Krzysztof Liedel i Paulina Piasecka

Wojna cybernetyczna – wyzwanie XXI wieku

Ewolucja pola walki oraz dynamika zjawisk determinujących przebieg współczesnych konfliktów to czynniki, które wpływają na kształtowanie podejścia państw do kwestii bezpieczeństwa narodowego i międzynarodowego. Przemiany te mają bezpośredni wpływ na sposób tworzenia i realizowania krajowych strategii i polityk bezpieczeństwa. Przenoszenie konfliktów w obszar cyberprzestrzeni jest efektem takich zmian oraz wpływu, jaki mają one na systemy bezpieczeństwa państw i organizacji międzynarodowych. Analiza nowych zagrożeń i sposobów przeciwdziałania im powinna być jednym z priorytetów instytucji odpowiedzialnych za bezpieczeństwo Polski.

Wojna jako zjawisko towarzyszy ludzkości od zarania jej dziejów. Wraz z postępem cywilizacyjnym i wzrostem wartości nowych, niematerialnych zasobów, następował rozwój innych obiektów konfliktu. Już nie tylko materialne bogactwo i władza stawały się powodem lub celem, dla których ludzie, plemiona i narody ze sobą rywalizowały bądź walczyły.

Tak jak zmieniają się przyczyny współzawodnictwa i walki, tak zmieniają się również jej formy i wyraz. Początki wojny i konfliktów między państwami przybierały przede wszystkim formę fizycznego starcia sił, w których narzędziami była wielkość sił zbrojnych, przygotowanie taktyczne i strategiczne dowódców oraz warunki prowadzonego starcia. Zgodnie ze zdaniem wygłoszonym przez Napoleona Bonaparte: „Bóg stoi po stronie liczniejszych batalionów", argumentem ostatecznym w tego typu starciu był militarny i gospodarczy potencjał państwa, który determinował możliwość wystawienia potężniejszej, lepiej uzbrojonej i przygotowanej do realizacji swoich działań armii.

Wraz z postępem technologicznym zwiększała się różnorodność dostępnych środków konfliktu. Już nie tylko w okopach, w bezpośrednim fizycznym starciu żołnierzy, toczyły się bitwy armii. Coraz większą rolę odgrywać zaczęły zaawansowane technologicznie środki walki, inteligentna broń, umożliwiająca dokonywanie precyzyjnych uderzeń niemal bez strat własnych, a ze znacznymi stratami dla wroga. Obecnie większość światowych armii inwestuje nie w powiększanie potencjału ilościowego, lecz dokonuje jakościowych zmian swoich oddziałów. Współczesne siły zbrojne to nie tylko armie i konwencjonalne środki walki wykorzystywane na wielką skalę. Istotną częścią składową – jeśli nie pod

względem liczby ludzi i sprzętu, to pod względem powagi realizowanych zadań oraz efektywności działania – są siły specjalne. Jest to wynik starań o zapewnienie zdolności szybkiej adaptacji sił zbrojnych państwa do tych nowych wyzwań i zagrożeń. W dobie konfliktów, w których stroną może stać się aktor pozbawiony podmiotowości prawnomiędzynarodowej, nieposiadający stałego terytorium ani nawet jasno określonej bazy działania, siły zbrojne muszą przybierać postać pozwalającą na elastyczne reagowanie, z dużą precyzją, na pojawiające się nagle zagrożenia ze strony niewielkich, zdeterminowanych grup[1].

Należy wspomnieć o tym, że poza przedmiotem konfliktów i formami, które one przybierają, następuje kolejna wielka zmiana, której instytucje i agendy państwowe oraz międzynarodowe stojące na straży bezpieczeństwa muszą być świadome. Zmiana ta dotyczy aktorów biorących udział w konflikcie.

W dobie społeczeństwa sieciowego, czyli społeczeństwa informacyjnego, w czasach, gdy coraz większa część aktywności społecznej zarówno odbywa się, jak i jest animowana poprzez komunikację na skalę globalną, przyszedł czas na rozpoznanie nowych aktorów biorących udział w globalnej grze. Poza podmiotami państwowymi mamy do czynienia z podmiotami niepaństwowymi, takimi jak międzynarodowe korporacje, transnarodowe grupy wpływające na postępowanie rządów czy grupy nielegalne, w tym zorganizowane grupy przestępcze i organizacje terrorystyczne. Fakt wejścia do międzynarodowej rozgrywki takich aktorów pociągnął za sobą jej deregulację.

Bez względu na to, jak krytykowane byłoby postępowanie państw i rządów, jakkolwiek negatywnie oceniane byłoby angażowanie się w wojny, interwencje zbrojne oraz „uderzenia prewencyjne", działania z nimi związane określone były ramami prawa międzynarodowego, konwencji i traktatów, które nie pozwalały na wyrwanie się ich spod kontroli. Ponadto w odniesieniu do najbardziej zabójczego środka walki, jaki został stworzony przez ludzkość, czyli broni jądrowej, gwarancją zachowania stosunkowo stabilnej sytuacji była doktryna wzajemnie gwarantowanego zniszczenia. Świadomość, że bez względu na to jak efektywny byłby atak przeciwko wrogiemu państwu i tak pociągnąłby on za sobą natychmiastowy odwet, była linią, której żadne państwo nie odważyło się przekroczyć. Jednak gwarancja ta obowiązywała jedynie między przeciwnikami, których zdefiniować można było w przestrzeni. Przejęcie kontroli nad bronią jądrową przez organizację terrorystyczną, nieposiadającą stałego terytorium, na które skierować można byłoby atak odwetowy, skutecznie niweluje atut wzajemności zniszczenia.

