Acta Politica Polonica nr 1/2021 (51) | www.wnus.edu.pl/ap | DOI: 10.18276/ap.2021.51-01 | 5–21

Współczesne zagrożenia cybernetyczne na przykładzie zjawiska cyberwojny. Analiza teoretyczna

MAREK GÓRKA
DR HAB., PROF. PK

ORCID: 0000-0002-6964-1581
Politechnika Koszalińska, Wydział Humanistyczny
e-mail: marek_gorka@wp.pl

Słowa kluczowe: cyberwojna, cyberzagrożenia, polityka cyberbezpieczeństwa

Abstract Po raz pierwszy w historii postęp w obszarze technologii cyfrowych stał się na tyle masowym zjawiskiem, że jest potencjalnie dostępny dla znacznej części populacji na świecie. Pozwala to niemal każdej osobie na rozpowszechnianie przekazów, co oznacza, że wielu ludzi ma możliwości omijania oficjalnych kanałów komunikacji, dyskredytowania i krytykowania sposobu sprawowania władzy w państwie. Kluczowym problemem jest to, że technologia cyfrowa zdominowała funkcjonowanie gospodarki, a także społeczeństwa, a jej powszechne zastosowanie jest również jednym z podstawowych fundamentów współczesnych działań militarnych. Zagrożenia w obszarze cyberprzestrzeni państwa, stają się coraz bardziej złożone, co wynika z tego, że przeciwnikiem mogącym wyrządzić wiele szkód może być zarówno obce i wrogo nastawione państwo jak i organizacje bądź pojedyncze osoby, które są profesjonalne i zdecydowane w swych działaniach.

Contemporary cyber threats on the example of the phenomenon of cyberwarfare. A theoretical analysis

Keywords: cyber warfare, cyber threats, cyber security policy

Abstract For the first time in history, advances in digital technology have become so massive that they are potentially accessible to a significant portion of the world's population. It allows almost any person to disseminate messages, which means that many people have the potential to bypass official channels of communication, to discredit and criticize the way government is run. A key problem is that digital technology dominates the functioning of the economy as well as society, and its widespread use is also one of the basic foundations of modern military operations. Threats in the area of the state's cyberspace are becoming more and more complex, because the adversary that can cause a lot of damage can be a foreign and hostile state as well as organizations or individuals who are professional and determined in their actions.

Wprowadzenie

Postęp technologiczno-komunikacyjny jest jednym z najważniejszych czynników, który przyczynił się do zmiany w prowadzeniu polityki państwa, a także funkcjonowania gospodarki i społeczeństwa. Główny element tej ewolucji polega na odejściu od scentralizowanego modelu w kierunku decentralizacji, co wynika z pojawiania się coraz to nowszych podmiotów determinujących rzeczywistość poprzez cyberprzestrzeń. Obecnie każda z instytucji publicznych, w większym lub mniejszym stopniu, obecna jest w cyberprzestrzeni.

Rozwój cybertechnologii stał się czynnikiem wielu zmian w prawie każdym aspekcie funkcjonowania państwa. Internet jest głównym czynnikiem globalnej rewolucji. Wiele urządzeń w codziennym życiu ma możliwość łączenia się z internetem – od telefonów, tabletów, telewizorów, odtwarzaczy mp3, po komputery stacjonarne. Dzięki technologiom jest stały dostęp do informacji – począwszy od naszych zainteresowań, nawyków, zawodu, aż po nazwy użytkowników i hasła do kont bankowych. Internet jest także narzędziem zapewniającym wiele pozytywnych możliwości rozwoju osób i organizacji, ale przyniósł jednocześnie wiele zagrożeń dla bezpieczeństwa instytucji państwa, organizacji z sektora prywatnego, a także zwykłych obywateli. Innymi słowy, proces globalizacji gospodarki, przeprowadzany w wyniku stosowania nowych technologii informacyjno-komunikacyjnych, nie tylko stwarza szanse na opłacalny rozwój w wielu dziedzinach współczesnej gospodarki, ale jednocześnie inicjuje pojawianie się nowych form rywalizacji politycznej i prowadzenia konfliktów między podmiotami politycznymi (Castells, 1996, s. 77–146). W środkach masowego przekazu bardzo często rozpatruje się wpływ przestępczości internetowej na funkcjonowanie instytucji rządowych i organizacji biznesowych, a także na życie osób prywatnych. Warto zauważyć, że – te wspomniane powyżej – negatywne zjawiska zachodzą zarówno w przestrzeni międzynarodowej, jak i regionalnej oraz lokalnej.

Aspekty badawcze w opisie cyberzagrożeń wobec państwa

Teza o szerokim oddziaływaniu internetu na politykę stanowi punkt wyjścia do analizy tematu dotyczącego aspektów lokalnych i globalnych w polityce bezpieczeństwa. Wpływ internetu na globalną politykę jest dużym wyzwaniem badawczym. Okazuje się bowiem, że trudno udowodnić związki między aktywnością cybernetyczną określonych organizacji a podjętymi decyzjami przez środowiska rządowe, które byłyby konsekwencją określonych zjawisk zachodzących w cyberprzestrzeni. Warto zatem pamiętać, że zachowania decydentów politycznych mogą być powodowane innymi czynnikami, które są niedostępne dla wiedzy publicznej, a tym samym obszar badawczy jest trudniejszy do analizy. Pojawienie się w życiu codziennym cyberprzestrzeni jeszcze bardziej skomplikowało, już i tak złożoną, interakcję między podmiotami lokalnymi a globalnymi. Technologia informacyjna stworzyła miejsce, w którym zjawiska globalne w różnych swych formach spotykają się z lokalnymi (Fontana, 2017, s. 99–104).

Analiza cyberzagrożeń może pomóc decydentom i analitykom zrozumieć tożsamość, motywacje i zamiary poszczególnych aktorów. Cyberprzestrzeń, podobnie jak środowisko

geopolityczne, podlega różnorodnym naciskom gospodarczym, politycznym i społecznym, dlatego można postawić tezę, że składa się ona z procesów, które wykraczają poza podstawową technologię i wchodzą w zakres zjawisk nauk społecznych.

Chociaż coraz więcej autorów w literaturze poświęca uwagę bezpieczeństwu cybernetycznemu, to jednak wciąż można odczuć potrzebę pogłębionej analizy na temat wpływu cyberbezpieczeństwa na funkcjonowanie państwa. Popularność cybertechnologii oraz powszechny dostęp do niej wraz z anonimowością użytkowników są wymieniane w literaturze przedmiotu jako główne czynniki kształtujące problematyczne zjawiska w cyberprzestrzeni (Aleksandrowicz, Liedel, 2014, s. 9–38; Jędrzejko, Morańska, 2013, s. 37–118).

Wzrost cyberzagrożeń, będących bezpośrednią zapowiedzią możliwych konfliktów, powoduje wiele pytań dotyczących m.in. tego, co sprawia, że rywalizacja polityczna jest tak atrakcyjna? I dlaczego określone podmioty polityczne coraz częściej wybierają wirtualną przestrzeń jako miejsce dokonywania przestępstw? Istnieje kilka czynników, które – przy udzielaniu odpowiedzi na powyższe pytania – można uwzględnić. Przede wszystkim wszechobecność technologii, która ułatwia wielu osobom, instytucjom i organizacjom pozyskanie narzędzi szkodliwego działania. Poza tym sprawcy mogą łatwo uzyskać dostęp do informacji z dowolnego miejsca za pośrednictwem urządzeń cyfrowych. Istnieje ponadto szeroki zakres możliwych przypadków cyberzagrożeń, niezależnie od stopnia profesjonalnej wiedzy technologicznej napastnika.

