ZNACZENIE TELEKOMUNIKACJI I TELEINFORMATYKI W SYSTEMIE BEZPIECZEŃSTWA PAŃSTWA

Andrzej Jóźwiak

Sesja Krajowego Sympozjum Telekomunikacji i Teleinformatyki, zorganizowana pod patronatem Biura Bezpieczeństwa Narodowego przez Komitet Elektroniki i Telekomunikacji PAN, to dowód na stopniowe rozszerzanie się spektrum dziedzin, które można określić wspólnym terminem – system bezpieczeństwa narodowego. Nasza wspólna praca świadczy także o coraz liczniejszych możliwościach podejmowania współdziałania pomiędzy instytucjami państwa, środowiskiem naukowym i podmiotami komercyjnymi w obszarach, w których wymiana doświadczeń może sprzyjać rozwojowi każdego z tych sektorów. Takim obszarem jest z pewnością szeroko rozumiana telekomunikacja i teleinformatyka, których miejsce i znaczenie w systemie bezpieczeństwa państwa postaram się teraz omówić.

I. BEZPIECZEŃSTWO NARODOWE

Precyzyjne zdefiniowanie samego pojęcia „bezpieczeństwo narodowe" nastręcza od dawna wielu problemów. Jest także przyczyną licznych sporów i polemik naukowych. Na potrzeby konferencji przyjmijmy definicję tego terminu, która znajduje się w opracowywanym przez Biuro Bezpieczeństwa Narodowego projekcie ustawy dotyczącym tego właśnie obszaru. Zapisano w nim, iż *bezpieczeństwo narodowe to stan, w którym nie są zagrożone byt, suwerenność, przetrwanie państwa oraz istnieją warunki do realizacji interesów narodowych i osiągania celów strategicznych Rzeczypospolitej Polskiej* [1]. Na tej podstawie można stwierdzić, że system bezpieczeństwa narodowego to całość mechanizmów przeciwstawiania się przez państwo wszystkim możliwym zagrożeniom (militarnym i niemilitarnym) z wykorzystaniem całego dostępnego mu potencjału (również militarnego i niemilitarnego).

Przy tak szeroko zdefiniowanym pojęciu bezpieczeństwa narodowego można przyjąć, iż w zakresie zainteresowania tej dziedziny życia społecznego leżą takie obszary, jak: obronność, ekonomia, ekologia czy komunikacja, w tym jej składowe – telekomunikacja i teleinformatyka.

Kategoria bezpieczeństwa narodowego, mimo niedookreślenia, występuje w wielu aktach prawnych, z których najważniejsza jest *Strategia bezpieczeństwa narodowego*, i w licznych ustawach, w tym tworzonej obecnie, porządkującej całość zagadnienia ustawie o bezpieczeństwie narodowym. Większość z nich uwzględnia od niedawna kwestie bezpieczeństwa teleinformatycznego, zarówno w postaci określonych zagrożeń, jak i środków przeciwdziałania im oraz ewentualnego zwalczania ich skutków.

II. STRATEGIA BEZPIECZEŃSTWA NARODOWEGO

Strategię bezpieczeństwa narodowego przyjmuje się w celu wspierania realizacji polityki Rzeczypospolitej Polskiej, zmierzającej do zapewnienia bezpieczeństwa narodowego. *Strategia* określa główne cele i priorytety polityki RP w zakresie zewnętrznego i wewnętrznego bezpieczeństwa państwa.

W szczególności uwzględnia:

- interesy Rzeczypospolitej Polskiej i cele strategiczne dotyczące bezpieczeństwa Rzeczypospolitej Polskiej;
- sposoby realizacji interesów Rzeczypospolitej Polskiej i osiągania przyjętych celów strategicznych;
- siły i środki niezbędne do wdrożenia przyjętych sposobów realizacji interesów Rzeczypospolitej Polskiej i osiągania celów strategicznych;
- organy administracji rządowej i państwowe jednostki organizacyjne zobowiązane do wykonywania zadań wynikających ze *Strategii*;
- warunki i istotne terminy realizacji zadań wynikających ze *Strategii*.

