest wyłącznie prawem refleksyjnym suwerenności w jej aktualnym kształcie. Nie jest jego celem nadrzędnym ochrona jakiegoś dobra prawnego, dlatego nawet stwierdzenie *ex post facto* faktycznego wpływu na ów proces polityczny, nie może wtórnie delegalizować zachowania, o ile skutek osiągnięto metodami legalnymi. Państwo takie musiałoby odwołać się do normowania faktycznego, a więc takiej konstrukcji własnych wewnętrznych norm, które pozwoli na skuteczne zablokowanie przepływu treści. Niewątpliwie możliwe byłoby także zastosowanie retorsji. Jednak brak możliwości ściśle rozumianej obrony przed takimi

[945] Chodzi tu o wykonywanie środków politycznych dostępnych podmiotom prawa międzynarodowego w sposób, który prowadzi do zakazanego prawem wymuszenia odpowiedniej reakcji. Legalne więc są w przypadku *coercion* środki, natomiast osiągane za ich pomocą cele prawo międzynarodowe uznaje za naruszenie suwerenności państwa. zob.także Farer T.J. *Political and Economic Coercion in Contemporary International Law*, The American Journal of International Law 79: (1985) ss.407-11

działaniami. Czysto teoretyczna możliwość odłączenie całego państwa od sieci, praktycznie nie zostanie wykorzystana, ze względu na dużo większe straty, które państwo decydujące się na takie działanie musiałoby ponieść. Ewentualna próba cenzorowania takiego dostępu, może wyłącznie takie działania utrudnić, nie może ich jednak zatrzymać.[946] Istotny jest także fakt, że operacja interferencyjna, jest przygotowywana na dłuższy okres czasu, co dodatkowo utrudnia przeciwdziałanie. Ewentualne środki temu celowi służące muszą być bowiem utrzymywane przez dłuższy okres czasu, a środki przeciwdziałania w cyberprzestrzeni wymagają dla swojej skuteczności dużej dolegliwości dla osób postronnych.[947] Jednakże państwo, które z jakichś powodów nie jest w stanie osiągnąć swoich celów przy pomocy inteferencji opisanej powyżej, zgodnie z zasadami *cyberlawfare*, zdecydować może o podniesieniu poziomu swojej operacji do interwencji w ów proces polityczny. Ponieważ kolejną istotną cechą cyberprzestrzeni jest jej przewidywalność, decyzja taka może zostać podjęta z bliską pewności oceną sytuacji, co jest kolejnym czynnikiem budującym pozycję państwa operację przeprowadzającego. Ma ono bowiem świadomość, że za ewentualną interwencję odpowiadać będzie wyłącznie na gruncie reżimu odpowiedzialności za czyny międzynarodowo zakazane. Szczegółowa analiza tej odpowiedzialności, wskazuje na kolejny etap w konstrukcji *cyberlawfare*. ARSIWA przypisuje bowiem odpowiedzialność za akt międzynarodowo zabroniony[948], pod warunkiem, że: (1) wynika on ze złamania normy, do przestrzegania której państwo to jest zobowiązane[949] i (2), że istnieje możliwość przypisania odpowiedzialności państwu naruszającemu.[950] Z kolei spełnienie pierwszej przesłanki przedmiotowej, definiowane jest jako zachowanie niezgodne

---

[946] Nawet tak daleko idące działania cenzorskie jak *Great China Firewall*, mogą być stosunkowo łatwo omijane na poziomie dotyczącym dostępu do niestrzeżonych, dodatkowo zabezpieczonych, informacji. Pozwala na to istnienie technologii służącej do zmiany systemu kodowania łączności, tzw. *Virtual Private Network(VPN)*, stosunkowo łatwo do pobrania i praktycznie uniemożliwiającego blokowania dostępu do serwerów położonych po drugiej stronie punktu wejściowego. zob. także Bischoff P. *What's the Best VPN for China?* Comparitech 1/18 (2018) ss.2-4

[947] zob. Past L. *Cyberspace - Just another domain of election interference?* The European Centre of Excellence for Countering Hybrid Threats, Strategic Analysis 8/2018 (2018) s.5

[948] zob. Art. 1 ARSIWA.

[949] zob. ibid. Art. 2(a)

[950] ibid. Art.2(b)

z normami wiążącymi podmiot, niezależnie od źródła tej normy.[951] Państwo przygotowujące operację, ma więc już na etapie planowania możliwość wyboru jednego z trzech stopni zaawansowania. Pierwszym, najniższym jest dokonanie *Cyber Network Explotiation.* CNE ma najmniejszy potencjał osiągania celów, ale jest w zasadzie niewykrywalne.[952] Wyłącza to zarówno faktycznie jak i prawnie[953] możliwość dochodzenia jakiejkolwiek odpowiedzialności od państwa, które operację przeprowadza. Nie jest jednak oczywiste, że interferencja zostanie uznana za przekraczającą próg wywołujący odpowiedzialność.[954] Głównym czynnikiem umożliwiającym opisane powyżej działania jest brak jasnych kryteriów odróżniających legalne *Cyber Network Exploitation* od operacji naruszającej zakaz interferencji. W przeciwieństwie do przywołanego wyżej przykładu rozgłośni, działanie przy pomocy *Big Data* czy w ogóle operacji cyberprzestrzennych ma dużo większą skalę, przede wszystkim poprzez fakt umożliwienia aktywnego działania podmiotom działającym przeciwko legalnemu rządowi (zamiast wyłącznie udostępniania treści do biernego odbioru). Należy tu zauważyć, że Międzynarodowy Trybunał Sprawiedliwości, wskazał, że samo wspieranie ruchów secesjonistycznych jest już czynem międzynarodowo zabronionym, właśnie jako złamanie zasady nieinterferencji.[955] W przypadku cyberprzestrzeni, nawet po spełnieniu tej przesłanki, nie ma jasności czy rzeczywiście działanie można zakwalifikować jako czyn zabroniony. Zamiast jasnego kryterium wskazanego przez MTS, mamy bowiem do czynienia z konfliktem dwóch reguł uznawanych w prawie międzynarodowym za równorzędne, a mianowicie zasady nieinterferencji i prawa do samostanowienia.

---

[951] zob. ibid. Art. 12

[952] Sposoby na wykorzstywanie *cyberlawafare* w celu utrudniania lub uniemożliwiania atrybucji zostaną szczegółowo omówione w dalszej części wywodu.

[953] Chodzi tu o przesłankę przypisywalności, wynikającą z ARSIWA.

[954] Orzecznictwo międzynarodowe, w odniesieniu do interferencji, przyjmuje istnienie bliżej nieokreślonego progu, po przekroczeniu którego zawsze nielegalna inteferencja będzie pociągać za sobą odpowiedzialność prawnomiędzynarodową sprawcy. zob. *Nicaragua...*Awards par. 186

[955] zob. Memoranda rządów Francji(par. 29) i Zjednoczonego Królestwa (par. 34) [w: *ICJ Advisory Opinion on the Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo,* ICJ Reports 2010 p. 403 i n.] zob. Także Kohen M. *The Principle of Non-Intervetnion 25 Years after Nicaragua Jugdement* Leiden,Jorunal of International Law 25 (2012)s.16

Konflikt ten oczywiście istnieje ze względu na zasadę wszechobecności cyberprzestrzeni. Dodatkowym utrudnieniem analizy będzie sytuacja, w której do owego wspierania będzie dochodzić wyłącznie w cyberprzestrzeni. Stosując wskazany już mechanizm przypisywania jurysdykcji zwyczajnej w części informatycznej cyberprzestrzeni, należałoby przyjąć że naruszenie suwerenności następuje dopiero w momencie przesłania informacji w oparciu o serwery wewnątrz jurysdykcji, w której znajdują się elementy części fizycznej cyberprzestrzeni, w oparciu o które następuje interferencja. Prowadziłoby to do paradoksalnej sytuacji, w której operacja technicznie opierająca się właśnie na pozbawieniu państwa będącego celem środków rozpowszechniania pewnych treści, nie będzie ingerencją w sprawy wewnętrzne tego państwa, dopóki nie będzie ona przeprowadzana w oparciu o infrastrukturę cyberprzestrzeni położoną na jego terytorium.

Cyberlawfare może być także użyte przy ataku konwencjonalnym. Klasycznym przykładem takiego działania może być wykorzystanie ataku cyberprzestrzennego do 'oślepienia' systemów państwa zaatakowanego, w celu łatwiejszego wykonania ataku konwencjonalnego. Większość systemów obronnych, polega bowiem na układach komputerowych, których wyłączenie prowadzić może do utraty kontroli nad przestrzenią powietrzną czy wodami terytorialnymi w sposób umożliwiający przeprowadzenie z nich uderzenia konwencjonalnego, na który odpowiedź kinetyczna będzie niemożliwa lub osłabiona ze względu na uprzedni atak konwencjonalny. W takiej sytuacji uznaje się, że operacja cybernetyczna jest zamkniętą całością, a jej skutki należy rozpatrywać odrębnie od ataku kinetycznego.[956] Należy z tego faktu wyprowadzić wniosek, że jeżeli atak, który był przygotowywany w cyberprzestrzeni nie nastąpi z jakiegokolwiek powodu, dalej dochodzi do ataku wobec państwa zaatakowanego, na który państwo to ma prawo działać w ramach uderzenia prewencyjnego lub wykonania proporcjonalnej samoobrony. Ponieważ atak taki jest przesłanką do jednostronnego użycia siły lub zastosowania represaliów lub retorsji, państwo które go przeprowadziło, może łatwo zmniejszyć faktyczny rozmiar strat się nawet gdyby nie udało mu się zanonimizować operacji do stopnia

[956] zob. Schmitt M.N. *Legal framework*...ss.252-7

uniemożliwiającego atrybucję.[957]

4. Aktorzy niepaństwowi.

Wzrost znaczenia tzw. *Non-state actors,* a więc rozmaitych grup, które znajdują pewne określone miejsce w obrocie prawnomiędzynarodowym nie będąc jednak w żaden sposób bezpośrednio umocowanymi do reprezentowania tradycyjnych podmiotów prawa międzynarodowego publicznego jest charakterystyczny dla sytuacji międzynarodowej XX i XXI wieku.[958] Przywołana powyżej definicja negatywna, oczywiście musi być uznana za niewystarczającą, podobnie jak pozostałe próby zdefiniowania tego zjawiska.[959] Jedyną wynikającą z praktyki państw próbą określenia czym są *non-state actors* był art. 6 Porozumienia z Cotonou.[960] Porozumienie to uznaje *non-state actors* za ważny element rozwoju obydwu podmiotów i wskazuje, że należą do nich; (1) społeczeństwo obywatelskie w kształcie nadanym przez lokalne tradycje; (2) organizacje społeczne i gospodarcze; (3)sektor prywatny.[961]

Wszystkie te definicje są przydatne do analizy kwestii udziału aktorów niepaństwowych w cyberprzestrzeni wyłącznie w ograniczonym stopniu. Aktorzy niepaństwowi działający w, i wpływający, na cyberprzestrzeń, nie stanowią bowiem organizacji w ścisłym znaczeniu, a raczej grupy, które wyłączy wspólny cel, którego osiąganie jest najprostsze w cyberprzestrzeni. Grupy takie najczęściej koncentrują się więc na przeprowadzaniu cyberoperacji lub nawet cyberataków skierowanych przeciwko podmiotom państwowym. Operacje te najczęściej prowadzone są

---

[957]por. Reisman W.M. *Criteria for the Lawful Use of Force in International Law*, Yale Journal of International Law 10 279,281 (1985), tegoż *Article 2(4): The Use of Force in Contemporary International Law* Faculty Scholarship Series 741 (1984) ss.74-8

[958]Część doktryny przyjmuje za definicję przytoczone powyżej przesłanki a więc właśnie udział w obrocie międzynarodowym i brak reprezentacji jakiegoś państwa. Tak na przykład Clapham A. *Non-state Actors* [w: zbiorowa, red. Chetail V. *Post-Conflict Peacebuilding: A Lexicon* Oxford University Press (2009) ss.200-212]

[959]cf. Santarelli N.C.Non-state Actor's Human Right obligations and responsibility under international law Revista Electronica de Estudios Internacional 13 (2013) ss.2-4

[960] zob. Art 6 Zawartego pomiędzy Unią Europejską a krajami Grupy ACP (Africa, Caribbean, Pacific) 2000/483/EC OJ L 317 15.12.2000 ss.3-385 w czerwcu 2000 roku, zawierającego regulacje ramowe współpracy obydwu tych podmiotów.

[961]ibid. Art. 6

przeciwko infrastrukturze krytycznej państw uznawanych za wrogie (w przypadku ataków) lub wykradania i ujawniania tajnych danych (w przypadku operacji poniżej poziomu ataku).[962] Wskazuje się więc, że cybernetycznymi aktorami niepaństwowymi są najczęściej indywidualni hakerzy, powiązani w grupy ze względu na określone cele ideologiczne. Mogą być to tzw. 'haktywiści', czyli osoby powiązane wspólnym celem ideologicznym, lub na przykład grupy podobne do rosyjskich 'hakerów-patriotów', zwalczających państwa wrogo nastawione do Federacji Rosyjskiej (jak choćby ataki na Gruzję podczas Wojny Pięciodniowej czy na Estonię po usunięciu przez nią pomnika żołnierzy Armii Czerwonej z centrum Tallinna)[963], lub też hakerów-najemników.[964] Oczywiście, rozmaite organizacje terrorystyczne, czy przestępcze, także częstokroć powołują do życia własne grupy wpływu w cyberprzestrzeni.[965] Żadna z tych grup nie może być jednak traktowana podobnie do grup najemniczych czy nieregularnych oddziałów wojskowych w rozumieniu Konwencji Genewskich.[966]

Mogą one bowiem stanowić albo element regularnych sił zbrojnych danego państwa[967] (do których stosują się odpowiednio przepisy dotyczące sił zbrojnych danego państwa) albo stanowić grupy, które nie spełniają nawet nisko postawionego progu minimum uniformizacji i wpływu określonego państwa by zostać uznanymi za

[962]Szacunki te dotyczą oczywiście wyłącznie danych o cyberoperacjach, których szczegóły zostały ujawnione. zob. także Gazula M.B. *Cyber Warfare Conflict Analysis and Case Studies*, Cybersecurity Interdyscyplinary Systems Laboratory (CISL) Massachusetts Institute of Technology (2017).

[963]cf. Bussolati N. *The Rise of Non-state actors in Cyberwarfare* [w:zbiorowa, red. Ohlin J.D., Govern K., Finkelstein Cl. *Cyber War: Law and Ethics for the Virtual Conflicts* Oxford University Press (2015)ss. 102-26]

[964]zob. Raport Laboratorium firmy Kaspersky *The Icefog Apt: A Tale of Cloak and Three Daggers*(Kaspersky Lab Zero) (2013). s.1 Raport ten opisuje losy grupy najemniczej działającej wyłącznie w cyberprzestrzeni i przeprowadzającej cyberoperacje na zasadach identycznych jak oddziały najemników biorą udział w światowych konfliktach zbrojnych i prognozuje znaczny wzrost liczb podobnych grup w najbliższym czasie.

[965]Jak choćby grupy cyberprzestrzenne wspierające organizację Państwa Islamskiego. por. Lohrmann D. *Cyber Terrorism: How Dangerous is the ISIS Cyber Caliphate Threat?* Govtech.com 9/15 (2015) ss.2-3

[966]Bassiouni M. Ch. *The New Wars and the Crisis of Compliance with the Law of Armed Conflict* Journal of Criminal Law and Criminology 98:3 (2008) ss.713-5

[967]Jak w przypadku ochotniczej Estońskiej Ligi Obrony Cybernetycznej (Küberkaitsellit), powołanej do życia w 2010 roku. Członkami KKL są cywile, jednak Liga funkcjonuje w ramach systemów Ministerstwa Obrony Estonii i poddana jest dowództwu wojskowemu.
cf. Kaska K. Osula A.M., Stinissen J. *The Cyber Defence Unit of the Estonian Defence League,* NATO Cooperative Cyber Defence Centre of Excellence(2013) ss.8-12

nieregularne jednostki pod kontrolą określonego państwa.[968] Oczywiście, należy także pamiętać, że do grup takich stosują się opisane w rozprawie niniejszej problemy z atrybucją. Wskutek tego, państwa, których suwerenność naruszono, nie mają możliwości reakcji w drodze przewidzianej przez prawo międzynarodowe.[969] W odróżnieniu też od cyberoperacji przeprowadzanych przez inne państwa - aktorzy niepaństwowi, mogą w cyberprzestrzeni wykorzystywać w pełni infrastrukturę państw trzecich, w tym odpowiednio przygotowane sieci prywatne.[970] Grupa hakerów, dysponująca siecią botów może wykonywać operacje mające skutki podobne do ataku jednakże o mniej trwałym charakterze.[971] Taka operacja, nie tylko nie ma skutków trwałych czy kinetycznyc,h więc nie może być zakwalifikowana jako atak, ale także wykonywana jest z wielu niezależnych od siebie systemów i jurysdykcji i w żaden logiczny sposób nie powiązanych, co utrudnia zarówno atrybucję (ponieważ BotNet nie ma jednego 'centralnego' komputera, który steruje działaniami pozostałych), jak i utrudnia obronę pasywną, ze względu na brak możliwości określenia kierunku działań. Co istotne, nawet w razie określenia tożsamości przeprowadzających operację aktorów niepaństwowych, działania państwa broniącego się napotkałyby na istotne problemy z wykonaniem własnej jurysdykcji wobec członków tych grup. Po pierwsze, wykonywanie jurysdykcji nadzwyczajnej wobec zidentyfikowanych członków takich grup, znajdujących się poza granicami państwa broniącego się (co jest najczęstszym przypadkiem) byłoby

[968] zob. Orzeczenie w sprawie *Prokurator v. Fatmir Limaj,Haradin Bala, Isak Musliu,* MTK IT-03-66, (2005) par. 88ff

[969] Przykładowo, podczas, związanych z kryzysami politycznymi, ataków rosyjskich hakerów na państwa bałtyckie i Gruzję, społeczność międzynarodowa w żaden sposób nie uznała odpowiedzialności Federacji Rosyjskiej (pomimo aresztowania rosyjskich obywateli w Estonii w związku z atakami na sieci telekomunikacyjnego tego państwa i potwierdzonego w materiale dowodowym udziału obywateli rosyjskich w pozostałych cyberoperacjach) zob. Carr. J. *Inside Cyber Warfare: Mapping the Cyber Underworld* O'Reilly Media, wyd. 2 (2011)par.16. Także Krebs B. *Lithuania weathers Cyber Attack, Braces for Round 2*, The Washington Postz 3 czerwca 2008 s.1 i Shachtman N. *Kremlin Kids: We Launched the Estonian Cyber War*, Wired 3/09 (2009) ss.1-2

[970] Chodzi tu o tzw. BotNety. Komputery prywatnych, często nieświadomych tego faktu, użytkowników zostają zarażone wirusami, które pozwalają wykorzystywać część ich mocy obliczeniowej osobom trzecim. Podmiot kontrolujący tak skonstruowaną sieć, może w dowolnym momencie wykorzystać wielką sumarycznie moc obliczeniową. zob. Zetter K. *Hacker Lexicon: Botnets. The Zombie Computer Armies that Earn Hackers Millions,* Wired/Security (2015) s.1

[971] Jak DDoS (Distributed Denial of Service), polegający na wykonywaniu z BotNetu takiej ilości połączeń do określonego serwera, które w konsekwencji powodują jego przeładowanie i wyłączenie.

