Cyberprzestrzeń – wczoraj i dziś cz. I

Geneza działań w cyberprzestrzeni w aspekcie powstawania zagrożeń militarnych

LESZEK KLICH

informatyk i programista od wielu lat projektuje bezpieczne rozwiązania informatyczne dla biznesu. Na UKSW pracuje nad dysertacją „Zagrożenia w cyberprzestrzeni jako współczesne wyzwania dla bezpieczeństwa i obronności Rzeczypospolitej Polskiej".

Wstęp

Publikacja poświęcona jest działaniom w cyberprzestrzeni. Dotyczy genezy oraz istoty zjawiska powstawania zagrożeń w aspekcie bezpieczeństwa państwa.

Jej celem jest identyfikacja wyzwań i wyodrębnienie najważniejszych uwarunkowań cyberataków na płaszczyźnie militarnej oraz wskazanie celów doskonalenia działań defensywnych i ofensywnych w Siłach Zbrojnych RP.

Nie sposób omówić zagadnienia bez przedstawienia rysu historycznego oraz determinantów, które w istotnym stopniu przyczyniły się do osłabienia bezpieczeństwa cyberprzestrzeni wielu państw. Niezbędne jest więc opisanie ewolucji technologicznej, jaka dokonała się na przełomie ostatnich dekad.

Pierwsza część publikacji dotyczy genezy zjawiska oraz wskazania uwarunkowań powstawania zagrożeń cywilnych i militarnych w cyberprzestrzeni, stanowiąc podstawę do dalszych badań nad zjawiskiem cyberataków – w tym cyberwojny.

Abstract

The publication is devoted to military activities in cyberspace. Section on the genesis of this phenomenon and essence of the emergence of risks in terms of military threats to the state requires scientific description. The aim of the publication is to present the threats and extract the most important determinants of cyber-attacks at the military level, as well as to indicate the goals for improvement of defensive and offensive operations in the Polish Armed Forces. There cannot be any discussion of the threats present in cyberspace without providing a historical view and presenting determinants which significantly contributed to the weakening of cyber security of many countries. Therefore, it is necessary to describe the technological evolution that has taken place in the last decades. The first part of the publication provides a description of the genesis of the phenomenon and indication of determinants giving rise to both civil and military threats in cyber space, while also serving as the basis for further research on the phenomenon of cyberattacks – including cyberwar.

Geneza zjawiska w ujęciu historycznym

Druga połowa XIX wieku przyniosła dynamiczny rozwój techniki i organizacji zarządzania. Postęp ten dotyczył także techniki komunikacji, czego najlepszym przykładem jest wynalezienie telegrafii oraz telefonii. Na początku XX wieku wynaleziono radiotelefon umożliwiający bezprzewodową łączność statkom, zaś rozwój druku przyczynił się do rozwoju rozpowszechnił prasy[1]. Wraz z migracją ludności następował nie tylko wzrost siły roboczej, ale i wzrost myśli technicznej i ekonomicznej. Powodowało to przyspieszenie postępu technologicznego w szeroko pojętym komunikowaniu, a zwłaszcza rewolucji w informatyce.

Trudno jednak określić, kiedy został zapoczątkowany proces komputeryzacji. Być może było to w latach czterdziestych, gdy skonstruowano pierwszy tranzystor, jednak istotnym przełomem było wyprodukowanie pierwszego mikroprocesora, który zastąpił układy lampowe. Spowodowało to gwałtowny spadek cen komputerów oraz wzrost ich mocy obliczeniowej.

Pierwsze maszyny cyfrowe pracowały dla wojska, wykonując skomplikowane obliczenia, zatem naturalną koniecznością okazała się potrzeba zapewnienia ich wzajemnej komunikacji, w celu przesyłania danych. Jednak ówczesne sieci realizowały jedynie połączenie pomiędzy komputerami bez mechanizmu routingu[2].

Idea Internetu, jako technologii sieci odpornej na atak atomowy, powstała podczas zimnej wojny, w obliczu szybko postępujących zbrojeń nuklearnych. Wówczas rząd amerykański zorientował się, że w przypadku ataku atomowego już w pierwszych minutach starcia może dojść do zniszczenia trady-

1. J. Kaliński, Globalizacja w perspektywie historycznej, w: Globalizacja od A do Z, s. 13 – 15.
2. Routing to kształtowanie ruchu w sieci za pomocą optymalnego kierowania pakietów po jak najkrótszej ścieżce.

LESZEK KLICH, PIXABAY

cyjnych środków komunikacji, co w konsekwencji może doprowadzić do przerwania łańcucha wydawania rozkazów na polu walki. Niezbędne było więc opracowanie medium transmisyjnego charakteryzującego się brakiem punktu centralnego, co mogłoby uchronić sieci wojskowe przed całkowitym paraliżem w przypadku takiego ataku[3]. Tego typu system łączności miał w założeniu umożliwić zachowanie systemu wydawania rozkazów, sprawowania kontroli i porozumiewania się podczas globalnego konfliktu[4].

W roku 1961 Leonard Kleinrock przedstawił koncepcję pakietowego przesyłu danych, polegającą na podziale danych na mniejsze zbiory. Jeżeli w trakcie transferu dochodziło do utraty pakietu, był on przesyłany ponownie, bez konieczności przesyłania wszystkich danych. Trzy lata później Paul Baran[5] z amerykańskiej instytucji zajmującej się problemami bezpieczeństwa narodowego[6] opublikował raport On Distributed Communications Networks przedstawiający propozycję zdecentralizowanej, elastycznej sieci komputerowej, której działanie nie może zostać zakłócone w przypadku awarii wielu węzłów. W następnych latach agencja DARPA utworzyła pierwszą sieć ARPANet, która była pierwszą wersją Internetu[7]. Zadaniem agencji było opracowywanie nowych technologii informatycznych dla celów wojskowych.

