ISSN 2078–4333. Вісник Львівського університету. Серія міжнародні відносини. 2017. Випуск 41. С. 53–64
Visnyk of the Lviv University. Series International Relations. 2017. Issue 41. P. 53–64

УДК 327:341

WYBRANE ASPEKTY CYBERZAGROŻEŃ W KONTEKŚCIE BEZPIECZEŃSTWA PAŃSTWA I SPOŁECZEŃSTWA

Marek Górka

Wydzial Humanistyczny Politechnika Koszalicska,
ul. Kwiatkowskiego, 6d/7, Koszalin, Polska,
e-mail: marek_gorka@wp.pl

Szybkie tempo rozwoju technologicznego w dziedzinie technologii informacyjno-komunikacyjnych spowodował uzależnienie infrastruktury publicznej i prywatnej od cyberprzestrzeni. Powszechne stosowanie technologii informatycznych wprowadza nowe zagrożenia. Ryzyko zaistnienia tragicznych wydarzeń zwięzanych z funkcjonowaniem cyberprzestrzeni zaczęło grozić infrastrukturze krytycznej, która definiowana jest jako niezbędny element dla funkcjonowania społeczeństwa i gospodarki. Cyberbezpieczeństwo stało się jednym z najpoważniejszych problemów zwięzanych z bezpieczeństwem narodowym. Zakres wyzwań i zagrożeń zwięzanych z cyberprzestrzenię obejmuje wiele aspektów życia codziennego, poczęwszy od prywatności, strat finansowych, szkód i zniszczeń fizycznych a skończywszy na niekorzystnym wpływie na skuteczność prowadzenia polityki przez rzęd. Te wyzwania i zagrożenia odzwierciedla szeroki zakres, w którym komputery będę inne urzędzenia technologiczne mogę stanowic broń dla wrogo nastawionych osób będź grup i organizacji.

Slowa kluczowe: cyberbezpieczeństwo; cyberprzestrzeń; cyberwojna; cyberatak; cyberwywiad; cyberprzestępstwo.

Wstęp

Coraz większe znaczenie jakie odgrywa cyberprzestrzeń w zakresie polityki bezpieczeństwa, powoduje pojawienie się wielu wyzwań co do metod i narzędzi zarządzania konfliktem na płaszczyźnie politycznej czy też militarnej. Rodzę się także wątpliwości powodowane napięciami między kwestiami prywatności, wolności informacji i bezpieczeństwa narodowego. Wyrafinowane metody stosowane w wielu incydentach cybernetycznych (o podłożu ekonomicznym bądź politycznym) stanowią przyczynek do podjęcia próby zrozumienia pojęć z zakresu zagrożeń, taktyki i procedur używanych w cyberprzestrzeni.

Współczesnym więc wyzwaniem na płaszczyźnie praktycznej jak i teoretycznej jest analiza możliwości i sposobów aktywnego reagowania na cyberzagrożenia. Zrozumienie badanych zjawisk jest dużym wyzwaniem badawczym, bowiem ich natura jest złożona. Cyberprzestrzeń bowiem obecna jest zarówno w wymiarze ponadnarodowym jak i jednostkowym, występuję też na płaszczyźnie politycznej, militarnej jak i gospodarczej, a przede wszystkim zaznacza swoje znaczenie w sensie globalnym oraz lokalnym.

Artykuł ma na celu podkreślenie ciągłego zagrożenia bezpieczeństwa cybernetycznego wobec różnych grup odbiorców. W tym sensie praca jest także próbą usystematyzowania wiedzy oraz wybranych definicji z obszaru cyberbezpieczeństwa. Jednym z planowanych zadań badawczych w artykule jest skonfrontowanie

podobieństw i różnic między takimi zjawiskami jak: cyberprzestępstwo, cyberatak, cyberwojna, cyberwywiad oraz cyberpropaganda.

Pytanie typu w jakim stopniu współczesne państwo może być narażone na cyberataki, nie jest tylko wyzwaniem dla służb odpowiedzialnych za bezpieczeństwo państwa, ale jest również problemem badawczym, z którym zmierzyć musi się nauka. Praca jest także okazja do podjęcia refleksji na temat tego, jaka forma zagrożeń (cyber czy konwencjonalna) w pierwszej dekadzie XXI wieku jest najbardziej prawdopodobnym zagrożeniem dla bezpieczeństwa narodowego?

Najnowsze rozwiązania technologiczne zwiększają powagę zagrożeń nad dotychczasowymi, klasycznymi wyzwaniami wobec bezpieczeństwa narodowego, wzbudzają również szereg lęków i niepokojów zarówno na międzynarodowym jak i lokalnym poziomie. Pojęcie bezpieczeństwa stopniowo ewoluowało, zwłaszcza od czasu rozpadu Związku Radzieckiego i końca zimnej wojny. Jednocześnie globalizacja zmieniła międzynarodowe zasady oraz normy codziennego życia, ułatwiła i przyspieszyła przepływ kapitału oraz technologii, z jednoczesnym osłabieniem barier narodowych.

