CZĘŚĆ TRZECIA

CYBERZAGROŻENIA BEZPIECZEŃSTWA PAŃSTWA

ROZDZIAŁ XVIII

Maciej Marczyk
Akademia Sztuki Wojennej

CYBERPRZESTRZEŃ RP I JEJ ZAGROŻENIA – WYBRANE PROBLEMY

Wstęp

W XXI wieku obronność jest płaszczyzną bezpieczeństwa narodowego, tworzącą sumę wszystkich cywilnych oraz wojskowych działań, których celem jest przeciwdziałanie i przeciwstawienie się wszystkim możliwym zagrożeniom bezpieczeństwa państwa, militarnym a także pozamilitarnym, mogącym przyczynić się do kryzysu polityczno-militarnego.

Obszar bezpieczeństwa cechuje się współwystępowaniem i wspólnym przenikaniem się zagrożeń militarnych i pozamilitarnych, na ogół o charakterze asymetrycznym. Ryzyko konfliktu zbrojnego na dużą skalę nie uległo zmniejszeniu zwłaszcza w sytuacji rozwijającego się konfliktu z Rosją, ale nie zniknęła także groźba konfliktów o formie regionalnej i lokalnej (przykład Ukrainy).

Zasadniczymi zagrożeniami dla środowiska bezpieczeństwa są zagrożenia o charakterze asymetrycznym. Najbardziej poważnymi zagrożeniami pozostają:

- terroryzm międzynarodowy, a także cyberterroryzm i terroryzm z wykorzystaniem broni masowego rażenia;
- proliferacja broni masowego rażenia i środków jej przenoszenia;
- zorganizowana przestępczość międzynarodowa, bazująca na przemycie broni i materiałów podwójnego zastosowania, handlu narkotykami i ludźmi, a także na nielegalnych operacjach finansowych oraz piractwo morskie.

Członkostwo w Sojuszu Północnoatlantyckim i Unii Europejskiej oraz strategiczne partnerstwo ze Stanami Zjednoczonymi Ameryki czy też współpraca z Wielką Brytanią, jest głównym punktem odniesienia dla polskiej polityki zagranicznej i obronnej. Żywotnie ważne dla Polski jest, aby

NATO i USA umacniały swoją pozycję na arenie międzynarodowej, podnosząc tym samym poziom bezpieczeństwa państw członkowskich i Polski.

Priorytetem dla Polski pozostaje rozwijanie, wspólnie z pozostałymi członkami NATO, instrumentów, których celem jest wzmocnienie kolektywnej obrony. Obejmują one przygotowanie przez Sojusz skutecznego zestawu sił wysokiej gotowości, a także aktywne uczestnictwo sojuszników w ramach Sił Odpowiedzi NATO. Wymaga to również efektywnego zaangażowania w obecność wojsk sojuszu (USA) na terenach państw stanowiących wschodnią flankę sojuszu, w tym Polski oraz sprawnych mechanizmów konsultacji w ramach Sojuszu Północnoatlantyckiego.

W przypadku wystąpienia kryzysu w dalszym otoczeniu Polski, gdy dojdzie do zaangażowania NATO lub UE, Rzeczpospolita Polska na mocy decyzji uprawnionych organów, będzie gotowa do uczestniczenia w działaniach sojuszniczych. Zaangażowanie Sił Zbrojnych RP w operacje reagowania kryzysowego będzie odbywać się zgodnie z priorytetami i zasadami określonymi w *Strategii udziału Sił Zbrojnych RP w operacjach międzynarodowych*. Zgodnie z koncepcją kompleksowego podejścia, oprócz sił zbrojnych wykorzystane będą instrumenty polityczne, dyplomatyczne, gospodarcze, przy współpracy organizacji pozarządowych.

Ponadto Siły Zbrojne RP utrzymują niezbędny potencjał sił wyspecjalizowanych do prowadzenia działań antyterrorystycznych, przeciwdziałania asymetrycznym i niemilitarnym zagrożeniom oraz zadań realizowanych w sytuacjach kryzysowych w ramach wsparcia działań władz cywilnych[29].

Zgodnie z Wizją Sił Zbrojnych RP 2030 operacje Sił Zbrojnych RP będą realizowane głównie w układzie sił międzynarodowych. Ich planowanie i dowodzenie będzie zintegrowane i realizowane przez międzynarodowe dowództwa i sztaby. Operacje o narodowym charakterze będą realizowane w ramach połączonej operacji obronnej, strategicznej operacji obronnej i operacji reagowania kryzysowego na terenie kraju. Będą one posiadały ograniczony przestrzennie i czasowo rozmach (z wyjątkiem operacji strategicznej – jeżeli nie nastąpi realizacja pkt 5 Traktatu Północnoatlantyckiego), a ich istotą będzie zminimalizowanie skutków powstałego zagrożenia.

W zależności od rozmachu, charakteru i celu operacji siły je realizujące będą tworzone przez zróżnicowane, co do wielkości komponenty: lądowy, powietrzny, morski, wojsk specjalnych, a także sił realizujących zadania w cyberprzestrzeni oraz w sferze informacyjnej[30].

Obrona cyberprzestrzeni stała się jednym z najczęściej podejmowanych tematów dotyczących bezpieczeństwa. Stabilność funkcjonowania

[29] Por. *Strategia rozwoju systemu bezpieczeństwa narodowego RP 2022, Rada Ministrów 9 kwietnia 2013*, *Strategia obronności Rzeczypospolitej Polskiej, Strategia sektorowa do strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej,* Warszawa 2009, s. 16-20.

[30] Tamże, s. 15.

i rozwój globalnego społeczeństwa informacyjnego jest uzależniony od otwartej, niezawodnej i – przede wszystkim – bezpiecznej cyberprzestrzeni. Podnoszenie świadomości w tym zakresie idzie w parze z gwałtownym wzrostem liczby incydentów komputerowych i nowych rodzajów zagrożeń. Polska również jest obiektem ataków cybernetycznych. Podobnie jak inne państwa stoi przed wyzwaniem, jakim jest wypracowanie zmian prawnych i organizacyjnych, pozwalających na zapewnienie właściwego poziomu bezpieczeństwa cyberprzestrzeni i funkcjonujących w niej obywateli.

