Świątkowska, J., Walka z cyberzagrożeniami jako wyzwanie stojące przed globalnym bezpieczeństwem, Przegląd Geopolityczny, 20, 2017, s. 162-177.

Joanna ŚWIĄTKOWSKA
Uniwersytet Pedagogiczny w Krakowie

WALKA Z CYBERZAGROŻENIAMI JAKO WYZWANIE STOJĄCE PRZED GLOBALNYM BEZPIECZEŃSTWEM

Abstrakt:
Artykuł jest analizą wpływu nowego rodzaju zagrożeń, płynących z cyberprzestrzeni na współczesne bezpieczeństwo międzynarodowe i relacje międzynarodowe. Jego celem jest także dokonanie oceny, czy działania prowadzone w cyberprzestrzeni są relewantne z punktu widzenia analiz geopolitycznych. Tekst zawiera opis kluczowych zagrożeń, które wynikają z przeniesienia życia społecznego do cyberprzestrzeni.

Słowa kluczowe: cyberprzestrzeń, cyberbezpieczeństwo, geopolityka, walka informacyjna, infrastruktura krytyczna.

Cyberprzestrzeń wpływa nie tylko na funkcjonowanie państw, społeczeństw, gospodarek. Coraz częściej działania w niej prowadzone, stają się istotne z punktu widzenia teorii stosunków międzynarodowych odnoszących się do mechanizmów działania różnorodnych procesów społecznych oraz politycznych. Cyberprzestrzeń jest zjawiskiem z którym zmierzyć się muszą także wszyscy, którzy analizują świat z wykorzystaniem optyki geopolitycznej.

Najbardziej tradycyjne rozumienie terminu geopolityka, wskazywać by mogło, że nie ma ona wiele wspólnego z cyberprzestrzenią. Celem niniejszego artykułu jest nie tylko dokonanie analizy tego, czy rzeczywiście geopolityka stanowi właściwe ramy do rozważań o cyberbezpieczeństwie, ale przede wszystkim wskazanie, jakie wyzwania płynące ze świata cyfrowego są aktualnie kluczowe dla stosunków międzynarodowych i globalnego bezpieczeństwa. To bowiem leży u podstaw zainteresowania geopolityki właśnie.

Definiowanie geopolityki i jej najważniejszych elementów

Czym zatem jest geopolityka? Definiowana jest ona m.in.: „jako nauka o charakterze interdyscyplinarnym badająca [...] wpływ czynników geograficznych i historycznych na powstawanie i funkcjonowanie państw (ośrodków siły)" (Lach, Wendt, red., 2010, s. 6-7; Sykulski 2009, s. 31). Według powszechnie wskazywanych założeń geopolityki, jedną z głównych determinant wpływających na funkcjonowanie państw, na realizowanie przez nich swoich

szeroko rozumianych celów, i w konsekwencji na ich pozycję na arenie międzynarodowej, są uwarunkowania geograficzne (por. W. J. Wilczyński 2016, s. 11). Powiązane z nimi inne, zagregowane czynniki wpływają na ogólną siłę państwa i możliwość realizowania interesów narodowych. O tym, jakie będą to interesy, i jednocześnie które czynniki będą najmocniej wpływać na ogólną pozycję państw na globalnej szachownicy, zależy w dużym stopniu od przyjęcia pewnej optyki rozumienia i interpretowania świata.

Zgodnie z twórcą geopolityki i jednym z jej najbardziej znanych reprezentantów F. Ratzelem, autorem pierwszej *Geografii politycznej,* terytorium jest traktowane jako kategoria najwyższa, która nie tylko determinuje działania poszczególnych aktorów, ale także stanowi ważny cel ich dążeń (P.L.Wilczyński 2010, s. 114). W tym kontekście, z punktu widzenia geopolityki, czynniki takie jak zasoby militarne, otoczenie polityczne, będą miały największy wpływ na realizowanie interesów powiązanych z poszerzeniem wpływów, terytorium, osłabianiem przeciwnika. Takie podejście wydaje się zbieżne z realistyczną wizją stosunków międzynarodowych.

Optyka ta stawia w centrum zainteresowania takie fundamentalne kategorie jak przestrzeń czy też czas[1]. Są one rozumiane bardzo tradycyjnie, w sposób jaki prezentował między innymi Izaak Newton. W jego wersji, przestrzeń traktowana jest jako niezmienny byt absolutny, który poprzedza pojawienie się rzeczy, obiektów. Przestrzeń dzielona jest przez podmioty, które występują obok siebie bezpośrednio, fizycznie (Stalder 2012, s. 166-168). Przestrzeń jest zatem kategorią nadrzędną wpływającą na wszystko co się w niej znajduje. Drugim parametrem, niezmiernie ważnym w kontekście mówienia o geopolityce jest kategoria czasu. Warunkiem możliwości bezpośredniego oddziaływania na siebie dwóch podmiotów, rzeczy jest współdzielenie czasu.
A zatem podsumowując, jeśli założymy, że geopolityka oparta na przestrzeni i współdzieleniu czasu, determinuje wraz z innymi czynnikami, takimi jak choćby zasoby militarne, realizację celów państwa sprowadzających się do powiększania potęgi i terytorium, to można zadać pytanie, gdzie znajduje w takim kontekście swoje miejsce cyberprzestrzeń, jaki ma ona wpływ na działania poszczególnych państw i przede wszystkim, czy i jak wpływa ona na środowisko bezpieczeństwa międzynarodowego.

[1] Autorka na określenie przestrzeni i czasu użyła (czy świadomie?) kantowskiego wyrażenia „kategorie", co powinno przypominać, że tak przestrzeń (fizyczna) jak i czas, nie stanowią właściwości świata, ale są cechami, lub „kategoriami" umysłu; cyberprzestrzeń w tym kontekście stanowi jedną z przestrzeni, w których żyjemy, ale której do niedawna sobie nie uświadamialiśmy (przyp. red.).

