Історико-політичні проблеми сучасного світу: Збірник наукових статей. – Чернівці: Чернівецький національний університет, 2019. – Т. 39. – С. 12-20
DOI: 10.31861/mhpi2019.39.12-20

Modern Historical and Political Issues: Journal in Historical & Political Sciences. – Chernivtsi: Chernivtsi National University, 2019. – Volume. 39. – pp. 12-20
DOI: 10.31861/mhpi2019.39.12-20

UDC: 327.88:341.241.2(1-HATO)

© Sylwia Leszczuk[1]

Cyberkonflikt w świetle artykułu 5 Traktatu Północnoatlantyckiego

Gwałtowny rozwój technologii – a co za tym idzie – również sfery cybernetycznej oraz powiązane z nią trudności w jej zdefiniowaniu, jak i zachodzące w niej zjawiska oraz brak nadążających unormowań prawnych i zbyt mała świadomość podmiotów publicznych i prywatnych życia społecznego co do niebezpieczeństw, jakie może generować, sprawiają, iż zaczyna ona służyć jako podstawa dla rozwoju zaawansowanych, trudnych do zneutralizowania zagrożeń, które są w stanie wpłynąć na świat realny. Istotnymi z punktu widzenia tekstu są przede wszystkim cyberataki oraz cyberwojna. W związku z wpływem, jaki świat wirtualny może wywrzeć na realia, organizacje takie jak NATO muszą w końcu ustosunkować się do zmian zachodzących na świecie. Tekst ma za zadanie przybliżyć ewentualność powołania się państwa członkowskiego Paktu Północnoatlantyckiego na słynny artykuł 5 Traktatu Północnoatlantyckiego.

Słowa kluczowe: cyberprzestrzeń, cyberwojna, cyberatak, cyberkonflikt, NATO, artykuł 5 Traktatu Północnoatlantyckiego.

Cyber conflict in the light of article 5 of the North Atlantic treaty

The rapid development of technology and hence also the cybernetic sphere, including the associated difficulties in defining it, as well as the occurrences within it and the lack of upholding legal regulations and too little awareness in public and private life as to the dangers it may generate, make it serve as a basis for the development of advanced and difficult to neutralize threats that are able to affect the real world. The most important in the context of the text are cyber attacks and cyberwar. Due to the impact that the virtual world can have on reality, organizations such as NATO must finally adapt to changes taking place in the real world. The aim of the text is to take a look at an possibility of invoking the famous article 5 of the North Atlantic Treaty by a member state of NATO.

Key words: cyberspace, cyberwar, cyber attack, cyberconflict, NATO, article 5 of the North Atlantic Treaty.

Wprowadzenie

Historia ludzkości od zarania dziejów budowana jest w oparciu o konflikt – zarówno w ujęciu metafizycznym, jak i materialnym. Wojna, pojawiająca się we wszystkich epokach historycznych, obecna we wszystkich cywilizacjach, wydaje się być nieodzownym elementem życia społecznego[2]. W rozumieniu Carla von Clausewitza jest ona *kontynuacją polityki innymi środkami* oraz *aktem przemocy, mającym na celu zmuszenie przeciwnika do spełnienia naszej woli*[3]. Do połowy XX wieku nie budziła w zasadzie wątpliwości znaczeniowych, jednakże wydarzenia mające miejsce na świecie po zakończeniu II wojny światowej rozpoczęły swoistą ewolucję w aspekcie jej pojmowania. Miano wojny zaczęto bowiem nadawać zjawiskom wymykającym się z ram «tradycyjnego» jej rozumowania, czyli odnoszącego się do bezpośrednich działań zbrojnych między zwaśnionymi stronami, przenosząc je na konflikty niekonwencjonalne, niekoniecznie powiązane ze starciami zbrojnymi. W efekcie utarły się pojęcia takie jak zimna wojna, wojna gospodarcza, wojna polityczna, czy wojna ideologiczna[4].

[1] Wydział Prawa, Uniwersytet w Białymstoku, Rzeczpospolita Polska. E-mail: sknpe@o2.pl.

[2] R. Wróblewski, *O definiowaniu wojny,* [w:] M. Kubiak, R. Wróblewski (red.), *Oblicza współczesnych wojen,* Warszawa 2018, str. 15.

[3] E. Sadowska, *Zagrożenia asymetryczne – definicja, świadomość społeczna i rola we współczesnym świecie,* Rocznik Bezpieczeństwa Międzynarodowego 2017, vol. 11, nr 2, str. 19.

[4] R. Wróblewski, *O definiowaniu wojny,* [w:] M. Kubiak, R. Wróblewski (red.), *Oblicza współczesnych wojen,* Warszawa 2018, str. 16.

Swoista rewolucja technologiczna i informacyjna zapoczątkowana w XX wieku, wydająca się wręcz przybierać tempa w pierwszych dwóch dekadach XXI wieku, nieodwracalnie wpłynęła na zmianę realiów, w jakich przyszło żyć współczesnym. W oczach obywateli świata Zachodu konwencjonalne konflikty zbrojne to odległa perspektywa, tocząca się «gdzieś indziej na świecie», pozornie nie mająca bezpośredniego wpływu na ich codzienne życie. Jednakże rozwój Internetu i nierozerwalnie związanej z nim cyberprzestrzeni wygenerował nowe rodzaje zagrożeń, wpisujące się w kategorię tzw. zagrożeń asymetrycznych[5] – pojęcia obejmującego zjawiska uprzednio nieznane bądź znacznie zmodyfikowane przez współczesne realia.