W 1965 roku Ted Nelson opisał koncepcję hipertekstu, czyli metody prezentacji powiązanych ze sobą informacji tekstowych. Wiele z postulowanych przez niego rozwiązań znalazło zastosowanie w późniejszej koncepcji WWW[8].

W roku 1989 Tim Berners-Lee ze szwajcarskiego instytutu cząstek elementarnych stworzył sieć, która pozwalała na przesyłanie informacji z dowolnego źródła do każdego rodzaju komputera. Dzięki temu, w niedalekim czasie, stworzono pierwszą internetową przeglądarkę[9].

Za początek komercjalizacji oraz gwałtownego rozwoju Internetu przyjmuje się lata 90. ubiegłego wieku, kiedy to dynamicznie rozwijały się nowe usługi: strony internetowe, poczta elektroniczna, wyszukiwarki, komunikatory, strumieniowe przesyłanie multimediów, sieci społecznościowe, fora, blogi i wiele innych. Na obszarze Polski, początek Internetu nastąpił w roku 1991, kiedy wykonano pierwsze połączenie z zagranicą[10].

Cyberprzestrzeń można więc traktować jako szeroko pojęty dorobek teleinformatyki, zaś skala wykorzystania tego medium jest ogromna – liczba urządzeń podłączonych do sieci w roku 2016 roku wynosi niemal 3,5 mld użytkowników i rośnie w szybkim tempie[11].

Tempo wzrostu wykorzystania cyberprzestrzeni nie wiąże się jednak wyłącznie z korzyściami dla społeczeństwa. Wraz z komputerami, ewoluowała elektroniczna walka. Początkowo „wojny" odbywały się w pamięci pojedynczego komputera, kiedy to w 1950 roku, pracownicy firmy Labs: H. Douglas McIlroy, Victor Vysottsky i Robert Morris, stworzyli podstawy gry „Wojny Rdzeniowe". Celem gry była walka programów w zwirtualizowanym środowisku, w którym każdy z walczących programów miał za zadanie zwalczyć konkurencyjny program. Gra rozpoczynała się załadowaniem dwóch programów do pamięci, przy założeniu ich losowej pozycji w rdzeniu. Zwycięstwo odnosił programista, który

3. Więcej: Krótka historia Internetu, http://www.kopernik.org.pl/przewodnik-po-wystawie/artykuly/kulturahistoria-internetu-krotka-historia-internetu (stan na 06.08.2016).
4. Więcej: Powstanie Internetu, http://www.oeiizk.edu.pl/informa/jazdzewska/ (stan na 07-08-2016.
5. Poul Baran opublikował w latach 1961 – 1964 11 prac pt. On Distributed Communications, poświęconych architekturze bezpiecznej rozproszonej komunikacji, które zainspirowały Roberts'a i Kleinrock'a zastosowania tych rozwiązań w rozproszonej architekturze sieci ARPANET.
6. Dalej: RAND Corporation.
7. Więcej: Historia Internetu, http://wiedzaiedukacja.eu/archives/47062 (stan na 07.08.2016).
8. World Wide Web.
9. P. Budzianowski, Krótka historia internetu czyli od arpanet do www.rzu.gov.pl, https://rf.gov.pl/publikacje/artykuly-pracownikow-i-wspolpracownikow/Piotr_Budzianowski_–_Krotka_historia_internetu_czyli_od_arpanet_do_www_rzu_gov_pl__35 (stan na 07.08.2016).
10. M. Grzelak, K. Liedel, Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, Bezpieczeństwo Narodowe, nr 22, II-2012, s. 125
11. Por. Internet users, http://www.internetlivestats.com/internet-users/ (stan na 05.08.2016).

stworzył najdłużej działający algorytm[12]. Wojny rdzeniowe zostały spopularyzowane w 1984 roku, gdy prof. A. K. Dewdney z University of Western Ontario opracował wraz ze swoim studentem szczegółowe reguły gry, tworząc cyfrowego arbitra walki w rdzeniu o nazwie MARS, tworząc dodatkowo składnię języka REDCODE[13].

Wraz z postępem technicznym, powstawały także wirusy komputerowe. Terminu „wirus" użył po raz pierwszy prof. Leonard M. Adleman w rozmowie telefonicznej z Fredem Cohenrem w roku 1981[14]. Wirusy to specyficzne programy zdolne do kopiowania siebie i infekowania innych programów za pomocą różnego typu nośników, w tym sieci komputerowych. Wirusy, tak jak inne oprogramowanie tego typu, zaliczane są do programów złośliwych. Stosowanie ich służy do wywoływania określonych skutków w systemach: usuwania lub modyfikacji danych, rozsyłania spamu, dokonywania ataków na serwery, kradzieży danych, niszczenia systemów czy przejęcia kontroli nad zainfekowanymi komputerami.

Współczesne oprogramowanie złośliwe jest wysoko zaawansowane, a skutki jego działania porównać można do broni masowego rażenia[15]. Jako przykład można przytoczyć atak wirusa Stuxnet[16], który zachwiał irańskim programem nuklearnym poprzez zniszczenie ponad 1 tys. wirówek oczyszczających uran w irańskich zakładach w Natanz (w pobliżu elektrowni jądrowej w Buszehr). Choć nie jest to pierwsze złośliwe oprogramowanie skierowane do zakłócenia pracy systemów sterowania czy nadzoru,[17] to jedną z jego funkcji stanowi zniszczenie istniejącego fizycznego urządzenia[18].

