# ANALIZA ZAGROŻEŃ TELEKOMUNIKACYJNYCH SEKTORA PUBLICZNEGO

*Krystian Baniak*

## ANALIZA ZAGROŻEŃ
Obszar publiczny

*Światowa gospodarka oraz ekonomia nie byłyby w stanie rozwijać się dzisiaj bez dostępu do informacji – są one uzależnione od krytycznej infrastruktury telekomunikacyjnej. Infrastruktura telekomunikacyjna jest jednak obszarem, w którym występuje wiele rozmaitych zagrożeń – skonkretyzowane, stanowią ryzyko dla jej ciągłości operacyjnej. Niniejszy artykuł jest próbą usystematyzowania tychże zagrożeń w obrębie sektora publicznego oraz określenia ich wpływu na bezpieczeństwo i obronność nowoczesnego kraju ery informatycznej.*

Infrastruktura telekomunikacyjna jest ważnym elementem każdego nowoczesnego państwa. Umożliwia wymianę informacji oraz rozwój ekonomii i gospodarki, a także poprawne funkcjonowanie struktur państwowych i publicznych. W ramach nowoczesnej infrastruktury telekomunikacyjnej wyróżnia się następujące usługi:

- transmisję przekazu głosowego,
- transmisję danych cyfrowych,
- transmisję obrazów ruchomych – wideo.

W szczególności odpowiednio do zastosowanej technologii transmisji i typu ograniczeń sprzętowych poszczególne usługi są świadczone w postaci osobnych podsystemów – warstw usług, lub w formie zunifikowanej – w ramach jednego systemu (np. *IP Multimedia System* – IMS).

Infrastrukturę telekomunikacyjną państwa tworzą następujące elementy – warstwy:

- publiczna infrastruktura komunikacyjna, dostępna dla ogółu obywateli – świadczona przez operatorów usług

- telefonia stacjonarna PSIN,
- telefonia mobilna GSM,
- sieć Internet;

- prywatna infrastruktura komunikacyjna, tworzona w ramach organizacji prywatnych

  - organizacje komercyjne,
  - organizacje akademickie i społeczne,
  - przemysł oraz systemy zaopatrzenia energetycznego;

- warstwa komunikacyjna sektora rządowego i służb państwa

  - służby ratownicze,
  - służby porządkowe oraz militarne,
  - struktury administracyjne,
  - struktury zarządzania w sytuacjach kryzysowych.

W ramach poszczególnych warstw odpowiednie organizacje tworzą zamknięte sieci telekomunikacyjne, przeznaczone dla związanych z nimi osób. Ze względu na potrzebę współpracy i konieczność wymiany informacji organizacje korzystają także z publicznych sieci komunikacyjnych, budując w ten sposób skomplikowane struktury zależności pomiędzy warstwami. W ten sposób sieci usług publicznych stają się krytycznym elementem z punktu widzenia jej użytkowników.

Złożoność powiązań pomiędzy wymienionymi warstwami oraz rosnące zależności wiążą się ściśle z wymienionymi poniżej czynnikami [1].

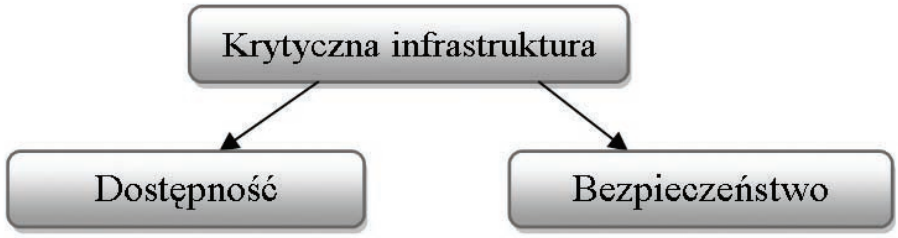
- Rosnący poziom złożoności systemów informatycznych – rośnie liczba obywateli korzystających z sieci Internet i zaspokajających za jej pomocą własne potrzeby – usługi.
- Wysoki poziom powiązań pomiędzy systemami – organizacje tworzą rozbudowane interfejsy informacyjne (np. strony WWW) oferujące usługi dla swoich klientów.
- Rosnący poziom skomplikowania interakcji i wzajemnych zależności pomiędzy dostawcami a odbiorcami usług oraz, co się z tym wiąże, uzależnienia od dostępności infrastruktury telekomunikacyjnej.