Literatura przedmiotu

W literaturze przedmiotu pojęcie cyberbezpieczeństwa postrzegane jest niezwykle szeroko. Fakt ten wynika przede wszystkim z wielopoziomowej interpretacji tego zjawiska. W artykule jednak definicja ta wpisana jest w ramy instytucjonalne. Dlatego też analizowane pojęcia odnoszą się do zagrożeń dla instytucji oraz organizacji spowodowanych przez technologię cyfrową. Warto zatem przedstawić aktualne prace badawcze, które korespondują z tematem artykułu oraz stanowią oparcie dla określenia zakresu analizowanego obszaru badawczego. Wiele współczesnych badań podkreśla złożoną naturę zachodzących procesów w obszarze cyberbezpieczeństwa. Przykładem tego jest książka Amos N. Guiora *Cyber-Security*, w której autor prezentuje dylematy z jakimi borykają się pracodawcy, liderzy korporacji, czy też przywódcy polityczni[10].

Szybkość i złożoność cyberataków wymaga innego podejścia do zarządzania bezpieczeństwem. Peter Trim i David Upton autorzy pracy *Cyber Security Culture*, podkreślają znaczenie dostosowania tempa pracy do zmieniających sie warunków otoczenia w cyberprzestrzeni [5]. W ten sposób zmiana podejścia - przy zastosowaniu aktualnych i rzetelnych systemów oraz procedur bezpieczeństwa - może pomóc instytucjom tworzyć politykę zapobiegania cyberprzestępstwom.

Dzisiejsza gospodarka cyfrowa jest wyjątkowo uzależniona od Internetu, jednak niewielu użytkowników lub decydentów posiada wystarczająca wiedzę w obszarze cyberzagrożeń. Ponadto wszelkiego rodzaju formy cyberprzestępczości stanowią główne zagrożenie dla integralności i dostępności danych oraz systemów komputerowych. Bezprecedensowym wyzwaniem jakie stoi przed każdą instytucją to zagrożenie ze strony cybertechnologii. Jest to o tyle ważny i wciąż nierozwiązany problem, bowiem jak wskazuje Mark Johnson w książce *Cyber Crime, Security and Digital Intelligence* cyberprzestępczość jest zjawiskiem dynamicznym i wciąż jego forma ewoluuje, stwarzając ustawicznie nowe wyzwania [11].

Praca pod tytułem *Cyber Power* autorstwa Solange Ghernaouti-Helie rozwija podejścia do kluczowych kwestii bezpieczeństwa cybernetycznego, wyjaśniając podstawowe zasady cyberprzestrzeni w sposób interdyscyplinarny [8]. Okazuje się zatem, że problematyka cyberbezpieczeństwa jest przestrzenią złożoną i aby ją zrozumieć warto stosować metody badawcze z odmiennych dziedzin naukowych.

W podobnym tonie wypowiada się Myriam Dunn Cavelty w pracy *Cyber-Security and Threat Politics*, która definiuje cyberzagrożenia w perspektywie ich natury [3]. Książka stara sie odpowiedzieć na pytania: na jakich warunkach, przez kogo, dla jakich przyczyn oraz konsekwencji stosowane są cyberataki w przestrzeni publicznej?

Kluczem do wyselekcjonowania podobieństw jak i różnic pomiędzy zachodzącymi cyberprocesami może być - zdaniem Jamesa Grahama, Ryana Olsona, Ricka Howarda redaktorów książki *Cyber Security Essentials* - m.in. analiza metod oraz motywacji cyberataków oraz najnowszych kierunków zagrożeń [4]. Dlatego też istotnym czynnikiem dla określenia poziomu cyberbezpieczeństwa jest czynnik ludzki. Pomimo tego, że większość organizacji przywiązuje dużą wagę do bezpiecznego przechowywania danych, to jednak nie każda organizacja inwestuje w szkolenia swoich pracowników. Joanna F. DeFranco w publikacji *What Every Engineer Should Know About Cyber Security and Digital Forensics* podkreśla właśnie ten aspekt, polegający na tym, że pracownik powinien nabyć umiejętność zrozumienia zagrożeń wynikających z rozwoju technologii oraz z procesu ich użytkowania [7].

Jeremy Swinfen Green w książce *Cyber Security* wskazuje, że cyberbezpieczeństwo jest często postrzegane jako domena specjalistów od technologii informatycznych, co może być mylące, ponieważ cyberzagrożenia mogą mieć swoje źródło także wewnątrz organizacji [9]. Warto zatem podkreślić, że tego typu błędy mogą powodować bezpośrednie szkody dla przychodów i zysków organizacji, jak również szkody pośrednie poprzez zmniejszoną efektywność, niższe morale pracowników i reputację wybranej instytucji.

W analogicznym obszarze wypowiadają się również Stephen J Zaccaro, Reeshad S. Dalal, Lois E. Tetrick, Julie A. Steinke redaktorzy książki *Psychosocial Dynamics of Cyber Security*, którzy akcentują w swych badaniach psychospołeczne znaczenie dynamiki pracy w środowisku bezpieczeństwa cybernetycznego [16].

Wiele najnowszych prac badawczych przyczynia się również do dyskusji na temat zmiany praktyk bezpieczeństwa narodowego i ich konsekwencji dla społeczności międzynarodowej. Reasumując, cyberbezpieczeństwo stało się centralnym punktem dla sprzecznych interesów instytucji i organizacji funkcjonujących zarówno na szczeblu krajowym jak i międzynarodowym.

