AUTOMATYKA • 2009 • Tom 13 • Zeszyt 2

Piotr Sienkiewicz*

Analiza systemowa zagrożeń dla bezpieczeństwa cyberprzestrzeni

1. Wprowadzenie

W grudniu 1999 roku na szczycie Unii Europejskiej w Helsinkach ogłoszona został inicjatywa e-Europe – *An Information Society for All*. Jej głównym celem było przyspieszenie działań na rzecz transformacji społeczeństwa europejskiego w społeczeństwo informacyjne. Dlatego stała się jednym z kluczowych elementów strategii Komisji Europejskiej. Podstawowe cele inicjatywy odpowiadają celom zawartym w raporcie UNESCO *Information for All Programme* (2006), które realizowane są na pięciu płaszczyznach:

1) Tworzenie i rozwój strategii informacyjnej na poziomie krajowym, regionalnym i międzynarodowym.
2) Rozbudowa potencjału zasobów ludzkich oraz zwiększanie umiejętności przydatnych w epoce informacji.
3) Wzmacnianie instytucji odpowiedzialnych za udostępnianie informacji publicznych.
4) Rozbudowa systemu przetwarzania i zarządzania informacja.
5) Upowszechnianie technologii informacyjnej w dziedzinie edukacji, nauki, kultury i komunikacji.

W dokumencie programowym eEurope 2005 zawarto następujący zapis: „Do roku 2005, Europa powinna dysponować nowoczesnymi usługami publicznymi on-line (e-rząd, e-nauka, e-zdrowie) i dynamicznym środowiskiem dla e-biznesu. Aby plany te mogły być urzeczywistnione, należy zapewnić szeroką dostępność do połączenia szerokopasmowego nabywanego po konkurencyjnych cenach oraz bezpieczną infrastrukturę informacyjną".

W marcu 2000 roku na posiedzeniu Rady Europy w Lizbonie przyjęto strategię budowy do 2010 roku najbardziej konkurencyjnej i dynamicznej bazującej na wiedzy, gospodarki świata, zdolnej do proporcjonalnego wzrostu gospodarczego, oferującej nowe miej-

* Warszawska Wyższa Szkoła Informatyki

sca pracy i większą spójność społeczną. Na szczycie UE w Feire w czerwcu 2000 roku przyjęto plan działania ujmujący dwa podstawowe cele:

1) „rozwój tańszego, szybszego i bezpiecznego Internetu" oraz „pobudzanie jego wykorzystania";
2) inwestowanie w ludzi i umiejętności, czyli tworzenie nowoczesnego kapitału ludzkiego (intelektualnego i społecznego).

O ile realizację drugiego z powyższych celów należy łączyć z rozwojem Europejskiej Przestrzeni Edukacyjnej i Europejskiej Przestrzeni Badawczej, o tyle można przyjąć, że pierwszy cel dotyczył tworzenia się Europejskiej Przestrzeni Cybernetycznej (EPC).

Te inicjatywy i wiele innych inicjatyw UE świadczą o podjęciu wyzwań cywilizacyjnych XXI wieku, albowiem łączą się z podstawowymi megatrendami: globalizacją i społeczeństwem informacyjnym (wraz z gospodarka opartą na wiedzy). Sprostanie tym wyzwaniom stało się możliwe dzięki dynamicznemu rozwojowi technologii informacyjnych ICT (*Information & Communication Technology*) oraz postępowi w takich dziedzinach nauki, jak: cybernetyka, elektronika, informatyka, telekomunikacja, automatyka, robotyka itp., które tworzą system wiedzy „trzeciej fali". Trudno byłoby sprostać tym wyzwaniom, gdyby nie polityczna wola „ponad podziałami" i zdolności kooperacji pozytywnej w skali regionalnej.