Z całości struktur komunikacyjnych należy wyłonić zbiór systemów, który jest istotny dla działania podstawowych funkcji państwowych i publicznych. Zbiór ten będziemy nazywać infrastrukturą krytyczną (IK).

## DEFINICJA KRYTYCZNEJ INFRASTRUKTURY TELEKOMUNIKACYJNEJ

Z uwagi na znaczenie KIT, jej charakterystycznymi cechami będą naturalnie dostępność oraz bezpieczeństwo (rys. 1).

Aby zapewnić dostępność oraz bezpieczeństwo infrastruktury, musimy zdefiniować zagrożenia, obszary ich występowania oraz oszacować ryzyko im towarzyszące. Poprawnie oszacowane ryzyko umożliwi dobranie właściwych środków zaradczych.




*Rys. 1. Atrybuty krytycznej infrastruktury informatycznej (KIT)*

*Krytyczną infrastrukturą telekomunikacyjną (KIT) nazywamy zespół sieci oraz struktur komunikacyjnych, które uszkodzone lub zniszczone, w sposób istotny wpłynęłyby na funkcjonowanie państwa (społeczeństwa).*

Zgodnie z Europejskim Programem Ochrony Infrastruktury Krytycznej (EPCIP[2]) wyróżnia się jedenaście sektorów wchodzących w skład KI [3]. Są to:

I. Energia.
II. Systemy informacyjne ICT.
III. Zasoby wodne.
IV. Żywność.
V. Opieka medyczna.
VI. Finanse.
VII. Bezpieczeństwo publiczne.
VIII. Administracja cywilna.
IX. Transport.
X. Przemysł chemiczny i energia jądrowa.
XI. Instytucje badawcze i programy kosmiczne (ang. *Space & Research*).

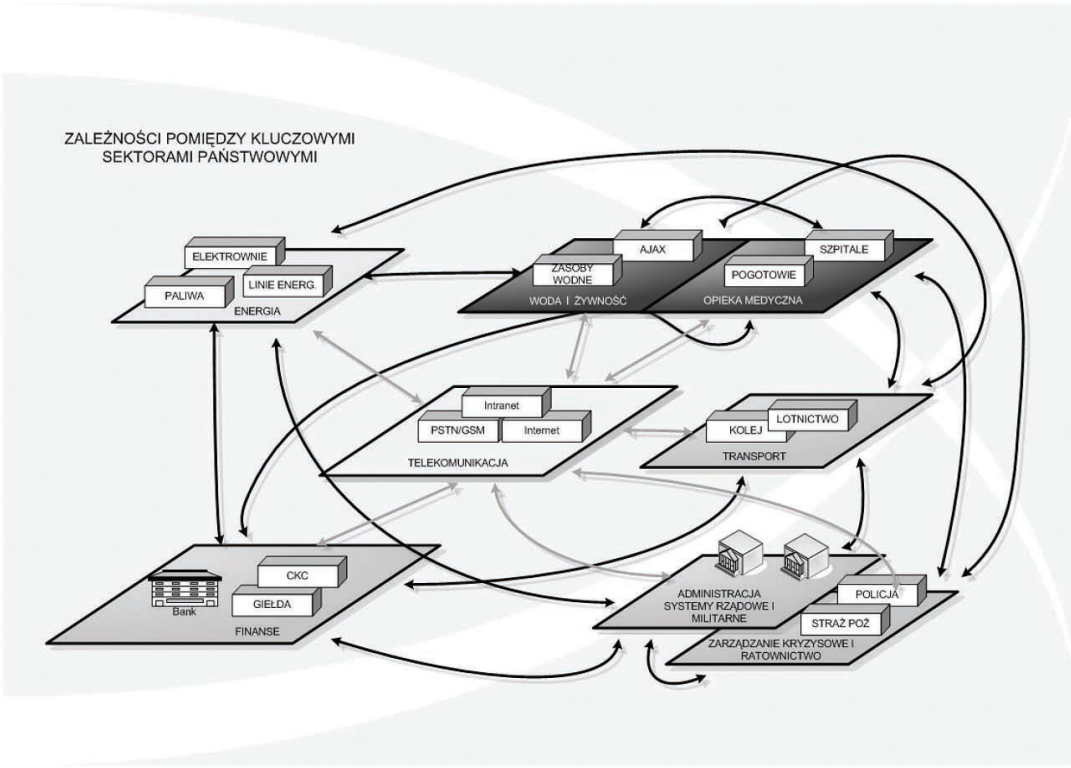
Każdy sektor składa się z wielu podstruktur, w tym systemów komunikacyjnych służących do wymiany informacji oraz systemów kontroli i monitorowania (ang. SCADA[3]). Wiele sieci typu SCADA jest wzajemnie zależnych, co w razie zagrożenia lub kryzysu może mieć implikacje w postaci efektu domina – załamania się powiązanych systemów.

