S T U D I A  N A D  B E Z P I E C Z E Ń S T W E M

**NR 2** **ss. 57–76** **ROK 2017**

ISSN 2543–7321

**Józef Sadowski**

Akademia Pomorska
Słupsk
jozef.sadowski@apsl.edu.pl

# CYBERNETYCZNY WYMIAR WSPÓŁCZESNYCH ZAGROŻEŃ

# A CYBERNETIC DIMENSION OF THE CONTEMPORARY THREATS

***Zarys treści*:** Rośnie podatność państw na zagrożenia cybernetyczne, w tym typu terrorystycznego. Prezentowane w artykule przykłady z ostatnich lat w Polsce i innych krajach świata wskazują, że tendencja ta będzie się systematycznie zwiększać, bowiem funkcjonowanie nowoczesnych społeczeństw nieodłącznie wiąże się z zapewnieniem stałego i prawidłowego funkcjonowania systemów informatycznych, służących zaspokajaniu podstawowych potrzeb (gromadzeniu i transmisji danych, monitorowaniu, sterowaniu, wspomaganiu zarządzania itp.). Do działań o charakterze agresji czy wręcz terroru cybernetycznego mogą się uciekać władze i służby wrogich państw, koncerny międzynarodowe, przestępcze organizacje o charakterze pozarządowym, nieformalne grupy użytkowników Internetu, a nawet pojedynczy użytkownicy. Celem ataków stają się elementy infrastruktury krytycznej, systemy bankowe, uzbrojenia i kierowania państwem, a nawet końcowi użytkownicy systemów. Ataki te przynoszą straty ekonomiczne liczone już w setkach milionów dolarów rocznie. Przewiduje się, że w niedalekiej przyszłości cyberataki staną się narzędziem szantażu w rękach przestępczości zorganizowanej i mogą stać się zarzewiem cyberkonfliktu a nawet cyberwojny.
***Słowa kluczowe*:** cyberataki, cyberzagrożenia, cyberterroryzm**,** cyberwojna, cyberkonflikt, wojna informacyjna.
***Key words*:** cyber-attacks, cyber threats, cyber-terrorism, cyberwar, cyberconflict, information warfare

Cyberbezpieczeństwo, cyberataki, cyberzagrożenia**,** cyberobrona itp. to pojęcia związane ze współczesnym Internetem. Internet (z ang. *inter-network*, dosłownie „między-sieć") – to ogólnoświatowy system połączeń między komputerami, określany również jako sieć sieci. W znaczeniu informatycznym Internet to przestrzeń

adresów IP przydzielonych hostom i serwerom połączonym za pomocą urządzeń sieciowych, takich jak karty sieciowe, z wykorzystaniem infrastruktury telekomunikacyjnej[1]. Internet w ogólnym znaczeniu to sieć komputerowa, czyli wiele połączonych ze sobą komputerów, zwanych również hostami.

Początki Internetu wiążą się z powstaniem sieci rozległej ARPANET i sięgają końca lat sześćdziesiątych XX w. Powszechnie uważa się, iż potrzeba jego stworzenia była konsekwencją prac amerykańskiej organizacji badawczej RAND Corporation, która prowadziła badania nad możliwościami dowodzenia w warunkach wojny nuklearnej. Na podstawie uzyskanych raportów podjąć miano prace projektowe nad skonstruowaniem sieci komputerowej mogącej funkcjonować mimo jej częściowego zniszczenia. Charles Herzfeld, dyrektor ARPA w czasach powstania ARPANET, obala jednak tak rozumiany mit genezy Internetu zauważając, iż od początku chodziło wyłącznie o zwiększenie potencjału naukowego przez połączenie oddalonych od siebie placówek badawczych wyposażonych w komputery[2].

W latach dziewięćdziesiątych ubiegłego wieku nastąpiła gwałtowna komercjalizacja i rozwój tego środowiska. Powstały nowe usługi: strony internetowe, poczta elektroniczna, wyszukiwarki, komunikatory, strumieniowe przesyłanie multimediów, sieci społecznościowe, fora, blogi i wiele innych. Wraz z rozwojem fizycznej infrastruktury globalnej sieci ciągle rośnie liczba jej użytkowników. W ostatnich latach technologia informatyczna bardzo się rozwinęła. Z administracyjnego narzędzia do wspierania optymizacji pracy biurowej przekształciła się obecnie w narzędzie przemysłu, administracji i wojskowości.

W Polsce pierwsze internetowe łącze analogowe zostało uruchomione 26 września 1990 r. Pierwsza transmisja internetowa miała miejsce w listopadzie 1990 r. Internet w Polsce dostępny jest oficjalnie od 20 grudnia 1991 r.[3] W sierpniu 1993 r. powstał pierwszy polski serwer WWW, pod nazwą „Polska Strona Domowa". W 1992 r. powstała pierwsza polska strona internetowa internet.pl, następnie w 1995 r. powstał polski portal internetowy Wirtualna Polska[4].

W drugiej dekadzie XXI w. społeczeństwa w coraz większym stopniu uzależnione są od informatyki. Do cyberprzestrzeni przenikają kolejne aspekty ludzkiej działalności. Globalny zasięg oraz możliwość natychmiastowego dostępu z dowolnego miejsca na Ziemi, w połączeniu z niewielkimi kosztami użytkowania sprawił, że coraz więcej podmiotów oraz indywidualnych osób decyduje się przenosić różne elementy swojej codziennej działalności do Internetu. Dzisiaj przeciętny Kowalski nie wyobraża sobie życia bez szybkiego dostępu do najświeższych informacji i poczty elektronicznej, bankowości internetowej, zakupów online, elektronicznej rezerwacji biletów czy kontaktu z rodziną i znajomymi przez portale społecznościowe oraz internetowe komunikatory. Komputery kontrolują, gromadzą informacje lub wręcz sterują wieloma dziedzinami życia (dostarczanie energii, komunikacja, transport, finanse, gromadzenie danych medycznych, danych statystycznych itp.).

[1] https://pl.wikipedia.org/wiki/Internet (dostęp: 21.01.2017).
[2] Charles Herzfeld on ARPAnet and Computers, (dostęp: 26.02.2014).
[3] 20 lat polskiego Internetu. di.com.pl. (dostęp: 03.01.2017).
[4] Historia Wirtualnej Polski SA. https://pl.wikipedia.org/wiki/Internet (dostęp: 27.01.2017).

Jednak w czasie, gdy cyberprzestrzeń ułatwia życie, przenikają do niej również negatywne formy ludzkiej działalności. Dając duże poczucie anonimowości, wykorzystywana jest przez organizacje przestępcze, a nawet niektóre państwa, do prowadzenia nielegalnej działalności lub agresji wobec innych państw czy podmiotów. Istnieje przeświadczenie, że współczesny przestępca może dokonać więcej zniszczeń za pomocą komputera niż bomb czy rakiet.

Cyberprzestrzeń jest „zależnym od czasu zbiorem połączonych systemów informacyjnych oraz ludzi/użytkowników wchodzących w interakcję z tymi systemami”[5]. Nie ma barier kontrolnych. Cele ataków są bardzo szerokie – zagrożone są sieci komputerowe oraz indywidualne komputery, a znalezienie luk w zabezpieczeniach – przede wszystkim z winy użytkowników (nieznajomość/lekceważenie przepisów, łapownictwo, frustracja, ideologia, modyfikacja systemów i danych, błąd organizacyjny lub techniczny, sabotaż, uszkodzenie lub kradzież elementów przesyłowych) – jest bardzo trudne. Zagrożone mogą być instytucje i urzędy państwowe oraz inne jednostki organizacyjne, w tym prywatni użytkownicy.