Ważnym problemem, także w badaniach naukowych, jest brak standardowej definicji cyberzagrożeń. Wielość definicji oraz interpretacji zjawisk mających charakter cybernetyczny powoduje, że trudno przyporządkować określone zdarzenie do opracowanych wcześniej pojęć. Dużym wyzwaniem badawczym jest zrozumienie, jak zjawiska z obszaru polityki, ekonomii, ale także kultury i psychologii wzajemnie się krzyżują i jakie mają konsekwencje na funkcjonowanie społeczeństwa.

Coraz większe znaczenie cyberprzestrzeni od początku XXI wieku wymaga od badaczy analizy zjawisk, które nigdy wcześniej nie istniały w formie cyfrowej. Internet jako szybki i zdecentralizowany środek komunikacji jest wykorzystywany w relacjach międzyludzkich na całym świecie. W niniejszym artykule podjęto próbę odpowiedzi na pytanie dotyczące obecnego stanu bezpieczeństwa cybernetycznego, przedstawiono więc teoretyczne refleksje na temat czynników determinujących rywalizację między państwami. Po drugie, praca stanowi punkt wyjścia do dalszej analizy na temat ewolucji zagrożeń i ich tworzenia poprzez cybertechnologię.

Opracowanie jest także przyczynkiem do rozważań oscylujących wokół pytania – w jaki sposób współczesne państwa funkcjonują w cyberprzestrzeni. Bez wątpienia jest to zadanie dla badaczy z zakresu nauk o polityce, bowiem technologia cyfrowa stała się istotną cechą przestrzeni publicznej XXI wieku. W artykule rozpatrzono jeden z aspektów wpływu rewolucji informacyjnej na szeroko rozumianą politykę, w tym także politykę bezpieczeństwa, poprzez skoncentrowanie się na zjawisku cyberwojny.

Te teoretyczne rozważania mają ogromne znaczenie dla postrzegania natury współczesnych konfliktów, które obok znanych już lądowych, morskich, powietrznych i stratosferycznych obszarów, prowadzone są również w wymiarze cybernetycznym. Można więc stwierdzić,

że to kolejny konflikt w długiej historii technologii wojskowej, który wymusza nowe koncepcje taktyczne i operacyjne. Globalna świadomość cyberwojny znacznie wzrosła w ciągu ostatnich kilku lat i wiele państw przygotowuje się do operacji obronnych i ofensywnych. W tej ewolucji technologicznej, która wiąże się ze zmianami w sferze gospodarczej, społecznej i politycznej, podkreśla się potrzebę zbadania zakresu odpowiedzialności państwa zarówno w sferze polityki wewnętrznej, jak i międzynarodowej.

Natura cyberzagrożeń – poruszana w aspekcie militarnym oraz pozamilitarnym to koncepcja bardzo popularna w debacie publicznej. Pomimo wielowymiarowego znaczenia dla państwa i jego obywateli, polityka bezpieczeństwa cybernetycznego nadal pozostawia wiele możliwości badań i analiz. Wydarzenia polityczne o znaczeniu międzynarodowym bardzo wyraźnie pokazują, że zjawisko hybrydyzacji konfliktów – z wykorzystaniem technologii informatycznych – wpisały się na stałe w sposób zarządzania sprawami zagranicznymi.

Zagrożenia dla państwa i społeczeństwa z powodu dominującej roli cybertechnologii stają się coraz bardziej argumentem przemawiającym za zmianą dotychczasowego modelu polityki bezpieczeństwa. Z tego powodu w artykule pokrótce przedstawiono znaczenie „cyberbezpieczeństwa" dla współczesnego państwa, jednak przede wszystkim skupiono się na militarnym nastawieniu do sfery cyfrowej i technologii informacyjnej.

Artykuł powstał na podstawie przeglądu dotychczasowych analiz i opinii badaczy z zakresu polityki cyberbezpieczeństwa. Punktem wyjścia w artykule jest zatem opinia, że refleksje badawcze mają wartość kształtowania i poszerzania debaty publicznej, a tym samym przyczyniają się do formułowania i tworzenia świadomej polityki na podstawie analiz naukowych, niezależnie od – czasem – sprzecznych stanowisk badawczych. W zamierzeniu podjęta w pracy analiza problemu funkcjonowania polityki bezpieczeństwa cybernetycznego opisuje szanse i słabe punkty powstałe w wyniku interakcji narodów i podmiotów niepaństwowych w cyberprzestrzeni. Ta interakcja jest wyraźna i dotychczas wystarczająco poznana w tradycyjnej, konwencjonalnej przestrzeni, ale w obszarze cybernetycznym wiedza na ten temat jest nadal niewystarczająca i pozostawia duży niedosyt co do zachodzących procesów i zjawisk. Obok więc zaprezentowanej perspektywy komparatystycznej, podjęto próbę usystematyzowania dotychczasowych badań dotyczących współczesnych zagrożeń cybernetycznych, zwłaszcza w obszarze polityki międzynarodowej, aby również lepiej zrozumieć podstawowe cechy domeny internetowej. Z politologicznego punktu widzenia w pracy scharakteryzowano zakres, w jakim istniejące metody analizy stosunków międzynarodowych można przenieść na arenę cybernetyczną i dostosować je w razie potrzeby do domeny cybernetycznej.

Celem artykułu jest więc refleksja nad kluczowymi zagadnieniami dotyczącymi cyberbezpieczeństwa. W zamierzeniu, podjęta w pracy próba opisu zachodzących zjawisk cybernetycznych we współczesnej polityce pozwoli również wskazać różnice pomiędzy tradycyjnym a nowoczesnym prowadzeniem konfliktów międzynarodowych.

Refleksja badawcza w artykule dotyczy kluczowych cech cyberkonfliktu, które stanowią charakterystyczne elementy definicji tego pojęcia. Podjęte w artykule rozważania mogą wywołać dyskusję na temat cyberprzestępczości, która w ostatnich latach wydaje się być poważnym

problemem dla polityki w jej wymiarze lokalnym oraz międzynarodowym. W artykule wskazano także zagrożenia, które mogą być czynnikami inicjującymi zmiany w postrzeganiu polityki cyberbezpieczeństwa przez współczesne państwo.

Podstawą artykułu jest teza, że cyberprzestrzeń jest nową formą przestrzeni publicznej, w której mogą zachodzić spory i konflikty natury społeczno-politycznej oraz militarnej. Jeśli zatem cyberwymiar jest polem dla działań politycznych, to wpływa on również na sposób rywalizacji między uczestnikami na arenie międzynarodowej. Tym samym, wszystkie możliwe cyberzagrożenia mogą kształtować sposób funkcjonowania państwa oraz jego instytucji, a także determinować naturę zawieranych sojuszy i prowadzonych konfliktów.

W ostatnich latach cyberwojna jest powszechnie uznawana, obok terroryzmu, za jedno z największych zagrożeń militarnych (Clarke, Knake, 2015, s. 11). Zaskakujące jest również, jak szybko cyberkonflikty zdominowały dyskurs globalnej polityki bezpieczeństwa. Warto zatem zastanowić się, czy obecnie pojawia się nowe zjawisko konfliktu zbrojnego? Czy przyszłe wojny będą toczone bez rozlewu krwi?

Ważnym wyzwaniem dla współczesnych nauk politycznych jest więc jak najlepsze zrozumienie istoty zagrożeń cybernetycznych, a także analiza wypracowanych przez podmioty polityczne metod obrony przed agresją, na którą szczególnie narażone są demokratyczne społeczeństwa i instytucje.

