Critical Infrastructure Resilience as the Factor for Structural Homeland Security

Niezawodność infrastruktur krytycznych jako element bezpieczeństwa strukturalnego państwa

Michał Choraś,
Instytut Telekomunikacji, UTP Bydgoszcz
chorasm@utp.edu.pl

Rafał Kozik,
Instytut Telekomunikacji, UTP Bydgoszcz

Adam Flizikowski,
Instytut Telekomunikacji, UTP Bydgoszcz

Witold Hołubowicz
Instytut Telekomunikacji, UTP Bydgoszcz

Abstracts

In this paper several factors regarding Critical Infrastructures Protection (CIP) are presented. The overview of the natural and cyber threats is given. Then, the current work and propositions of CI protection solutions of the European Project CIPRNet (Critical Infrastructure Preparedness and Resilience Research Network) are presented.

W artykule przedstawiono szereg aspektów ochrony infrastruktur krytycznych. Przedstawiono zagrożenia naturalne, a także coraz groźniejsze zagrożenia pochodzące z cyberprzestrzeni. Następnie przedstawiono propozycje projektu FP7 CIPRNet (Critical Infrastructure Preparedness and Resilience Research Network) w zakresie ochrony infrastruktur krytycznych.

KEY WORDS:

Critical Infrastructure Protection, homeland security, resilience, cyber security of critical infrastructure.

Ochrona Infrastruktury Krytycznej (CIP – Critical Infrastructure Protection), bezpieczeństwo strukturalne państwa, niezawodność, cyber bezpieczeństwo infrastruktury krytycznej.

WPROWADZENIE

W niniejszym artykule przedstawiono aspekty niezawodności infrastruktur krytycznych jako element bezpieczeństwa strukturalnego państwa.

Obywatele często traktują pewne dobra jako oczywiste i dostępne – już tylko chwilowy brak energii elektrycznej lub wody jest przez nich bardzo zauważalny. Infrastruktury odpowiedzialne za dostarczanie takich dóbr i zasobów określane są mianem krytycznych. Są one ściśle związane z sektorem energetycznym, wodnym, ochroną zdrowia, transportem, systemami finansowymi, systemami informacyjnymi, itp.

Na potrzeby niniejszego artykułu, autorzy przyjęli następującą definicję infrastruktury krytycznej:

„Infrastruktura krytyczna oznacza składnik, system lub część infrastruktury zlokalizowanej na terytorium danego państwa, które mają podstawowe znaczenie dla utrzymania niezbędnych funkcji społecznych, zdrowia, bezpieczeństwa, ochrony, dobrobytu materialnego lub społecznego ludności oraz których zakłócenie lub zniszczenie miałoby istotny wpływ na dane państwo w wyniku utracenia tych funkcji." (Dyrektywa Rady 2008/114/WE).

Z punktu widzenia obywateli dobra takie powinny być wysoce dostępne, a dostarczające je systemy niezawodne. z punktu widzenia państwa, powinny być one bezpieczne (odpowiednio chronione), niezawodne oraz odporne na zagrożenia naturalne (silny wiatr, powódź) lub nienaturalne (ataki terrorystyczne, błędy ludzkie).

Zagrożenia związane z infrastrukturami krytycznymi można zaklasyfikować w trzech głównych kategoriach (Robles, Choi, Cho, Kim, Park, i Lee, 2008, ss. 17-22).

Należą do nich:

- Zagrożenia naturalne – spowodowane zjawiskami naturalnymi, bez bezpośredniego udziału człowieka.
- Zagrożenia spowodowane działalnością człowieka – mogące być zarówno efektem błędu ludzkiego, jak i celowych działań (np. działania terrorystyczne, których celem są elementy infrastruktury krytycznej, włączając w to cyber ataki i cyber terroryzm).
- Zagrożenia wynikające z przypadkowych awarii technicznych, lub niedoskonałości technologii.

W niniejszym artykule poruszone zostaną m.in. następujące zagadnienia dot. niezawodności oraz bezpieczeństwa infrastruktur krytycznych:

- Zagrożenia dla infrastruktury krytycznej (naturalne, cybernetyczne);
- Prognozowanie i symulacja skutków wystąpienia zagrożeń naturalnych i nienaturalnych;
- Pozyskiwanie oraz współdzielenie informacji między operatorami infrastruktur krytycznych;
- Współoddziaływanie infrastruktur krytycznych na siebie (tzw. efekty kaskadowe);
- Systemy wspomagania decyzji w zakresie ochrony infrastruktur krytycznych;
- Systemy analizy konsekwencji podejmowanych decyzji.

