Halina Świeboda

Kształtowanie bezpieczeństwa cyberprzestrzeni

Ekonomiczne Problemy Usług nr 117, 777-785

2015

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 852 EKONOMICZNE PROBLEMY USŁUG NR 117 2015

HALINA ŚWIEBODA
Akademia Obrony Narodowej[1]

KSZTAŁTOWANIE BEZPIECZEŃSTWA CYBERPRZESTRZENI[2]

Streszczenie

Do istotnych problemów współczesnego społeczeństwa należy zaliczyć te, które generowane są dzięki rozwojowi technologii ICT. W szczególności dotyczy to zagrożeń, które pojawiły się wraz z ich zastosowaniem. Skutki zagrożeń wpływają na poziom bezpieczeństwa, który w istotny sposób warunkuje jakość życia społecznego i zapewnia stabilny rozwój społeczno-gospodarczy. W artykule przedstawiono wyniki analiz tendencji rozwoju ICT i ewoluujących zagrożeń, które stanowią podstawę kształtowania polityki bezpieczeństwa cyberprzestrzeni w kontekście bezpieczeństwa narodowego.
Słowa kluczowe: technologie ICT, bezpieczeństwo, cyberprzestrzeń, zagrożenia.

Wprowadzenie

Technologie ICT są dynamicznie rozwijającym się i jednym z najbardziej innowacyjnych sektorów, który ma bardzo duży wpływ na działania, procesy i efektywność w innych sektorach gospodarki. Polski rynek ICT szacuje się na prawie 16 mld USD (EITO, 2013), co daje Polsce 9 miejsce w Unii Europejskiej. Sektor ten odgrywa coraz większą rolę w strukturze Produktu Krajowego Brutto Polski oraz wpływa na profil eksportu. Aktualny udział ICT w tworzeniu polskiego PKB

---

[1] Wydział Bezpieczeństwa Narodowego, Instytut Inżynierii Systemów Bezpieczeństwa.

[2] Treści zawarte w niniejszym artykule odnoszą się do wybranych rezultatów badań przeprowadzonych w ramach projektu realizowanego w zakresie bezpieczeństwa i obronności państwa pt. „System Bezpieczeństwa Narodowego RP" finansowanego ze środków Narodowego Centrum Badań i Rozwoju na podstawie umowy nr DOBR/0076/R/ID1/2012/03 z dnia 18.12.2012 r. (kier. nauk. W. Kitler).

szacowany jest obecnie na ok. 5%, natomiast w 2020 roku szacuje się, że ma osiągnąć od 9% do 13% PKB, resort gospodarki prognozuje wzrost nawet o 15%.

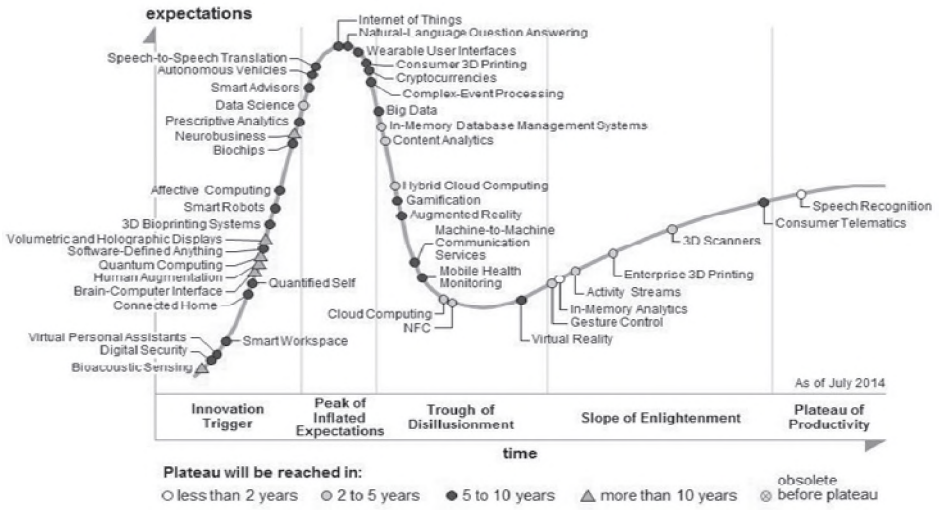
Szybkość, z jaką pojawiają się kolejne rozwiązania i zastosowania technologii, jest imponująca, przy tym niektóre rozwiązania pozostają tylko gadżetami, gdy inne innowacje są absorbowane w społeczeństwie. Oczekiwane zmiany, które mogą nastąpić w ciągu najbliższych 10 do 20 lat w obszarze ICT, to zmiana mocy i wielkości komputerów. Wśród trendów, które konsekwentnie są realizowane w obszarze technologii, w ujęciu globalnym, a które będą miały wpływ na bezpieczeństwo w przyszłości, wymienić można (Global ICT Developments and Trends 2030): komputer kwantowy, sieci semantyczne (Semantic Web, Web 3.0), rozwój serwisów społecznościowych i Web 2.0, komunikację mobilną, wzrost ilości danych, *cloud computing*. Prognozuje się (IDG 2013, Gartner 2013), że segment rozwiązań mobilnych będzie miał największą dynamikę wzrostu, a w roku 2015 tablety staną się podstawowymi narzędziami działów sprzedaży.