Cyberprzestrzeń – to przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Ułatwia ona użytkownikowi sieci kontakty w czasie rzeczywistym. Obejmuje wszystkie systemy komunikacji elektronicznej, które przesyłają informacje pochodzące ze źródeł numerycznych. Przestrzeń wirtualna stała się łatwym polem aktywności organizacji terrorystycznych. Rozwój informatyki generuje więc nowy rodzaj zagrożeń związanych z cyberterroryzmem. Ataki cybernetyczne[6] są jednymi z najbardziej skutecznych i jednocześnie uciążliwych (jeśli chodzi o szkody) działań uderzających we współczesne społeczeństwa. Cyberterroryzm staje się coraz bardziej powszechną metodą działania:

- do przeprowadzenia działań związanych z cyberatakiem jedynym potrzebnym narzędziem jest komputer i podłączenie do sieci;
- poprzez tworzenie wirusów, robaków komputerowych, tzw. koni trojańskich i przesyłanie ich docelowo w miejsce ataku, niszczenie serwerów, modyfikację systemów IT oraz fałszowanie stron www.

Istnieje wiele definicji cyberterroryzmu:

1) „neologizm opisujący dokonywanie aktów terroru przy pomocy zdobyczy technologii informacyjnej. Ma na celu wyrządzenie szkody z pobudek politycznych lub ideologicznych, zwłaszcza w odniesieniu do infrastruktury o istotnym znaczeniu dla gospodarki lub obronności atakowanego kraju. Polega na celowym zakłóceniu interaktywnego, zorganizowanego obiegu informacji w cyberprzestrzeni”[7].
2) „[...] groźba lub bezprawny atak wymierzony w system informatyczny lub zgromadzone dane, w celu zastraszenia czy wymuszenia na władzach pań-

[5] Cyberspace*: Definition and Implications,* Cooperative Cyber Defence Centre of Excellence, www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf (dostęp: 20.05.2012).

[6] Szerzej na temat cyberterroryzmu, D. Galan, *Cyberterroryzm jako nowe wyzwanie społeczeństwa informacyjnego,* http://academicon.pl/blogi_naukowe/bezpieczenstwo-w-sieci/cyberterroryzm-jako-nowe-wyzwanie-spoleczenstwa-informacyjnego (dostęp: 20.11. 2016).

[7] https://pl.wikipedia.org/wiki/Cyberterroryzm (dostęp: 27.01.2017).

stwowych lub jej przedstawicielach ustępstw lub oczekiwanych zachowań, w celu wsparcia określonych celów (np. politycznych). Aby działania takie zostały zakwalifikowane jako terroryzm informacyjny,

3) […] powinny wywoływać powszechne poczucie strachu"[8].
4) „[...] wykorzystanie sieci komputerowych jako narzędzia do sparaliżowania lub poważnego ograniczenia możliwości efektywnego wykorzystania struktur narodowych (takich jak energetyka, transport, instytucje rządowe itp.) bądź też do zastraszenia czy wymuszenia na rządzie lub populacji określonych działań"[9].
5) „[...] akt kryminalny popełniony przy użyciu komputera i możliwości telekomunikacyjnych, powodujący użycie siły, zniszczenie i/lub przerwanie świadczenia usług dla wywołania strachu, poprzez wprowadzanie zamieszania lub niepewności w danej populacji, w celu wpływania na rządy, ludność tak, aby wykorzystać ich reakcje dla osiągnięcia określonych celów politycznych, społecznych, ideologicznych lub głoszonego przez terrorystów programu"[10].
6) „[...] jest to obmyślony, politycznie umotywowany akt przemocy wymierzony przeciwko informacjom, programom, systemom komputerowym lub bazom danych, który mając charakter niemilitarny, przeprowadzony jest przez ponadnarodowe lub narodowe grupy terrorystyczne"[11].
7) „[...] jest skrytym, politycznie motywowanym atakiem przeciwko informacji, systemom lub programom komputerowym, bazom danych, których efektem jest przemoc przeciwko celom niewojskowym realizowanym przez grupy ponadnarodowe"[12].

Przedstawione definicje zawierają dwa zasadnicze wyróżniki, aspekty (jednocześnie części składowe cyberterroryzmu):

- celem aktu terrorystycznego jest technologia informatyczna (atakowane są komputery i systemy informatyczne z zamiarem przeprowadzenia sabotażu elektronicznego lub fizycznego) albo
- technologia informatyczna jest jedynie narzędziem (wykorzystywane są narzędzia informatyczne w celu manipulowania, penetracji lub kradzieży danych bądź wymuszenia takiego działania systemu, który jest zgodny z intencją terrorystów).

[8] D. Denning, *Cyberterrorism*, 2000, www.cs.georgetown.edu~denning/infosec/cyberterror-GD.doc (dostęp: 27.03.2004).
[9] A.J. Lewis, *Assessing the risk of cyber terrorism, cyber war and other cyber threats*, 2002, Center for Strategic amd International Studies, www.csis.org/tech/0211lewis.pdf (dostęp: 27.03.2004).
[10] L. Garrison, M. Grand, *Cyberterrorism*, 2001, *An evolving concept, NIPC highlights*, www. Nopc.gov./publication/highlight/2001/highlight-01-06.htm (dostęp: 04.04.2004).
[11] Tamże.
[12] M.M. Pollitt, *Cyberterrorism – Fact or Fancy*, http://www.cs.georgetown.edu/~denning/infosechtml/pollitt, (dostęp: 04.04.2004).

## Ewolucja zagrożeń cybernetycznych

Rozwój Internetu w XXI w. stał się stymulatorem zagrożeń cybernetycznych. Niegroźne robaki i wirusy przekształciły się ze zwykłych niedogodności w poważne wyzwania bezpieczeństwa oraz idealne narzędzia cyberszpiegostwa. Ataki cybernetyczne (w tym DDoS) stają się coraz powszechniejsze, lepiej zorganizowane. Wyrządzają coraz większe szkody administracji i gospodarce. Walka informacyjna stanowi potencjalnie zagrożenie także dla transportu, sieci dostaw energii oraz elementów infrastruktury krytycznej. W ocenie ekspertów potencjalne ataki cybernetyczne mogą obejmować oprogramowanie przeciwnika (software) lub systemy informacyjne i sprzęt komputerowy (hardware) i osiągnąć poziom, którego przekroczenie może zagrozić światowemu dobrobytowi, bezpieczeństwu i stabilności.

Niżej wybrane przykłady takiej działalności.

W 1986 r. KGB zwerbowało pięciu niemieckich hakerów, którzy włamali się do amerykańskiego Departamentu Obrony i uzyskane informacje przekazywali Rosjanom. Był to pierwszy przypadek szpiegostwa cybernetycznego[13].

Pierwsze przypadki ataków cybernetycznych w NATO miały miejsce podczas kryzysu w Kosowie (1996–1999). Działania ceberprzestępców doprowadziły, między innymi, do zablokowania na kilka dni kont e-mailowych uczestników operacji wojskowych NATO na Bałkanach oraz zakłóceń strony internetowej Sojuszu.

W marcu 2000 r. policja japońska ogłosiła, że w pracach nad oprogramowaniem umożliwiającym śledzenie ponad 150 pojazdów policyjnych, w tym pojazdów nieoznakowanych, uczestniczyli aktywni członkowie sekty Aum Shinryko. Co więcej, przynajmniej 8 japońskich firm prywatnych i aż 10 agencji rządowych przy pracach nad oprogramowaniem zatrudniało, bezpośrednio lub poprzez kooperantów, członków tej sekty. Tym samym istnieje prawdopodobieństwo zainstalowania przez nich „koni trojańskich" w opracowanym oprogramowaniu, które mogą być w przyszłości wykorzystane do przeprowadzenia ataku cyberterrorystycznego[14].

