PRZEGLĄD ZACHODNI
2013, nr 4

MIRON LAKOMY
Katowice

POLITYKA CYBERBEZPIECZEŃSTWA SOJUSZU PÓŁNOCNOATLANTYCKIEGO

Internet w XXI w. stanowi narzędzie o fundamentalnym znaczeniu dla życia społecznego, gospodarczego i politycznego państw. Liczba użytkowników sieci w ciągu ostatnich pięciu lat uległa podwojeniu i w 2012 r. wyniosła około 2,27 mld osób. Dowodzi to, jak wielkim zainteresowaniem cieszy się to medium we współczesnym świecie[1]. Internet jest powszechnie wykorzystywany już nie tylko przez indywidualnych użytkowników, ale także przez instytucje publiczne na poziomie lokalnym, państwowym i międzynarodowym. Cyberprzestrzeń staje się więc domeną, w której aktywność prywatna bardzo często przenika się z działalnością publiczną[2]. Coraz powszechniejsze wykorzystanie komputerów, technologii *ICT*[3] oraz sieci tak przez jednostki, instytucje państwowe, jak i ponadnarodowe rodzi jednak określone zagrożenia w wymiarze bezpieczeństwa. Paradoksalnie, ilościowy oraz jakościowy rozwój szeroko rozumianej cyberprzestrzeni otwiera bowiem zupełnie nowe możliwości jej szkodliwego wykorzystania.

Prawidłowo rozpoznając te wyzwania, od początku XXI w. coraz więcej rządów zaczęło zwracać uwagę na znaczenie sieci dla bezpieczeństwa państw. Zasadniczy przełom nastąpił jednak dopiero w kwietniu 2007 r., kiedy Estonia jako pierwsza w historii na masową skalę stała się obiektem motywowanych

[1] *The Internet's Population Doubled Over the Last Five Years*, Future Journalism Project, 19.04.2012, http://tumblr.thefjp.org/post/21384386610/the-internets-population-doubled-over-the-last-five-year (dostęp: 16.01.2013).

[2] Według nowelizacji ustawy o stanie wojennym z 2011 r. cyberprzestrzeń to: „przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami". Zob. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczpospolitej Polskiej (Dz. U. 2002 Nr 156, poz. 1301; 2003 Nr 228, poz. 2261; 2004 Nr 107, poz. 1135; 2011 Nr 222, poz. 1323).

[3] *Information and Communications Technology*. W Polsce najczęściej utożsamia się ją z teleinformatyką.

politycznie cyberataków. Mimo przynależności Estonii do Sojuszu Północnoatlantyckiego, ta tzw. pierwsza cyberwojna zakończyła się znaczącym sukcesem rosyjskich hakerów[4]. Od tego momentu problem ten został dostrzeżony przez całą społeczność międzynarodową. Jedne państwa, takie jak np. Stany Zjednoczone czy Izrael, w odpowiedzi na te wyzwania opracowały skuteczne modele polityki cyberbezpieczeństwa, przeznaczając na ten cel duże środki finansowe[5]. Inne jednak tylko w niewielkim stopniu przygotowały się na walkę ze stale ewoluującymi zagrożeniami teleinformatycznymi. Co ciekawe, wśród tej drugiej grupy znalazły się również kraje wysoko rozwinięte, które relatywnie często stają się celem rozmaitych cyberataków. W tym kontekście należy zauważyć, iż kwestie te stanowią rosnące wyzwanie nie tylko dla poszczególnych państw, ale także dla tradycyjnych sojuszy militarnych, w tym przede wszystkim dla Paktu Północnoatlantyckiego, tak w wymiarze prawnym, politycznym, jak i wojskowym. Wydarzenia z Estonii z 2007 r. udowodniły bowiem, iż *NATO* pozostało bezsilne wobec tych nowych zagrożeń. Problem jest tym istotniejszy, iż incydenty tego typu, dzięki swej zróżnicowanej i stale ewoluującej formie, mogą potencjalnie mieć skutki podobne do osiągalnych przy wykorzystaniu konwencjonalnego uzbrojenia[6]. Warto więc spróbować odpowiedzieć na pytanie, czym w zasadzie są zagrożenia teleinformatyczne oraz w jaki sposób stara się im przeciwdziałać Sojusz Północnoatlantycki?

CYBERPRZESTRZEŃ JAKO NOWY WYMIAR BEZPIECZEŃSTWA

W latach 80. i 90. XX w. szkodliwa działalność w jeszcze mało rozwiniętej cyberprzestrzeni wiązała się przede wszystkim z aktywnością nielicznych jednostek lub grup specjalistów, posiadających odpowiednią wiedzę i umiejętności, aby

---

[4] Warto podkreślić, że nie ma zgody badaczy co do tego, kto w rzeczywistości przeprowadził te ataki. Według jednych stały za tym rosyjskie władze. Tezę tę popierał również rząd Estonii. Zdaniem innej grupy ekspertów były one wynikiem mobilizacji rosyjskich haktywistów. Pojawił się też wątek organizacji *Nashi*, który jednak wydaje się mało prawdopodobny. Mimo tych wątpliwości, w literaturze specjalistycznej bardzo często określa się te incydenty mianem „pierwszej cyberwojny". Zob. K. Ruus, *Cyber War I: Estonia Attacked from Russia*, „European Affairs" 2008, No 9:1; H. Laasme, *Estonia: Cyber Window into the Future of NATO*, „Joint Force Quarterly" 2011, No 63.

[5] Choć należy pamiętać, iż w obu przypadkach cyberbezpieczeństwem zainteresowano się zdecydowanie wcześniej. Zob. A. Bógdał-Brzezińska, M.F. Gawrycki, *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Warszawa 2003; M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe. Haking, haktywizm i cyberterroryzm*, w: M. Terlikowski, M. Madej (red.), *Bezpieczeństwo teleinformatyczne państwa*, Warszawa 2009; M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku*, „Stosunki Międzynarodowe – International Relations" nr 3-4, 2010, s. 55-72.

[6] Zob. R.A. Clarke, R. Knake, *Cyberwar: The Next Threat to National Security and What to Do About It*, New York 2010.

włamywać się do rzadkich wówczas baz danych czy tworzyć pierwsze wirusy komputerowe. Wraz z rozwojem technologii komputerowych oraz Internetu tego typu praktyki zaczęły się nie tylko upowszechniać, ale i dywersyfikować. Obok wirusów pojawiły się inne rodzaje złośliwego oprogramowania (robaki, trojany czy *backdoory*[7]) i wcześniej niestosowane techniki *hakingu*, takie jak np.: *phishing*, *sniffing* czy *DDoS* (*Distributed Denial of Service*)[8]. Obok domorosłych hakerów coraz częściej działania podejmowały również ich zorganizowane grupy, o różnorodnej motywacji. Tym samym pojawiły się pierwsze poważne ataki z powodów politycznych, społecznych bądź finansowych. W tym kontekście należy stwierdzić, iż od przełomu XX i XXI w. doszło do dynamicznego rozwoju wieloaspektowej, szkodliwej działalności w cyberprzestrzeni, która stała się zagrożeniem dla bezpieczeństwa narodowego i międzynarodowego. W najprostszy sposób można je sklasyfikować jako:

– *haking*, będący działalnością w sieci, której celem jest sam akt udanego cyberataku, bez politycznego, społecznego lub ekonomicznego podtekstu[9];

– haktywizm, który można zdefiniować jako działalność hakerską (*haking*), motywowaną względami politycznymi lub społecznymi[10];

– cyberterroryzm rozumiany jako politycznie motywowany atak na komputery, systemy, programy lub sieci informatyczne;

– cyberszpiegostwo, rozumiane jako próba uzyskania niejawnych informacji w cyberprzestrzeni;

– wykorzystanie cyberprzestrzeni do prowadzenia działań zbrojnych w ramach kolejnego teatru wojny[11].