Wymienione aspekty poruszane są w realizowanym aktualnie projekcie badawczym 7 Programu Ramowego pt. CIPRNet (*Critical Infrastructure Preparedness and Resilience Research Network*) [www.ciprnet.eu], w którym partnerem jest UTP Bydgoszcz. Projekt CIPRNet rozpoczął się w marcu 2013 roku i koordynowany jest przez Fraunhofer Gesellschaft zur Förderung angewandter Forschung e. V.

ZAGROŻENIA DLA INFRASTRUKTURY KRYTYCZNEJ

W niniejszej sekcji opisane zostały główne typy zagrożeń dla elementów infrastruktury krytycznej. Każde zmaterializowane zagrożenie, powodujące zniszczenie lub ograniczenie funkcjonalności danego elementu infrastruktury krytycznej nie pozostaje bez wpływu na społeczeństwo (zgodnie z definicją IK).

Zagrożenia naturalne

Dwa główne źródła zagrożeń naturalnych to zjawiska hydrologiczno-meteorologiczne oraz zjawiska geologiczne. Do zjawisk hydrologiczno-meteorologicznych zaliczyć możena:

- Powodzie i osuwiska związane z wysokim stanem rzek, spowodowane długotrwałymi opadami.
- Cyklony tropikalne, fale sztormowe, porywisty wiatr, burze (grad, śnieżyce, itp.), silne wyładowania atmosferyczne.
- Długotrwałe susze, pożary, skrajnie wysokie/niskie temperatury powietrza,
- Lawiny śnieżne.

Zjawiska geologiczne, które mogą zakłócić działanie infrastruktury krytycznej lub całkowicie ją zniszczyć to przede wszystkim:

- Trzęsienia ziemi i ewentualnie towarzyszące im fale tsunami,
- Aktywność wulkanów,
- Inne zjawiska geologiczne, takie jak zapadanie się gruntów, upłynnianie gruntów czy ruchy mas skalnych.

Ponadto, niezależnie od przyczyny awarii danej infrastruktury, jej wpływ w mniejszym lub większym stopniu odczuwalny jest również dla prawidłowego funkcjonowania innych, powiązanych infrastruktur. Zależność taką nazywamy „efektem kaskadowym".

Przykładami klęsk naturalnych, które miały ogromny wpływ na działanie infrastruktury krytycznej na obszarze dotkniętym klęską były powódź w Europie Środkowo-Wschodniej w 2002 roku oraz trzęsienie ziemi w Japonii w 1995 roku. w artykule (Luiijf i Klaver, 2005, s.8), przytoczone zostały przykłady opisujące przypadki niedostępności infrastruktury krytycznej na skutek powodzi na rzekach Łaba i Dunaj. Zwrócono przy tym uwagę na brak wcześniejszej symulacji efektów takiej powodzi dla działania elementów infrastruktury takich jak linie telefoniczne, szpitale, kluczowe mosty, itp., a także na brak przygotowania (i planowania) do działań mających na celu minimalizację wpływu zaistniałych uszkodzeń na społeczeństwo.

Trzęsienie ziemi w okolicach Kobe, w 1995 roku również pokazało

podatność infrastruktury krytycznej na zagrożenia naturalne. w efekcie trzęsienia ziemi zniszczona została większość infrastruktury drogowej oraz kolejowej na obszarze dotkniętym klęską, a także port morski w Kobe. Oprócz oczywistego wpływu na lokalne społeczeństwo, zniszczenia infrastruktury krytycznej miały negatywny wpływ na przebieg akcji ratunkowych (znacząco utrudniony dostęp do szpitali), oraz były przyczyną ogromnych strat finansowych (Risk Management Solutions, 2005). Przypadek Kobe, a szczególnie wpływ zniszczeń infrastruktury drogowej na działanie szpitali (ograniczone możliwości zaopatrzenia, przyjmowania rannych, itd.) może posłużyć jako przykład „awarii kaskadowych".

