Bartłomiej Błaszczyk
Zakład Kryminalistyki
Wydział Prawa i Administracji Uniwersytetu Łódzkiego

Atak hakerski jako naruszenie prawa międzynarodowego

Wstęp

Wkrótce obchodzić będziemy trzydziestolecie istnienia Internetu. W ciągu stosunkowo niedługiego czasu globalna sieć wdarła się w codzienność, doprowadzając do tego, że wszystko opiera się na transmisji danych pomiędzy odbiornikami – od porannego sprawdzania poczty po przekazywanie informacji kluczowych z punktu widzenia obronności czy stabilności administracyjnej i gospodarczej państwa. Płynność i bezpieczeństwo transferu danych ma zatem ogromne znaczenie nie tylko z punktu widzenia osób fizycznych, ale także podmiotów prawa międzynarodowego. Z naruszaniem stabilności infrastruktury informatycznej związane są nierozerwalnie dwa pojęcia – cyberterroryzm oraz wojna informacyjna.

„Cyberterroryzm" to termin po raz pierwszy użyty przez Barry'ego Collina w latach 80. XX wieku, na krótko po pojawieniu się powszechnego dostępu do sieci. Collin nazwał tak świadome wykorzystywanie systemu informacyjnego, sieci komputerowej lub jej części składowych do wsparcia lub ułatwienia akcji terrorystycznej, bądź też – szerzej – wykorzystanie zdobyczy technologicznych w celu wyrządzenia szkody[1]. „Wojna informacyjna" to z kolei działanie polegające na zakłóceniu komunikacji przeciwnika i wprowadzeniu go w błąd co do stanu faktycznego[2]. Oprócz tych dwóch pojęć funkcjonuje jeszcze trzecie – tzw. wojna internetowa, definiowana jako przełoże-

[1] Por.: K. C. White, *Cyber-Terrorism: Modem Mayhem*, Carlisle 1998, s. 10; T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe AMW" 2005, nr 1 (160), [online] <www.amw.gdynia.pl/library/File/ZeszytyNaukowe/2005/Szubrycht_T.pdf> (dostęp: 25.02.2017).

[2] D. Delibasis, *The Right to National Self-defense: In Information Warfare Operations*, Bury St. Edmunds 2007, s. 25.

nie realnego konfliktu lub napięcia do cyberprzestrzeni, gdzie dochodzi do wirtualnego starcia. Udział w nim biorą przede wszystkim mniej lub bardziej zorganizowane grupy hakerów, ale także cyberterroryści, co sprawia, że pojęcia te zazębiają się. Wojna internetowa, choć dosłowne znaczenie tego terminu wydaje się zbliżone do powyżej przytoczonego, dotyczy jedynie takich sytuacji, w których państwo nie jest podmiotem inicjującym tego typu działania[3]. Obecnie coraz częściej poszczególne kraje lub ich obywatele dopuszczają się ataków na kluczowe zasoby informatyczne, co może doprowadzić do poważnych konsekwencji finansowych oraz praktycznie uniemożliwić normalne funkcjonowanie państwa.

Mianem pierwszej wojny w cyberprzestrzeni określa się tzw. incydent estoński. Estonia to republika postradziecka, która bardzo szybko stała się nowoczesnym państwem, nie tylko pod względem polityczno-gospodarczym, ale także technologicznym. W Estonii za pośrednictwem Internetu można uczestniczyć w wyborach, załatwiać większość spraw w urzędach oraz wykonywać szereg innych czynności, z dokonywaniem płatności za parkowanie włącznie.

W roku 2007, w odwecie za przeniesienie pomnika „brązowego żołnierza" z centrum Tallina na tamtejszy cmentarz wojskowy, hakerzy rosyjscy przepuścili serię ataków na strony i infrastrukturę najważniejszych organów konstytucyjnych Estonii, w tym rządu, prezydenta oraz niektórych ministerstw[4]. Wskutek tego wyłączone zostały serwery odpowiedzialne za świadczenie szeregu usług o znaczeniu strategicznym dla administracji państwowej, szczególnie o tak wysokim stopniu cyfryzacji jak Estonia. O powadze sytuacji świadczy fakt, iż estoński minister obrony Jaak Aaviksoo nawoływał do uznania tego incydentu za jawny atak. Część adresów komputerów-zamachowców udało się zidentyfikować, jako ich lokalizację wskazując okolice Kremla w Moskwie[5].

