Rozdział 12. Państwo neutralne w cyberprzestrzeni

Tomasz Srogosz

§ 1. Wprowadzenie

Pojęcie neutralności w prawie międzynarodowym kojarzone jest z paryskim aktem uznania i gwarancji wieczystej neutralności Szwajcarii i części Sabaudii z 20.11.1815 r. oraz art. 84 Aktu Końcowego Kongresu wiedeńskiego. Uznana przez mocarstwa neutralność Szwajcarii wiązała się z rzeczywistą przestrzenią, tj. terytorium państwowym, czego wyrazem był i nadal pozostaje nakaz poszanowania niepodległości i integralności terytorialnej. Potwierdziły to postanowienia V i XIII konwencji haskich (1907 r.) traktujące o prawach i obowiązkach mocarstw neutralnych w wojnie lądowej i morskiej[1]. Neutralność państwa sprowadza się m.in. do zakazu przeprowadzania wojska przez terytorium państwa neutralnego, zakazu zakładania i używania na jego terytorium urządzeń służących do komunikacji między siłami wojującymi, zakazu zaboru statku lub wykonywania prawa wizytacji na wodach terytorialnych państwa neutralnego, czy też wykorzystywania portów i wód neutralnych.

Dwieście lat po Kongresie wiedeńskim i ponad sto lat po podpisaniu konwencji haskich zmieniła się rzeczywistość stanowiąca tworzywo stosunków międzynarodowych i prawa międzynarodowego. Można nawet powiedzieć, że powstała nowa – wirtualna – nazywana cyberprzestrzenią lub piątym wymiarem. Państwa, jako uczestnicy stosunków międzynarodowych i podmioty prawa międzynarodowego, funkcjonują w niej, czego wyrazem są chociażby

[1] Konwencja dotycząca praw i obowiązków mocarstw i osób neutralnych w razie wojny lądowej (V Konwencja haska), Haga, 18.10.1907 r. (Dz.U. z 1927 r. Nr 21, poz. 163); konwencja dotycząca praw i obowiązków mocarstw neutralnych w razie wojny morskiej (XIII Konwencja haska), Haga, 18.10.1907 r. (Prawo międzynarodowe i historia dyplomatyczna. Wybór dokumentów, wstęp i opracowanie *L. Gelberg*, Warszawa 1954, t. I, s. 287–291).

strony internetowe urzędów państwowych. Bezpieczeństwo państwowe zależy od bezpieczeństwa w sieci. Nowym zjawiskiem są ataki cybernetyczne skierowane przeciwko władzom państwowym. W stosunkach międzynarodowych używa się coraz częściej pojęć cyberwojny, cybersabotażu, cyberterroryzmu lub cyberprzestępczości[2]. Ataki cybernetyczne stanowią jeden z elementów tzw. wojny hybrydowej. W związku z ewolucją stosunków międzynarodowych, rodzi się pytanie o pojęcie i znaczenie neutralności państwa we współczesnym prawie międzynarodowym. Czy utrwalona definicja neutralności państwa, ściśle związana z rzeczywistą przestrzenią stanowiącą terytorium państwowe, zdaje egzamin w dobie rewolucji cybernetycznej? Czy określone m.in. na Kongresie wiedeńskim pojęcie neutralności państwa wymaga redefinicji? Czy spełnia w XXI w. funkcję ochrony niepodległości i integralności terytorialnej państwa? Czy też może nie ma obecnie państw (wieczyście) neutralnych w rozumieniu prawa międzynarodowego? Aby odpowiedzieć na powyższe pytania należy przybliżyć cechy cyberprzestrzeni oraz nowe zjawiska cyberbroni, cyberataku, cyberwojny, konfrontując je z prawnomiędzynarodowym pojęciem siły zbrojnej. Powyższe rozważania zmierzają do ustalenia pozycji państwa neutralnego w cyberprzestrzeni. Czy silnie zakorzenione w postanowieniach Kongresu wiedeńskiego i konwencji haskich pojęcie neutralności chroni państwo w cyberprzestrzeni?