znacząco utrudnione. Jak wskazano powyżej, wykonywanie jurysdykcji nadzwyczajnej, jest sytuacją skrajną, która musi być uzasadniona okolicznościami. W przypadku operacji DDoS i w ogóle- operacji nie stanowiących cyberataku, a tym bardziej ataku ze skutkami kinetycznymi, zastosowanie jurysdykcji nadzwyczajnej jest w zasadzie wyłączone. Co więcej, nawet gdyby społeczność międzynarodowa uznała wykonywanie tej jurysdykcji za uzasadnione, doszłoby niewątpliwie do kolizji jurysdykcji nadzwyczajnych różnych państw. Wskazane powyżej przykłady operacji przeprowadzanych przez aktorów niepaństwowych, wydają się potwierdzać powyższą argumentację, ponieważ w żadnej z nich nie doszło do wykonania przez którekolwiek z państw stanowiących cel operacji swojej jurysdykcji nadzwyczajnej. Istotnym problemem jednak staje się sytuacja, w której ataku lub innego naruszenia suwerenności państwa dokonuje grupa stanowiąca tzw. *Non-state actors*. O ile bowiem niewątpliwie dochodzi do naruszenia suwerenności, kwestia ścigania staje się niezwykle problematyczna. W razie zwykłego ataku na terytorium państwowe dokonane przez *non-state actors*, odpowiedzialne może być państwo, z którego terytorium ataku dokonano, oczywiście na określonych przez prawo międzynarodowego zasadach. Odpowiedzialność może ponosić państwo, które na atak pozwoliło. Przede wszystkim, sama grupa będzie mogła być ścigana, państwo na którego terytorium przebywa, będzie miało obowiązek dokonania aresztowania i osądzenia grupy lub wydania ich państwu zaatakowanemu, a członkowie grupy będą ścigani przez państwa, których są obywatelami. Jednakże w przypadku ataku lub operacji cybernetycznej, przypisanie będzie dużo bardziej skomplikowane, zarówno prawnie jak i faktycznie. Po pierwsze, określenie miejsca ataku nie jest możliwe bez prześledzenia wszystkich programów maskujących IP i tożsamość przeprowadzającego operację. Możliwość kreowania fałszywych numerów IP, sugerujących zupełnie inne położenie geograficzne od miejsca, z którym dokonuje się połączenia z siecią jest w zasadzie podstawowym środkiem zabezpieczenia cyberoperacji. Po drugie, możliwe jest dokonywanie ataku z komputera, który się porusza. Na przykład, można wyobrazić sobie dokonanie ataku przez osobę, znajdującą się w pociągu, przekraczającym granice państw podczas trwania operacji

w cyberprzestrzeni Oczywiście, teoretycznie istnieje możliwość przypisania odpowiedzialności konkretnemu państwu, czy konkretnemu operatorowi sieci, ale w praktyce odpowiedzialność ta jest nie do wyegzekwowania. Nie można bowiem, uznać że sam fakt przejechania przez terytorium jakiegoś państwa osoby, która w danym momencie dokonywała cyberoperacji, dodatkowo logując się na przykład do sieci mającej infrastrukturę w państwie trzecim miałoby kreować odpowiedzialność po stronie tego państwa. Kolejnym problemem staje się możliwość dokonywania tzw. *spoofów*, czyli stosowanie programów fałszujących informację o lokalizacji urządzenia. Oczywiste jest, że państwa mają jurysdykcję nad elementami infrastruktury komputerowej położonej na ich terytoriach. Sytuacja komplikuje się jednak w przypadkach,w których wykorzystywana jest infrastruktura nie należąca do żadnej z jurysdykcji, na przykład kable podwodne położone na dnie morskim, regulowane osobnym traktatem i wyjęte spod jurysdykcji państwowej.[972] Oczywiście, zgodnie z definicją cyberprzestrzeni takie elementy także stanowią element fizycznej części cyberprzestrzeni.[973] Natomiast przypisanie odpowiedzialności państwu na drodze uznania jego kontroli nad określonymi grupami w cyberprzestrzeni jest nieomal niemożliwe. W momencie powstawania rozprawy niniejszej, nie zdarzył się ani jeden przypadek przypisania takiej odpowiedzialności, nawet przy zastosowaniu stosunkowo szerokich przesłanek testu *Tadić.* Stanowisko takie wydają się podzielać autorzy *Tallinn Manual 2.0*, którzy ograniczają zakaz interwencji w cyberprzestrzeni *explicite* do aktorów państwowych.[974]

Kolejnym problemem staje się sytuacja, w której nie chodzi o atak, a na przykład wyłącznie o hosting plików, które mogą zostać wykorzystanie do późniejszego ataku niezwiązanego z cyberprzestrzenią. Plikiem takim może być instrukcja dla drukarki 3d, umożliwiająca prosty wydruk zapalnika do bomby lub części pozwalających na

---

[972] zob. Lowe A.V.*The Problems of Extraterritorial Jurisdiction: Economic Sovereignty and the Search for a Solution* The International and Comparative Law Quarterly,34:3(1985) ss.724-746

[973] zob.Saffo P. *Disrupting Undersea Cables: Cyberspace's Hidden Vulnerability*, Atlantic Council (2013)

[974] zob. Rule 66 *Tallinn Manual 2.0* wraz z komentarzem IGoE par. 2. zob. Także Lotrionte C. *Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law*, The Cyber Defense Review 3:2 (2018) ss.74-8

złożenie broni maszynowej. Samo usunięcie takich plików, nie może być wystarczające, bowiem łatwość, z jaką można wykonać kopie, w praktyce wyłącza takie działanie jako skuteczne zapobieganie atakowi. Dodatkowo, jak wskazano powyżej - dokonanie samego tylko transferu danych, nie stanowi naruszenia suwerenności, nawet gdyby nastąpił on do strefy cyberprzestrzeni 'terytorialnej'. Zabezpieczenia pasywne. mogą bowiem zostać przełamane, a dane państwo (o ile wykorzystywało wyłącznie je) może nawet nie być świadome naruszenia własnego terytorium w tym zakresie. Podobną kwestią (a więc naruszenia suwerenności przy pomocy transferu danych) może być na przykład także oświadczenie opublikowane przez hakerów na stronie MSZ pewnego państwa i spełniające przesłanki przewidziane przez tzw. *Kazus Ihlena*[975] z późniejszym uzupełniającym go orzecznictwem. O ile sam precedens stał się źródłem dla świetnie ugruntowanej normy prawa zwyczajowego, która rozstrzygała kwestie związania państw oświadczeniami odpowiednio umocowanych jego przedstawicieli, w przypadku cyberprzestrzeni wydaje się ona stwarzać istotne zagrożenie wobec braku pełnej kontroli nad treściami, które mogą takie oświadczenia konstytuować. Konsekwencje faktyczne i stwarzane przez nie skutki prawne w razie publikacji podobnego oświadczenia i techniki umożliwiającej docieranie do tysięcy odbiorców bardzo krótkim okresie czasu mogą mieć bardzo doniosłe znaczenie. Praktyka międzynarodowa wskazuje jednak, że takie naruszenia są na porządku dziennym i nie tylko nie powodują one uruchomienia mechanizmów prawnych, ale wręcz należałoby się zastanowić, czy mają one nawet status zdarzeń prawnych

Normy ograniczające *ius ad bellum* (i w ogólności prawo do użycia siły) nie są wystarczająco skuteczne do przeciwdziałania przypadkom użycia siły przez *non-state actors.*[976] Można tu wskazać przykładowo starcie Izraela z Hezbollahem na granicy z

[975] Chodzi tu oczywiście o precedens decydujący w jakich okolicznościach oświadczenie przedstawiciela państwa może być dla tego państwa wiążące, wynikające ze sprawy rozpoznanej przed Stałym Trybunałem Sprawiedliwości Międzynarodowej *Legal Status of Eastern Greenland (Den. v. Nor.)*, publik. P.C.I.J. (ser. A/B) No. 53(1933).

[976] por. Kowalski M. *Ius ad bellum a systemowy charakter prawa międzynarodowego* [w: *Państwo a prawo międzynarodowe jako system prawa*, zbiorowa, red. Kwiecień R.] wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2005 s. 167-202

Libanem w 2006 roku.[977] Izrael ogłosił, że wykonuje swoje prawo samoobrony, wobec czego przeprowadzi operacje (w tym operacje odwetowe) na terytorium Libanu, pomimo uznania, że to nie państwo libańskie przeprowadziło uderzenie.[978] Brak atrybucji, a nawet podejrzewanego udziału państwa libańskiego oficjalnie potwierdził premier Izraela, Ehud Olmert, który nazwał Liban "zakładnikiem Hezbollahu", jednakże potwierdził, że działania na terytorium libańskim będą prowadzone.[979] Powszechną reakcją opinii międzynarodowej na to działanie było przyjęcie prawa do samoobrony Izraela, wliczając w to odpowiedź militarną skierowaną przeciwko Libanowi, wliczając w to naruszenie jego terytorium.[980]

W ten sposób Rada Bezpieczeństwa konkludentnie uznała, że działania *non-state actors* mogą uzasadniać działania kinetyczne wobec państwa z którego terytorium zostały przeprowadzone, nawet jeżeli odpowiedzialność za nie *per se* nie mogą być temu państwu przypisane. Wystarczającą przesłanką jest niespełnienie obowiązku przeciwdziałania atakom dokonywanym z własnego terytorium. Należy zwrócić uwagę, że przyjęta przez Radę legalność działań Izraela wykraczała poza zakres zwykłej samoobrony, ponieważ jego działania nie były obliczone na niezbędne powstrzymywanie trwającej agresji. Wydaje się więc, że prawo konfliktów zbrojnych przyznaje państwom bardzo szerokie uprawnienia do obrony własnej suwerenności przed aktorami niepaństwowymi. Prawo konfliktu cyberprzestrzennego nie wydaje się jednak przyjmować podobnych regulacji. Jego doktryna wskazuje, że prawo międzynarodowe może się stosować do operacji cyberprzestrzennych przeprowadzanych przez *non-state actors* wyłącznie w bardzo rzadkich przypadkach.[981] *Explicite* przyjęła też Grupa Ekspertów, że o ile działanie cyberprzestrzenne *non-state actors* nie zostanie prawidłowo atrybuowane państwu - nie można uznać go za naruszenie suwerenności państwa trzeciego (niezależnie od

[977] zob. raport o sytuacji na granicy libańsko-izraelskiej przedstawiony przez Jean-Marie Guéhenno, Radzie Bezpieczeństwa ONZ, nr 5489, 14 lipca 2006 roku ss.2-3.
[978] zob. Gray Ch. *International Law and the Use of Force*- Oxford University Press (2018), s.214 i n.
[979] zob. Komunikat Sekretariatu Gabinetu Rady Ministrów Izraela z dnia 16 lipca 2006 roku, punkt 1 i 2
[980] zob. Milanovic M. *Self-Defence and Non-state Actors:Intedeterminacy and Jus ad bellum* Ejil:Talk!,2/10 (2010) ss.2-4
[981] cf. *Rule 33 Tallinn Manual 2.0*

stopnia faktycznego naruszenia), ponieważ suwerenność państwa może naruszyć wyłącznie inne państwo.[982] Pomimo więc, że IGoE uznaje możliwość istnienia innego poglądu,[983] należy jednak wskazać, że uznawany za najbardziej reprezentatywny zbiór norm prawa konfliktu cyberprzestrzennego *TM 2.0* jak i praktyka międzynarodowa, stoją na stanowisku niezdolności aktorów niepaństwowych do dokonywania naruszeń suwerenności. Według IGoE, nie stoi to jednak na przeszkodzie wykonywaniu obrony przeciwko atakom przez nie przeprowadzanym.[984] Dokonywanie atrybucji opisanym powyżej grupom hakerskim jest w przypadku każdej atrybucji cyberprzestrzennej trudne. Ponadto TM 2.0 przyznaje prawo obrony na zasadach ogólnych jednak z zachowaniem poglądu o niemożliwości naruszenia suwerenności przez *non-state actors.* W oczywisty sposób ogranicza to możliwość prowadzenia tej obrony wyłącznie do ataków kinetycznych. W praktyce oznacza, to wyjęcie niekinetycznych (zarówno ataków jak i *CNE*) cyberoperacji prowadzonych przez aktorów niepaństowych z zakresu prawa międzynarodowego i normowanie ich wyłącznie poprzez *lex informatica*, co czyni z takich grup idealne narzędzie do prowadzenia operacji w ramach *cyberlawfare.* Wyjątkiem od tej zasady, mogłaby być sugestia IGoE by utworzyć specjalny reżim ścigania aktorów niepaństwowych w cyberprzestrzeni,[985] lub stosowania środków prawnych stosowanych dla działalności *stricte* policyjnej.[986] Obydwie te propozycje należy jednak uznać za nietrafione, ze względu na brak istotnych traktatów cyberprzestrzennych w tym zakresie, uniemożliwiający pierwszy i pośrednio drugi ze wskazanych sposobów zwalczania prowadzenia *cyberlawfare* przy pomocy *non-state actors*. Doskonałą ilustracją opisanego wyżej mechanizmu jest Konwencja Rady Europy przeciwko Cyberprzestępczości.[987] Zawarty w konwencji próg ilości ratyfikacji konieczny do wejścia w życie został osiągnięty dopiero w ciągu kilku lat

---

[982] zob. *ibid.* Także komentarz IGoE do *Rule 33* par.2

[983] ibid. Par. 2 *in finem*

[984] ibid. Par. 3 *in finem*

[985] ibid. Par. 5

[986] ibid. Par. 7

[987] Council of Europe Convention on Cybercrime, podpisana w Budapeszcie 23 października 2001 roku, ETS-185; wraz z protokołem dodatkowym przyjętym 28 stycznia 2003 w Strasbourgu,6 ETS-189

po podpisaniu przez członków-sygnatariuszy konwencji. Do 2018 roku, Konwencję podpisała mniej niż połowa państw członkowskich ONZ. Jest ona też krytykowana za oparcie o bardzo ogólne kryteria, wyłącznie terytorialną jurysdykcję i w istocie tworzenie *superfluum* prawnego w stosunku do rozpowszechnionych ustawodawstw krajowych, posiadających często identyczne regulacje czy też traktatów międzynarodowych o współpracy prawnej dotyczącej przestępstw w ogóle.[988]

5. Terytoria sporne i mikropaństwa.

Istotnym elementem *cyberlawfare* może być także prowadzenie ich z jurysdykcji sztucznych lub wręcz stworzonych na potrzeby takiego ataku.[989]Łatwość z jaką przenoszone mogą być elementy części fizycznej cyberprzestrzeni oraz wspomniana wcześniej cecha wszechobecności cyberprzestrzeni, oznaczają że wykonanie dowolnej nieomal cyberoperacji jest możliwe z dowolnego punktu na świecie. W konsekwencji możliwe jest wykorzystanie do takiego celu "mikronacji", czyli *quasi*-państw, państw nieuznawanych lub uznawanych częściowo i o niejasnym statusie międzynarodowym (terytoriów spornych). Przyjmuje się, że współcześnie te *quasi-podmioty* prawa międzynarodowego, coraz częściej znajdują swoje miejsce w katalogu aktorów prawa międzynarodowego, głównie poprzez spełnienie kryterium faktycznego wykonywania aspektów państwowości.[990] Terytoria takie najczęściej leżą z dala od głównym obszarów zainteresowań podmiotów prawa międzynarodowego, a ich utrzymanie w ramach strefy wpływów danego państwa, najczęściej uznawane jest za sprawę prestiżową. Często jednak takie niewielkie

---

[988] zob. Shalini M.*Budapest Convention on Cybercrime - An Overview* New Dehli Center for Communicaton Governance, International Law and Policy & Emerging Tech nad National Security 3/3/16 (2016) s.2

[989] Chodzi tu zasadniczo o terytoria, których status międzynarodowy, nawet jeżeli nie ustalony w kwestii pozytywnych przejawów suwerenności, może służyć do negowania wykonywania jurysdykcji innych państw, lub też utrudnić znacząco wykonywanie jurysdykcji nadzwyczajnej wobec *non-state actors* znajdujących się na tych terytoriach. zob. Dumieński Z.*Microstates as Modern Protected States:Towards a New Definition of Micro-Statethood,*Centre for Small States Studies, Institute of International Affairs of University of Iceland (2014) ss.17-9.

[990] zob. Perkowski M.Podmiotowość prawa międzynarodowego współczesnego uniwersalizmu w złożonym modelu klasyfikacyjnym, Temida 2 (2008) s.334

quasi-jurysdykcje, mogą mieć zastosowanie w ramach *lawfare*.[991] Z prawnego punktu widzenia wystarczy bowiem spełnić, w tym celu, choćby czasowo jedną z trzech podstaw jurysdykcji nad terytoriami spornymi, wskazanych przez Stały Trybunał Arbitrażowy w sprawie *Palmas*.[992] Inną drogą przeprowadzania cyberataków z *quasi-jurysdykcji* jest tworzenie "mikronacji",[993] spełniających podobne warunki faktyczne. Wykorzystanie takich *quasi-jurysdykcji*, umożliwia prowadzenia cyberoperacji spoza zasięgu jurysdykcji tradycyjnych państw, a także uniknięcie odpowiedzi skierowanej przeciwko aktorowi ją przeprowadzającemu.[994] Możliwość wykonania cyberoperacji o skutkach porównywalnych do przeprowadzanych przez państwa z owej *quasi-jurysdykcji* jest kolejnym ograniczeniem możliwości obrony własnej suwerenności przez państwa.[995]

Pierwszą historycznie próbą założenia mikronacji, w celu uzyskania szerokiego dostępu do informatycznej części cyberprzestrzeni, przy jednoczesnym faktycznym wyłączeniu jurysdykcji państw trzecich nad elementami części fizycznej, było tzw. Księstwo Sealandii.[996] Założona na opuszczonej morskiej platformie artyleryjskiej z czasów drugiej wojny światowej, Sealandia postawiła sobie za cel zapewnienie podmiotom zlokalizowanym na niej jak najszerszych możliwości działania w cyberprzestrzeni, przy pomocy mechanizmów opisanych powyżej. W tym celu na Sealandii założono celową spółkę *HavenCo*., deklaratywnie podległą wyłącznie ustawodawstwu sealandzkiemu w zakresie cyberprzestrzeni.[997]O ile jasne jest, że sam

---

[991] Jak przykładowe, stosowanie dzierżawionej bazy w Guantanamo przez Stany Zjednoczone do obchodzenia własnej legislacji dotyczącej praw osób aresztowanych. zob. Także Elsea J.K., Else D.H. *Naval Station Guantanamo Bay: Hisotry and Legal Issues Regarding Its Lease Agreements* Conregssional Research Service 7-5700 (2016) ss.6-9

[992] *Island of Palmas case* (Netherlands v. USA) Permanent Court of Arbitration, Award) II RIAA 829 (1928) Awards. Par.121

[993] zob.Straus E.S. *How to Start Your Own Country*, Paladin Press (1999) ss.22-30

[994] ONZ przyjmuje, że nie ma znaczenia czy w takiej sytuacji przeprowadzającym operację jest aktor państwowy czy niepaństwowy. zob. Dokument ONZ z dnia 15 czerwca 2011 A/66/152 (2011) s.18

[995] zob. Roscini M. *Cyber Operations...* s.101

[996] S.Simon *Weekend Edition:Profile-Sovereign Principality of Sealand* (N'tl P. Radio), audycja z 2001. cyt. za transkrpytem (dost. 1.sieprnia 2018 https://www.npr.org/programs/wesat/features/2001/sealand/081101.sealand.html)

[997] zob. *Sealand Internet Law,* czyli sealandzka "ustawa" regulująca prawa i obowiązki podmiotów działających w cyberprzestrzeni a deklaratywnie podległych jurysdykcji Sealandii. Zakazywała ona podmiotom zlokalizowanym na Sealnadii wyłącznie najcięższych *malum per se,* pozwalając na przechowywanie na własnych serwerach

projekt *HavenCo*, nie powiódł się,[998] to jednak z punktu widzenia prawa międzynarodowego stanowi on interesujący precedens. Fiasko *HavenCo* nie wynikało bowiem z interwencji jakiegokolwiek państwa czy organizacji międzynarodowej na Sealandii, a z zakazów, które państwa nakładały na poddane własnej jurysdykcji podmioty.[999] Dodatkowo należy zauważyć, że Sealandia pozostaje mikronacją, która utrzymuje wiele aspektów państwowości, w szczególności emituje walutę, używa swojej flagi i godła na arenie międzynarodowej, jak i dąży do uzyskania uznania międzynarodowego dla własnej jurysdykcji.[1000] Powołuje się także na uzyskanie niepodległości zgodnie z teorią deklaratywnego uznania,[1001] a także na faktyczne uznanie swojej państwowości przez Zjednoczone Królestwo, kiedy podczas procesu R. Batesa, założyciela Sealandii z oskarżenia publicznego - sąd brytyjski uznał się za niewłaściwy do rozparzenia skargi, ze względu na brak jurysdykcji poza terytorium brytyjskim.[1002] Na precedens wynikający z tego orzeczenia, powołał się także rząd brytyjski wezwany przez RFN do interweniowania w sprawie obywateli niemieckich, uwięzionych na platformie[1003] podczas tzw. *Incydentu Achenbacha*[1004] czyli próby "przewrotu rządowego" na Sealandii. Wobec bierności rządu brytyjskiego, rząd niemiecki nakazał swojemu ambasadorowi w Londynie negocjowanie uwolnienia własnych obywateli bezpośrednio na Sealandii, co zostało podniesione przez jej władze jako dalszy dowód uzyskania przez nią uznania międzynarodowego.[1005] Łatwo więc zauważyć, że kwestia suwerenności Sealandii, w wąskim zakresie poddania jej prawom części fizycznych cyberprzestrzeni na niej zlokalizowanych, w ogóle nie była przedmiotem rozważań. Łatwo więc sobie wyobrazić sobie

---

nieomal każdego rodzaju danych, w szczególności tych, które naruszałyby rozmaite traktaty międzynarodowe dotyczące ochrony praw autorskich

998 J.Grimmelmann *Death of a data haven:cypherpunks,WikiLeaks, and the world's smallest nation* "Ars Technica" 3/12 (2012) p.1

999 zob. Też Wu T. Goldsmith J. *Who controls...* ss.80

1000 S.Layock, Ch.West *Lost Countries. Exotic Tales form an old Stamp Album* The History Press (2017), roz. "Sealand" ss. 3 i n.