Wzajemne powiązania w ramach sektorów (rys. 2) mogą mieć charakter powiązań:

- geograficznych,
- natury fizycznej,
- natury informatycznej.

W wypadku infrastruktury komunikacyjnej interesują nas sieci i struktury służące do wymiany informacji międzysektorowej i wewnątrzsektorowej.

Powiązania między sektorami KI są bardzo skomplikowane. Niemniej jednak sektor komunikacyjny jest ogniwem, który spina pozostałe elementy, wychodząc tym samym na kluczową pozycję. Bez sprawnej komunikacji dzisiejsze społeczeństwo nie byłoby w stanie efektywnie funkcjonować.




*Rys. 2. Zależności pomiędzy sektorami kluczowymi*

Powiązania krytycznej infrastruktury telekomunikacyjnej przedstawiono w tabeli 1.

Podsumowując, należy stwierdzić, że infrastruktura komunikacyjna jest infrastrukturą krytyczną z punktu widzenia nowoczesnego społeczeństwa [3]. W Unii Europejskiej problem krytycznej infrastruktury ma szerszy wymiar z uwagi na skomplikowane powiązania pomiędzy państwami członkowskimi (ang. *Member States*) oraz wykorzystywanie paneuropejskich systemów informacyjnych.

2) EPCIP – European Program for Critical Infrastructure Protection, EU, utworzony w 2004 roku.

3) SCADA – Supervisory Control & Data Acquisition.

*Tabela 1. Powiązania w infrastrukturze telekomunikacyjnej*

| | |
|---|---|
| Czynniki geograficzne | ▪ Lokalizacja kluczowych elementów infrastruktury<br>▪ Przebieg traktów komunikacyjnych w odniesieniu do wymogów nadmiarowości<br>▪ Odległości pomiędzy centrami zapasowymi<br>▪ Położenie geograficzne a podatność na występowanie katastrof naturalnych oraz niestabilność polityczna |
| Czynniki fizyczne | ▪ Bezpieczeństwo fizyczne obiektów komunikacyjnych<br>▪ Ochrona przed nieautoryzowanym dostępem<br>▪ Bezpieczeństwo zasilania i energetyczne<br>▪ Wpływ środowiska naturalnego<br>▪ Zależność od stron trzecich |
| Czynniki informatyczne | ▪ Niezawodność technologii oraz oprogramowania<br>▪ Bezpieczeństwo traktów elektronicznych i odporność na zakłócenia transmisji<br>▪ Dostępność systemów informatycznych (bazy danych) |

## DEFINICJA OBSZARÓW ZAGROŻEŃ INFRASTRUKTURY TELEKOMUNIKACYJNEJ

Zgodnie z definicją zagrożenie jest wydarzeniem, którego wystąpienie ma niepożądany wpływ na poprawny stan obiektu. Przykładem zagrożenia będzie np. huragan lub kradzież. W procesie wymiany informacji pożądanym rezultatem jest bezpieczeństwo przesyłanych danych, gwarancja dostarczenia ich w niezmodyfikowanej formie i w odpowiednim czasie. Zagrożenia dla tych celów będą związane z zamierzonymi lub przypadkowymi incydentami zmodyfikowania, podsłuchania lub uniemożliwienia transmisji.

Incydenty niezamierzone są powodowane przez katastrofy naturalne, anomalie pogodowe, działania wojenne, awarie systemów wsparcia (zasilanie, HVAC) lub awarie sprzętu.

Incydenty zamierzone są ukierunkowanymi działaniami osób lub wrogich organizacji, mającymi na celu nielegalne wykorzystanie zasobów, usług lub przechwycenie (zmodyfikowanie) informacji.