Analizując powyższe zagadnienia można dostrzec wyraźną analogię do nowej epoki konfliktów. Brak określonego terytorium, mobilność celów oraz ano-

[1] Zob.: R. de Wijk, *The Limits of Military Power* [w:] R.D. Howard, R.L. Sawyer (red.), *Terrorism and Counterterrorism. Understanding the New Security Environment*, Guilford 2005, s. 482.

nimowość użytkowania narzędzi sieciowych również na cybernetycznym polu bitwy znacznie ogranicza możliwość skutecznego odwetu i powstrzymywania.

CZYM JEST WOJNA CYBERNETYCZNA?

Rozważania dotyczące wojny cybernetycznej warto rozpocząć od podjęcia próby zdefiniowania tego pojęcia. Nie jest to zadaniem prostym, bowiem mimo wielu prób definiowania nie został ustalony powszechnie akceptowany aparat pojęciowy w obszarze walki informacyjnej, a poszczególne koncepcje adekwatne są do koncepcji i podejść określonych „szkół myślenia”[2].

Walkę informacyjną można zdefiniować jako zorganizowaną w formę przemocy aktywność zewnętrzną państwa prowadzącą do osiągnięcia określonych celów politycznych, skierowaną na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływających przez nie informacji oraz ochronę własnych systemów informacyjnych przed podobnym działaniem przeciwnika[3]. Podobnie wskazuje się, że militarna walka informacyjna to zorganizowana w formę przemocy militarna aktywność zewnętrzna państwa prowadząca do osiągnięcia określonych celów politycznych, skierowana na niszczenie lub modyfikowanie systemów informacyjnych przeciwnika, jak również ochronę własnych systemów informacyjnego porozumiewania się i przepływającej przez te systemy informacji przed podobnym działaniem przeciwnika[4].

Według niektórych koncepcji pojęcie cyberwojny zostało stworzone przez hierarchie wojskowe w celu określenia kolejnego, wirtualnego tym razem pola bitwy. Cyberprzestrzeń, jako zjawisko tworzone przez człowieka, jest jednak płynna i trudna do jednoznacznego zdefiniowania. Dlatego też, mając na uwadze powyższe spostrzeżenia operuje się pojęciem cyberkonfliktu – zjawiskiem odmiennym od cyberwojny, które ma przybliżyć jej zrozumienie[5].

Cyberkonflikt, czyli konflikt cybernetyczny (*cybered conflict)* określony został jako konflikt angażujący różnorodne systemy ludzi, rzeczy, procesów i postrzegania, które związane są z sieciami komputerowymi, choć niekoniecznie całkowicie skomputeryzowane. Konfliktem cybernetycznym będzie zatem każdy konflikt, w którym sukces lub porażka są dla większości jego uczestników uzależnione od działań prowadzonych w sieciach komputerowych. W związku z tym tak długo, jak długo Internet pozostanie na tyle otwarty, jak jest dzisiaj, konflikty prowadzone na jakiejkolwiek płaszczyźnie będą podlegały „cybernetyzacji”. Wynika to z faktu, że obecnie niemal każdy aspekt ludzkiej działal-

[2] T. Jemioło, P. Sienkiewicz (red.), *Zagrożenia dla bezpieczeństwa informacyjnego państwa (Identyfikacja, analiza zagrożeń i ryzyka)*. Tom I. Raport z badań, Warszawa 2004, s. 74–75.
[3] *Ibidem*, s. 74.
[4] *Ibidem*, s. 75.
[5] Ch. Demchak, *Cybered Conflict vs. Cyberwar*, http://www.acus.org/new_atlanticist/cybered- conflict-vs-cyber-war

ności powiązany jest w jakimś stopniu z działaniem sieci cyfrowych[6].

Cyberkonflikty można podzielić na[7]:

- aktywizm – niedestrukcyjną działalność, w ramach której Internet służy wsparciu prowadzonej kampanii,
- haktywizm – kombinację aktywizmu i działań przestępczych; wykorzystuje on metody hakerskie przeciwko określonym celom w Internecie, by zakłócić ich funkcjonowanie, nie powodując przy tym poważnych strat; działalność ta ma na celu nie tyle zniszczenie zasobów przeciwnika, ale przede wszystkim zwrócenie uwagi na dany problem,
- cyberterroryzm – politycznie motywowany atak lub groźba ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach realizacji daleko idących politycznych i społecznych działań w szerszym rozumieniu tego słowa; jest to także użycie Internetu do komunikowania się, propagandy i dezinformacji przez organizacje terrorystyczne.

Jednym z zagrożeń wiążących się z cyberkonfliktami w kontekście bezpieczeństwa informacyjnego kraju jest to, że sieci komputerowe są faktycznie „sieciami nerwowymi kraju". W państwach wysoko rozwiniętych niezakłócone działanie cyberprzestrzeni jest podstawą nie tylko prawidłowego funkcjonowania gospodarki, ale także bezpieczeństwa kraju[8].