Atak na Estonię miał charakter ataku typu DDoS. W tego rodzaju atakach, nazywanych również atakami przeciążeniowymi, serwer-ofiara bombardowany jest napływem danych wysyłanych z dużej liczby komputerów, co powoduje jego przeciążenie i uniemożliwia funkcjonowanie[6]. Incydent estoński określany bywa często wielkim testem sprawności i przydatności stosowania cyberataków w prowadzeniu działań dezinformacyjnych podczas konfliktów zbrojnych.

---

[3] W. Smolski, *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, Wrocław 2015, [online] <www.repozytorium.uni.wroc.pl/dlibra/docmetadata?id=66149&from=publication> (dostęp: 15.03.2017).

[4] J. Gawinecki, B. Hołyst, *Identyfikacja i przeciwdziałanie zagrożeniom* cyberprzestrzeni, [w:] B. Hołyst (red.), *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, Warszawa 2014, s. 17–18.

[5] J. Kulesza, J. Kulesza, *odpowiedzialność państw za podejmowane w cyberprzestrzeni działania zagrażające międzynarodowemu pokojowi i bezpieczeństwu,* „Studia Prawno-Ekonomiczne" 2011, t. 33, s. 149–151.

[6] J. Gawinecki, B. Hołyst, op. cit., s. 27.

Jak widać na powyższym przykładzie, zagrożenie jest duże. Wystarczy bowiem grupa uzdolnionych hakerów, aby doprowadzić do realizacji najczarniejszych scenariuszy bez użycia chociażby jednego karabinu maszynowego. Wykorzystując luki systemu głosowania, za pomocą Internetu można wpływać na wyniki wyborów, a blokując strony internetowe odpowiedzialne za świadczenie przez państwo podstawowych usług – wywoływać niezadowolenie i sterować reakcjami społeczeństwa. Odpowiednio potężny atak typu DDoS może nawet doprowadzić do odcięcia od Sieci całego państwa, o czym boleśnie w roku 2014 przekonał się rząd Korei Północnej[7] .

Skuteczność tego rodzaju ataków jest na tyle wysoka, że obecnie obok broni konwencjonalnej podkreśla się skuteczność tzw. cyberbroni. Przez cyberbroń rozumie się różnego rodzaju programy komputerowe, których działanie opiera się na zakłócaniu funkcjonowania atakowanej sieci informatycznej. Jako przykład takiego oprogramowania wskazać można chociażby wirus o nazwie Stuxnet, zaprojektowany przy kooperacji izraelsko-amerykańskiej, którego celem było zakłócenie funkcjonowania irańskich wirówek służących do wzbogacania uranu. Co warte zaznaczenia, wirus ów wymknął się spod kontroli jego twórców i prócz powstrzymania na kilkanaście miesięcy irańskiego programu nuklearnego, spowodował także nieodwracalne szkody w dziesiątkach tysięcy komputerów na całym świecie[8]. Przykłady tego rodzaju złośliwego oprogramowania, tworzonego przy mniej lub bardziej oficjalnym wsparciu rządów państw, są zresztą o wiele liczniejsze, a jako przykłady podać można chociażby wirusy Flame, Snake czy robak znany pod nazwą „Czerwony Październik" służący do wykradania danych użytkowników komputerów w Europie Wschodniej.

Co prawda, istnieje możliwość pociągnięcia osoby fizycznej do odpowiedzialności za dokonanie ataku hakerskiego (może to najwyżej być utrudnione z uwagi na właściwość miejscową), jednakże kwestia odpowiedzialności państwa jako podmiotu prawa międzynarodowego wydaje się zdecydowanie bardziej złożona.

Odpowiedzialność na gruncie prawa międzynarodowego

Międzynarodowy Trybunał Sprawiedliwości wielokrotnie podkreślał, iż państwa ponoszą odpowiedzialność za swoje działania pozostające w sprzeczności z prawem międzynarodowym i naruszające uprawnienia pozostałych członków społeczności. Jednakże kwestia przesłanek, jakie zachowanie musi

[7] Ibidem, s. 20

[8] Por.: J. Gawinecki, B. Hołyst, op. cit., s. 19; zob. także online: <https://itsecurityenthusiast.wordpress.com/2010/10/07/wirus-stuxnet-usuwanie-infekcji/> (dostęp: 25.02.2017).

spełniać, aby zostać uznane za naruszenie prawa międzynarodowego, jest zdecydowanie bardziej skomplikowana niż w przypadku prawa karnego funkcjonującego na poziomie krajowym. Brak jest bowiem przede wszystkim bezwzględnie wiążącego aktu prawa międzynarodowego, a wszystkie ewentualne podstawy odpowiedzialności mają charakter dobrowolny i uznaniowy, zaś orzeczenie zapadłe na gruncie międzynarodowego organu sądowego o wiele łatwiej uznać za „prywatną opinię" niż w wypadku prawa krajowego.

