DOI: https://doi.org/10.34862/rbm.2020.2.9

Marek Kulczycki
Uniwersytet Wrocławski
marek.kulczycki@uwr.edu.pl
https://orcid.org/0000-0002-2713-3714

Rozwój zdolności NATO wobec zagrożeń cybernetycznych

Abstrakt: Zagrożenia, które związane są z cyberprzestrzenią, obejmują wszystkie podmioty współczesnego środowiska bezpieczeństwa, w tym również Organizację Traktatu Północnoatlantyckiego. Z uwagi na to, że stają się one coraz częstsze, bardziej złożone i dotyczą coraz więcej sektorów bezpieczeństwa, NATO zmuszone było podjąć określone kroki w dziedzinie cyberbezpieczeństwa. Przedmiotem badania w przedstawionym artykule są działania, które zostały podjęte przez Sojusz w odpowiedzi na dotychczasowe cyberzagrożenia. Zasadniczym celem badań było zidentyfikowanie tych działań, które przyczyniły się do rozwoju zdolności NATO do walki z zagrożeniami cybernetycznymi. W artykule wykorzystano metodę analizy krytycznej (literatury przedmiotu, artykułów naukowych, dokumentów, raportów, materiałów prasowych) oraz metodę historyczną. Głównym pytaniem badawczym jest: jakie dotychczasowe działania przyjęte przez Sojusz Północnoatlantycki przyczyniły się do budowy jego zdolności do zwalczania cyberzagrożeń? Główna teza artykułu zakłada, że dotychczasowe działania Sojuszu Północnoatlantyckiego będące odpowiedzią na zagrożenia cybernetyczne, miały wpływ na rozwój i wzmocnienie jego zdolności do obrony w tym obszarze. Rezultaty badań przedstawione w artykule wskazują na aktywność Sojuszu Północnoatlantyckiego w sferze cyberobrony, w szczególności tę, podjętą w okresie ostatnich pięciu lat. Należy się spodziewać, że działania te będą podstawą do dalszej aktywności Sojuszu, która obejmować będzie nie tylko działania defensywne, ale i również inne proaktywne służące poprawie bezpieczeństwa cybernetycznego wszystkich jego członków.

Słowa kluczowe: NATO, cyberbezpieczeństwo, cyberprzestrzeń, cyberzagrożenia, cyberobrona.

The Development of NATO's Capabilities of Tackling Cyber Threats

Abstract: Manifold dangers related to cyberspace concern all modern security environment entities, including the North Atlantic Treaty Organization. Due to the fact that they become ever more frequent and complex, NATO is in need of taking specific steps in this field. This paper presents the measures undertaken by the Alliance in response to current cyber threats. The main goal of the research was to identify those activities that have contributed to the development of NATO's capabilities concerning cyber threats. The article uses the method of critical analysis

(literature on the subject, scientific articles, documents, reports, press materials) and the historical method. The main research question is: what actions taken so far by the North Atlantic Alliance have contributed to extending its cyber threats capabilities? The thesis advanced in the article says that the North Atlantic Alliance's activities in this matter have impacted the development and the strengthening of its ability to defend this area. It should be expected that they will be the basis for the Alliance's further activity which will include not only defense policies, but also other pro-active activities in terms of contributing to the improvement of cyber security of all its members.

Keywords: NATO, cybersecurity, cyberspace, cyber threats, cyber defence

Wstęp

Gwałtowny rozwój technologii telekomunikacyjnej oraz systemów i narzędzi informatycznych w ostatniej dekadzie XX wieku sprawił, że zaczęły one odgrywać coraz ważniejszą rolę we wszystkich obszarach życia społecznego, w tym sferze militarnej. W 1993 roku ukazał się artykuł dwóch amerykańskich analityków zajmujących się bezpieczeństwem militarnym oraz stosunkami międzynarodowymi Johna Arquilla i Davida Ronfeldta – *Cyber war is Coming*. Jego autorzy przedstawili tezę, że nowe narzędzie, jakim jest Internet, które zaczyna opanowywać różne sfery życia człowieka, również będzie miało wpływ na obszar militarny i zasadniczo zmieni sposób prowadzenia wojny (Arquilla i Ronfeldt, 1997). Pomimo że pojawiły się pierwsze oznaki tego zjawiska, to w środowiskach polityczno-militarnych nie wszyscy zdawali sobie z tego sprawę i nie chcieli się z tą tezą zgodzić. Pierwsza dekada XXI wieku przyniosła jeszcze większe przyspieszenie w kwestiach zawansowania technologicznego wykorzystywanych narzędzi informatycznych i w konsekwencji potrzeby wykorzystania cyberprzestrzeni jako przestrzeni komunikacyjnej, tworzonej przez system powiązań internetowych.

Powstanie cyberprzestrzeni zapoczątkował proces zmian, który obejmował integrację techniczną oraz organizacyjną systemów informatycznych i telekomunikacyjnych, co doprowadziło do powstania zintegrowanej globalnej platformy teleinformatycznej. W pierwszej kolejności dokonano zmian w sposobie standaryzacji prezentacji informacji (ustalono jej format), następnie przeprowadzono integrację systemów informatycznych, a w końcu stworzono media elektroniczne, które dopełniły technosferę (Wrzosek, 2016, s. 45). Powyższe zmiany, związane z gwałtownym rozwojem technologii spowodowały, że „cyberprzestrzeń stworzyła zarówno wielkie możliwości, jak i poważne zagrożenia dla państw i podmioty niepaństwowe" (Osula i Rõigas, 2016, s. 11).

Sojusz Północnoatlantycki stosunkowo późno zaczął odpowiadać na zagrożenia

związane z cyberprzestrzenią, nie podejmując początkowo bezpośrednich działań powiązanych z rozwojem polityki bezpieczeństwa w cyberprzestrzeni. Pomimo że już w 1999 roku po raz pierwszy przeprowadzono atak na NATO, wykorzystując do tego cyberprzestrzeń, to i tak działania te nie wpłynęły w znaczący sposób na odpowiedź ze strony Sojuszu w kwestii cyberbezpieczeństwa. W konsekwencji doprowadziło to do zmarginalizowania problemu i zajęcia się innymi ważniejszymi wówczas problemami oraz wyzwaniami, przed którymi Sojusz miał stawić czoła i je rozwiązać. Już nieco inne, bardziej zaawansowane kroki podjęto w 2007 roku po ataku na Estonię, jednego z członków Sojuszu Północnoatlantyckiego. Właśnie ataki na to państwo pokazały między innymi możliwości wykorzystania cyberprzestrzeni do działań o szerokim spektrum i tym samym stały się podstawą do rozpoczęcia aktywności w tym obszarze ze strony Organizacji Traktatu Północnoatlantyckiego. Działania w tej sferze są rozwijane do dzisiaj, a ich znaczącym wynikiem są opracowane do tej pory dokumenty obejmujące zakres owej problematyki, a także działalność już istniejących instytucji zajmujących się tego typu zagrożeniami.