W kontekście Polski, najbardziej charakterystycznymi zjawiskami, które regularnie powodują zniszczenia elementów infrastruktury krytycznej są powodzie, szczególnie dotykające Polskę południową i południowo-zachodnią. Najbardziej dramatyczny przebieg miała powódź w roku 1997, która dotknęła głównie tereny obecnych województw śląskiego, opolskiego i dolnośląskiego, choć jej wpływ można było zaobserwować praktycznie na terenie całego kraju. w wyniku powodzi, zwanej również „powodzią tysiąclecia", uszkodzone zostały 843 szkoły, z których 100 uległo całkowitemu zniszczeniu, 4000 mostów, 14 400 km dróg, 2000 km torów kolejowych oraz 613 km wałów przeciwpowodziowych (Śląski Urząd Wojewódzki w Katowicach, 2012).

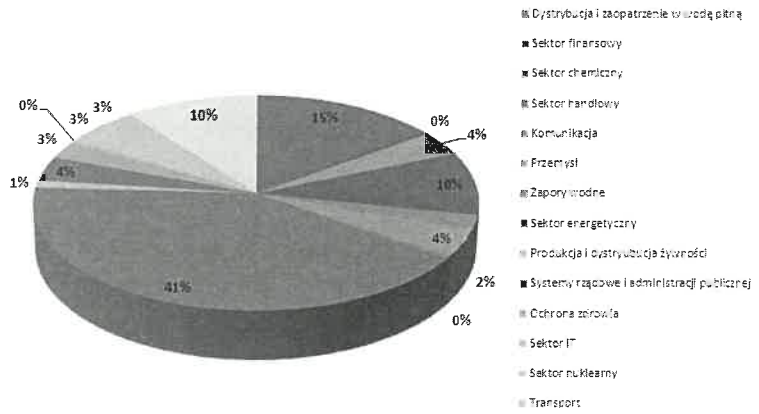
Zagrożenia cybernetyczne i aspekty cyber bezpieczeństwa w kontekście infrastruktur krytycznych

Zarówno sam termin "cyber bezpieczeństwo", jak i mnożące się przypadki cyber ataków wymierzonych w różne cele znane są od wielu lat. Rola cyber bezpieczeństwa wzrasta wraz z rozwojem technologii i usług informatycznych. Jednakże sposób w jaki cyber bezpieczeństwo postrzegane jest przez międzynarodową społeczność drastycznie zmienił się w 2007 roku, kiedy na skutek zmasowanego ataku wymierzonego w Estonię wyłączone zostały serwery oraz strony WWW agend rządowych oraz organizacji będących operatorami infrastruktury krytycznej. w krytycznym momencie nieosiągalne były usługi telefonii mobilnej oraz sektora bankowego (Iasiello, 2013, s.1 i 18; Kozik i Choraś, 2013).

Ponadto, doświadczenia ostatnich lat pokazują jednoznacznie trend dotyczący wyboru celów takich ataków – coraz większą uwagę atakujących

zdobywają systemy kontroli przebiegu procesów technologicznych lub produkcyjnych (np. SCADA, ang. *Supervisory Control And Data Acquisition*). Obserwuje się coraz większą ilość incydentów dot. bezpieczeństwa, związanych z takimi systemami. Fakt ten jest przyczyną coraz bardziej poważnego traktowania bezpieczeństwa infrastruktury krytycznej przez rządy państw oraz organizacje międzynarodowe, w wyniku czego zaobserwować można nowelizację strategii dotyczących bezpieczeństwa cybernetycznego krajów oraz coraz większą rolę jednostek (o różnym charakterze i zasięgu geograficznym) zwanych zespołami ds. reagowania na przypadki naruszenia bezpieczeństwa teleinformatycznego (CERT – z ang. *Computer Emergency Response Team).* Jednym z pierwszych takich zespołów zorientowanych na przeciwdziałanie atakom wymierzonym w infrastruktury krytyczne był amerykański ICS-CERT (*Industrial Control Systems Cyber Emergency Response Team*) założony w 2009 roku [9]. Celem działania tej organizacji jest minimalizacja wpływu cyber incydentów i ataków na działanie infrastruktury krytycznej, głównie poprzez monitorowanie oraz publikowanie informacji o podatnościach jej elementów. w corocznym raporcie (http://ics-cert.us-cert.gov/), opublikowanym w 2012 roku, ICS-CERT raportował 198 cyber incydentów zgłoszonych przez właścicieli zasobów używanych jako elementy infrastruktury krytycznej. Około 41% zgłoszonych incydentów miało miejsce w sektorze energetycznym, podczas gdy drugim najczęściej atakowanym obszarem był sektor odpowiedzialny za uzdatnianie oraz dystrybucję wody (ok. 15% zgłoszonych incydentów). Należy wspomnieć że ok. 3% incydentów uwzględnionych w raporcie dotyczyło organizacji działających w sektorze nuklearnym, a głównym celem atakujących była sieć informatyczna należąca do organizacji. Ponadto, ICS-CERT otrzymał zgłoszenia dotyczące 7 incydentów z sektora chemicznego, 5 związanych ze służbą zdrowia i transportem oraz 2 związanych z procesem dostarczania żywności. Różnorodność celów ataków cybernetycznych na infrastrukturę krytyczną obrazuje rys. 1.