Bezpieczeństwo cyberprzestrzeni RP

Mówiąc o zagrożeniu związanym z cyberprzestrzenią można mówić o: zagrożeniu w cyberprzestrzeni, zagrożeniu cyberprzestrzeni, zagrożeniu cybernetycznym lub cyberzagrożeniu. Dla ustalenia właściwej konwencji terminologicznej proponuje przyjąć, że cząstka *cyber*[31] jest w języku polskim pierwszym członem wyrazów złożonych wskazującym na ich związek z informatyką. Słowo *cyber* w polszczyźnie nie występuje, można jednak tę cząstkę interpretować jako powstałą od przymiotnika *cybernetyczny*. W związku z tym tworzone wyrazy zaczynające się od *cyber* - należy interpretować jako wyrazy złożone. W języku polskim wszystkie rzeczowniki złożone, których człony są wyrazami pospolitymi, pisze się łącznie. Wobec tego zasadnym staje się, aby zagrożenia związane z cyberprzestrzenią nazywać cyberzagrożeniami.

Cyberprzestrzeń nie posiada jednej powszechnie uznanej definicji. Dotychczas naukowcy nie doszli do konsensusu, czym ona właściwie jest. Dlatego ograniczę się jedynie do stwierdzenia, że cyberprzestrzeń to ogólnoświatowa wytworzona przez człowieka, podatna na cyberzagrożenia, współwłasność, która powinna być chroniona przez nas wszystkich. Jej natura polega na tym, że zwiększenie połączeń zwiększa współzależność połączonych elementów. Skuteczność działań zapewniających bezpieczeństwo bardzo złożonych współzależnych sieci i systemów wymaga coraz to nowych sposobów myślenia.

Istotnym pojęciem w procesie identyfikacji cyberzagrożeń jest środowisko cybernetyczne. **Środowisko cybernetyczne** „jest to zespół wszelkich elementów i czynników, będących w ścisłej współzależności, który wpływa na procesy informacyjne danego układu poprzez umacnianie stanów pożądanych i przeciwdziałanie stanom niepożądanym”[32].

Czynnikami środowiska cybernetycznego są energia i informacja. Elementami zaś są nie tylko serwery, terminale, stacje robocze, koncentra-

[31] http://www.polonistyka.fil.ug.edu.pl/?id_cat=300&id_art=1023&lang=pl (dostęp: 10.11.2014 r.).

[32] J. Wołejszo (red.) *Automatyzacja dowodzenia SZ RP w środowisku sieciocentrycznym*, Gdynia – Warszawa 2013, s. 102.

tory (ang. hub), przełączniki (ang. switch), oprogramowanie, czy inne urządzenia teleinformatyczne, ale również radiostacje, radiolinie, tory transmisyjne (kable światłowodowe czy miedziane, falowody) przesyłające dane i informacje bądź media transmisyjne (fale elektromagnetyczne czy promienie lasera).

Środowisko cybernetyczne zautomatyzowanych systemów dowodzenia wojskami i sterowania środkami rażenia (systemami uzbrojenia) nie składa się wyłącznie z komputerów oraz urządzeń teleinformatycznych. Jednak ogólnie pojęta informatyka, czyli platformy i łącza teleinformatyczne, a także komputery (serwery, terminale czy stacje robocze) oraz oprogramowanie stanowią podstawę oraz główny trzon zautomatyzowanego systemu tego typu. Informatyka, jako dziedzina zajmuje się usprawnianiem procesów informacyjnych poprzez ich automatyzację[33]. Zastosowanie informatyki w cybernetycznym środowisku zautomatyzowanych systemów wsparcia lub wspomagania dowodzenia i sterowania systemami uzbrojenia, jako odpowiedź na wyzwania współczesnego pola walki, staje się jak najbardziej uzasadnioną koniecznością, ze względu na fakt, iż zachodzi potrzeba sprawnego zorganizowania procesów informacyjnych oraz ich automatyzacji.

W raporcie World Economic Forum z 2012[34] roku cyberataki, zostały umieszczone na 4. miejscu wśród największych zagrożeń dla bezpieczeństwa i stabilności globalnej. Przed nimi znalazły się znaczne dysproporcje dochodów, przewlekły brak równowagi podatkowej, oraz wzrost emisji gazów cieplarnianych.

Również NATO zidentyfikowało zagrożenia w przestrzeni cybernetycznej jako jedno z czterech największych ryzyk dla pokoju na świecie, obok takich zjawisk jak: terroryzm, rozprzestrzenianie broni masowego rażenia i walka o dostęp do energii. Również w raporcie World Economic Forum z 2014[35] nasilenie cyberataków na dużą skalę uznane zostało obok awarii krytycznej infrastruktury informacyjnej i sieci teleinformatycznych oraz incydentów związanych z oszustwami i kradzieżami informacji za jedno z globalnych zagrożeń technologicznych.

Identyfikując cyberzagrożenia należy mieć na uwadze, iż istota cyberzagrożeń powoduje, że zarówno użytkownicy jak i właściciele systemów oraz sieci teleinformatycznych nie mają wpływu na ich istnienie. Pewne czynniki mogą stanowić zagrożenie lub nie. Cyberzagrożenie jest w swej istocie jedynie potencjalnym czynnikiem wywołującym szkodę. Zagrożenie musi zatem mieć możliwość oddziaływania na przedmiot, wykorzystując

[33] Zob. A. Rokicka-Broniatowska, *Wstęp do informatyki gospodarczej*, Szkoła Główna Handlowa – Oficyna Wydawnicza w Warszawie, Warszawa 2002.
[34] *Global Risks 2012*, Seventh Edition.
[35] *Global Risks 2014*, Ninth Edition.

jego podatność. Zgodnie z polską normą PN-I-02000:2002 podatnością są „wady i luki w strukturze fizycznej, organizacji, procedurach, zarządzaniu, administrowaniu, sprzęcie, oprogramowaniu, a także zamierzone lub niezamierzone działania personelu, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika". Ponadto powyższa norma zwraca również uwagę na fakt, że po pierwsze, „istnienie podatności nie powoduje szkód samo z siebie. Podatność jest jedynie warunkiem lub zestawem warunków, które umożliwiają uszkodzenie systemu lub zakłócenie działalności użytkownika przez atak. Po drugie, jeżeli podatność posiada zagrożenie, istnieje ryzyko"[36].