Strategia uwzględnia uwarunkowania wewnętrzne i zewnętrzne w realizacji interesów Rzeczypospolitej Polskiej i osiąganiu przyjętych celów strategicznych, w szczególności wewnętrzne i zewnętrzne zagrożenia bezpieczeństwa Rzeczypospolitej Polskiej.

Obowiązująca *Strategia bezpieczeństwa narodowego* z 2003 r. zwraca uwagę zarówno na zagrożenia z dziedziny telekomunikacji i teleinformatyki, jak również na działania i podmioty odpowiedzialne za ochronę przed tego typu zagrożeniami. *Coraz bardziej realne stają się dla Polski zagrożenia w sferze teleinformatycznej. Rośnie zagrożenie operacjami mającymi na celu dezorganizację kluczowych systemów informacyjnych instytucji rządowych oraz niektórych sfer sektora prywatnego, oddziałujących na system bezpieczeństwa państwa, a także operacjami związanymi z penetracją baz danych i prowadzeniem działań dezinformacyjnych.*

Zwalczanie zagrożeń dla rządowych systemów i sieci teleinformatycznych należy do kompetencji wyspecjalizowanych komórek cywilnych i wojskowych służb państwowych. Ich zadaniem jest zwalczanie przestępczości komputerowej wymierzonej w rządową i samorządową infrastrukturę telekomunikacyjną, w tym przeciwdziałanie atakom na jej elementy.

Do zapewnienia należytej ochrony tej infrastruktury niezbędny jest rozwój i utrzymanie zdolności do zapobiegania wszelkim zakłóceniom, jakie mogą wystąpić w tej sferze, a także zdolności do koordynacji procesów dochodzeniowych w ramach instytucji posiadających elementy rządowej infrastruktury teleinformatycznej. Wyznaczone służby będą podejmować działania wspólnie z sojusznikami, a także producentami i dostawcami urządzeń oraz oprogramowania informatycznego, krajowymi operatorami telekomunikacyjnymi i dostawcami usług internetowych, ośrodkami badawczymi i szkoleniowymi.

Aby podejmowane działania w tej dziedzinie były skuteczne, należy w sposób priorytetowy podejść do rozwoju i wdrażania rodzimej kryptografii oraz dostosować przepisy prawa telekomunikacyjnego, które wraz z szybkim postępem technologicznym mogą się okazać niewystarczające do zapewnienia bezpieczeństwa chronionej infrastrukturze teleinformatycznej [2].

III. SYSTEM OBRONNY PAŃSTWA

Jednym z elementów szeroko rozumianego systemu bezpieczeństwa państwa dla zapewnienia bezpieczeństwa narodowego, którego ramy wyznaczają akty prawne, jest jego system obronny. Terminem tym określamy skoordynowany wewnętrznie zbiór elementów organizacyjnych, ludzkich

i materiałowych wzajemnie powiązanych i działających na rzecz obrony państwa.

Celem systemu obronnego państwa jest:

- działanie na rzecz pokoju;
- wszechstronne przygotowanie państwa do odparcia ewentualnej agresji;
- likwidacja skutków zagrożeń.

Funkcjonowanie systemu obronnego państwa polega na podejmowaniu różnorodnych zadań i przedsięwzięć obronnych przez wszystkie ogniwa przygotowujące państwo do działania w okresie wzrostu zagrożenia jego bezpieczeństwa i na czas wojny.

System obronny państwa jest tworzony i działa na podstawie *Konstytucji RP*, jej przepisów dotyczących ustroju państwa, jego organów i kompetencji oraz innych ustaw określających założenia: militarne, gospodarczo-obronne, ochrony bezpieczeństwa obywateli i porządku publicznego.

W strukturze systemu obronnego państwa wyróżniamy trzy elementy:

- podsystem kierowania obronnością, obejmujący wszystkie organy władzy i administracji państwowej, samorządowej oraz dowództwa wojskowe, zgodnie z kompetencjami i zadaniami obronnymi przypisanymi im w obowiązujących aktach prawnych;
- podsystem militarny;
- podsystem niemilitarny.

System uzupełniają takie elementy, jak:

- polityka bezpieczeństwa;
- obronnie przygotowane społeczeństwo;
- infrastruktura obronna państwa.