Wpływ cyberprzestrzeni na funkcjonowanie człowieka

Rozwój technologii teleinformatycznych doprowadził do stworzenia cyberprzestrzeni[2], która całkowicie odmieniła życie człowieka i sposób funkcjonowania społeczeństwa. To nowe środowisko zmieniło także sposób myślenia o dwóch wspomnianych wcześniej kategoriach czasu i przestrzeni. Cyberprzestrzeń rzuciła tym samym wyzwanie dla zjawisk, koncepcji silnie na tych kategoriach opartych. Takich jak geopolityka właśnie. Dzięki istnieniu Internetu, człowiek zaczął funkcjonować w zupełnie nowym kontekście. Współcześnie, dany podmiot będąc w jednym miejscu globu jest w stanie oddziaływać, na drugi podmiot, który znajduje się zupełnie gdzie indziej. Podmioty te są jednocześnie w stanie wchodzić ze sobą w interakcje w czasie rzeczywistym. Jak powiedział Manuel Castells, „powstał nowy typ przestrzeni, pozwalający aktorom społecznym na współczasowość w różnych miejscach" (Stalder, ibid., por. także Świątkowska 2012).

Cyberprzestrzeń zrewolucjonizowała także sposób funkcjonowania społeczeństwa, w którym kluczowym zasobem stała się informacja i wiedza. Manuel Castells nazywa współczesne nam społeczeństwo „społeczeństwem wiedzy". To właśnie dostęp do wiedzy i informacji, jest czynnikiem, który oprócz tradycyjnych zasobów, takich jak na przykład potęga militarna, oddziałuje na funkcjonowanie społeczeństw, państw, podmiotów gospodarczych, wpływając między innymi na ich pozycję na arenie międzynarodowej. Wiedza daje potęgę, daje przewagę i jest czynnikiem sprawczym.

Współcześnie informacja i wiedza są także kluczowe z punktu widzenia prowadzenia konfliktów. Mogą stać się także ich przedmiotem. Dlatego właśnie myśląc o środowisku międzynarodowym, bezpieczeństwie globalnym, jak również o relacjach między najważniejszymi państwami i ich pozycjach na politycznej szachownicy, nie sposób nie dostrzec wpływu cyberprzestrzeni, która sama na informacji oraz wiedzy się opiera.

Cyberprzestrzeń i konflikty z nią związane

Cyberprzestrzeń jest nierozłącznie związana z wiedzą oraz z informacją. Jeśli żyjemy w erze, w której to właśnie te zasoby definiują konflikt, to jest oczywistym, że środowisko cyfrowe będzie nowym obszarem rywalizacji. Rywalizacja ta będzie miała kilka wymiarów, związanych z prowadzeniem szeroko rozumianej walki informacyjnej. Aby lepiej zrozumieć to zagadnienie warto jednak rozpocząć od dokonania krótkiej analizy tego czym jest informacja i jakie ma ona znaczenie oraz funkcje w konflikcie.

[2] W polskim porządku prawnym cyberprzestrzeń definiowana jest jako "przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne".

Według jednego z najwybitniejszych badaczy zagadnienia walki informacyjnej, Leopolda Ciborowskiego (1999, s 50), „*informacja to bodziec oddziałujący na układ recepcyjny człowieka, powodujący wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej (przedmiotu, procesu, zjawiska, pojęcia), który w jego przekonaniu (świadomości) kojarzy się z tym bodźcem*".

Bodziec ten pobudza człowieka do działania. Informacja jest zatem czynnikiem, za pomocą którego można oddziaływać na drugiego człowieka, na jego decyzje, zachowania i najważniejsze – na działania. Informacja to szczególny rodzaj sygnału, który sterować może także podmiotami nieożywionymi. Informacja jest zatem bardzo specyficzną formą sygnału, związaną konkretnie z człowiekiem[3].

Jeśli zatem zarówno człowiek, jak i maszyna funkcjonują w oparciu o odebrane informacje i sygnały, to łatwo zauważyć, że oddziaływanie, szczególnie wrogie, zarówno na informacje jak i na sygnały ma wpływ na efekt końcowy – zachowanie ludzi i maszyn. Właśnie dlatego informacja i sygnał stają się narzędziem walki – walki informacyjnej. Leopold Ciborowski wskazuje na trzy elementy walki informacyjnej – zakłócanie, obronę i zdobywanie. Obejmując zarówno działalność ofensywną jak i defensywną, walka informacyjna odgrywa współcześnie coraz ważniejszą rolę. Stało się tak dzięki pojawieniu się narzędzi teleinformatycznych i cyberprzestrzeni, operujących za pomocą informacji przedstawionej w postaci cyfrowej.

Cyberprzestrzeń wpływa na bezpieczeństwo międzynarodowe i na pozycję poszczególnych graczy na wiele sposobów. Dzięki narzędziom teleinformatycznym walka informacyjna rozumiana jako zdobywanie, obrona i atakowanie informacji, nakierowana zarówno na ludzi jak i na maszyny, może być realizowana z każdego miejsca na ziemi, w każdym dowolnym czasie i może mieć bardzo brzemienne w skutkach konsekwencje.

W przypadku oddziaływania na ludzi w środowisku cyfrowym mamy do czynienia głównie z chęcią osiągania skutków psychologicznych, kształtowania postaw, percepcji danego podmiotu, a w konsekwencji wpływania na jego zachowanie. W przypadku oddziaływania na maszyny celem jest zdobycie, zniekształcenie przechowywanej lub przekazywanej w niej informacji, bądź, zakłócenie funkcjonowania samej maszyny. W konsekwencji atakujący może doprowadzić albo do zniszczenia danego urządzenia, albo do sparaliżowania lub całkowitego zatrzymania procesów przez nie realizowanych.

Warto bliżej przyjrzeć się tym dwóm typom walki informacyjnej, zwanym na potrzeby niniejszego artykułu walką „miękką" (oddziaływanie głównie na człowieka) oraz „twardą" (oddziaływanie na maszynę, infrastrukturę) i dokonać analizy wpływu, jaki mogą one wywierać na bezpieczeństwo

[3] Dla uproszczenia, informacja i sygnał będą od tego momentu traktowane jako synonimy.

międzynarodowe. Pozwoli to także stwierdzić, czy o cyberprzestrzeni możemy mówić w kategoriach geopolitycznych.