Obecnie najbardziej syntetycznym aktem międzynarodowym traktującym o odpowiedzialności międzynarodowej są wyniki pracy Komisji Prawa Międzynarodowego (ang. *International Law Committee*). Organ ten został powołany do życia rezolucją Zgromadzenia Ogólnego ONZ nr 174 z dnia 21 listopada 1947 r. i ma za zadanie przygotowanie projektu kodyfikacji prawa międzynarodowego w dziedzinie odpowiedzialności państw. Projekt taki ostatecznie ukazał się w roku 2001 i chociaż – co znamienne dla prawa międzynarodowego publicznego – nie ma charakteru wiążącego, zasadne będzie uczynienie z jego postanowień punktu wyjścia dla rozważania przedmiotowego problemu.

Omawiany projekt przewiduje dla przypisania państwu odpowiedzialności za dokonanie międzynarodowo bezprawnego aktu konieczność kumulatywnego spełnienia dwóch przesłanek, wskazanych w jego art. 2. Są to możliwość przypisania aktu danemu państwu oraz fakt, iż stanowi on naruszenie międzynarodowego zobowiązania ciążącego na państwie-naruszycielu[9]. Obie przesłanki wynikają z utrwalonego orzecznictwa powstałego na gruncie prawa międzynarodowego, np. w sprawie amerykańskich zakładników w Teheranie (*USA przeciwko Iranowi*) rozpatrywanej przez Międzynarodowy Trybunał Sprawiedliwości (MTS)[10].

Możliwość przypisania państwu odpowiedzialności

Element przypisania często określany jest w doktrynie mianem przesłanki subiektywnej, w odróżnieniu od drugiej z przesłanek, jednakże na gruncie prawa międzynarodowego posługiwanie się tego rodzaju rozgraniczeniem może okazać się mylące. Sama kwestia określenia rodzaju odpowiedzialności uzależniona jest zazwyczaj od okoliczności towarzyszących danej sprawie i składających się na jej stan faktyczny.

---

[9] Niektórzy, jak np. J. Kulesza i J. Kulesza (op. cit., s. 153) proponują – obok tych dwóch przesłanek – wskazywanie także przesłanki negatywnej w postaci braku okoliczności wyłączających odpowiedzialność państwa.

[10] Sprawa dotycząca naruszenia nietykalności misji dyplomatycznej i urzędu konsularnego, *USA przeciwko Iranowi*, ICJ Reports 1980.

Zachowanie naruszające normy prawa międzynarodowego może mieć – podobnie jak w polskim prawie karnym – postać działania lub zaniechania. Przypadki stwierdzające występowanie odpowiedzialności za zaniechanie są niemal równie liczne jak w przypadku klasycznej odpowiedzialności za zachowanie o charakterze czynnym. Jako przykład przytoczyć można chociażby konstatacje zawarte w orzeczeniu MTS zapadłym we wspomnianej już sprawie amerykańskiej ambasady w Teheranie. W treści orzeczenia wprost wskazano, iż odpowiedzialność Iranu wynika z niepodjęcia czynności przez władze rządowe, co spowodowało niezapewnienie środków, których zastosowanie w danych okolicznościach było zasadne i konieczne[11].

Wydaje się przy tym oczywiste, iż państwo nie podejmuje działań w sposób charakterystyczny dla osób fizycznych. Akt działania bądź zaniechania ze strony państwa wymaga zaangażowania czynnika ludzkiego – osób działających w imieniu i na rzecz państwa[12]. Obecnie uważa się, iż przypisanie państwu odpowiedzialności możliwe jest w wypadku działania podmiotów dających się podzielić na kilka kategorii. Po pierwsze, są to organy państwa, których działanie bądź zaniechanie wywołuje odpowiedzialność państwa także wówczas, gdy ma charakter jedynie *ultra vires* – tzn. gdy wykracza poza udzielone tym organom uprawnienia bądź instrukcje. Po drugie, podmioty niebędące organami, ale na mocy wewnętrznego prawa danego państwa umocowane do wykonywania władztwa, o ile w danym wypadku owo władztwo wykonują i wykraczają poza zakres uprawnień bądź instrukcji, o których była mowa poprzednio. Po trzecie, organy innych państw, które pozostawione zostały do dyspozycji państwa odpowiedzialnego i działają w ramach jego władztwa, także w wypadku działania *ultra vires*. Kolejne kategorie to osoby lub grupy osób, o ile podstawą faktyczną ich działań jest instrukcja udzielona przez państwo lub też działania te wykonywane są pod kierunkiem państwa; a także takie same podmioty wykonujące działania państwa w wypadku, gdy nie funkcjonuje ono bądź nie podejmuje czynności związanych z wykonywaniem władztwa. Podobnie sytuacja wygląda w przypadku ruchu powstańczego, który doprowadził do powstania odpowiedzialnego państwa oraz wszystkich innych podmiotów i jednostek w sytuacji, gdy państwo traktuje jego czynności jako własne[13].