Ewolucja cyberzagrożeń skierowanych przeciw NATO

Organizacja Traktatu Północnoatlantyckiego od początku funkcjonowania musiała stawić czoła różnym formom zagrożeń, które związane były bezpośrednio ze zmieniającym się środowiskiem bezpieczeństwa. W okresie zimnowojennym były to w zasadniczej części zagrożenia związane z obszarem militarnym i dotyczące środowiska lądowego, powietrznego oraz morskiego. Jednak po rozpadzie świata bipolarnego sytuacja się zmieniła i coraz większą rolę zaczęły odgrywać zagrożenia pochodzące ze sfery pozamilitarnej. Z jednej strony związane one były z negatywnymi następstwami zmian zachodzących w różnych sferach bezpieczeństwa, w głównej mierze politycznego, ekonomicznego i społecznego. Z drugiej zaś obejmowały konsekwencje gwałtownego rozwoju cywilizacyjnego i dotykały między innymi różnych sfer bezpieczeństwa: energetycznego, ekologicznego czy też cybernetycznego. Coraz szybsze zmiany związane z rozwojem technologii współczesnego środowiska militarnego, a także jego skomplikowany wymiar, spowodowały konieczność przewartościowania i dokładnej analizy wszystkich elementów jego otoczenia. To właśnie między innymi te czynniki miały bezpośredni wpływ na pojawienie się nowego środowiska

prowadzenia działań militarnych – cyberprzestrzeni (The Economist, 2010)[1]. To z kolei stworzyło nowe spektrum zagrożeń, dla których należało przygotować nowe rozwiązania, dostosowane do działań w piątym wymiarze.

W środowisku zajmującym się zagrożeniami w cyberprzestrzeni możemy spotkać się z wieloma próbami zdefiniowania zarówno samego terminu cyberprzestrzeni, jak i dodatkowych pojęć związanych z tym środowiskiem, m.in. cyberbezpieczeństwo, cyberzagrożenia, czy też pojęcia *stricte* militarnego – wojny cybernetycznej[2]. Wszystkie te pojęcia dotyczą sfery cyber, a więc najprościej określając, wszystkiego, co ma związek z informatyką, a zwłaszcza z Internetem (SJP, 2020). Może to dotyczyć z jednej strony przestrzeni wirtualnej jako domeny, z drugiej zaś wykorzystania w niej wysoko technologicznie zaawansowanego sprzętu, niekoniecznie powiązanego z bezpieczeństwem militarnym. W NATO nie przyjęto oficjalnie definicji cyberprzestrzeni, jednak w sojuszniczych dokumentach pojawiają się mniej lub bardziej szczegółowe opisy tego medium elektronicznego[3]. Cyberprzestrzeń przedstawiono w rozległym ujęciu, wskazano, że jest ona tworzona nie tylko przez Internet, oprogramowanie i systemy informacyjne, lecz także przez ludzi wykorzystujących owe sieci i przez społeczne interakcje zachodzące wewnątrz tych sieci (Wrzosek, 2016, s. 45). Możemy więc wskazać główne cechy cyberprzestrzeni, które określają jej specyfikę i nadają odpowiedni status współczesnemu zagrożeniu. Należą do nich „globalny zasięg, wydajność, uniwersalność i w zasadzie taniość w dostępie. Te czynniki powodują, że kolejne dziedziny życia społecznego są przenoszone do świata wirtualnego" (Hoffmann, 2018, s. 12).

W literaturze przedmiotu spotykamy się z podziałem wykorzystania cyberprzestrzeni w polityce bezpieczeństwa na trzy grupy. Pierwsza z nich dotyczy cyberterroryzmu, który wiąże się z politycznie motywowanymi atakami na komputery, systemy i sieci informatyczne w celu osiągnięcia określonych korzyści. Kolejna grupa dotyczy działalności wywiadowczej, polegającej

[1] W literaturze przedmiotu można spotkać się z różnym podziałem środowiska działań militarnych. M. Wrzosek wskazuje na sześć przestrzeni operacyjnych, tj.: lądową, wodną, powietrzną, kosmiczną, spektrum elektromagnetyczne i cyberprzestrzeń (Wrzosek, 2018, s. 238).

[2] Istnieje bardzo wiele definicji związanych z tymi terminami (por.: Dereń i Rabiak, 2014; Hoffmann, 2018; Liedel i Piasecka, 2011; Wrzosek, 2018).

[3] Termin „cyberprzestrzeń" powstał w połowie lat sześćdziesiątych ubiegłego wieku i po raz pierwszy został wprowadzony w sztukach wizualnych przez Duńczyków, artystkę Susanne Ussing i architekta Carsena Hoffa. W 1984 roku termin ten został użyty pisarza Williama Gibsona w fantastyce naukowej (Lillemose, Kryger, 2015).

na próbie uzyskania niejawnych informacji z serwerów należących do osób fizycznych, instytucji rządowych oraz pozarządowych. Trzecia, nie mniej ważna grupa związana jest z wykorzystaniem cyberprzestrzeni do prowadzenia działań zbrojnych w ramach kolejnego teatru działań (Lakomy, 2011, s. 151). Dokonując próby analizy dotychczasowego oddziaływania środkami informatycznymi w celach militarnych, należy potwierdzić, iż zagrożenia te wypływały ze wszystkich wskazanych powyżej obszarów. Różniły się jedynie trzema zasadniczymi wskaźnikami: podmiotem wykonującym atak, formą i metodą oraz motywem jego przeprowadzenia.

Po raz pierwszy do poważnego cyberataku na instytucje NATO doszło w 1999 roku. Został on wykonany w odwecie za przeprowadzone przez Sojusz Północnoatlantycki ataki lotnicze na wybrane cele Federalnej Republiki Jugosławii podczas operacji „Allied Force". Dokonali tego niezidentyfikowani serbscy hakerzy komputerowi, którzy przeprowadzili ataki typu Denial Distribiuted of Service (DDoS) na główny serwer WWW siedziby NATO w Brukseli, który obsługiwał komórkę zajmującą się operacją NATO. W wyniku tego ataku hakerskiego serwer NATO został przeciążony przez otrzymywanie około dwóch tysięcy wiadomości dziennie. Adresy sprawców ataków, które zostały przeprowadzone w pierwszych dniach, pochodziły z Jugosławii, natomiast tych przeprowadzonych w dniach kolejnych, pochodziły z wielu miejsc naszego globu. W odpowiedzi na te ataki NATO podjęło działania związane z modernizacją wszystkich swoich serwerów, wymieniając je na nowsze, które posiadały większą moc obliczeniową, a więc znacznie trudniej można było je przeciążyć. Ponadto w serwerach zamontowano dodatkowe filtry, które blokowałyby złośliwe wiadomości e-mail, oraz wyłączono wszystkie dodatkowe usługi internetowe z wyjątkiem tych niezbędnych (Verton, 1999). Z tego też względu, w tym samym czasie również przeprowadzono ataki hakerskie na serwery Pentagonu. Związane to było między innymi z tym, że w operacji „Allied Force" w przeważającej części udział wzięło lotnictwo amerykańskie.