W obrębie cyberkonfliktów, przejawiających się jako cyberterroryzm lub sabotaż w obszarze walki informacyjnej, szczególnie poważnym zagrożeniem jest metoda ataków polegająca na spiętrzeniu i nałożeniu na siebie ataków na infrastrukturę krytyczną państwa dokonywanych w cyberprzestrzeni oraz fizycznie, na jej fizyczne elementy[9]. W wypadku ataku w cyberprzestrzeni zakłóceniu ulec może działanie materialnych elementów infrastruktury krytycznej państwa – w wypadku ataku na budynek mieszczący istotny węzeł sieciowy i zespół routerów może nastąpić załamanie komunikacji internetowej odczuwalne w skali regionu a nawet kraju. Tym samym cyberterroryzm może być zarówno aktem podłożenia bomby w strategicznym miejscu, zakłóceniem poprzez atak działania komunikacji opartej na łączach internetowych, jak i przekazywaniem poprzez sieci komputerowe treści zagrażających lub prowadzących do powstania zagrożenia bezpieczeństwa państwa. Przejęcie przez przeciwnika kontroli nad podsystemami infrastruktury krytycznej państwa może zagrozić systemom łączności, zapewniającym dopływ energii czy wody.

Do tych rozważań odnieść można także refleksje nad cyberwojną Jamesa A. Lewisa, który w tekście *Thresholds for Cyberwar* zauważył:

---

6 *Ibidem*.

7 Zob.: K. Liedel, *Zarządzanie informacją w walce z terroryzmem*, Warszawa 2010, s. 23–24.

8 D. Verton, *Black Ice: niewidzialna groźba cyberterroryzmu*, Helion, Warszawa 2004, s. 76.

9 Zob.: K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa państwa*, Warszawa 2004, s. 38.

„Ostatecznie decyzja o tym, czy coś jest aktem wojny, jest decyzją polityczną, szczególnie w wypadkach, które należą do szarej strefy zjawisk między irytacją a działaniami, które mają na celu zniszczenie państwa. [...] Najlepsze, na co możemy mieć nadzieję, to stwierdzenie, że atak cybernetyczny spowodował lub miał spowodować ofiary. Zniszczenie lub ofiary usprawiedliwiają odwołanie się do polityków w celu podjęcia decyzji, czy jest to akt wojny lub czy usprawiedliwia użycie przemocy jako reakcję. Zniszczenie danych i sieci, które jest formą fizycznego zniszczenia (jedynki i zera przestają istnieć lub zostają zastąpione) można uznać za akt wojny, ale trzeba brać pod uwagę skalę zniszczenia i wrażliwość danych, które mu uległy. Także ten, kto dokonał ataku, może wpływać na decyzję, czy dane działanie było aktem wojny. Kiedy niestabilny psychicznie angielski aktywista włamał się na publiczne strony Pentagonu i spowodował szkody w sieci w proteście przeciwko wojnie w Iraku, zostało to uznane za przestępstwo, a nie akt wojny. Gdyby jednak zaangażowane byłoby państwo, działanie to przesunęłoby się bliżej progu wojny. Gdyby włączono pośrednika, a fakt zlecenia danego działania przez państwo zostałby udowodniony, działanie takie także znalazłoby się bliżej przekroczenia progu aktu zastosowania siły”[10].

Takie ogólne rozważania, obejmujące wiele aspektów zjawiska, które określane są zarówno mianem wojny informacyjnej, jak i cyberwojny, posłużą jako punkt wyjścia do przedstawienia różnych koncepcji z tego obszaru badań nad bezpieczeństwem.

ATAKI W CYBERPRZESTRZENI

Dla zobrazowania zagrożeń związanych z cyberkonfliktami, warto przytoczyć **fakty najgłośniejszych cyberataków, do których doszło w 2010 r.** Żaden z nich nie został zakwalifikowany jako akt wojny, nie rozwinął się też w oficjalny konflikt, w który zaangażowane zostałyby siły całego rozwiniętego technologicznie państwa. Niemniej poniższe zestawienie stanowić może wyobrażenie o zmianach na przyszłych polach walki[11]:

- **Styczeń.** Brytyjskie MI5 ostrzega, że tajni agenci wywiadu z Chińskiej Armii Ludowo-Wyzwoleńczej i Ministerstwa Bezpieczeństwa Publicznego nawiązywali kontakty z przedsiębiorcami brytyjskimi na targach i wystawach, oferując „prezenty” – kamery i karty pamięci – zawierające złośliwe oprogramowanie, które zapewniałoby Chinom zdalny dostęp do zainfekowanych komputerów.
- **Styczeń.** *Google* ogłosił, że wykryty został wyrafinowany atak, który spenetrował jego sieci, oraz sieci ponad 30 innych firm amerykańskich. Celem ataków, które *Google* przypisał Chinom, była kradzież technologii oraz uzyskanie dostępu do poczty elektronicznej chińskich aktywistów.

[10] J. A. Lewis, *Tresholds for Cyberwar*, http://csis.org/files/publication/101001_ieee_insert.pdf, tłum. wł.