1001 E.Dynia *Uznanie państwa w prawie międzynarodowym. Zarys problematyki* wyd. UR (2017) ss.75 i n.

1002 Regina v. Bates(1968) *The case about Firearms Act*

1003 J. Grimmelman *Sealand, HavenCo...* par.29

1004 zob. Lehman-Taylor D. *The Plot against Prinicipality of Sealand*, Narratively (2019) s.2

1005 Lyon A.H.E. *The Principality of Sealand and Its Case for Sovereign Recognition* "Emory Intl. Law Rev." 29:3 (2015) ss.637-9

wykorzystania tak zlokalizowanej infrastruktury do przeprowadzenia dowolnej cyberoperacji. Samo istnienie tego prawa nie budzi w takiej sytuacji wątpliwości.[1006] W takiej sytuacji doszłoby więc do konfliktu podwójnie asymetrycznego (zarówno w rozumieniu prawa międzynarodowego publicznego jak i *lex informatica*). Dotyczyła by ona bowiem nie tylko operacji *per se*, ale także faktycznych możliwości odpowiedzi na owe działania zbrojne.

Ponieważ kryterium domniemanej legalności zawarte w punkcie 6 Testu Schmitta odnosi się do zasady prohibitywności prawa międzynarodowego - należy uznać za dopuszczane przeprowadzanie operacji cybernetycznych z *quasi-jurysdykcji*, choć w razie skutecznego dokonania atrybucji - mogą one powodować odpowiedzialność państwa, które za te operacje odpowiada.[1007] Przeprowadzenie operacji cybernetycznej z terytorium o nieuregulowanym statusie byłoby legalne wobec istniejącego *opinio iuris,*[1008] a więc także w rozumieniu prawa międzynarodowego publicznego. Nie stało by na przeszkodzie tej legalności nawet przeprowadzenie go przez aktora niepaństwowego. Jednak ewentualne środki obrony aktywnej mogłyby być skierowane wyłącznie przeciwko owej *quasi-jurysdykcji,* (przykładowo platformie, na której położona jest Sealandia).

[1006] zob. Rosicini *Cyber Operations...* ss.101, także zob raport wywiadu Królestwa Holandii AIV/CAVV o cyberoperacjach- *AIV/CAVV report of Cyberwarfare*, wraz z odpowiedzią rządu holenderskiego (2012) s.5

[1007] por. Art. 1 Draft Articles on Responsibility of States for Internationally Wrongful Acts, United Nations International Law Commission (2001), dalej powoływane jako *ARSIWA*

[1008] K.Ziolkowski *Ius ad bellum in Cyberspace-Some thoughts on the "Schmitt-Criteria" for Use of Force* "NATO CCD COE Pub."(2012) s.300

VI. Wnioski

Analiza powyższych faktów wskazuje, że brak przesłanek by twierdzić, że rozwój cyberprzestrzeni likwiduje suwerenność państwową czy też pozbawia państw narzędzi wykonywania swojej jurysdykcji. Dobra prawne chronione przez te instytucje pozostają niezmienne co do swojej treści aksjologicznej. Zarówno jednak suwerenność jak i stanowiąca jej pochodną jurysdykcja doznają znaczących zmian w swojej warstwie technicznej. Wynika ona ze specyfiki prawnej i faktycznej cyberprzestrzeni. Po pierwsze, sama cyberprzestrzeń jest zjawiskiem bez precedensu - ze względu na połączenie elementów fizycznych i niefizycznych. Po drugie, specyficzne cechy cyberprzestrzeni jak jej wszechobecność czy niemożliwość fizycznego zlokalizowania zmieniają znacząco środowisko, w którym wykonywane są normy prawa międzynarodowego publicznego - redefiniując ich *ratio legis,* a w konsekwencji same te normy. Po trzecie, fakt uznania cyberprzestrzeni za *quasi*-miejsce oznacza rewizję pojmowania zasady terytorialności jak i konieczność wykonywania suwerenności na wielu polach. Jej ostateczne istnienie będzie bowiem uzależnione od skutecznego istnienia suwerenności opartej o różne podstawy: (1) suwerenności terytorialnej (w świecie fizycznym - wobec fizycznej części infrastruktury), (2) suwerennośći funkcjonalno-terytorialnej (w informatycznej części cyberprzestrzeni stanowiącej *commons*), (3) suwerenności funkcjonalnej (w "cyberterytoriach" istniejących w informatycznej części cyberprzestrzeni) oraz (4) zdolności do ochrony własnej suwerenności przed naruszeniami na trzech wcześniej wskazanych polach. Cybersuwerenność danego państwa będzie funkcją wszystkich tych czterech elementów.

Wobec znaczących odrębności faktycznych cyberprzestrzeni konieczne staje się skonstruowanie odrębnego systemu prawnego uwzględniającego jej specyfikę i stanowiącego w tym zakresie uzupełnienie prawa międzynarodowego publicznego. Takim systemem prawnym staje się *lex informatica.* System ten pozwala uwzględnić

naturę cyberprzestrzeni ze względu na normowanie faktyczne inferujące normy prawne z afordancji kodu tworzącego cyberprzestrzeń i w konsekwencji - mających te same cechy. To z kolei umożliwia normowanie cyberprzestrzeni, a więc także wykonywanie jurysdykcji i istnienie suwerenności Jednocześnie *lex informatica* pozwala na wywieranie na afordancje wpływu przez normy prawa międzynarodowego publicznego i praw stanowionych w ramach jurysdykcji krajowych. *Lex informatica* stanowi więc swoisty pomost pomiędzy systemami normatywnymi obowiązującymi w cyberprzestrzeni i w świecie rzeczywistym, pozwalając na wzajemne normowanie tych systemów - pomimo ich niewspółmożliwości faktycznej.

Wzajemne powiązania *lex informatica* i prawa międzynarodowego publicznego będą stanowić podstawę dla zrozumienia funkcjonowania podstawowych dla tego ostatniego instytucji w cyberprzestrzeni - a więc także suwerenności i jurysdykcji. Należy przede wszystkim zauważyć, że suwerenność danego państwa ma w cyberprzestrzeni wiele wymiarów. Po pierwsze, państwa muszą liczyć się z ograniczeniami własnej (także istniejącej w świecie fizycznym) suwerenności wynikającymi z samego istnienia cyberprzestrzeni. Ograniczenia te wynikają z możliwości wpływu cyberprzestrzeni (a tym samym pozostałych podmiotów w niej aktywnych) na nieomal każdy element funkcjonowania współczesnego państwa. Ponieważ informatyczna część cyberprzestrzeni co do zasady stanowi *res communis omnium* - ograniczenia te mają swoje źródło poza jurysdykcją państw. Po drugie, państwa muszą chronić własną suwerenność fizyczną i informatyczną przed tymi naruszeniami poprzez sprawowanie kontroli nad własnymi sieciami komputerowymi i infrastrukturą stanowiącą elementy fizycznej części cyberprzestrzeni. Po trzecie, państwa nabywają prawa i obowiązki wynikające z suwerenności nad swoimi ”terytoriami” cyfrowymi (funkcjonującymi wyłącznie w informatycznej części cyberprzestrzeni), przez które faktycznie zyskują nowe pole dla jej wykonywania. Czwartym i ostatnim aspektem staje się utrata przez państwo monopolu na sprawowanie *imperium* we wszystkich elementach suwerenności, na które ma wpływ cyberprzestrzeń. Osłabienie tej władzy wynika oczywiście z

konstrukcji *lex informatica.* Jest ono jednocześnie prawem (spełniającym kryteria Fullera) jak i sposobem faktycznego wywierania wpływu na konstrukcję kodu cyberprzestrzeni. Ta ostatnia właściwość jest też przyczyną jego specyficznej multicentryczności. Afordancje tworzone są w drodze normowania faktycznego - nie sposób więc wskazać przymiotu monopolu normatywnego po stronie któregokolwiek z podmiotów, które je tworzą. Wobec tych przesłanek należy więc uznać, że owo ograniczenie znaczenia *imperium* państwowego ma także znaczenie teoretycznoprawne - nie zaś wyłącznie faktyczne. Przy podejmowaniu własnych decyzji sekurytyzacyjnych państwa muszą brać pod uwagę zarówno samą konstrukcję *lex informatica* jak i korelacje z prawem międzynarodowym publicznym i wynikające z nich metarnomy. Tylko bowiem w tej drodze możliwe jest wykonywanie suwerenności w trzech wspomnianych powyżej zakresach.

Ze względu na brak możliwości fizycznego zlokalizowania cyberprzestrzeni - traci także na znaczeniu zasada terytorialności. Nie sposób twierdzić, że suwerenność państwa w cyberprzestrzeni może być wyłączną władzą nad określonym terytorium. Brak bowiem możliwości wykreślenia w jej informatycznej części jakiegokolwiek terytorium a rozgraniczanie cyfrowych *quasi*-terytoriów odbywa się w drodze konstrukcji granic funkcjonalnych, w żaden sposób niepowiązanych z terytoriami w świecie fizycznym. Terytorialność nie zostaje jednak zlikwidowana całkowicie - opiera się bowiem o nią władza wykonywana przez państwa i tradycyjne podmioty prawa międzynarodowego wobec części fizycznej cyberprzestrzeni (w którym to zakresie państwa utrzymują w pełni własne *imperium*) jak i wobec ”terytoriów” cyfrowych (choć wyłącznie pośrednio - jako aspekt wykonywania opartej o terytorialność suwerenności wobec elementów fizycznej części).

Suwerenność tradycyjnie rozumiana oznacza przede wszystkim monopol na wykonywanie władzy na określonym terytorium (w sensie pozytywnym) i nie podleganiu wpływom innych podmiotów (w sensie negatywnym). Suwerenność pozytywna staje się w cyberprzestrzeni monopolem na wykonywanie określonych interesów państwowych (zgodnych jednak z zakresem tradycyjnie utożsamianym w doktrynie z suwerennością). Negatywnie pojmowaną suwerenność w części

informatycznej cyberprzestrzeni należy (podobnie jak w przypadku tradycyjnie pojmowanej suwerenności) uznać za wolność od wpływów obcych - jednak nie tyle w stosunku do jakiegoś określonego terytorium, co wobec zespołu interesów, wyznaczanego przez afordancje *lex informatica* i chronionego przez granice funkcjonalne. Utrzymanie określonego kształtu tych ostatnich stanowi więc materializację interesów państwa - podobnie jak ma to miejsce z terytorium w świecie fizycznym. Szczególnym wypadkiem takiej konstrukcji są suwerenne ”cyberterytoria”. Po pierwsze są one „terytoriami” w taki sposób, w jaki cyberprzestrzeń stanowi miejsce. Stosują się więc do niej odpowiednio normy regulujące terytorialność w prawie międzynarodowym publicznym. Po drugie, ze względu na konieczność oparcia takich stref o infrastrukturę fizyczną zlokalizowaną wyłącznie na terytorium państwa stanowią element ich tradycyjnej suwerenności. Wobec tego muszą być one normowane przez *lex informatica.* W konsekwencji przenoszą więc suwerenność w cyberprzestrzeni do domeny metanorm tego ostatniego. To z kolei oznacza, że naruszenie suwerenności cyberprzestrzennej jest tożsame z naruszeniem tradycyjnej suwerenności państwowej. Z prawnego więc punktu widzenia zarówno ”terytoria” cyfrowe jak i funkcjonujące w *commons* zespoły afordancji, tworzone w ramach wykonywania delimitowanych funkcjonalnie interesów - stanowią przejawy suwerenności państwowej.

Wobec zmian w pojmowaniu suwerenności, redefinicji musi także ulec (stanowiąca praktyczne zastosowanie suwerenności) jurysdykcja państwowa. Podstawową zmianą w stosunku do tradycyjnego obrotu międzynarodowoprawnego jest fakt, że podstawowym środkiem wykonywania jurysdykcji w cyberprzestrzeni staje się jurysdykcja nadzwyczajna. Jedynym wyjątkiem od tej zasady jest zastosowanie jurysdykcji zwyczajnej do wykonywania zadań tradycyjnie wiązanych z wykonywaniem suwerenności we własnych „terytoriach” cyberprzestrzennych. Przykładem takiego działania może być opisywana w niniejszej rozprawie instytucja estońskiej e-rezydencji. W zakresie przeciwdziałania naruszeniom suwerenności i egzekwowania własnych norm przez państwo - jurysdykcja zwyczajna (tradycyjnie wykonywana na określonym terytorium i wobec osób posiadających obywatelstwo

danego państwa) staje się w odniesieniu do cyberprzestrzeni wyłącznie subsydiarna. Jest ona bowiem skuteczna wyłącznie w odniesieniu fizycznej części cyberprzestrzeni zlokalizowanej terytorialnie. Dodatkowo, może być przez państwa wykorzystywana do pośredniego wywierania wpływu na normy *lex informatica* - poprzez normowania części źródeł afordancji, takich jak podmioty *ISP czy* standardy przepływu danych i w ten sposób używana do budowania narzędzi ochrony własnej suwerenności. Co do zasady więc jurysdykcja zwyczajna może być stosowana dla przeciwdziałania naruszeniom suwerenności w cyberprzestrzeni. W tym zakresie może być ona jednak stosowana wyłącznie w jej aspekcie preskryptywnym i to w zakresie opisanym powyżej. Jedynym bezpośrednim sposobem wykonywania jurysdykcji zwyczajnej w informatycznej części cyberprzestrzeni jest bowiem tworzenie suwerennych cyberterytoriów, jak opisano to powyżej na przykładzie Estonii. Państwa muszą jednak przeciwdziałać naruszeniom własnej suwerenności przede wszystkim przy pomocy jurysdykcji nadzwyczajnej. Wszystkie bowiem naruszenia tej ostatniej będą pochodzić z niepodlegającej lokalizacji cyberprzestrzeni w jej stanowiącej *commons* części informatycznej a zdecydowana część ewentualnych naruszeń nie będzie możliwa do fizycznego zlokalizowania nawet po osiągnięciu przez takie naruszenia pożądanych skutków. Nie będą więc miały też zastosowania koncepcje jurysdykcji oparte o terytorialność. Skuteczną ochronę suwerenności państwa mogą uzyskać wyłącznie w drodze wykonywania jurysdykcji nadzwyczajnej w oparciu o koncepcje chroniące właśnie interesy wynikające z suwerenności państwowej a nie terytorium (jak na przykład doktryna skutku). Naruszenia suwerenności dokonywane w cyberprzestrzeni zawsze będą dokonywane w jej informatycznej części i tylko środki w niej stosowane pozwalają państwom na ich uniknięcie. *De facto*, będą więc one zawsze naruszeniami zewnętrznymi (nawet jeżeli podmiot je przeprowadzający będzie znajdował się fizycznie na terytorium państwa, którego suwerenność zamierza naruszyć) i zawsze będą naruszać granicę funkcjonalną suwerenności danego państwa.

Kwestia samych naruszeń suwerenności jest w cyberprzestrzeni także niezmiernie skomplikowana. Przede wszystkim działania takie mogą mieć skutek wyłącznie w

cyberprzestrzeni, lub także w świecie fizycznym. W oczywisty sposób będzie to prowadzić do zróżnicowania systemu prawnego regulującego je. Naruszenia wywołujące skutki w świecie fizycznym - ataki mieszane wsparte przez działania cyberprzestrzenne czy też ataki cyberprzestrzenne mające ekwiwalent kinetyczny - wywołają skutki prawne zarówno w *lex informatica* jak i w prawie międzynarodowym (w tym odpowiednio stosowanym prawie konfliktów zbrojnych). W przypadku ataków niekinetycznych i operacji nie wywołujących skutków fizycznych, bezpośrednie skutki prawne będą ograniczone do *lex informatica,* a ewentualne skutki wywołane pośrednio w prawie międzynarodowym publicznym (jak na przykład wynikające z reżimu odpowiedzialności za czyny międzynarodowo zabronione) będą wynikać z naruszeń zasad nieinterwencji lub nieintereferencji. W praktyce jednak, ze względu na praktyczny brak możliwości dokonania atrybucji działań cyberprzestrzennych nie mających ekwiwalencji kinetycznej - zarówno odpowiedzialność za nie jak i środki zapobiegania im będą ograniczone do *lex informatica*. Cechą wspólną wszystkich operacji cyberprzestrzennych mających na celu naruszenie suwerenności państwa trzeciego jest brak możliwości ich rozróżnienia w sposób inny niż analiza ich skutków. Operacje nie tylko niekinetyczne, ale w nawet planowane i przeprowadzane poniżej poziomu użycia siły mogą potencjalnie uzyskać skutek najdalej idący. Cecha ta czyni opisane operacje niezwykle znaczącym zagrożeniem dla suwerenności, zagrożeniem często większym niż cybernetyczne ataki kinetyczne. Te ostatnie, chociaż faktycznie najgroźniejsze, są jednak regulowane przez prawo konfliktów zbrojnych. Jest więc jasne, że stanowią istotne naruszenie porządku prawnomiędzynarodowego, powodują reakcję społeczności międzynarodowej, a państwo będące celem takiej operacji może wykonywać prawo do obrony, w tym nawet obrony przy pomocy konwencjonalnych sił wojskowych.

Tymczasem operacje niekinetyczne i poniżej poziomu użycia siły pozostają w luce prawnej. W połączeniu z zasadą prohibitywności prawa międzynarodowego a także rozmaitymi regulacjami niuansującymi użycie siły o niskim stopniu intensywności (jak na przykład wynikającemu z *Nicaragua* progowi *border clashes*) operacje te są w zasadzie nienormowane a próg odpowiedzialności niejasno ustalony. W przypadku

operacji w świecie fizycznym rozróżnienia te są niewątpliwie uzasadnione. W cyberprzestrzeni jednak podobna operacja może mieć dowolną intensywność a dokonanie rozróżnienia niemożliwe na jakimkolwiek etapie operacji poza ostatnim. Dochodzi więc do istotnego ograniczenia prawa do obrony po stronie celów operacji cyberprzestrzennych na tym poziomie. Najbardziej oczywistym i bezdyskusyjnym w sensie prawnym środkiem obrony jest obrona pasywna i stosowanie *detterence - by - denial*. Niewątpliwie nie jest ona jednak wystarczająca. Konieczne jest więc rozszerzenie prawa do obrony suwerenności przed naruszeniami przy pomocy doktryny domniemania ograniczonej do odpowiedzi niekinetycznej (stanowiącej kompromis pomiędzy gwarantowaniem skutecznej obrony i unikaniem nadmiernej eskalacji konfliktu oraz nieproporcjonalności odpowiedzi) i *de lege ferenda* ugruntowanie tej instytucji w doktrynie prawa cyberprzestrzeni.

Wszechobecność cyberprzestrzeni w związku z normowaniem faktycznym ma jeszcze jeden istotny aspekt dla suwerenności państwowej. Wpływ na *lex informatica* mogą wywierać liczne podmioty nie będące tradycyjnymi podmiotami prawa międzynarodowego publicznego. Pierwszą grupę takich podmiotów stanowią *non-state actors*. Ponieważ ich wpływ na normowanie faktyczne jest porównywalny z tymi, które mają państwa - ich możliwości projekcji siły zmniejszają proporcjonalnie potencjał normowania cyberprzestrzeni przez państwa. Dodatkowo ponieważ operacje cyberprzestrzenne prowadzone przez aktorów niepaństwowych nie tylko muszą zostać atrybuowane, ale także (dla skuteczności remediów) przypisane państwu - tworzenie grup hakerskich stosowanych później jako *non-state actors* stanowi narzędzie stosunkowo łatwego naruszania praw państw trzecich, znacząco utrudniając odpowiedź i stosowanie remediów. Drugą grupą są ponadnarodowe organizacje mające bezpośredni wpływ techniczny na cyberprzestrzeń, jak *IANA* czy *ICANN*. Pomimo, że w istocie są podmiotami prawa prywatnego - ze względu na swoją faktyczną rolę odgrywaną w tworzeniu i utrzymywaniu globalnych sieci komputerowych zyskują status *sui generis* organizacji międzynarodowych. Państwa jednakże nie mają możliwości wpływu na te podmioty - pozostające nawet poza ich jurysdykcjami nadzwyczajnymi - w drodze innych działań niż tworzenie afordancji.