Więcej urządzeń mobilnych oznacza większe problemy z bezpieczeństwem dostępu, a także sprawnym zarządzaniem terminalami, wydajnością sieci, sprzętu i logiką systemu. Wzrost ilości danych stawia wyzwania dla systemów bezpieczeństwa w odniesieniu do zasobów danych w obszarze poszukiwania bezpiecznego, skutecznego przetwarzania i analizowania. Obok wyzwań w dziedzinie systemów bezpieczeństwa wynikających z rozwijających się technologii istnieje „ciemna" strona wykorzystania cyberprzestrzeni przez przestępców działających z bardzo różnych pobudek. Dynamiczny wzrost cyberzagrożeń, których skutki coraz częściej dotykają bezpieczeństwa państwa, wymusza podejmowanie i przyspieszenie prac nad przepisami prawa, działań organizacyjnych oraz podejmowania współdziałania między podmiotami cywilnymi i wojskowymi, a także na arenie międzynarodowej w celu zwiększenia poziomu bezpieczeństwa cyberprzestrzeni.

1. Implikacje dla bezpieczeństwa cyberprzestrzeni

Fazy dojrzałości technologii w odniesieniu do poziomu entuzjazmu konsumentów i mediów prognozuje, od 1995 roku, firma badawcza Gartner Inc.[3] w postaci modelu, który w zasadzie jest wykresem przedstawiającym cykle życia technologii na rynku wskazującym, jaką drogę przebędzie dana technologia w ciągu kilku lat. Model jest „podpowiedzią" dla nowych możliwości inwestycyjnych, wskazuje również kierunek w zakresie rozwoju systemów bezpieczeństwa (rys. 1).

[3] Gartner Inc. z siedzibą w Stamford, Connecticut, jest uważana za lidera badań w zakresie technologii informatycznych i doradczych. Niedawno opublikowała roczny raport na temat cyklu Gartner Hype, którym zgłasza ponad 1900 najnowszych trendów dotyczących technologii, bezpieczeństwa i IT.



Rys. 1. Model prognozy rozwoju technologii 2014

Źródło: Gartner (August 2014).