§ 2. Cyberprzestrzeń

Najczęściej cytowaną jest definicja cyberprzestrzeni sformułowana przez Departament Obrony USA, zgodnie z którą jest to „globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery"[3]. Jak wykazuje *J. Wasilewski*, mankamentem tej definicji jest pominięcie społecznej funkcji cyberprzestrzeni[4]. W istocie nie jest ona tylko fenomenem technologicznym, ale także

[2] Zob. np. konwencja o cyberprzestępczości, Budapeszt, 23.11.2001 r. (weszła w życie 1.7.2004 r.), European Treaty Series, Nr 185.

[3] Department of Defence Dictionary of Military and Associated Terms, s. 58, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (dostęp: 4.3.2016 r.), tłum. *J. Wasilewski*, Zarys definicyjny cyberprzestrzeni, Przegląd Bezpieczeństwa Wewnętrznego 2013, Nr 9 (5), s. 227

[4] *J. Wasilewski*, Zarys, s. 228.

społeczno-kulturowym. Cyberprzestrzeń jest obecnie jednym z fundamentów infrastruktury państwa oraz istotnym budulcem więzi społecznych, a w tym relacji politycznych. Współczesne państwo funkcjonuje w przestrzeni „realnej", jak i cyberprzestrzeni. Dotyczy to nie tylko polityki wewnętrznej, ale również międzynarodowej. Wszystkie urzędy państwowe, a w tym naczelne i centralne organy władzy oraz jednostki terenowe, korzystają z technologii IT. Dotyczy to sfery czysto informacyjnej, jak i wymiany danych między organami państwowymi lub obywatelami. Stąd też bezpieczeństwo państwa zależy również od bezpieczeństwa jego infrastruktury w cyberprzestrzeni. Dotyczy to wszystkich obszarów działalności, poczynając np. od służby zdrowia, poprzez ubezpieczenia społeczne, system podatkowy, porządek publiczny, wymiar sprawiedliwości, gospodarkę wodną i energetyczną, a kończąc na obronności. Można w XXI w. wyobrazić sobie paraliż państwa spowodowany zaburzeniem funkcjonowania infrastruktury cybernetycznej.

Technologia IT zmieniła społeczeństwa i narody, które zaczynają „wymykać" się władzy państwowej. Symbolem zmian jest maska *Guya Fawkesa*, kojarzona z ruchem internetowym *Anonymous*. Ma ona przypominać o anonimowości w sieci, sprzyjającej w walce z rządami (hasło ruchu brzmi – „obywatele nie powinni bać się swoich rządów, rządy powinny bać się swoich obywateli"). Anonimowość oraz wzmożona, trudna do kontroli komunikacja między użytkownikami Internetu, nieuznająca granic państwowych, jest obecnie wyzwaniem dla państw. Poza niepodważalną, pozytywną funkcją kulturową i komunikacyjną, sieć sprzyja negatywnym zachowaniom zagrażającym bezpieczeństwu państw, narodów i społeczeństw. Do cyberprzestrzeni przeniesione zostały wszystkie sfery działalności człowieka, a w tym przestępczość, której odcienie kojarzą się m.in. ze zbrodniami międzynarodowymi i aktami terrorystycznymi. W cyberprzestrzeni funkcjonują organizacje terrorystyczne (np. Al-Kaida, Państwo Islamskie). Stała się ona również polem zmagań między państwami, zarówno w codziennej polityce i rywalizacji, jak i w związku z konfliktami zbrojnymi.

