FOLIA 151

Annales Universitatis Paedagogicae Cracoviensis

Studia Politologica XII (2014)

Joanna Świątkowska

Współczesne wyzwania w zakresie ochrony infrastruktury krytycznej

Wprowadzenie

Sprawnie działająca i bezpieczna infrastruktura w coraz większym stopniu warunkuje funkcjonowanie, dobrobyt i możliwość rozwoju współczesnych państw oraz społeczeństw. W skomplikowanym układzie infrastruktur, na których opiera się większość elementów codziennej egzystencji, znajdują się takie, które spełniają szczególnie ważną rolę i których ewentualna niesprawność lub zniszczenie może mieć bardzo poważne konsekwencje społeczne. Te wyjątkowo istotne infrastruktury nazwane są infrastrukturą krytyczną (IK). Niezakłócone funkcjonowanie IK staje się w coraz większym stopniu ważne nie tylko z punktu widzenia dobrobytu i komfortu, ale także z punktu widzenia bezpieczeństwa. Infrastruktura usprawnia życie obywateli, gwarantuje rozwój państwa, ale także podwyższa poziom wrażliwości społecznej[1]. W wyniku rozwoju cywilizacyjnego, industrializacji oraz postępu technologicznego uzależnienie funkcjonowania wzrastającej ilości aspektów życia od coraz bardziej rozbudowanych infrastruktur jest nieuniknione, trend ten z pewnością będzie się pogłębiał. Państwa stoją zatem przed zadaniem wprowadzania rozwiązań, które zagwarantują bezpieczeństwo funkcjonowania najważniejszych elementów infrastruktury i jednocześnie nie wpłyną hamująco na ich rozwój.

Ochrona infrastruktury krytycznej (OIK) jest szczególnym wyzwaniem w zakresie polityki bezpieczeństwa, a także bardzo interesującym zagadnieniem badawczym. Sytuacja ta jest następstwem szeregu procesów i zmian, które aktualnie zachodzą w wielu państwach, szczególnie w tych rozwiniętych, i mają na obszar OIK bardzo duży wpływ. Przykładem takiego właśnie zjawiska są postępujące procesy zmian własnościowych, wynikające z deregulacji oraz prywatyzacji wielu sektorów publicznych. W konsekwencji, znacząca liczba infrastruktur, także krytycznych, znalazła się w rękach prywatnych przedsiębiorców, co istotnie wpłynęło na moż-

[1] W. Skomra, *Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego*, Rządowe Centrum Bezpieczeństwa, http://www.powiat-wloszczowa.pl/ochrona_ludnosci/OIK_w_systemie_zarzadzania_kryzysowego.pdf, dostęp 02.02.2013.

liwości zapewniania OIK przez sektor publiczny[2]. W celu skutecznego zapewniania bezpieczeństwa IK konieczne jest zatem ścisłe współdziałanie zarówno podmiotów publicznych, jak i prywatnych. Analiza problemów i przedstawienie rekomendacji służących najlepszemu organizowaniu takiej współpracy będzie jednym z przedmiotów niniejszego artykułu. Innym procesem znacząco wpływającym na OIK jest zjawisko globalizacji. Rosnąca współzależność między podmiotami w skali międzynarodowej, także w obszarze wzajemnych połączeń infrastruktur, stwarza nowy kontekst dla działań związanych z bezpieczeństwem, poniżej przedstawione zostaną jego najważniejsze cechy.