Do niedawna niektóre prognozowane trendy w rozwoju techniki i technologii oraz zagrożeń wynikających z ich wykorzystania wydawały się przewidywaniem typu *science fiction*, by w niedługim czasie stać się faktem. Dobrym przykładem zobrazowania tej dynamiki są informacje zawarte w raporcie ITU (Internet Reports: The Internet of Things; Geneva, November 2005), w którym znalazły się zapewnienia o tym, że w niedługim czasie komunikacja typu maszyna – maszyna i człowiek – maszyna (komputer) zostanie rozszerzona i obejmie przedmioty codziennego użytku domowego po czujniki monitorujące ruchy *Golden Gate Bridge* i po systemy wykrywania ruchu (trzęsień) ziemi. Był to zwiastun nadejścia nowej epoki, w której „dzisiejszy" Internet (danych i ludzi) ustępuje jutrzejszemu Internetowi Rzeczy (*Things Technological*). Obecnie doświadczamy spełnienia się tych zapowiadanych technologicznych trendów w postaci np. nowych inteligentnych rozwiązań Smart Grid[4], np. dla przedsiębiorstw energetycznych, czy nowoczesnych rozwiązań dla laboratoriów (medycznych i innych) dzięki wdrożeniu technologii REPID (*Radio Frequency Identification*) w standardzie EPC (*Electronic Product Code*)[5]. Wdrożenie takich systemów niesie ze sobą wiele problemów w dziedzinie bezpieczeństwa zarówno na poziomie rozwiązań technicznych oraz prawnych krajowych i międzynarodowych, jak też organizacyjno-funkcjonalnych. Jednym

[4] Umożliwiają one dynamiczne zarządzanie sieciami przesyłowymi i dystrybucyjnymi za pomocą punktów pomiarowych i kontrolnych rozmieszczonych na wielu węzłach i łączach.

[5] Rozwiązanie to, zwane często „Internetem produktów", stanowi połączenie technologii Internetu i powszechnie stosowanej na rynku identyfikacji przy pomocy fal radiowych (RFID).

z problemów jest kwestia prywatności i bezpieczeństwa (Świeboda 2013). Zastosowania ich sprawiają, że wymagania dla systemów bezpieczeństwa stają się coraz większe.

Cyberprzestrzeń stała się globalnym rynkiem złośliwych kodów używanych do działalności przestępczej, działa jak supermarket ze specjalnymi ofertami i dyskontem. Średnia cena skomplikowanego trojana waha się w granicach od 350 do 700 USD, podczas gdy lista skrzynek pocztowych, które mogą być celem takiego programu, kosztuje ok. 100 USD za milion pozycji. Twórcy złośliwych kodów mają nawet oferty specjalne. Wykryto ośrodek sprzedający trojana do przechwytywania płatności, który był oferowany za 400 USD dla pierwszych stu kupujących, tj. o 33% taniej niż normalnie (Raport Panda Software). Cyberprzestępcy mogą nawet przetestować swoje złośliwe oprogramowanie na zabezpieczeniach stosowanych przez producentów oprogramowania do ochrony danych. Przykładowe ceny różnych usług oferowanych na podziemnych forach zaprezentowano w tabeli 1 (Raport Trend Micro). Nakład finansowy niezbędny do tego, aby rozpocząć karierę cyberprzestępczą, jest minimalny.

Tabela 1

Przykładowy serwis za 50 dolarów

Usługa	Koszt usługi	Charakterystyka usługi
Podstawowa wersja oprogramowania typu crypter z różnymi dodatkami	kosztuje od 30 do 80 dolarów	Szyfrowanie plików służy przede wszystkim do ukrycia zainfekowanych plików lub złośliwego oprogramowania przed skanerami bezpieczeństwa.
Usługi VPN na okres 3 miesięcy	kosztują od 50 do 55 dolarów	Połączenie VPN gwarantuje anonimowość, dając hakerom dostęp do stron WWW.
Jednodniowy atak typu „odmowa usługi" (Denial of Service, DoS)	kosztuje od 30 do 70 dolarów	Ataki tego rodzaju służą do paraliżowania stron WWW i komputerów.
Instalacja wirusa ZeuS na hoście nabywcy	35 dolarów; instalacja na hoście sprzedawcy: 40 dolarów	ZeuS to jeden z najbardziej znanych botnetów, służący do zdalnej kradzieży osobistych danych z komputerów ofiar.
Kod źródłowy konia trojańskiego backdoor trojan	50 dolarów	Złośliwe oprogramowanie typu trojan udaje legalny program lub aplikację, aby kraść dane użytkownika.

Źródło: opracowanie na podstawie http://www.trendmicro.pl/cloud-content/us/pdfs/ security-intelligence/reports/rpt-zero-days-hit-users-hard-at-the-start-of-the-year.pdf.