Ponieważ organizacje te najczęściej kontrolują podstawy kodu - jak kontrola *ICANN* nad protokołami *IP* czy *DNS* - stosowanie przez państwa *lex informatica* do wykonywania własnych polityk w stosunku do tych podmiotów napotyka na istotne trudności faktyczne, jak ma to miejsce w sporze UE z *ICANN* o stosowanie norm *GDPR.*

Utrzymanie przez państwa suwerenności w cyberprzestrzeni wymaga więc przede wszystkim stosowania przez nie własnej jurysdykcji w sposób, który pozwala wpływać na *lex informatica* w sposób gwarantujący im tworzenie afordancji chroniących ich granice funkcjonalne. Bowiem to właśnie *lex informatica* i podjęte w niej decyzje sekurytyzacyjne (jako działające w czasie rzeczywistym - w odróżnieniu od norm prawa międzynarodowego) stanowią podstawowy środek zarówno obrony jak i wykonywania suwerenności.

Nie ma też wątpliwości, że wraz rozwojem technologii stosowanych w cyberprzestrzeni zwiększać się będzie zakres, w którym wykonywanie suwerenności w informatycznej części cyberprzestrzeni będzie kluczowe dla państw. Należy jednak zauważyć, że regulacje prawne dotyczące *stricte* takich elementów jak granice funkcjonalne, *leges speciales* określające zasady odpowiedniego stosowania zasady terytorialności do informatycznych ‘terytoriów’ i ich naruszeń wymagają *de lege ferenda* szybkiej kodyfikacji. Brak bowiem możliwości określenia ich w drodze praktyki cyberprzestrzennej ze względu na konflikty interesów poszczególnych państw. Nadto, ze względu na konieczność utworzenia podobnych norm nie tylko w *lex informatica*, lecz także w prawie międzynarodowym publicznym - konieczne byłoby nie tylko określenie praktyki, ale także *opinio iuris*. W związku z tym, za znaczenie skuteczniejsze należałoby uznać uregulowanie wspomnianych kwestii w drodze *black-letter law*. Ponieważ traktaty międzynarodowe nie odegrały dotychczas istotnej roli w tworzeniu prawa cyberprzestrzeni - zasadny wydaje się pogląd, według którego regulacje takie winny powstać w drodze ponadnarodowych kodyfikacji. Swoistą próbą stworzenia takowej jest *Tallinn Manual* i *Tallinn Manual 2.0*. Próbę tę należy niewątpliwie ocenić pozytywnie. *Tallinn Manual* jest jednak dokumentem niewiążącym prawnie - wynikiem prac doktryny nie mającej żadnego umocowania

prawnego. O ile regulacje te mogą stać się podstawą dla stworzenia prawa zwyczajowego - ze względu na powiązanie IGoE z Sojuszem Północnoatlantyckim, niewątpliwie postanowienia te byłyby kwestionowane przez część państw, co znacząco utrudniałoby określenie *opinio iuris* (które dla takich norm - jako funkcjonujących także w *ius gentium* - byłoby wymagane). *De lege ferenda* powinno się więc postulować stworzenie odpowiednich regulacji przez podmioty mające szerokie uznanie międzynarodowe, jak na przykład Komisja Prawa Międzynarodowego Narodów Zjednoczonych. Szczególnie istotne wydaje się powstanie regulacji dotyczących ”terytorialnych” stref informatycznej cyberprzestrzeni. Pozwalałyby one na skuteczne unormowanie tego kluczowego dla suwerenności państw elementu jej prawa a także poddanie naruszeń tychże kontroli sądowej. Kontrola taka - choć oparta o *lex informatica* i zasadę *ex aequo et bono* - skutkowałaby wydaniem orzeczeń skutecznych w prawie międzynarodowym publicznym, a tym samym możliwych do wyegzekwowania. Nie byłoby bowiem możliwości ominięcia ich w ramach *cyberlawfare* czy normowania faktycznego. Stworzenie podobnych metanorm pozwoliłoby na ochronę suwerenności państwowej przed najcięższymi ich naruszeniami (a więc kinetycznymi i niekinetycznymi cyberatakami) w drodze sądownictwa międzynarodowego. Brak natomiast możliwości skonstruowania środków prawnej ochrony przed naruszeniami suwerenności w drodze operacji cybernetycznych poniżej poziomu ataku. Stan ten wynika z utraty przez państwa kontroli nad podstawowymi elementami infrastruktury cyberprzestrzennej i w konsekwencji uniemożliwienie tworzenia afordancji w tym zakresie. Należy także pamiętać, że kontrola ta nie pozostaje nawet w dyspozycji organów czy organizacji międzynarodowych, na które państwa miałyby możliwość wywierania wpływu, a jest wyłącznie poddana podmiotom prawa prywatnego o niejasnym statusie międzynarodowym. Z formalnoprawnego punktu widzenia, pozostają one *non-state actors*, jednakże ich znaczenie faktyczne zrównuje ich znaczenie w systemie prawa narodów z organizacjami ponadnarodowymi. Także ich rola w normowanym faktycznie *lex informatica* jest równa, a w niektórych aspektach nawet bardziej doniosła niż państw. Należy także wskazać, że ewentualne kinetyczne

ataki na systemy należące do tych podmiotów, jako pozbawionych własnej suwerenności, oznacza naruszenie suwerenności państwa, w którym elementy tej infrastruktury są fizycznie zlokalizowane, co stanowi znaczące rozszerzenie odpowiedzialności państw, na terytoriach których elementy te są zlokalizowane.

Innym, równie istotnym, czynnikiem osłabiającym możliwość ochrony suwerenności w cyberprzestrzeni jest łatwość z jaką suwerenność ta może być naruszana przez operacje cyberprzestrzenne. Ataki mające ekwiwalencję kinetyczną, jako podlegające prawu konfliktów zbrojnych, uruchamiają gwarantowane przez nie prawo do samoobrony i podlegają sankcjom międzynarodowym. Jednak zarówno cybernetyczne ataki niekinetyczne i operacje poniżej poziomu ataku pozostają częstokroć regulowane w przeważającej części przez *lex informatica*. Oznacza to praktyczne (wobec takich naruszeń) wyłączenie możliwości obrony kinetycznej - mogącej stanowić akt agresji na państwo, które ataku nie przeprowadziło lub też odpowiedź nieproporcjonalną (ze względu niemożliwość określenia realnej skali ataku niekinetycznego). Praktyka międzynarodowa wskazuje natomiast, że (pomijając obronę pasywną opartą o *detterence - by- denial*) podstawowym środkiem obrony przed każdym rodzajem naruszeń w cyberprzestrzeni są operacje niekinetyczne - stosowane w ramach teorii domniemania intensywności naruszeń. Tak pojmowana obrona cybernetyczna pozwala na skuteczną obronę granic funkcjonalnych państw bez podejmowania wspomnianego ryzyka nieproporcjonalności odpowiedzi lub nieatrybuowalności naruszeń. Będzie ona również niewrażliwa na ograniczenia wynikłe z *cyberlawfare*, jak "sztuczne" jurysdykcje czy wykorzystywanie grup hakerskich będących aktorami niepaństwowymi. *De lege ferenda*, powszechne stosowanie takich operacji wymaga jednak powstania odpowiednich regulacji w prawie międzynarodowym publicznym - w drodze podobnej do wspomnianych już regulacji terytorialnych stref cyberprzestrzeni. - ponieważ także one stanowić będą metanormy prawa cyberprzestrzeni. Dotychczasowe ich regulacje dotyczą wyłącznie wąskiego zakresu, w którym do ataków niekinetycznych stosuje się prawo konfliktów zbrojnych.

Reasumując za bezpodstawne należy więc uznać twierdzenia, że powstanie cyberprzestrzeni likwiduje suwerenność czy wręcz suwerenne państwa. Państwa mogą wykonywać swoją suwerenność także w niej. Co więcej, tradycyjna suwerenność nad własnymi terytoriami stawia je na uprzywilejowanej pozycji pośród podmiotów sprawujących normowanie faktyczne cyberprzestrzeni. Muszą jednak liczyć się z osłabieniem ich władzy *imperium* tradycyjnie wiązanej z suwerennością - wynikającej właśnie z istnienia podmiotów niepaństwowych, których działania mają także na *lex informatica* istotny (choć co do zasady mniejszy) wpływ. Jednakże utrzymanie własnej suwerenności jest możliwe wyłącznie w przypadku skutecznego wykonywania jej w stosunku do całości cyberprzestrzeni. Przede wszystkim oznacza to, że państwa muszą dostosować swoje ustawodawstwa do specyfiki cyberprzestrzeni. To z kolei implikuje zmiany w wykonywaniu jurysdykcji. Państwa muszą stanowić normy dotyczące zlokalizowanych na własnych terytoriach elementów fizycznej części cyberprzestrzeni i podmiotów *ISP* w ramach całościowych polityk sekurytyzacyjnych, gwarantujących skuteczną obronę pasywną i tworzenie afordancji chroniących ich terytorialne strefy cyberprzestrzeni. Konieczne jest także wprowadzanie zmian do sposobu wykonywania jurysdykcji nadzwyczajnej uwzględniających możliwość skutecznej obrony własnych granic funkcjonalnych w informatycznej części cyberprzestrzeni a także ochrony własnych granic terytorialnych zarówno przed cyberatakami o skutkach kinetycznych, jak też przed atakami hybrydowymi, wykorzystującymi sieciowość współczesnych konfliktów zbrojnych. Konieczne jest także współdziałanie państw w ramach obrotu prawnomiędzynarodowego, zmierzające do rozszerzenia zakresu normowania metanormami - ze szczególnym uwzględnieniem regulacji “terytoriów” cyfrowych i niekinetycznych konfliktów cyberprzestrzennych. Kwestie te, kluczowe dla wykonywania suwerenności w cyberprzestrzeni, pozostają w aktualnym stanie prawnym w specyficznej luce prawnej wobec niewystarczalności regulacji transponowanych do prawa cyberprzestrzeni z tradycyjnego prawa międzynarodowego publicznego. Dla utrzymania własnej suwerenności państwa muszą także znacząco ograniczyć wpływ podmiotów prawa prywatnego, mających

istotny wpływ na architekturę cyberprzestrzeni poprzez poddanie ich *de lege ferenda* kontroli wyspecjalizowanych organizacji międzynarodowych.

O ile więc istnienie cyberprzestrzeni znacząco redefiniuje instytucję suwerenności (przede wszystkim - odrywając ją od zasady terytorialności i likwidując jej post-westfalską interpretację), to państwa mają wystarczające narzędzia by skutecznie wykonywać i chronić własne interesy (tradycyjnie z suwerennością utożsamiane). W aktualnym stanie prawnym znacząca część tych narzędzi nie jest jednak przez państwa wykorzystywana. Muszą więc państwa poszerzyć zakres wykonywania swojej jurysdykcji w cyberprzestrzeni zarówno w jej faktycznym jak i prawnym aspekcie. Ostatecznie więc to od woli politycznej państw zależeć będzie finalny kształt cyberprzestrzeni; potencjalnie mogącej zarówno ostatecznie zlikwidować państwa narodowe jak i zagwarantować ich istnienie i znaczenie w okresie tzw. IV rewolucji technicznej.

Bibliografia

Orzecznictwo sądowe

1. *Accordance with International Law ot the Unilateral Declaration of Independence in Respect of Kosovo* (Request for Advisory Opinion), ICJ Reports 2010,141 Gen. L. 141 (2010)
2. *Accordance with International Law ot the Unilateral Declaration of Independence in Respect of Kosovo*- ICJ Reports 2010, 141 Gen. L. 141 (2010), zdanie odrębne sędziego Bruno Simmy
3. *Burger King Corp. v. Rudzewicz* 471 U.S. 462, 105 S. Ct.2174 (1985)
4. *Carfano v. Metrosplash.com Inc* 339 F.3d 1119, (2003)
5. *Case Concerning Ius ad Bellum* Ethiopia-Eritreia Claims Commission, tom. XXVI ss. 457-469(2005).
6. *Case Concerning application of the Convention on the prevention and Punishment of Crime of Genocide*, I.C.J reports 1993, 325, 440;95 ILR 43, 158
7. *Case Concerning application of the Convention on the prevention and Punishment of Crime of Genocide*, I.C.J Reports 1993, 325, 440;95 ILR 43, 158, Zdanie odrębnego sędziego E. Lauterpachta
8. *Case Concerning Corfu Channel* I.C.J. Reports 1949, 244, Gen L No. 1
9. *Case Concerning East Timor* I.C.J Reports 1995, 90 Gen. L. No.84
10. *Case Concerning Military and Paramilitary Activities in and Against Nicaragua,* ICJ Reports 1986 (Merits) ,
11. *Case Concerning Military and Paramilitary Activities in and Against Nicaragua, Nicaragua v United States*, Merits, , (1986) I.C.J Reports 14, ICGJ 112 (ICJ 1986), OXIO 88, 27th June 1986, United Nations [UN]; International Court of Justice [ICJ]1986) ICJ Rep 14 ICGJ 112 (ICJ 1986)
12. *Case Concerning Military and Paramilitary Activities in and Against Nicaragua,*

Nicaragua v United States, Jugdment, , (1986) ICJ Rep 14, ICGJ 112 (ICJ 1986), OXIO 88, 27th June 1986, United Nations [UN]; International Court of Justice [ICJ]1986) ICJ Rep 14

13. *Case Concerning Military and Paramilitary Activities in and Against Nicaragua, Nicaragua v United States*, Jugdment, , (1986) ICJ Rep 14, ICGJ 112 (ICJ 1986), OXIO 88, 27th June 1986, United Nations [UN]; International Court of Justice [ICJ]1986) ICJ Rep 14 (1986) , zdanie odrębne sędziego Stephena Schwebela
14. *Case Concerning Oil Platforms* (Islamic Republic of Iran v. United States of America, International Court of Justice (ICJ), I.C.J Reports 2003 (2003)
15. *Case Concerning Oil Platforms,* I.C.J. Reports No.90 (161) (2003)
16. *Case Concerning Oil Platforms,* I.C.J. Reports No.90 (161) (2003) zdanie odrębne sędziego B. Simmy
17. *Case Concerning Oil Platforms,* I.C.J. Reports No.90 (161) (2003), zdanie odrębne sędzi Higgins
18. *Case Concerning Oil Platforms,* I.C.J. Reports No.90 (161) (2003), Memorandum Rep. Iranu
19. *Case Concerning Oil Platforms,* I.C.J. Reports No.90 (161) (2003), Awards
20. *Case Concerning the Corfu Channel*, Merits, ICJ Reports 1949 4, 35 (1949)
21. *Case Concerning Island of Palmas* STSM, 2 AIAA 829 (1928), UN Reports of International Arbitral Awards (2006)
22. *Case Concerning the difference between France and New Zealand,France-New Zealand* Arbitration Tribunal, 82 I.L.R. 500 (1990).
23. *Case concerning the difference between New Zealand and France concerning the interpretation or application of two agreements concluded on 9 July 1986 between the two States and which related to the problems arising from the Rainbow Warrior Affair.* United Nations Reports of International Arbitral Awards t. XX, 215-84(1990)
24. *Case concerning the Gabcikovo-Nagymaros Project* , I.C.J Reports 88, ICJ GL No. 92 (1997)

25. *Dow Jones Company Inc. v. Joseph Gutnick*, Supreme Court of Australia HCA 56, 210, CLR 575,194 ALR 433,77 (2002)
26. *First National Bank of Boston v. Belotti* 435 U.S. 765 98 S. Ct. 1407 (1978),
27. *Gencor Ltd v. Commission of the E.C.*, ECLI:EU:T 1999:65 (1995)
28. *ICANN v. EPAG* Sąd Rejonowy w Bonn syg. 10 O 171/18 (2018)
29. *ICANN v. EPAG* Wyższy Sąd Kolonii syg. 19 W 32/18 (2018)
30. *International Military Tribunal (Nuremberg) v. Streicher*, IMT Part. 22 (1946)
31. *Island of Palmas case (Netherlands v. USA)* Permanent Court of Arbitration, Award, II RIAA 829(1928)
32. *Jaloud v. Holandia*, Europejski Trybunał Praw Człowieka,Wielka Izba ETPcz, 47708/08 (2008)
33. *Julius Baer & Co. Ltd and Julius Baer Bank and Trust Co. Ltd v. Wikileaks, Wikileak org and Dynadot LLC* 535 F. Supp 2d 980 (2008)
34. *Julius Baer & Co. Ltd and Julius Baer Bank and Trust Co. Ltd v. Wikileaks, Wikileak org and Dynadot LLC* 535 F. Supp 2d 980 (2008) - zarządzenie sędziego, syg. CV08-0824 (2008)
35. *Julius Baer & Co. Ltd and Julius Baer Bank and Trust Co. Ltd v. Wikileaks, Wikileak org and Dynadot* Brief of Amici Curiae (2008)
36. *Legal Status of Eastern Greenland (Norway v. Denmark)*, PCIJ (1933) PCIJ Ser. A/B n.53,71
37. *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion*, ICJ Rep 1996 226 (1996)
38. *Michelangelo Delfino, et al .v. Agilent Tech.Inc*., 145 Cal. App 4th 790, H028993(2006)
39. *North Continental Shelf Case*, ICJ Reports 4, (1969), Zdanie odrębne sędziego Padilla Nervo
40. *North Continental Shelf Case*, ICJ Reports 4, (1969),Zdanie odrębne sędziego Tanaki
41. *North Continental Shelf Case*, Merits ICJ Reports 4, (1969)

42. *Nuclear Tests Case* (Australia & New Zealand v. France), I.C.J Reports 253,457 (1974)
43. *Nuclear Tests Case (Australia v. France*) I.C.J. Reports 1974, p. 253; General List No. 58 (1974)
44. *Nuclear Tests, New Zealand v France*, , I.C.J Rep 457, ICGJ 137 (ICJ 1974), (1974), Jugdment
45. *Nuclear Tests, New Zealand v France*, I.C.J Rep 457, ICGJ 137 (ICJ 1974), (1974),Admissibility,
46. Opinia Rzecznika Generalnego Europejskiego Trybunału Sprawiedliwości Marco Darmona w sprawach połączonych 89,104,114 (1988)
47. *Pelly v. Royal Exchange Assurance Co.* (1757), Burrow's Reports 341,347, 97 ER 342 (1757), Lord's Manfield Opinion
48. *People v. Blume*, 505 N.W 2d 843,443 Mich. 476 (1993)
49. *Prosecutor v. Fatmir Limaj,Haradin Bala, Isak Musliu*, Międzynarodowy Trybunał Karny ds. Byłej Jugosławii IT-03-66, (2005), Judgement
50. *Prosecutor v. Naletilić & Martinović,* Międzynarodowy Trybunał Karny do spraw Byłej Jugosławii IT-98-34-T, (2003)
51. *Prosecutor v. Tadić*, Międzynarodowy Trybunał Karny do spraw Byłej Jugosławii,IT-94-1-A (1999)
52. *Regina v. Paddy Roy Bates and Michael Roy Bates,*(1968), także jako *Firearms Act Case.*
53. *Reno et al. v. ACLU et al.* 521 U.S. 844, 117 S.Ct.2329, US L. 4037 (1997)
54. *Shaffer v. Heitner* , 433 U.S. 186, 97 S. Ct. 2569 (1977)
55. *Smith v. United States* 113 S. Ct. 2050; 124 L. Ed 2d 138(1993),
56. *Texas v. Johnson* 491 U.S. 397, 109 S. Ct. 2533(1989)
57. *The Case of S/S Lotus* PCIJ Ser. A, nr 1018, Publications of the Permanent Court of International Justice ser. A no. 10 (1927)
58. *The Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory*, Advisory Opinion, ICJ Reports 136, ICJ GL No. 131

(2004)

59. *Trail Smelter Case* (USA, Canada), Reports of International Arbitral Awards, United Nations, t.3919 (2006)
60. *UEJF et L.I.C.R.A. v. Yahoo! Fr. et Yahoo! Inc*., Tribunal de Grande Instance, RG 05308 (2000)
61. *UEJF et L.I.C.R.A. v. Yahoo! Fr. et Yahoo! Inc*., Tribunal de Grande Instance, RG 05308 (2000) Nakaz *interim* wydany przez Trybunał Wielkiej Instancji w sprawie L.I.C.R.A&U.E.J.F. v. Yahoo Inc & Yahoo Fr.z dnia 22 maja 2000 roku .
62. *UEJF et L.I.C.R.A. v. Yahoo! Fr. et Yahoo! Inc*., Tribunal de Grande Instance, RG 05308 (2000) Nakaz *interim* wydany przez Trybunał Wielkiej Instancji w sprawie L.I.C.R.A&U.E.J.F. v. Yahoo Inc & Yahoo Fr z dnia 11 listopada 2000 roku.
63. *United Nations Secretary General: Ruling on the Rainbow Warrior Affair Between France and New Zealand* 26 ILM 1346(1986)
64. *United Nations Secretary General: Ruling on the Rainbow Warrior Affair Between France and New Zealand* 26 ILM 1346(1986), Memorandum rządu Nowej Zelandii do Sekretarza Generalnego Organizacji Narodów Zjednoczonych ILM 1350
65. *United Nations Secretary General: Ruling on the Rainbow Warrior Affair Between France and New Zealand* 26 ILM 1346(1986), Memorandum rządu Francji do Sekretarza Generalnego Organizacji Narodów Zjednoczonych ILM 1350
66. *United States v. Microsoft Corp.* 15 F. Supp 3d 466 (2014)
67. *United States v. Microsoft Corp.* 15 F. Supp 3d 466 (2014), *In re Warrant to Search a Certail E-Mail Account Controlled and Maintained by Microsoft Corp*. 829 F. 3ed. 197, par. 222. (2018)
68. *United States v. Microsoft Corp.*No. 17-2 584 U.S. (2018)
69. *United States v. Aluminium Co. Of America*, 148 F 2d 416 (1945)

70. *USA v. Microsoft Corp.*, Supreme Court of United States, 584 U.S. (2018) (2017/18).