[11] *Significant Cyber Incidents Since 2006*, lista przygotowana przez Center for Strategic and International Studies, http://csis.org/files/publication/110103_Significant%20Cyber%20Incidents%20Since%202006_0.pdf

- **Styczeń.** Mayankote Kelath Narayanan, doradca ds. bezpieczeństwa narodowego Indii, poinformował, że jego biuro i biura innych departamentów rządowych zostały zaatakowane przez Chiny 15 grudnia 2009 r. Biuro premiera zaprzeczyło temu, że ich komputery zostały zaatakowane przez hakerów. M.K. Narayanan stwierdził, że nie była to pierwsza próba penetracji indyjskich komputerów rządowych.
- **Styczeń.** Grupa o nazwie „Irańska Cyber Armia" zakłóciła funkcjonowanie popularnej chińskiej wyszukiwarki *Baidu*. Użytkownicy byli przekierowywani do strony z irańskim przesłaniem politycznym. Wcześniej „Irańska Cyber Armia" włamała się do serwisu *Twitter* w grudniu 2009 r. i zamieszczała podobne wiadomości.
- **Styczeń.** Firma *Intel* ujawniła, że doświadczyła cyberataku w tym samym czasie, w którym *Google*, *Adobe* i inne firmy zostały zaatakowane. Hakerzy wykorzystali luki w przeglądarce *Internet Explorer*, które były wykorzystane także w innych atakach. *Intel* poinformował, że atak nie spowodował szkód w zakresie własności intelektualnej ani strat finansowych.
- **Marzec.** NATO i UE ostrzegły, że liczba ataków internetowych na ich sieci znacznie wzrosła w ciągu uprzednich 12 miesięcy, wskazując na Rosję i Chiny jako miejsca, skąd przeprowadzono najwięcej ataków.
- **Marzec.** *Google* ogłosił, że odkrył złośliwe oprogramowanie ukierunkowane na komputery wietnamskich użytkowników. *Google* poinformował, że złośliwe oprogramowanie nie było szczególnie wyrafinowane i było wykorzystywane do szpiegowania „potencjalnie dziesiątek tysięcy użytkowników, którzy pobrali oprogramowanie umożliwiające obsługę klawiatury w języku wietnamskim". Złośliwe oprogramowanie uruchomiło również rozproszone ataki typu DoS (*denial of service*)[12] na blogi zawierające wypowiedzi opozycji politycznej, w szczególności przeciwników wydobycia boksytów w Wietnamie.
- **Marzec.** Władze australijskie poinformowały o wykryciu ponad 200 ataków na sieci grupy prawnej, zajmującej się obroną kierownictwa firmy *Rio Tinto* sądzonego w Chinach, w celu uzyskania poufnych informacji na temat strategii obrony.
- **Kwiecień.** Chińskie firmy telekomunikacyjne przypadkowo przekazały błędne informacje *routingu*, czyli ukierunkowania przesyłu danych dla około 37 tys. sieci, powodując błędną transmisję ruchu internetowego przez Chiny. Incydent trwał 20 minut i naraził ruch z ponad 8 tys. sieci w USA, 8,5 tys. sieci chińskich, 1,1 tys. australijskich i 230 sieci francuskich.
- **Maj.** Ujawnione *memo* Kanadyjskiej Służby Bezpieczeństwa i Wywiadu (*Canadian Security and Intelligence Service* – CSIS) mówi, że „liczba ataków na komputery i sieci komputerowe rządu Kanady, uniwersytetów kanadyjskich, prywatnych

[12] Atak na system komputerowy lub sieć komputerową, mający na celu uniemożliwienie działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów.

firm i klientów indywidualnych sieci znacznie się zwiększyły [...] Ataki te nie dość, że są praktycznie niewykrywalne, to oferują wydajne, bezpieczne i mało ryzykowne środki do prowadzenia działalności szpiegowskiej"[13].

- **Lipiec.** Rosyjski agent wywiadu (rzekomo nazywający się Alexey Karetnikow) został aresztowany i deportowany po tym, jak przez dziewięć miesięcy pracował jako tester oprogramowania w korporacji *Microsoft*.
- **Październik.** Robak komputerowy *Stuxnet* – skomplikowane złośliwe oprogramowanie przeznaczone do zainfekowania *Siemens Industrial Control Systems* – zostało wykryte w Iranie, Indonezji i innych krajach, co prowadziło do spekulacji, że była to rządowa cyberbroń mająca uderzyć w irański program nuklearny.
- **Październik.** The Wall Street Journal poinformował, że hakerzy za pomocą złośliwego oprogramowania *Zeus,* dostępnego na czarnym rynku cyberprzestępczym za około 1,2 tys. dolarów, ukradli ponad 12 mln dolarów z pięciu największych banków w USA i Wielkiej Brytanii. *Zeus* wykorzystuje linki w e-mailach do kradzieży informacji o kontach, które hakerzy używają do przekazywania pieniędzy na konta bankowe, będące pod ich kontrolą. 100 „mułów" (mało znaczących członków organizacji przestępczej) zostało aresztowanych za otworzenie rachunków bankowych pod fałszywymi nazwiskami, na które hakerzy przelewali skradzione pieniądze.

NADCHODZI CYBERWOJNA?

W 1993 r. w trakcie badań nad nowymi postaciami konfliktów w ramach projektów badawczych RAND Corporation badacze John Arquilla i David Ronfeldt stworzyli analizę nadchodzących konfliktów epoki informacyjnej[14]. Ich analiza może stanowić podstawę do zbadania paradygmatu nowych konfliktów. W 1993 r. była to zaledwie prognoza. Dziś – ponad 17 lat później – staje się realnym faktem. W swoim opracowaniu J. Arquilla i D. Ronfeldt wzięli pod uwagę przede wszystkim postępujące stechnicyzowanie konfliktów zbrojnych. Wśród wymienianych przez nich pól zmian jest nie tylko rewolucja informatyczna, ale także postęp technologiczny w dziedzinach takich, jak pirotechnika, inteligentne pociski naprowadzane z powietrza i z ziemi, samoloty szpiegowskie, nowe metody wywiadu technicznego, nowe metody dowodzenia, kontroli, komunikacji i wywiadu (*command, control, communications and intelligence* – C^3I)[15]. Przyszłość wojny, jak stwierdzili badacze, zależy od tego, w jaki sposób te technologie będą wykorzystywane, a nie od samych technologii. Organizacja i technologia tworzą ramy wojny, szeroko definiowane przez dowodzących na polu walki i strategów.