Doświadczamy wzrostu liczby ataków ukierunkowanych, incydentów cyberszpiegostwa oraz cyberataków sponsorowanych przez rządy, obserwuje się wzrost znaczenia haktywizmu, rozwoju kontrowersyjnych „legalnych" narzędzi inwigilacji oraz zwiększoną liczbę ataków cyberprzestępczych na serwisy wykorzy-

stujące przetwarzanie w chmurze. W 2015 roku prognozowany jest kolejny etap w ewolucji aktywności cyberprzestępczej, w którym taktyki i techniki stosowane w zaawansowanych i ukierunkowanych atakach będą wykorzystywane w przestępczości internetowej motywowanej względami finansowymi (Kaspersky Security Bulletin 2014. Prognozy na 2015 rok).

W analizach raportów dotyczących zagrożeń najbardziej niepokojące są informacje o zagrożeniach typu regularnych operacji cyberwojennych sponsorowanych przez rządy i wzrost cyberszpiegostwa, w którym wykorzystuje się „legalne" narzędzia inwigilacji przez rządy, ataki na infrastrukturę opartą na chmurze (a w tę stronę zmierzają rozwiązania techniczne). Analiza ataków tylko z ostatniego roku pozwala postawić tezę o zbliżaniu się do wojny cybernetycznej. Wojna cybernetyczna polega na wykorzystaniu przez podmiot państwowy komputerów, Internetu oraz innych środków przechowywania lub rozprzestrzeniania informacji w celu przeprowadzenia ataków na systemy informatyczne wroga, w szczególności mogą to być systemy infrastruktury krytycznej. Jest to powodem coraz częstszego podkreślania wzrostu podatności sieci korporacyjnych z obszaru krytycznej infrastruktury (np. energetyki[6]), w której stosowane są systemy SCADA (Raport: *Zagadnienia bezpieczeństwa informacji w branży energetycznej*). Chociaż prawdopodobieństwo zaistnienia takiego zdarzenia jest niezmiernie małe, to potencjalne szkody szacuje się na bardzo duże.

Konieczność ochrony infrastruktury internetowej jako integralnej części obszaru bezpieczeństwa państwa wymusza na państwie działania w kierunku aktywnego rozpoznawania zagrożeń, stosowania monitoringu sieci przy użyciu sensorów zbierających dane o zagrożeniach. Systemami ochrony antywirusowej obszaru wojskowego zarządza wyspecjalizowana komórka MIL-CERT, wchodząca w skład Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych. Natomiast obszar cywilny i rządowy jest chroniony przez CERT.GOV.PL. Ponadto w ramach systemu cyberbezpieczeństwa funkcjonuje zespół cert.pl w strukturze NASK (Naukowej Akademickiej Sieci Komputerowej) oraz operują zespoły abuse firm telekomunikacyjnych i banków.

[6] Zarządzanie sieciami energetycznymi jest oparte na systemach teleinformatycznych. Zakresy funkcjonalne teleinformatycznego systemu zarządzania sieciami energetycznymi obejmują systemy: dyspozytorskie, zabezpieczeń i automatyki, sterowania, regulacji, telekomunikacji i łączności, pomiarów, techniczne systemy off-line, automatyki elektrowni. W nowoczesnych blokach energetycznych wieloma procesami praktycznie nie da się już sterować ręcznie, bez wsparcia ze strony skomputeryzowanych systemów zbierania danych i sterowania (tzw. Systemów SCADA – *Supervisory Control And Data Acquisition*).

2. Działania na rzecz zwiększenia bezpieczeństwa cyberprzestrzeni

Krajową cyberprzestrzeń kształtować będą przede wszystkim działania rządu w obszarze zintegrowanej informatyzacji państwa realizowane na podstawie Programu Zintegrowanej Informatyzacji Państwa (PZIP). Dalsza informatyzacja czyni nasz kraj coraz bardziej podatnym na zagrożenia w cyberprzestrzeni. Do niedawna problem cyberbezpieczeństwa pozostawał w zainteresowaniu podmiotów informatyzujących się, przede wszystkim przedsiębiorstw prywatnych i użytkowników świadomych konsekwencji wynikających z cyberzagrożeń. Obecnie ochrona cyberprzestrzeni jest jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa każdego państwa.