---

[11] Ibidem.

[12] Opinia doradcza w sprawie Niemieckich Osadników w Polsce, Międzynarodowy Trybunał Arbitrażowy, 1923, P.C.I.J., ser. B, nr 6, s. 22.

[13] Takie zasady odpowiedzialności przewidywał na przykład Projekt Konwencji w sprawie międzynarodowej odpowiedzialności państw za działania zakazane przez prawo międzynarodowe opracowywany przez Komisję Prawa Międzynarodowego w art. 1–12; *Official Records od the General Assembly, 56th Session, No. 10(A./56/10)*, za: B. Wierzbicki (red.), *Prawo międzynarodowe. Materiały do studiów*, Białystok 2008, s. 257 i nast.

O ile w przypadku standardowych działań przypisanie zachowania danemu państwu zazwyczaj nie budzi większych wątpliwości, o tyle w przypadku naruszenia cyberprzestrzeni innego kraju kwestia ta zdaje się być zdecydowanie bardziej skomplikowana. Samo bowiem stwierdzenie, iż atak hakerski dokonany został z terytorium innego państwa, a nawet przy wykorzystaniu jego rządowych serwerów nie jest wystarczające. Do takiego stwierdzenia uprawnia zresztą orzeczenie MTS w sprawie cieśniny Korfu, gdzie Trybunał wprost orzekł, iż nie można z samego faktu sprawowania kontroli nad danym terytorium wyciągać wniosku, że państwo musiało wiedzieć bądź też powinno mieć świadomość każdego bezprawnego zachowania dokonanego na jego obszarze ani też, iż musi ono znać tożsamość jego sprawców[14]. Sytuacja takiego braku świadomości w przypadku ataków hakerskich jest bardzo częsta. Przykładowo, w roku 2013 Korea Północna dokonała uszkodzenia infrastruktury elektronicznej swojego sąsiada z południa, wykorzystując ponad tysiąc adresów IP i urządzeń działających jako „komputery-zombie" znajdujących się poza obszarem tego państwa, co skutecznie utrudnia przypisanie odpowiedzialności[15].

Przeważająca część ataków hakerskich jest jednak przeprowadzana przez jednostki bądź organizacje niemające statusu państwa, co dodatkowo utrudnia przypisanie ich państwu. Zasadą jest bowiem, że państwo nie ponosi odpowiedzialności za zachowania przestępne, których dopuszczają się jego obywatele. Wyjątek od tej zasady omówiony został powyżej i odnosi się do sytuacji, w której państwo traktuje zachowanie jednostek jako własne albo też gdy działają one z jego polecenia. Wykazanie występowania tych przesłanek uznać należy jednakże za co najmniej trudne. O ile można wyobrazić sobie sytuację, że organ o charakterze niepaństwowym czy nawet osoba fizyczna wykonuje określone zadania na polecenie państwa, to przeprowadzenie skutecznego dowodu pozwalającego na uznanie odpowiedzialności „zleceniodawcy" jest już o wiele bardziej skomplikowane. W przypadku osób fizycznych trudno udowodnić popełnienie przestępstwa w formie zjawiskowej sprawstwa kierowniczego bądź polecającego, a tym bardziej dokonać skutecznego przypisania odpowiedzialności w wypadku podmiotu będącego innym państwem i mającym dalece bardziej rozwinięte możliwości w zakresie usuwania śladów swojego działania. Z takimi właśnie trudnościami dowodowymi spotkała się Estonia, co uniemożliwiło ostatecznie podjęcie zarówno przez nią, jak i przez społeczność międzynarodową jakichkolwiek kroków przeciwko Rosji. Nie było bowiem możliwości udowodnienia sprawo-

[14] Sprawa cieśniny Korfu, *Wielka Brytania przeciwko Albanii*, MCJ 1949, ICJ Reports 1949, s. 4.

[15] M. Schmitt, *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, „Virginia Journal of International Law", vol. 54, nr 3, s. 701.

wania przez Rosję owej „efektywnej kontroli" nad bezpośrednimi sprawcami, której wymagają standardy wykształcone na gruncie orzecznictwa MTS (tak np. w sprawie *Nikaragua przeciwko USA* z 1986 r.)[16].