Trzytygodniowa fala zmasowanych ataków cybernetycznych w Estonii latem 2007 r. na infrastrukturę teleinformatyczną doprowadziła do paraliżu państwa, blokując dostęp m.in. do systemu bankowego i sieci komórkowych. Wydarzenia te pokazały wzrastające źródło nowych zagrożeń dla strefy publicznej oraz bezpieczeństwa i stabilności państw (również państw NATO). O przeprowadzenie ataków oskarżono Rosję, jednak nie udało się zebrać dowodów pozwalających stwierdzić, że władze tego kraju były za nie formalnie odpowiedzialne[15].

Poważny atak na amerykański wojskowy system komputerowy przeprowadzono w 2008 r. Z wykorzystaniem pendrive'a wprowadzono do komputera armii amerykańskiej w bazie wojskowej na Bliskim Wschodzie oprogramowanie szpiegowskie. Wirus rozprzestrzenił się szybko i niepostrzeżenie zarówno w tajnych, jak i w jaw-

---

[13] T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe AMW" 2005, XLVI, nr 1 (160), s. 177.

[14] Tamże, s. 184.

[15] *Estonia leczy rany po pierwszej cyberwojnie*, „Gazeta Wyborcza", z 1 czerwca 2007; *Estonia Has no Evidence of Kremlin Involvement in Cyber Attacks*, RIA, Novosti, 6 września 2007 r., http://en.rian.ru/world/20070906/76959190.html (dostęp: 24.04.2012).

nych systemach informatycznych. Powstał „informatyczny przyczółek", z którego ściągnięto tysiące plików danych do serwerów będących pod zagraniczną kontrolą. W ten sposób armia amerykańska straciła wiele istotnych, a szczególnie tajnych informacji. Podobne incydenty odnotowano w niemal wszystkich państwach NATO. Od tego czasu cyberataki i cyberszpiegostwo stały się niemal ciągłym zagrożeniem[16].

Do zmasowanych ataków na rządowe strony internetowe i serwery doszło w Gruzji podczas konfliktu gruzińsko-rosyjskiego w 2008 r. Tym razem określenie „wojna cybernetyczna" nabrało bardzo konkretnego, materialnego wymiaru. Działania w cyberprzestrzeni nie doprowadziły do żadnych fizycznych zniszczeń, osłabiły jednak gruziński rząd w krytycznej fazie konfliktu. Wpłynęły również na zdolność komunikowania się ze zszokowaną opinią publiczną w kraju i na świecie[17].

Dnia 7 listopada 2008 r. „Financial Times" doniósł, że chińscy hakerzy zdołali już kilkakrotnie spenetrować sieć komputerową Białego Domu, z Chin zaatakowano też sieci komputerowe kampanii wyborczych ówczesnych kandydatów na prezydenta USA – Baracka Obamy i Johna McCaina.

W czerwcu 2010 r. upubliczniony został fakt wprowadzenia do systemu irańskich sieci informatycznych złośliwego oprogramowania (malware) „Stuxnet". Elektroniczny wirus zaatakował irański program nuklearny[18]. Stuxnet ujawnił kolejny gigantyczny jakościowy skok w destrukcyjnym potencjale cyberwojennym i pokazał potencjalne zagrożenie, jakie niesie ze sobą złośliwe oprogramowanie (malware) atakujące kluczowy system komputerowy zarządzający dostawami energii[19]. Po raz pierwszy udowodniono, że cyberataki mogą powodować rzeczywiste fizyczne zniszczenia i narażać życie ludzi.

O skali, w jakiej cyberprzestrzeń, a szczególnie funkcjonujące w sieci blogi oraz portale społecznościowe, może wywierać wpływ na bezpieczeństwo państw, świadczy przykład „arabskiej wiosny", która rozpoczęła się w 2011 r. Uczestnicy wydarzeń ulicznych i protestów, gdy odcięto ich od informacji w tradycyjnych środkach masowego przekazu, skutecznie organizowali się za pośrednictwem serwisów społecznościowych, takich jak Facebook i Twitter. Tendencja ta z pewnością będzie narastać w przyszłości wraz z coraz szerszym rozprzestrzenianiem się nowoczesnych technologii wśród użytkowników.

Jedną z podstawowych funkcji Internetu jest uzyskiwanie informacji. Dlatego powszechnie stosowaną praktyką jest użycie cyberprzestrzeni do celów wywiadowczych. Jak napisano w raporcie opracowanym przez służby kontrwywiadowcze Stanów Zjednoczonych[20], wybrane państwa (raport wymienia m.in. Chiny i Rosję) na szeroką skalę wykorzystują cyberprzestrzeń do zbierania danych wywiadowczych,

---

[16] R. Rybicki, *Prawo do cyberobrony*, „Polska Zbrojna" 2009, nr 35, s. 14.

[17] *Cyberwojna na Kaukazie*, http://technologie.gazeta.pl/technologie/1,89479,5575376 (dostęp: 22.09.2011).

[18] *Wirus w wirówkach*, „Polska Zbrojna" 2011, nr 5, s. 10.

[19] *Stuxnet, najgroźniejszy wirus świata. Czy to dzieło izraelskiego wywiadu*? – zob. newsweek.pl/stuxnet (dostęp: 23.03.2011).

[20] *Foreign Spies Stealing US Economic Secrets in Cyberspace, październik 2011 r.*, www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (dostęp: 20.05.2012).

szczególnie danych gospodarczych dotyczących nowoczesnych technologii, przemysłu obronnego, farmaceutycznego itp. Jak donosi Onet (22.12.2016 r.) na podstawie ujawnionego raportu CrowdStrike, firmy zajmującej się cyberbezpieczeństwem, rosyjskim hakerom udało się dokonać cyberataku w ukraińskiej armii poprzez zainstalowanie złośliwego oprogramowania na telefonach żołnierzy. Dzięki temu separatyści mieli dokładne dane na temat pozycji ukraińskiej armii i mogli prowadzić skuteczny ostrzał. Oryginalna aplikacja, napisana na system Android przez ukraińskiego oficera artylerii Jarosława Szerstiuka, pozwalała skrócić czas namierzania celu ostrzału dla używanych przez Ukraińców haubic D-30 z kilku minut do mniej niż 15 sekund. Żołnierzy zachęcano do pobierania aplikacji w mediach społecznościowych. Jak przyznawał sam Szerstiuk w wywiadach prasowych, ponad 9 tys. żołnierzy korzystało z aplikacji. Wprowadzali do niej m.in. swoją dokładną pozycję.

Z raportu CrowdStrike wynika, że od końca 2014 r. aż do 2016 r. wirus rozprzestrzeniał się wśród ukraińskich żołnierzy, dostarczając separatystom dokładnych danych dotyczących rozmieszczenia jednostek artyleryjskich przeciwnika. CrowdStrike sugeruje, że mogło to być przyczyną niezwykle wysokich strat poniesionych przez siły ukraińskie. Z ogólnodostępnych danych wynika, że armia Ukrainy straciła ponad 50% broni artyleryjskiej w ciągu dwóch lat trwania konfliktu i ponad 80% haubic D-30. To największy odsetek strat wśród wszystkich rodzajów broni znajdującej się na wyposażeniu ukraińskiej armii. Twórcy raportu uważają, że takie działanie nie może być efektem pracy amatorów, lecz hakerów na usługach GRU, rosyjskiego wywiadu wojskowego. CrowdStrike zidentyfikował autorów wirusa jako grupę posługującą się takimi nazwami, jak „APT 28" czy „Fancy Bear". To ci sami ludzie, którzy według CIA i FBI mieli się włamać do systemów Partii Demokratycznej podczas kampanii prezydenckiej w USA.

