Ekonomiczne Problemy Usług nr 1/2017 (126), t. 2

ISSN: 1896-382X | www.wnus.edu.pl/epu
DOI: 10.18276/epu.2017.126/2-25 | strony: 249–258

Piotr Sienkiewicz
Wojskowa Akademia Techniczna
Wydział Cybernetyki
e-mail: p.sienkiewicz45@gmail.com

Wyzwania i zagrożenia bezpiecznego rozwoju społeczeństwa informacyjnego

Istnieją znane wiadome – rzeczy, o których wiemy, że je wiemy. Istnieją również znane niewiadome – innymi słowy, wiemy, że są pewne rzeczy, których nie wiemy. Ale są również nieznane niewiadome – rzeczy, o których nie wiemy, że ich nie wiemy.

Donald Rumsfeld, 2002

Kod JEL: H56
Słowa kluczowe: społeczeństwo informacyjne, wyzwania cywilizacyjne, zagrożeni bezpieczeństwa, bezpieczeństwo cyberprzestrzeni
Streszczenie. W artykule przedstawiono aktualne problemy bezpieczeństwa informacyjnego państwa, będące skutkiem rozwoju technologii informacyjnych. Zagrożenia dla bezpieczeństwa państwa stanowią jedno z podstawowych wyzwań cywilizacyjnych. Przedstawiono podstawowe elementy strategii bezpiecznego rozwoju społeczeństwa informacyjnego.

Wprowadzenie

Czas, jaki upłynął od przełomu wieków uświadomił w sposób dramatyczny, że zagrożenia bezpieczeństwa w wymiarze zarówno narodowym, jak i międzynarodowym, są immanentną cechą współczesności (ponowoczesności). Ponadto, oczywistym faktem stała się niemal powszechna świadomość, że zjawiska niegdyś antycypowane, a których źródłem jest wzrost tempa zmian technologicznych i ich kumulacja w obszarze technologii elektronicznych i informacyjno-komunikacyjnych (ICT) niosą nie tylko „incydentalne" zagrożenia bezpieczeństwa, lecz stanowią podstawę zmian doktrynalnych dotyczących wizji (modeli) bezpieczeństwa międzynarodowe-

go (narodowego) oraz możliwych przyszłych konfliktów, w tym prowadzenia działań wojennych – w zasadzie w dowolnej skali. Powoduje to, że opinia publiczna, w tym także analitycy systemów, więcej uwagi poświęcają wyzwaniom cywilizacyjnym i zagrożeniom rozwoju społeczno-ekonomicznego niż szansom redukcji ryzyka, zarówno w skali lokalnej, jak i globalnej. Wraz z rozwojem rewolucyjnych technologii, takich chociażby, jak internet oraz *Internet of Things*, GPS, systemy komunikacji mobilnej, sieci semantyczne i systemy sztucznej inteligencji, nastąpił również rozwój różnorodnych „technologii podwójnego zastosowania", w tym „broni informacyjnych" o charakterze destrukcyjnym (ofensywnym). Okazało się, że to nie „maniacy komputerowi" (*netkids*), a organizacje przestępcze (np. terrorystyczne) i państwowe stanowić mogą istotne zagrożenie dla lokalnego, regionalnego i globalnego bezpieczeństwa. Z kolei, rezultatem postępu technologicznego w tym obszarze był rozwój mediów masowych i tzw. mediów społecznościowych, systemów globalnej inwigilacji i dezinformacji oraz platform sieciocentrycznych (NCW). O pierwszej wojnie w Zatoce (1991) pisano jako o „The First Information War", zaś krótko po jej zakończeniu przedstawiono „model Wardena", w którym wyróżniono – oprócz lądowego, morskiego, powietrznego i kosmicznego wymiaru wojny, jej „piąty wymiar", czyli cyberprzestrzeń (*cybespace*). Konsekwencją powyższej propozycji były koncepcje wywodzące się z RAND Corporation (J. Arquilla, D. Ronfeldt), a mianowicie: *netwar* i *cyberwar* jako formy „information warfare" (obok *political warfare* i *economic warfare*). Zaowocowały one konkretnymi projektami narodowymi i wspólnotowymi NATO, dotyczącymi systemów obrony przed cyberzagrożeeniami (*cyberdefence*), w tym takimi, jak amerykański „Projekt X" określający zakres, formy i środki prowadzenia wojny cybernetycznej (*cyberwar*). Intensywne prace badawczo-rozwojowe prowadzone są w szczególnie dostrzegalnej skali także przez Chiny, Rosję, Izrael, Indie, Pakistan, Iran. Konflikty takie, jak rosyjsko-gruziński czy obecny rosyjsko-ukraiński również charakteryzuje użycie w różnej skali środków cybernetycznych (*cyberweapons*), zaś szczególnego znaczenia nabrał zmasowany cyberatak na systemy informatyczne Estonii (2007) oraz użycie „Stuxnet" w ataku na atomowe instalacje Iranu.