Obecnie trudno wyodrębnić zagadnienia związane z komunikacją i informatyką jako składowe jedynie podsystemu niemilitarnego. Kwestie przekazywania i ochrony informacji są bowiem w każdym podsystemie i w każdym odgrywają niezwykle ważną rolę.

Poniżej przedstawiono te obszary systemu bezpieczeństwa państwa, w których telekomunikacja i teleinformatyka mogą mieć decydujący wpływ na powodzenie podejmowanych w ich ramach działań.

IV. OBSZARY ISTOTNE DLA BEZPIECZEŃSTWA NARODOWEGO W KONTEKŚCIE BEZPIECZEŃSTWA W TELEKOMUNIKACJI I TELEINFORMATYCE

W wąskim rozumieniu bezpieczeństwo teleinformatyczne i telekomunikacyjne jest uważane za zbiór zagadnień z dziedziny informatyki, dotyczący oceny i kontroli ryzyka związanego z korzystaniem z komputerów i sieci komputerowych, rozpatrywany z perspektywy poufności, integralności i dostępności danych.

Na potrzeby niniejszego opracowania, w celu pokazania związku pomiędzy omawianymi zagadnieniami a bezpieczeństwem państwa, należałoby jednak przyjąć zdecydowanie szerszą definicję. Zakładając, iż musimy brać pod uwagę działania z wielu dziedzin, obejmujące zarówno ochronę posiadanych informacji i sposobów ich przekazywania, jak i metody pozyskiwania danych z zewnątrz, złożoność tak opisanego zjawiska najlepiej oddaje tzw. wojna informacyjna. Może ona przybierać zarówno ofensywny, jak i defensywny charakter.

W literaturze przedmiotu podaje się, że *wojna informacyjna to operacje informacyjne prowadzone podczas kryzysu lub konfliktu w celu osiągnięcia lub poparcia konkretnych celów w odniesieniu do konkretnych przeciwników lub przeciwnika. Natomiast operacje informacyjne to działania podjęte w celu wywarcia wpływu na informacje i systemy informacyjne przeciwnika przy jednoczesnej obronie własnych informacji i systemów informacyjnych* [3].

Na tak określoną „wojnę" składają się ofensywne i defensywne działania, skierowane przeciw zasobom informacyjnym. Są to działania o charakterze „sukces-porażka". Wojnę prowadzi się, dlatego że te zasoby mają dla ludzi wartość. Działania ofensywne mają na celu zwiększenie wartości dla strony atakującej i zmniejszenie jej dla strony atakowanej. Operacje

defensywne zaś prowadzi się po to, by zapobiec potencjalnej utracie tej wartości.

Głównym przejawem działań o charakterze obronnym jest budowanie bezpiecznych systemów ochrony i przekazywania informacji. Prawdziwie bezpieczny system jest definiowany w zasadzie jako mechanizm wyidealizowany, praktycznie niemożliwy do osiągnięcia, który poprawnie i w całości realizuje tylko i wyłącznie cele zgodne z intencjami osoby nim się posługującej.

Zapewnienie bezpieczeństwa sprowadza się w praktyce do zarządzania ryzykiem. Wskazywane są potencjalne zagrożenia, szacowane jest prawdopodobieństwo ich wystąpienia, oceniany potencjał strat, następnie są podejmowane kroki zapobiegawcze w racjonalnym zakresie, biorąc pod uwagę możliwości techniczne i względy ekonomiczne.

Zagadnienia bezpieczeństwa teleinformatycznego i telekomunikacyjnego są szczególnie istotne dla tych wszystkich sektorów polityki bezpieczeństwa państwa, w których istnieje konieczność wykorzystywania przewagi informacyjnej i ochrony treści, do których dostęp powinien być ograniczony. Dotyczy to przede wszystkim:

1. Bezpieczeństwa militarnego

Zgodnie z decyzją ministra obrony narodowej za bezpieczeństwo teleinformatyczne uznaje się *całokształt przedsięwzięć zmierzających do zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych oraz ochrony informacji wytwarzanej, przetwarzanej, przechowywanej lub przekazywanej w tych systemach i sieciach przed przypadkowym lub celowym ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania poprzez zastosowanie w sposób kompleksowy technicznych, programowych, kryptograficznych oraz organizacyjnych środków i metod* [4].