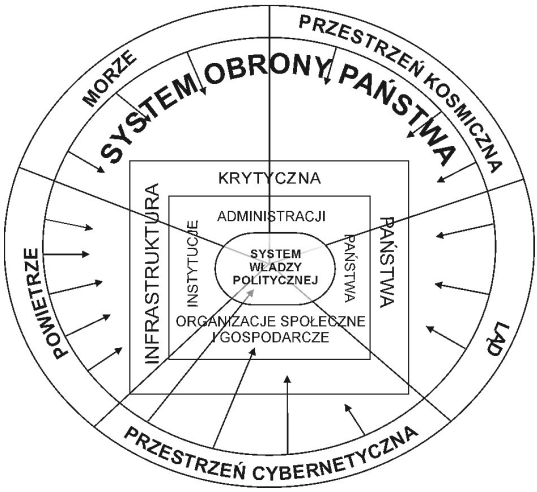
Jednakże, obok wręcz nieograniczonych możliwości innowacyjnych związanych ze społecznymi zastosowaniami ICT, pojawiła się ich „ciemna strona", w postaci nowych zagrożeń dla bezpieczeństwa oraz swoistej technologicznej amplifikacji niektórych znanych wcześniej zagrożeń bezpieczeństwa globalnego, regionalnego (lokalnego) i osobistego obywateli. Wśród zagrożeń bezpieczeństwa, które przyniósł rozwój ICT największą uwagę zwracają obecnie różnego rodzaju cyberprzestępstwa, a przede wszystkim cyberterroryzm. W Europejskiej Przestrzeni Bezpieczeństwa (rys. 1) należy zlokalizować bezpieczeństwo rozwijającej się EPC. Prawne i organizacyjne ramy EPC zawarte są nie tylko w Strategii Lizbońskiej, ale w wielu inicjatywach UE, a także poszczególnych państw członkowskich. W tym kontekście należy postrzegać np. „Rządowy program cyberprzestrzeni RP na lata 2008–2011" z października 2008 roku.

2. Cyberprzestrzeń

Pojęcie cyberprzestrzeni (*Cyberspace*) należy z pewnością łączyć z cybernetyką, która zgodnie z intencją jej twórcy Norberta Wienera była nauką o sterowaniu i komunikowaniu w obiektach (systemach) dowolnej natury. Jednakże, jako autora tego terminu, najczęściej przywołuje się Williama Gibsona, który w kultowej powieści cyberpunkowej „Neuroromancer", pisał: „To jest cyberprzestrzeń, konsensualna, halucynacja, doświadczana każdego

dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych. Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność".

Trudno uznać powyższe określenie cyberprzestrzeni za zadowalające z operacyjnego punktu widzenia, aczkolwiek trzeba przyznać, że Gibson trafnie oddaje sens globalnej przestrzeni cybernetycznej. Mogła się ona pojawić jako realny, a nie wirtualny byt, dzięki powstaniu Internetu i jego nieograniczonemu przestrzenią i czasem rozprzestrzenianiu się. Być może – jak sądził Stanisław Lem – stanowi odpowiedź na pytanie, które jeszcze nie został postawione, gdyż może stanowić początek ewolucji megasieci społecznych interakcji, której skutków nie sposób dziś przewidzieć.



Rys. 1. Przestrzeń zagrożeń bezpieczeństwa narodowego w społeczeństwie informacyjnym
Źródło: opracowanie własne

Analiza istotnych cech cybernetycznej przestrzeni pozwala rozpatrywać cybernetykę sieci nie jako technologii, lecz system – technosystem globalnej komunikacji społecznej, który charakteryzuje interaktywność i multimedialność.

Cyberprzestrzeń ukształtowały następujące procesy:

1) Proces integracji podstawowych form przekazu i prezentacji informacji (*data+texts+pictures+voices+movies*), który przyniósł multimedialność, „ucyfrowienie" infosfery ikonosfery.
2) Proces konwergencji ICT: systemów informatycznych, systemów telekomunikacyjnych i mediów elektronicznych.
3) Proces integracji technosfery, który ukształtował globalną zintegrowaną platformę teleinformatyczną.