1. Wyzwania

30 sierpnia 2012 roku na 99 posiedzeniu, Sejm RP uchwalił zmianę ustawy o stanie wojennym oraz kompetencjach Naczelnego Dowódcy SZ, zaś jedną ze zmian było przyznanie Prezydentowi praw do wprowadzenia stanu wojennego, gdy: „zaistnieją celowe działania, w tym o charakterze terrorystycznym, godzące w niepodległość, niepodzielność terytorium lub ważny interes gospodarczy Rzeczypospolitej Polskiej, a także zmierzające do uniemożliwienia lub zakłócenia wykonywania przez organy państwowe ich funkcji, podejmowane przez zewnętrzne w stosunku do niej podmioty, na lądzie, wodzie, w przestrzeni powietrznej, prze-

strzeni kosmicznej lub cyberprzestrzeni". W dokumencie założono, że znaczenie bezpieczeństwa w cyberprzestrzeni będzie rosło, podobnie jak odpowiedzialność państw za jej ochronę i obronę. Podkreślono także, że warunkiem niezakłóconego działania całego państwa jest bezpieczne funkcjonowanie systemu teleinformatycznego RP. 22 stycznia 2015 roku Prezydent RP w przesłaniu do dokumentu – „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej" zaznaczył, że już wcześniej dokonano pewnych zmian w polskim systemie prawnym w 2011 roku, wprowadzając do niego m.in. pojęcie cyberprzestrzeni oraz ustanawiając prawne podstawy nadzwyczajnego reagowania na występujące w niej zagrożenia. Doktryna wskazuje strategiczne kierunki działań dla zapewnienia pożądanego poziomu bezpieczeństwa RP w cyberprzestrzeni.

Tabela 1. Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej

	Charakterystyka definicji
Cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni)	proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej, a także będących w ich dyspozycji systemów teleinformatycznych oraz zasobów informacyjnych w globalnej cyberprzestrzeni
Bezpieczeństwo cyberprzestrzeni RP	część cyberbezpieczeństwa państwa, obejmująca zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mających na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni RP wraz ze stanowiącą jej komponent publiczną i prywatną teleinformatyczną infrastrukturą krytyczną oraz bezpieczeństwa przetwarzanych w niej zasobów informacyjnych

Źródło: Na podstawie: *Doktryna…* (2015).

Tabela 2. Współczesne zagrożenia społeczne w warunkach społeczeństwa informacyjnego

Rodzaj wojny	Przedmiot	Środki	Cele
Wojna sieciowa	zarządzanie percepcją docelowej populacji w celu wywierania wpływu na zachowania w skali narodowej	kształtowanie odbioru za pośrednictwem środków komunikacji sieciowej i kontrola informacji w celu wpływania na pełny zakres potencjalnych celów sfery społecznej	społeczeństwo w pełnym zakresie (w ujęciu politycznym, ekonomicznym, militarnym)
Wojna polityczna	wpływ na decyzje na szczeblu kierownictwa rządu oraz prowadzoną przez rząd politykę	środki, które wpływają na krajowe systemy polityczne oraz instytucje rządowe	systemy polityczne
Wojna gospodarcza	wpływ na decyzje oraz politykę na szczeblu rządowym	środki, które wpływają na krajową gospodarkę poprzez produkcję oraz dystrybucję dóbr (np. sankcje, blokady, kradzież technologii)	systemy ekonomiczne
Wojna cybernetyczna	osiąganie celów militarnych przez prowadzenie działań skierowanych przeciwko celom/obiektom militarnym	operacje wojskowe prowadzone na podstawie formuł informatycznych, które integrują wykorzystanie wiedzy, walki psychologicznej, pozorowanie/kamuflowanie i walkę elektroniczną	systemy wojskowe

Źródło: opracowanie własne.