71. Yahoo! Inc. v. L.I.C.R.A, 169 F. Supp. 2d 1181, 1194, Northern District of California (2001), także jako *Yahoo II*

72. Yahoo! Inc. v. L.I.C.R.A., 145 F. Supp 2d 1168,1171 Northern District of California (2001), także jako. *Yahoo I*

73. Manhattan Community Access Corp. et al. v. Deedee Halleck et al. No. 17-1702 587 U.S. (2019)

74. *Manhattan Community Access Corp. et al. v. Deedee Halleck et al.* 882 F. 3d 300 (2019)

Monografie

1. Asscher, L. *'Code' as Law. Using Fuller to Assess Code Rule*, Asser Press (2012)
2. Austin J. *The Province of Jurisprudence Determined,* Hackett Publishing (1832/ 1998)
3. Barrett M., Berford D., Skinner E., Vergles E .*Assured Access to the Global Commons, Supreme Allied Command Transformation* North Atlantic Treaty Organization, Norfolk (2011)
4. Baslar K. *The Concept of the Common Heritage of Mankind in International Law* Martinus Nijhoff Publishers (1998)
5. Bencsáth B.,Pék G.,Buttyán L., Félegyházi M. *DuQu: A Stuxnet like malware found in the wild CrySyS* Laboratory of Cryptography and System Security, Budapest University of Economics and Technology Press (2011)
6. Benhabib S. *Another Cosmopolitanism* Oxford University Press (2006)
7. Biegel B. *Beyond Our Control? Confronting the Limits of our Legal System in the Age of Cyberspace* MIT Press, Boston (2001)
8. Buchan R. *Cyber Espionage and International Law* Bloomsbury Publishing PLC (2019)
9. Buksiński T. *Monocentrism and Multicentrism as Legal Theories in the Global Era* Archiwum Filozofii Prawa i Filozofii Społecznej, Wydawnictwo Uniwersytetu Adama Mickewicza (2015)
10. Camilieri J., Falk J. *End of Sovereignty? The Politics of Shrinking and Fragmenting World* Edward Elgar Publishers (1992)
11. Carlson J., Yeomans N.-Whither *Goeth the Law - Humanity or Barbarity, The Way Out - Radical alternatives in Australia*, Smith and Crossley ed. Melbourne Lansdowne Press (1975)
12. Cartwright J.E. Joint Terminology for Cyberspace Operations Memorandum of Chiefs of Military Services Commanders of the Combatant Commands, Directors of The Joint Staff Directorate (2010)
13. Cena F.,Rapp A., Marcengo A., Brizio A., Hilviu D., Tirassa M. *The Role of Affordance in Cyber-Physical Systems for Behavioral Change*, Internet of Things - User-Centric IoT, Springer (2014),

14. Cox R.W. *Approaches to World Order*, Cambridge University Press(1989)
15. Crawford J. *The International Law Commissions Articles on States Responsibility- Introduction, Text and Commentaries* Cambridge University Press (2002)
16. Czaputowicz J. *Suwerenność* Polski Instytut Spraw Międzynarodowych (2013)
17. DeNardis L. *Protocol Politics:The globalization of Internet Governance* Massachusets Institute of Technology Press, 1st edition (2009)
18. Denza E. *Diplomatic Law* Oxford University Press 3rd ed. (2008)
19. Dinniss H.H. *CyberWarfare and the Laws of War* Swedish National Defence College, International Law Centre (2012)
20. Dinstein Y.*War, Aggression and Self-Defence* Cambridge University Press 3:184 (2003)
21. Dobrzeniecki K. *Lex informatica* wyd. "Dom Organizatora", (2008)
22. Dumieński Z. *Microstates as Modern Protected States:Towards a New Definition of Micro-Statethood* Centre for Small States Studies, Institute of International Affairs of Univeristy of Iceland (2014)
23. Dunlap Ch. J.- *Law and Military Interventions: Preserving Humanitarian Values in 21st Conlifcts*- Humanitarian Challenges in Military Intervention Conference, Carr Center for Human Rights Policy, Kennedy School of Government Harvard University, Washington D.C. (2001)
24. Durkheim E. *Zasady Metody Socjologicznej* Biblioteka Socjologiczna PWN (2016)
25. Dynia E. *Uznanie państwa w prawie międzynarodowym. Zarys problematyki* Wyd. Uniwersytetu Rzeszowskiego (2017)
26. Egan B. *International Law and Stability in Cyberspace* U.S Departament of Justice (2011)
27. Ehlert M. *I2P Usability vs. Tor Usability. A Bandwith and Latency Comparison* Humboldt Universitaet Berlin(2011)
28. Ehrlich E. *Grundlegung der Soziologie der Recht* Dunker & Humboldt Verlag (1913)
29. Ehrlich L. *Prawo międzynarodowe* Wydawnictwo Prawnicze, wyd.4 (1958)
30. Elcin M. *Lex Mercatoria in Interational Arbiration. Theory and Practice*, European University Institute (2012)

31. Elsea J.K., Elsea D.H. *Naval Station Guantanamo Bay: History and Legal Issues Regarding Its Lease Agreements* Congressional Research Service 7:57 (2016)
32. England G. *Memo on Cyberspace Defense of USA*, USA Department of Defense (2008)
33. Erickson J. *Hacking : The Art of Exploitation* wyd.2. No Starch Press (2008)
34. Finninn S. *Elements of accessorial modes of liability:Article25(3)(b) and (c) of the Rome Statue of the International Criminal Court*, Martnus Nijhoff Publishers, Boston, International Humanitarian Law Series 38. (2012);
35. Flanigan E.R. *Integrated Non-Kinetic Operations: The Frontier of Warfare in Search of Doctrine*. School of Advanced Air and Space Studies Air University (2010)
36. Froomkin A.M. *Almost free: An analysis of ICANN's Affirmation of Committments Cooperative Research and Development Agreement* (2010)
37. Gazula M.B. *Cyber Warfare Conflict Analysis and Case Studies*, Cybersecurity Interdyscyplinary Systems Laboratory (CISL) Massachusetts Institute of Technology (2017).
38. Gelberg I. *Prawo międzynarodowe i historia dyplomatyczna.* Polskie Wydawnictwo Naukowe t. 1 (1954)
39. Gibson W. *Burning Chrome* Harper Voyager (1986)
40. Gibson W. *Neuromancer* Ace Books (1984)
41. Goldman B. *The Applicable Law: General Principles of Law-Lex Mercatoria* Kluwer Academic (1987)
42. Goldoni M. *The Normativity of Code as Law: Toward Input Legitimacy Globalisation* Constitution Project, FWO Foundation (2011)
43. Goldsmith J. *The Terror Presidency:Law and Jugdement inside the Bush administration* NYC W.W. Norton (2007);
44. Goldsmith J. Wu T. *Who Controls The Internet?:Illusions Of A Borderless World*, Oxford University Press (2006)
45. Gray Ch. *International Law and the Use of Force* Oxford University Press, 4 wyd. (2018)
46. Grzebyk P. *Criminal Responsibility for the Crime of Aggression* Routledge Taylor and Francis Group,NY, Londyn (2013)

47. Guzman A. *The Consent Problem in International Law University of California*, Berkeley Working Paper Series (2011)
48. Hathaway O., Shapiro J. *How a radical plan to outlaw war remade the world* Simon and Schuster Nowy Jork wyd. 1 (2017)
49. Henry J. *Analysis: Activating the jurisdiction of the International Criminal Court over the Crime of Aggression*, PKI Journal 8/2018 Phillip Hirsch Institute (2018).
50. Heshmaty A. *E-Residency- how does it work?* LexisNexis PSL (2017)
51. Hillier T. *Sourcebook on Public International Law* Title I, Series II, Cavendish Publishing Ltd. (1998)
52. Holmberg E.J. *Armed Attacks in the Cyberspace. Do they exist and can they trigger the right to self-defense*, University of Stockholm Press (2015)
53. Janis M.W. *Jeremy Bentham and the Fashioning of 'International Law* 78 American Journal of International Law (1984)
54. Jennings R. *Sovereignty and International Law*, Oxford Scholarships (2002)
55. Jessup Ph. C. *Transnational Law* Yale University Press (1956)
56. Kaska K. Osula A.M., Stinissen J. *The Cyber Defence Unit of the Estonian Defence League* NATO Cooperative Cyber Defence Centre of Excellence(2013)
57. Kittrie O.F. *Lawfare: Law as a Weapon of War* Oxford Univeristy Press (2016)
58. Klabbers J., Piiparinen T. *Normative Pluralism and International Law: Exploring Global Governance* Cambridge University Press (2013)
59. Klimburg A. *A Darkening Web:The war for Cyberspace* Penguin Books Random House LLC (2017)
60. Kuerbis B.- *Defusing the cybersecurity dillema game through attribution and network monitoring*, Georgia Tech School of Public Policy; IGP (2018)
61. LaQuey T. *The Internet Companion: A Beginner's Guide to Global Networking* University of North Carolina Press (1994)
62. Lauterpacht H. *Recognition in Interntional Law* University Press (1947)
63. Lessig L.*Code and other Laws of Cyberspace* wyd. 2 Basic Books (2006)
64. Lessig L.*Code v. 2.0* Basic Books (2006)
65. Lew J.D.M. *Contemporary Problems in International Arbitration* Boston: Kluwer Academic (1987)
66. Libicki M. C. *Cyberspace in Peace and War*, Naval Institute Press (2016)

67. Libicki M.C.,*Conquest in Cyberspace: National Security and Information Warfare*, Rand Corporation/Cambridge University Press (2007)
68. Mills A. *Rethinking Jurisdiction in International Law* British Yearbook on International Law 84:1, Oxford University Press(2014)
69. Mills A. *The Confluence of Public and Private International Law: Justice, Pluralism and Subsidiarity in the International Constitutional Ordering of Private Law* Cambrigde University Press (2010)
70. Monte M. *Network Attacks and Exploitation: A Framework* Wiley Press (2015)
71. Morgan J. *Extra-legal norms: the irrelevance of the law (of contract)?*, Cambridge University Press (2013)
72. Mueller M. A U*nited Nations Committee for Internet-Related Policies? A fair assessment*. IGP 2018 School of Public Policy, Georgia Institute of Technology Press (2018)
73. Negroponte N. *Being Digital ,* A.Knopf Press NY (1995)
74. Nielsen M.A, Chang I.L. *Quantum Computation and Quantum Information* Cambridge University Press (2000)
75. Norman D.*The Design of Everyday Things* Basic Books (2002)
76. Norris A.J. *Legal Issues Associated with Unamanned Mairitime Systems* Selected Works of Andrew J. Norris Bepress U.S. Naval War College (2013)
77. Nuth M.S. *Lex Informatica and Cyberspace* University of Oslo Press (2017)
78. O'Conell M.E., Arimatsu L.,Wilmshurst E. *Cyber Security and International Law: Meeting Summary*, Chatam House Publications 8 (2012)
79. Olney M., Mullen P., Miklavcic K. Dan Kaminsky; *2008 DNS Vulnerability*, Sourcefire Vulnerability Research Team Report, Sourcefire Inc. (2009)
80. Ottis R. *Analysis of the 2007 Cyber Attacks Against Estonia form the Information Warfare Perspectve* Cooperative Cyber Defence Centre of Excellence, Tallin (2018)
81. Perkowski M. *Podmiotowość prawa międzynarodowego współczesnego uniwersalizmu w złożonym modelu klasyfikacyjnym* Temida 2 (2008)
82. Pernik P., Wojtkowiak J., Verschoor-Kirss A. *National Cyber Security Organisation: United States* NATO Cooperative Cyber Defence of Excellence Tallinn (2015)

83. Philpott D. *Revolutions in Sovereignty: How Ideas shaped Modern International Relations* Princeton University Press (2001)
84. Preece J., Rogers Y., Sharp H., Benyon D., Holland, Carey T. *Human-Computer Interaction* Addison-Wesley Longman(1994)
85. Roach J.A. *A Guide to Arctic Issues for Arctice Council observers* Centre for International Law of National University of Singapore (2017)
86. Rosario G. *Bibliotheca Scriptorum Qui Res in Sicila Gestas Sub Aragonum Imperio Retulere* wyd. Ex Regio Typographeo, digitalizacja Bayerische Staatsbibliothek (1791)
87. Roscini M. *Cyber Operations and the Use of Force in International Law* Oxford University Press (2016)
88. Rowe B., Wood D., Reeves D.,Braun F. *The Role of Internet Service Providers in Cyber Security* Institute for Homeland Security Solutions San Francisco (2011)
89. Ryngaert C. *Jurisdiction in International Law* Oxford Monographs in International Law, Oxford University Press (2008)
90. Sandoz Y., Swinarski Ch., Zimmermann B. *Komentarz do Protokołów Dodatkowych do Konwencji Genewskich* International Committee of the Red Cross, wyd. Martinus Nijhoff Publishers, Genewa (1987)
91. Schelling Th. C. *Arms and Influence,* Praeger Press,(1977)
92. Schmitt M.N., Vihul L.*Tallin Manual 2.0*, NATO Cooperative Cyber Defence Centre of Excellence w Tallinie, Cambrigde Univeristy Press (2018)
93. Schneier B. *Data and Goliath: The Hidden Battles to Collect Your Data and control Your World*. W. W. Norton & Company (2016)
94. Shaw M.N. *International Law*, Cambridge University Press 6th ed. (2008)
95. Snyder G.H. *Deterrence and Defense: Toward a Theory of National Security*, Priceton Legacy Library (1961)
96. Winterfeld J.Andress J.A. *Cyberwarfare* Safari Books (2019)
97. Zheng Y. *Technological Empowerment: The Internet, State and Society in China* Stanford University Press,(2018)
98. Zittrain J., Edelman B. *Empyrical Analysis of Internet Filtering in China* Berkman Center for Internet and Society, Harvard Law School (2003)

Artykuły

1. Abramson R. *Trademarks and the Internet, Advanced Seminar on Trademark Law*, par. 299303-10[w: PLI Patents, Copyright,Trademarks and Literary Course Handbook Series G4-965(1996)]
2. Aloupi N. *The right to Non-intervention and Non-interference,* Cambridge Journal of International and Comparative Law 4:15 (2015)
3. Ansong A. *The Concept of Sovereign Equality of the States in International Law*, GIMPA Law Review 2-1 (2016)
4. Armstrong W. *The Doctrine of Equality of Nations in International Law and the Relation of the Doctrine to the Treaty of Versailles*, The American Journal of International Law, 14:4 (1920)
5. Arquilla J., Ronfeldt D. *The Advent of Netwar*, RAND Corporation Santa Monica Law Review 94 (1996)
6. Asscher L., Dommering E.J., *Coding Regulation*, Asscher Press (2012)
7. Baird Z. *Governing the Internet:Engaging Government, Business and Nonprofits*, Foreign Affairs 11/12 (2002)
8. Baistrocchi P.A. *Liability of Intermediary Service Providers in the EU Directive on Electronic Commerce* 19 Santa Clara High Tech Journal 111 (2002)
9. Baker F., Montgomery D., Luckie M. et al. *Addressing the challenge of IP spoofing*, Internet Society (2015)
10. Bassiouni M. Ch. *The New Wars and the Crisis of Compliance with the Law of Armed Conflict*, Journal of Criminal Law and Criminology 98:3 (2008)
11. Beale J.H. *The Jurisdiction of a Soveregin State* Harvard Law Review 36:6 (1923)
12. Behrens P. *The extraterritorial reach of EU competition law revisited: The "effects doctrine" before the ECJ* ECONSTOR Disscussion Paper 3/16, Leibniz Inormationszentrum (2016)
13. Bekker P.H.F., *The World Court Finds that US Attacks on Iranian Oil Platforms in 1987-1988 were not justifiable as Self-Defense, but the United States did not*

violate the applicable treaty with Iran, Americal Society of International Law 8:25 (2003)

14. Benkler Y. *From Consumers to Users: Shifting the Deeper Structures of Regulation Towars Sustainable Commons and User Access*, 52 Federal Communications Law Journal (2000)
15. Bennoune K. '*Sovereignty vs. Suffering'? Re-examining Sovereignty and Human Rights through Lens of Iraq*, 13 European Journal of International Law (2002)
16. Berg T. *State Criminal Jurisdiction in Cyberspace: Is there a Sheriff on the Electronic Frontier?,* Michigan Bar Law Journal 79:3 (2000)
17. Berger K.P. *The Lex Mercatoria (Old and New) and the TransLex-Principles* Trans-Lex Law Research (2018)
18. Berman P.*Global Legal Pluralism*, 80 South California Law Review (2007)
19. Besson.A *Sovereignty*, Max Planck Stiftung, MPEPIL(2011)
20. Bethlehem D. *The End of Geography: The Changing Nature of the International System and the Challenge to the International Law,* European Journal of International Law 25:1 (2014)
21. Betts R.K. *Compromised Command,* Foreign Affairs 126 (2001)
22. Beverly R., Berger A., Hyun Y., Claffy K. *Understaning the efficacy of deployed Internet source address caldation filtering,* Proceedings of the 9th ACM SIGCOMM Conference on internet Measurement Conference, Chicago (2009)
23. Bialostozky N. *Extraterritoriality and National Security:Protective Jurisdiction as a Circumstance Precluding Wrongfulness*, Columbia Journal of International Law, 52:617 (2017)
24. Biller J., Schmitt M.N. *Un-Caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences*, EJIL:Talk! (2018)
25. Biller J.*, Schmitt M.N. Un-Caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences, EJIL:Talk!* (2018) s.1
26. Bischoff P. *What's the Best VPN for China?* Comparitech 1/2018(2018)
27. Blakesley Ch. *Criminal Law: United States Jurisdiction Over Extraterritorial Crime*, Journal of Criminal Law 73:6 (1982)
28. Bloomfield L.P. *Why Wars End: CASCON's Answers from History*, London School of Economics, Millenium Journal of International Studies 26:3 (1997)

29. Bonell M.J.*The law governing international commercial contracts and the actual role of the UNIDROIT Principles,* Uniform Law Review 23:1 (2018)
30. Bothe M. *Oil Platforms Case- A The Facts of the Case*, MPEPIL,(2011)
31. Bowcott O. *Dispute along cold war lines led to collapse of UN cyberwarfare talk*, The Guardian(2017)
32. Boyle J. *Foucault in Cyberspace: Surveillance, Sovereignty and Hardwired Censors*, University of Cincinnati Law Review 66 (1997)
33. Branscomb A.W. *Anonymity,Autonomy and Accounatability: Challenges to the First Amendment in Cyberspaces*, Yale Law Journal 104:7 (1995)
34. Bressie K. *Marine Jurisdictional Problems for Sumbarine Cables*, SubOptic 2016 (2016)
35. Brown G. *Why Iran Didn't Admit Stuxnet Was an Attack?* , Joint Forces Quaterly nr 63: 4 (2011)
36. Brownlie I, Crawford J. *Brownlie's Principles of Public International Law,* Oxford Univeristy Press (2012)
37. Brownsword R. *Code, Control and Choice: Why West is West and East is East.* Legal Studies 25:1 (2005)
38. Buxbaum H.L. *Territory, Territoriality, and the Resolution of Jurisdictional Conflict*, American Journal of Comparative Law 57:631 (2009)
39. Buzan B., Waever O., de Wilde J. *Security: A new framework for Analysis,* Lynne Rienner Publishers (1998)
40. Byassee K. *Jurisdiction of Cyberspace: Applying Real World Precedent to the Virtual Community*, Wake Forest Law Review 30:197 (1995)
41. Cameron I *The Protective Principle of International Criminal Jurisdiction* Dartmouth Publishing Company (1994)
42. Cameron I. *International Criminal Jurisdiction, Protective Principle,* Max Planck Stiftung MPEPIL (2018)
43. Canfil J.K. *Honing Cyber Attribution: A framework for Assesing Foreign States Compliticity,* Journal of International Affairs 70:1 (2016)
44. Canuel E. *The Four Arctic Law Pillars A Legal Framework,* Georgetown Journal of International Law 46:735 (2015)
45. Cassese A. *The Martens Clasue: Half a Loaf or Simply Pie in the Sky?* European Journal of International Law 11:1 (2000)