Rysunek 1. Cele ataków cybernetycznych na infrastrukturę krytyczną [http://ics-cert.us-cert.gov/].



Projekt FP7 CIPRNet

W marcu 2013 roku rozpoczął się projekt CIPRNet (*Critical Infrastructure Preparedness and Resilience Research Network*), współfinansowany przez Komisję Europejską w ramach Siódmego Programu Ramowego (FP7) (www.ciprnet.eu).

Prace w projekcie CIPRNet prowadzone są w trzech płaszczyznach:

- Część niebadawcza – stworzenie „sieci doskonałości", wymiana doświadczeń,
- Działania badawcze:
  - System wsparcia decyzji wraz z analizą konsekwencji,
  - Symulacje „what-if",
  - Aspekty bezpieczeństwa w „sieciach następnej generacji" (ang. *Next Generation Infrastructures*),
- Działania integracyjno-organizacyjne:
  - Integracja zasobów oraz wypracowanych w projekcie rozwiązań – VCCC (*Virtual Centre of Competence and expertise in CIP),*
  - Stworzenie fundamentów pod Europejskie Centrum Symulacji i Analizy w obszarze CIP (EISAC - *European Infrastructures*

Simulation and Analysis).

Nadrzędnym celem projektu CIPRNet jest stworzenie tzw. „sieci doskonałości" zrzeszającej ekspertów oraz zasoby z zakresu ochrony infrastruktur krytycznych (część niebadawcza projektu). Odbiorcami sieci doskonałości będą przede wszystkim europejskie i krajowe centra zarządzania kryzysowego, organy regulujące oraz ustawodawcze w dziedzinie infrastruktury krytycznej, instytucje badawczo-naukowe, sektor prywatny, oraz pośrednio społeczeństwa europejskich krajów (Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS, 2013).

Kolejnym celem działań w płaszczyźnie niebadawczej jest wzmocnienie oraz uporządkowanie obszaru badań i rozwoju w zakresie CIP poprzez stworzenie warunków do współdzielenia wiedzy oraz doświadczeń pomiędzy ekspertami zaangażowanymi w CIP. Wspomniana wcześniej „sieć doskonałości" CIPRNet będzie mieć znaczący wpływ na ustanowienie społeczności ekspertów, integrację zasobów oraz ułatwienie kooperacji pomiędzy naukowcami, ekspertami oraz użytkownikami infrastruktur krytycznych.

Biorąc pod uwagę część badawczą projektu, skupiającą się głównie na modelowaniu i symulacjach na potrzeby CIP, konsorcjum CIPRNet postawiło sobie za cel wsparcie organizacji zarządzających kryzysami i organizacji rządowych poprzez stworzenie innowacyjnych funkcjonalności w zakresie wsparcia decyzji. Dodatkowo w ramach działań badawczych, projekt CIPRNet wypracuje rozwiązania wspierające projektowanie bezpiecznych rozwiązań NGI (*ang. Next Generation Infrastructures*).

Celem działań w płaszczyźnie integracyjno-organizacyjnej jest wzmocnienie odporności i niezawodności infrastruktur krytycznych. Przeprowadzone zostaną warsztaty, demonstracje oraz sesje szkoleniowe, które pozwolą na walidację usług i innowacyjnych funkcjonalności wytworzonych przez konsorcjum. z drugiej strony, działania te przyczynią się do podniesienia świadomości ekspertów w zakresie ochrony oraz bezpieczeństwa infrastruktury krytycznej.