Naruszenie ciążącego na państwie zobowiązania o charakterze międzynarodowym

Druga z przesłanek odpowiedzialności państwa, ugruntowana w tradycji orzeczniczej sądów międzynarodowych, choć często bywa formułowana przy użyciu różnych pojęć[17], dotyczyć może zarówno naruszenia obowiązku wynikającego z traktatu, jak i zobowiązań pozatraktatowych.

Naruszenie międzynarodowego zobowiązania często łączy się z zachowaniem naruszającym prawa innych podmiotów. Kluczowym orzeczeniem dla utrwalenia tej przesłanki jest rozstrzygnięcie wydane przez Stały Trybunał Sprawiedliwości Międzynarodowej w sprawie marokańskich fosfatów. Dostrzeżono wówczas, iż zobowiązanie jednego państwa często wiąże się z występowaniem po stronie innego podmiotu prawa międzynarodowego określonego uprawnienia. Ostatecznie sformułowanie „naruszenie zobowiązań międzynarodowych" zostało doprecyzowane przez Międzynarodowy Trybunał Sprawiedliwości w wyroku zapadłym na kanwie sprawy *Barcelona Traction*, w którym Trybunał podzielił zobowiązania państw na wiążące tylko pomiędzy stronami (*inter partes*) w ograniczonym kręgu podmiotowym oraz zobowiązania wobec społeczności międzynarodowej traktowanej jako całość (*erga omnes*), najczęściej wynikające z norm o charakterze *ius cogens*[18].

Omawiając drugą przesłankę odpowiedzialności, bardzo istotne jest zwrócenie uwagi na zasadę suwerenności. Zasada ta, stosownie do treści rozstrzygnięcia Międzynarodowego Trybunału Arbitrażowego w sprawie *Island of Palmas* (*Holandia przeciwko USA*), oznacza niepodległość, tj. prawo do sprawowania władzy nad określonym fragmentem powierzchni ziemskiej funkcji państwa bez ingerencji ze strony innego państwa[19]. Pojęcie suweren-

---

[16] Military and Paramilitary Activities in and against Nicaragua, *Nikaragua przeciwko USA*, MTS 1986, 1984 ICJ REP. 392 (June 27).

[17] W sprawie fabryki w Chorzowie (*Niemcy przeciwko Polsce*, 1928) Stały Trybunał Sprawiedliwości Międzynarodowej używał sformułowania „breach of engagement", powtarzanego następnie w kilku innych orzeczeniach. W sprawie Rainbow Warrior z kolei (*Nowa Zelandia przeciwko Francji*, orzeczenie arbitrażowe z 1987), Trybunał wykorzystał stwierdzenie „any violation by a State of any obligation". Obecnie uważa się, iż wszystkie powyższe pojęcia są w istocie jednoznaczne.

[18] Barcelona Traction, Light and Power Company, Limited, *Belgia przeciwko Hiszpanii*, MCJ 1970, ICJ Rep 174.

[19] Island of Palmas, *Holandia przeciwko USA*, Międzynarodowy Trybunał Arbitrażowy 1928, 2 R.I.A.A. 829, 838.

ności odnoszone bywa obecnie także do cyberprzestrzeni, gdzie oznacza uprawnienie oraz obowiązek państwa do regulowania i kontrolowania aktywności w wirtualnym świecie oraz infrastrukturze elektronicznej znajdującej się na jego terytorium[20]. Konsekwentnie zatem przyjąć należy, iż jakakolwiek zewnętrzna ingerencja w znajdującą się na terenie atakowanego państwa infrastrukturę służącą do przesyłania danych stanowić będzie naruszenie suwerenności, także w wypadku, gdy ataku dokonano na platformę należącą do danego państwa, niezależnie od tego, gdzie ona się znajduje. Przyjmując zatem odpowiednio szeroką interpretację, można zaryzykować stwierdzenie, iż – pomimo faktu, że przestrzeń kosmiczna nie jest przypisywalna terytorialnie – celowe uszkodzenie satelity również stanowić będzie zamach na suwerenność kraju będącego jej emitentem[21].

Niezależnie od powyższego, niektórzy z ekspertów uważają, iż możliwe jest uznanie danego zachowania za naruszenie suwerenności także w wypadku, gdy nie wywołuje ono skutku obserwowanego poza światem wirtualnym, np. gdy system zostaje zainfekowany oprogramowaniem służącym do śledzenia zachowań jego użytkowników. Amerykańscy przedstawiciele doktryny podkreślają, iż rozumowanie takie jest uzasadnione z punktu widzenia celowościowego. Suwerenność ma bowiem dawać państwu prawo do podejmowania na swoim terytorium działań niezależnie od woli innych państw[22].