Wybrane zmiany w polityce bezpieczeństwa państwa

Polityka bezpieczeństwa cybernetycznego jest dość nowym zjawiskiem w obszarze zarządzania sferą publiczną. Każde z państw ma w różnym stopniu rozwiniętą infrastrukturę cyfrową z tego też m.in. powodu proces tworzenia poszczególnych cyberstrategii przez różne rządy przebiega w odmiennym tempie. Odmienność co do interpretacji i postrzegania kwestii bezpieczeństwa cybernetycznego infrastruktury krytycznej odzwierciedlają różne rozwiązania krajowe w państwach członkowskich Unii Europejskiej.

Niektóre rządy (np. Niemcy i Holandia) traktują bezpieczeństwo cybernetyczne jako kwestię bezpieczeństwa wewnętrznego, podczas gdy inne (np. Łotwa i Dania) uważają je za kwestię polityki obrony. Inne państwa (np. Finlandia i Włochy) postrzegają bezpieczeństwo cybernetyczne jako kwestię handlu i komunikacji. Nie brakuje także opinii w gronie europejskich decydentów politycznych, że wszelkie centralne regulacje dotyczące bezpieczeństwa cybernetycznego naruszają suwerenność państwa (Ilves, Evans, Cilluffo, Nadeau, 2016, s. 126–141).

Różnice widoczne są nie tylko na poziomie międzypaństwowym, ale także w rywalizacji między rządami a organizacjami niepaństwowymi (np. hakerzy czy też organizacje terrorystyczne). Zmotywowane grupy, które chcą zaszkodzić lub propagować określone idee, mogą wykorzystać różne zasoby online jako narzędzia do uzyskania zamierzonego celu. Przykładem tego mogą być hakerzy, którzy umieszczają komunikaty na określonych stronach internetowych, aby wyrządzić szkody wizerunkowe lub wyartykułować określony przekaz polityczny lub ideologiczny. Ponieważ w przypadku aktów wandalizmu, agresji i cyberataków na osoby bądź na

infrastrukturę cyfrową, technologia może być używana nie tylko jako środek komunikacji, ale także jako cel, a zatem konieczne staje się określenie motywu działania strony przeciwnej. Wykorzystanie technologii w celu ułatwienia działalności przestępczej zmusza rządy wielu państw (przy udziale odpowiednich służb) nie tylko do działań zapobiegawczych i zwalczających te groźne zjawiska, ale także do zdefiniowania i klasyfikacji tych zagrożeń. Istnieje bowiem wiele czynników ideologicznych, które następnie mogą być powodem stosowania cyberataków.

Bardzo ryzykowną hipotezą, choć wartą odnotowania, jest pogląd, że współczesna polityka międzynarodowa za sprawą cyberprzestrzeni w coraz większym stopniu oderwana jest od geografii. Chociaż powyższy pogląd wykazuje pewnego rodzaju nową tendencję w zakresie geopolityki, to jednak formułowanie stanowczych sądów i przekonań o tym, że geografia przestała odgrywać istotne znaczenie jest tezą postawioną na wyrost. W zrozumieniu problemu egzekwowania prawa w zakresie cyberbezpieczeństwa jest to, że sieć internetowa ma zasięg globalny, co oznacza, że fizyczne granice oraz dystans geograficzny są bez znaczenia w cyberprzestrzeni. Z tego m.in. powodu internet jest niemal idealnym miejscem dla organizacji, których celem są szkodliwe działania.

Współczesny rozwój technologiczny przyczynił się do tego, że granice między państwami tracą na znaczeniu i to samo dotyczy opisowych kategorii związanych z wojną. Obecne konflikty niewiele mają wspólnego z wypowiedzeniem wojny i podpisaniem traktatu pokojowego. Trudno dlatego powiedzieć, czy żyjemy w czasie pokoju, czy wojny. A zatem granice czy też linie oddzielające świat wirtualny od realnego tracą na znaczeniu. Rozwijająca się technologia sprawiła, że większość zadań wojskowych przypisuje się robotom. W takich okolicznościach trudno powiedzieć, jakie są granice odpowiedzialności określonego agresora za atak na przeciwnika.

Obecnie cyberprzestrzeń stawia nowe wyzwania przed służbami zajmującymi się cyberbezpieczeństwem. Globalna natura internetu ułatwia międzynarodowym korporacjom prowadzenie działalności gospodarczej. Stwarza także pokusę do kwestionowania indywidualnych regulacji i kontroli prowadzonych przez państwa narodowe, w wyniku czego perspektywa globalnych sieci przestępczych staje się realną alternatywą dla wielu organizacji (Castells, 1996, s. 21–25). Mimo że internet rewolucjonizuje wymianę handlową oraz przepływ finansów, to to tworzy również nowe zagrożenia. Globalna łączność za pomocą cybertechnologii znacznie ułatwia przestępcom działanie poza granicami państwa w celu prowadzenia nielegalnej działalności. Jest to szczególnie widoczne podczas prowadzenia dochodzeń przez organy ścigania. Okazuje się więc, że przepisy proceduralne, które regulują prowadzenie spraw karnych, mają charakter terytorialny, innymi słowy mają zastosowanie tylko na terytorium państwa, które ogłosiło te przepisy. Badania nad cyberzagrożeniami wymagają często śledzenia i gromadzenia dowodów w więcej niż w jednym państwie, co oczywiście oznacza, że proces ten jest regulowany prawem pochodzącym z wielu obszarów o odmiennej jurysdykcji. Jest to zatem kłopotliwe i prowadzi do nieskuteczności w dochodzeniach dotyczących cyberprzestępczości, ponadto cyberzagrożenia, co do swej formy i zasięgu, szybko ewoluują (Wall, 2008, s. 45–63). Przestępcy są nawet w stanie kierować swoją siecią oraz wysyłaniem e-maili tak, aby przechodziły one przez komputery

innych użytkowników w celu zminimalizowania prawdopodobieństwa identyfikacji prawdziwych sprawców.

Warto odnotować także, że coraz częściej prowadzone są dochodzenia dotyczące przypadków cyberataków, przekraczających granice państwowe. Okazuje się jednak, że niektóre rozwijające się państwa nie mają regulacji prawnych dotyczących nadużyć w cyberprzestrzeni. W takiej sytuacji określone organizacje bądź hakerzy mogą dokonywać przestępstw z minimalnym ryzykiem sankcji prawnych (Brenner, 2009, s. 127–162).

Ewolucja zagrożenia w kontekście rozwoju cybertechnologii

Rosnące i wciąż rozwijające się cyberzagrożenia mogą wpływać na wszystkie segmenty społeczeństwa, w tym osoby prywatne, przedsiębiorstwa, agencje rządowe oraz na inne podmioty publiczne. Kwestia cyberbezpieczeństwa ma i z pewnością będzie mieć ogromny wpływ na instytucje funkcjonujące w przestrzeni społeczno-politycznej na całym świecie. Biorąc pod uwagę zmieniającą się naturę internetu oraz globalny zasięg sieci, a także coraz większą potrzebę zapewnienia informacji społeczeństwu, można zauważyć ustawiczny proces zacierania granic znaczeniowych między dotychczasowymi pojęciami określającymi miejsce i rolę jaką pełnią podmioty w sferze polityki. Wyzwaniem dla rządów krajowych staje się więc opracowanie kompleksowych strategii radzenia sobie z kwestiami związanymi z bezpieczeństwem cybernetycznym. Powszechne jest traktowanie w sformułowanych cyberstrategiach – przez większość państw UE – zjawiska zagrożeń nie tylko w perspektywie systemów rządowych, ale także w ujęciu podmiotów prywatnych, które obecnie w dużym stopniu wspierają działania rządu lub kontrolują funkcjonowanie infrastruktury krytycznej. Zjawisko to stanowi dowód dla powyżej sformułowanej tezy, że instytucje z sektora prywatnego współcześnie kontestują monopol państwa w polityce bezpieczeństwa (Clark, Hakim, 2017, s. 1–18).