Biorąc pod uwagę powyższe, na potrzeby niniejszego artykułu można skonstruować definicję cyberprzestrzeni obejmującą nie tylko aspekty technologiczne, ale również społeczne, czy też politologiczne. Korzystając z definicji Departamentu Obrony USA można powiedzieć, że cyberprzestrzeń jest to globalna domena środowiska informacyjnego składająca się z współzależnych sieci tworzonych przez infrastrukturę technologii informacyjnej (IT) oraz zawartych w nich danych, włączając Internet, sieci telekomunikacyjne, systemy komputerowe, a także osadzone w nich procesory oraz kontrolery, stanowiąca

odrębną od rzeczywistej, a w tym pozbawioną podziału na granice administracyjne lub międzynarodowe, przestrzeń społeczną, kulturową, czy też politologiczną, w której zachodzą relacje społeczne, a w tym międzynarodowe. W ramach cyberprzestrzeni funkcjonuje m.in. wspólnota międzynarodowa, a więc zachodzą regulowane prawem międzynarodowym stosunki między państwami lub innymi podmiotami tegoż prawa[5]. Nową cechą tych stosunków jest oderwanie od przestrzeni wyznaczonej przez terytorium państwowe i granice międzynarodowe. Przenikają one Internet, sieci telekomunikacyjne i systemy komputerowe bez odniesienia do mapy politycznej świata. Droga jaką pokonują dane jest najczęściej trudna do ustalenia, tak jak i źródło ich pochodzenia. W sieci mieszają się bowiem użytkownicy prywatni z publicznymi, co sprawia, że stosunki międzynarodowe wymykają się ze znanej do tej pory przestrzeni operacyjnej, w której dominowały państwa.

Cyberprzestrzeń nie została zdefiniowana w prawie międzynarodowym, ale wydaje się, że nie ma takiej konieczności, skoro jest to raczej fenomen socjologiczny i jako taki powinien być definiowany przez socjologów lub politologów. Wyzwaniem pozostaje uregulowanie poszczególnych aspektów działalności podmiotów prawa międzynarodowego w piątym wymiarze. Przykładem jest tu konwencja o cyberprzestępczości. Należy zastanowić się chociażby nad prawem konfliktów zbrojnych, a w tym pojęciem neutralności. W stosunkach międzynarodowych toruje sobie bowiem drogę nowe zjawisko – cyberwojny.

§ 3. Cyberwojna a użycie siły zbrojnej

Cyberwojna jest terminem nie do końca ścisłym. Nawiązuje do pojęcia „wojny" (konfliktu zbrojnego) i „cyberprzestrzeni". Upraszczając można zatem powiedzieć, że jest to „wojna toczona w cyberprzestrzeni". Trudność polega na tym, że wojna (konflikt zbrojny) sprowadza się do użycia siły zbrojnej. Mimo że pojęcie konfliktu zbrojnego uległo ostatnio ewolucji obejmując tzw. „wojny asymetryczne", czyli z udziałem podmiotów niepaństwowych (np. grup terrorystycznych), to nadal jego cechą jest użycie broni celem fizycznego wyeliminowania sił zbrojnych przeciwnika. Czy zatem atak cybernetyczny można traktować jako użycie siły zbrojnej, a w tym broni? Czy można mówić o tzw. „cyberbroni"? Praktyka w tym zakresie dopiero się kształ-

[5] Por. *M. Lakomy*, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Katowice 2015, s. 11.