Cyberprzestrzeń jest niezwykle trudna do zdefiniowania jako «byt» w dużej mierze nienamacalny, funkcjonujący w rzeczywistości wirtualnej. Nie posiada ona jednej utartej definicji legalnej. Można ją określić jako ogół powiązań o charakterze wirtualnym, niematerialnym, powstałych i istniejących dzięki ich fizycznym manifestacjom, takim jak chociażby komputery czy infrastruktura telekomunikacyjna[6]. Jest ona nową sferą ludzkiej działalności, pewną kategorią zbiorczą, domeną funkcjonując w oparciu o zdefiniowane struktury informatyczne. Składa się ze wszystkich sieci komputerowych na świecie oraz wszystkiego, co te łączą i kontrolują[7]. Cyberprzestrzeń jest nierozerwalnie związana z siecią Internet, jednakże nie można ich ze sobą utożsamiać, gdyż cyberprzestrzeń sama w sobie jest pojęciem o wiele szerszym niż funkcjonująca w jej wymiarze «sieć sieci»[8].

W związku z faktem, iż rozwój technologiczny przebiega w ścisłym związku z rozwojem wojskowości, a błędem nie byłoby stwierdzenie, iż to militaria są siłą napędową znacznej większości innowacji w sferze technologii, informatyzacji i modernizacji, naturalnym jest zainteresowanie rozwijającą się bezustannie przestrzenią «cyber», jakie przejawia w tej kwestii Sojusz Północnoatlantycki – najpotężniejsza w dziejach świata organizacja militarna[9].

Celem tekstu jest podjęcie rozważań na temat ewentualnego uruchomienia przez Sojusz Północnoatlantycki artykułu 5 traktatu waszyngtońskiego w przypadku zaatakowania państwa zrzeszonego w strukturach organizacji poprzez użycie możliwości, jakie daje cyberprzestrzeń.

ZAGROŻENIA PŁYNĄCE Z CYBERPRZESTRZENI

Gwałtowny, niekontrolowany wręcz rozwój cyberprzestrzeni, a także trudności w jej zdefiniowaniu, jak i zachodzące w niej zjawiska oraz brak nadążających unormowań prawnych i zbyt mała świadomość podmiotów publicznych i prywatnych życia społecznego co do niebezpieczeństw, jakie może generować, sprawiają, iż służy ona jako wirtualna podstawa dla rozwoju coraz bardziej zaawansowanych zagrożeń, które są w stanie wpłynąć na świat realny. Istotnymi z punktu widzenia tekstu są cyberataki oraz cyberwojna.

Cyberatak, definiowany na rozmaite sposoby, najczęściej ze względu na potrzeby danego opracowania, nie posiada definicji legalnej. Uznać należy, iż jest to operacja przeprowadzona w cyberprzestrzeni, o ofensywnym charakterze, której celem jest spowodowanie obrażeń, a nawet

[5] Jednoznaczne zdefiniowanie pojęcia zagrożenia asymetryczne jest niezwykle trudne ze względu na różnorodność zjawisk jakie wpasowują się w tę kategorię. Wymienienie wspólnych cech charakterystycznych również nie wydaje się ułatwiać sprawy. Zagrożenia asymetryczne opierają się bowiem w głównej mierze na strategii, wykorzystaniu tych aspektów, w których atakujący ma przewagę, bądź jest w stanie ją szybko wygenerować. Asymetryczny konflikt zbrojny ma miejsce wówczas, gdy dochodzi do starcia z przeciwnikiem nierzadko rozproszonym lub zupełnie nieznanym, co do którego możliwość powzięcia akcji odwetowej wydaje się być znikoma, wyznaczającego cele, wykorzystującego metody działania, sposób walki i zorganizowanie, które nie mieszczą się w konwencjonalnym pojęciu wojny. (Szerzej: E. Sadowska, *Zagrożenia asymetryczne – definicja, świadomość społeczna i rola we współczesnym świecie*, Rocznik Bezpieczeństwa Międzynarodowego 2017, vol. 11, nr 2, str. 24. oraz Z. Ciekanowski, *Działania asymetryczne jako źródło zagrożeń bezpieczeństwa*, Nauki Humanistyczne i Społeczne Na Rzecz Bezpieczeństwa. Bezpieczeństwo i Technika Pożarnicza 2009, nr 3, str. 51.).

[6] T. R. Aleksandrowicz, *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, Przegląd Bezpieczeństwa Wewnętrznego 2016, nr 15, str. 11.

[7] M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw,* Katowice 2015, str. 71-78.

[8] J. Worona, *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Białystok 2017, str. 24-27.

[9] A. Kozłowski, *NATO wobec wyzwań i zagrożeń w cyberprzestrzeni*, Biuletyn OPINIE FAE nr 7, Warszawa 2016, str. 2.

śmierci osób lub uszkodzenia albo zniszczenia mienia[10]. Masowe cyberataki generowane przez podmioty państwowe stanowić mogą główną broń wykorzystywaną na potrzeby cyberkonfliktów. Na dzień dzisiejszy za większością cyberataków stoją jednakże pojedyncze jednostki i ugrupowania składające się z hakerów, niesankcjonowane oficjalnie przez państwa (nawet jeśli to z ich terytorium przeprowadzane jest dane natarcie), kierujące się przesłankami ideologicznymi, religijnymi, ekonomicznymi ale także chęcią zaistnienia we własnym środowisku i wywołania rozgłosu swoim działaniem.