Podobnie jak w przypadku krajowego prawa karnego, także na gruncie prawa międzynarodowego mówić możemy o okolicznościach wyłączających odpowiedzialność państwa. W doktrynie przyjmuje się, co do zasady, iż występuje sześć takich okoliczności: zgoda państwa, którego interes ma zostać naruszony, działanie w ramach legalnej samoobrony, stosowanie środków przeciwdziałania w ramach obowiązującego prawa międzynarodowego, działanie spowodowane w następstwie siły wyższej (*force majeure)*, działanie w sytuacji zagrożenia oraz działanie w stanie wyższej konieczności.

Możliwość oddziaływania

Jedna z podstawowych zasad społeczności międzynarodowej wyrażona jest w art. 2 ust. 4 Karty Narodów Zjednoczonych, który stanowi, iż wszyscy członkowie ONZ powstrzymują się od stosowania groźby lub użycia siły przeciwko całości terytorialnej lub niepodległości któregokolwiek państwa. Zastosowanie zaś samoobrony, stosownie do art. 51 tegoż aktu prawnego, przy-

[20] P. W. Franzese, *Sovereignty in Cyberspace: Can It Exist?*, „Air Force Law Review" 2009, vol. 64, s. 33–35, [online] <www.au.af.mil/au/awc/awcgate/law/af_law_review_cyber.pdf> (dostęp: 14.03.2017).

[21] M. Schmitt, op. cit., s. 705.

[22] Ibidem.

sługuje krajowi w przypadku, gdy stanie się on ofiarą „napaści zbrojnej". Samo pojęcie napaści nie zostało jednoznacznie zdefiniowane. I tak na przykład, stosownie do treści art. 3 Rezolucji Zgromadzenia Ogólnego ONZ nr 3314 z 14 grudnia 1974 r., do aktów agresji zaliczyć można ingerencję zbrojną w integralność terytorialną państwa, atak na jego siły zbrojne, wspieranie prowadzonej przez inne państwo agresji oraz „wysyłanie zbrojnych band, grup, sił nieregularnych lub najemnych, które dopuszczają się aktów zbrojnych". Definicja ta ma wprawdzie charakter otwarty, jednakże nie przesądza *explicite* o możliwości uznania za zbrojną napaść np. agresji mającej charakter ekonomiczny czy też inny, niewiążący się z bezpośrednim użyciem siły w stosunku do innego państwa[23]. Są jednakże akty prawa międzynarodowego, które przewidują możliwość uznania za naruszenie reguł prawa międzynarodowego aktów o charakterze innym niż ściśle związane z naruszeniem integralności kraju w drodze zbrojnej napaści. Stosownie do zapisu zawartego w Deklaracji Zasad Prawa Międzynarodowego dotyczących przyjaznych stosunków i współdziałania państw zgodnie z Kartą Narodów Zjednoczonych[24], zarówno zbrojny atak, jak i wszelkie formy naruszenia bądź usiłowania grożenia przeciwko podmiotowości danego państwa bądź jego politycznym, gospodarczym lub kulturalnym czynnikom stanowią naruszenie prawa międzynarodowego. Żadnemu państwu nie wolno używać lub zachęcać do użycia gospodarczych, politycznych lub jakiegokolwiek innego rodzaju środków przymusu, mających na celu podporządkowanie drugiego państwa w wykonywaniu jego suwerennych praw oraz celem zapewnienia sobie od niego jakichkolwiek korzyści. Wydawałoby się, iż powyższe sformułowanie będzie wystarczające do uznania za bezprawną ingerencję także ataku przeprowadzonego przy pomocy środków wyłącznie elektronicznych – z uwagi na posługiwanie się przez normę pojęciem „jakikolwiek inny środek".

Jak widać na przykładzie incydentu estońskiego, uznanie ataku wirtualnego za zbrojną napaść jest na razie jeszcze negowane, przynajmniej na kontynencie europejskim. Jednakże mnogość przypadków związanych z naruszeniem cyberprzestrzeni danego kraju oraz postępująca informatyzacja życia codziennego powodują, iż kwestia możliwości użycia siły w odpowiedzi na cyberatak jest coraz bardziej aktualna.