Haking oraz haktywizm, jakkolwiek będące z reguły działalnością nielegalną, z pewnością stanowią realnie najmniejsze zagrożenie. *Haking* jest najstarszą i z reguły najmniej istotną, z punktu widzenia bezpieczeństwa narodowego i międzynarodowego, formą szkodliwej działalności w cyberprzestrzeni. Rzeczywiste efekty *hakingu* mogą być poważne, jednak na ogół nie mają one większego

[7] Q. Gu, P. Liu, C.-H. Chu, *Hacking Techniques in Wired Networks*, Pennsylvania State University, http://s2.ist.psu.edu/paper/hack-wired-network-may-04.pdf (dostęp: 25.05.2013).

[8] *Rodzaje ataków hakerskich*, Wydziałowa Pracownia Komputerowa, Wydział Elektrotechniki, Elektroniki, Automatyki i Informatyki Politechniki Łódzkiej, http://www.wpk.p.lodz.pl/ (dostęp: 16.11.2012).

[9] Zob. Prezentacja: M. Terlikowski, *Haking, haktywizm, cyberterroryzm*, Polski Instytut Spraw Międzynarodowych, 23.04.2008, www.pism.pl (dostęp: 1.12.2012); M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe*..., s. 98-99.

[10] Haktywizm jest też często utożsamiany ze szkodliwą działalnością w sieciach teleinformatycznych, której celem jest manifestacja swojego stanowiska wobec szeroko rozumianych kwestii politycznych, społecznych lub gospodarczych. Można go więc uznać także za rodzaj obywatelskiego nieposłuszeństwa wyrażonego w sieci. Zob. *Electronic Civil Disobedience & Hacktivism*, „Zapatistas: the first 'postmodern' revolution", Zapatista Army of National Liberation, 17.10.2011.

[11] M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, „Stosunki Międzynarodowe – International Relations" nr 3-4, 2011, s. 151.

znaczenia dla instytucji państwowych i nie wywołują strat materialnych[12]. Haktywizm, będący praktyką stosowaną coraz powszechniej przez różnorodne kolektywy motywowanych politycznie hakerów, z reguły jest bardzo widowiskowy, jednak jego praktyczne skutki są dość ograniczone. Według François Paget, można wyróżnić trzy grupy haktywistów. Pierwsza z nich, *Anonymous*, swoje działania skupia na blokowaniu dostępu do określonych usług lub stron internetowych oraz wykradaniu informacji z komputerów należących do instytucji państwowych bądź wielkich korporacji. Druga grupa, tzw. cyberlokatorzy (*cyberoccupiers*), to właściwi aktywiści, którzy wykorzystują sieć w celach propagandowych oraz informacyjnych. Wreszcie trzecią są „cyberwojownicy", wchodzący w skład swoistych „cyberarmii" działających w Internecie przykładowo z pobudek patriotycznych[13]. Z szeroko rozumianą ideą haktywizmu kłócą się działania, których efektem byłyby straty odczuwalne dla całego społeczeństwa, czyli np. ataki na infrastrukturę krytyczną państwa. Celem haktywistów jest więc z reguły zwrócenie uwagi opinii publicznej na określony problem, a nie dokonanie trwałych szkód[14]. Tym samym zazwyczaj stanowią oni raczej niewielkie utrudnienie dla funkcjonowania instytucji rządowych czy organizacji międzynarodowych. W dużej mierze udowodniły to protesty *Anonymous* wokół umowy *ACTA* w styczniu 2012 r., w wyniku których wiele stron internetowych należących do polskich instytucji państwowych zostało zablokowanych[15]. Pewne wątpliwości można mieć co do trzeciej grupy wyodrębnionej przez François Paget, czyli „cyberwojowników". Jak udowodniły wydarzenia w Estonii, Gruzji czy Kirgistanie, trudno jest w zasadzie rozgraniczyć indywidualną działalność politycznie motywowanych hakerów od zorganizowanych akcji, zaplanowanych i przeprowadzonych przez czynniki rządowe.

Zagadnienie to łączy się poniekąd ze zjawiskiem cyberterroryzmu, który oprócz szeroko rozumianych pobudek politycznych, może zawierać w sobie także element osobistych lub grupowych korzyści. Ponadto od haktywizmu różni go cel, jakim jest wyrządzenie poważnych szkód, a przez to osłabienie poczucia bezpieczeństwa ludności. Przykładowo, pojedynczy atak przeprowadzony w sieci przeciwko infrastrukturze krytycznej państwa mógłby być uznany za akt cyberterroryzmu[16].

---

[12] M. Terlikowski, *Bezpieczeństwo teleinformatyczne państwa a podmioty pozapaństwowe...*, s. 98-99; Prezentacja: M. Terlikowski, *Haking, haktywizm, cyberterroryzm...*

[13] F. Paget, *Hacktivism. Cyberspace has become the new medium for political voices*, „McAfee Labs White Paper" 2012, s. 4.

[14] G. Coleman, *Coleman Discusses „Anonymous" as Civil Disobedience*, Steinhardt School of Culture, Education, and Human Development, http://steinhardt.nyu.edu/news/2011/3/11/Coleman_Discusses_Anonymous_as_Civil_Disobedience (data wejścia na stronę 21.11.2012).

[15] T. Grynkiewicz, *Weekendowy zamach na strony rządowe*, „Gazeta Wyborcza" 23.01.2012.

[16] Choć jak zauważyli Sarah Gordon i Richard Ford, w zasadzie nie ma zgody badaczy co do właściwej definicji tego zjawiska. Przykładowo, według *Denning's Testimony before the Special Oversight Panel on Terrorism*, cyberterroryzm to: „połączenie terroryzmu oraz cyberprzestrzeni. Generalnie, rozumie się przez to bezprawne ataki lub groźby ataków przeciwko komputerom, sieciom oraz znajdującym się w nich informacjom, w celu zastraszenia lub gwałtu rządu lub obywateli z pobudek

Do takich zdarzeń prawdopodobnie doszło w latach 2005 i 2007, kiedy – według części amerykańskich ekspertów – w ten sposób doprowadzono do poważnej awarii sieci energetycznej w Brazylii. Bez prądu pozostały wówczas miliony ludzi[17]. Do tej kategorii można także zaliczyć coraz widoczniejszą w sieci działalność tradycyjnych organizacji terrorystycznych, takich jak *Al Kaida*, *Hamas* czy *Hezbollah*[18].

Nieco inny charakter ma natomiast cyberszpiegostwo. Nie ulega wątpliwości, że wykorzystanie Internetu do zdobycia poufnych informacji jest zdecydowanie łatwiejsze, tańsze i mniej niebezpieczne niż tradycyjne formy tego procederu. W związku z tym w ostatnich latach można zauważyć zasadniczy rozwój takiej działalności w cyberprzestrzeni. Już w 2003 r. w Stanach Zjednoczonych w wyniku afery *Titan Rain* ujawniono, iż chińscy hakerzy wykradli z serwerów amerykańskiego rządu i korporacji dane dotyczące funkcjonowania, planów oraz technologii *NASA*, *Lockheed-Martin* czy *Redstone Arsenal*. To również specjaliści z Chin w 2007 r. dokonali serii skoordynowanych ataków, dzięki którym włamano się do komputerów należących do amerykańskiego Departamentu Obrony, Stanu oraz Handlu i Energii. Warto również przypomnieć odkrycie przez zespół *Information Warfare Monitor* chińskiej grupy *Ghostnet*, która w 2009 r. dokonała włamań do komputerów aż w 103 krajach, w tym m.in. w Niemczech, na Cyprze, w Tajlandii, Korei Południowej czy Pakistanie. Dzięki cyberprzestrzeni uzyskano także dostęp do komputera osobistego Dalajlamy[19].

Coraz większe znaczenie zdaje się mieć także wykorzystanie cyberprzestrzeni do działań zbrojnych w ramach kolejnego teatru wojny. Warto w tym kontekście przytoczyć raport amerykańskiego ośrodka badawczego *RAND*, który już w styczniu 1996 r. stwierdził, iż istnieje możliwość prowadzenia „strategicznej wojny w cyberprzestrzeni". Wśród czynników sprzyjających ewolucji wykorzystania sieci teleinformatycznych w tym kierunku w dokumencie wymieniono m.in.: niskie koszty działalności, brak tradycyjnych granic, zwiększoną możliwość prowadzenia działalności propagandowej, brak wywiadu strategicznego, brak systemów ostrzegania oraz oceny prawdopodobieństwa ataków, trudności związane ze współpracą międzynarodową oraz wrażliwość na ataki na terytorium USA[20]. Można również

politycznych lub społecznych". Zob. S. Gordon, R. Ford, *Cyberterrorism?* „Symantec Security Response White Paper" Cupertino 2003, s. 4.