Miękka walka informacyjna prowadzona w cyberprzestrzeni

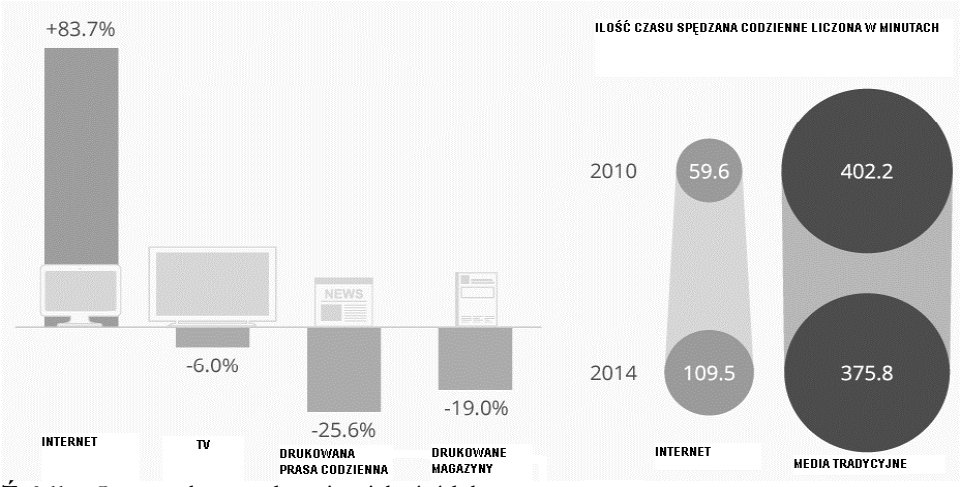
Pojawienie się mediów, najpierw drukowanych, a następnie radia i telewizji, zrewolucjonizowało funkcjonowanie społeczeństw. Ludzie kształtują swoją opinie, wybory, decyzje bardzo często pod wpływem informacji zaczerpniętych z mediów. Owe decyzje, wybory i opinie dotyczą bardzo różnorodnych sfer funkcjonowania człowieka. Począwszy od decyzji konsumenckich, po te polityczne. Media mają wpływ na obywateli, ci zaś w pośredni i bezpośredni sposób na decydentów – zarówno poprzez manifestowanie swojej woli (demonstracje, strajki, referenda) jak i w procesie wyborczym.

W okresie dominacji radia, telewizji i prasy drukowanej, przekaz z nich płynący zależał od ich właścicieli. Nadawane komunikaty były jednostronne, odbiorca raczej biernie przyjmował przekazywane treści. Internet zrewolucjonizował ten sposób komunikacji. Przede wszystkim pozwolił on każdemu, kto ma dostęp do Internetu i komputera, na stworzenie własnego medium, które docierać może do wielu odbiorców. Nie trzeba być dzisiaj pracownikiem ani właścicielem radia lub telewizji, aby docierać ze swoimi treściami do szerokiego grona odbiorców. Dzięki blogom, mediom społecznościowym, portalom tematycznym, można wpływać na innych, kreować poglądy, wymieniać się informacjami. Dodatkowo, komunikacja przestała być jednostronna. Internet daje możliwości wymiany komunikatów między odbiorcą i nadawcą (Goban-Klas, Sienkiewicz 1999, s. 29). Komunikacja jest dynamiczna i treść pod jej wpływem może ulegać zmianie.

Popularność Internetu jako medium komunikacyjnego stale rośnie, degradując inne formy komunikacji. Pokazują to badania i statystyki (Rys. 1). Internet to medium o olbrzymim i rosnącym potencjale, który wykorzystywany jest także przez tych, którzy prowadzą „miękką" walkę informacyjną, zorientowaną na realizację określonych celów politycznych. Internet dał możliwość psychologicznego oddziaływania na innych, jak żadne wcześniej medium. Przykładów jest wiele i są różnorodne.

W trakcie trwania tak zwanej Arabskiej Wiosny, po raz pierwszy, w sposób bardzo wyraźny, dostrzeżono jak wielką rolę w funkcjonowaniu określonych grup społecznych, w przebiegu ruchów politycznych, odgrywają media społecznościowe. Wydarzenia z końca pierwszej dekady XXI wieku, jakie miały miejsce między innymi w Tunezji, Iranie, Egipcie nazywane były „twitterowymi rewolucjami". W kontekście tych wydarzeń media społecznościowe pełniły funkcję logistyczną i mobilizacyjną. Pozwalały komunikować się na bieżąco, organizować protesty, zachęcać do udziału w nich. Ich rola w rozwoju wypadków była bardzo znacząca.

Rys. 1. Zmiany ilości czasu przeznaczanego na korzystanie z mediów w Polsce w okresie 2010-2014



Źródło: Oprac. wł. na podstawie wielu źródeł.

Inny wymiar wykorzystania przestrzeni cyfrowej do prowadzenia walki informacyjnej polegającej na osiąganiu efektu psychologicznego można zaobserwować w kontekście konfliktu na Ukrainie. Jest on nazywany konfliktem hybrydowym, czyli łączącym różne formy oddziaływania na siebie skonfliktowanych stron (Wasiuta 2016). Obok działań zbrojnych, obserwować można takie działania jak dywersja, manipulacja, dezinformacja, presja gospodarcza, wzmożone działania dyplomatyczne itd. Działania konwencjonalne uzupełniane są przez inne formy prowadzenia konfliktu. I w tym arsenale, coraz bardziej istotną rolę odgrywa cyberprzestrzeń. Konflikt na Ukrainie wyraźnie pokazał jak bardzo Internet stał się przestrzenią, gdzie w zmasowany sposób dochodzi do starcia między ideologiami. Informacje są manipulowane, zniekształcane, w końcu usilnie promowane. Bardzo specyficznym przykładem tych działań jest aktywność w sieci prowadzona przez t.zw. trolle internetowe – osoby, które w zmasowany sposób zarzucają Internet stronniczymi, często agresywnymi komentarzami i opiniami wspierającymi określoną politykę, czy wizję świata. Ponieważ w sieci może pisać każdy, bardzo trudno weryfikować wszystkie informacje (m.in. ze względu na ich ilość). Sieć daje też względne bezpieczeństwo - bardzo łatwo unikać odpowiedzialności za prezentowane treści. W końcu liczba odbiorców może być naprawdę duża, a przez to efekt działań bardzo wymierny. Działania takie mogą na masową skalę kreować nastroje społeczne, prowadzić do określonych działań mających skutki polityczne, do podziałów i konfliktów wewnętrznych, a nawet międzynarodowych. Jest to zatem realne i coraz częściej stosowane narzędzie oddziaływania.