Znacznie poważniejszy w skutkach był atak cybernetyczny, przeprowadzony w 2007 roku na Estonię, który określany jest również jako pierwsza cyberwojna (Urbanek, 2016). Nie był on wymierzony jak poprzedni przeciwko kwaterze głównej NATO, lecz przeciwko jednemu z państw sojuszniczych. Ataki były następstwem wydarzeń związanych z planami estońskiego rządu, które dotyczyły przeniesienia tzw. Brązowego Żołnierza – pomnika upamiętniającego radzieckich żołnierzy – na miejscowy cmentarz w Tallinie. Tym zamiarom sprzeciwiała się zarówno

Moskwa, jak i działacze mniejszości rosyjskiej w Estonii. Na początku protesty miały charakter pokojowy i obejmowały jedynie stolicę, natomiast później, po oficjalnym włączeniu się do niego Rosji, sytuacja zamieniła się w międzynarodowy kryzys. W dniu 27 kwietnia, w czasie kiedy na ulicach estońscy Rosjanie prowadzili walkę z policją, zaatakowane zostały estońskie serwisy rządowe tzw. atakami *denial of services* (DoS). „Dziś wiadomo, że te cyberataki, prowadzone przez wielu niezależnych hakerów, rozpoczęła rosyjska organizacja »Nasi«, podporządkowana Kremlowi (ona sama twierdzi, że jest niezależna od rosyjskiego rządu[4])" (Jalonen, 2009). W pierwszej kolejności cyberataki skierowane były na państwową infrastrukturę informatyczną, unieruchamiając strony internetowe parlamentu, ministerstw obrony i sprawiedliwości, partii politycznych, policji, a nawet szkół publicznych. Od 9 maja celem ataków stał się sektor prywatny, w tym bankowy i prasowy. Dwa największe banki zmuszone zostały do zawieszenia swoich usług on-line i wstrzymania transakcji zagranicznych. Przestał też funkcjonować największy estoński dziennik „Postimees". Wydarzenia tych 22 dni zostały poważnie potraktowane zarówno przez estoński rząd, jak i przez NATO, którego Estonia jest członkiem (Joubert, 2012). Podjęto dyskusję, czy artykuł piąty Traktatu Północnoatlantyckiego dotyczy także cyberwojny i cyberterroryzmu (Jalonen, 2009). Skutki tych wydarzeń miały wpływ nie tylko na rozpoczęcie działań w zakresie cyberobrony w Tallinie i Brukseli, ale i również w państwach niebędących członkami NATO, w Szwecji i Finlandii. Wydarzenia w Estonii z 2007 roku różnie zostały zinterpretowane i zakwalifikowane ze względu na ich sprawcę. Pośród wielu instytucji zajmujących się problematyką działań cybernetycznych istnieje również i taka opinia, iż była „rosyjską operacją informacyjną przeciwko Estonii" (Ottis, 2008, s. 6). Do końca 2007 roku nastąpił wzrost rywalizacji państw i podmiotów niepaństwowych w cyberprzestrzeni. Celem następnego ataku stał się kolejny członek NATO – Stany Zjednoczone. „W 2007 r. doszło do »elektronicznego Pearl Harbor« w Stanach Zjednoczonych, kiedy w serii skoordynowanych ataków włamano się do serwerów departamentów Obrony, Stanu, Handlu i Energii, gdzie uzyskano m.in. dostęp do informacji dotyczących funkcjonowania sieci elektroenergetycznej USA" (Lakomy, 2011, s. 146).

Znaczącym wydarzeniem związanym z wykorzystaniem cyberprzestrzeni

[4] Żadna organizacja ani grupa nie przyznała się do odpowiedzialności za cyberataki na Estonię w 2007 roku, chociaż niektóre osoby zostały powiązane z ich wykonywaniem.

do działań militarnych była wojna gruzińsko-rosyjska w 2008 roku. Określana jest ona mianem „drugiej cyberwojny" i stanowi pierwszy przypadek ataku sieciowego na dużą skalę (*computer network attack* – CNA) prowadzonego w parze z głównymi operacjami sił lądowych. Choć do przeprowadzonych ataków oficjalnie nie przyznała się żadna instytucja, to sposób ich wykonania wpisywał się w rosyjskie zdolności wynikające z walki informacyjnej i psychologicznej (Shakarian, 2011, s. 63). Pomimo że nie dotyczyły one bezpośrednio Sojuszu Północnoatlantyckiego, to pośrednio dwa państwa NATO były zaangażowane w złagodzenie oddziaływania cyberataków na gruzińskie instytucje rządowe. To między innymi udostępnienie rządowi w Tibilisi własnych serwerów przez Polskę, Estonię i Ukrainę poprawiło sytuację po zmasowanych atakach zorganizowanych struktur hakerów, kontrolowanych przez rosyjskie służby specjalne – GRU i FSB (Lakomy, 2011, s. 147). Wykorzystanie cyberprzestrzeni podczas tej wojny wskazało na jeszcze jeden ważny czynnik – na to, że może być równie użyta do prowadzenia działań propagandowych. Tak waśnie było w przypadku przejęcia gruzińskich witryn rządowych. Jeszcze tego samego roku dokonano także ataku cybernetycznego na amerykański wojskowy system komputerowy na Bliskim Wschodzie. Jedna forma jego przeprowadzenia była nieco odmienna od dotychczasowych, ponieważ wykorzystano do tego pendrive. Poprzez jego użycie „oprogramowanie szpiegowskie rozprzestrzeniło się niepostrzeżenie zarówno do tajnych, jak i do jawnych systemów. W ten sposób powstał »informatyczny przyczółek« z którego ściągnięto tysiące plików danych do serwerów będących pod zagraniczną kontrolą" (Theiler, 2011). W 2009 roku doszło do dwóch poważnych serii cyberataków, ich celami były między innymi serwery należące do instytucji państwowych, polityków, korporacji oraz instytucji badawczych niektórych państw NATO. W pierwszym przypadku chińska grupa szpiegowska dokonała uderzeń na wybrane cele w Stanach Zjednoczonych, na Łotwie i w Niemczech. W drugim przypadku akcja, przeprowadzona również przez chińskich hakerów, znana jako Operacja Aurora, wymierzona została między innymi w 20 amerykańskich korporacji, w tym koncern Northrop Grumman zajmujący się produkcją nowoczesnego uzbrojenia (Urbanek, 2016, s. 19).