[17] M. Mylrea, *Brazil's Next Battlefield: Cyberspace*, „Foreign Policy Journal" 15.11.2009, http://www.foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace/ (dostęp: 23.11.2012).

[18] Zob. C.A. Theohary, J. Rollins, *Terrorist Use of the Internet: Information Operations in Cyberspace*, „CRS Report for Congress" 08.03.2011; E. Lichocki, *Cyberterrorystyczne zagrożenie dla bezpieczeństwa teleinformatycznego państwa polskiego*, Warszawa 2008.

[19] T. Jordan, *Hakerstwo*, Warszawa 2011, s. 98-99; M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku...*, s. 144-148.

[20] *Strategic War...in Cyberspace*, „RAND Research Brief" 01, 1996; R.C. Molander, A.S. Riddile, P.A. Wilson, *Strategic Information Warfare: A New Face of War*, RAND Corporation, Santa Monica 1996.

przywołać opinię Alexisa Bautzmanna z francuskiego Centrum Analiz i Prognoz Zagrożeń Międzynarodowych (*Centre d'Analyse et de Prévision des Risques Internationaux – CAPRI*), zdaniem którego rozwój cyberprzestrzeni na przełomie pierwszej i drugiej dekady XXI w. sprawił, iż należy ponownie przemyśleć znaczenie bezpieczeństwa oraz narodowej suwerenności. Według niego można zauważyć rosnącą „militaryzację" Internetu, oznaczającą tworzenie jednostek wojskowych specjalizujących się w walce w środowisku sieciowym. Kompleksowe działania zmierzające w tym kierunku podjęły nie tylko Stany Zjednoczone, tworząc *USCYBERCOM*, lecz także np. Wielka Brytania[21]. Ruchy tego typu są przede wszystkim wynikiem świadomości rosnącego znaczenia cyberprzestrzeni jako nowego teatru wojny[22]. Potwierdzają to praktyczne przykłady. W 2007 r. Izrael wykorzystał wirus komputerowy w trakcie operacji *Orchard*, której celem było zniszczenie syryjskiego ośrodka badań nad bronią atomową. Dzięki zastosowaniu specjalistycznego oprogramowania, udało się oślepić systemy radarowe obrony powietrznej Syrii, dzięki czemu nalot bombowy nie spotkał się z reakcją sił powietrznych tego kraju[23]. Za przejaw pośredniego wykorzystania cyberprzestrzeni do prowadzenia działań zbrojnych uznaje się również wydarzenia na Kaukazie w sierpniu 2008 r. Wówczas rosyjscy hakerzy dokonali masowych ataków na strony internetowe należące do instytucji państwowych Gruzji. Zablokowano również najważniejsze serwery naukowe oraz komercyjne, w tym przede wszystkim te o charakterze informacyjnym. Według niektórych danych, poważne problemy dotknęły także gruzińską sieć telekomunikacyjną. Co prawda nie wykorzystano tu Internetu do właściwych działań zbrojnych, jednak cyberataki miały istotne znaczenie dla bieżącej propagandy wojennej. Z tego punktu widzenia sukces rosyjskich hakerów pozwolił Rosji na osiągnięcie pewnej przewagi politycznej w trakcie konfliktu, blokując jednocześnie możliwość prezentowania stanowiska przez Tbilisi. Istotne znaczenie mial także aspekt psychologiczny, związany z pozbawieniem gruzińskich obywateli dostępu do wielu najważniejszych usług internetowych. Przy czym należy pamiętać, iż Kreml nie podjął działań zmierzających do sparaliżowania infrastruktury krytycznej tego kraju[24].

W kontekście trzech omówionych wyżej zagrożeń – cyberterroryzmu, cyberszpiegostwa oraz militarnego wykorzystania sieci teleinformatycznych – coraz

---

[21] A. Bautzmann, *Le cyberespace, nouveau champ de bataille?*, „Diplomatie. Affaires Strategiques et Relations Internationales" 02.-03., 2012, s. 80-81.

[22] P. Sienkiewicz, *Wizje i modele wojny informacyjnej*, w: L.H. Haber (red.), *Społeczeństwo informacyjne – wizja czy rzeczywistość*, Kraków 2003, s. 376-377; J.A. Warden, *Enemy as a System*, „Airpower Journal" 1995, nr 9, s. 40-55.

[23] Zob. T. Rid, *Cyber War Will Not Take Place*, „Journal of Strategic Studies" 2012, No 1.

[24] Warto także przypomnieć, iż już w przypadku interwencji w Kosowie oraz w Iraku cyberprzestrzeń odgrywała ograniczoną rolę w działaniach zbrojnych. Zob. D.J. Smith, K. Mshvidobadze, *Russia, Georgia and the Shape of Cyber Wars to Come*, Georgian Security Analysis Center, 5.16.2011; D. Hollis, *Cyberwar Case Study: Georgia 2008*, „Small Arms Journal", 06.01.2011.

częściej wykorzystuje się termin „cyberwojna". Nie ulega wątpliwości, iż zjawisko to jest ściśle związane z działalnością państwową. Nie ma jednak pełnej zgody badaczy nie tylko co do samej definicji cyberwojny, ale także zasadności tego terminu. Przykładowo, w 2009 r. Eugene Spafford stwierdził, iż dotychczasowe wydarzenia nie dawały podstaw do formułowania opinii wskazujących na pojawienie się takiego zjawiska w stosunkach międzynarodowych[25]. Również Thomas Rid zauważył, iż mówienie o cyberwojnie jest nadużyciem, ponieważ dotychczasowe przykłady najpoważniejszych ataków teleinformatycznych nie spełniały kryteriów: śmiercionośności, instrumentalności oraz politycznej motywacji[26]. Z drugiej jednak strony, stale rosnąca grupa badaczy wskazuje na fakt, iż działania w cyberprzestrzeni w bliskiej przyszłości staną się pełnoprawnym elementem wojny. Podkreślał to m.in. były zastępca dyrektora amerykańskiej Narodowej Agencji Bezpieczeństwa (*NSA*) William Cromwell. Z pewnością najbardziej znanym orędownikiem szerokiej debaty na ten temat jest Richard Clarke, były doradca prezydentów Stanów Zjednoczonych Billa Clintona oraz George'a W. Busha. Sformułował on w zasadzie jedną z najciekawszych definicji tego pojęcia. Jego zdaniem cyberwojna jest „działalnością państw, mającą na celu penetrację systemów i sieci komputerowych innych podmiotów międzynarodowych dla dokonania określonych zniszczeń lub zakłóceń"[27]. Warto także przytoczyć opinię Piotra Sienkiewicza, według którego cechami wojny cybernetycznej są: uzyskanie przewagi informacyjnej, niewidzialność przeciwnika, cyberprzestrzeń jako teren działań, a czynnikiem krytycznym jest czas[28]. Wydaje się, iż obie te opinie stanowią właściwą odpowiedź na zarzuty stawiane m.in. przez Thomasa Rida, zbyt mocno utożsamiającego zjawisko cyberwojny z tradycyjnym, konwencjonalnym modelem konfliktu zbrojnego. Dotychczasowe doświadczenia jasno bowiem wskazują, iż sieci teleinformatyczne w ostatnich latach stały się w zdecydowanie większym stopniu niż wcześniej obiektem zainteresowania państw. Rządy nie tylko podejmują działania, których celem jest zabezpieczenie się przed zagrożeniami płynącymi z cyberprzestrzeni, ale – przynajmniej niektóre – rozwijają także swoje zdolności ofensywne. Pionierami tego typu polityki są m.in. Stany Zjednoczone oraz Izrael. To właśnie USA w 2009 r. jako pierwsze na świecie stworzyły odrębne dowództwo sił zbrojnych w cyberprzestrzeni (*USCYBERCOM*)[29], potwierdzając tym samym tezę o rosnącym znaczeniu sieci dla bezpieczeństwa narodowego i międzynarodowego. Stąd wydaje się, iż pojęcie cyberwojny, zawierające opisane wyżej aspekty militarne, szpiegowskie i terrorystyczne, jest jak najbardziej uprawnione.