Jak niemal każde zjawisko, wywołane rewolucją technologiczną w drugiej połowie XX wieku, także cyberprzestrzeń ma zarówno swą „jasną", jak i „ciemną" stronę. Cyberprzestrzeń jest obszarem zarówno kooperacji pozytywnej, jak i kooperacji negatywnej. Ta pierwsza oznacza niewątpliwy wzrost możliwości wszechstronnego zaspokojenia potrzeb społecznych, w tym potrzeby samorozwoju (samorealizacji), we wszystkich dziedzinach życia, a mianowicie:

1) W sferze edukacji: dzięki zwiększonym i ułatwionym możliwościom korzystania z globalnych zasobów danych, informacji i wiedzy (Europejska Przestrzeń Edukacyjna).
2) W sferze badań naukowych: dzięki wzrostowi zasobów wiedzy i wspomagania badań (Europejska Przestrzeń Badawcza).
3) W sferze komunikacji: dzięki rozwojowi sieci komunikacji społecznej w niespotykanej dotąd skali globalnej.
4) W sferze ekonomii: dzięki rozwojowi rożnych form e-biznesu i powstaniu tzw. gospodarki opartej na wiedzy.
5) W sferze kultury: dzięki niemal nieograniczonemu dostępowi do zasobów wirtualnej ikonosfery.
6) W sferze ludycznej: powstała arena globalnych igrzysk, gier i zabaw.
7) W sferze bezpieczeństwa: dzięki zwiększonej sprawności służb nastąpił wzrost bezpieczeństwa obywateli, jednakże kosztem utraty części wolności.

Niestety, „ciemna strona" oznacza, że cyberprzestrzeń stała się niebezpieczna, stając się źródłem zagrożeń bezpieczeństwa zewnętrznego (międzynarodowego) i wewnętrznego (narodowego). Możemy mieć do czynienia z następującymi zjawiskami:

1) Cyberprzestępstwa, czyli wykorzystanie cyberprzestrzeni dla celów kryminalnych, zarówno przestępstw pospolitych, jak i zorganizowanych.
2) Cyberinwigilacja, czyli wykorzystanie cyberprzestrzeni w celach kontroli społecznej (np. identyfikacja lokalizacji, częstości korzystania z ICT, treści przekazów itp.).
3) Cyberterroryzm, czyli działania terrorystyczne w cyberprzestrzeni.
4) Cyberwojna, czyli wykorzystanie cyberprzestrzeni w działaniach wojennych lub w operacjach innych niż wojna.

Cechy działań informacyjnych powodują, że istotnym problemem jest odróżnienie np. pospolitego przestępstwa (hacking, kracking, itp) od aktu inwigilacji (np. zgodnie z „Patriot Act") lub terroryzmu, a nawet działań wojennych (rys. 2).

Większość zagrożeń bezpieczeństwa systemów teleinformatycznych trudno zaliczyć do cyberterroryzmu, choć zapewne może się zdarzyć, iż trudno będzie odróżnić skutki działań nieuczciwych lub niemądrych pracowników od skutków cyberterroryzmu (rys. 3).

Rys. 2. Istota zagrożeń informacyjnych
Źródło: na podstawie: Information Warfare. 1996: Legal, Regulatory, policy and Organizational Considions for Assurance. 2nd Edition, Washington, s. 3