Identyfikując cyberzagrożenia należy brać pod uwagę fakt, iż oprogramowanie złośliwe staje się coraz bardziej wyrafinowane technicznie, możliwość odpowiedzi oraz ustalenie dokładnej drogi cyberataku na własny system teleinformatyczny są ograniczone. Cyberataki z powodzeniem mogą być prowadzone zarówno z terytorium atakowanego państwa jak i spoza jego granic. Uwzględniając otwartość oraz zasięg cyberprzestrzeni, możliwe jest skryte prowadzenie cyberataków i wykorzystanie podatnych systemów jako doskonałych narzędzi do jego przeprowadzenia. Cyberataki dość często nie zawierają informacji o tożsamości ani pochodzeniu atakujących. Dlatego przestępcy, terroryści, szpiedzy czy inne wrogie podmioty z powodzeniem wykorzystują do swojej działalności cyberprzestrzeń mając na względzie jej transgraniczny charakter. Działalność wojsk również jest podatna na cyberataki[37].

Zagrożenia bezpieczeństwa cybernetycznego stanowią jeden z najpoważniejszych wyzwań zarówno dla bezpieczeństwa publicznego jak i narodowego. Zagrożeń nie można zlikwidować. Usunąć natomiast można, w miarę możliwości, podatności własnego systemu. Nie można przecież wpłynąć na cyberprzestępcę, który z odległego kraju próbuje zakłócić działanie jakiegoś systemu. Można natomiast podjąć próbę zabezpieczenia systemu teleinformatycznego tak, aby był najbardziej jak tylko to możliwe, odporny na oddziaływanie intruza.

Siły zbrojne podczas działania zarówno w czasie pokoju, kryzysu jak i wojny są w znacznym stopniu zależne od sieci i systemów teleinformatycznych. Uzależnienie od informatyzacji stwarza nie tylko duże możliwości do prowadzenia sprawnych i skutecznych działań, ale również podatności na cyberzagrożenia. Duży zasięg wojskowych sieci i systemów teleinformatycznych stwarza dogodne warunki dla potencjalnego bądź realnego przeciwnika do przeprowadzenia cyberataków.

[36] PN-I-02000:2002, *Technika informatyczna*, *Zabezpieczenia w systemach informatycznych*, *Terminologia*, Polski Komitet Normalizacyjny, s. 12.

[37] S. Korycki, *System bezpieczeństwa Polski*, Warszawa 1994, s. 54.

Według kryterium poziomu wiedzy i umiejętności podmiotu zagrażającego sieciom i systemom teleinformatycznym cyberzagrożenia dzielą się na trzy kategorie:

- Początkujących, czyli tych, którzy polegają na innych, aby rozwinąć złośliwy kod,
- Zaawansowanych, czyli tych, którzy mogą rozwijać swoje własne narzędzia do wykorzystania publicznie znanych luk w zabezpieczeniach, a także potrafią odkrywać nowe luki w zabezpieczeniach,
- Profesjonalistów, czyli tych, którzy mają znaczne zasoby i potrafią przeznaczyć je do stworzenia luki w zabezpieczeniach systemów.

Pokonać zagrożenie oznacza wyeliminować podatności własnego systemu bądź czynniki potencjalnie niebezpieczne. Identyfikacja wszystkich cyberzagrożeń jest niemożliwa. W dynamicznie rozwijającym się świecie nieprzerwanie ewoluują, a ich liczba stale wzrasta. Cyberzagrożenia są równie liczne jak i złożone. Narzędzia, których używają wrogie podmioty, sposoby działania, cele, które wyznaczają oraz ofiary, które wybierają zmieniają się. Niemożliwe jest, zatem rozpoznawanie cyberzagrożeń przez jednego człowieka. Najlepsze wyniki można uzyskać poprzez pracę zespołu specjalistów posiadających różne specjalności.

Liczba źródeł cyberzagrożeń wciąż rośnie. Mogą nimi być zarówno konkurenci polityczni, gospodarczy lub ekonomiczni, skorumpowani członkowie organizacji (pracownicy czy działacze), grupy przestępcze, hakerzy, a także obce państwa zaangażowane w działalność szpiegowską lub wojnę informacyjną. Źródła cyberzagrożeń różnią się w zależności od zdolności podmiotów stwarzających zagrożenie, ich zaangażowania w działania oraz ich motywacji np.: korzyści ekonomiczne, gospodarcze, czy polityczne. Do źródeł cyberzagrożeń można zaliczyć:

- grupy przestępcze,
- hakerów,
- terrorystów (cyberterrorystów),
- osoby wtajemniczone w organizacji (krety),
- inne narodowości zaangażowane w działalność przestępczą,
- aktywizm polityczny,
- szpiegostwo,
- walkę informacyjną.

Owe źródła zagrożeń różnią się pod względem możliwości podmiotów, ich gotowości do działania oraz motywów, którymi się kierują, łącznie z korzyściami finansowymi. Potencjalnie podmioty będące źródłem cyberzagrożeń posługują się różnymi technikami ataków na sieci i systemy teleinformatyczne oraz ich elementy. Są w stanie przechwytywać lub wykradać wartościowe informacje. Rozmiar zagrożenia zależy od złożoności, skomplikowania sposobu przeprowadzenia cyberataku. Cyberataki mogą być

kombinacją wielu różnych technik. Za ich pomocą potencjalnie zagrażające podmioty mogą podejmować działania zarówno przeciwko celom pojedynczym, np. komputery osobiste bądź stacje robocze jak i zbiorowym, np. sieci i systemy teleinformatyczne podmiotów gospodarczych, politycznych bądź rządowych.

Kategorie te nie wykluczają się wzajemnie. Na przykład działania pojmowane przez jeden podmiot jako hacktivism mogą być pojmowane przez inny podmiot jako cyberterroryzm. Powyższa klasyfikacja ma na celu zidentyfikowanie głównych rodzajów istniejących zagrożeń, w celu określenia najbardziej odpowiedniego i skutecznego podejścia do zakresu ryzyka jakie stwarzają.