Cyberwojna, podobnie jak wcześniej wspomniana cyberprzestrzeń i cyberatak, również nie posiada jednej, ogólnie akceptowanej definicji. Określana jest jako nowy sposób zwalczania przeciwnika, służąca między innymi (ale nie jedynie!) do walki z nim poza fizyczną płaszczyzną starcia. Wykorzystywana może być z dużą skutecznością do walki z wrogim dowództwem sił zbrojnych, bez ograniczania się do zwalczania zasobów ludzkich na linii frontu[11]. Prowadzona mogłaby być w celu wywołania zakłóceń lub nawet całkowitego unieszkodliwienia systemów informatycznych wroga. Mimo użycia do jej określenia miana «cyber», niekoniecznie musi ona mieć wymiar jedynie wirtualny. W literaturze przedmiotu pojawiają się głosy, iż elementem cyberwojny będzie również przejęcie bądź zniszczenie technologii i systemów informatycznych przeciwnika przy użyciu konwencjonalnych metod, tj. np. z wykorzystaniem uderzenia żołnierzy lub broni balistycznej[12]. Cyberkonflikt (pojęcie używane nieraz w literaturze przedmiotu zamiennie z cyberwojną) to zatem konflikt cybernetyczny, angażujący systemy informatyczne, dane i procesy związane z sieciami komputerowymi oraz ludzi, do zadań których należy nadzorowanie i kontrola jego przebiegu[13]. Cyberwojną będzie więc wszelka *działalność państw mająca na celu penetrację systemów i sieci komputerowych innych podmiotów międzynarodowych dla dokonania określonych zniszczeń lub zakłóceń*[14].

Uderzenie wymierzone w komputery lub sieci przeciwnika może doprowadzić do znacznego uszkodzenia tzw. infrastruktury krytycznej[15], w efekcie czego spodziewać można się skutków w postaci odcięcia populacji od podstawowych środków koniecznych do egzystencji, takich jak bieżąca woda, elektryczność czy dostęp do służby zdrowia. W przypadku zniszczenia systemów nawigacyjnych, istnieje ryzyko sparaliżowania ruchu w przestrzeni powietrznej, a nawet do pojawienia się ofiar śmiertelnych, gdy zneutralizowana zostanie łączność między lotnictwem a naziemną obsługą kontroli lotów[16]. Istotnym elementem odróżniającym cyberwojnę od cyberataku jest prowadzenie pierwszej przez państwa, natomiast cyberataków dopuścić się może zarówno państwo jak i podmioty niepaństwowe, np. grupa terrorystyczna, organizacja pozarządowa.

NATO I CYBERPRZESTRZEŃ

Broń niekonwencjonalna, w danym przypadku cybernetyczna, stanie się wraz z dalszym rozwojem technologicznym chętnie wykorzystywanym orężem przy prowadzeniu konfliktów. Wojna wkracza bowiem do cyberprzestrzeni i *vice versa*, cyberprzestrzeń zaczyna mieć coraz większy wpływ na prowadzone w świecie materialnym działania zbrojne. Wizja konfliktu cybernetycznego jest przerażająca między innymi ze względu na możliwość precyzyjnego ukierunkowania jego przebiegu

[10] *Cyber warfare and international humanitarian law: The ICRC's position*, tekst dostępny na stronie: https://www.icrc.org/en/doc/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf.

[11] K. Boruc, *Cyberwojna – nowa forma czy uzupełnienie klasycznego konfliktu zbrojnego?* [w:] K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warszawa 2014, str. 98.

[12] P. Łuczuk, *Cyberwojna. Wojna bez amunicji*, Kraków 2017, str. 19.

[13] Ibidem, str. 21.

[14] M. Lakomy, *Cyberwojna jako rzeczywistość XXI wieku*, tekst dostępny na stronie: http://geopolityka.org /analizy/miron-lakomy-cyberwojna-jako-rzeczywistosc-xxi-wieku.

[15] Infrastruktura krytyczna to między innymi urządzenia, instytucje usługowe oraz inne dziedziny, dzięki którym możliwe jest prawidłowe funkcjonowanie m.in. gospodarki, polityki oraz administracji, koniecznych do poprawnego i właściwego zarządzania państwem. Ma istotny wpływ na zapewnienie bezpieczeństwa w kraju obejmując obiekty szczególnie ważne dla jego obronności i egzystencji jego obywateli, takie jak np. elektrownie, linie energetyczne, ujęcia wody pitnej, naziemne trasy transportowe, lotniska, porty. (Szerzej: J. Milewski, *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, Zeszyty Naukowe AON nr 4 (105) 2016.)

[16] *Cyber warfare and international humanitarian law: The ICRC's position... Op. cit.*

zgodnie z zamiarem sprawcy – przeciwnik może ominąć wszelkie przeszkody, takie jak chociażby granice państwowe i uderzyć pojedynczą osobę, grupę ludzi albo cały dany obszar[17]. Dodatkowo wykrycie autora danego incydentu graniczy z cudem, gdyż postacie kryjące się za atakami potrafią doskonale zamaskować wszelkie mogące do nich doprowadzić ślady. Ponadto, zlokalizowanie miejsca i sprzętu, z którego dokonano destrukcyjnego działania nie gwarantuje wcale ustalenia tożsamości sprawcy. Powyższe doprowadza do sytuacji, w której ewentualnie zebrany materiał dowodowy może nie być wystarczający do przypisania pełnej odpowiedzialności za atak danemu państwu, bądź ugrupowaniu. Istotną wydaje się również być kwestia wystąpienia zintegrowanego ataku, który mógłby być przeprowadzony z wielu miejsc na świecie, a wówczas wskazanie winnego za jego zrealizowanie pozostałoby najprawdopodobniej jedynie domniemaniem[18].