Pojęcie cyberterroryzmu wobec innych cyberzagrożeń

Różnice między takimi zjawiskami jak: cyberwojna, cyberatak, cyberprzestępczość, cyberterwywiad stają się coraz bardziej rozmyte. Różnorodność sprawców takich działań, jak: pojedyncze osoby, organizacje lub zideologizowane grupy bądź instytucje państwowe komplikują nie tylko definicje, ale i wybór oraz stosowanie działań defensywnych przed cyberzagrożeniami. Stąd jak można zrozumieć występujące podobieństwa, które zacierają granice semantyczne między wspomnianymi pojęciami [6, s. 70–76]. Każde z powyższych zjawisk w

cyberprzestrzeni posiada własne, indywidualne motywacje oraz cele, które jednak w praktycznym działaniu, nakładają się wzajemnie na siebie.

Cyberprzestępstwa

Warto zwrócić uwagę na potrzebę ustalenia granic między takimi pojęciami jak choćby: cyberterroryzm i cyberprzestępczość, które maja również znaczenia dla określenia sposobów ich zwalczania. W literaturze przedmiotu za główną różnicę między atakiem cybernetycznym i cyberterroryzmem uważa się kwestię intencji czy też motywacji sprawcy. Osoba dokonująca cyberataku może mieć m. in. motywy finansowe. Natomiast najważniejszą intencją cyberterrorysty jest zawsze motyw polityczny, społeczny lub religijny. Innymi słowy aktywność w cyberprzestrzeni w obu przypadkach może być analogiczna, jednak jej uzasadnienie będące podstawą działania w cyberprzestrzeni będzie już odmienne[6, s. 70–76].

Cyberprzestępstwa stanowią obecnie najbardziej rozpowszechnioną formę cyberzagrożeń; są one bardziej powszechne niż zjawisko cyberterroryzmu czy też wojny cybernetycznej toczonej przez państwa. Jednak główną różnicą między atakiem cybernetycznym i cyberterroryzmem jest intencja sprawcy.

Niektórzy cyberprzestępcy tworzą zorganizowane grupy do prowadzenia cyberprzestępczości. Przyjęcie specjalistycznych zestawów umiejętności i profesjonalizacja praktyk biznesowych stale rośnie m.in. na skutek posiadanych umiejętności technicznych oraz niezbędnych narzędzi i zasobów do prowadzenia cyberprzestępczości [6, s. 70–76].

Na cyberprzestępstwa składa się wiele rożnych działań, które występują w różnej formie jak np.: oszustwa, fałszerstwa, kradzieży własności intelektualnej, ingerencji w system danych, czy też nielegalnego dostępu do urządzeń oraz przechwytywania sygnału.

Jednym z najbardziej rozpowszechnionych metod są przestępstwa finansowe, które mogą wydawać się zupełnie niezwiązane z aktami cyberterroryzmu, ale w rzeczywistości są one ze sobą zintegrowane. Obecnie wiele organizacji terrorystycznych dokonuje tego typu przestępstw jak: fałszowanie kart kredytowych lub kradzież tożsamości, które pozwalają na dostęp do kont bankowych, a tym samym umożliwiają finansowanie działalności terrorystycznej [14, s. 3–7; 18, s. 19; 12, s. 142]. Okazuje sie więc, że kradzież tożsamości w rzeczywistości może być elementem większego ataku terrorystycznego. Badacze zauważają również, że podziemny świat cyberprzestępczości jest także swoistym «poligonem» dla hakerów, którzy rozwijają i doskonalą swoje umiejętności [2, s. 22–25].

Hakerzy

Grupy terrorystyczne mogą rekrutować wysoko wykwalifikowanych hakerów (na podstawie motywacji ideologicznych lub finansowych), aby za pomocą ich umiejętności dokonywać działań cyberterrorystycznych. Analizując charakter działań hakerów, cyberprzestępców oraz cyberterrorystów można stwierdzić, że nie ma większych różnic w metodach działania wśród tych grup. Obecnie hakerzy mogą umożliwić dostęp do każdej sieci komputerowej. Posiadają oni umiejętności oraz

narzędzia umożliwiające zainfekowanie określonych urządzeń szkodliwym oprogramowaniem.

Podstawowe różnice pozwalające odróżnić działalność cyberterrorystyczną od cyberprzestępczej polega nie tyle na zastosowaniu metod w uzyskaniu określonych celów, ale na ich sposobie wykorzystania. Przykładem ilustrującym powyższą odmienność jest sytuacja, polegająca na uzyskaniu dostępu do pewnego rodzaju informacji np. hasła dostępu. Jest to oczywiście działalność sprzeczna z prawem, jednak w przypadku hakera nie będzie miała ona takich konsekwencji społecznych, oczywiście pod warunkiem, że nie zostanie ona ujawniona i wykorzystana przeciwko wybranej osobie. Natomiast działalność cyberterrorystyczna polega na wykorzystywaniu wykradzionych informacji, które następnie mogą posłużyć do przeprowadzenia ataków lub wspierania na dalszym etapie działalności terrorystycznej. Okazuje się zatem, że nie każde zagrożenie ujawnienia skradzionych informacji z komputerów powinno być traktowane jako cyberterroryzm.