Oprócz coraz większej liczby osób korzystających z cyberprzestrzeni, mamy obecnie do czynienia ze wzrostem liczby po części autonomicznych urządzeń, które do komunikacji także używają sieci rozległej. Zjawisko to nazywane jest Internetem rzeczy[19], który stale się rozwija. Jest to koncepcja przedmiotów codziennego użytku, jednoznacznie identyfikowalnych, które są w stanie gromadzić, przetwarzać, bądź wymieniać dane za pośrednictwem sieci komputerowej[20].

Koncepcję tego zjawiska stworzył Kevin Ashton i zdefiniował go, jako ekosystem przedmiotów wyposażonych w sensory komunikujące się z komputerami. Obecny rozwój technologiczny spowodował, że idea ta urzeczywistniła się, stając się jednocześnie jednym z kluczowych motorów rozwojowych światowej gospodarki przyszłości. Miniaturowe dodatki do odzieży, inteligentny sprzęt domowy, automatyka budynkowa, autonomiczne samochody, inteligentne miasta, gospodarka wodna czy systemy obronne – wszystko to stanowi Internet rzeczy[21]. W rzeczywistości IoT to nie urządzenia, lecz ich wewnętrzne systemy, które umożliwiają wymianę danych z innymi urządzeniami. Skalę zjawiska można przybliżyć ilością danych transmitowanych przez te urządzenia. Według szacunków firmy Cisco, do 2018 roku grupa tych urządzeń wytwarzać będzie rocznie ponad 400 Zettabajtów danych[22]. Globalny rynek Internetu rzeczy rośnie obecnie w skali roku w tempie średnio 16,9%[23].

12. C. Fosnock, Computer Worms: Past, Present, and Future, East Carolina University, https://vxheaven.org/lib/pdf/Computer%20Worms:%20Past,%20Present,%20and%20Future.pdf, s. 2 (dostęp z dnia 08-06-2015).
13. Więcej na temat języka: http://corewar.co.uk/ryba/cws88.htm (stan na 04-08-2015).
14. Więcej: http://www.net-kom.pl/?historia-wirusow-komputerowych,31 (stan na 11.08.2016).
15. Dalej: BMR.
16. Stuxnet został odkryty w czerwcu 2010 roku, jednak zanim go zidentyfikowano, zdołał zainfekowa oraz zdestabilizować tysiące systemów sterowania w przemyśle.
17. Wcześniej wirus Flame wstrzymał prace kilku terminali naftowych, natomiast wirus Slammer doprowadził do unieruchomienia systemów bezpieczeństwa elektrowni jądrowej.
18. Zob. http://www.computerworld.pl/news/383495/Wojny.w.cyberprzestrzeni.html.
19. Dalej: IoT (ang. Internet of Things).
20. Więcej: https://pl.wikipedia.org/wiki/Internet_rzeczy (stan na 05.08.2016).
21. Internet Rzeczy w Polsce – raport, IAB Polska, http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf, s. 5.
22. Więcej: http://www.forbes.pl/czym-jest-internet-rzeczy-,artykuly,195983,1,1.html (stan na 05.08.2016).
23. IDC Publishes Three Landmark Reports in the IoT Space, http://www.idc.com/getdoc.jsp?containerId=prUS25658015 (stan na 05.08.2016).

Wzrost liczby podłączonych urządzeń do sieci Internet, to jednocześnie większa liczba dostępnych celów ataku, przez co rośnie skala negatywnej działalności podmiotów niepaństwowych i państwowych, powodując istotne zagrożenie dla współczesnych krajów, powszechnie wykorzystujących technologie teleinformatyczną. Mamy obecnie do czynienia z szybkim wzrostem szeregu negatywnych zjawisk, do których należy zaliczyć: cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych oraz cyberwojnę, rozumianą jako konfrontację pomiędzy państwami[24].

Wiele krajów, w szczególności mocarstw, dostrzega zagrożenie i przeznacza duże środki finansowe na obronę własnych systemów oraz prewencyjną ochronę. Środowiska naukowe, początkowo w państwach zachodnich, jeszcze w okresie zimnej wojny zauważyły bowiem, że rewolucja informatyczna niesie nowe, nieznane dotąd wyzwania w wymiarze politycznym, społecznym, gospodarczym, kulturowym, jak i wojskowym. W opracowaniach naukowych znaleźć można informacje o rosnących zagrożeniach dla funkcjonowania infrastruktury krytycznej kraju oraz systemu obronnego, co może skutkować m. in. poważnymi zakłóceniami w funkcjonowaniu współczesnych państw, a nawet utratą zdolności prowadzenia działań wojennych[25].

Rozwój społeczeństwa informacyjnego oraz technologii teleinformatycznych oddziałują także na Polskę, czego skutkiem była zmiana środowiska bezpieczeństwa kraju. W związku z tym, zauważyć można wzrost roli bezpieczeństwa informacyjnego – posiadającego ścisły związek z bezpieczeństwem wewnętrznym oraz zewnętrznym kraju. Bezpieczeństwo informacyjne rozpatrywane jest często jako część bezpieczeństwa informatycznego, w odniesieniu do narzędzi i procedur ochrony danych, informacji i systemów informacyjnych[26]. Istotne jest jednak rozszerzenie ujęcia bezpieczeństwa nie tylko do sfery technicznej, ale także do przestrzeni osobowej, ponieważ głównym emiterem informacji jest człowiek[27]. W związku z tym należy przyjmować, że bezpieczeństwo informacyjne funkcjonuje w powiązaniu z szeregiem tradycyjnych wymiarów bezpieczeństwa państwa[28]. Warto także podkreślić znaczenie walki informacyjnej, jako istotnej pozycji zarówno w otoczeniu zewnętrznym, jak i w otoczeniu wewnętrznym państwa, stanowiącej zagrożenie dla wszystkich sfer działalności – zarówno państwa, jak i jednostki.[29]

Badając zjawisko zagrożeń w cyberprzestrzeni, można nakreślić trendy rozwoju zagrożeń cybernetycznych, które wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne kraju. Zagrożenia te wynikają wprost z uzależnienia od technologii teleinformatycznej współczesnych krajów[30].