46. Cassese A. -*The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgement on Genocide in Bosnia*, The European Journal of International Law 18:4 (2007)
47. Castaneda F.A.C. *A call for rethinking the sources of international law: soft law and the other side of the coin*, Anuario Mexicano de Derecho International 13 (2013)
48. Cebrowski A.K. *CNE and CNA in the Network-Centric Battlespace: Challenges for Operators and Lawyers* International Law Studies 76 (2012)
49. Cebrowski A.K. *CNE and CNA in the Network-Centric Battlespace: Challenges for Operators and Lawyers* International Law Studies 76 (2012)
50. Chantler A., Broadhurst R. *Social Engineering and Crime Prevention in Cyberspace* SSRN Electronic Journal 10 (2008)
51. Chawki M. *Anonimity in Cyberspace: finding the Balance between the Privacy and Security,* Droit-Tic (2006)
52. Chung, K., Kalbarczyk, Z. T., & Iyer, R. K. *Indirect cyber attacks by perturbation of environment control: A data driven attack model,* HotSoS (2018)
53. Clancy E.A. *The tragedy of Global Commons*, Indiana Journal of Global Legal Studies, 5:2 (1998)
54. Clark Arend A. *International Law and the Preemptive Use of Military Force,* The Center for Strategic and International Studies and the Massachusetts Institute of Technology, The Washington Quaterly 26:2 (2003)
55. Colangelo A.J. *What is Extraterritorial Jurisdiction*, Cornell Law Review 99 (2014)
56. Coppel J. *A Hard Look at the Effects Doctrine of Jurisdiction in Public International Law,* Leiden Journal of International Law 6:1 (1993)
57. Cover R.M. *The Supreme Court, 1982 Term- Foreword; Nomos and Narrative* Yale Law School Law Scholarship Repository 2705 (1983)
58. Cramton R. C. *The Ordinary Religion of the Law School Classroom*, 29 Journal of Legal Education 247 (1978)
59. Crawford E. *The Modern Relevance of the Marten Clause* ISIL Yearbook of International Humanitarian and Refugee Law 6 (2006)
60. Dalhuisen J.H. The Sources of Modern Transnational Lex Mercatoria, Opinio Juris (2012)

61. Daniluk M. *Problem uznania rządu w prawie międzynarodowym na przykładzie uznania libijskiej Narodowej Rady Tymczasowej,* Studia Iuridica Lublinensia 20 (2013)
62. Daskal J. *The Un-terrytoriality of Data* 125 Yale Law Review (2015)
63. Davenport T. *Submarine Cables, Cybersecurity ad International Law: An Intersectional Analysis,* Catholic University Journal of Law and Technology25:1 (2015)
64. De Mul J. *Cyberspace Odyssey: Towards a Virtual Ontology and Anthropology* Cambridge Scholars Publishing (2010)
65. Demarest G.B. *Espionage in International Law,* Denver Journal of International Law and Policy 24:321 (1995-96)
66. Derian J.D. *Cyber-Deterrence,* Wired Magzine 9/94 (1994)
67. Devin C., Fellin T., Kauffman,Kopl R. *The Law and Big Data*, Cornell Journal of Law and Public Policy 27:357 (2017)
68. DeWeese G. *Anticipatory and Preemptive Self-Defense in Cyberspace: The Challenges of Imminence*, Architectures in Cyberspace 7 (2015)
69. Dewey J. *Austin's Theory of Sovereignty*, Political Science Quaterly, 9:1(1984)
70. Dommering E.Asscher L.F. *Coding regulation - Essays on the Normative Role of Information Technology*, Information Technology and Law Series T.M.C. ASSER Press/ Springer (2006)
71. Douglas L. *The importance of 'Big Data'* , Gartner IT Glossary *(2012)*
72. Draguiew D. *Unilateral Jurisdiction Clauses: The Case for Invalidity, Severability or Enforceability.,* Journal of International Arbitration 31:1 (2014)
73. Dunk von der F.G. *The role of law with respect to future space activities*, Elsevier Space Policy 12:1 (1996)
74. Durrani H.A. *The Bogota Declaration: A case Study on Sovereignty, Empire and the Commons in Outer Space.* 408 Columbia Journal of Transnational Law (2016)
75. Dworkin R. *No Right Answer,* Essays in Honor of H.L.A. Hart, Oxford Clarendon Press (1977)
76. Eagleton C. *The Form and Function of the Declaration of War*, American Journal of International Law 32 (1938)

77. Easterbrook F. *Cyberspace and the Law of the Horse,* University of Chicago Legal Forum 207:96 (1996)
78. Eichensehr K.E. *The Cyber-Law of Nations* The Georgetown Law Journal 103 (2015)
79. Fassbender B. *Peace of Westphalia (1648)*, Max Planck Stiftung , MPEPIL(2011)
80. Ferguson A.T. *Closing the Gaps: Cybersecurity for U.S. Forces and Commands* Joint Forces Staff College (2016)
81. Finch,jr. St.B. *Pueblo and Mayaguez: Legal Analysis,* Case Western Journal of International Law 9:183 (1977)
82. Flowers A., Zedally Sh. *Cyberwar: The What, When, Why, How,* IEEE Technology and Society Magazine (2014)
83. Foltz A.C. *Stuxnet, Schmitt Analysis and the Cyber 'Use of Force'*, Debate.Joint Forces Quaterly 67:447 (2012)
84. Fowler M.R., Bunck J.M. *What constitues the sovereign state*, Review of International Studies 22:4 Camridge University Press (1996)
85. Franck Th. M. *Who Killed Article 2(4)?: Changing Norms Governing the Use of Force by States*, American Journal of International Law 64 (1970)
86. Freeman E.H. *Cyber Courts and the Future of Justice*, Legally Speaking, Information Systems Security 14:1 (2005)
87. Froomkin A.M. *Toward a critical Theory of Cyberspace* Harvard Law Review 116 (2003)
88. Fuchs Ch. *Implications of Deep Packet Inspection (DPI) Surveillance for Society*, University of Uppsalla "PACT-Public Perception of Security and Privacy:Assessing Knowledge, Collecting Evidence, Translating Research into Action" (2018)
89. Fuller L.L. *The Morality of Law* , Yale University Press (1969)
90. Garwood-Gowers A. *Case Notes. Case Concerning Oil Platforms. Did the ICJ miss the boat on the law on the use of force?,* Melbourne Journal of International Law 5(2004)
91. Geiss R. *Asymmetric conflict structures*, International Review of the Red Cross 88:864(2006)
92. Gervais M. *Cyberattacks and the Laws of War* Berkeley Journal of International Law, 30:25(2012)

93. Gladstone J.A. *Determining Juirsidiction in Cyberspace: The "Zippo "Test or "Effects" Test?,* InSite "Where Parallels Intersect", Informing Science (2003)
94. Glennon M.J. *The Road Ahead:Gaps, Leaks and Drips*, 89 International Law Studies US Navy War College (2013)
95. Goldman B. *La lex mercatoria dans le contrats et l'arbitrage internationaux: realite et perspectives*, Journal du Droit International 106 (1979)
96. Goldsmith J. *Against Cyberanarchy*, University of Chicago Law Review 11:98 (1998),
97. Goldsmith J.L. *The Internet and the Abiding Significance of Territorial Sovereignty,* 5 Indiana Journal of Global Legal Studies (1998)
98. Goldsmith J.L., *Against Cyberanarchy*, 65 University of Chicago Law Review (1998)
99. Goodman W. *Cyber Deterrence: Tougher in Theory than in Practice?* Strategic Studies Quaterly 4:3 (2010)
100. Graham M. *Geography of Cyberspace,* Centre for Advanced Spectral Analysis Working Papers 8 (2011)
101. Grant Th. *Defining Statehood: The Montevideo Convention and its discontent* Columbia Journal of Transitional Law 37:(1998)
102. Greenberg M.H. *A Return to Liliput: The LICRA v. YAHOO! Case and the Regulation of Online Content in the World Market,* Berkeley Technology Law Journal 18 (2003)
103. Grimmelmann J. *Death of a data haven:cypherpunks,WikiLeaks, and the world's smallest nation,* Ars Technica 3/2012 (2012)
104. Gross G. *New ICANN agreement runs into Criticism*, CIO Review 10/09 (2009)
105. Hall S. *The Persistent Spectre: Natural Law, International Order and the Limits of Legal Positivism*, European Journal of International Law 12 (2001)
106. Handeyside H. *The Lotus Principle in ICJ Jurisdprudence: Was the ship ever afloat?* Michigan Journal of International Law 29:71 (2007)
107. Hang R. *Freedom for Authoritariasnim: Patriotic Hackes nad Chinese Nationalism,* The Yale Review of International Studies, 11:14 (2014)
108. Hare F. *Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?* Nato Cooperative Cyber Defence Center of Excellence (2018)

109. Harris M. *Why is Tony Blair lending credibility to Kazkhstan's dictator?* The Telegraph 2 II 2012 (2012)
110. Hart. H.L.A. *Bentham on Sovereignty,* Irish Jurist, 2:2 (1967)
111. Hartmann K., Giles K. *UAV Exploitation:A new domain for cyberpower*., 2016, 8th International Conference on Cyber Conflict, Cyber Power (2016)
112. Harvey T. *The Proper Legal Regime for 'Cyberspace'* 55 Pittsburgh Law Review (1994)
113. Hassan K. *Jus Cogens and Obligations Under the U.N. Charter,* Santa Clara Journal of International Law 3 (2005)
114. Hayman P.A., Williams J. *Westpahalian Sovereignty: Rights, Intervention, Meaning and Context*, Global Society 20:4 (2006)
115. Henkin L. *International Law After the Cold War*, Maryland Journal of International Law 15:147 (1991)
116. Hildebrandt M. *Extraterritorial Jurisdiction to Enforce in Cyberspace? Codin, Schmitt, Grotius in Cyberspace*. University of Toronto Law Journal wyd. 63:2 (2013)
117. Hoffman W., Levite A.E. *Private Sector Cyber Defense. Can Active Measures Help Stabilize Cyberspace?* Carnegie Endowment for International Peace (2017)
118. Hollis D.B. *An e-SOS for Cyberspace* Harvard International Law Journal, 52 (2011)
119. Hollis D.B. *Why States Need an International Law for Information Operations,* Lewis & Clarck Law Review 11 (2207)
120. Honan M. *Kill the password: A string of characters won't protect you,* Wired 12 czerwca (2012)
121. Honniball A.N. *The exclusive Jurisdiciton of Flag States: A Limitation on Pro-active Port States?* The International Journal of Marine and Coastal Law 31 (2016)
122. Honniball A.N. The exclusive Jurisdiciton of Flag States: A Limitation on Pro-active Port States? The International Journal of Marine and Coastal Law 31 (2016)
123. Hoss Cr. M Morgan-Forster J.*The Rainbow Warrior*, MPEPIL (2010)
124. Hovanesian M.D. *Hackers and Pishers and Frauds, OhMy!*, Business Week 6/2005(2005)

125. Howarth R.J. *Lex Mercatoria: Can General Principles Of Law Govern International Commercial Contracts?* Canterbury Law Review 10:36 (2004)
126. Hulnick A. *The Dilemma of Open Source Intelligence: Is OSINT Really Intelligence?* The Oxford Handbook of National Security Intelligence (2010)
127. Hunter D. *Cyberspace as Place and the Tragedy of Digital Anticommons* 91 California Law Review (2003)
128. Jansons J. *Was Stuxnet an Act of War Lessons Learned and Conflicts History* Baltic Defence College 4 (2017)
129. Jarmon J.A., Yannakogeorgeos P. *The Cyber Threat and Globalization: The Impact on National and International Security* Rowman and Litfield wyd.5 (2018).
130. Johnson D., Post D., *Law and Borders: The Rise of Law in Cyberspace,* 48 Stanford Law Review (1996).
131. Kaminsky D. *Black Hat Conference Lecture,* Black Hat Info-Sec Conference (2014).
132. Kang C., Nakashima E. *Tech Executives to Obama: NSA Spying Revelations Are Threatening Business*, Washington Post (2013).
133. Kang J. *Developments in the Law- The Law of Cyberspace,* 112 Harvard Law Review (1993)
134. Karska E. *Dorobek Konferencji Rewizyjnej Statutu MTK ze szczególnym uwzględnieniem poprawki definiującej zbrodnię agresji*, Kwartalnik Prawa Publicznego 10:3 (2010)
135. Katsh M.E. *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace,* University of Chicago Legal Forum 335(1996)
136. Keber T.O., Roguski N.P. *Ius ad bellum electronicum? Cyberangriffe in Lichte der UN-Charta und aktueller Staatenpraxis,* Archiv des Voelkerrechts wyd. Mohr Siebeck GmbH & Co. KG, 49:4408 (2011)
137. Kees A. *Responsibility of States for Private Actors*, Max Planck Stiftung, MPEPIL (2011)
138. Keizer G. *Stuxnet struck five targets in Iran, say researchers,* "Computerworld" 2/2011(2011)
139. Kernes M. *Black Hat: Kaminsky Talks DNS,,* Enterprise Networking Planet (2016)

140. Kerr O.S. *The next Generation Communications Privacy Act,* University of Pennsylvania Law Review 162:373 (2014)
141. Killaby G. *Great Game in Cold Climate. Canada's Arctic Sovereignty in Question,* Canadian Military Journal 2005 (2005)
142. Kley A., Tophinke E. *Ueberlick ueber die Reine Rechtslehre von Hans Kelsen,* Juristische Arbeistblaetter, 33:2 (2001)
143. Knight F.W. *The Haitan Revolution,* The American Historical Review 105:1 (2000)
144. Kohen M. T*he Principle of Non-Intervention 25 Years after Nicaragua Jugdement,* Leiden Journal of International Law25 (2012)
145. Kosi I. *Mr. GDPR: Interview with Giovanni Buttarelli,* New Europe wyd.5/2018 (2018)
146. Kowalski M. *Ius ad bellum a systemowy charakter prawa międzynarodowego,* wyd.UMCS (2005)
147. Kozłowski A. *Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan*, European Scientific Journal 2/2014 t.3 (2014)
148. Krebs B. *Lithuania weathers Cyber Attack, Braces for Round 2,* The Washington Post (2008)
149. Kretzmer D. *The inherent Right to Self-Defence and Proportionality in Ius ad Bellum,* European Journal of International Law 24, Oxford University Press (2013)
150. Kunig Ph. *Prohibition of Intervention,* Max Planck Stiftung MPEPIL (2008)
151. Kushner D. *The Communications Decency Act and the Indecent Indecency Spectacle* 19 Hastings Communications and Entertainment Law Journal 87:131 (1996)
152. Lambers R. *Code is not Law*, raport z konferencji Code as Code w Amsterdamie, INDICARE Team, Karlsruhe Institute of Technology (2004)
153. Langner R. *To kill a centrifuge. A technical analysis of what Stuxnet's Creators Tried to Achieve,* Langener Group (2013)
154. Lastowka G., Hunter D. *The Laws of the Virtual World,* California Law Review 92:1 (2004)
155. Lauterpacht H. *Recognition of States in International Law,* 53 Yale Legal Journal (1944).

156. Layock S., West Ch. *Lost Countries Exotic Tales from an old Stamp Album,* The History Press (2017)
157. Lehman-Taylor D. *The Plot against Prinicipality of Sealand*, Narratively 3/19 (2019)
158. Lemley M. *Shrinkwraps in Cyberspace,* Jurimestrics 35(1994)
159. Lessig L. *Code is Law,* Harvard Magazine 1/2001 (2001)
160. Lessig L. *The Architecture of Innovation,* 51 Duke Law Journal (2002)
161. Lessig L. *The Law of The Horse: What Cyberlaw Might Teach,* Harvard Law Review 113:501 (1999)
162. Lessig L. *The Laws of Cyberspace,* Taiwan Net 98 (1998).
163. Lessig L. *The Limits in Open Code: Regulatory Standards and the Future of the Net,* 14 Berkeley Tech Law Journal (1999)
164. Lessig L. *The Zones of Cyberspace,* Stanford Law Review 48:5/1996
165. Łętowska E. *Multicentryczność współczesnego systemu prawa i jej konsekwencje,* Państwo i Prawo 60:4 (2005)
166. Levinson D.J. *Collective Sanctions,* Stanford Law Review 56:345 (2003)
167. Lewis P.H.U. *Beigns Privatizing Internet's Operations*, The New York Times (1994)
168. Lidsky L.B. *Anonymity in Cyberspace: What Can we Learn from John Doe?* Boston College Law Review 50 (2009)
169. Lin H. *Offensive Cyber Operations and the Use of Force,* Journal of National Security 4:63 (2010).
170. Lipke D.J. *You Are Here: The race to bring Geography to the Borderless Web* , American Demographics 3/01 (2001)
171. Lister M. *The Legitimating Role of Consent in International Law,* Chicago Journal of International Law 1:1 (2011)
172. Litfin K.T. *Sovereignty in World Ecopolitics,* Mershon International Studies Review 41 (1997)
173. Litfin K.T. Sovereginty in World Ecopolitics, Mershon International Studies Review 41 (1997)
174. Lloyd D.O. *Sucession, Secession and State Membership in the United Nations,* New York University Journal of International Law and Politics 761(1993)

175. Lohrmann D. *Cyber Terrorism: How Dangerous is the ISIS Cyber Caliphate Threat?* Govtech.com (2015)

176. Loshin P. *Practical Anonymity: Hiding in Plain Sight Online Syngress*, Waltham (2013)

177. Lotrionte C. *Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law*, The Cyber Defense Review 3:2 (2018)

178. Luke T.W. *Simulated Sovereignity, Telematic Territoriality: The Political Economy of Cyberspace Theory*, Culture & Society 2nd Conference (1995)

179. Lyon A.H.E. *The Principality of Sealand and Its Case for Sovereign Recognition*, Emory International. Law Review 29:3 (2014)

180. Mačak K. *From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers,* Leiden Journal of International Law 30 (2017)

181. Mačak K.From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers Leiden Journal of International Law 30 (2017)

182. Maggs G.E. *How United States Might Justify a Preemptive Strike on a Rouge Nations Nuclear Weapon Development Facilities Under the U.N. Charter* , Syracuse Law Review 57:465 (2007)

183. Maillart J-B, *The limits of subjective territorial jursidtiction in the context of cybercrime,* ERA Forum 19:3 (2019)

184. Makinda S.M. *The United Nations and State Sovereignty: Mechanism for Managing International Security*, Australian Journal of Political Science 33(1998)

185. Mann F.A. *Recognition of Sovereignty* , The Modern Law Reviewed. 16:2 (1953)

186. Mann F.A.*The Doctrine of Jurisdcition in International Law*, 111 RCADI (1964)

187. Manta I.D., Burke-Robertson C. *Secret Jurisdiction*, Emory Law Journal 65:1313 (2016)

188. Margulies P. *Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility,* Melbourne Journal of International Law 16:496 (2013)

189. McCormack T.L.H., *A non liquet on nucelar weapons- The ICJ avoids the application of general principles of international humanitarian law,* International Review of the Red Cross 316 (1997)

190. McDonald A. *Declarations of War and Belligerent Parties: International Law Governing Hostilities Between States and Transnational Terrorist Networks,* Netherlands International Law Review 54:277 (2007)
191. McDougal M., Burke W. *The Public Order of the Oceans: A Contemporary International Law of the Sea,* Yale University International Law Review 54:1 (1965)
192. McDougal M.*The Intelligence Function and World Public Order,* Temple Law Quaterly/ Yale Law School Faculty Scholarship Series 25:69 (1972)
193. McSweeney B. *Identity and Security: Buzan and the Copenhagen School,* Review of International Studies 22:1 (1996)
194. Mefford. A. *Lex informatica: Foundations of Law on the Internet*, Indiana Journal of Global Legal Studies 5:1 (1997)
195. Melito S. *Cyber War and the Siberian Pipeline Explosion,* Defence and Security Alert 7/19 (2019)
196. Melzer N. *Cyberwarfare and International Law*, United Nations Institute for Disarmament Research (2011)
197. Menthe D.C. *Jurisdiction in Cyberspace: A Theory of International Spaces,* University of Michigan Telecommunications and Internet Law Journal 4 (1998)
198. Milanovic M. *Self-Defence and Non-state Actors: Intedeterminacy and Jus ad bellum*, Ejil:Talk!,2/10 (2010)
199. Miller M. *Is it Safe? Protecting Your Computer, Your Bussiness, and Yourself* , Online Que Publishing (2008)
200. Miller S.F. *Prescriptive Jurisdiction over Internet Acitivity: the need to Define and Establish the Boundaries of CyberLiberty,* Indiana Journal of Global Legal Studies 10:2(2003)
201. Molnar A.,Parsons Ch., Zouave E. *Computer network operations and'rule-with-law',* Australia Internet Policy Review Journal on Internet Regulation 6:14(2017)
202. Moore G.E. *Cramming more components onto integrated circuits,* Electronics Magazine 38:8, (1965).
203. Morawski L. *Główne problemy współczesnej filozofii prawa. Prawo w toku przemian,* Wydawnictwa Prawnicze Lexis Nexis Warszawa (2003)
204. Moyer E.*US hands internet control to ICANN* - CNET 10/16 (2016)