2. Bezpieczeństwo informacyjne państwa

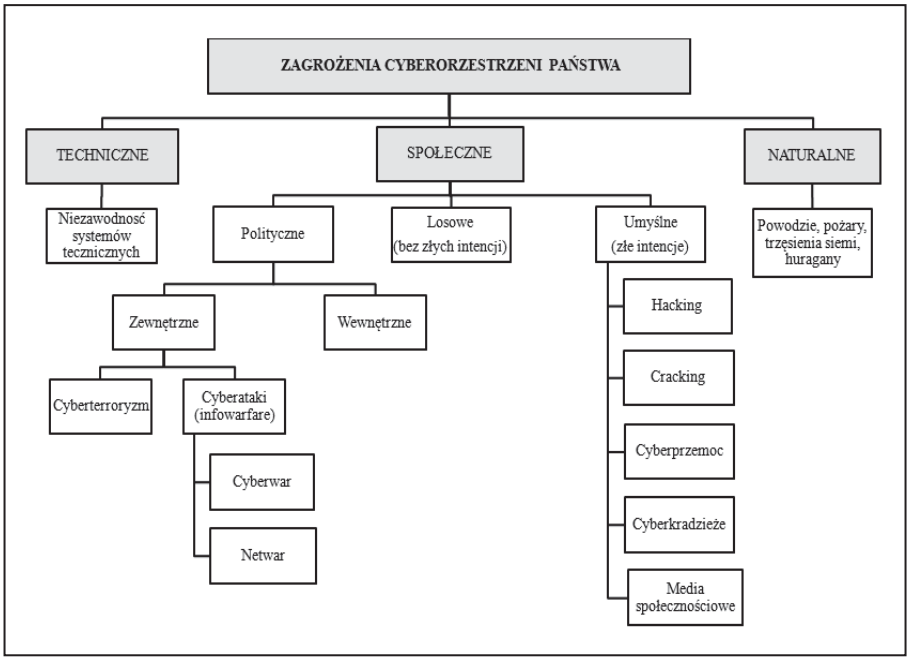
W Białej Księdze Bezpieczeństwa Narodowego RP (2013) wyodrębniono cztery główne grupy zadań bezpieczeństwa: obronność (bezpieczeństwo militarne, obrona narodowa), ochrona (bezpieczeństwo cywilne, niemilitarne; ochrona ludności, zasobów, infrastruktury i struktur państwa), bezpieczeństwo społeczne oraz bezpieczeństwo gospodarcze. Zadaniom odpowiadają właściwe sektory bezpieczeństwa narodowego (bezpieczeństwa państwa). Jednym z tzw. transsektorowych obszarów bezpieczeństwa narodowego jest bezpieczeństwo informacyjne, a infrastruktura informacyjna (teleinformatyczna) stanowi newralgiczny podsystem Krytycznej Infrastruktury Państwa (KIP). Bezpieczeństwo informacyjne jest jednym z podstawowych filarów bezpieczeństwa narodowego i obejmuje trzy główne obszary:

1. **Bezpieczeństwo zasobów informacyjnych –** systemy informacyjne (państwowe i pozapaństwowe): systemy informatyczne, telekomunikacyjne, sieci teleinformatyczne (rozpoznania, walki radioelektronicznej, systemy wspomagające decyzje), zasoby informacyjne (państwowe i pozapaństwowe), bazy danych, bazy wiedzy oraz inne zbiory informacyjne istotne dla efektywnego działania określonych organów (instytucji).

2. **Bezpieczeństwo systemów (sieci) teleinformatycznych** – obywateli, organizacji i instytucji państwa (rządowe, resortowe), elementy (podsystemy) Krytycznej Infrastruktury Państwa, sieci resortowe (wydzielone i korporacyjne).
3. **Bezpieczeństwo cyberprzestrzeni** – jako przestrzeni wytwarzania i wymiany informacji tworzonej przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami.