Po raz kolejny Sojusz Północnoatlantycki użyty został w wojnie informacyjnej w 2014 roku, podczas nielegalnej aneksji Krymu przez Federację Rosyjską. W przekazywanych publicznie przez stronę rosyjską informacjach, obawiano się „zajęcia baz Floty Czarnomorskiej przez NATO". W swojej antyukraińskiej

retoryce sympatycy Rosji odwoływali się przede wszystkim do drażliwych faktów historycznych – banderowców, nazistów, jak również do rzekomego zaangażowania NATO i Zachodu w „destabilizację Ukrainy" (Bryjka, 2015, s. 127). Znaczącym wydarzeniem w kontekście odpowiedzi na ataki cybernetyczne, które dosięgły nie tylko państwa NATO, ale także inne, spoza Sojuszu, była wypowiedź sekretarza generalnego NATO Jensa Stoltenberga w 2017 roku. Po serii ataków złośliwego oprogramowania NotPetya, które zostały przeprowadzone pod koniec czerwca na firmy i instytucje wielu państw europejskich, w tym członków NATO oraz Stanów Zjednoczonych5, powołał się on na uruchomienie artykułu traktatu waszyngtońskiego, dotyczącego obrony zbiorowej. Stwierdził, iż „w wypadku ataku cybernetycznego może zostać uruchomiony artykuł 5 Traktatu Północnoatlantyckiego, jeżeli operacja w sieci będzie »porównywalna« do działań wojskowych" (Cyber Defence 24, 2017).

Po analizie powyżej opisanych ataków cybernetycznych, które zostały wykonane bezpośrednio na instytucje NATO oraz na państwa sojusznicze, można przedstawić następujące wnioski. Pierwszy z nich dotyczy trudności w zidentyfikowaniu podmiotów, które je wykonały. W niektórych przypadkach podmioty te były powiązane z ośrodkami i instytucjami państw prowadzących wzmożoną aktywność związaną zarówno z wysoce zaawansowanym cybernetycznym szpiegostwem, jak i cybersabotażem. Drugi wniosek dotyczy form i metod ich przeprowadzenia. Rozwój technologiczny sprzętu związanego z obszarem informatycznym sprawił, iż wykonane do tej pory cyberataki różniły się od siebie. Ostatni wniosek związany jest z wyborem celów ataku, które również ewoluowały. Pierwsze ataki stworzyły zagrożenia dla bezpieczeństwa informatycznego, zarówno prywatnego, jak i instytucji czy państw sojuszniczych. W dalszej kolejności były skierowane w celu zagrożenia bezpieczeństwa krytycznych elementów ich infrastruktury. Pod tym względem, jak do tej pory, najwięcej ataków przeciwko NATO i jego państwom członkowskim przeprowadzono na Stany Zjednoczone.

Próba odpowiedzi NATO na „niewidzialne zagrożenia"

W związku z narastającymi zagrożeniami wynikającymi z użycia cyberprzestrzeni jako kolejnego środowiska walki oraz możliwością wykorzystania najnowszej

[5] Atak skierowany był głównie przeciwko Ukrainie, gdzie zostało zaatakowanych około 80 większych firm działających w tym państwie, włączając w to koncerny naftowe i firmy logistyczne.

technologii informatycznej w obszarze militarnym, jak również poza nim, Sojusz Północnoatlantycki stopniowo przystosowywał się, podejmując odpowiednie kroki w zakresie cyberbezpieczeństwa. Działalność ta w szczególności wzmogła się po szczycie NATO w Lizbonie w 2010 roku, kiedy to przyjęto nową koncepcję strategiczną, w której ujęto zapisy dotyczące cyberbezpieczeństwa. Przełom w tym zakresie przyniósł również walijski szczyt NATO w Newport we wrześniu 2014 roku, po którym oczekiwane rezultaty widać już teraz, w postaci przygotowanych do tego instytucji oraz narzędzi i instrumentów do tej skomplikowanej działalności sojuszniczej.

Należy podkreślić jednak, że pierwsze symptomy zainteresowania Sojuszu tą problematyką pojawiły się już na szczycie w Waszyngtonie w 1999 roku, kiedy to przyjęta kolejna koncepcja strategiczna zapoczątkowała proces „zmian struktury dowodzenia i sił w NATO w kontekście działań oraz planów związanych z cyberprzestrzenią" (Dereń i Rabiak, 2016, s. 1).

Kolejny raz skupiono uwagę na tej problematyce podczas szczytu w Pradze w 2002 roku. Cyberobrona, która po raz pierwszy znalazła się w programie politycznym tychże obrad, na stałe już została tematem dyskusji i w kolejnych spotkaniach najważniejszych przedstawicieli państw członkowskich NATO zaczęła odgrywać coraz ważniejszą rolę. Właśnie w 2002 roku, obok ważnych deklaracji związanych z przedsięwzięciami dotyczącymi wzmocnienia jego zdolności obronnych, w dokumencie końcowym szczytu – Deklaracji Szczytu Praskiego (*Prague Summit Declaration*), który został przyjęty 21 listopada 2002 roku, pojawił się również krótki zapis dotyczący wzmocnienia możliwości obrony Sojuszu przed cyberatakami (NATO, 2002). Ten ważny apel o udoskonalanie „zdolności do obrony przed atakami cybernetycznymi" nie do końca został doceniony przez wszystkich członków NATO, którzy przede wszystkim byli skoncentrowani na wdrażaniu pasywnych środków obrony, o które apelowali wojskowi (Theiler, 2011). Cztery lata później, na szczycie w Rydze, kolejny raz wskazano na potrzebę dodatkowej ochrony sojuszniczych systemów dowodzenia. Cyberataki z 2007 roku, które skierowane zostały przeciwko jednemu z państw NATO oraz rok później przeprowadzone na amerykańską infrastrukturę wojskową, a także te, zastosowane podczas konfliktu Gruzji z Rosją, jedynie potwierdziły potrzebę rozpoczęcia pilnych prac związanych z przeciwstawieniem się kolejnym tego typu zagrożeniom poprzez przygotowanie odpowiednich dokumentów, procedur oraz narzędzi. W tym kontekście już na szczycie Sojuszu Północnoatlantyckiego

zorganizowanym w Bukareszcie w 2008 roku przyjęto pierwszą politykę NATO w dziedzinie cyberobrony, zatwierdzając dokument *NATO Cyber Defence Policy, który* zapewniał państwom Sojuszu zdolność do wsparcia przeciwdziałania cyberatakom. Co istotne, deklaracja końcowa tego spotkania najważniejszych przedstawicieli Sojuszu Północnoatlantyckiego zawierała treści związane z kierunkiem polityki NATO w tym zakresie. Znalazły się tam zapisy dotyczące dalszego wzmocnienia kluczowych systemów dowodzenia Sojuszu przeciwko cyberatakom, a także propozycje umacniania powiązań w zakresie ich ochrony między NATO a państwami członkowskim (NATO, 2008). Również w 2008 roku w strukturach sojuszniczych powołano do działania placówkę badawczą prowadzącą interdyscyplinarne badania nad cyberbezpieczeństwem – Centrum Doskonalenia Obrony przed Cyberatakami NATO *(NATO Cooperative Cyber Defence Centre of Excellence* – NATO CCD COE). To centrum eksperckie, mające swoją siedzibę w Tallinnie, jest znaczącym wsparciem państw członkowskich w obszarze cyberobrony z uwzględnieniem różnych obszarów i poziomów jego funkcjonowania, w tym politycznego, prawnego oraz technicznego.