Według D. Arquilli i J. Ronfeldta, rewolucja informacyjna obejmuje nie

[13] *Significant Cyber Incidents, op. cit.*
[14] J. Arquilla, D. Ronfeldt, *Cyberwar is coming!,* [w:] *In Athena's Camp: Preparing for conflict in the information age*, RAND Corporation 1993, http://www.rand.org
[15] *Ibidem*, s. 25.

tylko zmiany w systemach i technologiach komputerowych. Wprowadza też zmiany w zakresie teorii zarządzania organizacją. Informacja staje się strategicznym zasobem, który w erze postindustrialnej staje się równie cenny jak wcześniej kapitał i praca. Zwiększa też efektywność wielu rodzajów działania, jednak nie jest to jedynym, ani nawet najważniejszym jej skutkiem. Podstawową zmianą wynikającą z rewolucji informacyjnej jest bowiem zmiana starych sposobów myślenia i działania. Rewolucja informacyjna zarówno w wymiarze technologicznym, jak i pozatechnologicznym, uruchamia mechanizmy, które prowadzą do głębokich przemian w funkcjonowaniu wielu instytucji. Podważa funkcjonalność struktur hierarchicznych, stawiając przed nimi wyzwania ze strony podmiotów sieciowych, wobec których struktury hierarchiczne są niemal całkowicie niewydolne. Jednocześnie stanowi ona czynnik dystrybucji siły, który sprzyjać może słabszym aktorom biorącym udział w ewentualnych konfliktach.

Co więcej, informacyjna rewolucja sprawia, że zagrożenia znacznie łatwiej przekraczają granice między państwami, instytucjami pełniącymi rolę strażników bezpieczeństwa oraz zacierają granice obszarów odpowiedzialności. Poszerza ona przestrzenny i czasowy horyzont zagrożeń, który musi być brany pod uwagę. Tym samym sprawia, że systemy państwowe, w szczególności zaś systemy bezpieczeństwa, muszą stać się bardziej otwarte[16].

J. Arquilla i D. Ronfeldt proponują rozróżnienie między „netwojną" (*netwar*), inaczej wojną sieciową, a cyberwojną, czyli wojną cybernetyczną. Zaznaczają przy tym, że podczas gdy zarówno wojna sieciowa, jak i wojna cybernetyczna związane są z technologiami informatycznymi i komunikacyjnymi, na najgłębszym poziomie są formami wojny o wiedzę:

- kto co wie?
- kiedy?
- gdzie?
- dlaczego?

a także wojny o to, jak bezpieczne są społeczeństwa i siły zbrojne w kontekście wiedzy o samych sobie i o swoich przeciwnikach[17].

Pierwszą z wymienionych kategorii, wymagającą szczególnej analizy, jest kategoria *netwar*. Definicja *netwar* („netwojny", wojny sieciowej) obejmuje konflikt związany z informacją, prowadzony na wysokim szczeblu między narodami bądź grupami społecznymi. Istotnym elementem tego konfliktu jest cel – wpływanie na to, co populacja, która jest celem ataku, wie o swojej tożsamości bądź o otaczającym ją świecie. Netwojna skupiać się może zatem na opinii publicznej, na elitach rządzących bądź obu tych celach. Aby w pełni zrozumieć to pojęcie i jego granice pragmatyczne, poświęcić trzeba odpowiednią uwagę używanym w ramach takiego konfliktu narzędziom, które obejmują:

- dyplomację,
- propagandę,
- kampanie psychologiczne,

[16] *Ibidem*, s. 26.
[17] *Ibidem*, s. 27.

- działania na poziomie wpływania na procesy polityczne lub kulturowe,
- dezinformację bądź manipulowanie lokalnymi mediami,
- infiltrację sieci komputerowych i baz danych,
- wysiłki w zakresie promowania opozycyjnych lub wrogich populacji będących celem grup w sieciach komputerowych[18].

Wojna sieciowa może zatem stanowić nową formułę, która uzupełnia spektrum konfliktów ekonomicznych, politycznych, społecznych i militarnych. Wojna sieciowa będzie miała wymiar głównie pozamilitarny, jednak istnieją pewne obszary wspólne z konfliktem militarnym. W tych obszarach wojna sieciowa będzie miała na celu wpływanie na C³I, przekształcając się częściowo w cyberwojnę. Wojna sieciowa może być prowadzona zarówno przez rządy i ich służby przeciwko wrogim grupom, jak i przez grupy społeczne przeciwko rządowi. Trzeba także zauważyć, że może być ona prowadzona także między sektorami niepaństwowymi, a mimo to wzbudzać zainteresowanie i niepokój podmiotów państwowych. Zakrojony na szeroką skalę konflikt tego rodzaju może bowiem wpływać na interesy narodowe państw, nawet jeśli nie są one w niego bezpośrednio zaangażowane.