[25] *Virtual Criminology Report*, McAfee Labs 2009, s. 8-12.

[26] Zob. T. Rid, *Cyber War Will Not Take Plac...*

[27] R.A. Clarke, R. Knake, *Cyberwar: The Next Threat to National Security and What to Do About It*, New York 2010; M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku...*, s. 151-152.

[28] P. Sienkiewicz, *Wizje i modele wojny informacyjnej...*, s. 376-377.

[29] D.M. Hollis, *USCYBERCOM. The Need for a Combatant Command versus Subunified Command*, „Joint Force Quarterly" Vol. 58, 2010, No 3.

ZAGROŻENIA TELEINFORMATYCZNE JAKO WYZWANIE DLA NATO

W świetle opisanych powyżej zagrożeń warto podjąć próbę wskazania kilku najpoważniejszych dylematów, przed którymi stoi obecnie Sojusz Północnoatlantycki. Podstawowym dokumentem, który reguluje współpracę państw członkowskich *NATO* jest traktat waszyngtoński z 4 kwietnia 1949 r. Art. 5 tego dokumentu stanowi:

> „Strony zgadzają się, że zbrojna napaść na jedną lub kilka z nich w Europie lub Ameryce Północnej będzie uważana za napaść przeciwko nim wszystkim; wskutek tego zgadzają się one na to, że jeżeli taka zbrojna napaść nastąpi, każda z nich, w wykonaniu prawa do indywidualnej lub zbiorowej samoobrony, uznanego przez artykuł 51 Karty Narodów Zjednoczonych, udzieli pomocy Stronie lub Stronom tak napadniętym, podejmując natychmiast indywidualnie i w porozumieniu z innymi Stronami taką akcję, jaką uzna za konieczną, nie wyłączając użycia siły zbrojnej, w celu przywrócenia i utrzymania bezpieczeństwa obszaru północnoatlantyckiego". Art. 6 doprecyzowuje, iż za zbrojną napaść rozumie się „napaść zbrojną na terytorium którejkolwiek ze Stron w Europie lub Ameryce Północnej (...); na siły zbrojne, okręty lub samoloty którejkolwiek ze Stron znajdujące się na tych terytoriach lub nad nimi"[30].

Tekst traktatu sporządzony w okresie narastającej zimnej wojny brał oczywiście pod uwagę jedynie możliwość wystąpienia konfliktu przy zastosowaniu środków konwencjonalnych oraz broni masowego rażenia. W tamtym okresie zapisy tego typu były więc w dużej mierze wystarczające, choć i tak niepozbawione pewnych kontrowersji[31]. Jednak w kontekście powyższych rozważań, ustalenia traktatu waszyngtońskiego wydają się nie przystawać do wyzwań XXI w.[32] Należy tu wskazać na kilka poważnych dylematów. Po pierwsze, napaść zbrojna w rozumieniu tego dokumentu pomija nie tylko same metody ataków oraz środki, jakie można wykorzystać w cyberprzestrzeni, ale także skutki tego typu działań. Cyberataki z reguły bowiem nie mają związku z kategorią terytorium państwowego. Jak słusznie zauważył Bryan W. Ellis, ze względu na swoją specyfikę sygnał elektroniczny jest poważnym wyzwaniem dla pojęcia granic państw, suwerenności oraz integralności terytorialnej. W zdecydowanej większości przypadków atak dokonany za pomocą sieci teleinformatycznej nie przyczynia się bowiem do powstania namacalnych, fizycznych zniszczeń dla „sił zbrojnych, okrętów lub samolotów", z czym tradycyjnie utożsamiana jest napaść. Szkody wyrządzone poprzez cyberprzestrzeń mają – zdaniem B.W. Ellisa – zupełnie inny, niematerialny charakter[33].

---

[30] *Traktat Północnoatlantycki*, Dz.U.00.87.970, Waszyngton, 04.04.1949.

[31] Zob. F. Costigliola, *France and the United States. The Cold Alliance Since World War II*, New York 1992, s. 68.

[32] Warto dodać, iż problem interpretacji i wdrożenia art. 5 traktatu północnoatlantyckiego pojawił się również w kontekście zagrożeń asymetrycznych i wojny z terroryzmem. Zob. S. Koziej, *Euroatlantycki „tandem bezpieczeństwa"*, w: P. Olszewski, T. Kapuśniak, W. Lizak (red.), *Bezpieczeństwo międzynarodowe. Wyzwania i zagrożenia XXI wieku*, Radom 2009, s. 56-57.

[33] B.W. Ellis, *The International Legal Implications and Limitations of Information Warfare: What Are Our Options?*, U.S. Army War College, Carlisle Barracks 2001, s. 3.

Pewnym rozwiązaniem tego dylematu byłoby oficjalne uznanie cyberprzestrzeni za kolejny teatr wojny[34]. W tym kierunku idzie praktyka niektórych państw członkowskich, w tym przede wszystkim Stanów Zjednoczonych, a także części gremiów eksperckich. Przyjmując takie rozwiązanie, włamanie komputerowe mogłoby zostać sklasyfikowane jako agresja zbrojna[35]. Niestety również i w tym wypadku powstają określone wątpliwości natury praktycznej. Biorąc pod uwagę często zdecentralizowany i anonimowy charakter ataków teleinformatycznych, przeprowadzanych np. przy użyciu sieci *botnet*[36], ich organizator mógłby się posłużyć komputerami należącymi do państwa trzeciego[37]. Tym samym odpowiedź na cyberatak mogłaby dotknąć kraju zupełnie z nim niezwiązanego.

Zagadnienie to łączy się z kolejnym dylematem, dotyczącym identyfikacji oraz właściwej interpretacji incydentów. Jak wspomniano wcześniej, istnieje zasadniczy problem dotyczący rozróżnienia między włamaniami inspirowanymi bądź przeprowadzonymi przez instytucje państwowe a aktami cyberprzestępczości. W wielu przypadkach jest to wręcz niemożliwe, działania te mają bowiem w praktyce bardzo podobny charakter. Przykładowo, aktywność zatrudnionych przez chińskie władze cyberszpiegów nie różni się niczym od tego typu działalności motywowanej względami finansowymi[38]. Co prawda, niemal zawsze da się zidentyfikować adres *IP*[39], z którego dokonano ataku, jednak nie oznacza to zarazem odkrycia tożsamości osób lub organizacji, które w rzeczywistości za nim stały. Z punktu widzenia mechanizmów reakcji Sojuszu Północnoatlantyckiego jest to problem o fundamentalnym znaczeniu. Zakwalifikowanie ataku jako działalności cyberprzestępczej nie pociągałoby bowiem za sobą uruchomienia rozwiązań na poziomie ponadnarodowym.

Po trzecie, należy zauważyć, iż nie ma ogólnie przyjętych i jednoznacznych kryteriów, które mogłyby pomóc w ocenie skali oraz znaczenia poszczególnych

[34] J.A. Warden, *Enemy as a System...*, s. 40-55; P. Sienkiewicz, *Wizje i modele wojny informacyjnej...*, s. 376-377.

[35] Zob. M.N. Schmitt (red.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge 2013, s. 42-52.

[36] Sieci *botnet* składają się z grupy komputerów, zainfekowanych złośliwym oprogramowaniem i kontrolowanych z zewnątrz. Mogą zostać wykorzystane np. do cyberataków typu *DDoS*. Zob. C. Wilson, *Botnets, Cybercrime and Cyberterrorism: Vulnerabilities and Policy Issues for Congress*, „CRS Report for Cogress" 29.01.2008.