Coraz więcej podmiotów dostrzega ten problem na poziomie strategicznym, kreując określone dokumenty (strategie, doktryny) dedykowane (lub w części poświęcone) „miękkiej" walce informacyjnej, także prowadzonej w świecie cyfrowym. Przykładem może być tutaj choćby dokument Federacji Rosyjskiej z 1997 roku zatytułowany *Plan Bezpieczeństwa Narodowego Federacji Rosyjskiej* gdzie jasno wskazuje się, że interesy narodowe można realizować przy wykorzystaniu przestrzeni informacyjnej. Dokument ten wskazuje, że właśnie z tego obszaru płynie duże zagrożenie dla funkcjonowania Federacji[4].

Przykładem państwa, które także dostrzegło rolę i znaczenie informacji, także tej wykorzystywanej w cyberprzestrzeni jest Polska. W 2015 roku Biuro Bezpieczeństwa Narodowego opracowało dokument znany jako *Doktryna Bezpieczeństwa Informacyjnego RP - Projekt*, który poświęcony został między innymi zagrożeniom płynącym z prowadzenia walki informacyjnej w cyberprzestrzeni[5]. Powstawanie podobnych dokumentów, świadczy o tym, że informacja stała się bardzo istotnym orężem budowania pozycji na arenie międzynarodowej i znajduje się w obszarze zainteresowania najważniejszych decydentów.

Analizując możliwości wykorzystania cyberprzestrzeni do prowadzenia walki informacyjnej, dostrzec należy także coraz poważniejsze zagrożenie płynące ze strony działalności terrorystów w Internecie. Sieć coraz bardziej intensywnie wykorzystywana jest do prowadzenia działań mających na celu szerzenie ideologii jakiej hołdują terroryści, promocji ich celów, ale także zastraszaniu odbiorców. Promowanie wizji świata ma doprowadzić między innymi do pozyskiwania nowych zwolenników, czy nawet rekrutów. Tak zwane Państwo Islamskie jest niezwykle aktywne właśnie na tym polu. Z drugiej strony Internet dał możliwość dużo większego zastraszania społeczności międzynarodowej i multiplikowania skutków działań podejmowanych przez terrorystów, które mają na celu wywołanie paniki wśród społeczeństw. Publikowanie on-line filmów z bestialskich egzekucji ma na celu wywołanie efektu psychologicznego wśród jak największej liczby odbiorców. To z kolei ma przełożyć się na osiągnięcie większej uległości wśród zastraszonych społeczeństw i określonego ich oddziaływania na polityków. Należy się spodziewać, że zjawisko to będzie się potęgować i będzie narastającym problemem dla całej społeczności międzynarodowej.

Kolejnym obszarem miękkiego wykorzystania cyberprzestrzeni w prowadzeniu walki informacyjnej, które ma duże znaczenie z punktu widzenia bezpieczeństwa, jest prowadzenie działalności szpiegowskiej. Dotyczy to zarówno państw jak i podmiotów niepaństwowych. Jak zostało powiedziane coraz większa ilość wrażliwych informacji jest gromadzona, przesyłana i

---

[4] *Russian Federation National Security Blueprint*, 1997, http://www.fas.org/nuke/guide/russia/doctrine/ blueprint.html, (dostęp: 03.02.2016).

[5] Biuro Bezpieczeństwa Narodowego, *Doktryna Bezpieczeństwa Informacyjnego - Projekt*, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf, (01.02.2016).

przetwarzana za pomocą systemów teleinformatycznych. Są to informacje ważne zarówno z punktu widzenia poszczególnych podmiotów gospodarczych (umowy, biznesplany, tajemnice handlowe), jak i informacje ważne z punktu widzenia bezpieczeństwa narodowego (tajemnice wojskowe, strategiczne informacje polityczne itd.). Włamując się do systemów teleinformatycznych poszczególnych firm jak i podmiotów publicznych można otrzymać dostęp do informacji, mających olbrzymią wartość. Za ich pomocą można wpływać na kształt wydarzeń międzynarodowych, można kreować je w określony, świadomy sposób. Skutki takich działań mogą być poważne, a ich skala już teraz jest ogromna.

W 2014 roku firma Symantec ujawniła działania grupy cyberprzestępców o nazwie Dragonfly, która przynajmniej od 2013 roku prowadziła działania cyberszpiegowskie nakierowane między innymi na firmy z polskiego sektora energetycznego. Także raport innej firmy Fireeye zatytułowany *APT28: A Window Into Russia's Cyber Espionage Operations?* opisuje działania grupy, która przez wiele lat prowadziła działania szpiegowskie nakierowane szczególnie na organizacje międzynarodowe, podmioty państwowe, w tym rząd polski[6].

Przykładem podobnego działania, którego z kolei celem padł polski resort obrony, to działania ujawnione przez generała Krzysztofa Bondaryka. Były szef ABW i Narodowego Centrum Kryptologii, w jednym z artykułów przekazał informacje o tym, że w wyniku działań hakerów skradzionych zostało kilkaset tysięcy maili z resortu obrony. Według tych informacji pierwsze ślady wrogich działań pojawiły się w 2009 roku, niewykluczone, że przestępcy działali już od 2006 roku. Udało im się prowadzić działania niepostrzeżenie aż do 2014 roku (Bondaryk 2015). Ogrom informacji jak i długość trwania ataku pokazuje skalę problemu. Nie jest to jednak wyłącznie polski problem. Badania pokazują, że średnio taka wroga, niezauważona aktywność w sieci trwa około 205 dni, zanim ktoś dostrzeże nieprawidłowości[7]. Można wyobrazić sobie jak wielką przewagę informacyjną w wyniku tych działań zbudować może agresor.

Należy ponadto pamiętać, że cyberprzestrzeń zwiększyła także możliwości budowania wpływu przez promocję „pozytywnego" przekazu. Państwa promują swoje wartości, swój wizerunek za pomocą sieci. Ma to na celu wywieranie wpływu na inne społeczeństwa, tak aby podejmowały one decyzje pożądane z punktu widzenia oddziałującego podmiotu. Jest to budowanie znanej z prac Josepha Nye'a „miękkiej siły" (soft power). Ważnym elementem, który tutaj warto szczególnie podkreślić jest to, że Internet, poprzez swoją dostępność i „przyjazność" w użyciu, szczególnie wśród młodszych użytkowników, jest narzędziem, które angażuje do budowania wizerunku całe

[6] Fireeye, *APT28: A Window Into Russia's Cyber Espionage Operations?,* https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html, (dostęp: 02.02.2016).