Kluczowa różnica odnosi się do działania zmierzającego do zmiany procesów, instrukcji lub innych procedur niezbędnych do funkcjonowania określonego systemu. Zmiany takie w niektórych przypadkach mogą doprowadzić do tragicznych konsekwencji. Oczywiście czym innym będzie naruszenie integralności systemu w celu krytyki, ośmieszenia wybranej osoby lub zamanifestowania określonych poglądów. Tego typu zmiany nie mają na celu doprowadzenia do uszkodzenia lub zniszczenia wybranych obiektów. Czym innym jest za to cyberterroryzm, którego działania polegają na naruszeniu integralności systemu w celu uzyskania kontroli nad systemami odpowiedzialnym za utrzymanie kontaktu elektronicznego, obsługę transportu, elektryczności czy też pracę i funkcjonalność szpitalach, banków itp.

Innym ważnym rozróżnieniem jest możliwość dostępu do informacji i zasobów informacyjnych. Jeżeli system jest elementem strategicznej infrastruktury krytycznej, jak np. bazy informacyjne policji lub innych służb odpowiedzialnych za bezpieczeństwo narodowe, to ich zablokowanie może być potraktowane jako wspierania działań terrorystycznych. Podobnie jak odmowa usługi komputerowej odpowiedzialnej za transport publiczny, której konsekwencje mogą być tragiczne. Różnica zatem polega na stopniu wrażliwości informacji oraz zasobów obsługiwanych przez określony system, co ma bezpośrednie przełożenie na konsekwencje takiego ataku [19, s. 181-186].

Zdaniem badaczy część hakerów może reprezentować podobne cechy charakteru do terrorystów. Analogia pomiędzy tymi stronami opiera się przede wszystkim na narcystycznym zaburzeniu osobowości. Wśród takich osób zauważyć można najczęściej wysokie poczucie własnej wartości, przekonanie o sukcesie, silną potrzebę przyciągnięcia uwagi i podziwu innych, negatywne reakcji w sytuacji zagrożenia własnych uczuć, a także brak empatii [19, s. 181–186].

Zdolność do wywołania cyberataku, a tym samym stworzenie zagrożenia dla bezpieczeństwa publicznego ze strony władz obcego państwa, organizacji terrorystycznej lub hakera w rzeczywistości są analogiczne. W kontekście prowadzonej analizy, ważne jest wskazanie na różnice jakie występują pomiędzy określeniem przejawu hakerstwa i cyberterroryzmu. Terroryzm jest zbrodnią, ale nie każde przestępstwo lub niezgodne z prawem korzystanie z systemu komputerowego

jest aktem terrorystycznym. Przede wszystkim, aby zakwalifikować działania w cyberprzestrzeni jako akt cybernetycznego terroru musi on zostać popełniony przez terrorystów, a nie przez hakerów. Literatura przedmiotu wskazuje również na odmienne cele, haker bowiem w przeciwieństwie do terrorysty nie kieruje się celami politycznymi ani nie ma zamiaru zabijać ludzi, by wywołać panikę lub szerzyć strach. Zatem, cyberterroryzm musi być rozumiany jako atak, mający swój początek w cyberprzestrzeni, motywowany politycznie, którego celem jest – poprzez wykorzystanie sieci komputerowej – zagrożenie dla życia lub inne poważne konsekwencje dla bezpieczeństwa publicznego oraz wywołanie paniki i strachu w społeczeństwie [21, s. 313–318].

Cyberatak

Do głównych skutków cyberataków należy zaliczyć awarię, dysfunkcjonalność bądź paraliż systemów odpowiedzialnych za pracę określonych urządzeń kluczowych dla wykonywania statutowych zadań przez instytucje państwowe lub prywatne. Przejawem takiej dysfunkcjonalności systemu może być zakłócenie integralności urządzeń, poprzez zmianę informacji lub danych; zablokowanie dostępu do systemu obsługującego określone urządzenia dla upoważnionych użytkowników; ujawnienie poufnych informacji istotnych z punktu widzenia żywotnych interesu organizacji, wystosowanie wirtualnych komend lub poleceń prowadzących do awarii w skutek których nastąpi fizyczne zniszczenie określonych urządzeń. Łatwo dostrzec, że skutki przedstawionych działań mogą wchodzić w zakres pojęciowy zarówno cyberprzestępstwa jak i cyberterroryzmu [6, s. 70–76].

Cyberataki najczęściej kierowane są na elementy infrastruktury krytycznej (usługi finansowe, produkcja, telekomunikacja, przesył i zarządzenie energią elektryczną czy też sieć wodociągowa). Innym ważnym celem cyberataków są instytucje państwowe, szczególnie w obszarze sprawowania władzy jak: Kancelaria Prezydenta, Urząd Rady Ministrów, Parlament, Biura Poselskie, czy też instytucje zajmujące się bezpieczeństwem publicznym.