Dotychczas popularny był pogląd, że dobrze funkcjonujące państwo stanowi kluczowe wsparcie dla systemu globalnego zarządzania. Choć nadal jest prawdą, że państwa i organizacje polityczne są integralną częścią globalnej polityki, to należy zauważyć, iż w wyniku postępu technologicznego pojawiły się nowe podmioty, których obecność oraz działania determinują globalną politykę. Ważną rolę odgrywa również społeczeństwo obywatelskie, które w pełni (bądź w ograniczonym zakresie) korzysta z podstawowych praw człowieka. Okazuje się więc, że również i obywatele dzięki cyberprzestrzeni mogą być kluczowym podmiotem zabierającym głos w dyskursie politycznym, a tym samym mogą wpływać na wydarzenia w wymiarze lokalnym, regionalnym czy też globalnym (Durch, Larik, Ponzio, 2016, s. 95–112). Jak wspomniano wcześniej, internet jest nowym środowiskiem, w którym obecnie funkcjonują niemal wszystkie agencje rządowe i administracyjne. A każdy przejaw cyberprzestępczości w znacznym stopniu wpływa na jednostki, firmy i bezpieczeństwo narodowe.

Postrzeganie stosunków międzynarodowych i rozumienie strategii wojskowej wywodzi się z doświadczeń XIX i XX wieku, a więc wiąże się z założeniami, że państwa są kompetentnymi podmiotami w polityce światowej, a porozumienia między nimi zmniejsza ryzyko wojny.

To tradycyjne rozumienie polityki szanuje granice narodowe i integralność terytorialną oraz zakłada, że przestępstwa transgraniczne stanowią wyjątki. Niektóre cechy cyberprzestrzeni nie odpowiadają jednak tradycyjnej logice funkcjonowania systemu państwa. Cyberprzestrzeń tworzy pole dla nowych narzędzi prowadzenia konfliktów, tym samym może przyczyniać się do unikania znanych dotychczas modeli prowadzenia działań militarnych (Choucri, Goldsmith, 2012, s. 70–77).

Wiele państw na świecie wciąż tworzy nowe strategie, dzięki którym będzie można chronić bezpieczeństwo narodowe. Kilka wieków temu armaty były szczytem rozwoju technologicznego. Potem pojawiły się lepsze karabiny, czołgi, statki i samoloty z pociskami. Obecnie narzędzia bezpieczeństwa narodowego wydają się pochodzić prosto z *science fiction*. Armia amerykańska jest liderem w rozwoju cybernarzędzi, które pomagają zachować bezpieczeństwo wojsk i zapewniają przewagę taktyczną nad wrogiem. Nowe technologie oferują precyzję w przeprowadzaniu ataku w nieznanej dotąd skali.

Gromadzenie informacji za pomocą sygnałów elektronicznych dalekiego zasięgu, czy też czujników, laserów i innych technologii od dawna stanowi element działań wywiadowczych. Dzięki tym narzędziom wiele rządów może uniknąć wysyłania ludzi do niebezpiecznych regionów w celu zebrania informacji. Postęp technologiczny będzie nadal przyspieszał, a cybertechnologia i jej rosnące wykorzystanie szybko staną się normą. Postęp technologiczny można wykorzystać jako skuteczny sposób na zmniejszenie liczby ofiar, ale zwiększa on zależność państwa od cybernarzędzi i w konsekwencji tworzy asymetryczną lukę. Rozwój technologii doszedł do tego etapu, że możliwa staje się do sformułowania teza, że istnieje możliwość wywołania konfliktu za pomocy internetu (Ventre, 2011, s. 213–230).

Każda innowacja w przemyśle zbrojeniowym wpływa nie tylko na losy wojny, ale i całego świata. Najlepiej ilustruje to przykład niezwykle lekkiego i wytrzymałego AK-47, który przyczynił się do odwrócenia losów wojen w XX wieku. Karabin szturmowy okazał się bronią tak śmiercionośną, prostą w użyciu i niezawodną, że każda pełnosprawna osoba mogła zabrać go na pole walki.

Cyberwojna to kolejny etap w długiej historii technologii wojskowej, który wymusza nowe koncepcje taktyczne i operacyjne. Jest to poważne zagrożenie, wynikające przede wszystkim z łatwego dostępu do komputerów, za pomocą których można spowodować duże szkody.

W konwencjonalnym konflikcie wszystko dzieje się zgodnie z ustalonymi i dobrze znanymi zasadami, a zatem większość działań taktycznych czy też strategicznych jest przewidywalna. Armia lub pocisk przemieszcza się z jednego punktu do drugiego, aby dokonać zniszczeń na terenie wroga. Zwycięzcą jest ten podmiot, który doprowadzi swoje wojska we właściwe miejsce i na czas. Cyberwojna natomiast daje napastnikowi dodatkową przewagę, pojawia się bowiem problem, do kogo strona atakowana powinna adresować odwet czy też kierować przekaz lub z kim powinna prowadzić negocjacje, gdy druga strona nie jest znana?

W tradycyjnym konflikcie określone inicjatywy i reakcje wobec zagrożenia były w jakiś sposób przewidywalne, zawierały bowiem czynnik uzasadniający użycie siły. W przypadku

cyberwojny element niepewności jest o wiele większy, co dotyczy przede wszystkim organizacji i państw międzynarodowych, które muszą ocenić, czy jest to akt wojny, represji, kontrataku itp.

Wojna konwencjonalna polega na przemieszczaniu wojsk i broni z jednej granicy kraju do drugiej. W przypadku cyberkonfliktu takie posunięcia nie są widoczne, a ich celem może być uszkodzenie, zmiana lub selekcja informacji, co w konsekwencji może prowadzić do kształtowania postaw społecznych, począwszy od nękania, szokowania aż po wywoływanie chaosu wśród obywateli państwa.

Dziś już nikt nie wątpi, że technologia w połączeniu z bronią konwencjonalną to skuteczny sposób prowadzący do przewagi w prowadzeniu konfliktu, zwłaszcza w wojnie, w której uczestniczą dwa, wrogie względem siebie, mocarstwa o podobnym rozwoju technologicznym.

Innym zjawiskiem związanym ze współczesnymi konfliktami zbrojnymi jest idea hybrydowości, rozumiana jako nowe podejście w badaniu konfliktów zbrojnych. Jest ona postrzegana jako współistnienie starych i nowych elementów wojen, klasycznych konfliktów zbrojnych i współczesnych wojen, supernowoczesnej technologii wojskowej i klasycznych narzędzi prowadzenia walki. Hybrydowość może obejmować walkę obu stron (państwa, grupy nieformalne, nieregularne ugrupowania zbrojne), przestrzeń konfliktu oraz charakter i sposoby zarządzania konfliktem. Główną cechą hybrydyzacji we współczesnych wojnach jest jednoczesne istnienie dwóch głównych płaszczyzn konfliktu, czyli terytorialnej i wirtualnej. Pierwszy wymiar odnosi się do klasycznego rozumienia państwa lub grup etnicznych mieszkających na stałe na danym terytorium. Drugi wymiar odnosi się do komunikacji w sieci z pominięciem terytoriów promujących wartości, zasady i idee (Gruszczak, 2011, s. 9–17).