tuje. Przykładem jest reakcja Estonii na cyberatak w 2007 r. Estoński minister obrony rozważał kwestię samoobrony indywidualnej lub zbiorowej przed atakiem zbrojnym na podstawie art. 5 Paktu Północnoatlantyckiego[6]. Jednak ministrowie państw NATO odmówili potraktowania cyberataku jako okoliczności wymagającej akcji zbrojnej w ramach samoobrony zbiorowej. W konsekwencji również rząd estoński zmienił kurs, kwalifikując w ostateczności cyberatak jako akt terrorystyczny, a nie użycie siły zbrojnej w rozumieniu prawa międzynarodowego. Trudno zresztą potraktować za użycie siły zbrojnej działań hakera, nawet na zlecenie rządu, który przeprowadza cyberataki z prywatnego mieszkania. Fizycznie mogą one pochodzić z każdego zakątka globu, poruszającego się pociągu pasażerskiego, prywatnego samochodu itp. Z drugiej strony podkreśla się, że pojęcie siły zbrojnej w rozumieniu art. 2 ust. 4 KNZ może obejmować operacje cybernetyczne. Decydujący jest tu bowiem skutek w postaci realnych zniszczeń dokonanych w celu wyeliminowania przeciwnika. Rozwój technologii cybernetycznych umożliwił przeprowadzenie operacji w postaci przesłania danych, których następstwem jest zakłócenie chociażby systemów decydujących o bezpieczeństwie w komunikacji. Skutkiem takiego „cyberataku" może być przykładowo katastrofa samolotu cywilnego lub wojskowego, porównywalna do sytuacji użycia broni kinetycznej (tradycyjnej). Zwolennicy takiego rozumowania przywołują fragment opinii doradczej MTS w sprawie legalności groźby lub użycia broni jądrowej, w której stwierdzono, że międzynarodowe prawo humanitarne stosuje się do „wszystkich form wojny i wszystkich form broni, zarówno tych z przeszłości, teraźniejszości, jak i przyszłości" pomimo różnic ilościowych i jakościowych między nimi[7]. Nie ulega wątpliwości, że tak jak niegdyś broń jądrowa, tak obecnie „cyberbroń" jest zjawiskiem nowym, co wiąże się z trudnością w zakwalifikowaniu jej jako użycia siły zbrojnej w rozumieniu art. 2 ust. 4 KNZ[8]. W tym zakresie praktyka dopiero się krystalizuje. Mimo to, można już teraz stwierdzić, że w sytuacjach cyberataków niosących za sobą takie same skutki jak użycie broni kinetycznej, można mówić o użyciu siły zbrojnej pod warunkiem przypisania ataku siłom zbroj-

[6] The North Atlantic Treaty, Waszyngton, 4.4.1949 r., UNTS, Vol. 34, s. 243 (wszedł w życie 24.8.1949 r.).

[7] *M. Roscini*, Cyber Operation and the Use of Force in International Law, Oxford University Press 2014, s. 130; Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, s. 36.

[8] Zob. *J.P. Jurich*, Cyberwar and Customary International Law: The Potential of a „Bottom-up" Approach to an International Law of Information Operations, Chicago Journal of International Law 2008, Vol. 9, No. 1, s. 284–286.

nym innego państwa. Zatem różnica między bronią tradycyjną (kinetyczną) a cybernetyczną sprowadza się do tego, że w przypadku tej pierwszej nie ma problemu ze wskazaniem sił zbrojnych państwa, natomiast w przypadku tej drugiej powiązanie z takimi siłami może okazać się trudne do udowodnienia. Inną kwestią jest to, że w przypadku tzw. cyberataków dochodzi raczej do cyberprzestępstw skierowanych przeciwko ludności cywilnej, a nie użycia siły zbrojnej zgodnie z zasadami prawa humanitarnego (tzn. proporcjonalności i rozróżniania między kombatantami a ludnością cywilną)[9].

Konkludując, „cyberwojna" wykracza poza klasyczne *ius ad bellum* oraz *ius in bello*. Jest pojęciem związanym z tzw. konfliktem hybrydowym, w którym państwo używa zarówno metod konwencjonalnych (siły zbrojnej – czy to jawnie, czy też w postaci tzw. *maskirowki*), jak i niekonwencjonalnych (np. ataków cybernetycznych). Nie ma charakteru wojny, agresji lub konfliktu zbrojnego w rozumieniu klasycznego prawa międzynarodowego. Zakwalifikowanie cyberataku jako użycia siły zbrojnej napotyka na trudności, w szczególności dowodowe. Może on być jednak potraktowany jako „inny środek przymusu wymierzony przeciwko osobowości państwa" w rozumieniu Deklaracji zasad prawa międzynarodowego[10], czyli nie jako naruszenie zakazu użycia siły zbrojnej, ale zakazu ingerencji w sprawy drugiego państwa. Kwalifikowany jest również jako cyberprzestępstwo, działalność wywrotowa, szpiegostwo lub sabotaż[11]. Dotyczy to zwłaszcza sytuacji, w których nie dochodzi do realnych zniszczeń, ale np. zakłócenia funkcjonowania IT mającego wpływ na bezpieczeństwo państwa.