Dodatkowo, w wyniku prac w projekcie CIPRNet powstanie VCCC - wirtualne centrum kompetencji w zakresie CIP. VCCC funkcjonować będzie jako platforma wymiany wiedzy z zakresu CIP, oferować będzie również dostęp do usług symulacji i analizy scenariuszy kryzysowych

wytworzonych w ramach projektu. Zakłada się, że VCCC będzie kolejnym krokiem rozwoju europejskiego centrum symulacji i analizy infrastruktur – EISAC.

Metody podnoszenia niezawodności infrastruktur krytycznych

Podczas gdy świadomość roli infrastruktury krytycznej dla funkcjonowania państwa i społeczeństwa oraz zagrożeń wynikających z funkcji jakiej pełnią jest coraz większa, zrozumienie złożoności powiązań pomiędzy różnymi infrastrukturami wciąż jest niewystarczające. Analiza zagrożeń powinna być zatem wsparta poprzez szerokie zastosowanie narzędzi symulacyjnych i analitycznych. Jednakże symulowanie złożonych zależności pomiędzy różnymi sektorami wymaga systematycznego podejścia, zaawansowanych technik modelowania i standardów, czego obecnie brakuje. Aktualnie, trudno oszacować wpływ awarii danej infrastruktury krytycznej (np. wyłączenie jednego elementu w skutek błędu ludzkiego, czy też ataku terrorystycznego) na sektory powiązane z nim. Inaczej mówiąc, nie istnieją efektywne metody modelowania i symulacji złożonych scenariuszy kryzysowych, które są w stanie dostarczyć informacji na temat tzw. „efektu kaskadowego" spowodowanego np. wyłączeniem jednego z elementów infrastruktury energetycznej. Co za tym idzie, trudno również estymować wpływ takiej awarii na bezpieczeństwo całych regionów czy też krajów. Dlatego też, jest to jedno z wyzwań projektu CIPRNet.

Narzędzia zwiększające świadomość sytuacyjną i wspierające decyzje operatorów infrastruktur krytycznych

Systemy wsparcia decyzji (DSS – *Decision Support Systems*) to narzędzia informatyczne wspierające operatorów w procesie podejmowania decyzji i zwiększające ich świadomość aktualnej sytuacji. Systemy takie używane są również w ramach ochrony infrastruktury krytycznej oraz zapewnienia bezpieczeństwa procesów technologicznych w przemyśle.

W 1987 roku firma Texas Instruments opracowała system GADS (*Gate Assignment Display System*) oferujący wsparcie decyzji dla amerykańskich linii lotniczych (United Airlines). w rezultacie użytkowania systemu przez obsługę i operatorów na amerykańskich lotniskach znacząco zredukowano opóźnienia lotów.

Innymi przykładami sektorów, w których systemy DSS są z powodzeniem używane są bankowość (systemy eksperckie służące do obsługi i zarządzania kredytami) oraz sektor hydrologii. Za przykład może posłużyć tu system wsparcia decyzji w procesie zarządzania ryzykiem wystąpienia powodzi na rzece Łaba, opracowany przez niemiecki instytut hydrologii (BfG – *Federal Institute of Hydrology*). Użycie systemu podczas powodzi latem 2002 roku zademonstrowało nie tylko efektywność narzędzi wspomagania ludzkich decyzji w zarządzaniu kryzysowym, ale przede wszystkim uświadomiło potrzebę rozwoju takich rozwiązań w świetle realnych zagrożeń.

Systemy DSS z powodzeniem wykorzystywane są również w innych sektorach związanych z infrastrukturą krytyczną, w szczególności w sektorze energetycznym (Xiao-Feng, Yu-Jiong, i Kun, 2008), nuklearnym (Lee, Mo, i Seong, 2007), nadzorowaniu procesu uzdatniania wody (Bo-Ping, Guo-xi, & Shi-yu, 2008) czy zapobieganiu wycieków ropy naftowej (Xie, Wang, i Bian, 2008). Wszystkie systemy opisywane w powyższych źródłach są skonfigurowane i dostosowane do potrzeb i specyfiki danego sektora (danego elementu infrastruktury krytycznej). Najczęściej wykorzystują one do wnioskowania metod statystycznych takich jak sieci Bayesa i ukryte Modele Markowa (HMM), rzadziej wykorzystywany jest opis ontologiczny.