Czym jest infrastruktura krytyczna – tradycyjne rozumienie i aktualne trendy

W tradycyjnym ujęciu IK rozumiano głównie w odniesieniu do „dróg, mostów, systemów wodnych czy też transportowych, które były strategiczne z punktu widzenia planu obronnego"[3]. OIK była rozpatrywana przede wszystkim w kontekście potencjalnego ataku przeprowadzonego przez wrogie podmioty państwowe i taki nurt dyskusji w tym obszarze utrzymywał się do zakończenia zimnej wojny. Nowa fala refleksji nad koniecznością OIK, jako zabezpieczania kluczowego elementu bezpieczeństwa narodowego, rozpoczęła się w połowie lat 90. ubiegłego stulecia[4]. Jednak prawdziwą cezurą stały się wydarzenia z 11 września 2001 roku[5]. Zmasowane ataki terrorystyczne przeprowadzone przeciwko Stanom Zjednoczonym pokazały jasno, że tradycyjne rozumienie IK oraz niebezpieczeństw jej zagrażających uległo dezaktualizacji i konieczne jest podjęcie nowych środków zapewniających jej ochronę. 11 września IK stała się celem ataków niekonwencjonalnych, a zniszczenia jakie zostały dokonane ukazały ogrom wyzwań przed jakimi stoi skuteczna obrona tego obszaru. Po tym wydarzeniu OIK stała się jednym z priorytetowych działań w coraz większej liczbie państw, a także ważnym przedmiotem rozmów i działań na poziomie międzynarodowym. Gruntownej zmianie uległ sam sposób definiowania IK i myślenia o zapewnianiu jej bezpieczeństwa. Poniżej przedstawione zostaną wybrane dominujące aktualnie trendy w obszarze tej dyskusji.

Nie istnieje jedna, powszechnie obowiązująca definicja IK. Poszczególne państwa określają ją na swój sposób, często różniący się między sobą. Ma to także odzwierciedlenie w odmiennych strategiach dotyczących OIK. Poniższy, krótki przegląd tego, jak definiowana może być IK, daje możliwość zaobserwowania ogólnego jej charakteru.

---

[2] *Protecting Critical Infrastructure in the EU. CEPS Task Force Report*, red. A. Renda, Centre for European Policy Studies 2010, s. 14.

[3] W. Wójtowicz, *Bezpieczeństwo infrastruktury krytycznej*, Ministerstwo Obrony Narodowej, Departament Polityki Obronnej, Warszawa 2006, s. 8.

[4] F. Umbach, *Critical Energy Infrastructure At Risk of Cyber Attack*, KAS International Report 9/2012, s. 38.

[5] Ibidem.

Definicja funkcjonująca w Stanach Zjednoczonych mówi, że infrastruktura krytyczna to

> systemy i obiekty, zarówno fizyczne, jak i wirtualne, na tyle kluczowe dla Stanów Zjednoczonych, że ich niesprawność lub zniszczenie miałoby destabilizujący wpływ na bezpieczeństwo, narodowe bezpieczeństwo ekonomiczne, narodową ochronę zdrowia, lub na dowolną kombinację tych elementów[6].

Brytyjska definicja mówi, że infrastruktura krytyczna składa się z

> tych obiektów, usług i systemów, które wspierają gospodarcze, polityczne i publiczne życie w Wielkiej Brytanii i których znaczenie jest na tyle istotne, że ich zniszczenie mogłoby: 1) spowodować utratę życia ludzkiego na dużą skalę, 2) mieć poważny wpływ na gospodarkę, 3) mieć inne poważne konsekwencje dla życia publicznego lub sprawić bezpośrednie trudności dla rządu[7].

Holenderskie rozumienie terminu sprowadza się do twierdzenia, że

> infrastruktura krytyczna dotyczy produktów, usług i towarzyszących im procesów, które w sytuacji zakłóceń funkcjonowania lub uszkodzeń, mogą powodować istotne kłopoty publiczne. Mogłoby się to przejawiać w ofiarach i powodować straty ekonomiczne[8].

Polska ustawa o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 mówi, że infrastruktura krytyczna to

> systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców[9].

Ustawa enumeratywnie określa te systemy. Należą do nich sytemy:

- zaopatrzenia w energię, surowce energetyczne i paliwa,
- łączności
- sieci teleinformatycznych,
- finansowe,
- zaopatrzenia w żywność
- zaopatrzenia w wodę,
- ochrony zdrowia,
- transportowe,
- ratownicze,

---

[6] *Protecting Ciritical Infrastructure...*, s. 22.