[7] Fireeye, *M-Trends 2015*, https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf, (dostęp: 02.02.2016).

społeczeństwa. Osiąganie celów wynikających ze strategii „miękkiej siły" jest z kolei najlepsze wtedy, gdy jest ona wiarygodna. Zaangażowanie społeczne, prawdziwa chęć zwyczajnych obywateli do włączania się w prowadzenie działań, zawsze taką wiarygodność zwiększa. W ten sposób jest to kolejna metoda oddziaływania międzynarodowego, gdzie informacja i cyberprzestrzeń odgrywają pierwszoplanową rolę.

Twarda walka prowadzona w cyberprzestrzeni

Opisane powyżej działania związane były bądź z nielegalnym pozyskaniem dostępu do informacji, bądź z uzyskiwaniem za pomocą informacji (także zmanipulowanej) wpływu na percepcję adresata. Realizacja interesów danego podmiotu odbywała się przede wszystkim przez zmianę zachowań drugiej strony (pod wpływem informacji), lub poprzez uzyskanie takich informacji o przeciwniku, które pozwalają na jego pokonanie, bądź uzyskanie nad nim przewagi. W przypadku prowadzenia „twardej" walki, dochodzi do takiego oddziaływania za pomocą narzędzi teleinformatycznych na systemy informatyczne, że w konsekwencji mamy do czynienia ze zniszczeniami fizycznymi, lub z paraliżem funkcjonowania pewnych procesów, usług itd. Są to najbardziej poważne działania jakie mogą być prowadzone w przestrzeni informacyjnej.

Jednym z elementów mocno narażonych na ataki cyfrowe, ważnych z punktu widzenia bezpieczeństwa międzynarodowego, jest infrastruktura krytyczna. Obejmuje ona usługi, obiekty, systemy, które warunkują bezpieczne i stabilne funkcjonowanie państwa. Ich zniszczenie może mieć bardzo negatywne konsekwencje dla gospodarki, bezpieczeństwa wewnętrznego czy nawet życia poszczególnych osób. Infrastruktura krytyczna najczęściej wyznaczana jest w takich sektorach jak sektor energetyczny, transportowy, sektor zdrowia, czy sektor chemiczny. Funkcjonowanie tych infrastruktur jest obecnie uzależnione od prawidłowego działania systemów teleinformatycznych. Co więcej, w ramach działania infrastruktury krytycznej, systemy teleinformatyczne są bardzo często odpowiedzialne za sterowanie procesami przemysłowymi. Oznacza to, że zakłócenie pracy systemów informatycznych może doprowadzić do zakłóceń w funkcjonowaniu elektrowni, szpitali czy systemów kontroli ruchu lotniczego. Skutkiem może być w najgorszym scenariuszu katastrofa prowadząca do śmiertelnych ofiar, zanieczyszczeń środowiska, jak też olbrzymie straty finansowe. Funkcjonowanie całego państwa może być utrudnione, a nawet zagrożone. Można zatem, wykorzystując dostęp do Internetu, wywołać poważne skutki polityczne.

Do niedawna brakowało przykładów w których podobne ataki byłyby zakończone „sukcesem" – czyli rzeczywistym zakłóceniem funkcjonowania jakiegoś podmiotu. Nie jest bowiem łatwo dokonać, aż tak skomplikowanego, poważnego ataku. Pierwszym szeroko opisanym atakiem, który przyniósł fizyczne szkody, był atak dokonany z wykorzystaniem wirusa Stuxnet. W

konsekwencji zniszczone zostały wirówki do wzbogacania uranu, a tym samym sparaliżowany został program nuklearny Iranu. W wyniku działania w cyberprzestrzeni, wpłynięto na funkcjonowanie konkretnego podmiotu politycznego i to w dodatku w bardzo newralgicznej sferze. Innym przykładem cyberataku na energetykę, który miał miejsce w 2015 roku, był *blackout* w Turcji. Pozbawił on prądu mieszkańców bardzo wielu miast.

Atak na infrastrukturę krytyczną, może nie być działaniem punktowym, może stanowić element wojny hybrydowej. Sytuację taką obserwujemy aktualnie Ukrainie. Na początku 2016 roku świat obiegła informacja mówiąca, że w wyniku ataku hakerów, udało się wyłączyć ukraińską elektrownię w Zaporożu. W wyniku awarii, na kilka godzin około 700 000 gospodarstw domowych utraciło dostęp do prądu. Eksperci prowadzą badania i analizy mające na celu zbadanie, kto stoi za atakiem. Podejrzenia padają na hakerów działających na usługach władz rosyjskich. Władze ukraińskie oficjalnie oskarżyły Rosjan o spowodowanie ataków. Wydaje się, że taki rodzaj prowadzenia konfliktu, będący uzupełnieniem działań konwencjonalnych będzie coraz częściej obserwowanym zjawiskiem. Inne przykłady wybranych cyberataków na infrastrukturę krytyczną podsumowuje poniższe zestawienie (Tab. 1).

Społeczność międzynarodowa coraz wyraźniej dostrzega niebezpieczeństwa jakie grożą stabilności infrastruktury krytycznej ze strony ataków prowadzonych w cyberprzestrzeni i skutki jakie mogą za tym iść. Dlatego podejmowane są próby działań mających na celu wspólne przeciwstawienie się tego typu zagrożeniom. Jedną z pierwszych prób szukania międzynarodowego porozumienia było forum Grupy Rządowych Ekspertów (Governmental Group of Experts) działającej w ramach ONZ. W ostatnim raporcie przyjętym przez Grupę, kwestia ochrony infrastruktury krytycznej stała się jednym z kluczowych elementów. Celem prac podjętych przez ekspertów było sformułowanie programu działań, które zmniejszą zagrożenie dla infrastruktury krytycznej.

Infrastruktura krytyczna może być jednak rozumiana znacznie szerzej, nie tylko jako infrastruktura należąca do konkretnego państwa. W kontekście Internetu, umownie można mówić o globalnej infrastrukturze krytycznej, czyli urządzeniach i sieciach umożliwiających światową komunikację Internetową. Poważne ich uszkodzenie może doprowadzić do skutków odczuwalnych globalnie, mających wpływ nawet na całą społeczność międzynarodową.