[37] Należy pamiętać, iż tak rosyjscy, jak i chińscy hakerzy potrafią przejmować kontrolę nad komputerami znajdującymi się np. w Ameryce Północnej czy w Europie. Zob. N. Sahrawat, *Chinese Botnet-for-Hire Uncovered*, „TheCTOForum" 22.09.2010, http://www.thectoforum.com (dostęp: 25.02.2013).

[38] Zob. A. Melnitzky, *Defending America Against Chinese Cyber Espionage Through the Use of Active Defenses*, „Cardozo Journal of International and Comparative Law" Vol. 20.2, winter 2012; *Communist Chinese Cyber-Attacks, Cyber-Espionage and Theft of American Technology*, Hearing Before the Subcommittee on Oversight and Investigations of the Committee on Foreign Affairs, House of Representatives, Serial No. 112-14, 15.04.2011.

[39] *Internet Protocol* (ang.).

ataków na sieci teleinformatyczne. O wadze problemu świadczy fakt, iż w niektórych państwach liczbę incydentów tego typu liczy się w milionach dziennie[40]. Szczegółowa analiza każdego z nich pod kątem reakcji międzynarodowej wydaje się mało realna. Stąd powstaje pytanie, które z tych wydarzeń należałoby uznać za tyle istotne, aby zainteresował się nim Sojusz Północnoatlantycki? Pewnym rozwiązaniem tego problemu mogłaby być reakcja tylko na te cyberataki, które miałyby charakter masowy (jak np. w Estonii bądź w Gruzji) lub poważnie zagroziłyby funkcjonowaniu infrastruktury krytycznej państwa. Takie rozwiązanie pomijałoby jednak pojedyncze incydenty o charakterze terrorystycznym lub szpiegowskim. Szczególnie w tym drugim przypadku nielegalne wyprowadzenie z serwerów kraju członkowskiego *NATO* informacji niejawnych mogłoby bowiem w zasadniczym stopniu wpłynąć na bezpieczeństwo całej wspólnoty euroatlantyckiej[41].

NATO WOBEC ZAGROŻEŃ DLA BEZPIECZEŃSTWA TELEINFORMATYCZNEGO

Pierwsze działania zmierzające do walki z cyberzagrożeniami *NATO* podjęło już na przełomie XX i XXI w., w reakcji na ataki serbskich hakerów podczas interwencji w Kosowie. W ich wyniku na kilka dni strona internetowa Sojuszu dotycząca misji na Bałkanach została zablokowana, co częściowo utrudniło jego politykę informacyjną. Na szczycie praskim w 2002 r. powołano więc Zdolność Reagowania na Incydenty Komputerowe (*Computer Incident Response Capability – CIRC*), z centrum koordynacyjnym w Brukseli i centrum technicznym w Mons. Głównym zadaniem tego nowego organu było wykrywanie oraz zwalczanie nie tylko wirusów komputerowych, ale także wszelkiego rodzaju włamań do sieci Sojuszu[42]. Podjęte wówczas prace okazały się jednak niedostateczne, gdyż objęły one jedynie niektóre obszary funkcjonowania samej organizacji, pomijając chociażby procedury udzielenia pomocy państwom członkowskim czy problem interpretacji art. 5 traktatu waszyngtońskiego. W świetle omówionych powyżej wyzwań

[40] *U.S. Nukes Face Up to 10 Million Cyber Attacks Daily*, US News, 20.03.2012, http://www.usnews.com/news/articles/2012/03/20/us-nukes-face-up-to-10-million-cyber-attacks-daily (dostęp: 30.11.2012).

[41] Wyzwań o charakterze prawnym, politycznym i wojskowym w kontekście zagrożeń teleinformatycznych jest naturalnie zdecydowanie więcej. Szerzej na temat wątpliwości oraz możliwych rozwiązań: A. Bufalini, *Les cyber-guerres à la lumière des règles international es sur l'interdiction du recours à la force*, w: M. Arcari, L. Balmond (red.), *La gouvernance globale face aux defis de la securité collective*, Napoli 2012; M.N. Schmitt (red.), *Tallinn Manual...*; E. Colarik, L. Janczewski, *Establishing Cyber Warfare Doctrine*, „Journal of Strategic Security" 2012, No 1; A.D. Sofaer, D. Clark, W. Diffie, *Cyber Security and International Agreements*, w: *Proceedings of a Workshop on Deterring Cyberattacks*, Washington D.C. 2010; M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku...*, s. 154-157.

[42] S. Myrli, *NATO and Cyber Defence*, NATO Parliamentary Assembly, 173 DSCFC 09 E BIS.

i dylematów nieprzygotowanie Sojuszu do walki z cyberzagrożeniami zostało w pełni obnażone dopiero w kwietniu 2007 r., podczas wydarzeń w Estonii. Wówczas rosyjscy hakerzy, ze względu na spór polityczny na linii Tallin-Moskwa wokół pomnika tzw. Brązowego Żołnierza, dokonali masowych ataków komputerowych na estońską cyberprzestrzeń. Ich łupem padły strony najważniejszych instytucji państwowych, mediów oraz banków. Premier Estonii stwierdził wówczas, iż na jego kraju przetestowano „nowy model wojny cybernetycznej". Tallin wezwał Sojusz Północnoatlantycki oraz Unię Europejską do podjęcia zdecydowanych działań zmierzających do znalezienia właściwej odpowiedzi na tego typu zagrożenia. Warto również przypomnieć wypowiedź estońskiego ministra obrony Jaaka Aaviksoo. Porównał on bowiem incydenty z kwietnia 2007 r. do zamachów terrorystycznych na *World Trade Center*. Podkreślił także, iż oznaczało to pojawienie się poważnego problemu dla Sojuszu Północnoatlantyckiego, który nie uznawał dotychczas cyberataków za akty o charakterze militarnym[43].

Nie ulega wątpliwości, iż to właśnie te wydarzenia przekonały władze Sojuszu do wagi zagrożeń teleinformatycznych. Co prawda, część krajów członkowskich ze Stanami Zjednoczonymi na czele już od dawna rozwijała swój potencjał w tej dziedzinie, jednak dopiero w kwietniu 2007 r. skala tego problemu została w pełni dostrzeżona przez samą organizację. Pierwszą reakcją *NATO* na te wydarzenia było wysłanie do Estonii kilku ekspertów komputerowych, którzy nie zdołali jednak odegrać większej roli. Następnie problem ten poruszono na spotkaniu Rosja – Unia Europejska w Samarze. W rezultacie tych doświadczeń bezpieczeństwo teleinformatyczne stało się kluczowym tematem omawianym na spotkaniach Sojuszu Północnoatlantyckiego w czerwcu i październiku 2007 r. Na pierwszym z nich przyjęto ramowy dokument, który wymienił najważniejsze działania, które należało podjąć w tej dziedzinie w przyszłości. W październiku natomiast na szczycie w Nordwijk ministrowie obrony zapoznali się z raportem oceniającym przygotowania organizacji do zwalczania zagrożeń w cyberprzestrzeni. Zawarto w nim wiele rekomendacji i zadań do zrealizowania w kolejnych latach[44]. Zainteresowanie tą problematyką potwierdzono już na początku następnego roku. W styczniu opracowano tajny dokument *NATO on Cyber Defence Policy*. Został on zatwierdzony przez głowy państw i rządów na szczycie w Bukareszcie 3 kwietnia 2008 r. Ponadto we wspólnej deklaracji końcowej z tego spotkania zawarto istotny punkt dotyczący cyberbezpieczeństwa. Stwierdzono w nim, iż *NATO* będzie podejmowało działania

[43] Zob. K. Ruus, *Cyber War I: Estonia Attacked from Russia...*; H. Laasme, *Estonia: Cyber Window into the Future of NATO...*; I. Traynor, *Russia Accused of Unleashing Cyberwar to Disable Estonia*, „The Guardian" 17.05.2007; *Estonia urges firm EU, NATO response to new form of warfare: cyber-attacks*, „The Sydney Morning Herald" 16.05.2007, http://www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfarecyberattacks/2007/05/16/1178995207414.html (dostep: 10.01.2013); M. Lakomy, *Znaczenie cyberprzestrzeni dla bezpieczeństwa państw...*, s. 61-62.