W sieciach i systemach teleinformatycznych, do zapewnienia łączności oraz przesyłania danych, zarówno na duże jak i małe odległości, stosowane są różne media transmisyjne. Oprócz przewodów, których technologia wytwarzania oparta jest na metalach (np. przewody miedziane), wykorzystywane są również fale elektromagnetyczne. Fala elektromagnetyczna rozchodzi się w powietrzu, ośrodkach stałych np. szkło (światłowody) oraz próżni. Właściwość ta czyni z fali elektromagnetycznej ważne, a czasem kluczowe medium transmisyjne, na którym oparte są bezprzewodowe sieci i systemy teleinformatyczne.

Bezprzewodowe sieci i systemy teleinformatyczne mają duże znaczenie dla działań w cyberprzestrzeni. Transmisja bezprzewodowa z powodzeniem może być wykorzystywana na bardzo dużych obszarach. Środowisko elektromagnetyczne (ang. *electromagnetic environment*) w wielu przypadkach jest podstawowym środowiskiem działania. To, właśnie dzięki bezprzewodowej łączności, a także transmisji danych zapewniona jest wysoka mobilność i swoboda działań, zarówno wojsk jak i personelu niezmilitaryzowanego. Fale elektromagnetyczne umożliwiają łączność oraz zapewniają niezbędne usługi w czasie działań. Do takich działań zalicza się np.: działalność rozpoznawczą, informacyjną, wykorzystywanie zautomatyzowanych systemów wsparcia i wspomagania dowodzenia oraz kierowania środkami walki czy sterowania środkami rażenia. W bezprzewodowych sieciach i systemach teleinformatycznych poza tym, co jest bezpośrednio użyteczne dla użytkowników, czyli łącznością i przesyłem danych i informacji, zachodzą również procesy niewidoczne nadawców i odbiorców np. synchronizacja czy sygnalizacja. Sieci i systemy bezprzewodowe, które usprawniają, a w wielu przypadkach umożliwiają działanie są jednak podatne na cyberzagrożenia.

Pierwszym podstawowym wymogiem dla sieci bezprzewodowej, aby urządzenia, media transmisyjne oraz styki[38] i złącza działające w środo-

[38]Styk jest realizacją połączeń dostępowych w punkcie odniesienia. Styk występuje np. między terminalem a adapterem terminala, bądź między zakończeniem sieciowym a terminalem.

wisku elektromagnetycznym były wzajemnie kompatybilne, jest ich standaryzacja. Dotyczy ona nie tylko urządzeń (ang. *hardware*), ale także ich oprogramowania (ang. *software*). I to właśnie owa standaryzacja z punktu widzenia cyberzagrożeń jest piętą achillesową bezprzewodowych sieci i systemów teleinformatycznych.

Właściwości środowiska elektromagnetycznego sprawiają, że jest ono bardzo trudne do odseparowania wyłącznie na własny użytek. Oznacza to, że np. fale radiowe dostępne są nie tylko dla osób, do których dane i informacje są adresowane, ale również dla odbiorców innych niż ci, którzy powinni je otrzymać. Dlatego bezprzewodowe punkty dostępowe powinny być możliwie najlepiej zabezpieczone przed nieuprawnionym dostępem.

Przestrzeń cybernetyczna jest uznana w sferze militarnej za kolejny, piąty (po przestrzeni lądowej, morskiej, powietrznej i kosmicznej) wymiar współczesnej przestrzeni konfrontacji zbrojnej. Na początku lat 90 XX w. John A. Warden, pułkownik z Sił Powietrznych USA w swojej teorii strategicznego paraliżu wskazał, że człowiek prowadzi działania w nowej przestrzeni nazwanej przez niego cyberprzestrzenią. Według Wardena każdą organizację (w tym przeciwnika) należy traktować jak strukturę składającą się z systemu 5 wzajemnie powiązanych okręgów (elity polityczne; instytucje podstawowe; infrastruktura; społeczeństwo; systemy obronne), składających się na całość i pełniących założone dla nich funkcje. Każdy z okręgów Wardena funkcjonuje w pięciu „wymiarach", którymi są następujące elementy: ląd; morze; powietrze; przestrzeń kosmiczna; przestrzeń cybernetyczna. Poglądy Wardena szybko znalazły odzwierciedlenie w amerykańskich poglądach na prowadzenie działań militarnych.

Przeprowadzona analiza upoważnia do uznania, że obecne wykorzystywanie tego pojęcia w terminologii militarnej ściśle wiąże się z konstruowaniem przez człowieka urządzeń i systemów elektronicznych służących do transmisji danych i informacji – sieci komputerowych (teleinformatycznych). Ocenia się, że przestrzeń cybernetyczna, jako zjawisko tworzone przez człowieka, jest płynna i trudna do jednoznacznego zdefiniowania.

Wraz z pojawieniem się nowych technologii teleinformatycznych oraz rozwojem sieci Internet pojawiły się nowe formy działań, takie jak cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych oraz cyberwojna, rozumiana jako konfrontacja w przestrzeni cybernetycznej przede wszystkim pomiędzy państwami.

Konflikt cybernetyczny, czyli cyberkonflikt *(ang. Cybered Conflict)* określony został jako konflikt angażujący różnorodne systemy ludzi, rzeczy, procesów oraz postrzegania, które związane są pośrednio lub bezpośrednio z sieciami teleinformatycznymi. Konfliktem cybernetycznym może być zatem każdy konflikt, w którym sukces lub porażka są dla większości jego

uczestników uzależnione od działań prowadzonych w przestrzeni cybernetycznej z wykorzystaniem sieci teleinformatycznych. W związku z tym jak długo Internet pozostanie na tyle otwarty, jak jest to dzisiaj, konflikty prowadzone na jakiejkolwiek płaszczyźnie będą podlegały „cybernetyzacji". Wynika to z faktu, że obecnie niemal każdy aspekt ludzkiej działalności powiązany jest w jakimś stopniu z działaniem sieci teleinformatycznych.