[7] Ibidem.

[8] Ibidem.

[9] Rządowe Centrum Bezpieczeństwa, *Infrastruktura Krytyczna*, http://rcb.gov.pl/?page_id=210, dostęp 02.02.2013.

- zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych[10].

W dużej mierze systemy, sektory, które wchodzą w skład IK, są podobne w poszczególnych państwach[11]. Istnieją także elementy „niecodzienne", np. w Stanach Zjednoczonych do zbioru IK zalicza się wybrane narodowe pomniki i monumenty.

W polskim prawodawstwie OIK rozumie się jako:

> wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działań i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie[12].

Eksperci podkreślają, że OIK to nie tylko działania podejmowane już w sytuacji zaistnienia kryzysu czy problemu. To całe spektrum czynności skierowanych na przeciwdziałanie zagrożeniom. Często wymienia się sześć głównych faz cyklu OIK. Składają się na nie[13]:

- **Faza 1: Analiza i ocena** – w tym elemencie identyfikuje się te elementy, obiekty, systemy, które są uznane za krytyczne. Następnie prowadzi się ocenę ich podatności na zagrożenia i określa słabe punkty, które mogą stanowić potencjalne niebezpieczeństwo. W końcu wskazuje się współzależności między danymi elementami, by wykryć możliwe powiązania. Ocena sprowadza się do określenia ewentualnego wpływu i skutków potencjalnej awarii lub zniszczenia IK.
- **Faza 2: Naprawa** – dotyczy działań prewencyjnych przed pojawieniem się problemu, tak aby uniemożliwić jego zaistnienie. W ramach tej fazy dokonuje się napraw elementów zidentyfikowanych wcześniej jako wrażliwe.
- **Faza 3: Wskaźniki i ostrzeganie** – faza ta ma miejsce przed i w trakcie incydentu, polega na monitorowaniu stanu i funkcjonowania IK i ocenianiu, czy występują czynniki, które należy raportować. Wyznaczone wskaźniki pozwalają na ocenę stanu lub tendencji jakie zachodzą w obszarze IK. Ostrzeżenie to działanie mające na celu informowanie właściwych podmiotów o możliwym niebezpieczeństwie lub już zaistniałym incydencie.
- **Faza 4: Łagodzenie** – pojawia się przed i w trakcie zdarzenia i dotyczy zastosowania wszystkich działań, które mają na celu zminimalizowanie negatywnych skutków zaistniałych zdarzeń.
- **Faza 5: Reagowanie na zdarzenie** – obejmuje wszystkie działania mające na celu wyeliminowanie przyczyny zdarzenia.
- **Faza 6: Rekonstrukcja** – sprowadza się do odbudowy zdolności IK i jej elementów.

---

[10] Ibidem.

[11] *Protecting Ciritical Infrastructure...*, s. 23.

[12] Rządowe Centrum Bezpieczeństwa, *Infrastruktura*…

[13] *Protecting Ciritical Infrastructure...*, s. 34.

Ryc. 1. Fazy cyklu OIK

Źródło: *Protecting Critical Infrastructure...*, s. 34

Aktualne trendy w obszarze infrastruktury krytycznej

Analizując definicje IK w poszczególnych państwach oraz polityki i strategie związane z zapewnianiem jej ochrony, można wyróżnić kilka ogólnych trendów, które są aktualnie dominujące.