Android jest obecnie najczęściej atakowanym mobilnym systemem operacyjnym na świecie. Co gorsza, liczba nowych rodzajów ataków i złośliwego kodu infekującego urządzenia pracujące pod kontrolą Androida dynamicznie wzrasta. Zainteresowanie cyberprzestępców platformą mobilną wynika oczywiście z popularności tego systemu wśród użytkowników smartfonów i tabletów. Zgodnie z raportem Gartnera, ponad 86% użytkowników urządzeń mobilnych korzysta właśnie z Androida, a niecałe 13% korzysta z systemu iOS. Firma F-Secure, jeden z popularnych producentów oprogramowania ochronnego na wszystkie platformy systemowe, podała, że w ostatnim czasie otrzymuje do analizy dziennie ponad 9 tys. zakażonych próbek.

Android jest bezsprzecznie najczęściej atakowaną platformą mobilną. Niezależne niemieckie laboratorium antywirusowe – AV-Test – udostępniło statystyki dotyczące liczebności ataków na urządzenia mobilne pracujące pod kontrolą tego systemu. Od stycznia 2013 r. zanotowano już łącznie ponad 15 mln próbek złośliwego oprogramowania. O dynamice wzrostu liczby ataków świadczy szybko zwiększająca się liczba zagrożeń w ostatnim czasie. Dla porównania, w całym 2015 r. laboratorium odnotowało około 4,5 mln zakażonych plików, natomiast w 2016 r. tylko do sierpnia było ich już ponad 7 mln. Problem coraz intensywniejszych ataków przeprowadzanych przez cyberprzestępców na posiadaczy urządzeń pracujących pod kontrolą systemu Android wynika głównie z braku masowych, regularnych aktualizacji tego

oprogramowania. Mimo że oficjalnie na rynku mamy już Androida 7.1.1., to jeszcze w sierpniu 2016 r. zaledwie 18,7% użytkowników smartfonów i tabletów miało na swoich urządzeniach system Android 6.0 Marshmallow, a olbrzymia większość pozostałych wciąż używa znacznie starszych odmian tego systemu mobilnego. W przypadku systemu iOS ten problem nie istnieje – zaledwie po kilku dniach od udostępnienia nowej wersji oprogramowania systemowego instaluje je ponad połowa użytkowników mobilnego sprzętu Apple[21].

W listopadzie 2014 r. NATO przeprowadziło największe na świecie ćwiczenia dotyczące cyberbezpieczeństwa, w których wzięło udział ponad 670 żołnierzy i cywilów z 80 organizacji i instytucji w 28 krajach. Manewry odbyły się w Tartu, na wschodzie Estonii, zaledwie 50 km od granicy z Rosją. Brytyjska gazeta nazywa ćwiczenia zarówno „imponującymi, jak i potrzebnymi" i dodaje, że „[…] od kiedy kryzys na Ukrainie wywołał impas w stosunkach Sojuszu z Rosją, na jaw wyszła cybernetyczna słabość NATO. […] kluczowe natowskie sieci dziennie narażone są na ponad 200 milionów podejrzanych zdarzeń. Prawie wszystkie to spam mailowy, ale co najmniej 100 wymaga dalszych badań, a ok. 30 okazuje się wysoce wyrafinowanymi próbami cyberszpiegowskimi". „Cyberataki mogą być równie niebezpieczne co ataki konwencjonalne. Mogą wyłączyć ważną infrastrukturę i mogą mieć wielki wpływ na nasze działania" – oświadczył szef NATO Jens Stoltenberg podczas wizyty w Tallinie[22].

Admirał Michael Rogers, który stoi również na czele „wojsk internetowych" Stanów Zjednoczonych, stwierdził, że „nie tylko Chiny, lecz również dwa inne państwa, których nie wymienił z nazwy, są w stanie w każdej chwili spowodować wyłączenie systemu energetycznego USA lub inne fragmenty infrastruktury publicznej o kluczowym znaczeniu. Co więcej, w USA ukazał się raport, którego autorzy przewidują nadchodzący cyberatak na infrastrukturę USA o katastrofalnych konsekwencjach, powodujący utratę życia i zniszczenia mienia na kolosalną skalę: mógłby on nastąpić już w okolicach 2025 roku. Cyberatak na elektrownie czy wodociągi może sparaliżować państwo i gospodarkę"[23].

Przedstawione przykłady obejmują zjawisko nazwane cyberprzestępczością. ***Cyberprzestępczość jest zjawiskiem narastającym, niebezpiecznym i przynoszącym przestępcom dochody większe niż handel bronią czy też handel narkotykami.*** W polskim prawie nie ma oficjalnej definicji cyberprzestępczości. Cyberprzestępstwo dotyczy przestępstw popełnianych w Internecie, za pomocą Internetu oraz przestępstw popełnianych za pomocą komputera.

Cyberprzestępczość według Rady Europy[24] dotyczy:

- fałszerstw komputerowych;
- oszustw komputerowych;

[21] M. Kowalski, *Android na celowniku cyberprzestępców,* http://softonet.pl/publikacje/aktualnosci/Android.na.celowniku.cyberprzestepcow,1876 (dostęp: 20.12.2016).

[22] http://wiadomosci.onet.pl/swiat/financial-times-nato-przeprowadzilo-wielkie-manewry-cybernetyczne/lr4sk (dostęp: 21.11.2014).

[23] „Gazeta Wyborcza" z 22.11.2014 r., Onet (dostęp: 22.11.2014).

[24] Na podstawie „Konwencji Rady Europy o cyberprzestępczości", sporządzonej w Budapeszcie dnia 23 listopada 2001 r., ogłoszonej w Warszawie 27 maja 2015 r. (Dz.U. 2015, poz. 728).

- przestępstw związanych z charakterem informacji zawartych w systemie informatycznym (np. z treściami pedofilskimi);
- przestępstw związanych z naruszaniem praw autorskich i praw pokrewnych.

Definicja cyberprzestępczości według Unii Europejskiej, przyjęta w 2007 r., zakłada, że cyberprzestępstwa składają się z 4 rodzajów przestępstw[25]:

- wymierzane przeciwko poufności, integralności danych, np. hacking, nielegalny podsłuch, szpiegostwo komputerowe, sabotaż komputerowy;
- przestępstwa „klasyczne" popełniane przy użyciu komputera, np. oszustwa komputerowe, fałszerstwo dokumentów, wyłudzenia towarów lub usług;
- przestępstwa „contentowe" (dotyczące zawartości komputerów, serwerów), np. dziecięca pornografia, dostarczanie instrukcji przestępczych (typu „jak zbudować bombę"), zakazane treści rasistowskie, faszystowskie;
- przestępstwa powiązane z naruszeniem praw autorskich i praw pokrewnych.

## Główniejsze wydarzenia związane z działalnością cyberprzestępczą w Polsce w 2015 r.[26]

Styczeń przynosi informacje o błędach w domenie GOV.pl. W sieci pojawia się raport pod tytułem ALERT(666) E-ZINE #1, którego autor informował, że stworzył ów raport, by zwrócić uwagę na problem bezpieczeństwa tej części sieci.

Na początku roku miał miejsce „poważny atak hakerski na prywatną pocztę elektroniczną osób pracujących w Ministerstwie Obrony Narodowej i Sztabie Generalnym Wojska Polskiego". Taką informację opublikował w marcu 2015 r. tygodnik „Wprost" a w listopadzie potwierdził ten atak były doradca Ministra Obrony Narodowej Krzysztof Bondaryk.

W kwietniu zaobserwowaliśmy masową kampanię rozsyłania na skrzynki e-mail fałszywych wiadomości, pochodzących rzekomo od Allegro, informujących o „włamaniu" na konto z prośbą o kliknięcie w zawarty w wiadomości link w celu odblokowania konta. W rzeczywistości strona wyłudzała opłatę. Wiadomość przychodziła z podrobionego adresu security@allegro.pl

Drugi kwartał zaczął się więc z phishingiem i to zjawisko będzie już towarzyszyło polskim internautom do końca roku. Z początkiem maja w skrzynkach polskich internautów, a w szczególności kont przypisanych do kont firmowych, pojawiły się informacje, rzekomo od Poczty Polskiej. Maile z załącznikami ze złośliwym oprogramowaniem typu ransomware, czyli szyfrującym pliki na dysku i wymuszającym wpłaty za ich odszyfrowanie. Jego najbardziej znanym przypadkiem jest Crypto-Locker.