Nierozerwalnym zjawiskiem powiązanym z cyberprzestrzenią jest transgraniczność, która w sposób nierozerwalny wiąże się z powstawaniem nowych trendów oraz procesów ewolucyjnych zagrożeń, obejmujących następujące, kluczowe zjawiska[31]:

- ✓ stały wzrost uzależnienia technologicznego na fundamentalne procesy biznesowe przy jednoczesnym rozmywaniu się granic międzyśrodowiskowych oraz procesów zarządzania przez poszczególne organizacje;
- ✓ wzrost profesjonalizacji ataków, który związany jest z doskonaleniem metod wypracowanych przez tradycyjne organizacje przestępcze – w tym przenoszenie tradycyjnych przestępstw do cyberprzestrzeni;
- ✓ zmiany technologiczne, będące między innymi efektem popularyzacji mobilnego przetwarzania

24. Strategia Bezpieczeństwa Narodowego 2014, s. 17.
25. M. Lakomy, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Uniwersytet Śląski, Katowice 2015, s. 8.
26. P. Sienkiewicz, Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni, Automatyka 2009 Tom 13, zeszyt 2, s. 588.
27. A. Żebrowski, Bezpieczeństwo informacyjne Polski a walka informacyjna, Roczniki Kolegium Analiz Ekonomicznych, nr 29/2013, s. 453.
28. Tamże, s. 16.
29. A. Żebrowski, Bezpieczeństwo informacyjne Polski a walka informacyjna, Roczniki Kollegium Analiz Ekonomicznych nr 29/2013, Uniwersytet Pedagogiczny w Krakowie, http://rocznikikae.sgh.waw.pl/p/roczniki_kae_z29_30.pdf, s. 447 (stan na 02-04-2013).
30. Zob. Strategia Bezpieczeństwa Narodowego 2014, http://www.bbn.gov.pl/ftp/SBN%20RP.pdf, s. 19.
31. A. Adamski, Przestępczość w cyberprzestrzeni, Dom Organizatora, Toruń 2001, s. 74.

danych oraz zwiększania się oddziaływania na społeczeństwo serwisów społecznościowych;
- ✓ znaczne osłabianie metod ochrony infrastruktury informatycznej, chronionej za pomocą dotychczasowych metod, do których zaliczyć można programy antywirusowe, zapory sieciowe czy aktywne systemy identyfikacji zagrożeń,
- ✓ silna presja czasu oraz kosztów, która ogranicza nakłady inwestycyjne na technologiczne i osobowe środki ochrony informacji, co jest obecnie warunkowane tradycyjnym modelem zwrotu z nakładów inwestycyjnych.

Czynniki te obecnie oddziałują na efektywność obszaru bezpieczeństwa, co z kolei powoduje wzrost presji na osoby odpowiedzialne za wybór rozwiązań bezpieczeństwa, przy równoczesnym zapewnieniu ich efektywności finansowej[32].

Jednym z efektów oddziaływania cyberprzestrzeni na systemy gospodarcze jest coraz większa globalizacja rynków, powiązanych poprzez międzynarodowe korporacje. Nie jest to zjawisko nowe. Już podczas wielkich odkryć geograficznych odkrywano nowe rynki, a towarzyszyły temu wielkie migracje ludzi. W epoce wiktoriańskiej handlowano towarami nie mniej intensywnie niż dziś[33]. Nie można jej ujmować wyłącznie jako procesu ekonomicznego, gdyż odbywa się na wielu płaszczyznach i powiązaniach ze wszystkimi dziedzinami życia społeczeństw. Paweł Dembiński, określił globalizację jako kurczącą się czasoprzestrzeń – nie w znaczeniu fizycznym, lecz jako głębokie odczucie, które przenika nas na wylot. Zaznaczył jednocześnie, że fakt tworzącej się globalizacji wynika z ciągłego zacieśniania się więzów współzależności – przede wszystkim między aktorami gospodarczymi, ale nie tylko. Globalizacja, jak pisze dalej autor, oznacza pewną wzajemną korelację, w której państwa współzależą od siebie. W cybernetyce taka współzależność nazywana jest sprzężeniem zwrotnym.[34] Globalizacja jest nieodłącznie związana z osieciowieniem, ponieważ cyberprzestrzeń jest jednym z determinantów wzrostu tego zjawiska (cyberprzestrzeń można traktować jednocześnie jako zasób oraz medium).

Istnienie w cyberprzestrzeni wielu podmiotów współzależnych, np. organizacji i systemów, generuje szereg istotnych problemów w obronie przed cyberatakami. W przypadku ataku na jeden z systemów lub organizację, uszkodzenie jednego z krytycznych punktów może powodować paraliż lub zakłócenia w działaniu innych punktów od niego zależnych. W przeszłości wiele elementów wchodzących w skład infrastruktury krytycznej funkcjonowało od siebie niezależnie bądź zależne w niewielkim stopniu. Niestety, postępująca globalizacja oraz rozwój technologiczny systemów infrastruktury krytycznej w coraz większym stopniu są ze sobą skorelowane w skali regionalnej, państwowej, a nawet międzynarodowej.[35]

Identyfikacja zagrożeń w cyberprzestrzeni

W Strategii Rozwoju Systemu Bezpieczeństwa Narodowego RP przewiduje się, że bezpieczeństwo narodowe Polski w drugiej dekadzie XXI kształtowane będzie dynamicznym procesem identyfikacji zagrożeń, podejmowania wyzwań, definiowania celów i sposobów ich realizacji. Jednocześnie prognozuje się występowanie sieci instytucji międzynarodowych i narodowych odpowiedzialnych za bezpieczeństwo, przy jednoczesnej integracji wysiłków cywilno-wojskowych. Kompleksowość i wieloaspektowość bezpieczeństwa państwa polskiego determinuje ścisłą integrację podstawowych dziedzin bezpieczeństwa zewnętrznego, militarnego, ekonomicznego, społecznego, ekologicznego, itd. oraz stale rosnące powiązania go z rozwojem gospodarczo-społecznym kraju[36].