W treści obowiązującej koncepcji strategicznej z Lizbony także zwrócono uwagę na bezpieczeństwo cybernetyczne. „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" (Biuro Bezpieczeństwa Narodowego, 2011, s. 206). Ważnym ustaleniem tego szczytu było również to, że Rada Północnoatlantycka otrzymała zadanie opracowania dogłębnej polityki cyberobrony NATO oraz planu jej wdrożenia. Rok po lizbońskim szczycie NATO, w czerwcu 2011 roku ministrowie obrony NATO przyjęli kierunki działania, określając wizję skoordynowanych wysiłków w zakresie cyberobrony w całym Sojuszu. Podkreślili również potrzebę takich działań ze względu na szybko zmieniające się zagrożenia oraz rozwój technologiczny. Te działania określono jako druga polityka NATO w zakresie cyberobrony (NATO, 2020). To między innymi te działania były powodem dalszych kroków ze strony NATO, ponieważ rok później cyberobronę wprowadzono do sojuszniczego procesu planowania

obrony oraz uruchomiono dwa sześcioosobowe zespoły szybkiego reagowania (*Rapid Reaction Team* – RRT), które miały być rozmieszczane za zgodą Rady Północnoatlantyckiej w celu wsparcia krajów będących obiektem poważnych ataków (Kasprzyk, 2015).

Wobec kolejnych narastających zagrożeń w cyberprzestrzeni NATO przyjęło na szczycie w Newport w 2014 roku przełomową deklarację, która określała między innymi, że cyberataki mogą prowadzić do powołania się na artykuł 5. Traktatu Północnoatlantyckiego, mówiący o obronie zbiorowej. W tym samym roku w Sojuszu podjęto również dwie ważne inicjatywy zmierzające do podniesienia zdolności w ramach cyberobrony. Pierwszą z nich było osiągnięcie pełnej zdolności operacyjnej przez Zespół Reagowania na Incydenty Komputerowe (*NATO Computer Incident Response Capability* – NCIRC). Stał się on głównym ośrodkiem walki Sojuszu z cyberprzestępczością, który zajmuje się incydentami i dostarcza NATO oraz sojusznikom aktualne informacje dotyczące wyzwań w zakresie bezpieczeństwa cybernetycznego. Ten dwustuosobowy zespół ekspertów odpowiada za cyberobronę wszystkich obiektów NATO, niezależnie od tego, czy jest to Kwatera Główna, czy sojusznicze stanowiska rozmieszczone na potrzeby operacji lub ćwiczeń (Babraj, 2918a; NATO, 2017). Aktywność sojuszniczych instytucji powołanych w ramach ochrony przed cyberzagrożeniami nabierała impetu. Już w listopadzie 2014 roku NATO przeprowadziło w Tartu, na wschodzie Estonii największe, jak na tamten okres, ćwiczenia dotyczące cyberbezpieczeństwa. W przedsięwzięciu tym, które odbyło się zaledwie 50 km od granicy z Rosją, wzięło udział ponad 670 żołnierzy i cywilów z 80 organizacji oraz instytucji pochodzących z 28 państw (Sadowski, 2017, s. 64).

Kolejnym zamierzeniem było uruchomienie pierwszej inicjatywy, mającej na celu nawiązanie współpracy z sektorem prywatnym (*NATO Industry Cyber Partnership*). To wydarzenie stworzyło wszystkim uczestnikom tejże inicjatywy możliwość szybkiej wymiany informacji na temat cyberzagrożeń, co przyczynia się do zwiększenia ich świadomości sytuacyjnej. Jej realizacja jest ważna nie tylko pod kątem opracowania nowych zdolności cyberobronnych dla NATO, ale też ze względu na to, że to firmy prywatne są operatorami znacznej części infrastruktury krytycznej (Kasprzyk, 2015). Do 2019 roku do tej inicjatywy przystąpiły 23 firmy.

Następny szczyt NATO, który odbył się w 2016 roku w Warszawie, przyniósł kolejne plany w zakresie zwiększania zdolności do obrony przed cyberzagrożeniami

(Biuro Bezpieczeństwa Narodowego, 2016). „Członkowie Sojuszu uznali przestrzeń cybernetyczną za obszar działań zbrojnych i w większym stopniu zobowiązali się do wzmacniania cyberobrony, w odniesieniu do swoich krajowych sieci i infrastruktury oraz traktowania jej jako priorytet. NATO i jego państwa członkowskie podjęły znaczące kroki strategiczne, operacyjne i techniczne, aby przeciwdziałać złośliwym działaniom cybernetycznym" (Berent, 2019). Podczas spotkania warszawskiego przyjęto także deklarację cyberbezpieczeństwa (*Cyber Defence Pledge*). Dokument ten zawierał między innymi postanowienia dotyczące konieczności wzmocnienia cyberbezpieczeństwa sieci państw sojuszniczych oraz ich infrastruktury, a także potrzebę przeciwstawiania rozwijającym się cyberzagrożeniom, tak aby państwa NATO były w stanie skutecznie bronić się w cyberprzestrzeni. Nawiązywał on między innymi do artykułu 3. Traktatu Waszyngtońskiego, który stwierdza, że „Strony […] będą utrzymywały i rozwijały swoją indywidualną i zbiorową zdolność do odparcia zbrojnej napaści" (Dz. U. 2000, nr 87, poz. 970). W deklaracji Sojusznicy potwierdzili stosowanie prawa międzynarodowego w cyberprzestrzeni oraz współpracę z Unią Europejską. Ważną częścią dokumentu była ta, dotycząca międzynarodowej współpracy poprzez edukację, szkolenia, a także wymianę informacji. Efekty wynikające z wdrożenia tej deklaracji przedstawiono na szczycie w Brukseli, jak również na pierwszej konferencji podsumowującej ten projekt w Paryżu w 2018 roku (Babraj, 2018b). „Sekretarz generalny NATO Jens Stoltenberg przyznał, że w ciągu niespełna dwóch lat od przyjęcia zobowiązania, niemal każdy sojusznik poprawił swoje zdolności cyberobronne. Liderem zmian w Europie jest Wielka Brytania, która zainwestowała 1,9 mld funtów za pośrednictwem narodowej strategii cyberbezpieczeństwa. Druga w kolejności Francja zainwestowała 1,6 mld euro" (*NATO, 2016*).

W 2018 roku przedstawiciele NATO podjęli kolejne inicjatywy związane z podniesieniem zdolności cyberobronnych. W czerwcu 2018 roku Rada Północnoatlantycka zatwierdziła Wizję i strategię Komitetu Wojskowego w sprawie cyberprzestrzeni jako domeny działań (*Vision and Strategy on Cyberspace as a Domain of Operations)*. Ten znaczący dokument określa kluczowe zagadnienia związane polityką, rozwojem zdolności, a także planowaniem operacyjnym i wykonywaniem zadań w zakresie działań NATO w cyberprzestrzeni (McKenzie, 2019). W tym samym roku, podczas szczytu brukselskiego jego uczestnicy wskazali

za wzrost aktywności w obszarze cyberzagrożeń[6], podkreślając między innymi fakt, iż stają się coraz częstsze, bardziej zagrażające bezpieczeństwu Sojuszu (Brent, 2019). Na szczycie w Brukseli w 2018 r. Sojusznicy podjęli jeszcze jedną bardzo ważną decyzję, dotyczącą utworzenia nowej komórki na poziomie operacyjnym w ramach wzmocnionej struktury dowodzenia NATO – Centrum Operacji Cyberprzestrzeni (*Cyberspace Operations Centre* – CyOC). Już w październiku ogłosiło ono wstępną gotowość do działania (NATO, 2020b). Głównym zadaniem tego komponentu jest zapewnienie świadomości sytuacyjnej w zakresie cyberprzestrzeni oraz koordynacji zagadnień operacyjnych dotyczących tej domeny, a także planowanie operacji NATO. Sygnatariusze zgodzili się również, że NATO może wykorzystywać krajowe zdolności cybernetyczne do swoich misji i operacji.