W maju polscy internauci masowo dostają e-maile z zainfekowanymi załącznikami, w których rzekomo była wystawiona faktura.

---

[25] www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298370,Czym-jest-cyberprzestepstwo.html (dostęp: 22.03.2017).

[26] www.cybsecurity.org/wpcontent/uploads/2016/02/RaportFBC_Cyberzagrozenia_2016.pdf (dostęp: 27.12.2016).

W czerwcu cyberprzestępca ukrywający się pod pseudonimem „Polsilver" włamał się do systemu informatycznego Plus Banku i szantażował ten bank, domagając się pieniędzy. Został zatrzymany na początku września. Ten przypadek był tematem wielu dyskusji i w jasny sposób wskazał na realne zagrożenie związane z bezpośrednim atakiem na infrastrukturę banku, a nie, jak bywa w większości przypadków – na komputery klientów bankowości elektronicznej.

Również w czerwcu Polskie Linie Lotnicze LOT poinformowały o awarii systemu teleinformatycznego, w wyniku której uziemiono kilkadziesiąt lotów.

Koniec lipca to StageFright – największa do tej pory dziura, jaką odkryto w Androidzie. Jeden MMS może umożliwić przejęcie kontroli nad większością smartfonów działających pod kontrolą systemu Android. Ofiara nie musi wykonywać żadnej akcji, nawet nie zorientuje się, że została zaatakowana, dlatego że udany atak spowoduje skasowanie śladów włamywacza z telefonu ofiary.

W sierpniu ponownie słyszymy o problemach dotyczących Androidów. Poważna dziura w Androidach podmienia zainstalowane aplikacje na fałszywe. Eksperci szacują, że problem dotyczy około 55% telefonów z Androidem, a za błąd odpowiedzialna jest klasa OpenSSLX509Certificate. Dziura pozwala podnieść uprawnienia aplikacji do poziomu uprawnień systemowych.

Pojawiają się również dane dłużników Getin Banku i Noble Banku. Na Torepublic sprzedawca korzystający z nicka „alialbania" zamieszcza ofertę sprzedaży listy zawierającej dane 18 000 dłużników, ujawniając w celu uwiarygodnienia oferty dane pierwszych 100 osób z listy. Do włamania doszło poprzez przejęcie kontroli nad komputerem pracownika banku.

We wrześniu odnotowano trzy nowe kampanie ataków złośliwego oprogramowania na polskich internautów. Wszystkie dotyczyły informacji rzekomo wysyłanych przez polskie firmy. Kampanie zawierały wezwanie do zapłaty, internauci otrzymywali faktury i dodatkowo np. wezwanie do zapłaty, pojawiła się również kampania mówiąca o protokole odbioru robót.

Listopad to kolejna kampania phishingowa, fałszywe e-maile tym razem podszywające się pod Polskie Koleje Państwowe, próba wyłudzania opłaty za SMS Premium.

Przedstawione przypadki cyberataków sugerują pytania o bezpieczeństwo w cyberprzestrzeni w Polsce. Zdaniem ekspertów, największe szkody w gospodarce spowodowałby atak na systemy energetyczne. Jednak uzależnienie naszego kraju od rozwiązań informatycznych, nadal mniejsze w stosunku do Zachodu, paradoksalnie zwiększa nasze bezpieczeństwo.

Jak wynika z badań polskich ekspertów zestawionych w tabeli 1, zagrożenie klasyczne, czyli akcje phishingowe, nadal dominuje. Podobnie jak w latach 2014–2015, można tylko odnotować przesunięcie się balansu z phishingu WWW na pocztę elektroniczną.

Zagrożenia związane z systemem operacyjnym Android to ponownie druga pozycja wśród liderów najbardziej prawdopodobnych zagrożeń. Powodem wysokiego stopnia zagrożeń jest otwarta architektura dystrybucji aplikacji i niewielka skłonność użytkowników do aktualizacji swoich systemów. Taką samą ocenę zebrało zagrożenie związane z wyciekami danych, co skłania cyberprzestępców do działań

**Tabela 1**

**Największe zagrożenia dla bezpieczeństwa w Internecie w 2016 roku – głos polskich ekspertów**

**Table 1**

**Greatest dangers of the year 2016 Internet safety – the voice of polish experts**

| Rodzaj zagrożeń | P[1] | P[2] |
|---|---|---|
| Phishing e-mail and WWW | **4,33** | 3,37 |
| Wycieki baz danych (dane osobowe, hasła, nr kart kredytowych itd.) | **4,21** | **4,12** |
| Zagrożenia dla platformy Android | **4,21** | 3,52 |
| APT – ataki ukierunkowane na organizacje, połączone ze spear phishingiem | **4,19** | **4,24** |
| Akcje cyberszpiegowskie na tle politycznym | 3,95 | **4,05** |
| Zagrożenia typu ransomware/scareware | 3,88 | 3,36 |
| Ataki DDoS na podmioty komercyjne | 3,86 | 3,50 |
| Zagrożenia w serwisach społecznościowych | 3,81 | 2,88 |
| Ataki Driver-by Download/Watering Hole | 3,71 | 3,36 |
| Powstawanie botnerów opartych o platformy mobilne | 3,69 | 3,17 |
| Cyberkonflikty pomiędzy państwami powiązane z atakami dedykowanymi | 3,67 | **4,31** |
| Ataki DDoS na administrację publiczną | 3,61 | 3,07 |
| Kradzież wirtualnych walut | 3,52 | 2,74 |
| Haktywizm | 3,43 | 2,67 |
| Ataki na system DNS | 3,36 | 3,69 |
| Ataki na system sterowania przemysłowego ICS/SCADA | 3,36 | **4,55** |
| Ataki na cloud computing | 3,33 | 3,88 |
| Zagrożenia związane z BYOD | 3,33 | 2,90 |
| Zagrożenia dla platformy iOS | 3,29 | 3,26 |
| Zagrożenia związane z „Internet of Things" (IoT) | 3,21 | 3,15 |
| Zagrożenia dla platformy Windows Phone/Mobile | 3,20 | 3,10 |
| Ataki na platformy hostingowe | 3,19 | 3,37 |
| Wykorzystanie gier sieciowych w atakach | 2,90 | 2,45 |
| Ataki na urządzenia medyczne | 2,36 | 3,95 |

**P[1] –** prawdopodobieństwo wystąpienia

**P[2]** – siła oddziaływania danego zagrożenia; wszystkie wartości oceny odnoszą się do skali 1–5 (1 – najmniejsze prawdopodobieństwo, 5 – największe prawdopodobieństwo)

Źródło: opracowanie własne na podstawie:
www.cybsecurity.org/wpcontent/uploads/2016/02/RaportFBC_Cyberzagrozenia_2016.pdf

wymuszających okup lub chcących skompromitować zaatakowaną organizację. Nie wszystkie zagrożenia wskazywane jako najbardziej prawdopodobne (kolumna $P^1$ w tabeli) jednocześnie wskazywane były podczas badań jako te, których konsekwencje wystąpienia byłyby najbardziej dokuczliwe i najgroźniejsze ($P^2$ w tabeli). Od lat eksperci identyfikują te same obszary najbardziej groźnych cyberataków.

W 2016 r. nastąpiło jednak kilka istotnych zmian w stosunku do 2015 r.:

- za jeszcze bardziej niebezpieczne uznane zostały ataki na systemy sterowania przemysłowego (wzrost z **4,33** na **4,55**);
- wzrosła ocena zagrożenia związana z atakami na platformy mobilne, w szczególności na system Android (wzrost z **3,15** na **3,52**), na iOS (z **3,00** na **3,26**) oraz Windows Phone/Mobile (z **2,80** na **3,10**);
- spadła ocena zagrożenia związana z atakami typu DDoS, zarówno na organizacje komercyjne (z **3,58** na **3,50**), jak i na administrację publiczną (z **3,38** na **3,07**).