Dużym zagrożeniem są wirusy lub konie trojańskie, których przeznaczeniem – jednym z wielu – jest zainfekowanie komputera, aby był on dostępny dla przejęcia i zdalnego sterowania. Do sytuacji takich dochodzi najczęściej w przypadku, jeśli użytkownik otworzy załącznik e-mail lub kliknie na link na stronie internetowej. Złośliwe oprogramowanie może skanować komputer ofiary do poufnych informacji (np. data urodzenia, numery kont bankowych, itp.), które następnie mogą być sprzedawane online lub wykorzystywane do produkcji fałszywych dokumentów tożsamości. Realizacja takiego zamierzenia stanowi duże ułatwienie dla wielu grup terrorystycznych, dla których docieranie do celu w niepostrzeżony sposób, stanowi gwarancję np. przeprowadzenia zamachu.

Ponadto, wewnętrzni pracownicy mogą uzyskać dostęp do poufnych danych o instytucji, w której pracują [6, s. 70–76]. Sposoby rozpowszechniania złośliwego oprogramowania nie są ograniczone tylko i wyłącznie do sieci. Nośniki pamięci będące zarazem upominkiem rozdawanym np. na targach i konferencjach mogą okazać się również sposobem pozwalającym na dostęp do zabezpieczonych systemów.

A zatem ominięcie systemu bezpieczeństwa jest możliwe z powodu nieuwagi bądź złośliwości wynikającej z frustracji zawodowej pracownika.

Duże znaczenie dla cyberbezpieczeństwa ma dynamicznie rozwijająca się działalność tzw. botnetów. Jest to sieć zainfekowanych komputerów kontrolowanych zdalnie przez atakującego. Botnety prowadzone przez przestępców mogą być wykorzystane przez terrorystów lub państwa narodowe w celu zdobycia poufnych danych, pozyskiwania funduszy lub zakłócenia dostępu do krytycznej infrastruktury krajowej [13, s. 58–64; 17, s. 5–32]. Tysiące takich komputerów może pracować równocześnie paraliżując pracę wybranych ofiar. Botnety, które specjalizują się w pozyskiwaniu danych są w stanie przechwytywać zawartość zaszyfrowanych stron i modyfikować je w czasie rzeczywistym.

Cyberatak nie jest odczuwany jednakowo we wszystkich dziedzinach. Mała firma może nie być w stanie przetrwać nawet jednego znaczącego ataku cybernetycznego. Z drugiej strony, firmy często nie zdają sobie sprawy, że zostały ofiarami cyberprzestępców. W wielu przypadkach instytucje nie są w stanie odzyskać poniesionych strat, które również nie są możliwe do oszacowania. W trosce o własną reputację wiele firm woli nie ujawniać, że ich systemy zostały naruszone.

Przy analizie możliwości zaistnienia cyberataku, trudno jest stwierdzić z pełnym przekonaniem, że infrastruktura krytyczna pozostanie nietknięta i zawsze będzie funkcjonalna w razie potrzeby. Prawdopodobnie przy wystarczających nakładach czasu, motywacji i środków, terrorysta bądź haker będzie prawdopodobnie w stanie przeniknąć każdy system, który jest dostępny bezpośrednio z Internetu.

Cyberwywiad

Cyberszpiegostwo polega na wykorzystywaniu systemów komputerowych lub technologii informacyjnej do nielegalnego uzyskania poufnych informacje od rządu, sektora prywatnego lub innego podmiotu [6, s.70-76]. Cyberwywiad dotyczy przede wszystkim nieupoważnionych działań takich jak: przeglądanie i kopiowanie danych, a także pozyskiwanie – poprzez bezprawne testowanie konfiguracji komputerów oraz mechanizmów obronnych systemu – informacji na temat technologii i zabezpieczeń instytucji docelowej [9, s. 26–35].

Służby wywiadowcze są szczególnie zainteresowane informacjami odnoszącymi się po pierwsze: do technologii w tym także wojskowych, po drugie: do informacji na temat treści związanych ze strategią rozwoju i po trzecie: do prowadzonych negocjacji oraz zawieranych umów dotyczących działalności gospodarczej. W Stanach Zjednoczonych rząd szacuje, że ponad 100 organizacji pracujących na rzecz obcego wywiadu regularnie próbuje włamać się do systemów komputerowych rządu USA i firm amerykańskich. Większość ataków cybernetycznych na systemy rządowe USA wydają się pochodzić z Chin [6, s. 70–76].

Zagrożenia cybernetyczne mają szczególne znaczenie dla władz Kremla. Rosyjski rząd, w tym jego wojsko, rozwija systemy wywiadowcze w celu poprawy ich ofensywnych i defensywnych cybermożliwości. Rosja prowadzi szereg działań, w tym gromadzenie informacji gospodarczych i technologicznych na temat krajów zachodnich.

Również Chiny próbują pozyskać informacje z zakresu polityki, handlu i bezpieczeństwa. Głównymi sprawcami tych czynności jest Departament Trzeci Armii Ludowo-Wyzwoleńczej. Wysoce prawdopodobna jest teza, że w innych częściach globu, a nawet wobec własnego sektora prywatnego mogą być przeprowadzenie podobne działania. Można także przypuszczać, że informacje dotyczące konkretnej technologii, którą Chiny zamierzają rozwijać lub realizować są i będą centralnym punktem zainteresowania służb wywiadowczych tego państwa. Chińscy hakerzy kierują swoje działania w różne sektory przemysłu zachodnich, w tym elektroniki, telekomunikacji, energetyki, lotnictwa i obrony. Prawdopodobne odbiorcami skradzionych danych handlowych są chińskie przedsiębiorstwa państwowe, które dominują w chińskiej gospodarce [6, s. 70–76].