Dziś coraz rzadziej podejmowane są próby włamania się do sejfów lub przemieszczania się po korytarzach budynków w celu odkrywania poufnych danych. Złośliwe oprogramowanie (np. trojany) kopiuje i wyprowadza poufne dane lub przejmuje kontrolę nad wybrana instytucją.

Ogromnym zagrożeniem stali się hakerzy, którzy przez uruchomienie zainfekowanego programu w sieci administracji publicznej organizują coś w rodzaju niewidzialnego włamania. W takim przypadku pojedyncza maszyna lub cała sieć nie wykonuje już poleceń swojego prawdziwego właściciela, ale zdalnie jest manipulowana przez intruza.

Szkodliwe programy niszcząc środki komunikacji lub transportu przeciwnika uniemożliwiają mu wykonywanie rozkazów, koordynowanie pracy instytucji państwowych lub pozbawiają instytucji kontaktu z obywatelami, co może prowadzić do podejmowania ryzykownych decyzji. Takie przypadki mogą spowodować m.in. chaos w systemach ratunkowych, lotniskach, dostawach energii, a ostatecznie doprowadzić do katastrof przez łańcuch szkodliwych konsekwencji.

Skala wykorzystania internetu w życiu codziennym stała się jednym z najbardziej niesamowitych zjawisk w historii ludzkości. To nie tylko środek komunikacji, ale także centrum globalnej infrastruktury informacyjnej, która wpływa na kulturę organizacyjną instytucji publicznych. Zjawisko to zmieniło funkcjonowanie każdego elementu życia codziennego, począwszy od standardów komunikacji, transakcji finansowych, a skończywszy na praktyce lekarskiej. Internet stał się więc uniwersalną przestrzenią interakcji społecznych, handlu, uprawiania polityki i prowadzenia określonych działań wpływających na bezpieczeństwo państwa i jego obywateli.

Konflikty aktywizują i wspomagają rozwój ważnych elementów w dziedzinie informacji i komunikacji. Możliwość ich zastosowania na polu bitwy może więc gwarantować sukces militarny (Suissa, 2012, s. 9–30), dlatego przemysł, technologia, kultura, dyplomacja i wojna są objęte tym samym projektem geopolitycznym. Wojna prowadzona za pomocą narzędzi cyfrowych jest więc działaniem obejmującym wszystkie rodzaje przestrzeni publicznej. Za Edwardem Waltzem można stwierdzić, że konflikt ten obejmuje środki podjęte w celu zachowania integralności i ochrony systemu komputerowego przed eksploracją, uszkodzeniem lub zakłóceniem w celu osiągnięcia przewagi informacyjnej (Wlatz, 1998, s. 85).

Cyberwojna – natura zjawiska

Cyberprzestrzeń przyjęło się określać jako „nowe pole bitwy" i w naturalny sposób ten „nowy wymiar konfliktu" stał się celem działań państwa. Taki rozwój sytuacji zmienia relacje między państwami i ich obywatelami, wzmacniając siłę pierwszego kosztem drugiego. Jak nowe domeny cyfrowe zmieniają politykę międzynarodową pozostaje jednak pytaniem otwartym. Oprócz tego istnieje kwestia sporna, która skupia znaczącą uwagę badaczy i analityków, a dotyczy pytania, czy nowa technologia faworyzuje aktorów słabszych czy też silniejszych pod względem militarnym? Z jednej strony wiele środowisk (zwłaszcza w kręgach politycznych) postrzega cyberwojnę jako broń słabych – strategiczny korektor, który wzmacnia mniejsze narody i podmioty niepaństwowe w walce z silniejszymi wrogami. Z drugiej strony, inni (zwłaszcza w środowiskach akademickich) są sceptyczni co do wyrównującego potencjału nowej technologii, którą niektórzy postrzegają jako broń silnych, służącą wzmocnieniu przewagi, jaką cieszą się militarnie lepsi aktorzy względem słabszych przeciwników.

W teorii zmiany zachodzące na podstawie cybertechnologii zakładają istnienie cyberwojny, w której o wyniku konfliktu nie decyduje ani ilość, ani mobilność armii; zamiast tego rząd oraz podległe mu służby, które mają ogromne możliwości manipulowania informacjami, co daje im zdecydowaną przewagę nad pozostałymi podmiotami w przestrzeni publicznej (Arquilla, Ronfeldt, 1993, s. 141).

Współczesne państwo jest bardziej niż kiedykolwiek zależne od komunikacji cyfrowej. Bezpieczeństwo narodowe i stabilność gospodarcza zależą od przepływu informacji, gdzie technologia jest głównym narzędziem. Nawet jednak najbardziej zaawansowana technologia staje się bezużyteczna w przypadku awarii sprzętu lub oprogramowania, czego częstą przyczyną są szkodliwe działania hakerów, cyberprzestępców czy cyberterrorystów. Dotychczasowe czynniki determinujące konwencjonalnych charakter wojny, jak na przykład odległość geograficzna, tracą ponadto na znaczeniu.

Cyberwojna to pojęcie, które na nowo definiuje formułę konfliktów zbrojnych i umieszcza je w kontekście zakłóceń w systemach informatycznych. Współczesny świat jest tak uzależniony od technologii, że działania w sferze finansów, gospodarki, polityki, kultury oraz postępu technologicznego nierozerwalnie związane są z codziennymi już procesami cyfrowymi. W związku z tym niemożliwe jest oddzielenie działań w świecie rzeczywistym od działań wirtualnych,

a konflikty realizowane i zarządzane przez narzędzia cyfrowe na trwałe zakorzeniły się we współczesnych praktykach działaniach militarnych (Rid, 2012).

Richard Clarke, ekspert ds. bezpieczeństwa narodowego i były doradca Białego Domu ds. terroryzmu, definiuje cyberwojnę jako „działanie polegające na przenikaniu – przez państwo lub organizację działającą na polecenie określonego rządu – cyberprzestrzeni innego kraju w celu spowodowania szkód lub zakłóceń" (Li, 2015). Metoda kontrolowania informacji pod kątem korzyści politycznych i strategicznych nie jest nowa. Manipulowanie sieciami komputerowymi stanowi nowy sposób osiągnięcia tych celów. Osoby fizyczne, firmy i rządy mogą manipulować przepływem informacji w cyberprzestrzeni w celach propagandowych bądź z zamiarem zbierania i klasyfikowania informacji, paraliżowania lub niszczenia kluczowych instalacji infrastruktury.

W kontekście licznych zastosowań internetu i nowych technologii, konflikty zbrojne niedalekiej przyszłości będą zawierały stały element „cyber". Kontynuując tę myśl, pojęcie cyberwojny można zdefiniować jako działania podejmowane przez państwa i podmioty niepaństwowe polegające na penetracji sieci komputerowych przy użyciu narzędzi cybernetycznych w celu zniszczenia, fałszowania lub zniszczenia danych lub systemów komunikacji. Zjawisko to może również odnosić się do aktów przestępczości szpiegowskiej i wojny gospodarczej oraz może obejmować działania wspierające operacje wojskowe na poziomie taktycznym i operacyjnym lub jako działania realizowane w celu osiągnięcie efektów strategicznych (Pearson, 2010, s. 25–26).

W rzeczywistości cyberwojna mogłaby być narzędziem, pozwalającym słabszym państwom zrównoważyć potęgę militarną pozostałych, silniejszych państw, przez naruszenie ich głównych systemów obrony dzięki m.in. zmianie danych zawartych w harmonogramie rozmieszczania jednostek czy też kierowanie kluczowego personelu do niewłaściwych miejsc. Ponieważ logistyka wojskowa jest coraz częściej projektowana tak, aby zapewniać jak najszybciej wystarczające wsparcie i w jak najbardziej odpowiednim momencie, to sabotaż oprogramowania zmieniającego priorytety, cele i osie czasu może wstrzymać lub sparaliżować operacje wojskowe (Lindsay, 2020, s. 1–19).