Nieco wcześniej wskazano już, iż część przedstawicieli amerykańskiej doktryny twierdzi, że naruszenie cyberprzestrzeni innego państwa może być kwalifikowane jako naruszenie jego suwerenności, jak również że dopuszczalne jest zastosowanie środków przeciwdziałania (ang. *countermeasures*) w razie niemożności uznania ataku hakerskiego za zamach zbrojny w ści-

[23] A. Wyrozumska, W. Czapliński, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 1999, s. 486.

[24] Rezolucja Zgromadzenia Ogólnego ONZ nr 2625 (XXV) z dnia 24 października 1970 r.

słym tego słowa znaczeniu. Przez „środki przeciwdziałania" rozumieć należy działania lub zaniechania państwa wymierzone w inne państwo, które w innym wypadku stanowiłyby – stosownie do opisanych powyżej przesłanek bezprawności – naruszenie prawa międzynarodowego; nie są nim jednakże z uwagi na fakt zastosowania ich jako odpowiedź na bezprawne zachowanie innego państwa. Zastosowanie tych środków mieści się zatem w ramach okoliczności wyłączającej bezprawność, co odróżnia je z kolei od innych opisanych powyżej środków prawnych polegających na podjęciu działania mieszczącego się w granicach prawa, ale nieprzyjaznych – retorsji. Ponieważ okoliczności, które pozwalają na uznanie, że dane zachowanie państwa jest dozwolone w ramach „kontratypu", mają doniosłe znaczenie z punktu widzenia odpowiedzialności międzynarodowej, ich zakres wielokrotnie był przedmiotem zainteresowania Międzynarodowego Trybunału Sprawiedliwości[25].

Następstwa przypisania państwu odpowiedzialności

Na przykładzie incydentu estońskiego widać doskonale, jak rozległe rozmiary mogą mieć szkody wywołane przez naruszenie cyberprzestrzeni kraju poszkodowanego. Przypisanie konkretnemu państwu odpowiedzialności mogłoby jednak wywoływać dla niego szereg innych konsekwencji niż zastosowanie opisanych powyżej środków przeciwdziałania. Stosownie do treści przywoływanego już wyroku w sprawie fabryki chorzowskiej, „jest zasadą prawa międzynarodowego, że naruszenie zobowiązania międzynarodowego pociąga za sobą obowiązek udzielenia reparacji w należytej formie. Reparacje te […] muszą w możliwie największym stopniu eliminować wszystkie konsekwencje nielegalnego aktu oraz przywrócić sytuację, która według wszelkiego prawdopodobieństwa zaistniałaby, gdyby ten akt nie został popełniony"[26]. Oznacza to, iż państwo dopuszczające się naruszenia cyberprzestrzeni innego podmiotu prawa międzynarodowego również byłoby zobowiązane do naprawienia wyrządzonej szkody. Jednocześnie zaznaczenia wymaga, iż tego rodzaju restytucja nie ma charakteru penalnego – jej celem nie jest bowiem ukaranie naruszyciela czy też napiętnowanie jego niezgodnego z prawem międzynarodowym postępowania, ale przede wszystkim usunięcie jego skutków.

Oprócz tego postuluje się, że poza naprawieniem szkody państwo poszkodowane może domagać się udzielenia gwarancji niedopuszczenia do podobnych naruszeń w sytuacji, gdy okoliczności sprawy będą tego wymagały[27].

[25] M. Schmitt, op. cit., s. 701.

[26] *Niemcy przeciwko Polsce*, STSM 1928, 1927 P.C.I.J. (ser. A) nr 9 (July 26).

[27] A. Zbaraszewska, *Dylematy międzynarodowej odpowiedzialności państw*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2007, nr 1, s. 57.

Wydaje się, iż z taką właśnie sytuacją mamy do czynienia w wypadku ataku hakerskiego, przynajmniej w niektórych jego odmianach. Wprowadzenie do infrastruktury poszkodowanego złośliwego oprogramowania może – obok obowiązku jego usunięcia i restytucji strat – pociągać za sobą żądanie, aby użyte złośliwe oprogramowanie nie mogło zostać wykorzystane w razie pozostania w którymkolwiek z elementów zainfekowanej infrastruktury.

Pełne naprawienie szkody powstałej na skutek dopuszczenia się przez państwo czynu uznanego za bezprawny przez społeczność międzynarodową może – stosownie do treści projektu przywoływanego już uprzednio aktu dotyczącego odpowiedzialności za naruszenie prawa międzynarodowego – przybrać formą restytucji, kompensacji, czyli wypłaty odszkodowania w pieniądzu, ale jest to możliwe jedynie wówczas, gdy szkoda daje się oszacować jako wartość materialna. Można też żądać udzielenia satysfakcji, np. w formie uroczystych przeprosin, co miało miejsce w przywoływanej już sprawie incydentu w cieśninie Korfu. Wyliczone powyżej rekompensaty mogą pojawiać się samodzielnie, jak również występować wspólnie w razie niemożności uzyskania pełnego naprawienia szkody przy wykorzystaniu tylko jednego z powyższych środków[28].