Rządy wielu państw znacznie poszerzyły liczbę personelu służb wywiadowczych oraz przeprowadzanych przez nich operacji, które są bezpośrednim następstwem zamachów z 11 września 2001 roku. Pomimo jednak wzrostu liczby agencji wywiadowczych oraz osiągnięć technologicznych i wzrostu budżetu głównym problemem wywiadu jest niewystarczająca liczba analityków [1, s. 214]. Okazuje się bowiem, że służby wywiadowcze bardzo dobrze radzą sobie z wypełnianiem jednego z głównych swoich obowiązków jakim jest pozyskiwanie informacji, jednak drugim zadaniem – równie trudnym i ważnym – jest ich właściwa analiza, polegająca m.in. na interpretacji, scalaniu i weryfikacji danych. Innymi słowy służby pozyskują więcej informacji niż są w stanie przyswoić i zanalizować.

Cyberwojna

W obszarze prowadzonego cyberkonfliktu obie walczące ze sobą strony wykorzystują informacje za pomocą środków technologicznych z urządzeń lub systemów w celu uzyskania przewagi nad przeciwnikiem. Walka opiera się na trzech zasadach odnoszących się po pierwsze: do poziomu wywiadu, czyli pozyskiwania i gromadzenia informacji, po drugie: cybermilitarnego dotyczącego przeprowadzania ataków i po trzecie: kontrwywiadowczego polegającego na zapewnieniu ochrony dla własnych zasobów informacyjnych oraz innych aktywów.

Pod pewnymi względami, konsekwencje cyberwojny mogą być analogiczne jak w przypadku prowadzenia konwencjonalnej wojny. Jednak zauważyć należy, że w przypadku – znanych już opinii publicznej – cyberataków, które miały miejsce np. w Kirgistanie w styczniu 2009 roku, czy też w Estonii na przełomie kwietnia i maja 2007 roku, trudno jest do końca zidentyfikować, który podmiot (państwo, organizacja, osoba) jest odpowiedzialna za atak.

Zdolność krajów do określenia źródła cyberataku, może prowadzić do odwetu zarówno w cyberprzestrzeni jak i w tradycyjnym znaczeniu. Odwet może być zinterpretowany jako samoobrona, jeśli jest on proporcjonalny i dokonany z konieczności.

Wiosną 2007 roku, praca rządowych systemów komputerowych w Estonii została zakłócona poprzez liczne ataki cybernetyczne. Ataki te – jak początkowo sądzono – zostały zaaranżowane przez rosyjskie grupy przestępcze i prawdopodobnie za wiedzą władz Kremla. Botnety zostały wykorzystane do przeciążenia estońskich stron

internetowych, w wyniku czego ofiarą padły m.in. systemy rządowe, kanały medialne czy też serwery bankowe.

Podobna sytuacja wystąpiła w czerwcu 2008 roku na Litwie, której rząd stanął w obliczu cyberataków, a które były odpowiedzią na uchwaloną przez parlament – trzy dni wcześniej – ustawę zakazującą używania symboli komunistycznych. W wyniku decyzji władz litewskich ponad trzysta stron internetowych zostało zaatakowanych.

W dniu 20 lipca 2008 roku strona internetowa prezydenta Gruzji została unieruchomiona w wyniku ataku Denial of Cyber Service (DOCS). W dniu 8 sierpnia 2008 roku, doszło ponownie do skoordynowanego cyberataku na gruzińskie strony rządowe, w tym samym czasie, kiedy siły rosyjskie były zaangażowane w walkę z siłami gruzińskimi. Konflikt ten uważany jest za pierwszy tego typu, w którym przeprowadzone były równocześnie działania zbrojne przy użyciu środków konwencjonalnych jak i cybernetycznych.

W dniu 18 stycznia 2009 roku, dwa główne serwery internetowe w Kirgistanie zostały sparaliżowane przy użyciu ataków typu DDoS. Ataki miały miejsce w tym samym dniu, kiedy to strona rosyjska naciskała rząd w Kirgistaie, aby ten zamknął dostęp do bazy lotniczej w Manas w Biszkeku dla sił wojskowych USA. Reasumując, można zauważyć, że prawie każdy konflikt polityczny i wojskowy w obecnych czasach ma swój odpowiednik w cyberprzestrzeni.

Cyberpropaganda

Zagrożenie stwarzane przez cyberterroryzm polega na wzbudzaniu strachu, poprzez stymulowanie określonych emocji wykorzystując do tego celu nowoczesne technologie informacyjne. Ważny jest także zawarty w komunikatach propagandowych określony wizerunek przekazu składającego się z kodów kulturowych, odwołujących się do estetyki popkultury, dzięki czemu dokonuje się wzmocnienia tradycyjnego wsparcia dla działalności terrorystycznej.