NATO, jako najpotężniejszy politycznie i militarnie sojusz na świecie, jest niewątpliwie oczywistym celem ewentualnych ataków przeprowadzonych przy wykorzystaniu cyberprzestrzeni[19]. W trakcie operacji NATO w Kosowie Sojusz musiał zmierzyć się z popierającymi serbską stronę konfliktu haktywistami[20], którzy doprowadzili do kilkudniowego zablokowania elektronicznych skrzynek pocztowych i zakłócenia funkcjonowania strony internetowej NATO. Wydarzenie, choć nie wywołało poważniejszych szkód w prowadzeniu misji, stało się dla Sojuszu pierwszym impulsem do podjęcia działań w celu niedopuszczenia, by podobna sytuacja miała miejsce w przyszłości. W efekcie w 2002r. na szczycie w Pradze ówcześni przywódcy państw wchodzących w skład Sojuszu przyjęli *Program obrony w cyberprzestrzeni* (The CyberDefenceProgramme*)*, zawierający wytyczne, których wdrożenie miałoby zwiększyć bezpieczeństwo sieci organizacji[21] oraz powołano *Zespół reagowania na incydenty komputerowe* (NATO Computer Incident Response Capability – NCIRC), którego zadaniem było wykrywanie i zwalczanie złośliwego oprogramowania[22].

Jednakże zdarzeniem, które w pełni otworzyło oczy państwom Paktu Północnoatlantyckiego była seria ataków przeprowadzona w 2007 roku przeciwko systemom informatycznym i telekomunikacyjnym Estonii. Wydarzenie to, określane w literaturze przedmiotu jako *I cyberwojna,* przeprowadzone zostało przecież przeciwko państwu należącemu do struktur NATO. W związku z tym przywódcy kraju rozważali powołanie się na artykuł V Traktatu Północnoatlantyckiego[23], jednakże ze względu na brak jednomyślności ze strony pozostałych członków Sojuszu i ogólną niepewność co do kwalifikacji zdarzenia jako napaści zbrojnej w myśl art. 51 Karty Narodów Zjednoczonych[24] oraz braku pewności, iż w danym przypadku art. 5 traktatu waszyngtońskiego w ogóle jest możliwy do zastosowania, z pomysłu ostatecznie zrezygnowano[25].

Jednym ze skutków wydarzeń z Estonii było powołanie Centrum Doskonalenia Cyberobrony NATO w Tallinie (CooperativeCyberDefence Center of Excellence – CCDCOE). Kolejnym – wzrost świadomości co do skutków i spustoszeń, jakie z powodzeniem przeprowadzone ataki mogą wywołać w infrastrukturach rozwiniętych państw, coraz bardziej uzależnionych od sieci i komputerów. Taki

[17] T. Wheeler, *In cyberwar, there are no rules. Why the world desperately needs digital Geneva Conventions,* tekst dostępny na stronie: https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense.

[18] B. Józefiak, *Czy atak w cyberprzestrzeni uruchomi artykuł 5 traktatu NATO?*, tekst dostępny na stronie internetowej: https://www.cyberdefence24.pl/czy-atak-w-cyberprzestrzeni-uruchomi-artykuł-5-traktatu-nato.

[19] M. Lakomy, *Conditions to Invoke the Principle of Artice 5 of The North Atlantic Treaty in Case of a Cyberattack or a Cyber Conflict*, [w:] J. Świątkowska (red.), *NATO Road to Cybersecurity,* The Kosciuszko Institute 2016, str. 35.

[20] Haktywizm jest kombinacją aktywizmu i działań przestępczych, polegającą na wykorzystaniu metod hakerskich przeciwko określonym celom z zamiarem zakłócenia ich funkcjonowania. Działalność ta nastawiona jest na zwrócenie uwagi na dany problem. (Szerzej: P. Łuczuk, *Cyberwojna. Wojna bez amunicji*, Kraków 2017, str. 21.).

[21] V. Joubert, *Five years after Estonia's cyber attacks: lessons learned for NATO?*, Redearch Paper, NATO Defence College Research Division 2012, nr 76, str. 2.

[22] A. Kozłowski, *NATO wobec wyzwań i zagrożeń w cyberprzestrzeni*, Biuletyn OPINIE FAE nr 7, Warszawa 2016, str. 2-3.

[23] Artykuł 5 Traktatu Północnoatlantyckiego, Waszyngton, 4 kwietnia 1949 r. Dz.U.2000.87.970.

[24] Art. 51. Karty Narodów Zjednoczonych, Dz. U. 1947 nr 23 poz. 90.

[25] A. Kozłowski, op. cit., str. 3.

stan rzeczy doprowadził w końcu do zmiany w podejściu NATO co do problemu, zwiększając potrzebę ustanowienia nowej polityki odnoście jego zwalczania[26].

Koncepcja Strategiczna NATO z 2010 r. zakłada, iż Sojusz rozwijać będzie *możliwości zapobiegania, wykrywania, obrony przed atakami cybernetycznymi oraz odtwarzania zdolności po nich, w tym wykorzystując proces planowania NATO na rzecz wzmocnienia i koordynacji narodowych zdolności w dziedzinie obrony cybernetycznej, włączając instytucje NATO w scentralizowany system ochrony cybernetycznej oraz integrując system monitorowania, ostrzegania i reagowania cybernetycznego NATO z państwami członkowskimi*[27]. Jednocześnie zawarto w niej stwierdzenie, *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*[28].