205. Mueller M. *The core Internet institutions abandon the US Government,* Internet Governance Project, Georgia Tech School of Public Policy 11/13 (2013)
206. Murphy C. *Lon Fuller and the Moral Value of the Rule of Law,* Law and Philosophy 24 (2005)
207. Nagraja Sh. ,Anderson R. *The snooping dragon: social-malware surveillance of the Tibetan movement,* University of Cambrigde Computer Laboratory 749 (2009).
208. Nelken D. *Eugen Ehrlich, Living Law, and Plural Legalities,* Theoretical Inquiries in Law 9:2(2008)
209. Neocleous M. *Police, Power, all the way to heaven. Cujus est solum and the no-fly zone,* Radical Philopsophy 182 5:14 (2013)
210. Nguyen R. *Navigating "Jus ad Bellum" in the Age of Cyber Warfare*, California Law Review 101:4 (2013)
211. Nieznański E. *Logika Deontyczna w systemie S5,* Studia Philosophiae Christianae 43, Uniwersytet kardynała Stefana Wyszyńskiego (2007)
212. Ohlin J.D. *Did Russian CyberIntefererence in the 2016 Election Violate International Law?* Texas Law Review 15:79 (2017)
213. Okoniewski E.A. *Yahoo!,Inc. V. LICRA: The French Challenge to Free Expression in the Internet,* American University International Law Review 18:6 (2002).
214. Oppenheim L. *International Law (Lauterpacht edition)* wyd. 8 Longmans, Green and Co (1995).
215. Osofsky H.M. *Climate Change Litigation as Pluralist Legal Dialogue,* 43 Stanford Journal of International Law 19 (2007)
216. Paganini P. *Cyber espionage campaign based on Havex RAT hit ICS/SCADA systems,* Security Affairs, 6/14(2014)
217. Paganini P. *GCHQ accused of illegal Computer Network Exploitation activities*, Security Affairs 4/15 (2015)
218. Paganini P. *NATO officially recognizes cyberspace a warfare domain,* Security Affairs 1/2016 (2016)
219. Parrish, Austen L. *The Effects Test: Extraterritoriality's Fifth Business,* Maurer Faculty Paper 893(2008)

220. Parry J.T. *What is the Grotian tradition in international Law?* University of Pennsylvania Journal of International Law 35: 299 (2014)

221. Past L. *Cyberspace - Just another domain of election interference?* The European Centre of Excellence for Countering Hybrid Threats, Strategic Analysis 8/2018 (2018)

222. Patrikios A. *Resolution of Cross-Border E-Business Disputes by Arbitration Tribunals on the Basis of Transanational Substantive Rules of Law and E-Business Usages: The Emergence of Lex Informatica*, 21st BILETA Conference (2006)

223. Perrit Jr. H.H. *Jurisdiction in Cyberspace,* 41 Villanova Law Review, (1996)

224. Petereson M.J. *The Use of Analogies in Developing Outer Space Law International Organisation,* Cambridge University Press 51:2 (1997) .

225. Petrovic J. *The Old Brigde of Mostar and Increasing Respect for Cultural Property in Armed Conflict,* The Humanitarian Law Series, Martinus Nijhoff Publishers(2013)

226. Phillipe X. *The principles of universal jurisdiction and complementarity: how do the two principles intermesh?* International Review of the Red Cross 88:862 (2006)

227. Philpott D. *Revolutions in Sovereignty: How Ideas shaped Modern International Relations,* Princeton University Press (2001)

228. Plakokefalos I. *The Use of Force by Non-States Actors and the Limits of Attribution of Conduct: A Reply to Vladyslav Lanovoy,* European Journal of International Law 28:2 (2017)

229. Pomerlau M. *State and Non-state hackers: Different tactics, equal threat?* Public Sectors 360, Defense Systems(2015)

230. Pomerleau M. *What is ISR in non-physical domains*, C4ISRNET(2016)

231. Pont du G.F. *The Criminalisation of True Anonymity in Cyberspace,* Michigan Telecommunications and Technology Law Review tom 7:191 (2001)

232. Posner E.A., Lichtman D. *Holding Internet Service Providers Accountable*, John M. Olin Law & Economics Working Paper 217 (2004)

233. Post D. *Anarchy, State and the Internet: An Essay on Law-Making in Cyberspace* , Journal of Online 1995 3:44 (1995)

234. Post D., Johnson D. *Chaos Prevailing on Every Continent:Towards a New Theory of Decentralized Decision-Making in Complex Systems,* 73 Chicago-Kent Law Review (1998)

235. Post. D., Johnson D. *Law and Borders- The Rise of Law in Cyberspace,* 48 Stanford Law Review (1997)

236. Postel J., Zaw-Sing S., T*he Domain Naming Convention for Internet User Applications,* Network Working Group (1982)

237. R.Roman *Settling Sovereignty Claims over the Hans Island*, Masters of Public Policy and Global Affairs University of British Columbia (2016)

238. Rabello A.M. *Non Liquet - From Modern Law to Roman Law,* Annual Survey of International and Comparative Law 101:2 (2004)

239. Radbruch G. *Gesetzliches Unrecht und Uebergesetzliches Recht*, Sueddeutsche Juristenzeitung 46 (1946)

240. Radin S. *Global Armed Conflict? The Threshold of Extraterritorial Non-International Armed Conflicts,* US Navy War College, International Law Studies 89 (2003)

241. Rado G. *Legitimate Military Targets,* "The Crimes of War Project", The Humanitarian Law Series, Martinus Nijhoff Publishers(2013)

242. Radsan A.J. *The Unresolved Equatio of Espionage and International Law*, Michigan Journal of International Law 28:3(2007)

243. Ramcharan R. *ASEAN and Non-interference: A Principle Maintained ,* Contemporary South Asia 22 (2000)

244. Raport amerykańskiego DHS (Department of Homeland Security) *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense - in - Depth Strategies*. Industrial Contorol Systems Cyber Emergency Response Teams (2016)

245. Reagan R. *Statement on United States Oceans Policy*, Administration of Ronald Reagan, Public Papers, National Archives and Records Administration (1983).

246. Reidenberg J.R. *Lex informatica: The formulation of Information Policy Rules through technology,* Texas Law Review 76:553; (1998)

247. Reindl A.P. *Choosing Law in Cyberspace: Copyright Conflicts on Global Networks,* Michigan Journal of International Law 19:3 (1998)

248. Reisman W.M. *Criteria for the Lawful Use of Force in International Law,* Yale Journal of International Law 10 (1985)
249. Rivkin D.W. *The importance of extraterritorial jurisdiction*, International Bar Association Report of the Task Force on Extraterritorial Jurisdiction (2017)
250. Rivkin Jr. D.B. i Casey L.A. *The rocky shoals of international law,* The National Interest 35 (2000/2001)
251. Robillard N. *Diffusing a Logic Bomb,* SANS Institute (2004).
252. Rollins J., Henning A.C. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations,* Congressional Research Service 5 (2009)
253. Rooney J.M. *The Relationship between Jurisdiction and Attribution after Jaloud v. Netherlands,* Netherlands International Law Review 62-3 (2015)
254. Rostow E.V. *The Legality of the International Use of Force by and from States* , Yale Law School Faculty Scholarship Series, Paper 21:28 (1985)
255. Sabanal dal P. *Thingbots: The future of Botnets in the Internet of Things*, IBM Security Intelligence (2016)
256. Saffo P. *Disrupting Undersea Cables: Cyberspace's Hidden Vulnerability* Atlantic Council (2013)
257. Sagliocca A. *Cambrigde Analytica and Big Data: where are we now? Some post-scandal reflection on the Data Analytics and Political Consulting Gain* Ingenium, (2018)
258. Samie N. *The Doctrine of "Effects" and the Extraterritorial application of Antitrust Laws,* University of Miami Inter-American Law Review 14:23(1982)
259. Sanger E., Kickpatrick D., Perlroth N. *The World Once Laughed at North Korean Cyberpower. No More,* New York Times 16.XI.17 (2017)
260. Santarelli N.C.*Non-state Actor's Human Right obligations and responsibility under international law,* Revista Electronica de Estudios Internacional 13 (2013)
261. Schachter O. *In Defense of International Rules on the Use of Force,* University of Chicago Law Review 53:113 (1986)
262. Scharf M.P. *Aut dedere aut iudicare,* Max Plack Stiftung, MPEPIL (2011)
263. Scheinpflug Ch. *The Global Civic Society as normative entity?* GRIN Geistenwissenschaft (2012)
264. Schimmer L., ZZZ (autor pozostał anonimowy) *Peer Profiling and Selection in the I2P Anonoymous Network* PET-CON (2009)

265. Schmithoff C.M. *Das neue Recht des Welthandels,* Rabel Journal of Comparative and International Law, Private Law 28, Mohr & Siebeck (1964)
266. Schmitt M. *Cyber Operations in International Law: The use of Force, Collective Security, Self-Defense and Armed Conflicts Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Option for U.S.Policy* National Academic Press (2010)
267. Schmitt M., Biller J. *The NotPetya Cyber Operation as a Case Study of International Law,* European Journal of International Law, EJIL:Talk!11/17 (2017)
268. Schmitt M., Vihul L. *Respect for Sovereignty in Cyberspace,* Texas Law Review 7:95 (2018)
269. Schmitt M.N. '*The Use of Force' in Cyberspace:A Reply to Dr Ziolkowski,* NATO CCD COE Publications (2012)
270. Schmitt M.N. *Computer Network Attack and the Use of Force in International Law: Thoughts on Normative Framework,* Columbia Journal of International Law 37 (1999)
271. Schmitt M.N. Computer Network Attack and the Use of Force in International Law: Thoughts on Normative Framework, Columbia Journal of International Law 37 (1999)
272. Schmitt M.N. *Cyber Operations and the Jus Ad Bellum Revised*, 56 VIII Villanova Law Review, Charles Widget School of Law Digital Resources 569 (2011)
273. Schmitt M.N. *In Defense of Due Dilligence in Cyberspace,* The Yale Law Journal Forum 125:68 (2015)
274. Schmitt M.N. *International Law and Cyber Attacks: Sony v. North Korea*, justsecurity.org 17/12/18 (2018)
275. Schmitt M.N., Vihul L. *International Cyber Law Politicized: The UN GGE's Failure to Advance Cybernorms*, Just Security 30/06/17 (2017)
276. Schmitt M.N., Vihul L. *The nature of International Law CyberNorms*, Tallinn Paper 5 (2014)
277. Schmitt M.N., Vihuul L. *Respect for Sovereignty in Cyberspace*, Texas Law Review 95 (2017)

278. Schmitt M.N.*Cyber Operations and the Jus in Bello: Key Issues,* Naval War College International Law Studies 40 (2011)

279. Schmitt. M, Maurer T. *Protecting Financial Data in Cyberspace: Precedent for Further Progress on Cyber Norms?* JustSecurity 28/08/17 (2017)

280. Schmurer E.B. *E-stonia and the Future of the Cyberstate: virtual governments come online,* Snapshot 28/01/15 (2015)

281. Seong-Hun, Byung-Hyun L.,Sung-Hyuck I.Gyu-In Jee *Effect of Spoofing on Unmanned Aerial Vehicle using Counterfeited GPS Signal,* Journal of Postitioning Navigation and Timing 4:2 (2015)

282. Shachtman N. *Kremlin Kids: We Launched the Estonian Cyber War,* Wired, Inside Cyberwarfare (2012)

283. Shackelford S. *When it comes to Cyber Security, Passive Defence is Best,* Indiana University, The Conversation (2019)

284. Shalini M.Budapest *Convention on Cybercrime - An Overview*, New Dehli Center for Communicaton Governance, International Law and Policy & Emerging Tech nad National Security 3/3/16 (2016)

285. Shen Y. *Cyber Sovereignty and the Governance of Global Cyberspace,* Chinese Political Sciences Review 1/16 (2016)

286. Silver D.B. *Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter,* International Law Studies 76 (2014)

287. Silver D.B. Computer Network Attack as a Use of Force under Article 2(4) of the United Nations Charter.International Law Studies 76 (2014)

288. Simon C. *The technical Construction of Globalism Internet Governance and DNS Crisis*, rkey.com (2005)

289. Singh P. A *Death Knell for the International Norms of Cyber Conflict* Modern War Institute (2019)

290. Solum L.B., Minn Ch. *The Layers Principle: Internet Architecture and the Law,* 79 Notre Dame Law Review, 815 (2004)

291. Sommer J.H. *Against Cyberlaw,* Berkeley Technology Law Journal 3:15 (2000)

292. St.John D.*The Bogota Declaration and the Curious Case of Geostationary Orbit*, Denver Journal of International Law and Policy 1/13(2013)

293. Stahl W.M. *The Uncharted Waters of Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cyerbsecurity.* Georgia Journal of International and Comparative Law 40 (2008)

294. Stang G. *Global Commons: Between cooperation and competition* Brief Issue 17, European Union Institute for Security Studies, (2013)

295. Stauffacher D., KavanaghC. *Confidence building measures and international cyber security,* Cyber Policy Process Brief, ICT for Peace Foundation (2013)

296. Stefik M *Shifting the Possible: How trusted systems and Digital Property Challenge Us to Rethink,* Digital Publishing Berkley Technical Law Journal 12:137 (1997)

297. Stefik M. *Letting Loose the Light:Igniting Commerce in Electronic Publication,* Internet Dreams: Archetypes, Myths and Metaphors 219 (1996)

298. Stemler A. *Regulation 2.0: The Marriage of New Governance and Lex Informatica,* Vanderbildt Journal of Entertainment and Technology 19:1 (2016)

299. Stemler A., Regulation 2.0: The Marriage of New Governance and Lex Informatica,Vanderberg Journal of Entertainment and Technology Law, t. XIX:1,110 (2016)

300. Stone J. *Non Liquet and the Function on Law in International Community* 35 British Yearbook of International Law.(1959)

301. Sukosd M. *Policy and Marketing Strategies for Digital Media* Routledge, Taylor and Francis (2014)

302. Sulmasy G. *Counterintuitive: Intelligence Operations and International Law* Berkeley Law Scholarship Repository 1:1(2006)

303. Swedin E.G. *Science in the Contemporary World:an Encylopaedia,* ABC-CLIO(2005)

304. Symeonides C. *Choice of Law in the American Courts in 1995: A Year in Review* , American Journal of Competitive Law 44:181 (1996).

305. Tamanaha B. Z. *How an Instrumental View of Law Corrodes the Rule of Law,* 56 DePaul University Law Review 469 (2007)

306. Tanenbaum M. *Kinetic War vCyber War: The Potential Battlefields Ahead,* MSSPALert, (2018)

307. Tarjanne F. *Internet Governance: Towards Voluntary Mulilateralism, Internet Domain Names: Informations Session, Meeting of Signatories and Potential*

Signatories of the Generic Top Level Domain Memorandum of Understanding, ITU Geneva (1997)

308. Thompson L. *Cyber Alliances: Collective Defense Becomes Central To Securing Network, Data,* Forbes (2014)
309. Thompson L. Cyber Alliances: Collective Defense Becomes Central To Securing Networks, Data, Forbes (2014)
310. Thumfart J. *Francisco de Vitoria and the Nomos of the Code: The Digital Commons and Natural Law, Digital Communication as a Human Right* Just Cyberwarfare, Springer International Publishing, tłumaczenie - Harris E.(2017)
311. Ticehurst R. *The Martens Clause and the Laws of Armed Conflict*, International Review of the Red Cross 317 (1997)
312. Toomey P. *The NSA continues to violate Americans* Internet Privacy Rights, ACLU National Security Project (2018)
313. Trachtman, J. *Cyberspace, Sovereignty, Jurisdiction, and Modernism* Indiana Journal of Global Legal Studies: 5:2 (1998),
314. Trakman L. *The Law Merchant : The Evolution of Commercial Law,* Fred B. Rothman Publishing (1983).
315. Trakman L. The Law Merchant: The Evolution of Commercial Law, Fred B. Rothman & Co. (1983)
316. Treves T. *Piracy,Law of the Sea, and Use of Force: Developments off the Coast of Somalia,* European Journal of International Law 20 (2009)
317. Ulpian, *Komentarze do Edyktów* (Digesta Justiniana 50.17.54)
318. Valdar A. *Understanding Telecommunications Networks,* London Institute of Enigineering and Technology Publishing (2006)
319. Vamosi R. *The man who changed internet security,* CNET (2008)
320. Walters L.G. *Online Casino Risk. A safe bet or risky business?* Walters Law Group (2019)
321. Waxman M.C. *Cyberattacks and the Use of Force: Back to the future of article 2(4),* Yale Journal of International Law 36:2 (2011)
322. Weitzenboeck E. M. *Hybrid net: the regulatory framework of ICANN and the DNS*, International Journal of Law and Techonolgy 22:1 (2014)
323. Williams B.T. *The Joint Force Commander's Guide to Cyberspace Operations*, Joint Forces Quaterly nr 23 (2014)

324. Williamson M. Terrorism, *Was and International Law: The Legality of Use of Force Against Afghanistan in 2001,* Liverpool Law Review 31 (2010).

325. Wilson G.G. *Use of Force and War,* American Journal of International Law 26 (1932)

326. Worster W. *Law, Politics, and the Conception of the State in State Recognition Theory,* Boston University Law Journal 27:115(2005)

327. Worster W. *Sovereignty Two Competing Theories of State Recognition,* Exploring Geopolitics 2/10 (2010)

328. Worster W.Th. Law, *Politics and the Conception of the State in State Recognition Theory,* Boston University International Law Journal 27:115 (2009)

329. Worster William *Sovereignty Theories of State Recognition,* Exploring Geopolitics wyd. I/15 (2015)

330. Wortham A. *Should Cyber Exploitation Ever Consitute a Demonstration of Hostile Intetn That May Violate UN Charter Provisiones Prohibiting the Threat or Use of Force,* Federal Communications Law Journal 64:3 Maurer School of Law: Indiana University (2012)

331. Wright A., de Flippi P. *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN,(2015)

332. Wright Q. *When does war exist?*, American Journal of International Law,26:2 (1932)

333. Wu T. *Cyberspace Sovereignty?-The Internet and International System,* Harvard Journal of Law and Technology, 10:3 (1997)

334. Wu T. *Cyberspace Sovereignty?-The Internet and the International System*, 10 Harvard Journal of Law and ARV. J.L. & TECH. 647, 648 (1997)

335. Wu T., *Cyberspace Sovereignty? The Internet and the International System,* Harvard Journal of Law and Technology 10:647 (1997)

336. Wu, T. *When Code Isn't Law,* Virginia Law Review 89 (2003);

337. Yang C. *Law Creeps onto Lawless Net*, Business Week 56 (1994)

338. Yoo J. *War by other means: an insider account on war on terror,* Atlantic Monthly Press 1st ed. (2006)

339. Yousof I.Katsumata H. *From "Non-interference" to "Open and Frank Discussions,* Asian Survey, 44:2 (2004)

340. Zbiorowa, red Cameron L., Demeyere B.,H. La Haye E., Lackner-Niebergall H. *The updated Commentary on the First Geneva Convention-a new tool for generating respect for international humanitarian law*, International Review of The Red Cross, 97 (2015)
341. Zbiorowa, Oracle Big Data,Integrated Cloud Applications
342. Zbiorowa,red. Czossek C., Ziolkowski K., Ottis R *International Conference on Cyber Conflict*, NATO CCD COE Publ. Tallin (2012).
343. Zbiorowa, *The Icefog Apt: A Tale of Cloak and Three Daggers*, Raport Kaspersky Lab Zero (2013).
344. Zbiorowa, *Tracking GhostNet:Investigating a Cyber Espionage Network Information Warfare Monitor*, Munk Centre for International Studies, Univeristy of Toronto Law Review48 (2009)
345. Zdrnja B. *An Israeli patriot program or a trojan?* InfoSec Diary Handlers Blog (2009).
346. Zemanek K. *Armed Attack* , Max Planck Stiftung, MPEPIL(2012)
347. Zetter K. *Hacker Lexicon: BotnetThe Zombie Computer Armies that Earn Hackers Millions*, Wired/Security (2015)
348. Zhang W. *Extraterritorial Jurisdiction on Celestial Bodies,* Elsevier Space Policy 47 (2019)
349. Zied T.,Khemakhem M. *Sybil Nodes as a Mitigation Strategy against Sybil Attack,* Procedia Computer Science 32 (2014)
350. Zimmermann A. *International Law and 'Cyber Space'*, European Society of International Law Reflections 3:1 (2014)
351. Ziolkowski K. *Ius ad bellum in Cyberspace-Some thoughts on the "Schmitt-Criteria" for Use of Force,* NATO CCD COE Pub Tallinn.(2012)
352. Zipporah B.W. *The Limits of Vision of Karl Llewelyn and the Merchant Rules*, 100 Harvard Law Review 465(1987).