Rozwój zagrożeń w cyberprzestrzeni powoduje, że zachowanie bezpieczeństwa przestrzeni tworzonej przez systemy teleinformatyczne, usługi, wraz z relacjami z użytkownikami jest obecnie istotnym problemem na poziomie krajowym i międzynarodowym. Tymczasem raporty krajowe i zagraniczne, publikowane przez zespoły reagujące CERT[37], agencje Unii Europejskiej[38] oraz firmy komercyjne alarmują, że techno-

32. Tamże.
33. E. Czarny, Wstęp, w: Globalizacja od A do Z, s. 5.
34. Zob. Paweł H. Dembiński, Globalizacja. Wyzwanie i szansa, http://porozumienie.kik.opoka.org.pl/tekst/gl/dembinski.html.
35. Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022, s. 24.
36. Szerzej: Strategia Rozwoju Systemu Bezpieczeństwa Narodowego RP 2022, s. 7, 32.
37. Computer Emergency Response Team. Zespół powołany do reagowania na zdarzenia naruszające bezpieczeństwo w sieci Internet.
38. Np. ENISA, EC3/ Europol.

logiczne zagrożenia bezpieczeństwa są coraz bardziej zaawansowane, zaś skala incydentów rośnie z roku na rok. Wzrasta także przestępczość opierająca się na nielegalnej działalności w cyberprzestrzeni[39].

Polski zespół CERT ostrzegł w raporcie Krajobraz bezpieczeństwa polskiego Internetu w 2015, że cyberprzestrzeń stała się otwarcie i jawnie, piątym polem walki (cyber-walki), co stało się jasne dzięki ujawnieniu zakresu internetowej działalności szpiegowskiej i sabotażowej[40]. Raport pozwala zapoznać się z najnowszymi wyzwaniami w cyberprzestrzeni, które mogą oddziaływać na krajowe sieci informatyczne. Przede wszystkim w 2015 roku zespół zaobserwował wzmożenie ataków ukierunkowanych[41], skierowanych przeciwko dużym instytucjom oraz firmom. Pojawiły się także nowe rodzaje ataków złośliwego oprogramowania atakującego polskie systemy bankowe, które dotychczas były używane wyłącznie do ataków na banki zachodnie. Zidentyfikowano także coraz bardziej wyrafinowane oprogramowanie złośliwe szyfrujące dane[42] dedykowane również systemom Android, a co gorsze – Linux[43], który to system uważany był dotychczas za o wiele bezpieczniejszy niż popularny system Windows. Stale wzrasta także liczba banków oraz ich klientów, będących celami phishingu,[44] zaś fałszywe strony coraz częściej utrzymywane są na polskich serwerach. Liczba znanych serwerów sterujących botnetami[45] nie zmieniła się znacząco, ale zwrócono uwagę na zwiększenie ich odporności na przejęcie poprzez zastosowanie algorytmicznego generowania nazw domen. Co istotne – zostały ujawnione podatności w używanych powszechnie bibliotekach kryptograficznych spowodowane błędami w ich kodzie oraz sposobach ich użycia, a dzięki temu, skrócony został czas potrzebny na ich złamanie[46].

Dynamiczny rozwój oprogramowania dedykowanego dla cyberprzestępców to niebezpieczna tendencja. Dodatkowo osoby lub grupy dokonujące ataków nie muszą obecnie dysponować wiedzą na temat bezpieczeństwa systemów do przeprowadzenia ataku. Narzędzia ewoluują w niebezpiecznym kierunku, gdzie każdy informatyk może stać się potencjalnym cyberprzestępcą poprzez pozyskanie tego typu narzędzi bez posiadania szczegółowej wiedzy na temat ich działania. Badania wskazują, że choć liczba i złożoność ataków rośnie, wiedza atakujących spada[47].

Klasycznym przykładem dokonania cyberataków na inne państwo było zablokowanie dostępu do prezydenta i parlamentu, partii politycznych, wszystkich ministerstw, mediów, systemów bankowych i sieci komórkowych Estonii w 2007 roku. Dodatkowo została odcięta łączność tego kraju z Unią Europejską[48]. O przeprowadzenie ataków oskarżono Rosję, jednak nie udało się zebrać dowodów pozwalających stwierdzić, że władze tego kraju były za nie formalnie odpowiedzialne[49]. 8 kwietnia 2010 roku Kongres USA