Deklaracja szczytu walijskiego z 5 września 2014 roku nakreśliła zagrożenia mogące wiązać się z cyberprzestrzenią, wskazując na potencjalnie destrukcyjną siłę cybeataków oraz zapewniła, iż Organizacja Traktatu Północnoatlantyckiego potwierdza zasady niepodzielności bezpieczeństwa Sojuszu oraz zapobiegania, wykrywania, odporności, przywracania funkcjonalności i obrony przed atakami cybernetycznymi[29]. W celu zmierzenia się z zagrożeniem przyjęto Wzmocnioną Politykę Cyberobrony (EnhancedCyberDefence Policy). Przełomowym okazało się być zawarte w deklaracji stwierdzenie, iż prawo międzynarodowe (w tym międzynarodowe prawo humanitarne – *ius in bello*), jak i Karta Narodów Zjednoczonych obowiązują w odniesieniu do cyberprzestrzeni[30]. Powrócono również do kwestii ewentualnego zastosowania artykułu 5 Traktatu Północnoatlantyckiego w przypadku, gdyby ofiarą ataków przeprowadzonych przy użyciu cyberprzestrzeni padł jeden z członków Sojuszu. Zadecydowano, iż w sytuacji ataku cybernetycznego, adekwatność powołania się na artykuł 5, będzie każdorazowo oceniana przez Radę Północnoatlantycką na podstawie analizy konkretnego przypadku[31]. Na dzień dzisiejszy żadne z dotychczas zrealizowanych uderzeń nie zostało uznane za uzasadniające odwołanie się do samoobrony zbrojnej na podstawie art. 5 Traktatu Północnoatlantyckiego oraz art. 51 Karty Narodów Zjednoczonych[32].

Na szczycie NATO w Warszawie uznano ostatecznie cyberprzestrzeń za obszar działań, na równi z powietrzem, lądem i morzem (oraz przestrzenią kosmiczną[33])[34]. Decyzja ta zbliżyła Sojusz do

[26] D. C. Alexander, Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses, str. 3.

[27]Koncepcja Strategiczna NATO z 2010r., pkt. 19, Lizbona 2010, tekst dostępny na stronie: https://www.bbn.gov.pl/download/1/15758/koncepcjastrategicznanato.pdf.

[28] Ibidem, pkt. 12.

[29] S. Jackson, *NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Agression Qualifies as an Armed Attack*, Center for Infrastructure Protection and Homeland Security, George Mason University 2016, str.1.

[30] Deklaracja szczytu walijskiego złożona przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Walii 5 września 2014 r., pkt. 72, tekst dostępny na stronie: https://www.bbn.gov.pl/ftp/dok/Deklaracja%20szczytu%20walijskiego.pdf.

[31] M. Veenendaal, K. Kaska, P. Brangetto, *Is NATO Ready to Cross the Rubicon on Cyber Defence?*, Cyber Policy Brief, Tallin 2016, str. 3.

[32] B. Józefiak, *Czy atak w cyberprzestrzeni uruchomi artykuł 5 Traktatu NATO?*, tekst dostępny na stronie: https://www.cyberdefence24.pl/czy-atak-w-cyberprzestrzeni-uruchomi-artykul-5-traktatu-nato.

[33] Cyberprzestrzeń nazywana jest w literaturze przedmiotu piątą sferą działalności (the fifth domain). Jednakże deklaracja końcowa szczytu NATO w Warszawie nie uwzględnia w tekście przestrzeni kosmicznej. (Szerzej: Deklaracja końcowa szczytu NATO w Warszawie wydana przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r., pkt. 70, tekst dostępny na stronie: https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf.).

[34] Deklaracja końcowa szczytu NATO w Warszawie wydana przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r., pkt. 70, tekst dostępny na stronie: https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf.

usprawiedliwienia ewentualnej odpowiedzi na atak cybernetyczny ze strony wrogiego podmiotu, nawet przy użyciu broni konwencjonalnej[35].

ZASTOSOWANIE ARTYKUŁU 5 TRAKTATU PÓŁNOCNOATLANTYCKIEGO W ODPOWIEDZI NA CBERATAK

Artykuł 5 Traktatu Północnoatlantyckiego powstał w zupełnie odmiennych realiach niż te, w których świat znajduje się obecnie. Z tego samego powodu cała struktura funkcjonowania Sojuszu wymaga transformacji celem dostosowania NATO do zupełnie nowych wyzwań i warunków, z jakimi musi się aktualnie mierzyć. Zmiany muszą nastąpić również w interpretacji artykułu 5, by mógł on pozostać funkcjonalnym w obliczu współczesnych zagrożeń. I chociaż od spisania treści Traktatu Waszyngtońskiego minęło już wiele lat, nie ma w zasadzie wątpliwości, iż artykuł 5, który ukształtował tak naprawdę strukturę oraz mechanizmy działania NATO, pozostaje w znacznym stopniu siłą napędową Sojuszu i świadczy o jego przydatności dla zrzeszonych państw, jako że obrona zbiorowa przed siłami nieprzyjaciela pozostaje głównym zadaniem organizacji[36].

W świetle zapewnień poczynionych przez przywódców państw na szczytach NATO, a w szczególności w 2014 roku w Walii oraz w 2016 roku w Warszawie, można stwierdzić, iż Sojusz faktycznie zmienia swoje podejście do zagrożeń płynących z cyberprzestrzeni, decydując się na modyfikację swojego rozumienia implikacji zawartych w treści artykułu 5. Jednakże, mimo iż NATO zadeklarowało możliwość powołania się na dany przepis, sposób w jaki Rada Północnoatlantycka rozpatrzyć miałaby zasygnalizowany cyberatak pozostaje wciąż nieznany[37]. Brak konkretnych wytycznych sprawia, iż z jednej strony możliwym jest rozpatrzenie każdego kazusu w sposób zindywidualizowany i elastyczny[38], jednakże taki stan rzeczy prowadzić może również do wewnętrznych sporów co do zaadaptowania konkretnego stanowiska w danej sprawie i do całkowitej uznaniowości podyktowanej czysto politycznymi pobudkami. Jasną jest kwestia konwencjonalnej napaści zbrojnej na którekolwiek z państw członkowskich – wówczas Sojusz jest w stanie odpowiedzieć na atak przy użyciu wchodzących w jego kolektywne zasoby tradycyjnych sił zbrojnych. Co jednak państwa członkowskie NATO mogłyby uczynić w przypadku konfliktu rozgrywającego się w sieci? Czy NATO ograniczyłoby się jedynie do odpowiedzi za pomocą środków cybernetycznych, czy też zdecydowałoby się odpowiedzieć na cyberatak przy użyci broni konwencjonalnej? Na chwilę obecną jakakolwiek decyzyjność w zakresie reagowania na cyberataki pozostaje w zupełności uznaniowa, oparta o analizę wyodrębnionych przypadków, z racji na fakt, iż w przypadku ataku cybernetycznego Sojusz, nie dysponujący wciąż klarownymi normami, miałby do rozważenia wiele zmiennych.