Jak wynika z dotychczasowej działalności, wdrażanie polityki Sojuszu Północnoatlantyckiego w zakresie cyberobrony odbywa się na wszystkich poziomach tej organizacji. Oczywiście na poziomie strategicznym nadzór nad tą działalnością sprawuje Rada Północnoatlantycka, pełniąc główną funkcję w zarządzaniu kryzysowym związanym z cyberobroną. Inne, usytuowane na niższych poziomach komórki i instytucje podporządkowane są także działalności Rady Północnoatlantyckiej. Należą do nich Komitet Cyberobrony NATO (*NATO Cyber Defence Committee – NCDC) oraz* Rada NATO ds. Zarządzania Cyberobroną (*NATO Cyber Defence Management Board* – NCDMB). Pierwsza z wymienionych instytucji odgrywa główną rolę w realizacji sojuszniczej polityki cyberobrony, zapewniając również doradztwo państwom sprzymierzonym na poziomie eksperckim. Druga odpowiada natomiast za koordynację zamierzeń związanych z cyberobroną w cywilnych i wojskowych organach NATO na poziomie roboczym. Mówiąc o organach współpracujących ze sobą w ramach współdziałania sojuszniczego, należy wskazać jeszcze Komitet Konsultacyjny, Kontroli i Dowodzenia (*Consultation, Control and Command Board* – C3B), który jest odpowiedzialny za konsultacje problemów technicznych i wdrożeniowych w zakresie cyberobrony.

Szczególną rolę w działalności sojuszniczej związanej z obroną przez cyberzagrożeniami odgrywają szkolenia i ćwiczenia. Szkolenia prowadzone są

[6] W okresie przygotowawczym do szczytu NATO w Brukseli odnotowanych zostało około 500 tys. incydentów z routerami w 54 krajach, w tym w państwach NATO.

w celu poprawy świadomości sytuacyjnej sojuszników, a także innych podmiotów w nich uczestniczących, dotyczącej zagrożeń pochodzących z cyberprzestrzeni. Głównym celem ćwiczeń jest wzmocnienie koordynacji i współpracy między sojusznikami oraz poprawa zdolności cyberofensywnych NATO. Przykładem takiej działalności jest coroczne ćwiczenie NATO w dziedzinie cyberprzestrzeni – *Exercise Cyber Coalition*[7].

NATO prowadzi działania przeciw cyberzagrożeniom poprzez zarówno powołane do tego instytucje sojusznicze, jak i współpracę w ramach państw członkowskich. Poszukuje również innych form kooperacji z krajami spoza NATO. Dotyczy to inicjatyw skierowanych do krajów europejskich, takich jak Szwecja czy Finlandia, ale także do państw pozaeuropejskich, np. Japonii. Ten kierunek współpracy został zgłoszony w 2018 roku w czasie wizyty premiera Japonii Shinzo Abe w Centrum Doskonalenia Obrony przed Cyberatakami NATO w Tallinnie (Estonian Word, 2018).

W opublikowanym w 2020 roku raporcie sekretarza generalnego NATO Jensa Stoltenberga podkreślono, iż cyberbezpieczeństwo stanowi część głównego zadania NATO, jakim jest obrona zbiorowa sojuszników (NATO, 2020a). W dokumencie bardzo dużo miejsca poświęcono tej problematyce. Sekretarz generalny między innymi wskazał zasadnicze przedsięwzięcia, które przyczyniły się do podniesienia zdolności Sojuszu w zakresie cyberbezpieczeństwa. Zaliczył do nich na przykład utworzenie Centrum Operacji Cyberprzestrzeni, przyjęcie wspólnych ustaleń dotyczących rozwijania nowych technologii celem uporządkowania prac w zasadniczych obszarach prowadzonych przez Sojusz oraz zaktualizowanie wymagań NATO związanych z przygotowaniem sojuszniczych systemów komunikacji cywilnej w zakresie ich odporności na cyberzagrożenia. Wskazano w nim także, iż potencjalnym celem cyberataków może być infrastruktura energetyczna. W dokumencie tym zwrócono również uwagę na działania związane z cyberbezpieczeństwem w ramach programów realizowanych w NATO8, a także znaczenie prowadzonych szkoleń i konferencji. Ważnym elementem aktywności

[7] W tegorocznych ćwiczeniach *Cyber Coalition 2020*, które odbyły się w Estonii w dniach 18–22 listopada, wzięły udział 24 państwa NATO, a także przedstawiciele 4 krajów partnerskich (Finlandii, Irlandii, Szwecji i Szwajcarii) i 4 krajów obserwujących. Głównym celem ćwiczeń była współpraca sojusznicza i zdolność przystosowania się do zmieniającego środowiska bezpieczeństwa, w tym usprawnienie koordynacji, współpracy i wymiany informacji w całej wirtualnej domenie NATO.

[8] Dotyczy to programu *NATO Science for Peace and Security*, według którego w 2019 roku sfinansowano m.in. 49 projektów współpracy w 22 krajach partnerskich. 18% podjętych projektów dotyczyło cyberbezpieczeństwa,

Sojuszu było przeprowadzenie przez Zespół ds. polityki cyberprzestrzeni badania stanu wsparcia wywiadu dla operacji w cyberprzestrzeni. Ich efektem było dokonanie szczegółowej analizy niedociągnięć w tym obszarze, a także wskazania i zalecenia dotyczące ich usunięcia i poprawy działania (Babraj, 2020).

Podsumowanie

Na podstawie analizy środowiska bezpieczeństwa pod względem jego zagrożeń, należy stwierdzić, iż w pierwszych dwóch dekadach XXI wieku cyberprzestrzeń nabrała szczególnego znaczenia. Szybki rozwój środków teleinformatycznych w zakresie ich technologicznego zaawansowania oraz łatwa i powszechna możliwość dostępu do zasobów globalnej sieci nie tylko stworzyły znaczne możliwości udoskonalenia życia codziennego, ale wygenerowały również nowe spektrum zagrożeń.