Aby precyzyjnie zdefiniować obszary zagrożeń w ramach infrastruktury telekomunikacyjnej, postanowiliśmy zastosować następujący jej podział strukturalny.

- **Organizacja** – formalny podmiot sprawujący kontrolę nad daną infrastrukturą telekomunikacyjną.
- **Personel** – pracownicy zarządzający, korzystający z danej infrastruktury i ją utrzymujący.
- **Polityka bezpieczeństwa** – założenia, standardy, procedury, wytyczne, normatywy bezpiecznego korzystania z infrastruktury w ramach danej organizacji.
- **Placówki** – obiekty fizyczne należące do organizacji (budynki, obiekty techniczne).
- **Infrastruktura** – środki technologiczne – elementy zapewniające funkcjonowanie organizacji, przetwarzanie i przesyłanie informacji.

Mając zdefiniowane elementy składowe infrastruktury, zajmiemy się obszarami, w których występują zagrożenia. Przedstawiony podział jest wynikiem licznych obserwacji i analiz; często stosuje się go w zestawieniach zagrożeń telekomunikacyjnych [4,5,6].

- **Środowisko/energia** – systemy zasilania, wentylacji, klimatyzacji, uzdatniania powietrza (ang. HVAC) oraz bezpieczeństwa fizycznego.
- **Technologia** – sprzęt oraz oprogramowanie.
- **Dane/transmisja** – sieci transmisyjne, ich topologie, redundancja, synchronizacja. W wypadku transmisji są to metody przechowywania, reprezentacji oraz przesyłania danych.
- **Czynnik ludzki** – polityka bezpieczeństwa, świadomość personelu i użytkownika końcowego, wpływ regulacji prawnych, zagadnienia związane z etyką pracy. Jest to najważniejszy obszar zagrożeń, gdyż najbardziej nieprzewidywalny.

Następnie zostaną omówione poszczególne obszary zagrożeń wraz z przykładami problemów ściśle z nimi związanych.

*Zagrożenia obszaru środowiskowego*

- Występowanie katastrof naturalnych: powodzi, huraganów, trzęsień ziemi.
- Zawodność systemów energetycznych oraz zasilania zapasowego (dostępność paliwa, zagrożenie pożarowe składów paliwa).
- Sabotaż oraz zagrożenia terrorystyczne instalacji i obiektów fizycznych.
- Odporność na włamania i szczelność systemów kontroli dostępu – bezpieczeństwo lokalizacji:

    - możliwość obserwacji przez osoby postronne;
    - polityczne i kryminalne uwarunkowania danej lokalizacji geograficznej (np. występowanie zamieszek, niestabilność polityczna regionu);
    - odległość od zabudowań i terenów publicznych – dostępność;
    - ogrodzenia, czujniki, monitoring, środki ochrony bezpośredniej;
    - ochrona fizyczna, szkolenie i zaufanie do kadry.

- Nieskuteczny system monitorowania i analizy logów.
- Zależność od zasobów i wsparcia, które nie są trwałe.

Możliwość wykorzystania słabości ochrony fizycznej jest poważnym zagrożeniem, gdyż eliminacja wybranej placówki może oznaczać powstanie szkód o globalnym dla danej organizacji zasięgu. Związane jest to z występowaniem skomplikowanych powiązań i zależności pomiędzy systemami korzystającymi z infrastruktury krytycznej.

Bezpieczeństwo energetyczne polega na wyposażeniu wielu źródeł zasilania w niezbędne do funkcjonowania elementy. Jednym z poważniejszych zagrożeń fizycznych jest często zależność od jednej elektrowni lub systemu dostaw (w przypadku procesów produkcji).