39. System Bezpieczeństwa Cyberprzestrzeni, NASK, Warszawa 2015, s. 1.
40. Raport dostępny pod adresem: https://www.cert.pl/news/single/krajobraz-bezpieczenstwa-polskiego-internetu-2015-raport-roczny-naszej-dzialalnosci/ (stan na 07.08.2016).
41. Ataki ukierunkowane APT (ang. Advanced Persistent Threats), są złożonymi, długotrwałymi i wielostopniowymi działaniami kierowanymi przeciwko konkretnym celom.
42. Chodzi tutaj o oprogramowanie typu ransom (okup), które szyfruje automatycznie dane osobiste użytkownika i wymaga okupu za ich odszyfrowanie.
43. Wolny system operacyjny z rodziny Unix, stworzony przez Linusa Torvaldsa.
44. Metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję, w celu wyłudzenia określonych informacji (np. danych logowania, szczegółów karty kredytowej) lub nakłonienia ofiary do określonych działań. Więcej: https://pl.wikipedia.org/wiki/Phishing.
45. Botnet to grupa komputerów zainfekowanych złośliwym oprogramowaniem pozostającym w ukryciu przed użytkownikiem i pozwalającym kontrolującym jego twórcom na zdalną kontrolę, która może powodować zdalne rozsyłanie spamu oraz inne ataki z użyciem zainfekowanych komputerów.
46. Tamże.
47. M. Kurek, A. Ludynia, Zagrożenia związane z udostępnianiem aplikacji w sieci Internet, Ogólnopolska Konferencja Informatyki Śledczej z dnia 8-9 stycznia 2009, Ernst & Young, s. 7.
48. E. Lichocki, Bezpieczeństwo teleinformatyczne Sił Zbrojnych RP w dobie zagrożeń cybernetycznych, s.1.
49. M. Grzelak, K. Liedel, Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, https://www.bbn.gov.pl/.../str125-139MichalGrzelakKrzysztofLiedel.pdf (stan na 06.08.2016).

otrzymał informację o przekierowaniu przez Chiny 15% danych transmitowanych między instytucjami państwowymi USA. W rezultacie przez 18 minut, ruch internetowy amerykańskiego Senatu, Departamentu Obrony, NASA oraz Departamentu Handlu skierowany był przez Chiny. Tego typu działanie mogło spowodować wyciek danych i narazić USA na kolejne ataki. Przeanalizowany ruch sieciowy przez Chiny mógł służyć do uzyskania dodatkowych informacji niezbędnych do planowania przyszłych ataków na cele w USA[50].

W styczniu 2012 roku za pomocą sieci botnet zaatakowano polskie strony rządowe. Wyspecjalizowane grupy cyberprzestępców koordynowały te ataki pod pretekstem sprzeciwu wobec wprowadzenia przez rząd międzynarodowego porozumienia ACTA (ang. Anti-Counterfeiting Trade Agreement). W wyniku tych działań czasowo niedostępne były serwisy m. in. Kancelarii Premiera, Sejmu, czy Ministerstwa Kultury[51]. Choć w rzeczywistości ataki na polskie serwisy rządowe nie stanowiły realnego zagrożenia dla bezpieczeństwa kraju, wykazały słabość państwa w ochronie cyberprzestrzeni. Do ataków odniósł się w sposób istotny Stanisław Koziej, który stwierdził, że żadne ataki w cyberprzestrzeni nie mogą być lekceważone w przyszłości, a przekaz medialny uświadomił społeczeństwu znaczenie bezpieczeństwa tego obszaru[52].

Ataki w cyberprzestrzeni wyróżnia często niepaństwowy charakter oraz anonimowość, co utrudnia bądź też uniemożliwia identyfikację przeciwnika. Świadczyć o tym może m.in. raport przygotowany dla Amerykańsko-Chińskiej Rewizyjnej Komisji Gospodarczej i Bezpieczeństwa, który uwzględniał cybernetyczne włamania i zakłócenia w Chinach po 1999 r. Dowiódł on, że w większości dokonanych ataków w cyberprzestrzeni, ich źródło było niemożliwe do zidentyfikowania[53]. Zauważyć także należy zatarcie granic w cyberprzestrzeni pomiędzy sferą cywilną a wojskową, co wymusza potrzebę opracowania nowych form ochrony, niezależnie od obszaru, którego zagrożenia te dotyczą. Należy również uwzględnić możliwość jednoczesnego cyberataku na obiekty wojskowe oraz cywilne, więc naturalną potrzebą jest zdolność ich współpracy oraz komunikacji, bez których atak może skazać państwo na porażkę[54].

Na polu walki od zawsze największe znaczenia miała informacja, która jest warunkiem koniecznym do osiągnięcia celu. Przewagę informacyjną można rozumieć jako posiadanie większych zasobów informacji od strony przeciwnej, ale także sprawniejsze ich wykorzystanie. Umożliwiają to szybkie systemy i technologie informacyjne, co wymusza konieczność ich ochrony przed negatywnym oddziaływaniem strony przeciwnej[55].

Obecne ujęcie pola walki uległo przekształceniu, a broń operująca w cyberprzestrzeni dołączyła do arsenału środków walki. Narzędzia cybernetyczne – także przeznaczone do uderzeń na cele cywilne, mogą być wykorzystywane na skalę agresji militarnej, o czym zdano sobie sprawę po ataku na WTC[56] w Stanach Zjednoczonych. Na świecie odnotowuje się stały wzrost zainteresowania militarnym i wywiadowczym zastosowaniem nowych technologii informatycznych do walki informacyjnej[57].

W strukturze armii Chin wykryto jednostkę 61398, której zadania dotyczą operacji w cyberprzestrzeni. Jak wynika z raportu firmy Mandiant, za atakami na amerykańskie firmy stała chińska armia powiązana z jednostką 61398[58]. Zamrożony konflikt pomiędzy Chinami a USA trwa od lat, zaś amerykański Google podejrzewa hackerów z Chin powiązanych z chińskim rządem m.in. o atak na serwery z 2009 roku, kiedy doszło do kradzieży kont działaczy na rzecz praw człowieka w Chinach[59].