Proces ten nie ominął również sfery militarnej. Środowisko bezpieczeństwa NATO zostało poszerzone o zagrożenia generowane za pośrednictwem technologii teleinformatycznej przy wykorzystaniu cyberprzestrzeni. Dlatego też zarówno sam Sojusz, jak i jego państwa członkowskie podjęły w ostatnim dziesięcioleciu istotne decyzje w dziedzinie cyberobrony. Początkowo Sojusz Północnoatlantycki traktował te formy zagrożenia pobocznie, bez zbytniego ich docenienia ze względu na ich incydentalność, koncentrując się w tym czasie na innych zagrożeniach. Cyberataki skierowane przeciw NATO postrzegane były jako zagrożenia o ograniczonym zakresie i niewielkim niszczącym potencjale.

Zasadnicza zmiana stanowiska w tym obszarze nastąpiła po 2007 roku, kiedy to cyberzagrożenia z dotychczasowego wyzwania dla bezpieczeństwa informatycznego przekształciły się w zagrożenia dla bezpieczeństwa podmiotów infrastruktury krytycznej zarówno Sojuszu, jak i jego państw członkowskich. Ta zmiana myślenia oraz dalsze wydarzenia związane z rozwojem zagrożeń cybernetycznych były podstawą do określenia w obowiązującej koncepcji strategicznej oraz innych dokumentach dalszych działań w zakresie rozwijania zdolności sojuszniczych w tym obszarze.

Jak widać, kierunki dotychczasowych przedsięwzięć sojuszniczych realizowanych w ramach ochrony i obrony przed zagrożeniami cybernetycznymi są całkowicie zbieżne z trzema zadaniami, które ujęte zostały w obowiązującej

a 20% zaawansowanych technologii (Babraj, 2020).

koncepcji strategicznej. Dotyczą one rozwijania zdolności w zakresie obrony zbiorowej, zarządzania kryzysowego oraz bezpieczeństwa kooperatywnego. Realizacja obecnej polityki NATO w tym zakresie, jak również przyjęte plany wskazują, że kierunek ten nadal będzie rozwijany.

Jak wskazują przedsięwzięcia podjęte przez Sojusz Północnoatlantycki w zakresie przeciwdziałania i zwalczania cyberzagrożeń w okresie ostatnich pięciu lat, to oprócz zasadniczych zadań realizowanych przez wyspecjalizowane instytucje Sojuszu, równie ważne są te, związane z rozwojem narodowych zdolności państw sojuszniczych w dziedzinie cyberbezpieczeństwa. Bardzo ważnym obszarem w zakresie rozwijania zdolności NATO wobec zagrożeń cybernetycznych jest także rozpoczęcie współpracy z innymi podmiotami międzynarodowymi oraz państwami spoza Sojuszu.

Zbudowany przez NATO potencjał do wspólnego przeciwstawienia się zagrożeniom nie tylko chroni sieci informatyczne instytucji sojuszniczych, ale i wspiera członków Sojuszu Północnoatlantyckiego w budowie narodowych zdolności cyberobrony. Co więcej, w NATO rozpoczęto również dyskusję na temat możliwości i mechanizmów użycia sił cyberofensywnych przez poszczególne kraje w ramach obrony zbiorowej. W kontekście tych działań Sojusz Północnoatlantycki nie poprzestaje na możliwościach i inicjatywach wewnętrznych. Aktywność NATO w ramach walki z cyberzagrożeniami wykracza bowiem poza państwa członkowskie i nie dotyczy już tylko państw europejskich, lecz sięga daleko poza kontynent.

Bibliografia

Arquilla, J. i Ronfeldt, D. (1997). *Cyberwar is Coming!* W: Arquilla, J. i Ronfeldt, D. (red.), *In Athena's Camp: Preparing for Conflict in the Information Age* (p. 23–59). Santa Monica: RAND Corporation. Dostęp: https://www.rand.org/pubs/reprints/RP223.html [28.11.2020].

Babraj, R. (2018a, 1 maja). Sojusz Północnoatlantycki – ewolucja w podejściu do cyberobrony. *www.cyberpolicy.nask.pl.* Dostęp: https://cyberpolicy.nask.pl/nato-cyberobrona-zagrozenia-hybrydowe/ [5.11.2020].

Babraj, R. (2018b, *25 maja*). *Cyber Defence Pledge. www.cyberpolicy.nask.pl.* Dostęp: https://cyberpolicy.nask.pl/cyber-defence-pledge%ef%bb%bf/ [4.11.2020].

Babraj, R. (2020, *24 marca*). Raport NATO za 2019 rok. *www.cyberpolicy.nask.pl.* Dostęp: https://cyberpolicy.nask.pl/aktualnosci/raport-nato-za-2019r/ [28.11.2020].

Biuro Bezpieczeństwa Narodowego (2011, 17 stycznia). *Koncepcja Strategiczna NATO z 2010 r.* Dostęp: https://www.bbn.gov.pl/pl/wydarzenia/2694,KoncepcjaStrategicznaNATOtlumaczenie.html [28.11.2020].

Biuro Bezpieczeństwa Narodowego (2016). Deklaracja końcowa szczytu NATO w Warszawie. *Bezpieczeństwo Narodowe,* (37–40), 205–242. Dostęp: https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_

szczytu.pdf [4.11.2020].

Brent, L. (2019, 12 luty). Rola NATO w cyberprzestrzeni. *www.nato.int.* Dostęp: https://www.nato.int/docu/review/pl/articles/2019/02/12/rola-nato-w cyberprzestrzeni/index.html [4.11.2020].

Bryjka, F., (2015). *Cyberprzestrzeń w strategii wojny hybrydowej Federacji Rosyjskiej*. W: T. Grabińska, Z. Kuźniar (red.), *Bezpieczeństwo personalne a bezpieczeństwo strukturalne* (t. 6, s. 115–131). Wrocław: Wydawnictwo WSOWL. Dostęp: https://www.researchgate.net/publication/313338435_Cyberprzestrzen_w_strategii_wojny_hybrydowej_Federacji_Rosyjskiej [3.11.2020].

Cyber Defence 24. (2017, 12 lipca). *Eksperci NATO: Państwo sprawcą ataku NotPetya. Ukraina wśród ofiar*. Dostęp: https://www.cyberdefence24.pl/eksperci-nato-panstwo-sprawca-ataku-notpetya-ukraina-wsrod-ofiar [4.11.2020].

Dereń, J. i Rabiak, A. (2014). *NATO a aspekty bezpieczeństwa w cyberprzestrzeni*. W: M. Górka (red.), *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku* (s. 202–221). Warszawa: Difin. Dostęp: https://www.researchgate.net/publication/272818724_NATO_a_aspekty_bezpieczenstwa_w_cyberprzestrzeni [4.11.2020].

Estonian World (2018, January 13). *Japan to join the NATO Cyber Defence Centre of Excellence in Tallinn*. Dostęp: https://estonianworld.com/security/japan-join-nato-cyber-defence-centre-excellence-tallinn/ [6.11.2020].

Górka, M. (2018). *Cyberbezpieczeństwo jako wyzwanie dla współczesnego państwa i społeczeństwa*. W: T. Dębowski (red.), *Cyberbezpieczeństwo wyzwaniem XXI wieku* (s. 31–50). Łódź-Warszawa: ARCHAEGRAPH. Dostęp: https://depot.ceon.pl/handle/123456789/14956 [4.11.2020].