Cyberbezpieczeństwo obejmuje specjalny obszar wojskowy i obszar pozawojskowy związany z działaniem administracji, przedsiębiorstw, obywateli i innych podmiotów korzystających z nowych technologii. Obszar ten należy rozpatrywać z punkt u widzenia:

1. Uregulowań prawnych w odniesieniu do ochrony informacji (niejawnej, wrażliwej, danych osobowych, możliwości stosowania systemów teleinformatycznych, itp.).
2. Działań organizacyjnych w kontekście odpowiedzialności za tworzenie strategii i polityki bezpieczeństwa, wdrożenia i nadzorowania.
3. Technicznych, programowych i organizacyjnych zabezpieczeń bezpieczeństwa systemów ICT, w tym internetu.
4. Dynamiki zjawisk związanych z pozyskiwaniem, przetwarzaniem, przesyłaniem i przechowywaniem informacji, wymuszającej monitoring oraz adaptację systemów bezpieczeństwa do zmieniającego się otoczenia.



Rysunek 1. Typologia zagrożeń bezpieczeństwa informacyjnego

Źródło: opracowanie własne.

Jeżeli pod pojęciem cyberprzestrzeni rozumie się przestrzeń przetwarzania i wymiany informacji, tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami, to wynika stąd, że cyberprzestrzeń nie ma określonych granic politycznych, ani geograficznych. Różnorodność technologii oraz rozwiązań technicznych i organizacyjnych powoduje, że działania w zakresie bezpieczeństwa informacyjnego (cyberprzestrzeni) stają coraz bardziej złożone i o ograniczonej przewidywalności, stanowiąc jedno z istotnych wyzwań bezpiecznego rozwoju społeczeństwa informacyjnego. Można zatem rozpatrywać bezpieczeństwo cyberprzestrzeni na poziomie:

- społecznym (utrata określonych wartości społecznych, politycznych, kulturowych z powodu destrukcyjnych działań skierowanych na określone zasoby infosfery i technosfery),
- informacyjnym (utrata wartościowych danych, informacji, wiedzy jako skutków niepożądanych destrukcyjnych działań na zasoby infosfery),
- technicznym (utrata lub obniżenie niezawodności zasobów technologicznych i programowych tworzących technosferę, w tym KIP).

Zapewne w najbliższym czasie cyberprzestrzeń RP kształtować będą przede wszystkim działania właściwych organów państwa na podstawie „Programu Zintegrowanej Informatyzacji Państwa" (PZIP) lub dokumentu podobnej rangi, określającego kluczowe wyzwania w obszarze informatyzacji – istotne dla rozwoju społeczeństwa informacyjnego. Celem programu jest stworzenie spójnego, logicznego i sprawnego systemu informacyjnego państwa dostarczającego e-usługi na poziomie krajowym i europejskim, w sposób efektywny w sensie jakościowym i kosztowym. Program powinien wyrażać związany ideą rozwoju nowoczesnego cyfrowego społeczeństwa informacyjnego, zgodnie z długookresową strategią rozwoju kraju.

3. Organizacyjne podstawy bezpieczeństwa cyberprzestrzeni

Krajowe rozwiązania w obszarze bezpieczeństwa cyberprzestrzeni w pełni odpowiadają europejskim uregulowaniom. Zgodnie z inicjatywą „i2010 – Europejskie społeczeństwo informacyjne na rzecz wzrostu i zatrudnienia", każde państwo członkowskie powinno opracować swój własny plan działania na rzecz bezpieczeństwa. Ponadto w Europejskiej Strategii Bezpieczeństwa (2003 r.) i Strategii Bezpieczeństwa Wewnętrznego (2010 r.) określono trzy wspólne obszary: terroryzm, przestępczość zorganizowana i bezpieczeństwo cybernetyczne. Na kształt polskiego systemu bezpieczeństwa cybernetycznego wpływał również dokument „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona przestrzeń" (2013 r.). Należy podkreślić, że w uregulowaniach prawnych na poziomie Unii Europejskiej, pojęcie cyberprzestrzeni łączone jest też z pojęciem tzw. informacyjnej infrastruktury krytycznej (*Critical Information Infrastructure* – CII), która wpisana jest w ramy Europejskiego Programu Ochrony Infrastruktury Krytycznej (*European Programme for Critical*