Systemy informatyczne wykorzystywane w monitoringu elementów infrastruktury krytycznej mają na celu zwiększenie świadomości sytuacyjnej (ang. *situational awareness*) operatora nadzorującego infrastrukturę. Kluczowym problemem jest dostarczenie odpowiedniej informacji w odpowiednim czasie (najczęściej odpowiednio szybko), ale także przedstawienie informacji w zrozumiały dla operatora sposób. Zarządzanie oparte o systemy informatyczne pozwala na zwiększenie świadomości sytuacyjnej i szybkie reagowanie poprzez estymowanie, na podstawie obserwacji, aktualnego stanu infrastruktury krytyczne (Choraś, Renk, Kozik, i Hołubowicz, 2010). Należy przy tym zaznaczyć, że narzędzia służące do monitoringu stanu infrastruktury krytycznej będące aktualnie w użyciu, nie są zaprojektowane w sposób umożliwiający operatorowi całkowity ogląd sytuacji i pełną jej świadomość. Zazwyczaj rozwiązania takie musza być w znacznej mierze wsparte doświadczeniem operatora i oferują dostęp jedynie do nieprzetworzonych danych, wykorzystując zazwyczaj tabularyczny sposób ich prezentacji. Często ilość takich danych, sposób ich wizualizacji oraz złożoność zależności pomiędzy nimi jest przytłaczająca dla operatora, obniżając nie tylko możliwości ich analizy, ale również zdolność do podejmowania decyzji dotyczących infrastruktury w czasie rzeczywistym.

Jako przykład może posłużyć tu sektor energetyczny, w którym zaobserwować można ostatnio zwiększone nakłady i inwestycje w rozwój sieci energetycznych. Jest to podyktowane faktem, iż większość aktualnie istniejących sieci dystrybucyjnych nie była tworzona z myślą o zapewnieniu maksymalnej efektywności. Dodatkowo ze wzrostem wymagań na monitorowanie i kontrolowanie systemów dystrybucyjnych powstała wizja nowej, zintegrowanej i inteligentnej sieci energetycznej, czerpiącej korzyści z wymiany informacji pomiędzy jej rozproszonymi (na dużych obszarach) elementami.

Narzędzia pozyskiwania i współdzielenia informacji w zakresie bezpieczeństwa infrastruktury krytycznej

Jak pokazują dotychczasowe wyniki prac w projekcie CIPRNet (dokument D5.1: „*Formal Requirements Specification*"), przedstawiciele służb i organizacji działających w zakresie CIP oraz docelowi użytkownicy systemu wsparcia decyzji CIPRNet, jednoznacznie wskazują na potrzebę współdzielenia informacji w zarządzaniu kryzysowym. Jednocześnie wskazują na pewne problemy związane z pozyskiwaniem i współdzieleniem informacji zarówno podczas kryzysu jak i w fazie przygotowania do niego. Należy tu zauważyć że użytkownicy i interesariusze projektu CIPRNet obejmują społeczność międzynarodową (pochodzą z różnych krajów Europy) oraz są przedstawicielami szerokiego spektrum organizacji – operatorzy infrastruktur krytycznych, agencje rządowe zajmujące się zarządzaniem kryzysowym, obszar naukowo-badawczy, itd.

Jako jeden z głównych problemów występujących w planowaniu działań podczas kryzysu, wskazują oni na trudność z dostępem do informacji, które są podstawą do budowy całościowego obrazu sytuacji kryzysowej. Innymi słowami, użytkownicy wskazują na fakt istnienia informacji, które byłyby idealnym dopełnieniem aktualnej świadomości kryzysu, zwracając jednocześnie uwagę na problem z efektywnym wykorzystaniem tychże informacji.

Kolejnym wyzwaniem, jednakże cały czas związanym z problemem współdzielenia informacji, jest zapewnienie wymiany informacji

poprzez zintegrowanie dwóch lub więcej systemów wpierających działania, a należących przy tym do różnych organizacji. Wspomniana niekompatybilność zauważalna jest nie tylko podczas kryzysu i w ramach reakcji na niego, ale również podczas planowania czy symulacji możliwych efektów i działań będących reakcją na kryzys. Opisywanemu problemowi towarzyszy brak standaryzacji w aspekcie interfejsów, modeli i metod modelowania, co ewidentnie pogłębia problem oraz hamuje możliwości kooperacji różnych służb i organizacji.