Hoffmann, T. (2018). *Główni aktorzy cyberprzestrzeni i ich działalność*, W: T. Dębowski (red.), *Cyberbezpieczeństwo wyzwaniem XXI wieku.* (s. 11–22). Łódź–Wrocław: Wydawnictwo Naukowe ARCHAEGRAPH. Dostęp: https://depot.ceon.pl/handle/123456789/14956 [4.11.2020].

Jalonen, J. (2009, 12 maja). Dni które wstrząsnęły Estonią. *www.eesti.pl.* Dostęp: https://www.eesti.pl/dni-ktore-wstrzasnely-estonia-11963.html [6.11.2020].

Joubert, V. (2012). *Five Years After Estonia's Cyber Attacks: Lessons Learned for NATO?* (Research Paper No 76). Rome: NATO Defense College. Dostęp: https://www.files.ethz.ch/isn/143191/rp_76.pdf [4.11.2020].

Kasprzyk, A. (2015, 29 lipca). PISM o polityce NATO w cyberprzestrzeni. *www.polska-zbrojna.pl.* Dostęp: http://k.polska-zbrojna.pl/home/articleshow/16710?t=PISM-o-polityce-NATO-w-cyberprzestrzeni# [6.11.2020].

Lakomy, M. (2011). Cyberwojna jako rzeczywistość XXI wieku. *Stosunki Międzynarodowe – International Relations*, *44*(3–4), 141–161. Dostęp: https://www.researchgate.net/publication/322274797_Cyberwojna_jako_rzeczywistosc_XXI_wieku [5.11.2020].

Liedel, K. i Piasecka, P. (2011). Wojna cybernetyczna – zagrożenie XXI wieku. *Bezpieczeństwo Narodowe*, 17/I, 15–28. Dostęp: https://www.bbn.gov.pl/download/1/7008/1wojnacybernetyczna.pdf [6.11.2020].

Lillemose, J. i Kryger, M. (2015, August 24). The (Re)invention of Cyberspace. *Kunstkritikk Nordic ArtReview*. Dostęp: https://kunstkritikk.com/the-reinvention-of-cyberspace/ [26.11.2020].

McKenzie, P.J. (2019). NATO's Vision and Strategy on the Cyberspace Domain. *JAPCC Journal 28*. Dostęp: https://www.japcc.org/cyberspace-notam/ [16.11.2020].

Michalewski, E. (2010). Analiza systemów sieciocentrycznych. *Studies & Proceedings of Polish Association for Knowledge Management***,** 32, 143-154. Dostęp: http://www.pszw.edu.pl/images/publikacje/t032_pszw_2010_michalewski_analiza_systemow_sieciocentrycznych.pdf [3.11.2020].

North Atlantic Treaty Organization [NATO]. (2002, November 21). *Prague Summit Declaration*. Dostęp: https://www.nato.int/cps/en/natohq/official_texts_19552.htm [7.11.2020].

North Atlantic Treaty Organization [NATO]. (2008, April 3). *Bucharest Summit Declaration*. Dostęp: https://

www.nato.int/cps/en/natolive/official_texts_8443.htm [4.11.2020].
North Atlantic Treaty Organization [NATO]. (2016, July 8). *Cyber Defence Pladge,* Dostęp: https://www.nato.int/cps/en/natohq/official_texts_133177.htm [4.11.2020].
North Atlantic Treaty Organization [NATO]. (2017, May) *NATO Cyber Defence*. Dostęp: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_05/20170515_1705-factsheet-cyber-defence-en.pdf [6.11.2020].
North Atlantic Treaty Organization [NATO] (2020a). *The Secretary General's Annual Report.* Brussels: NATO Public Diplomacy Division. Dostęp: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf [6.11.2020].
North Atlantic Treaty Organization [NATO]. (2020b, September 25). *Cyber defence*. Dostęp: https://www.nato.int/cps/en/natohq/topics_78170.htm [5.11.2020].
Osula, A.M. i Rõigas, H. (Eds.). (2016). *International Cyber Norms Legal, Policy & Industry Perspectives*. Tallinn: The NATO Cooperative Cyber Defence Centre of Excellence. Dostęp: https://ccdcoe.org/library/publications/international-cyber-norms-legal-policy-industry-perspectives/ [4.11.2020].
Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Tallinn: The NATO Cooperative Cyber Defence Centre of Excellence. Dostęp: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf [6.11.2020].
Robinson, N. (2016, 8 czerwca). NATO: zmiana biegów w cyberobronie. *NATO Review.* Dostęp: https://www.nato.int/docu/review/pl/articles/2016/06/08/nato-zmiana-biegow-w-cyberobronie/index.html [28.11.2020]
Sadowski, J. (2017). Cybernetyczny wymiar współczesnych zagrożeń. *Studia nad bezpieczeństwem*, 2, 57–76. Dostęp: https://zeszyty-bn.apsl.edu.pl/index.php/snb/article/view/45/110 [3.11.2020].
Shakarian, P. (2011). The 2008 Russian Cyber-Campaign Against Georgia. *Military Review*, Nov–Dec, 63–68. Dostęp: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20111231_art013.pdf [6.11.2020].
Słownik języka polskiego. (2020). Dostęp: https://sjp.pwn.pl/sjp/cyber;2553911%5b [6.11.2020]
The Economist. (2010, July 1). *Cyberwar. The threat from the internet*. Dostęp: https://www.economist.com/leaders/2010/07/01/cyberwar [4.11.2020].
Theiler, O. (2011, 4 września), Nowe zagrożenia: wymiar cybernetyczny. *NATO Review.* Dostęp: https://www.nato.int/docu/review/pl/articles/2011/09/04/nowe-zagrozenia-wymiar-cybernetyczny/index.html [7.11.2020].
Traktat Północnoatlantycki sporządzony w Waszyngtonie dnia 4 kwietnia 1949 r., (Dz. U. 2000, nr 87, poz. 970).
Urbanek, A. (2016). Cyberwojna – zagrożenie asymetryczne współczesnej przestrzeni bezpieczeństwa. *Studia nad bezpieczeństwem*, (1), 5–32. Dostęp: https://zeszyty-bn.apsl.edu.pl/index.php/snb/article/view/5/ [3.11.2020].
Verton, D. (1999, April 4). Serbs launch cyberattack on NATO. *Federal Computer Week*. Dostęp: https://fcw.com/articles/1999/04/04/serbs-launch-cyberattack-on-nato.aspx [6.11.2020].
Wrzosek, M. (2016). Operacje w cyberprzestrzeni. Założenia teoretyczne i praktyka. *Kwartalnik Bellona*, *687*(4), 42–59. Dostęp: https://kwartalnikbellona.com/resources/html/article/details?id=157751 [3.11.2020].
Wrzosek, M. (2018). *Wojny przyszłości. Doktryna. Technika. Operacje militarne*. Warszawa: Wydawnictwo Fronda.