3. Zagrożenia

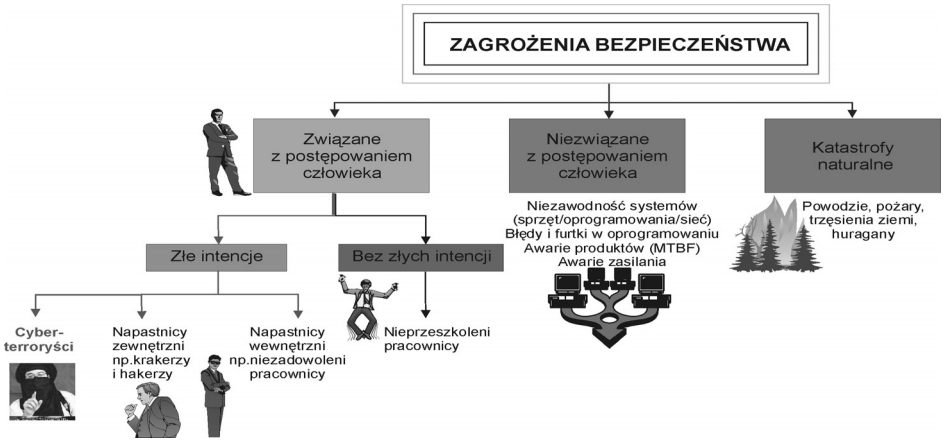
Powszechność stosowania ICT stwarza szansę wszechstronnego rozwoju społecznego, lecz jednocześnie przynosi zagrożenia wpływające na zmniejszenie poczucia bezpieczeństwa. Spowodowało to wzrost znaczenia bezpieczeństwa informacyjnego jako ważnego elementu obszaru bezpieczeństwa personalnego i narodowego [7]. Wraz z rozwojem technologicznym wystąpiła konieczność zapewnienia bezpieczeństwa systemów informacyjnych i sieci teleinformatycznych, ich poufności, integralności i nienaruszalności.[1)]

Wraz ze stosowaniem nowoczesnych technologii pojawiła się kategoria Krytycznej Infrastruktury[2)], której zniszczenie lub uszkodzenie może osłabić bezpieczeństwo państwa, w tym jego zdolności obronne. W nowoczesnych państwach Krytyczna Infrastruktura w znacznym stopniu odpowiada za procesy homeostazy, czyli dynamicznej równowagi funkcjonalnej (w rozumieniu systemowym), warunkując prawidłowe działanie mechanizmów adaptacyjnych społeczeństw, w tym reakcji na coraz bardziej dynamicznie pojawiające się nowe zagrożenia np. przestępstw komputerowych. Wynika to z wielopoziomowych interakcji pomiędzy sektorami gospodarki powiązanej sieciami telekomunikacyjnymi, bowiem elementy tej infrastruktury są współzależne.

---

1) Firma Ernst & Young szacuje, że straty z powodu przestępstw w cyberprzestrzeni wynoszą około 5 miliardów dolarów rocznie, zaś średnia wartość przestępstwa w Sieci to 90000 USD. Natomiast według SEARCH straty te wynoszą znacznie więcej, bo aż 40 miliardów dolarów. Jest to ekonomiczny wymiar strat spowodowanych brakiem skutecznych systemów bezpieczeństwa.

2) Ustawa o zarządzaniu kryzysowym, 2007



Rys. 3. Typologia zagrożeń bezpieczeństwa systemów informacyjnych
Źródło: opracowanie własne