Cyberterroryści wykorzystują efekty globalizacji i nowoczesnej technologii do planowania, koordynowania i realizacji swych kampanii. Posiadają oni szczególną umiejętność korzystania z serwisów społecznościowych, takich jak Facebook i Twitter, które pozwalają im z jednej strony zbierać informację, a z drugiej promować i rozpowszechniać swój przekaz niemal bez ograniczeń. Ponieważ celem terrorystów jest generowanie rozgłosu i zwrócenie uwagi na ich przyczyny, Internet stanowi więc wygodne narzędzie pozwalające na ominięcie cenzury i udostępnianie niefiltrowanych wersji transmitowanych wydarzeń na cały świat. Nie dziwi więc fakt, że terroryści wykorzystują Internet do realizacji swoich celów [20, s. 1–12].

Przykładem są artykuły w magazynie «Inspire», instruujące jak zbudować bombę przy wykorzystaniu dostępnych środków w domu lub w którym miejscu najlepiej podłożyć i zdetonować ładunek, aby spowodować jak najwięcej szkód. Dzięki Internetowi nie ma już potrzeby podróży do Afganistanu na szkolenie terrorystyczne. Wszystkie przykłady z zakresu działań terrorystycznych mogą być czytane i oglądane przez każdego z laptopem podłączonym do Internetu. Reasumując cyberprzestrzeń jest przydatna dla terrorystów, ponieważ za jej pomocą można komunikować się z publicznością, znaleźć potencjalnych rekrutów wśród swoich zwolenników i uruchomić kampanię psychologiczną [12, s. 47–53].

Podsumowując, okazuje się zatem, że Internet jest potężnym narzędziem do rozprzestrzeniania ideologii oraz prowadzenia rekrutacji. Na przykład w Iraku, powstańcy wykorzystywali cyberprzestrzeń, nie tylko aby koordynować ataki na siły zbrojne, ale filmowali zamachy po czym udostępniali materiały w celu propagowania własnych sukcesów [15, s. C1–C21]. Tak tworzony przekaz w cyberprzestrzeni wzmacniał i jeszcze bardziej radykalizował grupy o skrajnych przekonaniach. Internet okazał się więc doskonałym narzędziem komunikacji i indoktrynacji.

Pomimo tego że dokonywane są wysiłki w celu likwidowania bądź marginalizowania tego typu stron, to nadal pojawiają się nowe witryn moderowane przez organizacje terrorystyczne. Dopiero od niedawna służby wywiadowcze rozpoczęły monitorowanie tego typu miejsc w cyberprzestrzeni, obawiając się, że mogą one przyczynić się do rozwoju działalności terrorystycznej [15, s. C1–C21]. Istnieje również opinia, iż w interesie bezpieczeństwa jest to, aby nie zakłócać tego typu komunikatów i nie blokować o tej tematyce stron internetowych, ponieważ pozwalają one zbierać i gromadzić informacje wywiadowcze [18, s. 17]. Jednak monitorowanie Internetu jest trudnym zadaniem z uwagi na ogromną liczbę stron oraz dynamiczny proces rozpowszechniania informacji.

Zakończenie

Część problemów w obszarze cyberbezpieczeństwa leży po stronie nieprzygotowanych i nieprzeszkolonych w tym zakresie pracowników. Każda bowiem osoba, bez względu na pełnione obowiązki i zajmowane stanowisko, odgrywa ważną rolę w zapewnieniu bezpieczeństwa. Dowodem potwierdzającym to przypuszczenie, jest fakt, że jeden odebrany e-maila zainfekowany wirusem, może narazić całą organizację na ogromne szkody. Dlatego też, istotne z punktu widzenia instytucji biznesowej jak i państwowej jest ustawiczny i nieprzerwany proces stosowania zabezpieczeń na każdym etapie funkcjonowania organizacji. Ważna jest także troska o edukację pracowników w zakresie cyberbezpieczeństwa.

Instytucje publiczne oraz przedsiębiorstwa uczestnicząc w dynamicznych procesach polegających na dostosowaniu świadczonych usług do nowych strategii cyfrowych, często tworzą luki w systemach lub wadliwe cyberkonfiguracje, stwarzając w ten sposób doskonałą okazję dla cyberprzestępców. Instytucje zdają sobie sprawę, że względy bezpieczeństwa muszą być częścią transformacji cyfrowej. Każda z tych organizacji w procesie rozwoju wykorzystuje narzędzia m.in. z obszaru «social media». Cyfrowe rozwiązania mogą prowadzić do większej efektywności, z tego też powodu stały się już dawno nieodłącznym elementem funkcjonowania człowieka w codziennym życiu. Ponieważ cyberprzestępczość jest zjawiskiem bardzo opłacalnym, dlatego też instytucje publiczne oraz organizacje biznesowe zmuszone są do wdrażania bardziej zaawansowanych narzędzi zabezpieczeń i stosowania rygorystycznych norm w miejscu pracy.

Technologia informatyczna jest ważnym punktem odniesienia dla dalszych badań i analiz dotyczących złożonych problemów bezpieczeństwa cybernetycznego. Z pewnością rozwój i wykorzystanie cybernetycznych zdolności stanowi intrygujący przyczynek do dalszych badań.

BIBLIOGRAFIA

1. Aid M. M., Intel wars: The secret history of the fight against terror, Nowy Jork 2012.

2. Carr J., Inside Cyber Warfare, 2nd Edition Mapping the Cyber Underworld, Publisher: O'Reilly Media 2011.

3. Cavelty M.D., Cyber-Security and Threat Politics: US Efforts to Secure the Information Age, Routledge 2007.

4. Cyber Security Essentials, red., J. Graham, R. Olson, R. Howard, CRC Press 2010.

5. Cyber Security Culture: Counteracting Cyber Threats through Organizational Learning and Training, red., P. Trim, D. Upton, Routledge 2016.