§ 4. Kwestia neutralności państwa

Konwencje haskie definiując neutralność nie ograniczają się tylko do zakazu naruszania terytorium poprzez użycie siły zbrojnej. Obejmują inne prawa i obowiązki państw neutralnych i stron wojujących, a w tym zakaz zakładania

[9] Por. *R.G. Wedgwood*, Proportionality, Cyberwar, and the Law of War, International Law Studies. U.S. Naval War College 2002, Vol. 76, s. 227–230.

[10] Deklaracja zasad prawa międzynarodowego, rezolucja Zgromadzenia Ogólnego ONZ z 24.10.1970 r., RES/2625/XXV, w: Zbiór dokumentów, Polski Instytut Spraw Międzynarodowych, Warszawa 1970, Nr 10.

[11] Zob. *J.M. Beard*, Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target Under International Humanitarian Law, Vanderbilt Journal of Transnational Law 2014, Vol. 47, s. 139.

na terytorium państwa neutralnego stacji radio-telegraficznej lub jakiegokolwiek aparatu, przeznaczonego do użytku jako środek dla komunikacji pomiędzy siłami wojującymi oraz zakaz używania wszelkiej instalacji tego rodzaju, założonej przez nich przed wojną na terytorium państwa neutralnego w celu wyłącznie wojskowym, która to instalacja nie była otwarta dla korespondencji publicznej. Z cyberprzestrzenią kojarzony może być również art. 8 Konwencji haskiej, zgodnie z którym państwo neutralne nie jest zobowiązane zabronić lub ograniczyć stronom wojującym używalności kabli telegraficznych lub telefonicznych i aparatów telegrafu bez drutu, które są bądź ich własnością, bądź własnością towarzystw albo osób prywatnych. Problem sprowadza się do tego, że sieć internetowa jest w znacznej mierze własnością prywatną, tj. firm telekomunikacyjnych. Postanowienia Konwencji haskich w tym zakresie są niedostosowane do aktualnej rzeczywistości. Cyberprzestrzeń jest fenomenem nieporównywalnym z instalacjami radio-telegraficznymi. W przypadku tych ostatnich można określić drogę jaką przebywa informacja, przechodząca np. przez terytorium państwa neutralnego. Sieć internetowa jako piąty wymiar nie stwarza takiej możliwości. Dane przekazywane są w oderwaniu od fizycznego wymiaru, często z użyciem urządzeń satelitarnych. Dlatego też postanowienia Konwencji haskich dotyczące sieci telefoniczno-telegraficznych zazwyczaj nie znajdą zastosowania, chyba że możliwe jest udowodnienie, iż działania podejmowane przez jedną ze stron wojujących przeciwko drugiej podejmowane były przy użyciu infrastruktury cybernetycznej zlokalizowanej na terytorium państwa neutralnego lub używanej przez administrację tegoż państwa[12]. Podobnie zastosowania nie znajdą pozostałe regulacje odnoszące się *stricte* do przestrzeni fizycznej, czyli terytorium państwa neutralnego, a w tym: zakaz przeprowadzania przez terytorium państwa neutralnego wojsk lub taborów z amunicją lub aprowizacją, nakaz internowania wojsk stron wojujących, zakaz zaboru statku i wykonywania prawa wizytacji, zakaz utworzenia trybunału kaperskiego, zakaz odstępowania stronie wojującej okrętów wojennych, amunicji i wszelkiego sprzętu wojennego oraz zasady pozostawania na wodach terytorialnych państwa neutralnego okrętów wojennych stron wojujących. W pewnym zakresie w cyberprzestrzeni można uwzględnić treść art. 4 V Konwencji haskiej, zgodnie z którym na terytorium państwa neutralnego nie mogą być formowane oddziały, przeznaczone do walki, ani otwierane biura