Podsumowanie

Z uwagi na postępującą informatyzację wszystkich sfer życia publicznego oraz prywatnego bezpieczeństwo systemów służących do transmisji i przetwarzania danych cyfrowych nabiera obecnie kluczowego znaczenia. Mimo to odpowiedzialność za spowodowanie celowych zakłóceń w funkcjonowaniu infrastruktury służącej do obsługi przesyłu informacji przez Internet nadal nie jest do końca uregulowana. Podobnie nie znaleziono jeszcze uniwersalnego mechanizmu pozwalającego na stosowanie środków przeciwdziałania przeciwko państwu-naruszycielowi. Jednakże ze względu na znaczenie strategiczne połączeń internetowych oraz coraz większy nacisk na bezpieczeństwo danych jest niemalże pewne, iż wkrótce spory zaistniałe na gruncie stanów faktycznych podobnych do kazusu estońskiego staną się przedmiotem rozstrzygnięć sądów międzynarodowych.

Być może trudności z przypisaniem państwu odpowiedzialności za działanie osób i organizacji, spotykane często w „klasycznych" kazusach, a jeszcze bardziej skomplikowane na gruncie nowoczesnych technologii, spowodują zrewidowanie kwestii przypisywania odpowiedzialności za czyny tego rodzaju podmiotów. Jedno jest pewne – społeczność międzynarodowa jeszcze

[28] D. Shelton, *Righting Wrongs: Reparations in the Articles on State Responsibility*, „American Journal of International Law" 2002, nr 96, s. 833 i nast.

nie jest przygotowana na skuteczne przeciwdziałanie i piętnowanie ataków hakerskich dokonywanych przez jednego z ich członków, co rodzi niebezpieczną sytuację, która w niedługim czasie będzie wymagała pilnego rozwiązania.

Literatura

Delibasis D., *The Right to National Self-defense: In Information Warfare Operations*, Bury St. Edmunds 2007.

Franzese P. W., *Sovereignty in Cyberspace: Can It Exist?*, „Air Force Law Review" 2009, vol. 64.

Gawinecki J., Hołyst B., *Identyfikacja i przeciwdziałanie zagrożeniom* cyberprzestrzeni, [w:] B. Hołyst (red.), *Technika kryminalistyczna w pierwszej połowie XXI wieku. Wybrane problemy*, Warszawa 2014.

Kulesza J., Kulesza J., *Odpowiedzialność państw za podejmowane w cyberprzestrzeni działania zagrażające międzynarodowemu pokojowi i bezpieczeństwu*, „Studia Prawno-Ekonomiczne" 2011, t. 33

Schmitt M., *"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law*, „Virginia Journal of International Law", vol. 54, nr 3.

Shelton D., *Righting Wrongs: Reparations in the Articles on State Responsibility*, „American Journal of International Law" 2002, nr 96.

Smolski W., *Cyberterroryzm jako współczesne zagrożenie bezpieczeństwa państwa*, Wrocław 2015.

Szubrycht T., *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe AMW" 2005, nr 1 (160).

White K. C., *Cyber-Terrorism: Modem Mayhem*, Carlisle 1998.

Wierzbicki B. (red.), *Prawo międzynarodowe. Materiały do studiów*, Białystok 2008.

Wyrozumska A., Czapliński W., *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, Warszawa 1999.

Zbaraszewska A., *Dylematy międzynarodowej odpowiedzialności państw*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2007, nr 1.

Summary

Cyber attakcs as a violation of the international law

Key words: cyber attack, hacking, internet war, international law, State's responsibility.

The 21st century is the age, when using Internet to administrate the State is no longer a science fiction, but rather new reality, with which the legal system has to cope with. However, despite having many advantages, relying on digital data transfer may also cause some significant threats, one of which is undoubtedly being a victim of a cyber attack.

The case of a great importance is especially situation, when electronic systems owned by one of States is getting hacked by the other State, which may be recognised as an internationally wrongful act.

The article is aimed to describe the types of threats that appear in connection with the digital world, explain the basis of claim the State responsible for an attack as well as a conditions of such a statement. Also some place is devoted to describe possibilities of the use of countermeasures and ways of restitution of damages caused by the cyber attack.