Autorsko wyodrębnione części publikacji zbiorowych

1. Arimateu L. *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations* [w: zbiorowa red. Czosseck C., Ottis R, Ziolkowski K. *4th*

International Conference on Cyber Conflict NATO CCD COE Publications, (2012)

2. Barsotti R. *Armed Reprisals* [w: zbiorowa, red. Gazzini T., Tsagourias N. *The Use of Force in International Law* Routledge (2012)]
3. Bussolati N. *The Rise of Non-state actors in Cyberwarfare*, [w:zbiorowa, red. Ohlin J.D., Govern K., Filnkelstein Cl. *Cyber War: Law and Ethics for the Virtual Conflicts* Oxford University Press (2015)]
4. Chung, K., Kalbarczyk, Z. T., & Iyer, R. K. *Indirect cyber attacks by perturbation of environment control: A data driven attack model* HotSoS 2018 [w: *Annual Symposium and Bootcamp on Hot Topics in the Science of Security* Raleigh, USA (2018)]
5. Clapham A. *Non-state Actors* [w: zbiorowa, red. Chetail V. *Post-Conflict Peacebuilding: A Lexicon* Oxford University Press (2009)]
6. Corn P.G., Talyor R., *Soveregnity in the Age of Cyber* [w: zbiorowa, red. Corn P.G., Taylor R. *Symposium on Sovereignty, Cyberspace and Tallin Manual 2.0* The American Society of International Law, American Journal of International Law Unbound 111 (2017)]
7. DeWeese G.S. *Anticipatory and Preemptice Self-Defense in Cyberspace: The Challenge of Imminence* [w: zbiorowa, red. Maybaum M., Osula A-M, Lindstroem L. *Architectures in Cyberspace* NATO CCD Center of Excellence, Tallinn (2015)
8. Dinstein Y. *Legitimate Military Objective Under The Current Jus In Bello*. *The principle of distinction and military objectives* [w:zbiorowa, red. A.E. Wall *Legal and Ethical Lessons of NATO Kosovo's campaign* International Law Studies 78 (2016)
9. Eberlin Ph. Gasser H.-P., Wenger Cl.F. [w: zbiorowa,*Komentarz do Protokołów Dodatkowych do Konwencji Genewskich* red. Sandoz Y., Swinarski Ch., Zimmermann B. International Committee of the Red Cross, wyd. Martinus Nijhoff Publishers, Genewa (1987)]
10. Ekstedt V., Parkouse T., Clemente D. *Commitments, Mechanisms & Governance* [w:zbiorowa, red. Klimburg A. *National Cyber Security* Framework Manual NATO Cooperative Cyber Defence Centre of Excellence, Tallinn(2018)]

11. Feld H. *Structured to Fail: ICANN and the 'Privatization'Experiment* [w:zbiorowa, red. Thierer A.D., Wayne C. *Who Rules the Net?:Internet Governance and Jurisdiction* Cato Institute(2003)]
12. Geldenhuys D. Origins of Contested Statehood [w:zbiorowa, red. Geldenhuys D. *Contested States in World Politics*, Palgrave Macmillan(2009)]
13. Glueck Sh. *Crimes Against Humantiy* [w: zbiorowa, red. Mettraux G. *Perspectives on Nuremberg Trials*,Oxford University Press (2008)]
14. Hartmann A., Giles K. *UAV Exploitation: A New Domain for Cyber Power* 8th International Conference on Cyber Conflict [w: zbiorowa, red. Pissanidis N., Roigas H., Veenendaal M. *Cyber Power* NATO CCDCOE Publications (2016)
15. Heinegg v. W.H. Legal Implications of Territorial Sovereignity in Cyberspace[w: zbiorowa, red. Czossek C., Ziolkowski K., Ottis R. 4th International Conference on Cyber Conflict NATO CCD COE Publications(2012)]
16. Herrera G.L. *Cyberspace and Sovereignty: Thoughts on Physical Space and Digital Space* 12 wykład wygłoszony na 47 konwencji rocznej Towarzystwa Studiów Międzynarodowych (ISA Convention),[w: zbiorowa, red. Cavelty M.D., Mauer V., Krishna- Hensel S.F. *Power and Security in the Information Age* Routledge(2008)
17. Kranz J. *Suwerenność państwa i prawo międzynarodowe* [w: zbiorowa, red. Wołpiuk W.J. *Spór o suwerenność* Wydawnictwo Sejmowe (2001)]
18. Lindquist S.A, Cross F.C.Stability, Predictability And The Rule Of Law [w: zbiorowa, red. Cross F.C., Lindquist S.A. *Stare Decisis As Reciprocity Norm*, University of Texas Law School Press (2007)]
19. Mačák K. *Is the International Law of Cyber Security in Crisis?* [w:zbiorowa, red. Pissanidis N., Rõigas H., Veenendaal M. *8th International Conference on Cyber Conflict Cyber Power* NATO CCD COE Publications (2016)]
20. Marchetti R. *Modes of Governance for the Global Commons*[w:zbiorowa, red. Catalano C. *Global Commons: threat or opportunity* Finmeccanica (2013)]
21. Matza C., Kosinski M., Navec G., Stillwell D.J. *Psychological targeting as an effective approach to digital mass persuasion* [w: zbiorowa, red. Fiske T. *Proceedings of National Academy of Science* 117:48 (2017)]

22. Meyer P. *Outer Space and Cyberspace: A Tale of Two Security Realms* [w: zbiorowa, red. Osula A.M., Roigas H. *International Cyber Norms: Legal, Policy & Industry Perspectives* NATO CCD Centre of Excellence(2016)]
23. Pasch J. *State Obligation to Punish Core International Crimes and the Proposed Crimes against Humanity Conventions* [w: zbiorowa, red. Bergsmo M., Tianying T. *On the proposed Crimes against Humanity Convention* FICHL Publication Series 18 (2014)
24. Riccardi A., Natoli T. *Borders and International Law: Setting the Stage*[w: zbiorowa, red Natoli T., Riccardi A. Borders, L*egal Spaces and Territories in Contemporary International Law*, Springer (2019)]
25. Ryngaert C.- T*he Concept of Jurisdiction in International Law*,[w:zbiorowa, red. Orakhlelashvili *A.Research Handbook on Jurisdiction nad Immunities in International Law* Research Handbooks in International Law series, Edward Elgar Publishing (2009)
26. Sander B.T*he Sound of Silence: International Law and the Governance of Peacetime Cyber Operations* [w: zbiorowa, red. Minarik T., Alatalu S., Biondi S., Signoretti M., Tolga I., Visky G. *11th International Conference on Cyber Conflict Silent Battle* NATO CCD COE Publications (2019)
27. Schmitt M. *Targeted Killings and International Law: Law Enforcement, Self-Defense*[w:zbiorowa red. Arnold R., Quenivet N., *International Humanitarian Law and Human Rights Law. Towards a New Merger in International Law* Martinus Nijhoff Publishers (2008)]
28. Shackelford J., Anders R.B. *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem* [w:zbiorowa, red. Czosseck C., Podins K. Conference on Cyber Conflict Proceedings, CCD COR Publications (2010)]
29. Stockburger P.Z. *From Grey Zone to Customary International Law: How adopting the Precautionary Principle may help crystalize the due dilligence principle in Cyberspace* 10th International Conference on Cyber Conflict [w: zbiorowa,red. Minarik T., Jakschis R., Lindstroem L. *CyCon X Maximising Effects*, NATO CCD COE Publications (2018)
30. Strange S. *The Westfailure System* [w:zbiorowa red. Cox M. *20th Century International Relations* SAGE, (2007)

31. Wood, M. *Use of Force, Prohibiton of Threat* [w: zbiorowa, red. Wolfram R. Max Planck Stiftung (2013)

Akty prawa krajowego i unijnego,

1. Claryfing Lawful Overseas Use of Data Act (*CLOUD Act*), H.R.4943 (115th) Pub.L 115-141 U.S.C. 2523 (2017-2018)
2. Communications Decency Act, 47 U.S.C. §230 (1997)
3. Consolidated Approprations Act,(2019-2020) H.R.648 (116th), Pub.L. 115-41, §2701 U.S.Code.
4. Digital Millenium Copyright Act (*DCMA Act*) *(*112th) Stat. 2860 (1998), Pub.L. 105-304
5. Dyrektywa Parlamentu Europejskiego i Rady 2004/460 z dnia 10 marca 2004 roku ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji. Dz. Urz UE syg. L077
6. Dyrektywa Parlamentu Europejskiego i Rady 2016/1148 z dnia 6 lipca 2018 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii. Dz. U. syg. UE L 194/1
7. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2000/31 z dnia 8 czerwca 2000 roku w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego. pub. w Dz. Urz. UE z 17 lipca 2000, syg. L/178, CELEX32000L0031
8. Federal Cybersecurity Enhancement Act (2016) H.R. 2029 (114th) S. 1869 Rep. 114-378
9. Federal Information Security ManagementAct (2002) (107th) 44 U.S.C.(35)(III) §3541
10. Federal Infrastructure Safety Act Amendment (2008) H.R. 6304 (110th) P. Law 110-261
11. FISA Amendments Act, H.R. 6304 (2008) (110th) Pub. L.110–261 U.S.C. 50 (36) §1801

12. Foreign Intelligence Surveillance Act 1978 (95th) 50 U.S.C. (36) §1801
13. FOSTA-SESTA Act (2018), H.R.1865 115th Con. (2017-2018);
14. Homeland Security Presidential Directive-23 (2008)
15. Karta Praw Podstawowych Unii Europejskiej ogłoszona przez Parlament Europejski Radę i Komisję 30 marca 2010 roku, Dz. U. UE syg.2010/C 83/02
16. Konwencja o jurysdykcji i uznawaniu oraz wykonywaniu orzeczeń sądowych w sprawach cywilnych i handlowych, podpisana w Lugano 16 września 1988 roku Dz.U. 2000 nr 10 poz. 132
17. National Cybersecurity and Communications Integration Centre Act (2014) U.S.C. 659 014
18. National Cybersecurity and Critical Infrastructure Protection Act (2014) (113th). H.R. 3696
19. National Security Presidential Directive-54/ Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) (2008)
20. Presidential Decision Directive 63 PDD NSC 63 (1998)
21. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/2120 z dnia 25 listopada 2015 r. ustanawiające środki dotyczące dostępu do otwartego internetu oraz zmieniające dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, a także rozporządzenie (UE) nr 531/2012 w sprawie roamingu w publicznych sieciach łączności ruchomej wewnątrz Unii . opublikowane w Dzienniku Urzędoweym UE, Dz.U. pod syg. L 310 z dnia 26 listopada 2015,1-18, nr CELEX 32015R2120
22. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu ich danych oraz uchylenia dyrektywy 95/46/WE (Ogólne Rozporządzenie O Ochronie Danych) Dz. Urz.UE syg. L 119/1, CELEX 32016R0679
23. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12

grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych, publikacja w Dz.U. UE L 351/1,CELEX 3A32012R1215

24. Regulacja Parlamentu Europejskiego i Rady z grudnia 2012 o syg. 1215/2012 w sprawie jurysdykcji i uzanawania orzeczeń sądowych oraz ich wykonywania (tzw. Bruksela I).Dz.U UE L 351, z 20 grudnia 2012 roku.
25. Telecommunications Act of 1996, 47 U.S.C. §230,17 USC §512 (1996)
26. Trusted Internet Connections Initiative OMB M-08-16, M-08-05 (2007)
27. US Departament of Defense Directive *Use of International Airspace by U.Military Aircraft and for Missile and Projectile Firings*, 4540.1 (2015)

Umowy międzynarodowe

1. *Konwencja Rady Europy o Cyberprzestępczości*, podpisana w Budapeszcie 23 października 2001 roku, ETS-185 (*Konwencja Budapesztańska*)
2. *Konwencja Rady Europy o Cyberprzestrzstępczości* - Protokół Dodatkowy przyjęty 28 stycznia 2003 w Strasbourgu, 6 ETS-189
3. *Traktat z Cotonou*, zawarty 23 czerwca 2000 roku pomiędzy Unią Europejską a krajami Grupy ACP (Africa, Caribbean, Pacific)
4. *Traktat Webster- Ashburton,* zawarty 9 września 1842 pomiędzy Stanami Zjednoczonymi a Zjednoczonym Królestwem
5. *Summaries of Conventions, Treaties and Agreements administered by WIPO*. Publikacja WIPO nr. 442E/13, Genewa (2013)
6. *Układ o zasadach działalności państw w zakresie badań i użytkowania przestrzeni kosmicznej łącznie z Księżycem i innymi ciałami niebieskimi* zawarty 27 stycznia 1967 roku pomiędzy Stanami Zjednoczonymi, Wielką Brytanią i Związkiem Sowieckim, prawomocny od 10 października 1967 (*Traktat o Przestrzeni Kosmicznej*)

7. *Konwencja Narodów Zjednoczonych o Prawie Morza*, zawarta 10 grudnia 1982 roku w Montego Bay, prawomocna od 16 listopada 1994, Dz. U. 2002 nr 59 poz. 543 (także jako *United Nations Convention on the Law of the Sea- - UNCLOS*)
8. *Rzymski Statut Międzynarodowego Trybunału Karnego* sporządzony w Rzymie dnia 17 lipca 1998
9. *Statut Międzynarodowego Trybunału Sprawiedliwości* Dz.U 1947 23 poz. 90
10. *Konwencja o Prawach i Obowiązkach Państw,* sygnowana w Montevideo 26 grudnia 1933 roku, podczas 7 Międzynarodowej Konferencji Państwa Amerykańskich, prawomocna od 26 grudnia 1934 roku (*Konwencja z Montevideo)*
11. *Paris Call for Trust and Security in Cyberspace*, Deklaracja UNESCO z 12 października 2018 roku
12. *Międzynarodowa Konwencja O Morzu Pełnym*,zawarta w Genewie dnia 29 kwietnia 1958 r.,Dz.U. 1963 nr 33 poz. 187
13. *Konwencja o szelfie kontynentalnym*, sporządzona w Genewie dnia 29 kwietnia 1958 roku, Dz.U. 1964 nr 28 poz. 179
14. *Konwencja Wiedeńska o Prawie Traktatów,* sporządzona w Wiedniu dnia 23 maja 1969 Dz.U. 90 nr 74 poz. 439
15. *Konwencja międzynarodowa o ochronie kabli podmorskich,* sporządzona w Paryżu 14 marca 1884 roku, Dz. U. 1935 nr 17 poz.97
16. *Karta Narodów Zjednoczonych*, podpisana 26 czerwca 1945 roku w San Francisco, wejście w życie 24 października 1945 roku, Dz. U. 1947nr 23 poz. 90
17. Konwencje Genewskie z dnia 12 sierpnia 1949 o ochronie ofiar wojny, Dz.U. 1956 nr 38 poz. 171
18. Protokół Dodatkowy do Konwencji Genewskich z dnia 12 sierpnia 1949 o ochronie ofiar wojny, dotyczący ochrony ofiar międzynarodowych konfliktów zbrojnych sporządzony 8 czerwca 1977 w Genewie (*I Protokół Dodatkowy*) Dz.U. 1992 nr 41 poz. 175
19. Protokół Dodatkowy do Konwencji Genewskich z dnia 12 sierpnia 1949 o

ochronie ofiar wojny, dotyczący ochrony ofiar niemiędzynarodowych konfliktów zbrojnych sporządzony 8 czerwca 1977 w Genewie (*II Protokół Dodatkowy*) Dz.U. 1992 nr 41 poz. 175

20. Konwencja dotycząca praw i zwyczajów lądowej(II Konwencja Haska z 29 lipca 1899 roku) opublikowana w Dz. Ust. 1927 nr 21 poz. 161.
21. *Konwencja Haska o ochronie dóbr kultury w razie konfliktu zbrojnego* wraz z załącznikami podpisana w Hadze 14 maja 1954 (Dz.U. z 1957 nr 46 poz. 212 zał.)
22. *Konwencja w sprawie Międzynarodowych Przepisów o zapobieganiu zderzeniom na morzu*, podpisana w Londynie w 1972 roku. Dz.U. 1977 nr 15 poz. 61).*(COLREG)*
23. *Konwencja z Lugano* z dnia 16 września 1988 r. o jurysdykcji i wykonywaniu orzeczeń sądowych w sprawach cywilnych i handlowych
24. Konwencja dotycząca praw i zwyczajów wojny lądowej, podpisana w Hadze 29 czerwca 1899 roku, weszła w życie 4 września 1900 roku. *(Haga II)*
25. Konwencja dotycząca praw i zwyczajów wojny lądowej, podpisana w Hadze 18 października 1907 roku., Dz. U. 1927 nr 21 poz. 161*(Haga IV)*
26. *Karta Międzynarodowej Współpracy w sprawie Internetu*- projekt traktatu, nigdy nie sygnowany
28. Projekt Protokołu Dodatkowego do Konwencji Budapesztańskiej Konferencja *Octopus* Rady Europy, niesygnowany

Pozostałe źródła

1. Arkin W.M., Ivansevic B. *Civilian Deaths in the NATO Air Campaign* Raport Human Rights Watch (2000)
2. Building an Effective European CyberShield in EU Cooperation to the Next Level, Biuletyn Komisji Europejskiej/EPSC (European Political Strategy Centre) wyd. 24 (2017)
3. *Bylaws For Internet Corporation For Assigned Names And Numbers*- ICANN Board of Directors, (2018)
4. *Conduct of the Persian Gulf War. Final Report to Congress* (1992)

5. Curran J., Akplogan A.A. et al. *The Montevideo Statement on the Future of Internet Cooperation,* ICANN (2013)
6. *Deklaracja mocarstw uczestniczących w Kongresie Wiedeńskim z dnia 13 marca 1815 roku* British and Foreign State II. 663. Dig
7. Emmerson B. *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism,* Zgromadzenie Ogólne ONZ, A/HRC/25/59 (2014)
8. England G. *The strategy for Homeland Defense and Civil Support* US Departament of Defense (2005)
9. *Field Manual FM 34-52* United States Department of Army (2006)
10. *Field Manual FM2-23.3* United States Department of Army (2006)
11. *GDPR Working Group Report*, publikacja Komisji Europejskiej (2018)
12. Geuhenno J.-M. *Raport Rady Bezpieczeństwa ONZ z 18 września 2013 roku o sytuacji na granicy libańsko-izraelskiej* nr 5489, dnia 14 lipca 2006 roku.
13. *ICRC Databases on International Humanitarian Law*, Międzynarodowy Komitet Czerwonego Krzyża (2019)
14. Komunikat Sekretariatu Gabinetu Rady Ministrów Izraela z dnia 16 lipca 2006 roku
15. Lietzen I. *Third Facebook-Cambride Analytica Hearing: data breach prevention and cures* komunikat prasowy Parlamentu Europejskiego (2018)
16. Rezolucja Rady Bezpieczeństwa ONZ 1368/2001
17. Rezolucja Rady Bezpieczeństwa ONZ 1373/2001
18. Rezolucja Rady Bezpieczeństwa ONZ 487 z dnia 19 czerwca 1981.
19. European (Union)Network and Security Agency Securing data in cyber space, raport ENISA dla Komisji Europejskiej, 4, Heraklion (2013)
20. Rezolucja Zgromadzenia Ogólnego ONZ A/RES/20/2131 z 21 grudnia 1965 roku, tzw. *Declaration on the Inadmissabilitiy of Intervetnion in the Domestic Affairs of States and the Protection of their Independence and Sovereignty*
21. Rezolucja Zgromadzenia Ogólnego ONZ A/RES/36/103 z 9 grudnia 1981 roku.
22. Rezolucja Zgromadzenia Ogólnego ONZ A/RES/375(IV) z 6 grudnia 1949 ,
23. Scott K.D. et al. *Cyberspace Operations*, US Joint Chiefs of Staff, Joint Publications 3-21R (2018)
24. *The National Strategy to Secure Cyberspace*, USA Homeland Security, (2003)

25. *US Joint Chief of Staff Electronic Warfare Joint Publication* F.M. 3.13.-1 (2015)