[44] S. Myrli, *NATO and Cyber Defence...*

na rzecz „wzmocnienia (...) kluczowych systemów informacyjnych przeciwko cyberatakom". Podkreślając znaczenie *NATO on Cyber Defence Policy*, strony zobowiązały się do budowy struktur, które miały przejąć odpowiedzialność za realizację nowych wytycznych w tej dziedzinie. Zadeklarowano także chęć rozwoju współpracy w wymiarze cyberbezpieczeństwa między Sojuszem Północnoatlantyckim a państwami członkowskimi, co należy uznać za próbę politycznej odpowiedzi na wydarzenia w Estonii[45].

Już w maju 2008 r. 7 członków *NATO* wraz z Sojuszniczym Dowództwem Transformacji (*Allied Command Transformation – ACT*) utworzyło w Tallinie Centrum Doskonalenia Cyberobrony (*Cooperative Cyber Defence Centre of Excellence – CCD COE*). Pierwotnie w ramach nowej instytucji współpracowały: Estonia, Niemcy, Włochy, Łotwa, Litwa, Słowacja oraz Hiszpania. Podczas ceremonii założycielskiej dowódca ds. transformacji gen. James Mattis stwierdził, iż centrum ma przygotować *NATO* do wyzwań pojawiających się w cyberprzestrzeni. Do głównych zadań tej struktury zaliczono: przygotowywanie doktryn i koncepcji walki z zagrożeniami teleinformatycznymi, prowadzenie wspólnych ćwiczeń i kursów dla państw członkowskich, prowadzenie badań, analizę cyberataków oraz doradztwo. Polska dołączyła do grona państw współpracujących w *CCD COE* dopiero w listopadzie 2011 r. Warto podkreślić wysoką aktywność i przydatność tego nowego organu. Przykładowo, pod koniec 2012 r. Centrum opublikowało, po trzech latach prac, podręcznik *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Zawarto w nim opinie grupy ekspertów na temat możliwości zastosowania istniejących norm prawa międzynarodowego do konfliktów w cyberprzestrzeni. Jest to obecnie jedno z nielicznych tak kompleksowych opracowań na ten temat. Z pewnością należy ocenić je pozytywnie jako podstawę do dalszych prac organizacyjnych i prawnych w tej dziedzinie nie tylko dla Sojuszu Północnoatlantyckiego, ale także dla Organizacji Narodów Zjednoczonych[46]. Ponadto, struktura ta organizuje regularne ćwiczenia i szkolenia dla specjalistów z zakresu cyberbezpieczeństwa, w tym np. *Baltic Cyber Shield* 2010, *Locked Shield* 2012 i 2013[47]. W tym kontekście nie ulega wątpliwości, iż instytucja ta nie tylko stała się symbolem rozciągnięcia na Estonię natowskiego parasola bezpieczeństwa teleinformatycznego, ale uzyskała także szeroki wachlarz uprawnień, które mają przyczynić się do wypracowania bardziej skutecznych rozwiązań w tej dziedzinie[48].

---

[45] *Bucharest Summit Declaration*, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Bucharest on April 3 2008, NATO Official Texts 03.04.2008; S. Myrli, *NATO and Cyber Defence*....

[46] Zob. M.N. Schmitt (red.), *Tallinn Manual*...

[47] *Cyber Defense Exercises*, NATO Cooperative Cyber Defence Center of Excellence, http://www.ccdcoe.org/353.html (dostęp: 27.05.2013).

[48] *NATO opens new center of excellence on cyber defence*, North Atlantic Treaty Organization News, 14.05.2008, http://www.nato.int/docu/update/2008/05-may/e0514a.html (dostep: 25.11.2012); *Przyjęcie Polski do Centrum Cyberobrony NATO w Tallinie*, Ministerstwo Obrony Narodowej RP,

Na początku 2008 r. powstała także druga struktura odpowiedzialna za cyberbezpieczeństwo Sojuszu – Organ Zarządzający Cyberobroną (*Cyber Defence Management Authority – CDMA*). W przeciwieństwie do *CCD COE*, przekazano mu zadania przede wszystkim w wymiarze praktycznym. *CDMA* uzyskało szerokie uprawnienia w zakresie reagowania na zagrożenia teleinformatyczne, jak również koordynacji wysiłków państw członkowskich oraz innych organów *NATO*. Do jego kompetencji zaliczono również kwestie związane z wypracowaniem odpowiednich procedur i standardów, jeśli chodzi o zapobieganie, wykrywanie i odpieranie cyberataków. Co ciekawe, w kontekście omówionych powyżej dylematów stwierdzono, iż *CDMA* powinno zajmować się wszystkimi zagrożeniami teleinformatycznymi, bez względu na to, czy są one inspirowane przez państwa, czy też są aktami cyberprzestępczości. *CDMA* stanowi więc jedną z centralnych instytucji odpowiedzialnych za ochronę *NATO* oraz państw członkowskich w wypadku poważnych ataków hakerskich. Dysponuje ona odpowiednim potencjałem, aby udzielić natychmiastowej pomocy zaatakowanemu przez sieć państwu członkowskiemu, co stanowiło problem w kwietniu 2007 r. O jej dynamicznym rozwoju może świadczyć fakt, iż już w ciągu pierwszych 10 miesięcy funkcjonowania przeprowadziła wspólnie ćwiczenia państw członkowskich w cyberprzestrzeni. Wysłała także swojego eksperta do Gruzji w sierpniu 2008 r.[49]

Równolegle z rozbudową struktur odpowiedzialnych za bezpieczeństwo teleinformatyczne, Sojusz prowadził dalsze prace w wymiarze koncepcyjnym. Świadczyła o tym deklaracja końcowa szczytu w Strasburgu z 4 kwietnia 2009 r., gdzie ponownie podkreślono, że cyberbezpieczeństwo stało się priorytetem dla Paktu Północnoatlantyckiego. Potwierdzono także, iż organizacja będzie kontynuowała wysiłki na rzecz rozwoju potencjału w tej dziedzinie, mając świadomość szkodliwych działań podejmowanych w sieci tak przez państwa, jak i aktorów pozapaństwowych. Za dotychczasowe sukcesy *NATO* uznano powołanie nowych instytucji zajmujących się cyberbezpieczeństwem (*CCD COE*, *CDMA*) oraz usprawnienie już tych istniejących (*CIRC*). Co ciekawe, zadeklarowano chęć wzmocnienia współpracy w tej dziedzinie między *NATO* a krajami partnerskimi oraz innymi organizacjami międzynarodowymi. Podkreślono też potrzebę prowadzenia sojuszniczych ćwiczeń w cyberprzestrzeni[50].

17.11.2011, http://mon.gov.pl/pl/artykul/12117 (dostęp: 25.11.2012); *The Tallin Manual*, CCD COE, http://ccdcoe.org/249.html (dostęp: 26.11.2012).

[49] Obecnie *CDMA* występuje w procesie decyzyjnym *NATO* jako *Cyber Defence Management Board*. Zob. *NATO sets up Cyber Defence Management Authority in Brussels*, „ComputerWeekly" 4.04.2008, http://www.computerweekly.com/news/2240085580/Nato-sets-up-Cyber-Defence-Management-Authority-in-Brussels (dostęp: 26.11.2012); S. Myrli, *NATO and Cyber Defence...*; *Defending the networks. The NATO Policy on Cyber Defence*, NATO 2011, http://www.nato.int/nato_static/assets/pdf/pdf_2011_08/20110819_110819-policy-cyberdefence.pdf (dostęp: 27.05.2013).

[50] *Strasbourg/Kehl Summit Declaration*, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Strasbourg/Kehl, 4.04.2009.