Eksperci, których wyniki badań zawiera raport[27], oprócz zagrożeń wskazanych w tabeli 1, zaproponowali również własne:

- ataki na systemy płatności internetowych,
- ataki na sieci bezprzewodowe (WiFi, GSM),
- zatruwanie informacji w ogólnodostępnych systemach bezpieczeństwa (np. w serwisach virustotal.com, malwr.com),
- shadow IT / Insider (nieautoryzowane rozwiązania IT wewnątrz organizacji),
- inwigilacja realizowana np. poprzez miejski monitoring,
- kompromitacja urządzeń biometrycznych,
- systemy komputerowe instalowane w środkach komunikacji oraz w gospodarstwach domowych,
- ataki terrorystyczne wspomagane atakami na infrastrukturę,
- ransomware na platformy serwerowe,
- wykorzystanie podatności w aplikacjach webowych.

W cytowanym raporcie przedstawione są również wypowiedzi ekspertów z dziedziny cyberzagrożeń. Oto niektóre z nich:

- Przyszłe zagrożenia[28], które będą dominowały za 3–5 lat będą ściśle powiązane z wdrażaniem nowych technologii, które dotychczas są wykorzystywane w wąskim zakresie i dlatego uważa się je za bezpieczne. Przykładem może być biometryka.
- W 2016 r. zagrożenia dotyczące systemów mobilnych znajdą się już w głównym nurcie problemów bezpieczeństwa. We wszystkich obszarach potrzebny będzie większy nacisk na monitorowanie i szybką reakcję[29].
- 2015 r. pokazał, że nie musimy sami infekować się złośliwym oprogramowaniem, bo robią to za nas producenci naszego sprzętu, m.in. firmy Lenovo (SuperFish) czy Dell (eDellRoot), a z ataków na tzw. Internet of Things dalej

[27] Tamże.
[28] Jakub Bojanowski, Partner Deloitte Polska, Raport FBC…, s. 13.
[29] Arkadiusz Buczek, Specjalista ds. Cyberbezpieczeństwa T-MOBILE POLSKA S. A., tamże, s. 13.

nie wynika żadne realne zagrożenie dla przeciętnego Kowalskiego. Skłaniam się więc do tezy, że dalej borykać będziemy się z:

a) socjotechniką i użytkownikami bezmyślnie klikającymi na linki i załączniki w podrobionych e-mailach,
b) kontami przejmowanymi ze względu na słabe lub domyślne hasło oraz
c) brakiem wyobraźni producentów oprogramowania, prowadzącym do pojawiania się w ich rozwiązaniach znanych od lat błędów[30].

- Olbrzymie zyski cyberprzestępców z szantażowania firm oraz zwykłych użytkowników za pomocą złośliwego oprogramowania typu ransomware, sprawiły, że rok 2016 (i kolejne – dop. autora) będzie obfitował w jeszcze bardziej wyrafinowane sposoby szantażu. Może to być np. ransomware albo szantaż związany z blokowaniem dostępu do popularnych usług. Coraz częściej będziemy mieli do czynienia z sytuacją, w której cyberprzestępcy będą szantażowali firmy, iż opublikują ich wrażliwe dokumenty, jeśli nie zostaną spełnione finansowe oczekiwania. Z uwagi na olbrzymią skuteczność i braki w edukacji związanej ze świadomością zagrożeń, możemy spodziewać się jeszcze większej liczby kampanii wykorzystujących najsłabsze ogniowo, czyli użytkownika[31].
- To co przewidywałem rok temu, czyli wzrost cyberzagrożeń na tle politycznym, niestety się sprawdziło. Nie widzę przyczyny, dla której ten trend miałby się odwrócić. Myślę, że może wręcz narastać, o czym świadczą chociażby ostatnie masowe ataki na sieci i serwisy w Turcji. Ten problem będzie dotyczyć zarówno rozgrywek na poziomie państw, jak i haktywizmu. Dodatkowo sądzę, że jeszcze bardziej może dać się we znaki powszechne atakowanie Internetu Rzeczy. Po serii ataków raczej będących ciekawostkami, możliwe jest wystąpienie ataków o poważnych, niebezpiecznych konsekwencjach[32].

## Prognozowane cyberzagrożenia w roku 2017

Oto wybrane przewidywania ekspertów z firmy F-Secure[33] dotyczące cyberzagrożeń:

- Zagrożenia USA przez chińskich cyberszpiegów

W 2016 r. głośno mówiło się o szpiegostwie ze strony Rosjan, a nawet o ich zaangażowaniu w proces wyborów prezydenckich w USA. Jednak prawdziwe zagrożenie, z którym powinna liczyć się nowo wybrana władza w Stanach Zjednoczonych, może nadejść ze strony Chin. W 2015 r. amerykańskie Biuro ds. Zarządzania Personelem (*Office of Personnel Management*) poinformowało o wykryciu naruszenia bezpieczeństwa danych, które mogło dotyczyć nawet 14 mln osób.

---

[30] Piotr Konieczny, Chief Information Security Officer, Niebezpiecznik, tamże.
[31] Borys Łącki, Pentester LogicalTrus, tamże, s. 14.
[32] Mirosław Maj, CEO / CIO Fundacja Bezpieczna Cyberprzestrzeń / ComCERT.PL, tamże.
[33] http://di.com.pl/cyberzagrozenia-w-2017-roku-przewidywania-ekspertow-f-secure-56190 (dostęp: 28.12.2016).

- Złośliwe oprogramowanie przez Wi-Fi – (Sean Sullivan, doradca ds. bezpieczeństwa)

Destrukcyjne możliwości botnetów i ataków DDoS to trend, który utrzyma się w przyszłym roku. Potencjalnie może zostać stworzony pierwszy „robak Wi-Fi", czyli szkodliwe oprogramowanie, które szybko rozprzestrzeniałoby się w obszarach miejskich w wyniku zainfekowania routerów za pomocą sieci bezprzewodowej. Zainfekowane urządzenie zawierałoby kod, który kopiowałby się w routerach za pomocą połączenia z siecią Wi-Fi. Po zainfekowaniu danego routera robak próbowałby replikować się na innych urządzeniach.

- Europejska debata na temat kryptografii – (Erka Koivunen, dyrektor ds. bezpieczeństwa informacji)

Kryptografia stanowi fundament dla bezpieczeństwa cyfrowej informacji. Dzięki zastosowaniu kryptografii informacje przechowywane lub przesyłane w formie elektronicznej są chronione przed szpiegami, przestępcami i nieuczciwymi firmami.

- Więcej ataków DDoS z wykorzystaniem Internetu Rzeczy – (Mika Ståhlberg, dyrektor ds. technicznych)

Atak na firmę Dyn z wykorzystaniem złośliwego oprogramowania Mirai stanowił niemałe zaskoczenie w 2016 r. Ogromne zainteresowanie ze strony mediów to efekt uboczny niezrozumienia przez producentów, jak dużym zagrożeniem jest brak odpowiednich zabezpieczeń ich urządzeń z kategorii Internetu Rzeczy (IoT).

Urządzenia IoT są na wczesnym etapie rozwoju technologicznego i pojawiają się pewne wady, których nie były w stanie ujawnić testy w kontrolowanych warunkach laboratoryjnych. Po ataku z użyciem oprogramowania Mirai pewna firma wycofała z produkcji swoje kamery internetowe, zdając sobie sprawę z tego, że luka w zabezpieczeniach konkretnego modelu może zostać wykorzystana przez hakerów. W 2017 r. urządzenia IoT będą w większym stopniu wykorzystywane do przeprowadzania ataków DDoS. Następnym etapem, który zapewne nastąpi w 2018 r., będzie atakowanie samych użytkowników. Istotne jest, by rządzący, branża cyberbezpieczeństwa oraz producenci wspólnie zadbali o odpowiednią ochronę nowo powstałych inteligentnych środowisk.