Infrastructure Protection – EPCIP). Program ten uwzględnia m.in. działania NATO dotyczące wspólnej polityki obrony przed atakami cybernetycznymi prowadzone przez Centrum ds. Współpracy w Dziedzinie Obrony przed Atakami Cybernetycznymi (*Co-operative Cyber Defence Centre of Excellence*). Polska pozostaje stroną konwencji międzynarodowych, które mają znaczenie dla rozwoju cyberbezpieczeństwa. Wśród dokumentów międzynarodowych szczególne znaczenie mają:

- Konwencja Rady Europy o zwalczaniu terroryzmu (27.01.1977 r.),
- Konwencja o zwalczaniu cyberprzestępczości RE (23.11.2001 r.),
- Konwencja Rady Europy o zapobieganiu terroryzmowi (maj 2005 r.).
- Program Sztokholmski wraz z Planem Działania.

W Programie Sztokholmskim Rada Europejska apeluje m.in. do państw członkowskich o udzielenie pełnego poparcia krajowym platformom powiadamiania, odpowiedzialnym za walkę z cyberprzestępczością i podkreśla, że konieczna jest współpraca z krajami spoza Unii Europejskiej. Wzywa państwa członkowskie do poprawy współpracy prawnej w sprawach dotyczących cyberprzestępczości. Dokument wskazuje na potrzebę podjęcia działań na rzecz utworzeniu europejskiej platformy identyfikowania cyberprzestępczości oraz przeciwdziałania i zwalczania, przy wykorzystaniu możliwości oferowanych przez Europol. Ponadto istotne znaczenie dla krajowych rozwiązań mają także inne dokumenty takie, jak:

- Decyzja Rady Ministerialnej OBWE nr 3/04 z 7.12.2004 r. oraz nr 7/06 z 5.12.2006 r. w sprawie działań związanych ze zwalczeniem wykorzystywania internetu do celów terrorystycznych,
- Decyzja Rady Ministerialnej OBWE nr 5/07 z 30.11.2007 r. związana z partnerstwem publiczno-prywatnym z zwalczaniu terroryzmu,
- Europejska Agenda Cyfrowa Rady Europejskiej.

Ponadto Polska podpisała Konwencję Rady Europy z 23 listopada 2001 roku o cyberprzestępczości, którą ratyfikowała w 2009 roku. Podstawowymi krajowymi regulacjami zdefiniowanymi w tym obszarze są:

- ustawa o zarządzaniu kryzysowym,
- ustawa o prawie telekomunikacyjnym,
- ustawa o informatyzacji podmiotów realizujących zadania publiczne,
- ustawa o świadczeniu usług drogą elektroniczną,
- prawo bankowe.