Problem samej kwalifikacji ataku cybernetycznego jako napaści zbrojnej został rozwiązany w treści uprzednio wspomnianych deklaracji, przyjętych kolejno w Walii oraz Warszawie. Teoretycznie, kwestia ta jest klarowna – przywódcy państw członkowskich uznali, iż dane cyberataki skierowane przeciwko członkom NATO mogą usprawiedliwić aktywację indywidualnej oraz zbiorowej samoobrony w ramach struktur Paktu Północnoatlantyckiego, *ius in bello* ma zastosowanie do działań prowadzonych w cyberprzestrzeni, a ją samą zaliczyli do obszaru operacyjnego działań organizacji[39]. Jednakże w praktyce cyberataki charakteryzuje ogromna trudność we wskazaniu kryjącego się za nimi sprawcy, a sama specyfika budowy sieci sprawia, iż określenie miejsca, z którego atak przeprowadzono, sprawiłoby wiele problemów. Warto również zaznaczyć, że niektóre ataki specjalnie

[35] P. Paganini, *NATO officially recognizes cyberspace as warfare domain*, tekst dostępny na stronie: https://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html.

[36] B. Winid, *Artykuł 5. Traktatu Waszyngtońskiego jako fundament NATO*, tekst dostępny na stronie: *https://www.bbn.gov.pl/download/1/1025/artykul5.pdf*.

[37] S. Jackson, *NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Agression Qualifies as an Armed Attack*, Center for Infrastructure Protection and Homeland Security, George Mason University 2016, str. 2.

[38] M. Lakomy, *Conditions to Invoke the Principle of Artice 5 of The North Atlantic Treaty in Case of a Cyberattack or a Cyber Conflict*, [w:] J. Świątkowska (red.), *NATO Road to Cybersecurity*, The Kosciuszko Institute 2016, str. 36.

[39] Ł. Boguszewski, *Cyberataki a artykuł V po szczycie NATO w Brukseli*, tekst dostepny na stronie: https://www.cyberdefence24.pl/polityka-cookies/cyberataki-a-artykul-v-po-szczycie-nato-w-brukseli.

przeprowadzane są przez grupy osób, celowo rozproszonych pod względem miejsca – w świecie cyberprzestrzeni nie istnieją bowiem granice terytorialne.

Uruchomienie artykułu 5 Traktatu Północnoatlantyckiego wymaga wskazania przeciwnika. Ustalenie pojedynczych osób lub zgrupowania stojących za faktycznym przeprowadzeniem ataku nie warunkuje ustalenia «zleceniodawcy», a co za tym idzie – może uniemożliwić dowiedzenie, iż to dane państwo stoi za wywołaniem danego cyberkonfliktu. Udowodnienie, iż między jednostką dopuszczającą się ataku a władzami potencjalnie wrogiego państwa istnienie jakieś sankcjonujące powiązanie może okazać się nader trudne w wykonaniu, o ile w ogóle możliwe, co z kolei niweluje szanse na wskazanie winnego, które usatysfakcjonowałyby wymogi prawne powołania się na prawo do samoobrony[40]. Znakomita część ataków cybernetycznych pozostałaby więc jedynie w cieniu domniemań.

Często zwraca się uwagę na to, że możliwość przywołania art. 5 dotyczyłaby jedynie ataków wiążących się ze znacznymi stratami materialnymi albo w skutek których pojawiły się ofiary w ludziach[41]. Nietrudno wyobrazić sobie uderzenie przypuszczone na systemy sterujące działaniem elektrowni atomowej, której uszkodzenie mogłoby doprowadzić do szkód zarówno w wymiarze materialnym, czyli chociażby środowiskowym, gospodarczym, energetycznym ale również skutkować utratą życia i zdrowia przez ludność. Jednakże atak przypuszczony «jedynie» na sieć nie zmotywowałby raczej NATO do konwencjonalnej odpowiedzi militarnej w ramach samoobrony. Ewentualnością byłaby akcja odwetowa wymierzona w systemy teleinformatyczne przeciwnika, jednakże zważywszy na opisaną powyżej problematykę jego namierzenia oraz przyjęcie przez Sojusz raczej defensywnego stanowiska w kwestii rozwoju zabezpieczeń cybernetycznych, taki scenariusz również wydaje się mało prawdopodobny.

Warto wspomnieć, iż artykuł 5 nie może być zastosowany w przypadku, gdy mamy do czynienia z masowym szpiegostwem przy wykorzystaniu cyberprzestrzeni[42], mimo iż przejmowanie ogromnych ilości danych za pomocą sieci to nie tylko hipotetyczna możliwość, ale rzeczywista, wykorzystywana na globalną skalę procedura, która odbywa się praktycznie nieustannie, mogąca w pośredni sposób prowadzić do katastrofalnych skutków w zakresie utrzymania bezpieczeństwa danych krajów i organizacji.