W takim ujęciu konflikt cyberterrorystyczny utożsamiany jest z wojnami sieciowymi (*ang. Netwar*), które mogą być prowadzone przede wszystkim na poziome społecznym[39]. Ich celem jest wpływanie na postawy i zachowania społeczne, zmienianie i wpływanie na to co dane społeczeństwo wie lub myśli, że wie. Tego rodzaju konflikty utożsamia się lub postrzega jako współczesną wersję wojen propagandowych, które są znane z historii. Mogą je toczyć zarówno państwa jak i organizacje pozapaństwowe np.: korporacje gospodarcze, handlowe, itp.

W literaturze przedmiotu wyróżnia się następujące rodzaje cyberkonfliktów:

- aktywizm – jako niedestrukcyjna działalność, w ramach której Internet służy wsparciu prowadzonej kampanii,
- haktywizm – będący kombinacją aktywizmu i działań przestępczych; wykorzystuje się metody hakerskie przeciwko określonym celom w Internecie, by zakłócić ich funkcjonowanie, nie powodując przy tym poważnych strat; działalność taka ma na celu nie tyle zniszczenie zasobów strony atakowanej (potencjalnego przeciwnika), ale przede wszystkim zwrócenie uwagi na dany istotny zdaniem atakującego problem;
- cyberterroryzm – jest politycznie motywowanym atakiem lub groźbą ataku na komputery, sieci lub systemy informacyjne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie oraz grupach społecznych 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.

W grupie cyberkonfliktów, przejawiających się jako cyberterroryzm lub sabotaż sieciowy w obszarze walki informacyjnej, szczególnie poważnym zagrożeniem jest metoda ataków polegająca na spiętrzeniu oraz nałożeniu na siebie ataków na infrastrukturę krytyczną państwa[40] dokonywanych

[39] http://www.angelfire.com/az/sthurston/Cyberwar.html (dostęp: 15.05.2016 r.).

[40] W *Ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* definiuje się infrastrukturę krytyczną jako: „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców", por.: http://www.nowastrategia.org.pl/ infrastruktura-krytyczna-krotka-analiza zagadnienia/ (dostęp: 28.04.2016 r.).

w przestrzeni cybernetycznej oraz fizycznie, na jej fizyczne elementy.

Wojna cybernetyczna[41] (*ang. Cyber-Warfare*) polega na wykorzystaniu komputerów, Internetu i innych środków przechowywania lub rozprzestrzeniania informacji w celu przeprowadzania ataków na systemy teleinformatyczne potencjalnego przeciwnika. W odróżnieniu od cyberkonfliktu są to działania, które mają zakłócić lub zniszczyć systemy teleinformatyczne i komunikacyjne potencjalnego przeciwnika.

Wojnę cybernetyczną, która może być również elementem wojny informacyjnej[42] od klasycznych wojen odróżnia przede wszystkim środowisko walki. Są nim systemy i sieci teleinformatyczne. W takiej wojnie strona atakująca przy minimalnych nakładach materialnych zdolna jest w znacznym stopniu sparaliżować infrastrukturę krytyczną lub gospodarkę państwa strony przeciwnej, o ile ta infrastruktura oparta jest w wystarczająco wysokim stopniu na systemach i sieciach teleinformatycznych. Wojna cybernetyczna jest więc atakiem w dużym stopniu asymetrycznym, co umożliwia prowadzenie tego rodzaju wojen państwom słabszym przeciwko silniejszym.

W ramach wojny cybernetycznej, napastnik może dążyć do realizacji swoich różnych celów strategicznych polegających na rozpowszechnianiu propagandy lub wywoływaniu paniki pośród ludności cywilnej. Może także powodować trwałe uszkodzenie kluczowych elementów infrastruktury krytycznej strony przeciwnej, zwłaszcza technologicznej (elektrownie, systemy komunikacyjne, itp). Ataki te mogą też być narzędziem wywiadu technologicznego oraz pozyskiwania informacji.

Do przeprowadzenia ataków cybernetycznych mogą być wykorzystywane różne środki (narzędzia) walki, np.: komputery zombie[43] używane do rozproszonych ataków odmowy usług DDoS[44]; exploity[45], które pozwalają na przejęcie kontroli nad systemami; metody socjotechniczne, które z kolei ukierunkowane są na manipulację zachowaniami ludzi, i inne. Ataki tego typu mogą osłabić lub uszkodzić też systemy wykorzystywane przez siły

[41] Według niektórych koncepcji pojęcie cyberwojny zostało stworzone przez hierarchie wojskowe w celu określenia kolejnego, wirtualnego tym razem pola bitwy.

[42] Wojna cybernetyczna jest częścią większej całości jaką jest wojna informacyjna.

[43] Komputer zombie jest komputerem przyłączonym do Internetu, w którym bez wiedzy jego posiadacza został zainstalowany program sterowany z zewnątrz przez inną osobę.

[44] DDoS (ang. *Distributed Denial of Service*) – atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania poprzez zajęcie wszystkich wolnych zasobów, przeprowadzany równocześnie z wielu komputerów (np. zombie).

[45] Exploit jest programem mającym na celu wykorzystanie błędów w oprogramowaniu (np. przepełnienie bufora na stosie lub stercie, czy format string) w celu przejęcia kontroli nad działaniem procesu i wykonania odpowiednio spreparowanego kodu maszynowego (*ang. Shellcode*). Osoby używające exploitów bez niezbędnej wiedzy o mechanizmach ich działania często nazywa się *Script Kiddies*.

zbrojne przeciwnika. Sytuacja taka może doprowadzić do ich całkowitego odsłonięcia na polu walki, zwłaszcza podczas prowadzenia walki elektronicznej.

Wojna cybernetyczna jest uznawana przez specjalistów za konflikt o wysokiej intensywności. W czasie jej prowadzenia wykorzystywane są różnorodne technologie, takie jak: dowodzenia i kontroli; gromadzenia informacji wywiadowczych; przetwarzania i dystrybucji informacji; identyfikacji „przyjaciel – wróg" czy „inteligentnej" broni.

W ramach wojny cybernetycznej mogą być realizowane również działania ofensywne z wykorzystaniem nowoczesnych technologii polegające na: „oślepianiu" przeciwnika; przeciążaniu i infiltracji jego systemów informacyjnych, a zwłaszcza rozpoznania, dowodzenia i kontroli.