W sektorze bezpieczeństwa militarnego zadania z zakresu ochrony systemów i sieci teleinformatycznych realizują:

a) w jednostce (komórce) organizacyjnej

- kierownik jednostki (komórki) organizacyjnej,
- pełnomocnik ochrony,

- administrator systemu,
- inspektor bezpieczeństwa teleinformatycznego;

b) Centrum Bezpieczeństwa Teleinformacyjnego;
c) Wojskowe Biuro Bezpieczeństwa Łączności i Informatyki;
d) organy bezpieczeństwa systemów łączności i informatyki jednostek organizacyjnych wszystkich szczebli dowodzenia;
e) Centrum Zarządzania Systemami Teleinformatycznymi;
f) Służba Kontrwywiadu Wojskowego.

Niezwykle ważna jest ochrona teleinformatyczna systemów łączności w trakcie pełnienia misji zagranicznych przez polskie kontyngenty wojskowe, szczególnie na obszarach bezpośrednich działań bojowych. W tym wypadku jej skuteczność może decydować wprost o życiu czy zdrowiu żołnierzy i dlatego coraz większy nacisk kładzie się na odpowiednie przygotowanie i zabezpieczenie pod tym względem operacji z udziałem polskich sił.

2. Bezpieczeństwa wewnętrznego

Za zagwarantowanie bezpieczeństwa telekomunikacyjnego i teleinformatycznego w działaniach związanych z zapewnieniem bezpieczeństwa wewnętrznego na poziomie państwa jest odpowiedzialna Agencja Bezpieczeństwa Wewnętrznego.

Do ustawowych zadań Agencji Bezpieczeństwa Wewnętrznego należy, między innymi, zapewnienie bezpieczeństwa systemów i sieci teleinformatycznych, w których są wytwarzane, przechowywane, przetwarzane lub przekazywane informacje niejawne stanowiące tajemnicę państwową lub służbową. Zadania ABW w tym zakresie realizuje wyspecjalizowany zespół Departamentu Bezpieczeństwa Teleinformatycznego – Jednostka Certyfikująca.

Jednostka Certyfikująca przeprowadza certyfikacje systemów i sieci teleinformatycznych oraz środków (wyrobów) w zakresie:

- ochrony kryptograficznej;
- ochrony elektromagnetycznej;
- ochrony akustycznej.

Certyfikacja środków ochrony bezpieczeństwa teleinformatycznego jest prowadzona według polskich i europejskich norm oraz kryteriów oceny.

Każdy system lub sieć teleinformatyczna, przeznaczone do przetwarzania informacji niejawnych stanowiących tajemnicę państwową, musi uzyskać certyfikat akredytacji bezpieczeństwa teleinformatycznego. Uzależnione jest to od zastosowania certyfikowanych środków ochrony oraz przedstawienia przez użytkownika, zatwierdzonych przez służbę ochrony państwa, *Szczególnych wymagań bezpieczeństwa systemu lub sieci TI* i *Procedur bezpiecznej eksploatacji*.

3. Bezpieczeństwa ekonomicznego

Zagadnienia z zakresu teleinformatyki i telekomunikacji stanowią także ważny element zapewnienia państwu bezpieczeństwa w dziedzinie ekonomii i szeroko rozumianego funkcjonowania gospodarki kraju. Przyjmując za punkt wyjścia omawiane wcześniej zagadnienia militarne, trzeba podkreślić, że szczególnej ochronie podlegają technologie, dane i systemy przekazywania informacji wykorzystywane w przemyśle zbrojeniowym oraz w niezwykle ważnej z punktu widzenia bezpieczeństwa państwa gałęzi – ekonomii. Nieuprawniony dostęp do tzw. wrażliwych informacji mógłby spowodować kryzys i zagrożenie dla państwa także w innych kluczowych dziedzinach gospodarki, chociażby w sektorze energetycznym. Nietrudno wyobrazić sobie paraliż systemu dostarczania energii do prywatnych odbiorców, a co ważniejsze, do różnego rodzaju instytucji i przedsiębiorstw w razie cyberataku na wykorzystywaną do tego celu infrastrukturę.