Sporo miejsca poświęcono tej problematyce także na szczycie w Lizbonie w 2010 r. Przede wszystkim rozbudowa natowskich zdolności działania w sieci (pkt 2) znalazła się wśród najważniejszych priorytetów organizacji. Do najpoważniejszych wyzwań o charakterze transnarodowym, obok takich spraw jak proliferacja broni masowego rażenia lub terroryzm (pkt 24), zaliczono właśnie zagrożenia teleinformatyczne. W tym kontekście, szczególne znaczenie położono na rozbudowę możliwości *Computer Incident Response Capability*, która miała osiągnąć pełną gotowość operacyjną do końca 2012 r. Zadeklarowano także, iż Sojusz będzie blisko współpracował w tej dziedzinie z Unią Europejską oraz Organizacją Narodów Zjednoczonych[51]. Ciekawe sformułowanie zawarto również w przyjętej w Lizbonie nowej koncepcji strategicznej. Stwierdzono tam bowiem, iż:

> „Ataki cybernetyczne stają się coraz częstsze, lepiej zorganizowane i bardziej kosztowne, biorąc pod uwagę szkody, jakie wyrządzają administracjom rządowym, biznesowi, gospodarce, a potencjalnie także transportowi, sieciom dostaw i innej infrastrukturze krytycznej; mogą one osiągnąć poziom, którego przekroczenie zagraża narodowemu i euroatlantyckiemu dobrobytowi, bezpieczeństwu i stabilności. Źródłem takich ataków mogą być obce siły wojskowe i służby wywiadowcze, zorganizowane grupy przestępcze, terrorystyczne i/lub grupy ekstremistyczne"[52].

Potwierdzono tym samym rosnącą świadomość nowych wyzwań, które pojawiły się w cyberprzestrzeni na początku XXI w.

Bezpośrednią kontynuacją tych wysiłków było przyjęcie 8 czerwca 2011 r. zaktualizowanego dokumentu *NATO Policy on Cyber Defence*, który zwrócił szczególną uwagę na kilka kwestii. Przede wszystkim dokument ten opierał się na przekonaniu, iż zabezpieczenie cyberprzestrzeni jest warunkiem *sine qua non* realizacji w XXI w. kluczowych funkcji Sojuszu Północnoatlantyckiego, a więc reagowania kryzysowego i kolektywnej obrony. Po drugie, uznano, iż priorytetem jest prewencja cyberataków oraz obrona infrastruktury krytycznej tak samej organizacji, jak i państw członkowskich. Po trzecie, wskazano na potrzebę budowy scentralizowanego systemu zabezpieczeń sieci Sojuszu. Po czwarte, zaakcentowano kwestię określenia minimalnych wymogów dla zabezpieczeń komputerowych krajów członkowskich na obszarach bezpośrednio związanych z funkcjonowaniem struktur wojskowych organizacji. Po piąte, potwierdzono chęć pomocy sojusznikom w celu osiągnięcia postulowanych standardów zabezpieczeń. Wreszcie po szóste, podkreślono potrzebę współpracy nie tylko z organizacjami międzynarodowymi, ale także ze środowiskiem naukowym oraz sektorem prywatnym[53]. Warto również

---

[51] *Lisbon Summit Declaration*, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Lisbon, 20.11.2012.

[52] *Koncepcja Strategiczna NATO*, Biuro Bezpieczeństwa Narodowego, 17.01.2011, http://www.bbn.gov.pl/portal/pl/2/2694/Koncepcja_Strategiczna_NATO__tlumaczenie.html (dostęp: 26.11.2012).

[53] Za J. Healey, L. van Bochoven, *NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow*, „Atlantic Council Issue Brief" 27.02.2012, s. 3.

wspomnieć o ustaleniach poczynionych na szczycie *NATO* w Chicago w maju 2012 r. Potwierdzono tam przywiązanie państw członkowskich do rozwoju sojuszniczych zdolności reagowania kryzysowego w cyberprzestrzeni, które miało być oparte od końca 2012 r. na wspomnianej już *Computer Incident Response Capability*. Celem reformy tego organu było wprowadzenie takich procedur, które pozwoliłyby na objęcie pełną ochroną *CIRC* wszystkich obszarów funkcjonowania organizacji. Co więcej, podkreślono także potrzebę daleko idącej współpracy w tej dziedzinie z partnerami międzynarodowymi, w tym przede wszystkim z Unią Europejską, Radą Europy, Organizacją Narodów Zjednoczonych oraz Organizacją Bezpieczeństwa i Współpracy w Europie[54].

Jednym z najciekawszych rezultatów tych prac było wysunięcie w 2011 r. projektu powołania specjalnych, sześcioosobowych Zespołów Szybkiego Reagowania (*Rapid Reaction Teams*), które *NATO* natychmiast mogłoby skierować do zaatakowanego w cyberprzestrzeni państwa członkowskiego. Według zapowiedzi, miały one osiągnąć pełną operacyjność do końca 2012 r. Inicjatywa ta została skierowana przede wszystkim do państw, które nie zdążyły jeszcze wypracować odpowiednich rozwiązań w dziedzinie bezpieczeństwa teleinformatycznego bądź nie dysponują wystarczającym potencjałem. Według projektu, *RRT* powinny być uruchomione tylko po otrzymaniu odpowiedniego wniosku od kraju członkowskiego oraz w pełni mu podlegać. Z jednej strony, inicjatywę tę należy więc uznać za próbę instytucjonalizacji natowskiej praktyki wysyłania do zaatakowanych państw swoich ekspertów. Z drugiej natomiast, można ją zinterpretować jako gest podkreślający znaczenie sojuszniczej solidarności także w wymiarze cyberprzestrzeni[55].

Pierwszego lipca 2012 r. *NATO* powołało również Agencję ds. Komunikacji i Informacji (*NATO Communications and Information Agency – NCIA*), która powstała z połączenia: *NC3A*, *NACMA*, *NCSA* i *ALTBMD*. Jest odpowiedzialna za usługi w zakresie *C4ISR*, czyli dowodzenia, kontroli, komunikacji, komputerów, wywiadu oraz obserwacji i rozpoznania. Posiada bardzo szeroki zakres kompetencji, rozciągający się od prac badawczych i koncepcyjnych, przez rozwój potencjału w tej dziedzinie, aż po prowadzenie misji i szkoleń. Jednym z najważniejszych aspektów działalności *NCIA* jest cyberobrona. Najdonioślejszym dotychczas efektem prac Agencji było wsparcie udzielone Międzynarodowemu Projektowi Rozwoju Zdolności Cyber-Obrony (*Multinational Cyber Defence Capabilities Development Project*), zainicjowanemu w marcu 2013 r. przez pięć państw Sojuszu: Kanadę, Danię, Holandię, Norwegię i Rumunię. Zasadniczym celem tego projektu jest rozwój krajowych zdolności obrony przed zagrożeniami teleinformatycznymi poprzez kooperację międzynarodową. Jego autorzy przewidują m.in. koordynację

[54] *Chicago Summit Declaration*, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago, 20.05.2012.

[55] *NATO Rapid Reaction Team to fight cyber attack*, North Atlantic Treaty Organization News, 13.03.2012, http://www.nato.int/cps/en/natolive/news_85161.htm (dostep: 26.11.2012).

narodowych prac badawczych i technicznych w tej dziedzinie oraz wymianę informacji o zagrożeniach i sposobach ich zwalczania. Jest to inicjatywa w pełni otwarta dla innych państw członkowskich Paktu[56].

Warto również pamiętać, iż w ramach struktur *NATO* funkcjonują inne organy, posiadające uprawnienia w zakresie cyberbezpieczeństwa. Należy do nich zaliczyć m.in.:

– Wydział Wschodzących Wyzwań dla Bezpieczeństwa Kwatery Głównej (*Headquarters Emerging Security Challenges Division*), który zajmuje się nietradycyjnymi zagrożeniami dla bezpieczeństwa Sojuszu Północnoatlantyckiego, w tym m.in. cyberbezpieczeństwem, terroryzmem oraz proliferacją broni masowego rażenia;

– Agencja C3 (*C3 Agency*), która zajmuje się m.in. rozpoznawaniem potrzeb operacyjnych oraz wdrażaniem nowych rozwiązań w dziedzinie cyberbezpieczeństwa;

– Sojusznicze Dowództwo Transformacji (*Allied Command Transformation*), które jest odpowiedzialne przede wszystkim za koncepcyjne podejście do tej problematyki. Ponadto, dowództwo nadzoruje funkcjonowanie *CCD COE* w Tallinie.