Polska cyberprzestrzeń wojskowa jest częścią cybernetycznej obrony kraju. Jest też istotną częścią przestrzeni natowskiej. Siły zbrojne są zobligowane do reagowania na incydenty w resortowych sieciach teleinformatycznych. Ta zdolność powinna być budowana we współpracy z Agencją Komunikacji i Informacji NATO NCIA (*ang. NATO Communications and Information Agency*) oraz poszczególnymi członkami sojuszu. Ocenia się, iż sieci teleinformatyczne naszych sił zbrojnych i agencji rządowych, w których przesyłane są informacje niejawne, nie powinny być częścią publicznych sieci teleinformatycznych oraz systemów publicznie dostępnych. Taka separacja powinna następować z wykorzystaniem mechanizmów kryptografii, a więc szyfratorów mających certyfikaty krajowej władzy bezpieczeństwa odpowiednich służb[46], które zapewniają ochronę wszystkich danych przekazywanych między elementami sieci. W praktyce najsłabszym ogniwem tworzonych systemów bezpieczeństwa teleinformatycznego są ludzie, czyli użytkownicy przenoszący dokumenty między komputerami na nośnikach informacji, takich jak tokeny, USB czy zewnętrzne twarde dyski. Zachodzi zatem potrzeba realizacji przedsięwzięć ochronnych tych systemów, zwłaszcza defensywnych. Za skuteczne uznaje się je z wykorzystaniem elementów operacyjnego rozpracowywania przeciwnika. Przede wszystkim należy rozpoznać i monitorować zagrożenia oraz potencjał ewentualnego przeciwnika, którym nie zawsze będą siły zbrojne innego państwa. Coraz głośniej mówi się o wojnach hybrydowych[47] oraz o atakach sponsorowanych. Państwa, które wspierają terroryzm, współpracują z gru-

[46] Funkcję krajowej władzy bezpieczeństwa pełni Szef Agencji Bezpieczeństwa Wewnętrznego w stosunkach międzynarodowych w sferze cywilnej oraz w sferze wojskowej – za pośrednictwem Szefa SKW.

[47] Wojna hybrydowa to wojna niewypowiedziana. Formalnie nawet nie wojna. Ale giną na niej ludzie, używa się ciężkiej broni, biorą w niej udział wojskowi – choć bez oznaczeń. Stanowi mieszankę metod klasycznie militarnych – przede wszystkim nieregularnych działań zbrojnych (partyzantka, sabotaż, dywersja, akty terrorystyczne) – ale też zawiera elementy walki informacyjnej (propaganda, dezinformacja), ekonomicznej oraz cybernetycznej.

pami przestępczymi, które działają również w cyberprzestrzeni. Grupy hakerów do kradzieży informacji lub działań destrukcyjnych można wynająć, podobnie jak najemników do prowadzenia klasycznych operacji wojskowych, z użyciem broni kinetycznej[48]. Podkreśla się, iż w ochronie przestrzeni cybernetycznej ważną rolę odgrywa rozpoznawanie takich grup i sieci ich powiązań. Z jednej strony podejmuje się działania obronne, buduje się odpowiednie zdolności w tym zakresie, a z drugiej śledzi się informacje o nowych metodach ataków sieciowych, analizuje się, co robią nasi potencjalni przeciwnicy. Buduje się też sojusze na kilku poziomach w zakresie współpracy technologicznej, między uczelniami, organami ścigania, sądami, służbami specjalnymi. Ważną rolę odgrywa też partnerstwo z sektorem prywatnym. Ocenia się, iż taki system powinien dać możliwość przygotowania do obrony, reagowania i zatrzymania sprawców. Sama technologia nie wystarczy bowiem do uzyskania zdolności obronnych.

Rozważając problem aktywnych działań w sieciach teleinformatycznych naszych sił zbrojnych należy podkreślić, iż realizowany jest on w ramach walki elektronicznej w wyniku zakłócania elektronicznego. Należy brać pod uwagę w tej sytuacji możliwość niezamierzonych naruszeń pracy w systemy naszych sojuszników a nawet wojsk własnych, bowiem cyberprzestrzeń nie zna granic państwowych.

W Polsce w 2008 roku powołano zespół reagowania na incydenty komputerowe – CERT.GOV. Jest on częścią ABW (Departamentu Bezpieczeństwa Teleinformatycznego) i ma wszystkie uprawnienia właściwe tym służbom. W MON funkcjonuje natomiast MIL-CERT dla sił zbrojnych. Ocenia się, iż żadna z polskich instytucji rządowych nie jest jednak w stanie samodzielnie bronić się przed atakami hakerów. Wobec tego CERT Polska we współpracy z Departamentem Bezpieczeństwa Teleinformatycznego ABW stworzył system wczesnego ostrzegania o zagrożeniach internetowych o nazwie ARAKIS-GOV24[49]. System ten nie jest typowym środkiem zabezpieczającym i w żadnym wypadku nie zastępuje standardowych systemów zabezpieczających typu firewall, antywirus, czy systemy detekcji/prewencji intruzów. Zawiadamia on o próbach rozprzestrzeniania się robaków sieciowych, botnetów, skanowaniach danych z zewnątrz oraz infekcjach komputerów wewnątrz chronionej sieci. Jego zadaniem jest wykrywanie przede wszystkim anomalii, które mogą wskazywać na ataki hakerskie, a nawet na jego przygotowania do niego.

[48] Broń kinetyczna jest rodzajem broni służącej do niszczenia celu przez gwałtowne dostarczenie mu energii kinetycznej. Za klasyczne przykłady pocisku kinetycznego uznaje się: kamień, strzałę, czy pocisk pistoletowy, karabinowy, rakietowy, itp.

[49] http://media.wp.pl/kat,1022945,opage,4,title,Cyberterroryzm-co-robi-Polska-by-uchronic-sie-przed-atakami-hakerow,wid,16257187,wiadomosc.html?ticaid=113e57 (dostęp: 04.05.2016 r.).