Jednym z najbardziej newralgicznych elementów globalnej infrastruktury internetowej są światłowody płynące po dnach oceanów. Używane są one do przekazywania 99% transkontynentalnego ruchu internetowego. Skutki potencjalnych, długotrwałych uszkodzeń światłowodów mogą mieć tragiczne konsekwencje. Dobrze ilustruje to wydarzenie jakie miało miejsce w 2008 roku. W ciągu zaledwie sekund, w wyniku awarii światłowodów, Egipt stracił 70% swojego dostępu do Internetu a India 50-60%, podczas gdy w Pakistanie

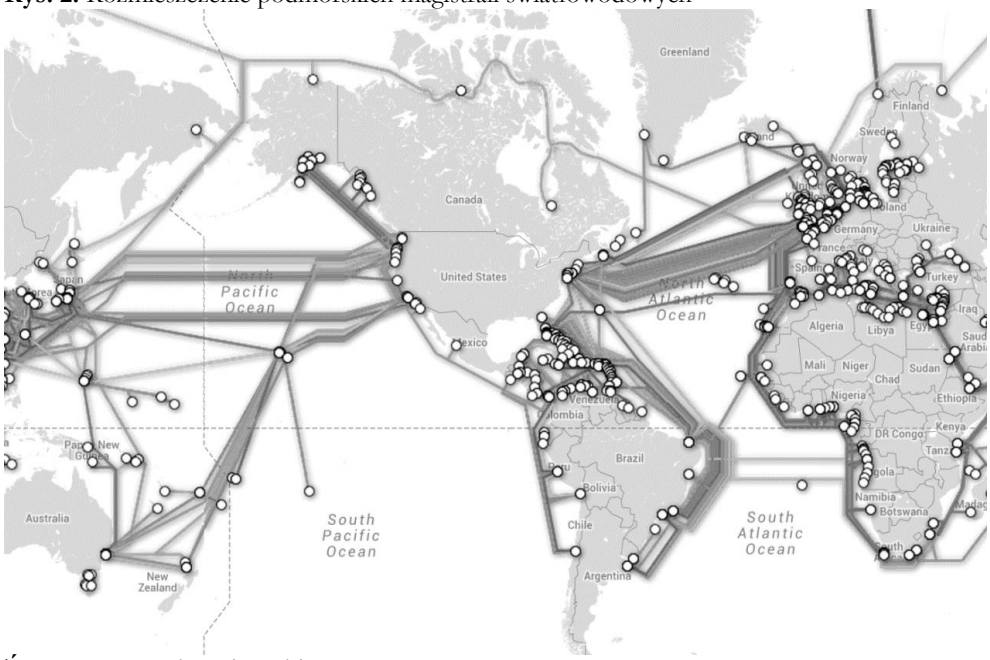
Tab. 1. Przykłady cyberataków na infrastrukturę krytyczną

CYBERATAK	CZAS, MIEJSCE	SEKTOR	OPIS
Worcester Air Traffic Communications Attack	1997, Stany Zjednoczone	Transport lotniczy	Atakujący doprowadził do wyłączenia linii telefonicznych obsługujących wieżę kontrolną, służby ochrony lotniska, lotniskowej straży pożarnej, służby pogodowej. Również unieruchomiony został system oświetlenia pasa startowego.
System dostawy wody pitnej	1999, Australia	Dostawa wody	Były pracownik firmy doprowadził do dezaktywacji obsługiwanego drogą radiową systemu alarmowego, co w konsekwencji wprowadziło zakłócenia w dostawie pitnej wody, w tym jej zanieczyszczenie.
System sygnalizacji kolei CSX	2003, Stany Zjednoczone	Transport kolejowy	Robak internetowy SoBig zainfekował system komputerowy obsługujący ruch kolejowy kompanii CSX, obsługującej 23 stany amerykańskie. Awaria spowodowała odwołania pociągów i opóźnienia w transporcie kolejowym.
Zanik dostawy prądu w pn.-wsch. części Ameryki Północnej	2003, Stany Zjednoczone, Kanada	Dostawa energii elektrycznej	Pozbawionych prądu zostało około 50 mln osób. Awaria mogła być spowodowana wystąpieniem robaka internetowego Blaster, który mógł zakłócić system alarmujący o awarii. Całkowity koszt strat wyniósł od 4 do 10 mld dolarów amerykańskich.
System filtracji wody	2006, Stany Zjednoczone	Dostawa wody	Atakujący przejął kontrolę nad głównym komputerem zarządzającym systemem filtracji wody. Używał go do rozsyłania spamu oraz przetrzymywania pirackiego oprogramowania. Wcześniej włamał się na podłączony do Internetu komputer pracownika firmy obsługującej system, a następnie w sposób zdalny zainstalował wirusa i oprogramowanie szpiegujące na głównym serwerze obsługującym system filtracji
Wirus Stuxnet	2010, Iran	Energia atomowa	Atak na systemy obsługujące irańskie elektrownie atomowe; spowodował poważne kłopoty w funkcjonowaniu elektrowni.

Źródło: Rządowe Centrum Bezpieczeństwa, 2013, *Narodowy Program Ochrony Infrastruktury krytycznej*, s. 49-50.

dostępu do sieci nie miało 12 milionów ludzi, a w Arabii Saudyjskiej 4,7 miliona. Szacuje się, że w ciągu 24 godzin awaria przyniosła straty w wysokości 64 milionów dolarów[8]. Choć awaria ta była najpewniej spowodowana przyczynami naturalnymi lub wypadkiem, pokazuje to jak wielki potencjał miałyby celowe działania, zmierzające do zaburzenia funkcjonowania światłowodów. Jest to jedno z potencjalnych zagrożeń płynących choćby ze strony organizacji terrorystycznych. Poważne uszkodzenie infrastruktury Internetu, mogłoby doprowadzić do globalnych problemów gospodarczych. Należy podkreślić, że wiele z kluczowych światłowodów przebiega w pobliżu regionów politycznie niestabilnych (Rys. 2).