*Zagrożenia obszaru technologicznego*

- Brak mechanizmów zwielokrotniania i redundancji sprzętowej i logicznej (np. brak alternatywnych torów transmisyjnych).
- Występowanie błędów produkcyjnych lub konstrukcyjnych (błędy

logiczne trudne do wykrycia), które mogą być szczególnie niebezpieczne w wypadku uzależnienia od jednego dostawcy sprzętu.
- Jakość oprogramowania – występowanie błędów, kosztowne procedury testowania poprawek i wdrażania ich w życie. Poprawki oprogramowania mogą doprowadzić do destabilizacji pracy systemu poprzez zmianę lub unieruchomienie logiki działania aplikacji.
- Bezpieczeństwo oprogramowania – występowanie błędów pozwalających na przejęcie kontroli nad aplikacją (sprzętem).
- Odporność technologii transmisji na przechwycenie i zakłócenia elektromagnetyczne oraz na warunki środowiskowe.
- Cykl życia urządzeń i czas do pierwszej awarii.
- Odporność na warunki pracy i wpływ środowiska.

Odpowiednio zaprojektowany i wykonany sprzęt oraz oprogramowanie jest kluczem do sukcesu w tym obszarze. Niestety rzeczywistość jest inna i należy zwrócić uwagę na poprawne podejście do kwestii wyboru i procedur użytkowania. Ważne są także rozwiązania alternatywne (dywersyfikacja dostawców) oraz odpowiedni cykl życia wyposażenia. Nie należy wprowadzać nowych rozwiązań bez dokonania testów zgodności ze standardami i deklaracjami producenta. Wewnętrzne standardy organizacji powinny mieć najwyższy priorytet w tej kwestii, gdyż wiążą się bezpośrednio ze sprawnością operacyjną instytucji.

W przypadku rozwiązań telekomunikacyjnych ważną kwestią jest także odporność na zakłócenia elektromagnetyczne oraz niski poziom strat w postaci emisji wtórnej. Istotne podsystemy przetwarzające informację poufną i tajną powinny unikać technologii otwartego dostępu typu WiFi, a przynajmniej stosować dodatkowe zabezpieczenia. Należy brać pod uwagę możliwości podsłuchania lub zapisania transmisji poprzez emisję elektromagnetyczną lub nielegalne podpięcie się do systemu i dlatego trzeba przedsięwziąć odpowiednie środki kontroli na wyższych warstwach kanału informacyjnego (na poziomie warstwy transportowej lub aplikacyjnej modelu OSI).

Odporność technologii wykorzystywanych w infrastrukturze powinna uwzględniać warunki pogodowe i kalkulować sytuacje ekstremalne występujące w regionie użytkowania. Radiolinie – planowanie radiowe, na przykład, powinno uwzględniać zmienne warunki, takie jak deszcz czy śnieg, i zapewniać odpowiedni margines tolerancji. Wiąże się to z procesem pla-

nowania i określania warunków brzegowych dla infrastruktury (bezpieczna metodologia).

*Zagrożenia obszaru danych i sieci*

- Techniki transmisji (np. bezprzewodowe) oraz protokoły przesyłania danych (nieszyfrowane) nie zawsze umożliwiają poufny, integralny oraz uwierzytelniony przekaz (potwierdzenie deklarowanego źródła lub odbiorcy przekazu).
- Topologie projektowanych sieci mogą nie zapewniać odporności na uszkodzenia lub pracować z mniejszą niż szacowana wydajnością – problem poprawnego projektowania i skalowalności.
- Jakość implementacji standardów jest przyczyną braku kompatybilności pomiędzy sprzętem różnych dostawców.
- Synchronizacja (niepoprawna, uszkodzona) sieci i elementów toru transmisji może być źródłem problemów.
- Zarządzanie i aktualizacja oprogramowania oraz konfiguracji urządzeń sieciowych (bezpieczeństwo).
- Stopień skomplikowania stanowi zagrożenie dla funkcjonowania – łatwość popełnienia pomyłki.

Sieci komputerowe i telekomunikacyjne są podstawą systemów wymiany informacji. Projektowanie ich oraz opieka nad wdrożeniem i utrzymaniem jest kluczową sprawą. „Dziurawy" i nieefektywny system wymiany danych będzie łatwo kompromitowalny i mało użyteczny. W krytycznym momencie musi on działać pewnie i efektywnie. Istotnym zagadnieniem jest etap planowania, zwłaszcza w kontekście pojemności i wydolności sieci, która ma zapewnić parametry w sytuacji kryzysowej, często wiążącej się ze znacznym wzmożeniem ruchu.