Istotnym z punktu widzenia przedstawionej problematyki jest niewątpliwie również artykuł 4 Traktatu Północnoatlantyckiego. W sytuacji, gdy skorzystanie z artykułu 5 okazałoby się trudne albo wręcz niekorzystne politycznie, powołanie się na treść artykułu 4[43] mogłoby okazać się adekwatnym wyjściem. Udzielenie pomocy przez inne państwa Sojuszu, takiej jak chociażby użyczenie serwerów bądź zapewnienie wsparcia udzielonego przez ekspertów oraz wymiana doświadczeń mogłoby pozwolić na sprawniejsze uporanie się z atakiem[44].

WARUNKI KONIECZNE DLA ZASTOSOWANIA ARTYKUŁU 5 TRAKTATU PÓŁNOCNOATLANTYCKIEGO

Jedną z propozycji w przypadku rozważania możliwości powołania się na artykuł 5 Traktatu Waszyngtońskiego w przypadku wystąpienia cyberataku skierowanego przeciwko członkowi Sojuszu, jest przeanalizowanie informacji uzyskanych na podstawie zastosowania poniższego schematu:

1. Określenie zasięgu ataku: czy atak dotkną jedno czy więcej państw Sojuszu? Prawdopodobieństwo powołania się na artykuł 5 wzrastałoby wraz z liczbą podmiotów poszkodowanych;
2. Określenie czasu trwania i natężenia ataku: czy był to pojedynczy incydent, czy też seria uderzeń; czy atak był krótkotrwały, czy może rozciągnięty w czasie;

[40] V. Joubert, *Five years after Estonia's cyber attacks: lessons learned for NATO?*, Redearch Paper, NATO Defence College Research Division 2012, nr 76, str. 3.

[41] B. Józefiak, *Czy atak w cyberprzestrzeni uruchomi artykuł 5 Traktatu NATO?*, tekst dostępny na stronie: https://www.cyberdefence24.pl/czy-atak-w-cyberprzestrzeni-uruchomi-artykul-5-traktatu-nato.

[42] Ibidem.

[43] Artykuł 4 Traktatu Północnoatlantyckiego, Waszyngton, 4 kwietnia 1949 r. Dz.U.2000.87.970.
Strony będą się wspólnie konsultowały, ilekroć, zdaniem którejkolwiek z nich, zagrożone będą integralność terytorialna, niezależność polityczna lub bezpieczeństwo którejkolwiek ze Stron.

[44] A. Kozłowski, *op. cit.*, str. 10.

3. Określenie skutków ataku: czy zdarzenie doprowadziło do uszkodzenia bądź istotnych zniszczeń infrastruktury krytycznej; czy w bezpośrednim lub pośrednim efekcie atak doprowadził do śmierci lub utraty zdrowia ludzi;
4. Określenie, czy sprawcą ataku było państwo, organizacja międzynarodowa lub czy też czyn nie został przypadkiem zainicjowany przez podmiot wewnętrzny zaatakowanego kraju, czyniąc go sprawą wewnętrzną danego państwa[45];
5. Określenie zaatakowanych obiektów oraz określenie celów ataku. Można tu wyznaczyć następujące kategorie: atak skierowany przeciwko militariom państwa, atak ukierunkowany na infrastrukturę krytyczną oraz inne sfery witalne dla państwa, chociażby cywilne[46].

Nim bardziej doniosłe, rozległe i zorganizowane, a także nikczemne okażą się konsekwencje ataku, tym większe stanie się prawdopodobieństwo reakcji NATO bazującej na prawie do samoobrony.

PODSUMOWANIE

Dynamiczne zmiany zachodzące w obecnych czasach na świecie zmuszają do wdrażania coraz szybszych i gwałtowniejszych zmian. Wyjątkiem w tym zakresie nie są nawet tak potężne i obecne na globalnej arenie od lat organizacje międzynarodowe, jaką bez wątpienia jest Organizacja Traktatu Północnoatlantyckiego. W związku z rozwojem i coraz szerszym zastosowaniem sfery «cyber» w odniesieniu do funkcjonowania ludzkości, również ta płaszczyzna musiała zostać objęta zainteresowaniem Sojuszu.

Zawarty w Traktacie Północnoatlantyckim słynny artykuł 5, upoważniający w przypadku zbrojnej napaści państwa członkowskie Sojuszu do udzielenia pomocy Stronie lub Stronom napadniętym w ramach wykonywania prawa do indywidualnej lub zbiorowej samoobrony, uznanego na mocy artykułu 51 Karty Narodów Zjednoczonych, na mocy decyzji podjętych przez przywódców NATO znalazł zastosowanie w przypadku skierowania przeciwko któremukolwiek z członków Organizacji ataku przy wykorzystaniu możliwości, jakie obecnie zapewnia cyberprzestrzeń. W związku z tym zrównano *de facto* pewien rodzaj ataków cybernetycznych z konwencjonalnym atakiem zbrojnym. Atak taki musiałby oczywiście przejawiać cechy, mogące pozwolić na zakwalifikowanie go jako faktyczne zagrożenie dla bezpieczeństwa, stabilności i wartości budujących Sojusz.

Mimo braków występujących w uregulowaniach przedstawionej tematyki oraz braku ujednoliconego systemu odpierania cyberataków wypracowanego przez członków NATO uciekających się dotychczas do wdrażania zabezpieczeń na poziomach krajowych, widać znaczne ożywienie Sojuszu w odniesieniu do zagrożeń, jakie generuje cyberprzestrzeń. Dotychczasowe doświadczenia w zakresie cyberniebezpieczeństw pokazały, jak poważne mogą być konsekwencje dalszego bagatelizowania problemu. W związku z tym dalsze prace Sojuszu w tej dziedzinie wydają się nieuniknione.