Rys. 2. Rozmieszczenie podmorskich magistrali światłowodowych



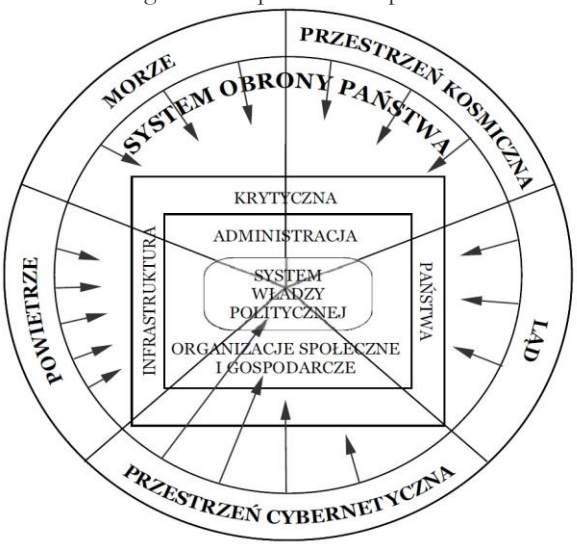
Źródło: www.submarinecablemap.com

Wrogie działania płynące z cyberprzestrzeni, których celem jest infrastruktura krytyczna (państwowa lub też globalna), to nie jedyne „twarde" sposoby wykorzystania środków cyfrowych w ramach działań mających geopolityczne skutki. Cyberprzestrzeń warunkuje także działania prowadzone przez siły zbrojne poszczególnych państw, co oznacza, że cyberprzestrzeń przenika, najbardziej tradycyjne zasoby, kluczowe z punktu widzenia perspektywy geopolitycznej. Współcześnie wojska komunikują się, walczą ze sobą, rozpoznają pole walki przy wykorzystaniu narzędzi cyfrowych. Szczególnie

[8] Gady F., *Undersea Cables: The Achilles Heel of our Economies*, http://www.huffingtonpost.com/franzstefan-gady/undersea-cables-the-achil_b_799808.html, (dostęp: 03.02.2016).

widoczne jest coraz częstsze rozbudowywanie arsenałów „cyfrowej broni" umożliwiającej prowadzenie ofensywnych działań nakierowanych na przeciwnika. Zatem w cyberprzestrzeni państwa widzą kolejną domenę, gdzie prowadzone mogą być konflikty (Rys. 3).

Rys. 3. Przestrzeń zagrożeń bezpieczeństwa państwa



Źródło: Sienkiewicz, Świeboda 2006, s. 58 (za J.A. Warden 1995, s. 47).

Powszechnie wiadome jest, że wojska stosujące nowoczesne rozwiązania teleinformatyczne są dużo bardziej efektywne, lepiej radzą sobie na polu walki. Z drugiej strony podmioty stosujące rozwiązania oparte na nowoczesnych technologiach muszą coraz mocniej dbać o bezpieczeństwo. Jak pisze R. Drozd (2015), „uwypukla się wiodącą rolę cyberprzestrzeni w budowaniu zdolności bojowych (wyposażenie platform bojowych w nowoczesne technologie), jej niekwestionowane znaczenie w integrowaniu poszczególnych uczestników działań zbrojnych (wojska lądowe, siły powietrzne, marynarka wojenna i wojska specjalne oraz w budowaniu międzynarodowych relacji wojskowych i koalicji (NATO, sojusze dwustronne, koalicje regionalne.

Z punktu widzenia ofensywnego wykorzystania cyberprzestrzeni na polu walki, warto zauważyć, że ma ono miejsce szczególnie często w pierwszej fazie konfliktu zbrojnego i jest prowadzone w celu wsparcia działań konwencjonalnych, ułatwienia ich prowadzenia oraz zmultiplikowania ich efektów. Ilustracją takiej sytuacji jest wydarzenie jakie miało miejsce w 2007 roku, kiedy dzięki użyciu narzędzi cyfrowych Izraelczycy zmanipulowali i zneutralizowali działanie systemu obrony powietrznej Syrii. Udało się przeprowadzić skuteczny atak na syryjskie radary, które nie wykryły izraelskich samolotów. Dzięki temu wojsko izraelskie, było w stanie dokonać ataku i

zbombardować określone wcześniej cele praktycznie bez żadnej reakcji strony przeciwnej[9].

Rozwój cyberprzestrzeni doprowadził do pewnego paradoksu. Z jednej strony państwa lepiej ztechnologizowane są w stanie prowadzić bardziej zaawansowane działania z wykorzystaniem narzędzi teleinformatycznych. Multiplikowana jest ich siła i możliwości, szczególnie w sieciocentrycznym środowisku, gdzie informacja może stanowić warunek osiągania przewagi i sukcesu. Z drugiej jednak strony, są one bardziej narażone na skuteczne cyberataki. Strona słabiej zdigitalizowana może być wręcz bardziej bezpieczna. Daje to także możliwości oddziaływania na podmioty państwowe, podmiotom niepaństwowym. Wcześniej nie miały one wystarczających sił i środków, aby realnie, wrogo oddziaływać na całe państwa. Teraz, w wyniku rozwoju środków cyfrowych, takie możliwości okazały się realne.

Cyberprzestrzeń na stałe wpisała się w środowisko funkcjonowania sił zbrojnych i należy się spodziewać, że będzie coraz mocniej wykorzystywana do celów militarnych. Jest to czynnik istotnie wpływający na działania poszczególnych państw, bardzo często zmieniający nawet układ sił.

Geopolityka a cyberbezpieczeństwo

Powyżej opisane zostały przykłady, jak cyberprzestrzeń może zostać wykorzystana do prowadzenia działań mających wpływ na poszczególne podmioty, państwa a w konsekwencji całą społeczność międzynarodową. Kluczowi gracze stanęli w obliczu wielu całkiem nowych zagrożeń, które zmieniają dynamikę relacji międzynarodowych i wymagają stosowania zupełnie odmiennych narzędzi i działań. Zmodyfikowane zostały stare koncepcje, takie jak walka asymetryczna, działania terrorystyczne, ale także pojawiły się zupełnie nowe pojęcia jak prowadzenie działań wojennych w cyberprzestrzeni.

Cyberprzestrzeń w tak istotny sposób wpłynęła na funkcjonowanie współczesnych państw, że musi być brana pod uwagę także w kontekście dokonywania analiz strategicznych i geopolitycznych. I choć jej podstawowe cechy sprawiają, że w pierwszej ocenie wydawać by się mogło, że cyberprzestrzeń jest odseparowanym od geopolityki zagadnieniem, to bardziej zaawansowana analiza pokazuje, że byłaby to błędna ocena. Stratedzy, planiści, myśląc o realizacji działań poszczególnych państw, analizując zagrożenia mające wpływ nawet na sytuację geopolityczną, muszą brać pod uwagę nowe, cyfrowe środowisko funkcjonowania współczesnych podmiotów.