Zgodnie z inicjatywą i2010 – *Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia*, każde państwo członkowskie powinno opracować swój własny plan działania na rzecz bezpieczeństwa. W „Europejskiej strategii bezpieczeństwa" (2003 r.), która stanowiła kanwę dla problemów i wyzwań w środowisku bezpieczeństwa międzynarodowego, oraz w „Strategii bezpieczeństwa wewnętrznego" (2010 r.) w spójny sposób określono wspólne części, takie jak: terroryzm, przestępczość zorganizowana i bezpieczeństwo cybernetyczne, które mają wpływ na zarówno krajowy, jak i międzynarodowy wymiar bezpieczeństwa. Na kształtowanie się systemu bezpieczeństwa cyberprzestrzeni w naszym kraju wpływ będzie miał również dokument „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona przestrzeń" (2013). Promuje przestrzeganie już istniejących przepisów międzynarodowych w dziedzinie cyberprzestrzeni i deklaruje pomoc państwom członkowskim oraz propaguje współpracę międzynarodową w dziedzinie bezpieczeństwa cybernetycznego. Konkretne działania państw członkowskich mają być ukierunkowane na:

- zwiększenie odporności w dziedzinie bezpieczeństwa cybernetycznego systemów informacyjnych,
- ograniczenie cyberprzestępczości,
- wzmocnienie międzynarodowej polityki UE w dziedzinie bezpieczeństwa cybernetycznego i obrony cybernetycznej.

Pierwszy Rządowy Program Ochrony Cyberprzestrzeni RP opracowany został w 2009 roku przez ABW i MSWiA i obejmował lata 2009–2011. Program ten został zaktualizowany dokumentem: Rządowy Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016. Na podstawie programu ochrony cyberprzestrzeni 2009–2011 prowadzono prace nad dokumentem Polityka Ochrony Cyberprzestrzeni RP, który przyjęto 23 czerwca 2013 roku po rocznej konsultacji społecznej, prowadzonej przez MIAC na stronie internetowej. Polityka Ochrony Cyberprzestrzeni RP (2013) będzie wyznaczała działania w zakresie systemu bezpieczeństwa cyberprzestrzeni dla podmiotów: „dostarczających" bezpieczeństwo i beneficjentów bezpieczeństwa, jednocześnie tworząc podstawy pod system zarzą-

dzania bezpieczeństwem cyberprzestrzeni na poziomie strategicznym. W projekcie Strategii Rozwoju Systemu Bezpieczeństwa Narodowego 2020 podkreśla się działania w kierunku wzmocnienia aktywnego udziału Polski w budowie i funkcjonowaniu unijnych i sojuszniczych struktur obrony cybernetycznej. W dokumencie tym zwrócono uwagę na konieczność udoskonalenia zasad i mechanizmów współpracy pomiędzy MON i ABW oraz stroną cywilną a wojskowym systemem obronnym państwa i to wyznacza kierunek najbliższych działań w tym względzie. W prognozach rozwoju systemów bezpieczeństwa cyberprzestrzeni należy uwzględnić działania podejmowane w ramach problemów, które stworzyła Ustawa z 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw. Nowe przepisy pozwalają Prezydentowi RP wprowadzić jeden z stanów nadzwyczajnych (w zależności od okoliczności: stan klęski żywiołowej, stan wyjątkowy lub stan wojenny), gdy np. atak cybernetyczny na system zarządzania siecią energetyczną zagraża bezpieczeństwu państwa.

Działania te wyznaczają kierunek rozwoju krajowych systemów bezpieczeństwa cyberprzestrzeni oraz nadają kierunek rozwiązań legislacyjnych.

Podsumowanie

Im bardziej zależymy od cyberprzestrzeni, tym bardziej zależymy od jej bezpieczeństwa. Bezpieczna cyberprzestrzeń chroni nasze swobody i prawa oraz nasze zdolności do prowadzenia działalności gospodarczej, gwarantując rozwój ekonomiczny i poprawę jakości życia. Aby cyberprzestrzeń pozostała otwarta, wolna i bezpieczna w środowisku internetowym, powinny mieć zastosowanie te same normy, zasady i wartości dla wszystkich jej użytkowników.