Kolejną kategorią, również objętą badaniami RAND Corporation, jest cyberwojna. Zgodnie z definicją analityków tej instytucji, jest to sposób prowadzenia operacji wojskowych zgodnie z zasadami związanymi z informacją jako zasobem strategicznym. Jego głównym celem jest zakłócenie funkcjonowania lub zniszczenie systemów komunikacyjnych i informacyjnych przeciwnika oraz osiągnięcie przewagi poprzez zgromadzenie maksymalnej wiedzy na temat przeciwnika przy jednoczesnym zapobieganiu uzyskania przez przeciwnika informacji na temat własnych stron – słabych i mocnych. Osiągnięcie takiej przewagi informacyjnej wyraża się przede wszystkim w takim oddziaływaniu na systemy komunikacyjne i informacyjne przeciwnika, aby wpływać na posiadaną przez niego wiedzę, m.in. na temat:

- identyfikacji własnych oddziałów,
- gdzie się znajduje,
- co może zrobić,
- kiedy może to zrobić,
- które zagrożenia zwalczać najpierw[19].

Zgodnie z teorią RAND, wojna cybernetyczna jest konfliktem o wysokiej intensywności. Może ona angażować różnorodne technologie, m.in.:

- technologie dowodzenia i kontroli,
- technologie gromadzenia informacji wywiadowczych,
- technologie przetwarzania i dystrybucji informacji,
- technologie identyfikacji „przyjaciel-wróg",
- systemy „inteligentnej" broni[20].

Może przejawiać się ona takimi działaniami ofensywnymi, jak:

- „oślepianie" przeciwnika,
- przeciążanie systemów,

[18] *Ibidem*, s. 28.
[19] *Ibidem*, s. 30.
[20] *Ibidem*, s. 30.

- infiltracja systemów komunikacyjnych i informacyjnych[21].

Jak zaznaczono wcześniej, rewolucja informacyjna pociąga za sobą konieczność wprowadzania zmian organizacyjnych we współczesnych armiach, tak aby ich poszczególne komponenty funkcjonowały bardziej jako powiązane sieci niż jako odseparowane struktury hierarchiczne. Szczególny wpływ ma ten proces na siły zbrojne współczesnych państw, które przystosowując się do nowej formy konfliktu muszą przechodzić głębokie zmiany organizacyjno-funkcjonalne.

ARMIE CYBERPRZESTRZENI

Sieciowo-centryczne środki walki (*net-centric warfare)* to kolejne pojęcie, którego zbadanie jest konieczne dla pełnego zrozumienia zmian, jakie w obszarze bezpieczeństwa przynosi szeroko rozumiana cyberwojna. Doktryna ta, zbadana i wdrażana przez armię Stanów Zjednoczonych, została opisana w raporcie przygotowanym przez Departament Obrony USA[22]. Dokument ten przedstawia istniejącą strategię, której celem jest przełożenie przewagi informacyjnej, wspartej zaawansowaną technologią informacyjną, na przewagę militarną poprzez stworzenie sieciowych struktur łączności między geograficznie rozprzestrzenionymi oddziałami. Taka sieciowa organizacja, w połączeniu ze zmianami technologicznymi, organizacyjnymi oraz zmianami w przygotowaniu personelu, może skutkować nowymi formami zachowania organizacji.

Zgodnie z filozofią amerykańskiej armii, współczesny żołnierz potrzebuje informacji, tak jak żołnierz armii napoleońskiej potrzebował karmy dla koni, a żołnierze frontów II wojny światowej potrzebowali paliwa[23]. Zakreśla to zupełnie nowy obszar działań wojennych, których bezpośrednim celem jest proces dowodzenia i kontroli przeciwnika. Działania w cyberprzestrzeni nie podlegają tym samym prawom co działania w świecie fizycznym, więc inaczej mierzyć trzeba „sukces" w walce cybernetycznej oraz inaczej definiować działania prowadzone w tej przestrzeni. W tradycyjnym konflikcie zwycięstwo definiowane było jako zniszczenie infrastruktury przeciwnika. Powodowało to jednak nie tylko utratę jakiegokolwiek potencjalnego wsparcia ze strony lokalnej społeczności, ale tworzyło także groźbę całkowitej zapaści organizmu państwowego, co mogło prowadzić do stanu państwa upadającego lub upadłego (*failing state*, *failed state),* niezdolnego do samodzielnego funkcjonowania i stanowiącego zagrożenie dla stabilności całego regionu[24].

Nowe zagrożenia, z jakimi zmagać się mają siły zbrojne w obszarze cyberkonfliktów, to m.in. ocena relatywnej wartości informacji w sytuacji, w której czas jest kluczowym czynnikiem dla sukcesu prowadzonej operacji. Mimo że ry-

[21] *Ibidem*, s. 30.

[22] Department of Defense. *The Implementation of Network-Centric Warfare*. Washington, D.C., 2005, http://www.au.af.mil/au/awc/awcgate/transformation/oft_implementation_ncw.pdf

[23] M. J. Basla, *The Cyber Domain: How is it Changing the Warfighter*, http://www.rusi.org/downloads/assets/Cyber_Domain_and_the_Warfighter_RDS_Summer_09.pdf

[24] *Ibidem*.

zyko w tym obszarze jest trudno mierzalne, konieczne jest wypracowanie metod, które pozwolą na dokładne określenie wartości informacji. Innym wyzwaniem, z jakim przyjdzie się zmagać jest problem ochrony informacji niejawnych. Nowa kultura informacyjna związana z funkcjonowaniem w skomputeryzowanym środowisku, powoduje przejście od zasady *need-to-know* (udostępniania informacji jedynie tym, którzy jej potrzebują) do zasady *need-to-share* (potrzeby dzielenia się informacją).