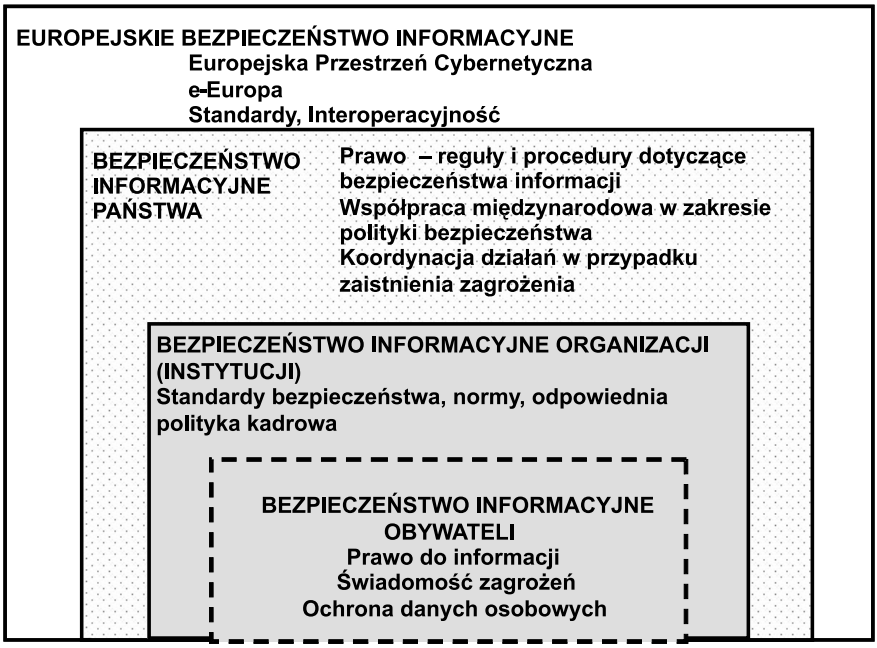
Bezpieczeństwo informacyjne, często utożsamiane jest z bezpieczeństwem informatycznym odnoszonym do narzędzi i procedur ochrony danych, informacji i systemów informacyjnych. Zapewnienie bezpieczeństwa systemów (sieci) informacyjnych, ich stabilności, niezawodności itp. stanowi „jądro" bezpieczeństwa informacyjnego. Zasoby informacyjne posiadają charakter zasobów strategicznych. Są czynnikiem rozwoju cywilizacyjnego i gospodarczego (są towarem i „kreatorem" Gospodarki Opartej na Wiedzy), sprzyjają powstawaniu nowych branż i profesji, a także miejsc pracy itp. Infrastrukturę informacyjną państwa tworzą: normy informacyjne, zasoby informacji, systemy informacyjne, instytucje informacyjne, systemy organizacyjno-techniczne gromadzenia, przechowywania, przetwarzania i przekazywania informacji. Ryzyko utraty wartościowych zasobów informacyjnych jest immanentną cechą systemów bezpieczeństwa (tab. 1).

Tabela 1
Zagrożenia bezpieczeństwa przestrzeni cybernetycznej

MOŻLIWE ZAGROŻENIA	MOŻLIWE SKUTKI ZAGROŻEŃ
Zagrożenia systemowe – Cyberataki – Cyberterroryzm – Cyberkontrola (inwigilacja) – Operacje informacyjne Zagrożenia pospolite Cyberprzestępcy: – hakerzy – krakerzy – wandale – frustraci	– Zagrożenia dla bezpieczeństwa EPC (degradacja wartości systemów i zasobów – Obniżenie zdolności obronnych – Degradacja krytycznej infrastruktury informacyjnej – Destabilizacja krytycznej infrastruktury – Zakłócenia systemów kierowania i administracji unijnej (państwowej) – Straty (zakłócenia rozwoju) podmiotów gospodarczych – Straty (zakłócenia działania) osobiste obywateli

Źródło: opracowanie własne

Bezpieczeństwo informacyjne ze względu na liczność interakcji powinno być analizowane na kilku płaszczyznach bezpieczeństwa: państwa, bezpieczeństwo organizacji i instytucji oraz obywatela (rys. 4).



Rys. 4. Płaszczyzny bezpieczeństwa informacyjnego
Źródło: opracowanie własne

Komisja Europejska do cyberprzestępstw zalicza wszystkie nadużycia przy użyciu nowych technologii informatycznych: od fałszerstw i oszustw w internecie (np. z użyciem cudzych kart kredytowych) przez zamieszczanie nielegalnych treści (pornografia dziecięca, propagowanie terroryzmu), po ataki na systemy informatyczne, powodujące ich zablokowanie, uszkodzenie, albo kradzież informacji.[3)]

Kwestia cyberbezpieczeństwa, czyli bezpieczeństwa EPC została podjęta na forum G8 a także przez Radę Europy w międzynarodowej konwencji dotycząca przestępczości informatycznej w dniu 8 listopada 2001.