Agencja Wywiadowcza Departamentu Obrony USA opublikowała

50. Chiny przechwyciły ruch internetowy USA, więcej: http://goo.gl/5qJ2bj (21.12.2011).
51. Zob. Biuletyn analityczny nr 2, Rządowe Centrum Bezpieczeństwa, http://rcb.gov.pl/wp-content/uploads/biuletyn/2.pdf, s. 7.
52. Zob. http://www.bbn.gov.pl/pl/wydarzenia/3643,dok.html (stan na 25-01-2012).
53. J. Fallows, Cyber Warriors, 2010, s. 60, cyt. za: J. Świątkowska, I. Bunsch, Cyberterroryzm. Nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku, Instytut Kościuszki, s. 2.
54. Polityka ochrony cyberprzestrzeni RP, s. 5.
55. G. Nowacki, Znaczenie informacji w obszarze bezpieczeństwa narodowego, WAT, s. 113.
56. World Trade Center.
57. R. Tarnogórski, Prawo konfliktów zbrojnych a cyberprzestrzeń, Biuletyn Polskiego Instytutu Spraw Międzynarodowych, Nr 31 (1007) 26 marca 2013, PISM, s. 1.
58. Więcj: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (stan na 08.08.2016).
59. Zob. http://di.com.pl/sa-dowody-ze-chinska-armia-robi-cyberataki-na-amerykanskie-firmy-47580 (stan na 08.08.2016).

dane o największych i najbardziej niebezpiecznych państwach w cyberprzestrzeni. Dokonano także podziału na uczestników związanych z agencjami wywiadowczymi państw – w tym działających bez wsparcia własnych rządów. Wśród wymienionych krajów pojawią się Chiny, Rosja, Iran oraz Korea Północna. Jeśli chodzi o kradzież tajemnic handlowych czy technologii, jako największe zagrożenie wskazano Chiny, zaś największym zainteresowaniem specjalistów tego państwa cieszą się rozwiązania technologiczne wykorzystywane przez obce armie[60].

Kolejnym zagrożeniem dla wielu państw jest Rosja, która rozwija własną cyberarmię. Kraj ten budzi poważne obawy ze względu na dokonywanie ataków na infrastrukturę krytyczną innych państw, nawet mimo wykrycia tego typu działalności. Głównym kierunkiem cyberdziałań Rosji jest wywiad, który na podstawie zdobytych informacji umożliwia podejmowanie odpowiednich decyzji geopolitycznych[61].

Współcześnie granice pomiędzy środowiskiem wewnętrznym i zewnętrznym, militarnym i pozamilitarnym zostały zatarte, zaś globalizacja i wzrastająca współzależność skutkuje nieprzewidywalnością zjawisk, co zostało zaakcentowane w najnowszej Strategii Bezpieczeństwa Narodowego RP[62].

Wyraźnie dostrzec można wzrost znaczenia działań hybrydowych lub też, jak należałoby obecnie stwierdzić – wojny hybrydowej, rozumianej jako strategii połączenia działań tradycyjnych oraz informacyjnych, łączącej różnorodne elementy działań charakterystycznych dla wojny konwencjonalnej, nieregularnej, cybernetycznej[63]. Wojna hybrydowa, prowadzona także bez jej wypowiedzenia, może stanowić niezwykle agresywną i złożoną formę działań wojennych.[64]

W nadchodzących dekadach prognozuje się wzrost wyzwań i zagrożeń transnarodowych i asymetrycznych, do których zalicza się również terroryzm w cyberprzestrzeni oraz wzrost rywalizacji i konfrontacji pomiędzy podmiotami zarówno niepaństwowymi, jak i między państwami[65]. Zapewnienie ochrony cyberprzestrzeni RP jest więc jednym z istotnych wyzwań, którym Polska będzie musiała stawić czoło w perspektywie nadchodzącego dwudziestolecia[66].

Wnioski

O skali problemów wynikających z konieczności ochrony cyberprzestrzeni i konieczności podjęcia wyzwań z tym związanych świadczy choćby zapis w Strategii Bezpieczeństwa Narodowego RP o potrzebach zapewnienia ochrony podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni. Działania zmierzające do zwiększenia bezpieczeństwa tego obszaru muszą opierać się na identyfikacji i ściganiu sprawców, prowadzeniu walki informacyjnej oraz konieczności podejmowania działań profilaktycznych[67].

Konieczność rozwijania ochrony własnych zasobów teleinformatycznych – w tym doskonalenia ochrony infrastruktury krytycznej nie budzi wątpliwości, zaś ilość wyzwań tworzy nowe obszary zainteresowania dla teoretyków i praktyków bezpieczeństwa.

Cyberataki na cywilne i wojskowe systemy teleinformatyczne posiadają szereg istotnych atutów w porównaniu z atakami tradycyjnymi. Należy wymienić choćby niższe koszty przeprowadzenia ataku w cyberprzestrzeni oraz możliwość wynajęcia grupy cyberprzestępczej, co pozwala na przeprowadzenie ukierunkowanego ataku[68] lub szeregu ataków zarówno na cele cywilne, jak i państwowe. Istotną zaletą tego typu negatywnej działalności w cyberprzestrzeni jest możliwość przeprowadzenia ataku na dowolne państwo przy zachowaniu wysokiego poziomu anonimowości w celu utrudnienia identyfikacji oraz motywów ataku.

Rozwinięciem niniejszej części publikacji będzie kolejna część, opisująca obecny poziom zagrożeń militarnych w kontekście cyberwojny.

60. Zob. http://www.cyberdefence24.pl/423842,wywiad-usa-wskazuje-najwiekszych-graczy-w-cyberprzestrzeni (stan na 08.08.2016).
61. Tamże.
62. Strategia Bezpieczeństwa Narodowego 2014, s. 17.
63. Defense lacks doctrine to guide it through cyberwarfare, nextgov.com. Auditors Find DoD Hasn't Defined Cyber Warfare, darkreading.com.
64. War on Terrorism: Defining "hybrid warfare",canadafreepress.com (stan na 10-01-2016).
65. Biała Księga Bezpieczeństwa Narodowego RP, s. 12.
66. Tamże, s. 13.
67. Strategia Bezpieczeństwa Narodowego 2014, s. 35.
68. Szerzej: https://blog.trendmicro.pl/2015/10/05/slow-kilka-o-atakach-ukierunkowanych.