Działania na rzecz budowania zdolności w zakresie cyberobrony i cyberbezpieczeństwa trwają także w naszym sektorze obronnym. W ramach MON (NCK) powstało w 2015 roku Centrum Operacji Cybernetycznych[50], którego zadaniem jest ochrona SZ RP przed atakami w przestrzeni cybernetycznej. Centrum jest asumptem do tworzenia i wykorzystania cyfrowych jednostek wojskowych, których żołnierze i dowódcy będą wyposażeni w najnowsze technologie informacyjne i będą mogli prowadzić działania defensywne i ofensywne w cyberprzestrzeni.

W ramach Narodowego Systemu Rozwoju Koncepcji i Eksperymentowania badania prowadzi Zespół ekspertów wojskowych (również cywilnych naukowców z ośrodków badawczych), który rozpatruje działania militarne w cyberprzestrzeni skupiając się na jej aspektach prawnych w tym *Koncepcji działań w cyberprzestrzeni dla SZ RP*. Zespół pracuje pod kierunkiem specjalistów z Centrum Doktryn i Szkolenia CDiSSZ z Bydgoszczy.

Resort ON jak każda inna organizacja narażony jest na ataki cybernetyczne i ingerencje z zewnątrz w systemy teleinformatyczne dowództw i wojsk. Zaawansowane technicznie ataki cybernetyczne typu DoS lub DDoS mogą być także przeprowadzone na różne systemy teleinformatyczne wykorzystywane w SZ RP, np.:

- systemy dowodzenia i kierowania obronnością Sił Zbrojnych (Państwa);
- systemy kontroli i naprowadzania lotnictwa;
- satelitarne i radiowe systemy nawigacyjne;
- systemy łączności cyfrowej, satelitarnej i radiowej;
- zautomatyzowane systemy dowodzenia;
- systemy kierowania systemami walki;
- systemy rozpoznania;
- systemy teleinformatyczne, bazy danych, oprogramowanie;
- systemy optoelektroniczne techniki bojowej;
- systemy powiadamiania (Broadcasting);
- stacjonarne i mobilne systemy telekomunikacyjne (sieci wymiany informacji),

Ważne zatem jest, aby to Naczelny Dowódca (DO RSZ) dysponował możliwościami oddziaływania w ramach opisywanego systemu na całe siły zbrojne, od poziomu najwyższego po najniższe taktyczne szczeble dowodzenia [51].

W Polsce, tak jak w innych krajach europejskich, obserwuje się ciągły rozwój technologii teleinformatycznej, a co za tym idzie, rozwój sieci bez-

[50] Kilka lat wcześniej powstało CBC – Centrum Bezpieczeństwa Cybernetycznego w Białobrzegach, zob.: W. Lorenz, *Polska na cyberfroncie*, http://www.rp.pl (dostęp: 12.04.2016 r.).

[51] Zob. *Decyzja 275/ MON z dnia 13.07.2015 roku w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej*, poz. 208, NCK, D.U. z 14.07.2015 r.

przewodowych. Brak uświadomienia niebezpieczeństwa wynikającego z niedostatecznych zabezpieczeń teleinformatycznych sieci bezprzewodowych przed cyberatakiem jest głównym zagrożeniem dla bezpieczeństwa teleinformatycznego jednostek organizacyjnych podległych Ministerstwu Obrony Narodowej. Brak dostatecznego wykształcenia czy wyobraźni administratorów sieci może prowadzić do fatalnych skutków, które decydować będą o bezpieczeństwie państwa.

Na rynku niewojskowym (cywilnym) bezpieczeństwem systemów i sieci komputerowych zajmuje się CERT Polska (Computer Emergency Response Team), który jest zespołem powołanym do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet.

CERT Polska działa od 1996 roku (do końca roku 2000 pod nazwą CERT NASK), a od roku 1997 jest członkiem FIRST (Forum of Incidents Response and Security Teams). W ramach tej organizacji współpracuje z podobnymi zespołami na całym świecie. Zespół CERT Polska działa w strukturach Naukowej i Akademickiej Sieci Komputerowej, przez którą jest finansowany.

Do głównych zadań zespołu należy:

- rejestrowanie i obsługa zdarzeń naruszających bezpieczeństwo sieci,
- alarmowanie użytkowników o wystąpieniu bezpośrednich dla nich zagrożeń,
- współpraca z innymi zespołami IRT (Incidents Response Team),
- prowadzenie działań zmierzających do wzrostu świadomości dotyczącej bezpieczeństwa teleinformatycznego,
- prowadzenie badań i przygotowanie raportów dotyczących bezpieczeństwa polskich zasobów Internetu,
- niezależne testowanie produktów i rozwiązań z dziedziny bezpieczeństwa teleinformatycznego,
- prace w dziedzinie tworzenia wzorców obsługi i rejestracji incydentów, a także klasyfikacji i tworzenia statystyk.

Zagrożenia bezpieczeństwa płynące z przestrzeni cybernetycznej są zagrożeniami realnymi, obecnymi w codziennej rzeczywistości życia jednego z podmiotów obszaru bezpieczeństwa państwa jakim są SZ RP, zatem rozpoznanie, osiągnięcie, utrzymanie i doskonalenie systemu bezpieczeństwa, w tym wczesnego ostrzegania przez tego typu zagrożeniami, staje się nieodzowne do zapewnienia przewagi nad siłami zbrojnymi innych państw.

W *Strategii Bezpieczeństwa Narodowego RP* cyberprzestrzeń została określona kolejnym środowiskiem walki zbrojnej co determinuje, iż SZ RP winny dysponować zdolnościami defensywnymi i ofensywnymi w cyberprzestrzeni, tak by skutecznie realizować funkcję potencjalnego odstraszа-

nia przeciwnika[52]. Istotne jest więc aby były one gotowe, samodzielnie bądź też we współpracy z sojusznikami do prowadzenia operacji ochronnych i obronnych w przypadku wystąpienia cyberwojny, czy też cyberkonfliktu. Ponadto w Strategii podkreślone zostały w szczególności działania zmierzające do poprawy koordynacji działań Sił Zbrojnych wraz z sektorem prywatnym oraz administracją publiczną i państwową[53]. Zarówno w aspekcie profilaktyki, jak i działań prewencyjnych w cyberprzestrzeni istotna będzie współpraca poszczególnych komórek resortu obrony narodowej czy też Sił Zbrojnych z sektorem prywatnym a w szczególności z podmiotami sektora finansowego, telekomunikacyjnego, energetycznego jak i opieki zdrowotnej czy tez transportowego.