Termin cyberwojna kojarzony jest również z koncepcją szpiegostwa gospodarczego, sabotażem, a nawet cyberterroryzmem. Średnio co cztery miesiące środki masowego przekazu na terenie Unii Europejskiej informują o niektórych cyberatakach na systemy informacyjne. Przy tej okazji często wskazuje się, że źródłem tych szkodliwych działań są środowiska powiązane z reżimem Rosji lub Chin, których konsekwencje są na tyle poważne, że powodują problemy dyplomatyczne.

Naukowcy od dawna starali się zrozumieć trwałość i uniwersalność konfliktów międzynarodowych (Libicki, 2009, s. 179–181). Jedną z popularnych koncepcji jest teoria wskazująca, że wojny wynikają z nierównowagi upadających imperiów, narodów, antypatii etnicznej lub religijnej, a nawet prób odwrócenia uwagi od problemów lokalnych lub wewnętrznych (Arquilla, 2011, s. 39; Mehan, 2009, s. 19–48). W kontekście wielu analiz, pojawia się jednak często pytanie, czy ta technologia naprawdę oznacza nową erę konfliktów na świecie? I czy istniejące przyczyny wojen są analogiczne i podobne do konfliktów prowadzonych w cyberprzestrzeni?

Kiedy na początku lat 90. ubiegłego wieku David Ronfeldt przedstawił koncepcję cyberwojny, wielu profesjonalistów definiowało to zjawisko przede wszystkim w kategoriach zdobycia pewnej wiedzy o swoim przeciwniku (Arquilla, Ronfeldt, 1993, s. 141–165). Dziś siły zbrojne zwiększają swój potencjał w zależności od postępu technologicznego, innowacji cyfrowych, inwestycji w rozwój cyberpotencjału przemysłu czy też wielkości budżetu obrony.

Kluczowe jest również bezpieczeństwo przepływu informacji, którego zakłócenie może szybko odbić się na zdolności sił zbrojnych do walki; w tym przypadku wojsko nie będzie w stanie kontrolować swoich jednostek i monitorować ich statusu oraz pozycji, a tym samym nie będzie mogło kontynuować bitwy ani prowadzić kampanii. A zatem ofensywa wojskowa, dokonywana za pomocą takich cybernarzędzi, może skutecznie i szybko osiągnąć zakładane cele a w konsekwencji zwycięstwo.

W literaturze przedmiotu cyberataki postrzegane są podobnie do operacji specjalnych, a także narzędzi, które są w stanie rozwiązać międzynarodowy kryzys lub przynajmniej czasowo doprowadzić do rozbrojenia bez konieczności wypowiadania wojny (Farwell, Rohozinski, 2011, s. 23–40). Na przykład wirus komputerowy Stuxnet i atak na irańskie procesy wzbogacania uranu mogą czasowo spowolnić wysiłki Teheranu w produkcji broni atomowej.

Estonia jest pierwszym państwem, które doświadczyło, jak dużym zagrożeniem może być taki atak. 27 kwietnia 2007 roku serwery rządowe, a także strony internetowe, serwisy internetowe, systemy bankowe oraz telekomunikacyjne zostały całkowicie sparaliżowane przez w pełni skoordynowany, przygotowany wcześniej i pochodzący z zewnątrz atak na sieć informatyczną tego państwa. Była to odpowiedź na decyzję władz Estonii o przeniesieniu pomnika upamiętniającego żołnierzy Armii Czerwonej. Obecnie wiele wskazuje, że inicjatorem tej akcji była, współpracująca z Moskwą, rosyjska grupa „Ours" (Dereń, Rabiak, 2014, s. 202–221).

Choć technologia cyfrowa odgrywa znaczącą rolę we współczesnych konfliktach zbrojnych, to należy jednak podkreślić, że wywiad i wojna informacyjna nie są w stanie całkowicie zastąpić ludzi.

Część obserwatorów i badaczy jest sceptyczna co do skuteczności działań cyberofensywnych, jako argument wskazują na ograniczenia w prowadzeniu tego typu konfliktów. Twierdzą, że takie ataki na infrastrukturę cywilną nie przyczyniają się do skuteczniejszego prowadzenia walki przez armię. Jako analogię do cyberataku podawany jest przykład tymczasowego odcięcia energii lub innych źródeł podtrzymujących infrastrukturę państwa i gospodarki, które nie prowadzą do złamania woli społeczeństwa do walki, a wręcz przeciwnie – wzmagają opór państwa i jego obywateli.

Istnieją również wątpliwości co do reakcji na cyberataki. Jak atakowane państwo, oraz społeczność międzynarodowa, powinno zareagować, jeśli cyberagresorem jest jeden z głównych lub dominujących podmiotów mających broń jądrową i szeroki wachlarz gotowych działań? Innym wyzwaniem co do podejmowanych narzędzi odwetowych jest także sytuacja, w której napastnikiem nie jest państwo tylko zespół hakerów?

Cyberataki w Estonii, Gruzji i Iranie, które wstrząsnęły opinią publiczną dowodzą, że coraz częściej takie narzędzia cyfrowe będą wykorzystywane przez różne państwa do rozwiązywania problemów politycznych.

W związku z nieprzewidywalną naturą każdego konfliktu, w tym także cyberwojny, należy mieć świadomość, że takie działania mogą szybko przekształcić się w coś znacznie poważniejszego i zagrozić bezpieczeństwu międzynarodowemu. Nowoczesna technologia staje się coraz bardziej nieodzowną częścią codziennego życia. Powszechne wykorzystanie informacji, w i za pośrednictwem cyberprzestrzeni, jest czynnikiem innowacyjności gospodarczej, ale jest także źródłem asymetrycznego podziału świata.

W ciągu ostatniej dekady technologie informacyjne były często wykorzystywane do usprawniania funkcjonowania rządów, zwiększania skuteczności wojskowej, rozwijania nowych usług handlowych, poprawy produkcji towarów i usług. Oprócz tych korzyści, rosnące uzależnienie od cybertechnologii stworzyło jednak nowe luki w zabezpieczeniach, a tym samym nowe wyzwania dla polityki bezpieczeństwa.

Cyberwojna otwiera szeroki wachlarz możliwych do zastosowania instrumentów przymusu i niszczenia infrastruktury państwa. W świecie cybernetycznym walka toczy się przez działania, które mogą nadejść z dowolnego miejsca i dotrzeć do dowolnego regionu na świecie, co wyraźnie przewyższa tradycyjne działania wojenne. W tym przypadku liczba wojska, a także strategiczne położenie nie ma znaczenia. Walka przenosi się z jednego serwera na drugi, a nie z prowincji do prowincji lub z centrum na peryferia. Miarą siły nie jest liczba głowic rakietowych, ale miliony zainfekowanych komputerów.

Cechą wyróżniającą cyberwojnę jest użycie przemocy przez manipulowanie informacjami, a także przeniesienie konfliktu z klasycznych działań wojennych na poziom cyberprzestrzeni. Tak prowadzony konflikt może składać się z wielu stosowanych technik, począwszy od kłamstw, poprzez propagandę aż po manipulację.

Tak prowadzony konflikt wpływa destabilizująco na funkcjonowanie instytucji publicznych, a co za tym idzie na poziom bezpieczeństwa narodowego. Działania takie często prowadzą wyspecjalizowane organizacje wsparcia współpracujące z obcym państwem (Lindsay, 2020, s. 1–19). Ten typ wojny jest charakterystyczny dla szpiegostwa przemysłowego lub krajowego przemysłu wojskowego, gdzie często dochodzi do sabotażu lub kompromitowania partnerów zagranicznych przed władzami lub organizacjami międzynarodowymi.