Bibliografia

1. A. Adamski Przestępczość w cyberprzestrzeni, Dom Organizatora, Toruń 2001.
2. Auditors Find DoD Hasn't Defined Cyber Warfare, darkreading.com.
3. Biała Księga Bezpieczeństwa Narodowego RP.
4. Biuletyn analityczny nr 2, Rządowe Centrum Bezpieczeństwa, http://rcb.gov.pl/wp-content/uploads/biuletyn/2.pdf.
5. P. Budzianowski Krótka historia internetu czyli od arpanet do www.rzu.gov.pl, https://rf.gov.pl/publikacje/artykuly-pracownikow-i-wspolpracownikow/Piotr_Budzianowski_–_Krotka_historia_internetu_czyli_od_arpanet_do_www_rzu_gov_pl__35 (stan na 07.08.2016).
6. E. Czarny Wstęp, w: Globalizacja od A do Z, Warszawa 2004.
7. Defense lacks doctrine to guide it through cyberwarfare, nextgov.com.
8. P.H. Dembiński Globalizacja. Wyzwanie i szansa, http://porozumienie.kik.opoka.org.pl/tekst/gl/dembinski.html.
9. J. Świątkowska, I. Bunsch Cyberterroryzm. Nowa forma zagrożenia bezpieczeństwa międzynarodowego w XXI wieku, Instytut Kościuszki.
10. C. Fosnock Computer Worms: Past, Present, and Future, East Carolina University, https://vxheaven.org/lib/pdf/Computer%20Worms:%20Past,%20Present,%20and%20Future.pdf, s. 2 (dostęp z dnia 08-06-2015).
11. M. Grzelak, K. Liedel Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu, Bezpieczeństwo Narodowe, nr 22, II-2012.
12. 1Historia Internetu, http://wiedzaiedukacja.eu/archives/47062 (stan na 07.08.2016).
13. http://di.com.pl/sa-dowody-ze-chinska-armia-robi-cyberataki-na-amerykanskie-firmy-47580 (stan na 08.08.2016).
14. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf (stan na 08.08.2016).
15. http://www.bbn.gov.pl/pl/wydarzenia/3643,dok.html (stan na 25-01-2012).
16. http://www.computerworld.pl/news/383495/Wojny.w.cyberprzestrzeni.html.
17. http://www.cyberdefence24.pl/423842,wywiad-usa-wskazuje-najwiekszych-graczy-w-cyberprzestrzeni (stan na 08.08.2016).
18. https://pl.wikipedia.org/wiki/Internet_rzeczy (stan na 05.08.2016).
19. IDC Publishes Three Landmark Reports in the IoT Space, http://www.idc.com/getdoc.jsp?containerId=prUS25658015 (stan na 05.08.2016).
20. Internet Rzeczy w Polsce – raport, IAB Polska, http://iab.org.pl/wp-content/uploads/2015/09/Raport-Internet-Rzeczy-w-Polsce.pdf.
21. Internet users, http://www.internetlivestats.com/internet-users (stan na 05.08.2016).
22. Krótka historia Internetu, http://www.kopernik.org.pl/przewodnik-po-wystawie/artykuly/kulturahistoria-internetu-krotka-historia-internetu (stan na 06.08.2016).
23. Kurek M., Ludynia A., Zagrożenia związane z udostępnianiem aplikacji w sieci Internet, Ogólnopolska Konferencja Informatyki Śledczej z dnia 8-9 stycznia 2009, Ernst & Young.
24. M. Lakomy Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Uniwersytet Śląski, Katowice 2015, s. 8.
25. E. Lichocki Bezpieczeństwo teleinformatyczne Sił Zbrojnych RP w dobie zagrożeń cybernetycznych.
26. G. Nowacki Znaczenie informacji w obszarze bezpieczeństwa narodowego, WAT.
27. Polityka ochrony cyberprzestrzeni RP.
28. Powstanie Internetu, http://www.oeiizk.edu.pl/informa/jazdzewska/ (stan na 07-08-2016.
29. https://www.cert.pl/news/single/krajobraz-bezpieczenstwa-polskiego-internetu-2015-raport-roczny-naszej-dzialalnosci/ (stan na 07.08.2016).
30. P. Sienkiewicz Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni, Automatyka 2009 Tom 13, zeszyt 2.
31. Strategia Bezpieczeństwa Narodowego 2014.
32. Strategia Rozwoju Systemu Bezpieczeństwa Narodowego RP 2022.
33. Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022.
34. System Bezpieczeństwa Cyberprzestrzeni, NASK, Warszawa 2015.
35. R. Tarnogórski Prawo konfliktów zbrojnych a cyberprzestrzeń, Biuletyn Polskiego Instytutu Spraw Międzynarodowych, Nr 31 (1007) 26 marca 2013, PISM.
36. War on Terrorism: Defining "hybrid warfare",canadafreepress.com (stan na 10-01-2016).
37. http://corewar.co.uk/ryba/cws88.htm (stan na 04-08-2015).
38. http://www.forbes.pl/czym-jest-internet-rzeczy-,artykuly,195983,1,1.html (stan na 05.08.2016).
39. http://www.net-kom.pl/?historia-wirusow-komputerowych,31 (stan na 11.08.2016).
40. J.W. Wójcik Oszustwa finansowe. Zagadnienia kryminologiczne i kryminalistyczne, Wydawnictwo JWW, Warszawa 2008.
41. A. Żebrowski Bezpieczeństwo informacyjne Polski a walka informacyjna, Roczniki Kolegium Analiz Ekonomicznych, nr 29/2013, s. 453.