W Polsce tak jak w innych krajach europejskich, obserwuje się ciągły rozwój technologii teleinformatycznej, a co za tym idzie, rozwój sieci bezprzewodowych. Brak uświadomienia niebezpieczeństwa wynikającego z niedostatecznych zabezpieczeń teleinformatycznych sieci bezprzewodowych przed cyberatakiem jest głównym zagrożeniem dla bezpieczeństwa teleinformatycznego jednostek organizacyjnych podległych Ministerstwu Obrony Narodowej.

Zakończenie

Autor wyraża przekonanie, że warunkiem niezbędnym do funkcjonowania każdego systemu teleinformatycznego, także wojskowego, zwłaszcza w obszarze cyber-, jest wyposażenie go w środki techniczne zapewniające bezpieczeństwo wymiany oraz współdzielenia informacji pomiędzy takimi samymi oraz różnymi poziomami (szczeblami) kierowania. Jednocześnie, w celu poprawy bezpieczeństwa, a także minimalizowania błędów w obsłudze czy też dostępie do zasobów sieci, stworzyć należy możliwość automatycznego rejestrowania pracy w sieciach teleinformatycznych, a także kontroli wymienianych informacji. Przestrzeganie procedur bezpieczeństwa wymiany informacji, identyfikacji urządzeń i połączeń, jak również zastosowanie zabezpieczeń technicznych użytkowanego sprzętu, stwarza bariery dla osób nieuprawnionych, które skutecznie powinny chronić współdzielenie danych przy pomocy wojskowych sieci teleinformatycznych. Zatem aby spełnić oczekiwania techniczne w aspekcie systemów teleinformatycznych obszaru bezpieczeństwa państwa, cyberprzestrzeni militarnej (Sił Zbrojnych), infrastruktury krytycznej, należałoby brać pod rozwagę niżej wymienione przedsięwzięcia:

1. Bezpieczeństwo transmisji informacji – zgodne z potrzebami ochrony zabezpieczenie linii i urządzeń przekazujących informacje na potrzeby systemów teleinformatycznych.

[52] *Strategia Bezpieczeństwa Narodowego RP*, Warszawa 2014, s. 32.
[53] Tamże, s. 34-35.

2. Wpływ oprogramowania na bezpieczeństwo informacji w systemach teleinformatycznych – umożliwia działanie urządzeń wykorzystując ustalone mechanizmy zarządzania oraz kolejność realizacji poszczególnych zadań.
3. Ochrona fizyczna – realizowana jest praktycznie poprzez przedsięwzięcia zabezpieczenia bezpośredniego.
4. Ochrona kryptograficzna systemów teleinformatycznych – stosuje się ją przy przekazywaniu informacji w formie transmisji danych.

Powinna gwarantować następujące atrybuty:

- poufności – właściwość przypisana do danych określająca, do jakiego stopnia dane te nie mogą zostać udostępnione lub ujawnione nieuprawnionym osobom lub podmiotom;
- integralności – zabezpieczenie przed nieautoryzowaną modyfikacją danych;
- uwierzytelniania – akt weryfikacji deklarowanej tożsamości podmiotu;
- niezaprzeczalności – brak możliwości wyparcia się swego uczestnictwa w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie[54].

W przypadku dynamicznego rozwoju środowiska sieci i systemów komputerowych – cyberprzestrzeni wymiany informacji, pojawiały się nowe pojęcia związane chociażby z ochroną i zarządzaniem tego obszaru. Środowisko sieci i systemów komputerowych zwane cyberprzestrzenią jest również istotnym obszarem dla państw funkcjonujących na arenie międzynarodowej. Korzystanie z nowoczesnych technologii w cyberprzestrzeni wpływa również na poziom bezpieczeństwa państwa czy sił zbrojnych. Cyberprzestrzeń stała się nowym wymiarem prowadzenia działalności gospodarczej, funkcjonowania obywateli, obszarem walki i działalności państwa. Korzystanie z nowych rozwiązań stale będzie wymagać od wszelkich podmiotów w cyberprzestrzeni ciągłego poszerzania wiedzy i rozwiązań zwiększających poziom bezpieczeństwa w tym środowisku.

Bibliografia

1. *Decyzja 275/ MON z dnia 13.07.2015 roku w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej*, poz. 208, NCK, Dz.U. z 14.07.2015 r.
2. Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002.

[54] Por. D. L. Pipkin, *Bezpieczeństwo informacji: ochrona globalnego przedsiębiorstwa*, D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, WNT, Warszawa 2002.

3. *Global Risks 2012*, Seventh Edition.
4. *Global Risks 2014*, Ninth Edition.
5. Korycki S., *System bezpieczeństwa Polski*, Warszawa 1994.
6. Rokicka-Broniatowska A., *Wstęp do informatyki gospodarczej*, Szkoła Główna Handlowa – Oficyna Wydawnicza w Warszawie, Warszawa 2002.
7. *Strategia Bezpieczeństwa Narodowego RP*, Warszawa 2014.
8. *Strategia obronności Rzeczypospolitej Polskiej, Strategia sektorowa do strategii bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2009.
9. *Strategia Rozwoju Systemu Bezpieczeństwa Narodowego RP 2022*, Warszawa 2013.
10. *Technika informatyczna, Zabezpieczenia w systemach informatycznych, Terminologia, Polski Komitet Normalizacyjny*.
11. Wołejszo J. (red.) *Automatyzacja dowodzenia SZ RP w środowisku sieciocentrycznym*, Gdynia – Warszawa 2013.
12. www.angelfire.com (dostęp: 15.05.2016 r.).
13. www.media.wp.pl (dostęp: 04.05.2016 r.).
14. www.nowastrategia.org.pl (dostęp: 28.04.2016 r.).
15. www.polonistyka.fil.ug.edu.pl (dostęp: 10.11.2014 r.).
16. www.rp.pl (dostęp: 12.04.2016 r.).

Liczba znaków ze spacjami: 42 883