Nowe metody prowadzenia walki powodują powstanie nowych zagrożeń i jednocześnie nowych korzyści. Jedną z najważniejszych korzyści jest stały i elastyczny dostęp do ekspertów. Funkcjonując w środowisku Web 2.0 (sieci internetowej współtworzonej przez użytkowników), siły zbrojne działają w wymiarze umożliwiającym współpracę, w której udział brać mogą wszyscy – od dowódców do operatorów pola walki. Inne korzyści z funkcjonowania cyberprzestrzeni – jeśli nie jako pola walki, to jako czynnika pola walki – są następujące:

- możliwość zapewnienia funkcjonowania sieciowych kanałów komunikacji w sytuacji awarii bądź zniszczenia innych kanałów komunikacji,
- możliwość zapewniania szkolenia nawet w odległych lokalizacjach,
- możliwość lepszego zrozumienia celów i intencji przeciwnika[25].

Priorytety w zakresie kształtowania środowiska cyberbezpieczeństwa określają także inne państwa. Analiza zamierzeń i planów Wielkiej Brytanii w tym obszarze prowadzi do wyznaczenia trzech głównych celów[26]:

I. *Ludzie*: zasoby ludzkie mają być kluczowym elementem budowania zdolności zapewnienia cyberbezpieczeństwa Wielkiej Brytanii. Przewidziana została rola nie tylko dla wojska i sektora publicznego, ale także dla obywateli.
II. *Partnerstwa:* efektywne partnerstwa z podmiotami sektora prywatnego, dostarczającymi technologiczną bazę dla sieciowej obrony oraz wieloletnią ekspertyzę w zakresie przeciwdziałania atakom w cyberprzestrzeni. Jako priorytet pod uwagę brane są także partnerstwa międzynarodowe, szczególnie ze Stanami Zjednoczonymi.
III. *Obrona sieciowa:* pierwszy priorytet operacyjny, oparty na systemie ochrony zasobów cybernetycznych państwa.

Szczególnie praktyczny wymiar mają działania w celu zapewnienia cyberbezpieczeństwa, podejmowane przez Estonię. Państwo to powołało do życia oddział ochotników, Ligę Obrony Cybernetycznej (LOC), w skład której wchodzą inżynierowie, pracownicy banków, wielkich korporacji i ministerstw. Na wypadek cyberwojny LOC podlegać ma wojskowemu dowództwu[27].

MIĘDZYNARODOWY WYMIAR CYBERBEZPIECZEŃSTWA

W obszarze bezpieczeństwa cyberprzestrzeni swoje działania realizują

[25] *Ibidem*.
[26] J. Basset, *Cyber Priorities After SDSR 2010*, http://www.rusi.org
[27] K. Zuchowicz, *Pierwsza armia Internetu*, http://www.rp.pl

nie tylko państwa, ale także organizacje międzynarodowe i sojusze militarne. Sygnałem tego jest choćby szczyt NATO w Lizbonie (19–20 listopada 2010 r.) oraz przyjęta tam nowa Koncepcja Strategiczna[28]. W dokumencie tym, wśród wyzwań dla wspólnego, kooperatywnego bezpieczeństwa, zaraz po proliferacji broni masowego rażenia i terroryzmie, wskazano zagrożenie cyberatakami. Jak zapisano w Koncepcji, cyberataki stają się coraz częstsze, są dobrze zorganizowane a przez to coraz bardziej destrukcyjne i kosztowne. Mogą zagrażać infrastrukturze krytycznej państwa, a przez to funkcjonowaniu transportu, gospodarki i administracji. Istotnym aspektem tego zagrożenia jest fakt, iż jego sprawcami mogą być obce wojska, służby wywiadowcze, organizacje przestępcze, grupy terrorystyczne i/lub grupy ekstremistyczne. Zagrożenie to traktowane jest jako zagrożenie nie tylko dla pojedynczych państw, ale dla całego obszaru euroatlantyckiego.

Zobowiązania zawarte w nowej Koncepcji Strategicznej Sojuszu dotyczą zwiększania zdolności państw członkowskich i samej organizacji w zakresie zapobiegania atakom, wykrywania ich, z ochrony przed nimi i odbudowy po nich, z użyciem procesu planowania NATO dla wzmacniania i koordynowania krajowych zdolności w zakresie cyberobrony. Celem określonym w Koncepcji jest stworzenie centralnej cyberochrony dla wszystkich członków NATO oraz lepsza integracja świadomości dotyczącej cybernetycznego wymiaru funkcjonowania państw, ostrzegania i reagowania NATO z krajami członkowskimi.

Działania w tym obszarze prowadzi także Unia Europejska. Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) prowadzi na co dzień działania, które mają służyć zapewnieniu „bezpieczeństwa społeczeństwa informacyjnego" Europy. Jest ono uszczegółowiane jednak jako bezpieczeństwo „komputerów, telefonów komórkowych, bankowości oraz funkcjonowania Internetu dla wspierania cyfrowej gospodarki Europy"[29].

Bezpieczeństwo cyberprzestrzeni staje się zatem priorytetem. Trend ten jest częścią zjawiska znacznie szerszego, tj. przesuwania na czoło listy priorytetów w zakresie przeciwdziałania zagrożeniom o charakterze pozamilitarnym, określanych mianem „nowych wyzwań". Działania zmierzające do sprostania im przybierają także formę organizacyjną. Unia Europejska stworzyła „2CENTRE" – Centrum do spraw Cyberprzestępczości w zakresie Doskonalenia Szkoleń, Badań i Edukacji (*Cybercrime Centre of Excellence Network for Training, Research and Education*[30]).