Aby wzmacniać system bezpieczeństwa cyberprzestrzeni, występuje konieczność stałego analizowania nowych trendów w ICT oraz rozpoznawania i badania nowych zagrożeń, jakie mogą się z nimi wiązać. Powinno także skłaniać do monitorowania zagrożeń i wyzwań „pozatechnicznych". Efektem takich działań mogłyby być prognozy bezpieczeństwa cyberprzestrzeni opracowywane np. w ramach prowadzenia analizy ryzyka.

Absorpcja technologii i jej wykorzystanie rodzi konkretne potrzeby dla systemów bezpieczeństwa cyberprzestrzeni. W ramach dokumentu Polityka Ochrony Cyberprzestrzeni RP przewiduje się:

- wzmocnienie zespołów odpowiedzialnych za reagowanie na cyberataki (Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, cert.pl, zespoły abuse);

- budowę płaszczyzny współpracy pomiędzy administracją i przedsiębiorstwami a także obywatelami oraz możliwość wymiany informacji o zagrożeniach;
- ustanowienie Krajowego Systemu Reagowania na Incydenty Komputerowe;
- wprowadzenie zasad zarządzania ryzykiem związanym z funkcjonowaniem cyberprzestrzeni.

1 czerwca 2013 roku rozpoczęło działalność Narodowe Centrum Kryptologii, które będzie zajmowało się m.in. budową systemów i doskonaleniem technik pozwalających na lepsze monitorowanie Internetu oraz wszelkich transmisji i połączeń, również szyfrowanych. Prace te będą prowadzone pod nadzorem Agencji Bezpieczeństwa Wewnętrznego oraz Służby Kontrwywiadu Wojskowego. Działania w tym zakresie będą również wyznaczały rozwój bezpiecznej cyberprzestrzeni.

Literatura

1. Global ICT developments and trends 2030, http://www.ballaratict.com.au/bict_2030/report/ch04.php.
2. http://www.cert.gov.pl/portal/cer/30/23/Rzadowy_program_ochrony_cyberprzestrzeni_RP_na_lata_20092011__zalozenia.html.
3. http://www.gartner.com/technology/analysts.jsp.
4. Internet Reports: The Internet of Things; Geneva, November 2005, http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf.
5. Kaspersky Security bulletin 2014, http://securelist.pl/analysis/7298,kaspersky_security_bulletin_2014_ogolne_statystyki_dla_2014_r.html.
6. Kaspersky Security bulletin. Prognozy na 2015, http://securelist.pl/analysis/7296,kaspersky_security_bulletin_2014_prognozy_na_2015_rok.html.
7. Program Zintegrowanej Informatyzacji Państwa, Ministerstwo Administracji i Cyfryzacji, czerwiec 2013.
8. Raport Panda Software, http://www.pzb.net.pl/index.php/Latest/Supermarket-zlosliwych-kodow.html.
9. Raport Trend Micro, http://www.trendmicro.pl/cloud-content/us/pdfs/security-intelligence/reports/rpt-zero-days-hit-users-hard-at-the-start-of-the-year.pdf.
10. Świeboda H. (2012), *Ograniczenie swobody działania w cyberprzestrzeni*, w: *Metodologia badań bezpieczeństwa narodowego*, red. P. Sienkiewicz, M. Marszałek, H. Świeboda, Wyd. AON, Warszawa.
11. Świeboda H. (2013), *Problem prywatności w społeczeństwie informacyjnym*, ZN Ekonomiczne Problemy Usług nr 763, Szczecin.

SHAPING THE CYBERSPACE SECURITY

Summary

Important problems of modern society include those that are generated by the development of ICT. In particular, the risks that have emerged along with their application. The effects of threats affect the level of security, which significantly determines the quality of community life and provides a stable socio-economic development. The article presents the results of analyzes of trends in the development of technology and evolving threats, which are the basis for developing a cyber security policy in the context of national security.

Keywords: ICT, security, cyberspace, threats.

Translated by Halina Świeboda