Jednocześnie, zauważyć można (co również potwierdzają użytkownicy końcowi biorący udział w projekcie CIPRNet) brak współpracy i możliwości pozyskiwania oraz współdzielenia zasobów na linii sektor prywatny – sektor publiczny, oraz ograniczone możliwości współpracy międzynarodowej. Jak wiadomo, kryzys związany z infrastrukturą krytyczną często wykracza poza jeden system, organizację czy sektor, a w przypadku klęsk żywiołowych o wielkiej skali – również poza granice państwowe, dlatego współdzielenie informacji jest jednym z kluczy do efektywnego wykorzystania wszystkich istniejących zasobów.

Analiza konsekwencji, analiza „what-if" oraz bezpieczeństwo rozwiązań typu NGI

Jednym z głównych wyzwań badawczych projektu CIPRNet jest stworzenie zaawansowanego systemu wsparcia decyzji (DSS), oferującego innowacyjne usługi dla szeregu użytkowników końcowych zaangażowanych w zarządzanie kryzysowe oraz ochronę infrastruktury krytycznej w trakcie kryzysu. System DSS przede wszystkim ma za zadanie rozwiązanie problemu oceny zagrożeń, na które podatne są poszczególne elementy infrastruktury krytycznej, a także oceny wpływu tych zagrożeń na infrastrukturę (np. ograniczenie poszczególnych funkcjonalności) i na społeczeństwo.

Jednym z produktów projektu CIPRNet będzie system wsparcia decyzji z analizą konsekwencji. Analiza konsekwencji odbywać będzie się w czasie rzeczywistym lub zbliżonym do rzeczywistego. Oprócz modeli i danych historycznych do analizy konsekwencji posłużą także rzeczywiste dane gromadzone z sensorów na obszarze, w którym zaistniała sytuacja kryzysowa. w szczególności wykorzystywane będą dane z sensorów sejsmologicznych oraz hydro-meteorologicznych (np. obserwacja poziomu rzek). Głównym zadaniem analizy konsekwencji będzie

rozszerzenie świadomości sytuacyjnej operatora o informacje dotyczące wpływu danego zagrożenia na społeczeństwo.

Wykorzystane techniki symulacyjne pozwolą także na zasymulowanie oraz analizę różnych, możliwych przebiegów wydarzeń dotyczących sytuacji kryzysowej związanej z infrastrukturą krytyczną (analiza „what-if"). Wartością dodaną tej usługi będzie możliwość weryfikacji istniejących podatności systemów w różnych przypadkach zaistniałego kryzysu.

Analiza i symulacje „what-if" działać będą w trybie *„offline"*, nie wykorzystują więc danych w czasie rzeczywistym (np. danych sensorycznych), a dane statystyczne (np. model terenu, dane historyczne, itp.).

Ponadto, konsorcjum CIPRNet skupi się na projektowaniu bezpiecznych Infrastruktur Następnej Generacji (NGI – *Next Generation Infrastructures*). Rozwój Infrastruktur Następnej Generacji (NGI) jest naturalnym trendem ewolucji infrastruktur krytycznych (np. *Smart Grids* – inteligentne sieci energetyczne). Działania w tej części projektu skupione będą na czterech płaszczyznach, obejmujących: technologie, aspekty bezpieczeństwa, aspekty prawne i aspekty organizacyjne.

Wnioski

W artykule przedstawione zostały podstawowe aspekty dotyczące zagrożeń oraz ochrony infrastruktury krytycznej (CIP) w kontekście roli jaką infrastruktura krytyczna odgrywa dla bezpieczeństwa strukturalnego państwa. Jednym z opisanych aspektów jest klasyfikacja zagrożeń. w sekcji drugiej podzielono je na fizyczne zagrożenia naturalne oraz zagrożenia cybernetyczne, które przy obecnym tempie rozwoju sieci teleinformatycznych wymagają coraz większej uwagi rozważając bezpieczeństwo infrastruktury krytycznej. Pokazują to przykłady ataków cybernetycznych na elementy infrastruktury, które miały miejsce na przestrzeni ostatnich lat. Wpływ przytoczonych incydentów na społeczeństwo oraz na stabilność atakowanych krajów pokazuje jak istotnym elementem bezpieczeństwa strukturalnego kraju jest ochrona infrastruktury krytycznej oraz minimalizacja zagrożeń dotyczących tej infrastruktury (włączając w to zagrożenia cybernetyczne).