NATO zdecydowało, że wyzwania bezpieczeństwa w cyberprzestrzeni będą objęte działaniami powołanej

[28] *Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation*, Lizbona 19–20 listopada 2010, http://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf

[29] ENISA – Securing Europe's Information Society, http://www.enisa.europa.eu/

[30] *Cybercrime Centre of Excellence Network for Training*, Research and Education, http://www.2centre.eu/

w sierpniu 2010 r. jednostki Międzynarodowego Sztabu NATO o nazwie Dział Nowych Wyzwań dla Bezpieczeństwa (ang. *Emerging Security Challenges Division*)[31]. Wyrazem działań na rzecz cyberbezpieczeństwa Sojuszu i jego państw członkowskich jest także stworzenie w stolicy Estonii Kooperacyjnego Centrum Doskonalenia Cyberobrony *(Cooperative Cyber Defence Centre of Excellence*, CCD COE). Misją CCD COE jest wzmacnianie zdolności, współpracy i wymiany informacji w ramach NATO, krajów członkowskich i partnerów Sojuszu przez edukację, badania i rozwój oraz konsultacje. CCD COE ma stać się głównym źródłem ekspertyzy we wspólnej cyberobronie poprzez gromadzenie, tworzenie i dystrybucję wiedzy[32].

Działania na rzecz budowania zdolności w zakresie cyberobrony i cyberbezpieczeństwa trwają także w Polsce. W Białobrzegach działa Centrum Bezpieczeństwa Cybernetycznego, którego zadaniem jest ochrona polskiej armii przed atakami w cyberprzestrzeni. Jest to pierwszy krok na drodze do utworzenia cyfrowych jednostek wojskowych, których żołnierze i dowódcy będą wyposażeni w najnowsze technologie informacyjne[33].

IMPLIKACJE NOWEJ FORMY PROWADZENIA KONFLIKTÓW

Rozważając zagadnienia związane z nowym polem i środkami walki oraz wyłonieniem się nowej formy konfliktów, jaką jest wojna cybernetyczna we wszystkich swoich postaciach, warto podsumować najważniejsze zmiany, jakie przynosi ona dla bezpieczeństwa współczesnych państw oraz doktryn militarnych rządzących współczesnym bezpieczeństwem[34]:

I. Zachodzi zmiana w postrzeganiu pola walki – cyberwojna jest znacznie mniej związana z geograficznymi wyznacznikami pola walki, znacznie bardziej zaś z architekturą cyberprzestrzeni.
II. Cyberwojna zmienia rozumienie tego, co stanowi atak – w przeciwieństwie do wcześniejszych wojen i konfliktów cyberwojna nie musi oznaczać fizycznego zniszczenia przeciwnika, a jedynie uderzenie w krytyczne elementy jego systemu informacyjnego i komunikacyjnego.
III. Na poziomie strategicznym cyberwojna może doprowadzić do realizacji zasady strategicznej centralizacji i taktycznej decentralizacji; zalew informacją i dezinformacją w trakcie konfliktu w cyberprzestrzeni, przy jednoczesnym uwzględnieniu tempa, w jakim podejmowane są działania w przestrzeni cyfrowej może sprawić, że hierarchiczne dowodzenie okaże się niemożliwe: podejmowanie decyzji co do każdej kwestii taktycznej, która jest problemem na polu walki, przez instytucje szczebla centralnego, będzie niemożliwe w czasie dostępnym na podjęcie takiej decyzji. Cyberwojna stanie się przyczynkiem do dal-

[31] *New NATO division to deal with Emerging Security Challenges*, http://www.nato.int/cps/en/SID-6E509263-lBF11962/natolive/news_65107.htm?selectedLocale=en
[32] *The Cooperative Cyber Defence Centre of Excellence (CCD COE)*, http://www.ccdcoe.org
[33] W. Lorenz, *Polska na cyberfroncie*, http://www.rp.pl
[34] J. Arquilla, D. Ronfeldt, *Cyberwar...*, *op. cit.*, s. 45.

szego usamodzielniania jednostek wojskowych prowadzących poszczególne działania bojowe w cyberprzestrzeni. Zjawisko to związane jest z przekształcaniem się struktur hierarchicznych w struktury sieciowe, gdzie procesy dowodzenia i kontroli muszą ustępować miejsca procesom konsultacji i koordynacji, będącym podstawowym budulcem organizacji sieciowych.

Cyberwojna, a raczej pojawienie się takiej formy konfliktu, ma swoje dobre i złe strony. Z jednej strony konflikt między państwami, czy też między podmiotami niepaństwowymi a państwami, nie musi pociągać za sobą ofiar w ludziach. Z drugiej, stanie się obiektem ataku nie jest już poprzedzone ruchami wielkich mas wojska ani też manewrami z użyciem różnych rodzajów sił zbrojnych. Zaskoczenie stanie się jeszcze bardziej nieodłącznym atrybutem współczesnych konfliktów a wyzwanie, jakie stawiają, będzie wymagało rosnącej elastyczności i zdolności dynamicznej adaptacji państwowych struktur odpowiedzialnych za bezpieczeństwo państwa, jego obywateli i interesów.