Inna dziedzina ekonomii podatna na zagrożenia bezpieczeństwa teleinformatycznego i telekomunikacyjnego to szeroko rozumiane rynki finansowe. Czarne scenariusze przewidują możliwość sztucznego wywołania przez cyberterrorystów krachu na giełdach, zablokowania systemu bankowego czy wywołania paniki w społeczeństwie, która w konsekwencji, na zasadzie efektu domina, mogłaby doprowadzić do załamania całego państwowego systemu finansów publicznych.

Dla obywateli, w tym przede wszystkim osób prowadzących działalność gospodarczą, równie istotne będzie tworzenie systemów zabezpieczeń teleinformatycznych w ramach ich przedsiębiorstw czy innego rodzaju podmiotów. Pozwalają one chronić zasoby firmy przed nieuczciwą konkurencją

i wywiadem gospodarczym, czyli wrogimi działaniami ze strony osób dążących do nielegalnego zdobycia wiedzy stanowiącej własność i dorobek jej posiadacza.

4. Innych dziedzin

Inne obszary, w których zagadnienia teleinformatyki i telekomunikacji mogą mieć istotne znaczenie dla całości systemu bezpieczeństwa państwa, to ochrona danych osobowych, wymiar sprawiedliwości czy ekologia. Ujawnienie informacji, do których dostęp powinien być chroniony, mogłoby doprowadzić do zmniejszenia poczucia bezpieczeństwa obywateli bądź do katastrofy naturalnej, której skutki trudno dziś precyzyjnie przewidzieć.

V. PODSUMOWANIE

Z punktu widzenia Biura Bezpieczeństwa Narodowego, teleinformatyka i telekomunikacja to kwestie, którym na poziomie państwa należy poświęcić więcej niż dotychczas uwagi, gdyż zaniedbania w tej dziedzinie mogą doprowadzić do równie negatywnych konsekwencji, jak nieskuteczne działania sił zbrojnych czy zaniechania w obszarze zapewnienia bezpieczeństwa energetycznego państwa. Doskonałym przykładem i dowodem na to może być przeprowadzony kilka miesięcy temu cyberatak na oficjalne, państwowe serwisy internetowe Estonii. Biorąc pod uwagę, iż jest to jeden z najbardziej zinformatyzowanych krajów w UE oraz że przez Internet odbywa się tam głosowanie w wyborach czy składanie deklaracji podatkowych, incydent ten mógł w bezpośredni sposób oddziaływać na funkcjonowanie całego państwa i zagrażać jego bezpieczeństwu. Jest to niezwykle istotne doświadczenie, z którego trzeba wyciągnąć wnioski, aby zapobiegać podobnym sytuacjom w przyszłości.

Korzyścią, jaka powinna wyniknąć z sympozjum, mogłaby być dalsza owocna współpraca pomiędzy podmiotami reprezentującymi różne sektory życia społecznego. Takie współdziałanie, wymiana doświadczeń i wzajemne wsparcie z pewnością przyczynią się do uświadomienia całemu środowisku znaczenia kwestii bezpieczeństwa teleinformatycznego w różnych dziedzinach funkcjonowania państwa. Dyskusja, którą podejmujemy dzięki inicjatywie Komitetu Elektroniki i Telekomunikacji PAN, to doskonały

początek współpracy i rozpoczęcie debaty nad sposobami udoskonalenia mechanizmów zabezpieczenia naszego kraju przed zagrożeniami o charakterze uznawanym za wirtualny, chociaż w rzeczywistości nie mniej realnymi niż te fizyczne, do których zwalczania jesteśmy już jednak lepiej przygotowani.

Literatura

[1] Biuro Bepieczeństwa Narodowego, projekt ustawy o bezpieczeństwie, Warszawa 2007, s.1.

[2] *Strategia Bepieczeństwa Narodowego z lipca 2003.*

[3] Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji,* Wydawnictwo Naukowo Techniczne, Warszawa 2002, s. 11 i 23.

[4] *Decyzja Ministerstwa Obrony Narodowej nr 24 w sprawie organizacji szczególnej ochrony systemów i sieci telekomunikacyjnych w resorcie obrony narodowej z dnia 31 stycznia 2006 r.*