References

1. Aleksandrowicz T. R., *Bezpieczeństwo w cyberprzestrzeni ze stanowiska prawa międzynarodowego*, Przegląd Bezpieczeństwa Wewnętrznego 2016.
2. Alexander D. C., Cyber Threats Against the North Atlantic Treaty Organization (NATO) and Selected Responses.
3. Boguszewski Ł., *Cyberataki a artykuł V po szczycie NATO w Brukseli*, tekst dostepny na stronie: https://www.cyberdefence24.pl/polityka-cookies/cyberataki-a-artykul-v-po-szczycie-nato-w-brukseli.
4. Boruc K., *Cyberwojna – nowa forma czy uzupełnienie klasycznego konfliktu zbrojnego?* [w:] K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji,* Warszawa 2014.

[45] B. Józefiak, *Czy atak w cyberprzestrzeni uruchomi artykuł 5 Traktatu NATO?*, tekst dostępny na stronie: https://www.cyberdefence24.pl/czy-atak-w-cyberprzestrzeni-uruchomi-artykul-5-traktatu-nato.

[46] M. Lakomy, *Conditions to Invoke the Principle of Artice 5 of The North Atlantic Treaty in Case of a Cyberattack or a Cyber Conflict*, [w:] J. Świątkowska (red.), *NATO Road to Cybersecurity*, The Kosciuszko Institute 2016, str. 37-39.

5. Ciekanowski Z., *Działania asymetryczne jako źródło zagrożeń bezpieczeństwa*, Nauki Humanistyczne i Społeczne Na Rzecz Bezpieczeństwa. Bezpieczeństwo i Technika Pożarnicza 2009, nr 3.

6. *Cyber warfare and international humanitarian law: The ICRC's position*, tekst dostępny na stronie: https://www.icrc.org/en/doc/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf.

7. Deklaracja końcowa szczytu NATO w Warszawie wydana przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r., tekst dostępny na stronie: https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf.

8. Deklaracja końcowa szczytu NATO w Warszawie wydana przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r., tekst dostępny na stronie: https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf.

9. Deklaracja szczytu walijskiego złożona przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Walii 5 września 2014 r., pkt. 72, tekst dostępny na stronie: https://www.bbn.gov.pl/ftp/dok/Deklaracja%20szczytu%20walijskiego.pdf.

10. Jackson S., *NATO Article 5 and Cyber Warfare: NATO's Ambiguous and Outdated Procedure for Determining When Cyber Agression Qualifies as an Armed Attack*, Center for Infrastructure Protection and Homeland Security, George Mason University 2016.

11. Joubert V., *Five years after Estonia's cyber attacks: lessons learned for NATO?*, Redearch Paper, NATO Defence College Research Division 2012, nr 76.

12. Józefiak B., Czy atak w cyberprzestrzeni uruchomi artykuł 5 Traktatu NATO?, tekst dostępny na stronie: https://www.cyberdefence24.pl/czy-atak-w-cyberprzestrzeni-uruchomi-artykul-5-traktatu-nato.

13. Karta Narodów Zjednoczonych, Dz. U. 1947 nr 23 poz. 90.

14. Koncepcja Strategiczna NATO z 2010r., pkt. 19, Lizbona 2010, tekst dostępny na stronie: https://www.bbn.gov.pl/download/1/15758/koncepcjastrategicznanato.pdf.

15. Kozłowski A.*, NATO wobec wyzwań i zagrożeń w cyberprzestrzeni*, Biuletyn OPINIE FAE nr 7, Warszawa 2016.

16. Lakomy M., *Conditions to Invoke the Principle of Artice 5 of The North Atlantic Treaty in Case of a Cyberattack or a Cyber Conflict*, [w:] J. Świątkowska (red.), *NATO Road to Cybersecurity*, The Kosciuszko Institute 2016.

17. Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw,* Katowice 2015.

18. LakomyM., *Cyberwojna jako rzeczywistość XXI wieku*, tekst dostępny na stronie: http://geopolityka.org/analizy/miron-lakomy-cyberwojna-jako-rzeczywistosc-xxi-wieku.

19. Łuczuk P., *Cyberwojna. Wojna bez amunicji*, Kraków 2017.

20. Milewski J., *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, Zeszyty Naukowe AON nr 4 (105) 2016.

21. Paganini P., *NATO officially recognizes cyberspace as warfare domain*, tekst dostępny na stronie: https://securityaffairs.co/wordpress/48484/cyber-warfare-2/nato-cyberspace-warfare-domain.html.

22. Sadowska E., *Zagrożenia asymetryczne – definicja, świadomość społeczna i rola we współczesnym świecie*, Rocznik Bezpieczeństwa Międzynarodowego 2017, vol. 11, nr 2.

23. Traktat Północnoatlantycki, Waszyngton, 4 kwietnia 1949 r. Dz.U.2000.87.970.

24. Veenendaal M., Kaska K., Brangetto P., *Is NATO Ready to Cross the Rubicon on Cyber Defence?*, Cyber Policy Brief, Tallin 2016.

25. Wheeler T., *In cyberwar, there are no rules. Why the world desperately needs digital Geneva Conventions*, tekst dostępny na stronie: https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense/ [data dostępu: 16.03.2019r.].

26. Worona J., *Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy*, Białystok 2017.

27. Wróblewski R., *O definiowaniu wojny,* [w:] M. Kubiak, R. Wróblewski (red.), *Oblicza współczesnych wojen,* Warszawa 2018.