[12] *W. Heintschel von Heinegg*, Neutrality in Cyberspace, w: *C. Czosseck, R. Ottis, K. Ziolkowski* (eds.), 2012 4th International Conference on Cyber Conflict, Talin 2012, s. 39, https://ccdcoe.org/publications/2012proceedings/CyCon_2012_Proceedings.pdf (dostęp: 18.3.2015 r.).

werbunkowe na korzyść stron wojujących. Nie chodzi tu o rzeczywiste zorganizowanie biura, ale o budowanie stron internetowych przeznaczonych do werbowania lub formowania oddziałów na terytorium państwa neutralnego.

Jak wskazuje *W. Heintschel von Heinegg*, neutralność chroni przede wszystkim infrastrukturę cybernetyczną fizycznie zlokalizowaną na terytorium państwa neutralnego, statkach do niego przynależnych i w placówkach dyplomatycznych lub taką, która przynosi korzyści temu państwu w zakresie działalności rządowej. Podnosi przy tym, że może tu chodzić nie tylko o ataki podejmowane w cyberprzestrzeni, ale również w realnej rzeczywistości, mające na celu zniszczenie takiej infrastruktury[13]. W tym zakresie nie ma jednak problemu ze zdefiniowaniem neutralności państwa, związanej z jego fizycznym terytorium. W przypadku działań podejmowanych w cyberprzestrzeni może to natomiast stanowić problem. Założyć można, że czynnikiem decydującym o naruszeniu neutralności państwa powinien być skutek dający się określić w przestrzeni fizycznej – np. katastrofa, werbowanie, formowanie oddziałów, uszkodzenie serwerów naziemnych, zakłócenie funkcjonowania administracji publicznej.

Dlatego też z punktu widzenia działalności państw w cyberprzestrzeni kluczowe są artykuły 1 V i XIII Konwencji haskiej, zgodnie z którymi terytorium państwa neutralnego jest nienaruszalne[14]. Ich treść wyznacza istotę neutralności w powszechnym prawie zwyczajowym, zdefiniowaną już podczas Kongresu wiedeńskiego. Jak wskazano wcześniej, skutek może polegać także na realnym zniszczeniu porównywalnym z użyciem broni kinetycznej. Nie mógł on zaistnieć podczas wykorzystania tradycyjnych sieci telefoniczno-telegraficznych, które miały jedynie zastosowanie do wymiany informacji pisemnych lub ustnych. Skutek związany z cyberatakiem daje się powiązać z przestrzenią fizyczną, czyli terytorium państwowym. W związku z szeroko pojętą nienaruszalnością terytorium państwa neutralnego przeprowadzanie takich cyberataków przez strony wojujące uznać należy za zabronione w świetle prawa zwyczajowego i art. 1 Konwencji haskich. Strony wojujące zobowiązane są do powstrzymywania się od wszelkich wrogich aktów naruszających terytorium państwa neutralnego, włącznie z użyciem siły zbrojnej. Nienaruszalność terytorium państwowego sprowadza się nie tylko do zakazu użycia siły zbroj-

[13] *Ibidem*, s. 37-39.