6. Dean A., Cyber Threats in the 21st Century, «Security», 2012 r., nr 49/9.

7. DeFranco J. F., What Every Engineer Should Know About Cyber Security and Digital Forensics, CRC Press 2013.

8. Ghernaouti-Helie S., Cyber Power: Crime, Conflict and Security in Cyberspace, CRC Press 2013.

9. Gyrka M., Mossad. Poraïki i sukcesy tajnych siuïb izraelskich, Warszawa 2015.

10. Green J. S., Cyber Security: An Introduction for Non-Technical Managers, Routledge 2015.

11. Guiora A. N., Cyber-Security: Geo-Politics, Law, and Policy, CRC Press 2016.

12. Johnson M., Cyber Crime, Security and Digital Intelligence, Routledge 2013.

13. Lappin Y., Virtual Caliphate, Waszyngton 2011.

14. McLaughlin K.L., Cyber Attack! Is a Counter Attack Warranted?, «Information Security Journal: A Global Perspective», 2011 r., vol.20/1.

15. Negroponte J. D., Palmisano S.J., Segal A., Defending an Open, Global, Secure, and Resilient Internet, Nowy Jork 2013.

16. Pedersen Ch., Much Ado about Cyber-space: Cyber-terrorism and the Reformation of the Cyber-security, «Pepperdine Policy Review», 2014 r., nr 7/1.

17. Psychosocial Dynamics of Cyber Security, red., S. J Zaccaro, R.S. Dalal, L.E. Tetrick, J. A. Steinke, Routledge 2016.

18. Rid T., Cyber War Will Not Take Place, «Journal of Strategic Studies», 2011 r., vol. 35/1.

19. Rollins J., Wilson C., Terrorist Capabilities for Cyberattack: Overview and Policy Issues, «CRS Report for Congress», 22 stycznia 2007 r.

20. Topor S., Cyber criminal and cyber terrorist - two concepts that need to be differently treated, International Scientific Conference «Strategies XXI», 2016 r., nr 3.

21. Weimann G., Cyberterrorism. How Real Is the Threat?, «Special Report», 2014 r., vol. 119.

22. Voicescu M., Cyber terrorism and bioterrorism -new forms of terrorists action. size, effects and countermeasures, International Scientific Conference «Strategies XXI», 2012 r., nr3.

Стаття надійшла до редколегії 10.12.2016
Прийнята до друку 23.12.2016

ОКРЕМІ АСПЕКТИ КІБЕР-ЗАГРОЗ У КОНТЕКСТІ БЕЗПЕКИ ДЕРЖАВИ ТА СУСПІЛЬСТВА

Марек Гурка

Кошалінський технологічний університет,
вул. Квятковського, 6d/7, м. Кошалін, Польща,
e-mail: marek_gorka@wp.pl

Швидкі темпи розвитку в сфері інформаційно-комунікаційних технологій привели до узалежнення від нових технологій як громадської інфраструктури, так і приватного життя. Широке використання інформаційних технологій представляє нові ризики та загрози. Ризики трагічних подій, пов'язаних з функціонуванням кіберпростору, стали погрожувати критично важливій інфраструктурі, яка визначається як необхідний елемент для функціонування суспільства і економіки. Кібербезпека стала однією з найсерйозніших проблем, пов'язаних з національною

безпекою. Масштаби проблем і ризиків кіберпростору включають в себе багато аспектів повсякденного життя, починаючи від особистого життя, фінансових втрат, фізичну шкоду і руйнування і закінчуючи несприятливим впливом на ефективність політики, що проводить уряд тієї чи іншої країни. Ці виклики і загрози відображає широкий діапазон, в якому комп'ютери або інші технологічні пристрої можуть перетворюватися на зброю для ворога чи великих груп і організацій задля реалізації ворожих дій, заходів тощо.

***Ключові слова*:** кібербезпека; кіберпростір; кібервійна; кібератаки; кіберзлочинність.

SELECTED ASPECTS OF CYBER THREATS IN THE CONTEXT OF THE SECURITY OF THE STATE AND SOCIETY

Marek Gorka

Koszalin University of Technology,
6d/7, Kwiatkowskiego Str. Koszalin, Poland,
e-mail: marek_gorka@wp.pl

The rapid pace of technological development in the field of ICT addiction has caused public infrastructure and private from cyberspace. The widespread use of information technology introduces new risks. The risk of tragic events related to the functioning of cyberspace began to threaten critical infrastructure, which is defined as a necessary element for the functioning of society and the economy. Cyber security has become one of the most serious problems related to national security. The scope of the challenges and risks of cyberspace involves many aspects of everyday life, ranging from privacy, financial loss, physical harm and destruction and ending with the adverse impact on the effectiveness of policies by the government. These challenges and threats reflects the wide range in which computers or other technological devices can provide weapons for hostile individuals or groups and organizations.

Key words: cyber security; cyberspace; cyberwar; cyber attack; cyberintelligence; cybercrime.