Infrastruktura krytyczna w postaci sieci transmisyjnych spełnia swoje zadanie, jeśli:

- Topologia charakteryzuje się odpornością na uszkodzenia (redundantny sprzęt oraz alternatywne trasy) i adaptacją do zmieniających się warunków (występowanie awarii).
- Transmisja jest bezpieczna – informacje są przesyłane w poufny, nienaruszony sposób. Osoby trzecie nie są w stanie wprowadzić zakłóceń lub uzyskać dostępu.

- Konfiguracja i zarządzanie siecią jest zdefiniowanym cyklicznym oraz udokumentowanym procesem.
- Personel jest przygotowany i przeszkolony na wypadek sytuacji kryzysowych – każdy wie, co ma robić i do kogo raportuje – sytuacje te są regularnie ćwiczone w praktyce.
- Zdefiniowano plan współpracy z partnerami, polegający na wzajemnej pomocy w sytuacjach kryzysowych (wykorzystanie zasobów innej organizacji).

*Zagrożenia obszaru czynnika ludzkiego*

- Zagrożenia fizyczne – kradzież, sabotaż, terroryzm.
- Zagrożenia mentalne – intencja oszukania, wprowadzenia w błąd, zmiany opinii publicznej na temat podmiotu.
- Zagrożenia etyczne – niezadowoleni obywatele, pracownicy, zemsta.
- Zagrożenia organizacyjne – nieświadome działanie szkodliwe, wynikające z niewiedzy użytkownika systemu.
- Brak polityki bezpieczeństwa.
- Nierealistyczna lub niejednoznaczna polityka bezpieczeństwa (PB).
- Brak wsparcia kardy menedżerskiej dla egzekwowania PB.
- Nierealistyczne regulacje prawne i luki prawne.
- Brak szkoleń i kampanii uświadamiających użytkowników.

Czynnik ludzki jest odpowiedzialny za niedoskonałość rozwiązań oraz za wykorzystywanie systemów w celach nieprzewidzianych i niedozwolonych. Jest źródłem ustawicznych problemów w każdym systemie informacyjnym. Kluczową sprawą jest więc uprzedzanie faktów oraz precyzyjne definiowanie przeznaczenia systemu na etapie przygotowywania polityki bezpieczeństwa, będącej zbiorem dozwolonych czynności w ramach rozważanego systemu. Politykę bezpieczeństwa w konsekwencji realizuje się przez ustalenia, dobór standardów, procedur, wytycznych i regulacji, które z kolei są realizowane za pomocą środków kontroli. Zawodności czynnika ludzkiego nie jesteśmy w stanie wyeliminować, a więc realistyczny i w pełni wdrożony projekt polityki bezpieczeństwa jest jedynym optymalnym rozwiązaniem tego problemu.

Analiza zagrożeń opiera się na wiedzy na temat problemów i zachowań ludzi, którzy je wywołują. Wiedza ta pochodzi z doświadczeń i obserwacji wynikających z użytkowania systemów komunikacyjnych. Jednakże metoda ta nie pozwala przewidzieć nowych elementów, nie jest w stanie zgłębić ludzkiej pomysłowości oraz nieprzedywalności.

Alternatywą jest analiza podatności systemu. Polega ona na ustaleniu słabych punktów oraz usterek systemu. W odróżnieniu od analizy zagrożeń, ta metodologia pozwoli na zabezpieczenie przed nowymi, nieznanymi typami ataków, likwidując problem w zarodku – usuwając lub poprawiając słabość – podatność systemu.

Analiza podatności jest wstępem do fazy szacowania ryzyka oraz doboru środków eliminacji ryzyka.

Szczegółowe przedstawienie metod szacowania ryzyka wykracza poza zakres niniejszego opracowania. Jedna z metod jest przedstawiona w referacie Dariusza Kulawika w dalszej części tego opracowania.

## WPŁYW ZAGROŻEŃ NA STAN BEZPIECZEŃSTWA KRAJU

Dzisiejszy świat jest pełen zależności politycznych i ekonomicznych, w których ramach państwa współzawodniczą ze sobą, często wykorzystując kwestionowane metody wspomagania swojej pozycji. Znajduje to swoje odzwierciedlenie w społeczeństwie. Internet i świat usług przesyłania informacji, dając iluzoryczną anonimowość, zachęca do zwiększania swoich szans poprzez wykorzystywanie luk w bezpieczeństwie systemów informatycznych. Wykorzystywanie ułomności technologii lub logiki systemów można podzielić na kategorie ze względu na motywację atakującego [2]:

- operacje wywiadowcze,
- szpiegostwo przemysłowe (technologiczne),
- podziemie komputerowe,
- motywy polityczne.