[14] *The territory of neutral Powers is inviolable (V Konwencja haska), Belligerents are bound to respect the sovereign rights of neutral Powers and to abstain, in neutral territory or neutral waters, from any act which would, if knowingly permitted by any Power, constitute a violation of neutrality* (XIII Konwencja haska).

nej, ale również w przypadku „innego środka przymusu wymierzonego przeciwko osobowości państwa" – zakazu ingerencji w sprawy drugiego państwa. Jeżeli zatem cyberataku nie można zakwalifikować jako użycia siły zbrojnej, to może być on potraktowany jako mieszanie się w sprawy drugiego państwa. Taki wniosek może wynikać z tego, że w jego zasięgu znalazły się instytucje i systemy decydujące o bezpieczeństwie państwa. *Ergo* – cyberatak pochodzący od sił zbrojnych lub innych służb drugiego państwa, którego skutek, porównywalny z użyciem siły zbrojnej lub groźby jej użycia albo użyciem innego środka przymusu skierowanego przeciwko osobowości państwa, nastąpił na terytorium państwa neutralnego, stanowi naruszenie neutralności i rodzi odpowiedzialność międzynarodową.

Pamiętać należy również o tym, że neutralność rodzi obowiązki nie tylko po stronie państw uczestniczących w konflikcie zbrojnym, ale także po stronie państwa neutralnego. Przede wszystkim powinno ono powstrzymać się od aktywności w cyberprzestrzeni, która stwarza korzyści dla jednej ze stron wojujących. W szczególności zobowiązane jest do zapobiegania cyberatakom przeprowadzanym z jego terytorium przeciwko stronom wojującym. Zgodnie z art. 5 V Konwencji haskiej taki czyn należy uznać za sprzeczny z neutralnością i powinien być przez państwo neutralne karany.

* * *

Konkludując, neutralność państwa w cyberprzestrzeni nie jest *expressis verbis* regulowana prawem haskim. Konwencje haskie, jak i *ius in bello*, odnoszą się do przestrzeni fizycznej i klasycznych konfliktów zbrojnych. Mogą w stosunku do cyberprzestrzeni co najwyżej być stosowane odpowiednio[15]. Nie można jednak mówić, że neutralność państwa w sieci nie istnieje. Trudność sprowadza się do tego, że w cyberprzestrzeni nie ma granic państwowych, tradycyjnie określających zakres zwierzchnictwa terytorialnego, a tym samym neutralności. Dlatego też za decydujący uznać należy skutek porównywalny z użyciem siły zbrojnej, jej groźby lub „innego środka przymusu wymierzonego przeciwko osobowości państwa", chociażby w postaci uszkodzenia infrastruktury cybernetycznej, katastrofy, paraliżu administracji państwowej. W tym sensie zastosowanie mają artykuły 1 V i XIII Konwencji haskiej, stanowiące o istocie neutralności państwa. Mimo to, w związku ze specyfiką

[15] Por. *M.N. Schmitt*, Cyberspace and International Law: The Penumbral Mist of Uncertainty, Harvard Law Review Forum 2012–2013, Vol. 126, s. 176–180.

cyberprzestrzeni, a w tym stosunków międzynarodowych w niej zachodzących, tradycyjne prawo dotyczące neutralności państwa może wymagać szczególnej wykładni, uwzględniającej tą specyfikę, a w nawet modyfikacji[16]. Dlatego też należałoby zastanowić się nad traktatowym uregulowaniem działalności podmiotów prawa międzynarodowego w cyberprzestrzeni, a w tym neutralności państw (byłaby to trzecia konwencja, po V i XIII Konwencji haskiej, normująca kwestię neutralności państwowej). Jednak do tego czasu lub do momentu wykształcenia się odpowiednich norm zwyczajowych w tym zakresie, należy bazować na pojęciu neutralności państwa zdefiniowanym podczas Kongresu wiedeńskiego, a następnie rozwiniętym w Konwencjach haskich.

[16] Por. *W. Heintschel von Heinegg*, Territorial Sovereignty and Neutrality in Cyberspace, International Law Studies 2013, Vol. 89, s. 144–145.