[3)] Amerykańskie FBI, które ocenia, że w USA rocznie sięgają one od 67 do 400 mld dolarów. Liczba stron internetowych z pornografią dziecięcą w latach 1997–2005 wzrosła 15-krotnie. Sprzedaż tego rodzaju plików przynosi przestępcom rocznie w USA i Europie miliard dolarów. Brytyjskie władze szacują, że liczba oszustw bankowych z użyciem internetu wzrosła w ostatnich dwóch latach 80 razy.

Do najważniejszych postanowień Konwencji Rady Europy należy zaliczyć:

- harmonizację narodowych systemów prawnych dotyczących zdefiniowania cyberprzestępstw,
- wypracowanie standardów prowadzenia postępowania karnego oraz procedur sądowych dostosowanych do zasad działania globalnej sieci teleinformatycznej,
- stworzenie szybkiego i skutecznego systemu współpracy międzynarodowej w zakresie bezpieczeństwa EPC.

Tabela 2
Konsekwencje prawne decyzji Ramowej

Rada Europy	UE
Nieuprawniony dostęp (hacking)	
– umyślny, bezprawny dostęp do całości lub części systemu informatycznego, – z naruszeniem zabezpieczeń – z zamiarem pozyskania danych informatycznych lub innym nieuczciwym zamiarem (opcja) – lub w odniesieniu do systemu informatycznego, który jest połączony z innym systemem informatycznym	– umyślny, bezprawny dostęp do całości lub części systemu informatycznego – karalny jako przestępstwo, – przynajmniej w przypadkach, które nie są przypadkami – mniejszej wagi. – przestępstwo popełniane jest z naruszeniem zabezpieczenia (opcja)
Ingerencja w dane	
– umyślne, bezprawne niszczenie, kasowanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych – poważna szkoda skutek ()opcja)	– umyślne bezprawne usunięcie, uszkodzenie, pogorszenie, zmiana zatajanie lub uczynnienie niedostępnymi danych komputerowych w systemie informatycznym, – karalne jako przestępstwo, – przynajmniej w przypadkach, które nie są przypadkami – mniejszej wagi.
Ingerencja w system	
– umyślne, bezprawne poważne zakłócanie funkcjonowania systemu informatycznego poprzez wprowadzanie, transmisję, niszczenie, wykasowywanie, uszkadzanie, dokonywanie zmian lub usuwanie danych informatycznych	– umyślne poważne naruszenie lub przerwanie funkcjonowania systemu informatycznego poprzez wprowadzanie, przekazywanie, uszkadzanie, zmienianie, zatajanie lub uczynnienie niedostępnymi – danych komputerowych – karalne jako przestępstwo, – przynajmniej w przypadkach, które nie są przypadkami – mniejszej wagi.

Źródło: A.Adamski, PISM 2008

Odrębną regulacją Unii jest objęta ochrona krytycznej infrastruktury (tab. 2), od czasu gdy w roku 2005 Komisja Europejska przyjęła decyzję o opracowaniu Zielonej Księgi

przedstawiającej możliwości działania Europejskiego Programu Ochrony Infrastruktury Krytycznej (EPOIK). Wyrażono wtedy zgodę na utworzenie sieciowego systemu ostrzegania o zagrożeniach dotyczących krytycznej infrastruktury krytycznej CIWIN (*Critical Infrasturcture Warning Information Network*). Koordynacja Badań nad Krytyczną Infrastrukturą Informacyjną (*Critical Information Infrastructure Research Coordination*) realizowana jest w ramach 6. Programu Ramowego UE. Centrum Bezpieczeństwa Systemów Teleinformatycznych uczestniczy w projekcie, którego celem jest utworzenie europejskiej sieci współpracy w celu ochrony krytycznej infrastruktury informacyjnej w Europie. Sieć ta pozwoli na koordynację badań nad bezpieczeństwem krytycznej infrastruktury informacyjnej oraz umożliwi powstanie Europejskiej Przestrzeni Badawczej (ERA) ukierunkowanej na ochronę tej infrastruktury. Główny cel projektu zostanie osiągnięty dzięki realizacji celów praktycznych, w tym identyfikację i analizę programów badawczych, inicjatyw podejmowanych w poszczególnych krajach Unii w dziedzinie ochrony i rozwoju krytycznej infrastruktury informacyjnej; budowę i umocnienie platformy dyskusji i wymiany informacji; ułatwienie współpracy między podmiotami działającymi w sferze infrastruktury krytycznej. Harmonizacja i koordynacja celów związnych z bezpieczeństwem EPC stanowi warunek konieczny minimalizacji ryzyka zagrożeń w tym różnych form cyberataków.