W dalszej części niniejszego artykułu zaproponowane zostały metody podnoszenia niezawodności infrastruktury krytycznej, które znacząco przyczynią się do wzrostu bezpieczeństwa strukturalnego krajów.

Należą do nich przede wszystkim systemy wsparcia decyzji zwiększające świadomość sytuacyjną operatów podczas kryzysu oraz narzędzia pozyskiwania i współdzielenia informacji w różnych fazach ochrony infrastruktury krytycznej (tj. zarówno w fazie przygotowania kryzysu, jak i po zaistnieniu incydentu). Istotnym elementem ochrony infrastruktury krytycznej są także modelowanie oraz symulacje prawdopodobnych scenariuszy kryzysowych wraz z analizą i oceną wpływu analizowanego kryzysu na bezpieczeństwo kraju (np. wpływ na społeczeństwo lub wpływ na ekonomię danego kraju).

W artykule przedstawiono również projekt CIPRNet, współfinansowany w ramach europejskiego Siódmego Programu Ramowego (FP7), a także rozwiązania i podejście wypracowane w projekcie, zorientowane na podniesienie niezawodności infrastruktury krytycznej.

Podziękowania (Acknowledgment)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 312450. The European Commission's support is gratefully acknowledged.

The work is also funded by Polish National Centre for Research and Development (NCBiR) from funds for science in the years 2013-2016 allocated for the international projects.

References

Bo-ping, Z., Guo-xi, W., & Shi-yu, S., "Research on Decision Support System of Water Pollution Control Based On Immune Agent," In Proc. of International Symposium on Computer Science and Computational Technology, ISCSCT, vol.1, 2008.

Choraś M., Renk R., Kozik R., Hołubowicz W., „Inteligentne sieci energetyczne: aktualny stan i trendy rozwojowe," SIWE'10, Wisła, 2010

Dyrektywa Rady 2008/114/WE, z dnia 8 grudnia 2008 r,. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, Dziennik Urzędowy Unii Europejskiej, 23.12.2008

Fraunhofer Institute for Intelligent Analysis and Information Systems IAIS, "EU Network of Excellence for more resilient Critical Infrastructures", FP7 CIPRNet project Press Release, 2013

Iasiello, E., "Cyber attack: a dull tool to shape foreign policy," Cyber Conflict (CyCon), 2013 5th International Conference on , vol., no., pp.1,18, 2013

Kozik, R.; Choraś M., "Current Cyber Security Threats and Challenges in Critical Infrastructures Protection", The Second International Conference on Informatics & Applications, ICIA, Łódź 2013

Lee, S. J., Mo, K., & Seong, P. H., "Development of an Integrated Decision Support System to Aid the Cognitive Activities of Operators in Main Control Rooms of Nuclear Power Plants," In Proc. of IEEE Symposium on Computational Intelligence in Multicriteria Decision Making (MCDM), 2007.

Luiijf, E.A.M., Klaver, M. H A, "Critical infrastructure awareness required by civil emergency planning," Critical Infrastructure Protection, First IEEE International Workshop on , vol., no., pp.8 pp., 2005

Risk Management Solutions, Inc. 1995 Kobe Earthquake 10-year Retrospective. Newark, CA., 2005

Robles, R. J., Choi, M. K., Cho, E. S., Kim, S. S., Park, G. C., & Lee, J., "Common threats and vulnerabilities of critical infrastructures,". International Journal of Control and Automation (1), 17-22, 2008

Xiao-Feng, D., Yu-Jiong, G., & Kun, Y., "Study on intelligent maintenance decision support system using for power plant equipment." In Automation and Logistics, ICAL 2008.

Xie, L., Wang, Z., & Bian, L., "The Research of Oiled Flood Precaution Decision Support System," In Proc. of International Seminar on Business and Information Management, ISBIM '08, vol.2, December 2008.

Zagrożenia w województwie śląskim z uwzględnieniem zagrożeń naturalnych występujących w kopalniach, Śląski Urząd Wojewódzki w Katowicach, 2012

Źródła internetowe:

CIPRNet, www.ciprnet.eICS-CERT.

http://ics-cert.us-cert.gov/