Wykorzystywanie informacji w konfliktach pomiędzy podmiotami politycznymi, gospodarczymi lub społecznymi, to nic innego jak działania nielegalne i agresywne, mającymi na celu osłabienie rywala pomówieniami, które mogą zaszkodzić jego wizerunkowi lub w przypadku zdobycia poufnych danych mogą posłużyć do uzyskania wiedzy w celu przejęcia kontroli nad określonym obszarem życia społecznego bądź gospodarczego. W takiej sytuacji nie bez znaczenia są również częste ataki, których celem jest przeciążenie strony internetowej instytucji administracyjnej lub umieszczenie w niej wirusa bądź innego złośliwego oprogramowania.

Cyberatak jako podstawa cyberwojny

Jak odróżnić cyberatak od cyberwojny? Zgodnie z popularną definicją w środowisku akademickim, cyberatak może stanowić wstęp do cyberwojny, gdy jest częścią prawdziwego konfliktu zbrojnego lub spełnia określone standardy, jeśli nie dochodzi do fizycznej wojny. Chociaż poglądy na temat poszczególnych standardów różnią się od stopnia uszkodzenia, które jest powszechnie uznawane za podstawowe kryterium oceny. Biorąc pod uwagę nieprzewidywalność procesów zachodzących w cyberprzestrzeni i jej ścisły związek z życiem ludzi, w literaturze przedmiotu dostrzegalne jest znacznie większe zaniepokojenie katastrofalnymi skutkami, jakie cyberataki mogą przynieść społeczności międzynarodowej niż konsekwencjami będącymi efektem tradycyjnych wojen (Wlatz, 1998, s. 85).

Profesor Matthew C. Waxman definiuje cyberataki jako „próbę zmiany, zniszczenia, degradacji lub zniszczenia systemów i sieci komputerowych oraz informacji lub programów na komputerach wroga". Profesor Michael N. Schmitt zauważa, że ataki sieciowe „mogą być działaniami pojedynczych hakerów lub zorganizowanej grupy" (Feil, 2012, s. 518). Te szerokie terminy i ich definicje odzwierciedlają masowe zastosowanie technologii w strategii obronnej i ofensywnej.

Zbieranie informacji jest niezbędne dla każdego państwa w czasie pokoju lub konfliktu. Czy jednak użycie sieci komputerowych w celu infiltracji innego podmiotu politycznego można uznać za użycie siły? Z pewnością świadomość przewagi technologicznej może być narzędziem wywierania wpływu na inne państwo. Próby wywarcia presji są częścią międzynarodowej geopolityki; mogą wymuszać lub zachęcać do przestrzegania warunków i porozumień między podmiotami politycznymi.

Cyberataki są najczęściej anonimowe, co oznacza, że zidentyfikowanie nadawcy jest niezwykle trudne lub całkowicie niemożliwe. Nawet zakładając, że identyfikacja napastnika jest możliwa, często atak kończy się tak szybko, że nie zawsze jest jasne, czy użycie siły do samoobrony było uzasadnione. Istnieje kilka czynników, takich jak: dotkliwość, natychmiastowość, inwazyjność, domniemana legitymizacja, które pozwalają ocenić, czy agresja spełnia kryteria cyberataku.

Czasami skutki cyberataków są podobne do skutków zainicjowanego przymusu lub szkodliwych działań, które nie są tradycyjnie i powszechnie uważane za użycie siły; są to na przykład sankcje gospodarcze, szpiegostwo lub określone działania pod przykryciem. Niektóre operacje mogą powodować niedogodności lub zakłócenia w funkcjonowaniu państwa i realizowanych przez jego instytucje zadań. Należy jednak pamiętać, że władza korzystając z nowoczesnych środków komunikacji, może wykorzystywać sieci społecznościowe lub serwisy informacyjne do promowania pewnych norm, postaw, wartości czy też zasad.

Środki techniczne pomagają zachować międzynarodowe zasady humanitarne, unikając masowych zniszczeń, do czego najczęściej dochodzi podczas konwencjonalnych konfliktów. Nie jest jednak wykluczone, że cyberbroń może spowodować podobną katastrofę. Prosty błąd w kodzie komputerowym może zniszczyć podstawowe usługi publiczne w całym państwie, co może w takim wypadku spowodować ogromne szkody wśród ludności cywilnej.

Cyberwojna, jak każdy konflikt, wiąże się ze strategią opartą na dysponowaniu określonymi informacjami, a jej uczestnicy za każdym razem muszą odpowiedzieć na pytania – jak są podejmowane działania, czy ich wykonanie oparte jest na prawdziwych informacjach, czy po prostu na przekonujących danych, czyli na ile rozumowanie jest właściwe, czy wynika z manipulacji wroga? Albo jakie działania należy podjąć, aby stać się wobec wroga nieuchwytnym, a jego decyzje i działania stały się przewidywalne? Rozwiązanie tych kwestii dotyczyło dotąd toczonych konfliktów zbrojnych, jednak postęp technologiczny z jednej strony ułatwia, a z drugiej – komplikuje budowę strategii wojskowej.

Współczesne konflikty zbrojne oparte są – obok tradycyjnych źródeł informacji – na danych elektronicznych. W tej dziedzinie nastąpiła znacząca rewolucja w sprawach wojskowych; innowacjami są m.in.: cyfryzacja kanałów łączności i uzbrojenia, pozyskiwanie znaczących danych wywiadowczych na podstawie zdjęć satelitarnych oraz działań prewencyjnych czy sabotażu w cyberprzestrzeni.

Następuje zmiana ofensywnych technik akcji, takich jak paraliż infrastruktury krytycznej, do której należą m.in.: komunikacja, rynki finansowe, administracja publiczna oraz produkcja i zaopatrzenie w energię, surowce i paliwa. Sieci informacyjno-komunikacyjne wspierają ponadto szpitale, transport czy wodociągi, a także elektrownie jądrowe, a zatem awaria lub zakłócenie tych obszarów może mieć poważne konsekwencje dla bezpieczeństwa publicznego.

Przewaga technologiczna ułatwia także rozpoznanie celów, transmisję danych, koordynację sił zbrojnych, inteligentne zarządzanie, uzbrojenie, co daje rządom najbardziej dokładny i globalny obraz sytuacji, umożliwiając podejmowanie natychmiastowych i odpowiednich decyzji strategicznych, podczas gdy przeciwnik nie jest świadomy rzeczywistej sytuacji (Ventre, 2011, s. 6).

Obserwacja znaczenia i roli jaką odgrywa informacja we współczesnym społeczeństwie, może prowadzić również do tego, że dzisiejsze konflikty w znacznej części oparte są na wiedzy. Będą więc realizowane w celu pozyskania globalnej informacji i utrzymania dominującej pozycji nie tylko w technologicznej, ale także kulturowej cyberprzestrzeni. Globalny charakter konfliktu oznacza zatem, że obejmuje on sferę polityczno-militarną, techniczno-gospodarczą i ideologiczno-kulturową.

Wojna w cyberprzestrzeni, jak każdy konflikt, polega głównie na zadawaniu ciosów przeciwnikowi z tą różnicą, że odbywa się to przy użyciu czcionek i symboli zamiast siły. Jednym z głównych celów jest manipulowanie dostępną wiedzą i zdobycie monopolu na dysponowanie odpowiednimi informacjami. Zamiar ten można realizować poprzez m.in. działania szpiegowskie, inwigilację elektroniczną lub sabotaż.