Należy także dodać, iż w sensie formalnym polityczną pieczę nad całością polityki cyberbezpieczeństwa *NATO* sprawuje przede wszystkim Rada Północnoatlantycka, która formułuje ogólne założenia kierunków jej rozwoju. W sensie praktycznym jest ona konkretyzowana na poziomie Komitetu Planowania i Polityki Obrony (*Defense Policy and Planning Committee*)[57].

ZAKOŃCZENIE

Polityka cyberbezpieczeństwa *NATO* od początku XXI w. przeszła poważną ewolucję. Zainicjowana przede wszystkim w wyniku incydentów wokół interwencji zbrojnej w Kosowie, przez wiele lat pozostała na dalszym planie działalności Sojuszu Północnoatlantyckiego. Państwa członkowskie, skupiając się na innych wyzwaniach obejmujących przede wszystkim wojnę z terroryzmem oraz opracowanie nowej koncepcji strategicznej, zignorowały coraz wyraźniejsze sygnały zagrożeń pojawiających się w cyberprzestrzeni. W tym kontekście dopiero bezsilność struktur Paktu Północnoatlantyckiego wobec ataków komputerowych na Estonię w kwietniu 2007 r. doprowadziła do przełomu. Od tej pory państwa *NATO* w stopniu zdecydowanie większym niż wcześniej podjęły działania zmierzające do opracowania właściwej reakcji na te wyzwania. Prace w tej dziedzinie przebiegały dwutorowo, z jednej strony podjęto rozbudowę praktycznych środków reagowania

[56] Zob. *Multinational Cyber Defence Capability Development – MN CD2*, NATO Communications and Information Agency, Brussels 2013.

[57] Za J. Healey, L. van Bochoven, *NATO's Cyber Capabilities...*, s. 4.

na incydenty teleinformatyczne, z drugiej natomiast przygotowano odpowiednie założenia koncepcyjne. Szczególnie wartościowym osiągnięciem Sojuszu było zbudowanie systemu wzajemnie wspierających się organów, których zadaniem jest nie tylko zabezpieczenie infrastruktury krytycznej samego *NATO*, ale także pomoc państwom członkowskim. Co więcej, działania podjęte po 2007 r. wskazywały, iż Sojusz pragnął zapobiec powtórzeniu się sytuacji nie tylko z Estonii, ale także z Gruzji. Tak bowiem należało rozumieć zapisy dotyczące wspierania w cyberprzestrzeni również partnerów Paktu Północnoatlantyckiego. Za dużą zaletę przyjętych rozwiązań należy uznać również stosunkowo prostą strukturę organizacyjną, której priorytetem jest przede wszystkim obrona państw członkowskich, koordynacja, wspólne ćwiczenia oraz podnoszenie kompetencji w tej dziedzinie. Innym pozytywnym aspektem nowej polityki bezpieczeństwa teleinformatycznego *NATO* jest z pewnością rosnąca świadomość dynamicznej natury zagrożeń pojawiających się w sieci. Implikuje to regularne aktualizowanie tak rozwiązań koncepcyjnych, jak i praktycznych wobec stale zmieniających się uwarunkowań cyberprzestrzennych. Wreszcie, warto podkreślić fakt prowadzenia przez Sojusz konsultacji z innymi organizacjami międzynarodowymi, środowiskiem naukowym i sektorem prywatnym, co jest niezbędne, aby trafnie identyfikować wyzwania i prawidłowo nań reagować.

Z drugiej jednak strony, jak słusznie zauważyła Hăly Laasme, polityka cyberbezpieczeństwa Sojuszu Północnoatlantyckiego pominęła wiele istotnych kwestii[58]. Jakkolwiek zapewniono sobie szerokie spektrum narzędzi reagowania na incydenty w cyberprzestrzeni, to nie ustalono wszystkich niezbędnych procedur i mechanizmów o charakterze politycznym, prawnym i militarnym. Przede wszystkim, mimo ciekawych propozycji *CCD COE*, nie zdecydowano się na jasną deklarację dotyczącą interpretacji art. 5 traktatu waszyngtońskiego. Tym samym jego wykorzystanie w wyniku ewentualnej cyberwojny pozostałoby decyzją *stricte* polityczną, co naturalnie osłabia zaufanie do sojuszniczej solidarności w tej dziedzinie oraz utrudnia jego późniejszą implementację. Po drugie, pojawia się także pytanie, czy Pakt Północnoatlantycki jako organizacja powinien dysponować ofensywnymi środkami walki w cyberprzestrzeni? Według Johna B. Sheldona nawet pozytywna odpowiedź może być trudna do realizacji ze względu na niechęć krajów członkowskich do dzielenia się najnowszymi narzędziami i technikami ataków komputerowych[59]. Po trzecie, w żadnym oficjalnym i jawnym dokumencie[60] Sojuszu nie określono również, które z incydentów teleinformatycznych

[58] H. Laasme, *Estonia: Cyber Window into the Future of NATO...*, s. 63.

[59] Zob. J.B. Sheldon, *NATO and Cyber Defense: Hanging Together or Hanging Separately?* United Nations Institute for Disarmament Research, http://www.unidir.org/en/Audio/listerAudio/id-Conference:165 (dostęp: 27.05.2013).

[60] Ciekawe pomysły na ten temat pojawiły się w *Tallin Manual on the Internaitonal Law Applicable to Cyber Warfare*, który nie ma jednak żadnej mocy obowiązującej. Zob. M.N. Schmitt (red.), *Tallinn Manual...*, s. 42-52.

mogłyby się spotkać z reakcją całej organizacji. Pod uwagę, jak wskazano wcześniej, należałoby tu wziąć tak skalę ataków, czas trwania, jak i rzeczywiste zagrożenie, nie tylko dla infrastruktury krytycznej, ale i informacji niejawnych. Ponadto, jak stwierdzili Jason Healey i Leendert van Bochoven, otwartą kwestią pozostaje także identyfikacja sprawcy ataku. Trudno bowiem oczekiwać, aby Pakt Północnoatlantycki reagował w sytuacjach, w których sprawcami są obywatele poszkodowanego kraju członkowskiego[61]. Wreszcie, nie określono jasnego stosunku wobec aktów cyberszpiegostwa, które również mogą wywrzeć istotny wpływ na bezpieczeństwo *NATO*.

Reasumując należy stwierdzić, iż Sojusz Północnoatlantycki po 2007 r. zbudował ciekawą i – jak na razie – efektywną strategię walki z zagrożeniami teleinformatycznymi. Jednocześnie nie wypracowano jednak stanowiska wobec kilku wymienionych wyżej dylematów natury prawnej i politycznej. Wydaje się, iż jest to największa słabość jego nowej polityki cyberbezpieczeństwa. Prawidłowe ustosunkowanie się do tych wątpliwości może mieć bowiem w przyszłości fundamentalny wpływ na sytuację bezpieczeństwa całej strefy euroatlantyckiej.

ABSTRACT

Dynamic development of the Internet since the end of the 20th century, despite its indisputable advantages, opened new challenges to the security of states. The first major cyber-incidents took place in the 1980s and 1990s. Later on they evolved into organized, harmful activities both of states and non-state actors. A breakthrough in this respect took place in 2007, when Estonia became the first country to be massively attacked by politically motivated hackers. It proved that the North Atlantic Treaty Organization was not prepared to fight these unconventional threats. Over the next six years, NATO elaborated a new cyber security policy based on the awareness that ICT technologies are increasingly important for the international environment. This process was accompanied by the development of new structures and institutions, which were tasked to fight cyber attacks. On the one hand, in this context, it is important to underscore that NATO has employed the proper way of countering these challenges. On the other hand, however, it did not address multiple, still valid dilemmas concerning, among others, the interpretation of article 5 of the Washington Treaty. Finding a way to solve these problems will determine the security of the Euro-Atlantic community in the future.

[61] J. Healey, L. van Bochoven, *NATO's Cyber Capabilities...*, s. 6.