4. Zakończenie

W 2003 roku Komisja Europejska zaproponowała powołanie ponadnarodowej, europejskiej agencji zajmującej się zapewnieniem bezpieczeństwa w Internecie. Europejska Agencja Bezpieczeństwa Sieci i Informacji (The European Network and Information Security Agency) rozpoczęła działalność w styczniu 2004 roku i będzie działać przez okres siedmiu lat. Wówczas kompetencje ENISA, przejmie ustanowiony w grudniu 2007 roku, Europejski Urząd ds. Rynku i Łączności Elektronicznej.

Nowe wyzwania i zagrożenia cyberprzestrzeni spowodowały powstanie pierwszego dokumentu obejmującego kwestie bezpieczeństwa przestrzeni cybernetycznej państwa w postaci „Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009–2011". Celem strategicznym programu jest wzrost poziomu bezpieczeństwa cyberprzestrzeni państwa. Wśród celów szczegółowych w Programie wymienia się m.in. zwiększenie poziomu bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa skutkujące zwiększeniem poziomu odporności państwa na ataki cyberterrorystyczne. Jest to początek poważnej pracy nad zagadnieniem ochrony kluczowych zasobów telekomunikacyjnych oraz informatycznych, co dla rozwiniętej gospodarki jest tak samo ważne, jak rozwiązywanie problemów energetycznych i ekologicznych. Może to przynieść oczekiwaną standaryzację pojęć, postaw i praktyk w zakresie bezpieczeństwa narodowego – sprowadzanego nie tylko do fizycznych ataków na materialną infrastrukturę, bezpieczeństwo energetyczne lub walkę ze skutkami klęsk żywiołowych, ale także zabezpieczenia przed „cyberinwazją".

Bezpieczeństwo Unii Europejskiej, w tym bezpieczeństwo narodowe RP posiada istotny wymiar w cyberprzestrzeni, zaś waga zagrożeń dla bezpieczeństwa Europejskiej Przestrzeni Cybernetycznej i ochrony cyberprzestrzeni RP będzie rosnąć z roku na rok.

Literatura

[1] Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: szanse, zagrożenia, wyzwania*. Kraków 1995.
[2] Information and Communications Technologies OECD Information Technology Outlook 2008.
[3] Komunikat Komisji do Parlamentu Europejskiego i Rady w sprawie oceny Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), Bruksela, dnia 1.6.2007, KOM(2007)285.
[4] Kowalczyk M., *e-urząd w komunikacji z obywatelem*. WAiP, Warszawa 2008.
[5] Rządowy program ochrony cyberprzestrzeni RP na lata 2008–20011, Warszawa 2008.
[6] Sienkiewicz P., *Terroryzm w cybernetycznej przestrzeni*. [w:] Cyberterroryzm nowe wyzwania XXI wieku. Warszawa 2009.
[7] Świeboda H., *Bezpieczeństwo informacyjne dla bezpieczeństwa narodowego*. ZN AON nr 3, 68, 2007.
[8] Świeboda H., *Zagrożenia informacyjne bezpieczeństwa narodowego RP*. Rozprawa doktorska, AON Warszawa 2009 (w przygotowaniu).
[9] Świeboda H., *Zagrożenia informacyjne w odbiorze społecznym*. [w:] Cyberterroryzm nowe wyzwania XXI wieku. Warszawa 2009.
[10] *Zielona Księga. w sprawie europejskiego programu ochrony infrastruktury krytycznej*, Bruksela, 17.11.2005, COM(2005)576 końcowy.