- Człowiek i maszyna na straży cyberbezpieczeństwa

Szkodliwe oprogramowanie w klasycznym wydaniu jest coraz mniej skuteczne wobec zabezpieczeń punktów końcowych, które są obecnie dostępne. Hakerzy muszą wykazywać się bardziej innowacyjnym podejściem i większym zaangażowaniem niż kiedyś – ich działalność wymaga stosowania socjotechnik, na przykład z wykorzystaniem wiadomości e-mail do wyłudzenia danych (*phishing*). Innym sposobem może być też znalezienie zapomnianego przez administratora IT serwera i wykorzystanie go do spenetrowania sieci. Do nowych trendów na bieżąco dostosowuje się branża cyberzabezpieczeń. By sprostać nowym wyzwaniom w walce z zagrożeniami, niezbędne będzie połączenie sztucznej inteligencji oraz czynnika ludzkiego. Analiza ryzyka, testy penetracyjne, ocena zagrożeń, reagowanie na incydenty i analiza śledcza to tylko część zadań, które można usprawnić przez odpowiednią współpracę maszyny z człowiekiem. W 2017 r. właśnie ten rodzaj kooperacji będzie cieszył się największym zainteresowaniem podmiotów z branży.

Kolejne przewidywania w obszarze cyberbezpieczeństwa na rok 2017 przedstawiają eksperci firmy Fortinet[34]:

- Zautomatyzowane i naśladujące działania ludzi ataki będą wymagać inteligentniejszej ochrony

Zagrożenia stają się coraz bardziej inteligentne i zdolne do autonomicznego działania. W nadchodzącym roku należy spodziewać się złośliwego oprogramowania z adaptacyjnymi algorytmami uczenia się na podstawie udanych ataków. Malware nowej generacji będzie mieć orientację sytuacyjną, czyli będzie rozumieć swoje otoczenie i samodzielnie decydować o dalszych działaniach. Można powiedzieć, że program zacznie działać podobnie do człowieka prowadzącego atak: będzie rozpoznawać środowisko, identyfikować cele, wybierać odpowiednie metody ataku i inteligentnie unikać wykrycia.

- Producenci urządzeń Internetu Rzeczy (IoT) będą odpowiadać za naruszenia bezpieczeństwa

Ataki na urządzenia IoT mogą powodować ogromne zakłócenia i generować duże zyski. Staną się one coraz bardziej wyrafinowane i ukierunkowane na wykorzystywanie słabych punktów komunikacji IoT i całego łańcucha gromadzenia danych. Przewidujemy m.in., że powstaną gigantyczne Shadownety — botnety urządzeń IoT, których nie da się zobaczyć ani zmierzyć konwencjonalnymi narzędziami. Brak poprawy zabezpieczeń w urządzeniach z kategorii Internetu Rzeczy może mieć fatalny wpływ na cyfrową gospodarkę. Użytkownicy będą się wzbraniać przed ich zakupem w obawie przed cyberatakami. Będziemy świadkami rosnącej presji na dostawców tych urządzeń, mającej doprowadzić do utworzenia i egzekwowania standardów bezpieczeństwa, według których to producenci będą odpowiedzialni za działanie swoich produktów w obliczu cyberzagrożeń.

- 20 miliardów urządzeń Internetu rzeczy najsłabszym ogniwem w atakach na chmurę

Najsłabszym ogniwem bezpieczeństwa chmury nie jest jej architektura, lecz fakt, że dostęp do zasobów chmurowych mają miliony zdalnych urządzeń. W nadchodzącym roku spodziewamy się wykorzystania urządzeń końcowych do włamań i ataków na dostawców chmury. Firmy i instytucje będą coraz częściej wdrażać całościowe strategie ochrony oraz segmentacji, pozwalające na tworzenie, zarządzanie i wzmacnianie spójnych polityk bezpieczeństwa pomiędzy środowiskami fizycznym, wirtualnym i chmurowym.

- Inteligentne miasta znajdą się na celowniku cyberprzestępców

Wraz z coraz większą popularnością systemów automatyzacji i zarządzania wzrośnie liczba cyberataków skierowanych przeciwko nim. Potencjalna przestrzeń ataków na takie środowisko jest gigantyczna – celem mogą być czujniki, oświetlenie, systemy ogrzewania i wentylacji, alarmy pożarowe, systemy kierowania ruchem, windy, systemy awaryjne itd. Skuteczne włamanie do dowolnego ze zintegrowanych systemów mogłoby ogromnie zakłócić życie społeczeństwa. Ostatnio doszło już do wycieku danych z systemów dużej amerykańskiej sieci handlowej w wyniku wyko-

[34] www.conowego.pl/aktualnosci/jakie-cyberzagrozenia-czekaja-nas-w-2017-roku-infografika-20378 (dostęp: 25.11.2016).

rzystania luki w zabezpieczeniach systemu ogrzewania i wentylacji sterowanego z użyciem protokołu IP. Systemy te staną się cennymi celami dla cyberprzestępców i cyberterrorystów.

- Ostatnia fala ransomware to tylko otwarcie bramy

Spodziewamy się bardzo precyzyjnych ataków wymierzanych m.in. w celebrytów, polityków i duże organizacje. Poza samym blokowaniem dostępu do systemów, ataki te będą się też zapewne wiązać z kradzieżą poufnych lub osobistych danych, używanych następnie do wymuszeń i szantażu. Można też oczekiwać, że koszty okupów związanych z takimi atakami będą coraz wyższe. Ataki wymierzone w zwykłych użytkowników i obywateli były dotychczas nieopłacalne dla napastników — okup, jaki przeciętny użytkownik byłby gotów zapłacić za odblokowanie dysku twardego, samochodu lub drzwi wejściowych czy też wyłączenie alarmu pożarowego, jest po prostu za mały. Przewidujemy, że w 2017 r. nastąpi przełamanie tej bariery poprzez wprowadzenie ataków zautomatyzowanych, które pozwolą przestępcom masowo wymuszać niewielkie haracze od wielu ofiar jednocześnie. Szczególnie narażone staną się urządzenia IoT.

- Technologia odpowiedzią na problem braku specjalistów ds. cyberbezpieczeństwa

Współczesny brak wykwalifikowanych specjalistów ds. cyberbezpieczeństwa oznacza, że wiele organizacji i państw uczestniczy w gospodarce cyfrowej, będąc obarczonymi wielkim ryzykiem. Nie mają one doświadczenia i kompetencji koniecznych do stworzenia polityki bezpieczeństwa, ochrony krytycznych zasobów w różnych środowiskach sieciowych czy identyfikowania i odpowiedzi na zaawansowane ataki. Rozsądne firmy będą korzystać z usług doradców ds. bezpieczeństwa, którzy będą ich przewodnikami po zawiłym świecie bezpieczeństwa komputerowego, lub z oferty dostawców zarządzanych usług zabezpieczeń (MSSP), którzy zaproponują gotowe do użytku rozwiązanie zabezpieczające. Inną możliwością będzie przeniesienie większości infrastruktury do środowiska chmurowego, gdzie dodanie zabezpieczeń jest kwestią kilku kliknięć.

Inne prawdopodobne cyberzagrożenia w 2017 r. to:

- Tak zwane ataki pod fałszywą banderą

Ważnym problemem w walce z cyberprzestępcami staje się ustalenie autorstwa cyberataków. Działania w zakresie identyfikowania twórców danej kampanii cyberprzestępczej mogą spowodować ryzyko zastosowania technik kierujących badaczy na fałszywą ścieżkę.