Zagrożenia mają wpływ na następujące kluczowe elementy państwa:

- ekonomię – w postaci wydatków pokrywających koszty usuwania problemów i zagrożeń,
- bezpieczeństwo wewnętrzne (militarne),
- wizerunek międzynarodowy – kraj, który nie potrafi zadbać o bezpieczeństwo własnych systemów komunikacyjnych, może nie być wiarygodnym partnerem lub sojusznikiem,
- osiągnięcia technologiczne – szpiegostwo przemysłowe, wykorzystujące luki w bezpieczeństwie komunikacyjnym, bezpośrednio wpływa na straty w zakresie łamania prawa patentowego lub wyłączności na technologie,
- opinię publiczną – poczucie bezpieczeństwa społeczeństwa wiąże się z sukcesami na arenie publicznej, a nie z porażkami, które są szybko rozgłaszane przez media,
- stosunki dyplomatyczne – zaufanie między partnerami to zaufanie w stosunku do ich infrastruktury,
- sprawność operacyjną – łączność w sferze publicznej oraz rządowej, która jest sprawna zarówno w czasie spokoju, jak i w stanie wyjątkowym.

Zagrożenia oraz ich konsekwencje powodują, że kwestia bezpiecznej i dostępnej KI jest sprawą najwyższej wagi każdego nowoczesnego państwa w dzisiejszej rzeczywistości geopolitycznej.

## PODSUMOWANIE

Bezpieczeństwo krytycznej infrastruktury telekomunikacyjnej jest skomplikowanym zagadnieniem. Zapewnienie odpowiedniego poziomu obsługi oraz gotowości jest często wysiłkiem ponad możliwości organizacji. I dlatego kluczowa jest współpraca opiekunów KIT z odpowiednimi organami państwowymi oraz innymi organizacjami świadczącymi usługi telekomunikacyjne.

Zagadnienie współpracy oraz metodologii postępowania jest od dawna przedmiotem rozważań Komisji Europejskiej, która w ramach programu EPCIP [3] opublikowała w grudniu 2006 roku propozycję dyrektywy regulującej kwestie krytycznej infrastruktury w Unii Europejskiej.

Kluczowymi elementami metodologii opieki nad KI są:

- Identyfikacja KI w ramach każdego państwa członkowskiego (ang. *Member State* – MS).
- Ustanowienie ośrodka koordynacji KI w ramach MS jako punktu kontaktu z właścicielami KI danego państwa.
- Formalne wymogi odnośnie do definicji, implementacji i nadzoru KI w postaci odpowiednich ustaw.
- Centralna koordynacja.

Współpraca pomiędzy dostawcami usług oraz pomiędzy nimi a agencjami rządowymi (lub unijnymi) okazuje się bardzo istotna w procesie poprawy bezpieczeństwa i dostępności sieci telekomunikacyjnych w Europie. Wspólny dialog pozwoli określić i wyodrębnić systematykę zagrożeń oraz opracować spójną politykę przeciwdziałania.

*Literatura*

[1] *Gordon A. Gow: Policymaking for Critical Infrastructure,* Ashgate Publishing Ltd. 2005, s. 4.

[2] *NCS, The Electronic Intrusion Threat to Nation Security and Emergency Preparedness Telecommunication,* DIANE Publishing, 1994.

[3] *Commission of the European Communities, Green Paper on a European program for critical infrastructure protection,* Brussels 17.11.2005, COM(2005) 576 Final.

[4] *Availability and Robustness of Electronic Communications Infrastructures,* January 2007, Report for European Commission prepared by Alcatel-Lucent.

[5] Rauscher, Karl F., *Protecting Communications Infrastructure, Bell Labs Technical Journal Homeland Security Special Issue,* Volume 9, Number 2, 2004.

[6] Rauscher, Karl F., Krock, Richard E., Runyon, James P., *Eight Ingredients of Communications Infrastructure: A Systematic and Comprehensive Framework for Enhancing Network Reliability and Security Bell Labs Technical Journal Homeland Security Special Issue,* Volume 9, Number 2, 2004.