W tego typu przypadkach głównym motywem prowadzenia konfliktu jest ograniczenie swobody działania przeciwnika przez zdyskredytowanie go w oczach sojuszników (Wlatz, 1998, s. 85). Skuteczna wartość informacji zależy zatem nie od jej prawdziwości, ale od sposobu jej rozpowszechniania. Jest skuteczna, o ile jest uważana za prawdziwą przez innych, którzy przyjmują ten punkt widzenia i wartości.

Podsumowanie

Cyberprzestrzeń bardziej przypomina domenę kosmiczną, w której potężne państwa mogą monitorować, patrolować, wywierać wpływ i powstrzymywać agresję, ale nie mogą sprawować kontroli terytorialnej w taki sposób, w jaki jest tradycyjnie rozumiany podczas konfliktów naziemnych. Cyberprzestrzeń to dynamiczny system pozostający w ciągłym ruchu. Nie ma też odizolowanego pola bitwy w internecie. Zamiast tego pole bitwy będzie siłą rzeczy obejmowało systemy cywilne wszystkich pasm, ponieważ cele są rozrzucone po całym współczesnym świecie i nie są kontrolowane ani bronione przez rządy. W ostatecznym rozrachunku zagrożenie wojną cybernetyczną jest bardzo realne, ale też rażąco zawyżone. Nawet akty równoznaczne z cyberwojną nigdy dotąd nie doprowadziły do konfliktu zbrojnego w świecie rzeczywistym (McGraw, 2013, s. 109–119).

Wszystkie wymienione powyżej zjawiska w połączeniu z działaniami militarnymi, których celem jest zdobycie przewagi na polu bitwy lub zwiększenie własnej siły militarnej można nazwać cyberwojną. Tym, co łączy cyberterroryzm i cyberwojnę, jest chęć wyrządzenia przeciwnikowi rzeczywistych szkód. Niewątpliwie można zaobserwować stopniowy proces odchodzenia od konwencjonalnego sposobu prowadzenia wojny.

Zagrożenia cybernetyczne są poważne; istnieje rosnące zagrożenie niestabilnością zarówno na poziomie regionalnym, jak i globalnym. Odstraszające teorie i strategie opracowane i stosowane podczas zimnej wojny nie znajdują już pełnego zastosowania w świecie wirtualnym. Stosunki międzynarodowe w XXI wieku obejmują dużą liczbę nowych podmiotów politycznych, które zaistniały i prowadzą swoja działalność publiczną w cyberprzestrzeni.

Reakcje polityczne pozostają daleko w tyle w stosunku do wydarzeń w wirtualnej rzeczywistości. Skala i zakres cyberzagrożeń nie są nadal w pełni poznane, a dynamika ich zmian powoduje, że dotychczasowe narzędzia analityczne muszą ulegać ustawicznej ewolucji. W dużej mierze wynika to z szybko zmieniającej się natury interakcji w cyberprzestrzeni, jej pełnego zakresu i wpływu na otoczenie społeczno-gospodarczo-politycznego oraz potencjału i możliwości ewentualnego agresora.

Bibliografia

Aleksandrowicz, T.R., Liedel, K. (2014). Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia. W: K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji* (s. 9–38). Warszawa: Difin.

Arquilla, J., Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, *12* (2), 141.

Arquilla, J. (2011). The Computer Mouse that Roared: Cyberwar in the Twenty-First Century. *Brown Journal of World Affairs*, *18*, 39.

Brenner, S.W. (2009). *Cyberthreats: The Emerging Fault Lines of the Nation State*. Oxford: Oxford University Press.

Castells, M. (1996). The Information Age: Economy. *Society and Culture*, *1*, 77–146.

Choucri, N., Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*, *68* (2), 70–77.

Clark, R.M., Hakim, S. (2017). Protecting Critical Infrastructure at the State, Provincial, and Local Level: Issues in Cyber-Physical Security. W: R.M. Clark, S. Hakim, *Cyber-Physical Security Protecting Critical Infrastructure* (s. 1–18). Philadelphia: Springer.

Clarke, R., Knake, R. (2010). Cyber *War: The Next Threat to National Security and What To Do About It*. New York: HarperCollins Publishers.

Dereń, J., Rabiak, A. (2014). NATO a aspekty bezpieczeństwa w cyberprzestrzeni. W: M. Górka, *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku* (s. 202–221). Warszawa: Difin.

Durch, W., Larik, J., Ponzio, R. (2016). Just Security and the Crisis of Global Governance. *Survival. Global Politics and Strategy*, *58* (4), 95–112.

Farwell, J.P., Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, *53* (1), 23–40.

Feil, J.A. (2012). Cyberwar and Unmanned Aerial. Vehicles: Using New. Technologies, from Espionage to. Action. *Case Western Reserve Journal of International*, *45*, 518.

Fontana, I. (2017). Disentangling the cyber politics–cyber security nexus: the new challenge of global politics. *Global Affairs*, *3* (1), 99–104.

Gruszczak, A. (2011). Hybridity of contemporary armed conflicts - Critical analysis. W: B. Zapała, W. Sokała, *Asymmetry and hybridity – the old army against new conflicts* (9–17). Warszawa: Biuro Bezpieczeństwa Narodowego.

Ilves, L.K., Evans, T.J., Cilluffo, F.J., Nadeau, A.A. (2016). European Union and NATO Global Cybersecurity Challenges: A Way Forward. *Journal of the Center for Complex Operations*, *6* (2), 126–141.

Jędrzejko, M., Morańska, D. (2013). *Pułapki współczesności. Cyfrowi Tubylcy. Socjopedagogiczne aspekty nowych technologii cyfrowych*. Dąbrowa Górnicza–Warszawa: ASPRA-JR

Kaiser, R. (2015).The birth of cyberwar. *Political Geography*, *46*, 11.

Li, Y. (2015). Is a Cyberwar Coming? – The alleged Sony hacking warns of the grave consequences of cyberwarfare. *Beijing Review*. Pobrane z: http://www.bjreview.com/ expert/txt/ 2015-01/12/content_663937.htm (10.07.2020).

Libicki, M.C. (2009). Cyberdeterrence and Cyberwar. *RAND Corporation*, 179–181.

Lindsay, J.R. (2020). Cyber conflict vs. Cyber Command: hidden dangers in the American military solution to a large-scale intelligence problem. *Intelligence and National Security*, *1*, 1–19.

McGraw, G. (2013). Cyber War Is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*, *36* (1), 109–119.

Mehan, J.E. (2009). CyberWar, CyberTerror, CyberCrime. *IT Governance*, 19–48.

Pearson, I. (2010). Cyberwar threats are all too real, assures futurologist. *Engineering & Technology*, *5*, 25–26.

Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, *35* (1), 5–32.

Suissa, R. (2012). *Military Resilience in Low-Intensity Conflict: A Comparative Study of New Directions Worldwide*. Plymouth: Lexington Books.

Ventre, D. (2011). Cyberconflict: Stakes of Power. W: D. Ventre, *Cyberwar and Information Warfare* (s. 213–230). Londyn: Wiley – ISTE.

Ventre, D. (2011). *Cyberwar and Information Warfare*. Londyn: Wiley – ISTE.

Wall, D.S. (2008). Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology*, *22* (1–2), 45–63.

Wlatz, E.(1998). *Information Warfare, Principles and Operations*. Norwood: Artech House Boston.

Cytowanie

Górka, M. (2021). Współczesne zagrożenia cybernetyczne na przykładzie zjawiska cyberwojny. Analiza teoretyczna. *Acta Politica Polonica*, *1* (51), 5–21. DOI: 10.18276/ap. 2021.51-01.