- Wojna informacyjna

Coraz częściej stwierdza się przypadki ujawniania zhakowanych informacji dla agresywnych celów. Istnieje ryzyko, że cyberprzestępcy poprzez manipulowanie informacjami będą próbowali wykorzystać gotowość ludzi do przyjmowania fałszywych danych za prawdziwe.

- Podatność na cybersabotaż

Różnorakie systemy i obiekty infrastruktury krytycznej państwa są połączone z Internetem. przy czym często ich ochrona pozostawia wiele do życzenia lub po prostu nie istnieje, pokusa uszkodzenia lub zakłócenia ich pracy może okazać się łakomym kąskiem dla cyberprzestępców.

- Włamania do systemów płatniczych

Wraz ze wzrostem popularności i rozpowszechnienia systemów płatniczych rośnie zainteresowanie nimi również wśród cyberprzestępców. Możemy także spodziewać się na forach podziemia oferowania na sprzedaż wyspecjalizowanych zasobów lub szkodliwych działań w ramach modelu „atak jako usługa".

- Ransomware

Dalszy wzrost liczby oprogramowania ransomware z jednoczesnym malejącym zaufaniem atakowanych do twierdzenia, że wraz z zapłatą okupu nastąpi zwrot utraconych danych.

## Podsumowanie

Cyberzagrożenia stają się coraz liczniejsze, bardziej inteligentne, działają autonomicznie i są coraz trudniejsze do wykrycia. Powracają też stare zagrożenia, ale wzmocnione nowymi technologiami, które przekraczają kolejne granice unikania detekcji i wskazania sprawców. Powodują skutki różnego charakteru: bezpieczeństwa państwa, jego systemów, emocjonalne i finansowe różnych organizacji i obywateli. Cyberprzestępczość dotyka milionów rocznie, ale konsumenci (około 75% wszystkich legalnych stron internetowych) nadal nie podejmują działań w celu własnej ochrony. W 2015 r. 594 mln ludzi na całym świecie padły ofiarą przestępstwa internetowego. Ransomware rozszerzyło swoje działania przestępcze na dowolne urządzenia podłączone do sieci: smartfony, systemy Mac i Linux Symantec a nawet inteligentne zegarki i telewizory.

Straty powstałe w wyniku działalności cyberprzestępców na świecie wyniosły w 2011 r. 388 mld dolarów, w 2013 r. straty te wyniosły już 445 mld dolarów.

W celu ograniczenia tego niebezpiecznego trendu konieczne jest pilne wzięcie odpowiedzialności na wielu poziomach, które obejmują dostawców zabezpieczeń, rządy państw, jak i konsumentów. Bez szybkiego działania istnieje poważne ryzyko zaburzenia rozwoju globalnej, nie tylko cyfrowej gospodarki.

## Bibliografia

*Estonia leczy rany po pierwszej cyberwojnie*, „Gazeta Wyborcza", 1 czerwca 2007.

Rybicki R., *Prawo do cyberobrony*, „Polska Zbrojna" 2009, nr 35.

Szubrycht T., *Cyberterroryzm, jako nowa forma zagrożenia terrorystycznego*, „Zeszyty Naukowe AMW" 2005, XLVI, nr 1 (160).

*Wirus w wirówkach*, „Polska Zbrojna" 2011, nr 5.

„Konwencja Rady Europy o cyberprzestępczości", sporządzona w Budapeszcie dnia 23 listopada 2001 r., ogłoszona w Warszawie 27 maja 2015 r. (Dz.U. 2015, poz. 728).

Charles Herzfeld on ARPAnet and Computers (dostęp: 26.02.2014).

Cyberspace*: Definition and Implications*, Cooperative Cyber Defence Centre of Excellence, www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf dostęp: 20.05.2012).
*Cyberwojna na Kaukazie*, http://technologie.gazeta.pl/technologie/1,89479,5575376.
Denning D., *Cyberterrorism*, 2000, www.cs.georgetown.edu~denning/infosec/cyberterror-GD.doc, (dostęp: 27.03.2004).
*Foreign Spies Stealing US Economic Secrets in Cyberspace*, październik 2011 r., www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf (dostęp: 20.05.2012).
Galan D., *Cyberterroryzm jako nowe wyzwanie społeczeństwa informacyjnego*, http://academicon.pl/blogi_naukowe/bezpieczenstwo-w-sieci/cyberterroryzm-jako-nowe-wyzwanie-spoleczenstwa-informacyjnego (dostęp: 20.11.2016).
Garrison L., Grand M., *Cyberterrorism*, 2001, *An evolving concept, NIPC highlights*, www.Nopc.gov./publication/highlight/2001/highlight-01-06.htm (dostęp: 04.04.2004).
„Gazeta Wyborcza", 22.11.2014 r., Onet (dostęp: 22.11.2014).
Historia Wirtualnej Polski SA. https://pl.wikipedia.org/wiki/Internet (dostęp: 27.01.2017).
Kowalski M., *Android na celowniku cyberprzestępców,* http://softonet.pl/publikacje/aktualnosci/Android.na.celowniku.cyberprzestepcow,1876 (dostęp: 20.12.2016).
Lewis A.J., *Assessing the risk of cyber terrorism, cyber war and other cyber threats*, 2002, Center for Strategic amd International Studies, www.csis.org/tech/0211lewis.pdf (dostęp: 27.03.2004).
Pollitt M.M., *Cyberterrorism – Fact or Fancy*, http://www.cs.georgetown.edu/~denning/infosechtml/pollitt, (dostęp: 04.04.2004).
*Stuxnet, najgroźniejszy wirus świata. Czy to dzieło izraelskiego wywiadu*? – zob. newsweek.pl/stuxnet, (dostęp: 23.03.2011).
*20 lat polskiego internetu*. di.com.pl. (dostęp: 03.01.2017).
https://pl.wikipedia.org/wiki/Cyberterroryzm
www.ccdcoe.org/articles/2010/Ottis_Lorents_CyberspaceDefinition.pdf (dostęp: 20.05.2012).
http://en.rian.ru/world/20070906/76959190.html (dostęp: 24.04.2012).
http://wiadomosci.onet.pl/swiat/financial-times-nato-przeprowadzilo-wielkie-manewry-cybernetyczne/lr4sk (dostęp: 21.11.2014).
www.cybsecurity.org/wpcontent/uploads/2016/02/RaportFBC_Cyberzagrozenia_2016.pdf (dostęp: 27.12.2016).
http://di.com.pl/cyberzagrozenia-w-2017-roku-przewidywania-ekspertow-f-secure-56190
www.conowego.pl/aktualnosci/jakie-cyberzagrozenia-czekaja-nas-w-2017-roku-infografika-20378 (dostęp: 25.11.2016).
www.infor.pl/prawo/prawo-karne/przestepstwa-komputerowe/298370,Czym-jest-cyberprzestepstwo.html (dostęp: 22.03.2017).
https://us.norton.com/cyber-security-insights (dostęp: 24.01.2017).

## Summary

Countries' vulnerability to cybernetic dangers, including cyberterrorism, increases. Recent years examples from Poland and world countires presented in the article below suggest that such tendency will continue to rise, since modern community functioning is inseparably connect with the provision of constant and well-functioning automatic sys-

tems, to match the supply of basic needs services such as (data storage and transmission, monitoring and control processes, management support, etc.). An act of violence or cybernetic terror activity may be employed by the enemy countries government and agencies, international concerns, non-government organized crime groups, network associated groups or even individuals. The objectives of such terrorism may be critical infrastructure elements, banking systems, weapon systems, homeland security systems or even individual Internet users. Cyber-attacks can deal massive economical loss reaching hundreds of millions of dollars annually. Predicting the future, cyber-attacks may be commonly practiced by organized crime groups as extortion or become embers of cyberconflict or even cyberwar.