Tabela 3. Strategiczne rządowe dokumenty regulujące cyberbezpieczeństwo RP

Dokument	Najważniejsze uregulowania
Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011 – założenia (2009)	zwiększenie poziomu bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa; zwiększenie poziomu odporności państwa na ataki cyberterrorystyczne; stworzenie i realizacja polityki bezpieczeństwa cyberprzestrzeni, spójnej dla wszystkich podmiotów administracji publicznej oraz innych współtworzących krytyczną infrastrukturę teleinformatyczną państwa; zapewnienie ścisłej współpracy sektora państwowego z sektorem prywatnym operatorów telekomunikacyjnych
Rządowy program ochrony cyberprzestrzeni RP na lata 2011–2016 (2010)	projekt działań prawno-organizacyjnych, technicznych i edukacyjnych, których celem jest zwiększenie zdolności do zapobiegania i zwalczania zagrożeń bezpieczeństwa cyberprzestrzeni państwa; powołanie Międzyresortowego Zespołu Koordynującego ds. Ochrony Cyberprzestrzeni RP (MZKOC) oraz jednostki technicznej zarządzania i koordynowania zadań w zakresie ochrony cyberprzestrzeni RP; wdrożenie rozwiązań chroniących krajową infrastrukturę teleinformatyczną oraz zapewniających przeciwdziałanie i reagowanie na incydenty sieciowe, w tym o charakterze cyberterrorystycznym; zwiększenie świadomości użytkowników w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni
Polityka Ochrony Cyberprzestrzeni RP (2013)	zakłada osiągnięcie odpowiedniego poziomu bezpieczeństwa cyberprzestrzeni państwa; cel ten ma być zrealizowany dzięki systemowi skutecznej koordynacji i wymiany informacji między użytkownikami cyberprzestrzeni; zobowiązuje do dokonania przeglądu regulacji prawnych w celu nowelizacji przepisów; zaleca właściwe kształcenie kadry administracyjnej w dziedzinie bezpieczeństwa systemów teleinformatycznych; zaleca się prowadzenie kampanii edukacyjno-prewencyjnej w ramach edukacji szkolnej dzieci i młodzieży
Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej (2015)	doktryna jest dokumentem koncepcyjnym oraz wykonawczym w stosunku do Strategii Bezpieczeństwa Narodowego RP (2014); określa cele w dziedzinie cyberbezpieczeństwa, opisuje środowisko, wskazując na zagrożenia, ryzyka i szanse, a także rekomenduje najważniejsze zadania, jakie powinny być realizowane w ramach budowy systemu cyberbezpieczeństwa państwa; zawarto zgodę na działania ofensywne: zwalczanie (dezorganizowanie, zakłócanie i niszczenie) źródeł zagrożeń (aktywna obrona oraz działania ofensywne); wskazano na potrzebę rozwoju w pełni kontrolowanych przez państwo systemów teleinformatycznych i technologii, przy zachowaniu zgodności z narzędziami oraz technologiami NATO i sojuszników, na których oparta byłaby obrona i ochrona krytycznych systemów państwa; zaleca się by działania na rzecz bezpieczeństwa w cyberprzestrzeni były podejmowane z uwzględnieniem ochrony praw człowieka i obywatela oraz poszanowaniem prawa do wolności słowa i prywatności; proporcjonalność środków bezpieczeństwa w stosunku do zagrożeń powinna być oparta na efektywnej i wiarygodnej analizie ryzyka; zaleca stosowanie tzw. najlepszych praktyk, opracowanie programów kształcenia kadr oraz „ścieżek kariery" pozwalających angażować najlepszych specjalistów; promuje udział w społecznych inicjatywach wspierających cyberbezpieczeństwo RP (wolontariat dla cyberbezpieczeństwa, w tym cyberobrony państwa); zaleca podejmowania decyzji na podstawie analizy ryzyka oraz monitoring i regularne audyty bezpieczeństwa

Źródło: opracowanie własne na podst. dokumentów.

Podsumowanie

W Polsce odpowiedzialność za bezpieczeństwo oraz ochronę cyberprzestrzeni RP jest rozproszona, gdyż nie funkcjonuje jeden podmiot koordynujący działania w obszarze zarządzania bezpieczeństwem informacyjnym państwa. Poszczególne instytucje odpowiadają za ochronę określonych sektorów krytycznej infrastruktury państwa, cyberbezpieczeństwo administracji państwowej i użytkowników prywatnych. Z oczywistych względów do priorytetów w zakresie ochrony i obrony należą potrzeby systemu bezpieczeństwa narodowego. Z kolei, do istotnych współczesnych problemów politycznych, a także badawczo-rozwojowych, należy zaliczyć np.: identyfikację swoistych cech cyberprzestrzeni i specyfikację zagrożeń cybernetycznych dla bezpieczeństwa narodowego, monitoring i ewaluację ryzyka zagrożeń cybernetycznych dla bezpieczeństwa narodowego RP i Europejskiej Przestrzeni Cybernetycznej, a ponadto uwarunkowania organizacyjne i prawne bezpieczeństwa cybernetycznego UE, NATO i RP, ryzyko groźby „cybernetycznego Pearl Harbor". Bezpieczeństwo cyberprzestrzeni wymaga aktywności państwa nie tylko z zakresie ochrony strategicznych „zasobów informacyjnych", ale także w obszarze działań zmierzających do aktywnego zapewnienia lub wsparcia bezpiecznego funkcjonowania infrastruktury krytycznej, w tym kluczowych systemów teleinformatycznych i oferowanych przez nie usług. Cyberbezpieczeństwo obejmuje także problemy projektowania bezpiecznych i efektywnych systemów cyberobrony państwa (organizacji, instytucji). Jest jednym z najważniejszych wyzwań politycznych i badawczo-rozwojowych pierwszej połowy XXI wieku, być może w podobnym stopniu jak ENIGMA była wyzwaniem dla kryptologów z kresu II wojny światowej.