Przede wszystkim cyberprzestrzeń jest obszarem, w którym realizuje się coraz więcej interesów poszczególnych aktorów, w tym państw narodowych. Działania prowadzone w cyberprzestrzeni mogą skutecznie wpływać na

[9] Page L., *Israeli sky-hack switched off Syrian radars countrywide*, http://www.theregister.co.uk/2007/11/22/israel_air_raid_syria_hack_network_vuln_intrusion / (04.02.2016).

stabilność funkcjonowania państwa, na kierunki i decyzje polityczne. Mogą mieć poważne konsekwencje dla sytuacji geopolitycznej poszczególnych graczy. Cyberprzestrzeń wpływa także na zasoby konwencjonalne, tradycyjnie używane do realizowania poszczególnych działań przez rozmaitych aktorów (państwowych i niepaństwowych). Narzędzia teleinformatyczne mogą na przykład multiplikować efekty działań militarnych, czy też mogą znacząco wpływać na działania związane z obronnością.

Środowisko cyfrowe zmieniło dotychczasowe zasady gry na szachownicy geopolitycznej. Przykładem może być choćby to, że dzięki działaniom prowadzonym w cyberprzestrzeni zmianie ulega definicja siły i relacje między graczami. Wysoce rozwinięte kraje, które w porównywaniu klasycznych potencjałów są niedoścignione przez mniej zaawansowane podmioty, z uwagi na uzależnienie od technologii, stają się jednocześnie bardziej wrażliwe. Pojawiające się wrażliwości wykorzystać mogą relatywnie łatwo i skutecznie aktorzy, którzy w standardowej rywalizacji nie mieliby szans. Zarówno aktorzy państwowi jak i niepaństwowi. Ci ostatni zyskali narzędzia i możliwości do prowadzenia działań mających wpływ na globalną sytuację. Analiza uzależnienia światowej sieci od relatywnie łatwej do uszkodzenia infrastruktury pokazuje przykładowe zagrożenie jakie może mieć miejsce.

Wszystko to wykazuje, że narzędzia cyfrowe wprowadziły ludzkość w funkcjonowanie w całkiem nowym środowisku, które wpływa na relacje międzynarodowe, na działania poszczególnych graczy i ich pozycje na arenie międzynarodowej. Choć geopolityka w swych fundamentach zakorzeniona jest w czynnikach bardziej „twardych" takich jak dostęp do energii, wielkość terytorium, uzbrojenie, siła militarna, to aby realnie oceniać współczesny świat, należy do tej klasycznej układanki czynników włączyć działania prowadzone w cyberprzestrzeni. Przenikają one bowiem w chwili obecnej wszystkie inne znane obszary funkcjonowania człowieka. Właśnie dlatego coraz bardziej istotne staje się podejście mówiące, że „współczesna geopolityka, która stara się stworzyć wielowymiarową analizę świata, nie ogranicza się do powielania tradycyjnych koncepcji badawczych i w coraz większym stopniu wychodzi poza tradycyjne, geograficzne aspekty analiz geopolitycznych (morze, ląd, powietrze, kosmos) (Potulski 2010, s. 106).

Zajmując się geopolityką, badaniem funkcjonowania środowiska międzynarodowego, należy brać pod uwagę ten nowy czynnik. Tylko przy wnikliwym analizowaniu potencjału jaki daje cyberprzestrzeń, będzie możliwe zrozumienie wszystkich czynników wpływających na aktywność podmiotów politycznych. Dzięki temu też w pełni będzie można dokonywać ocen i podejmować określone działania w odniesieniu do zapewniania bezpieczeństwa międzynarodowego, jak i bezpieczeństwa poszczególnych państw.

Literatura

Bondaryk, K., 2015, *MON bezbronne w cyberprzestrzeni*, Raport: Wojsko – Technika - Obronność, nr 11.

Ciborowski, L., 1999, *Walka informacyjna,* Wydawnictwo ECT, Toruń.

Drozd, R, 2015, *Odczarować cyberprzestrzeń*, Przegląd Sił Zbrojnych, nr 6.

Goban-Klas, T., Sienkiewicz, P., 1999, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Wyd. Fundacji Postępu Telekomunikacji, Kraków.

Lach, Z., Wendt, J. (red.), 2010, *Geopolityka. Elementy teorii, wybrane metody i badania,* Instytut Geopolityki, Częstochowa.

Madej, M., Terlikowski, M., (red.), 2009, *Bezpieczeństwo teleinformatyczne państwa,* PISM, Warszawa.

Narodowy Program Ochrony Infrastruktury Krytycznej, 2013, Rządowe Centrum Bezpieczeństwa, Warszawa.

Potulski, J., 2010, *Wprowadzenie do geopolityki*, Wyd. Uniwersytetu Gdańskiego, Gdańsk.

Sienkiewicz, P., Świeboda, H., 2006, *Niebezpieczna przestrzeń cybernetyczna*, Transformacje, t. 47–50, nr 1–4.

Stalder, F., 2012, *Manuel Castells. Teoria Społeczeństwa sieci*, Wyd. Uniwersytetu Jagiellońskiego, Kraków.

Sykulski, S. L., 2009, *Geopolityka – słownik terminologiczny,* Wyd. Naukowe PWN, Warszawa.

Świątkowska, J., 2012, *Walka informacyjna a bezpieczeństwo międzynarodowe w latach 1990-2011,* Uniwersytet Pedagogiczny im. KEN, Kraków (praca doktorska niepublikowana).

Warden, J. A., 1995, *The Enemy as a System,* Air Power Journal, t. 9, nr 1, s. 47.

Wasiuta, O., 2016, *Geneza pojęcia i zmiany podejścia do wojny hybrydowej w zachodnim dyskursie politycznym i wojskowym*, Przegląd Geopolityczny, 17, s. 26-40.

Wilczyński, P. L., 2010, *Terytorium w myśli strategiczno-wojskowej,* Przegląd Geopolityczny, tom 2.

Wilczyński, W. J., 2016, *Znaczenie geopolityki (artykuł redakcyjny)*, Przegląd Geopolityczny, tom 16, s. 9-14.

Fight against cyber threats as a challenge facing global security

The article is an analysis of the impact of the new kinds of threats coming from cyberspace to contemporary international security and international relations. It also aims to assess whether activities in cyberspace are relevant from the point of view of geopolitical analyzes. The text contains a description of the key risks that result from the transfer of social life in cyberspace.

Key words: Cyberspace, cybersecurity, geopolitics, information warfare, critical infrastructure.