Bibliografia

Alberts, D.S., Garstka, J.J., Hayes, R.E., Signori, D.A., (2001). *Understanding Information Age Warfare*. Waszyngton: DoD CCRP.

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (2013). Warszawa: BBN.

Castells, M., (2003). *Galaktyka Internetu*. Poznań.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej (2015). Warszawa: BBN.

Goban-Klas, T., Sienkiewicz, P. (1999). *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*. Kraków.

Pacek, B., Hoffmann, R. (2013). *Działania sił zbrojnych w cyberprzestrzeni*. Warszawa: Wydawnictwo AON.

Polityka Ochrony Cyberprzestrzeni RP (2013). Warszawa: MIAC.

Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2009–2011 – założenia (2009). Warszawa: MSWiA.

Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016 (2010). Warszawa: MSWiA.

Sienkiewicz, P. (2006). *Społeczeństwo informacyjne jako społeczeństwo ryzyka*. Kraków.

Sienkiewicz, P. (2007). *Bezpieczeństwo i wolność w globalnym społeczeństwie informacyjnym*. Warszawa.

Sienkiewicz, P., Świeboda, H. (1999). *Niebezpieczna przestrzeń cybernetyczna, wyzwania*. Kraków.

Sienkiewicz, P., Świeboda, H. (2001). Bezpieczeństwo regionalnej przestrzeni cybernetycznej. W: C. Hales, B. Mikuła (red.), *Społeczeństwo informacyjne. Gospodarka, technologie, procesy*. Kraków: Wydawnictwo Uniwersytetu Ekonomicznego.

Sienkiewicz, P., Świeboda, H. (2010). Analiza systemowa bezpieczeństwa cyberprzestrzeni państwa. *Studia i Materiały Polskiego Stowarzyszenia Zarządzania Wiedzą, Bezpieczeństwo – środowisko – przestrzeń – rolnictwo, 33*.

Sienkiewicz, P., Świeboda, H. (2010). Information threats of national security of Republic Poland. Проблемы Управления Безопасностью Сложных Систем, Moskwa.

Sienkiewicz, P., Świeboda, H. (2010). Bezpieczeństwo europejskiej przestrzeni cybernetycznej. *Zeszyty Naukowe Akademii Marynarki Wojennej, 51* (181A).

Sienkiewicz, P., Swieboda, H., Lichocki, E. (2006). Analiza systemowa zjawiska cyberterroryzmu. *Zeszyty Naukowe AON, 2* (63).

Sienkiewicz, P., Świeboda, H. (2009). Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej. W: M. Madej, M. Terlikowski (red.), *Bezpieczeństwo teleinformatyczne państwa*. Warszawa: Wydawnictwo PISM.

Sienkiewicz, P., Świeboda, H., Szczepaniuk, E. (2015). Cybersecurity in Poland. W: L. Janczewski, W. Caelli (red.), *Cyber Conflicts and Small States*. Wyd. ASHGATE.

CHALLENGES AND THREATS
OF INFORMATION SOCIETY DEVELOPMENT SAFETY

Keywords: information society, information security, threats, civilization challenges, critical infrastructure

Summary. Modern security systems in information society, both national and international, require the consideration of new possibilities, risk and dangers. Information threats, cyber terrorism and info wars are new challenges for security and peace.

Translated by Piotr Sienkiewicz

Cytowanie

Sienkiewicz, P. (2017). Wyzwania i zagrożenia bezpiecznego rozwoju społeczeństwa informacyjnego. *Ekonomiczne Problemy Usług, 1* (126/2), 249–258. DOI: 10.18276/epu.2017.126/2-25.