Jednym z nich jest odejście od obiektowego rozumienia IK i ewolucja w stronę definicji systemowej. W przeważającej mierze IK nie jest traktowana jako pojedyncze, odseparowane elementy, ale jako sieć skomplikowanych, wzajemnie połączonych systemów. W konsekwencji, OIK koncentruje się nie tylko na bezpieczeństwie samych obiektów, ale na zapewnieniu ciągłości usług i funkcjonalności jakie dana infrastruktura dostarcza[14]. Taka zmiana definiowania i rozumienia niesie za sobą zmianę spojrzenia na zagrożenia. Aby zapewnić funkcjonalność IK, nie możemy chronić jej tylko przed takimi niebezpieczeństwami, które są zagrożeniem dla samego obiektu, np. przed awarią prądu. Konieczne jest całościowe spojrzenie na problem. OIK musi wtedy brać pod uwagę szerokie spektrum niebezpieczeństw, zagrażających nie tylko bezpieczeństwu obiektu jako takiego, ale także wszystkim elementom składowym, które zapewniają jego funkcjonowanie. Przykładem takich zagrożeń jest np. epidemia lub wrogie działania ludzi z wewnątrz. Systemowe traktowanie IK prowadzi zatem do stosowania całościowego podejścia do zagrożeń (ang. *all-hazard approach*). Niebezpieczeństwa dla IK są bardzo zróżnicowane, nieprzewidywalne i pochodzą z wielu źródeł zarówno konwencjonalnych, jak i niekonwencjonalnych. Trzeba mieć na uwadze zarówno zagrożenia spowodowane przez człowieka (np. terroryzm), jak i niebezpieczeństwa będące wynikiem sytuacji naturalnych (np. powódź)[15].

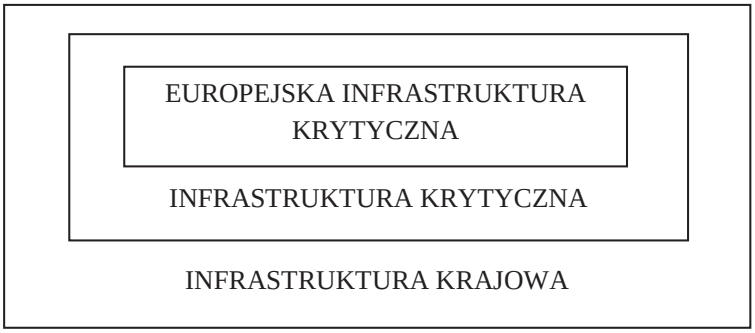
Jedną z cech charakterystycznych dla IK jest jej wzrastająca współzależność w odniesieniu do innych infrastruktur. Wynikiem tego procesu jest sytuacja wzmożonej wrażliwości. W konsekwencji zniszczenia jednej infrastruktury występuje duże prawdopodobieństwo uszkodzenia połączonej z nią innej infrastruktury, co dalej doprowadzić może do „efektu domina". Postępujący proces występowania i pogłębiania się współzależności między infrastrukturami występuje zarówno wewnątrz państw, jak i na poziomie międzynarodowym. Zjawisko to nabrało znaczenia i będzie się rozwijało szczególnie w obliczu postępującego procesu globalizacji. IK w jednym kraju w coraz większym stopniu staje się uzależniona od prawidło-

[14] W. Skomra, *Ochrona infrastruktury...*, s. 3.

[15] *Protecting Ciritical Infrastructure...*, s. 4.

wego funkcjonowania IK w innym państwie. Problem, który pojawi się w jednym miejscu, bardzo szybko może mieć konsekwencje dla innego podmiotu. Można zatem powiedzieć, że IK połączona z innymi infrastrukturami krajowymi oraz tymi w innych państwach tworzy wielowymiarową konstrukcję, a w zapewnianie jej bezpieczeństwa zaangażowane muszą zostać coraz to nowe podmioty, także o charakterze ponadnarodowym. Przykładem może być tutaj Unia Europejska i jej inicjatywa Europejskiego Programu Ochrony Infrastruktury Krytycznej. Kluczowym komponentem tego działania jest Dyrektywa Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony. „Europejska infrastruktura krytyczna" lub EIK oznacza infrastrukturę krytyczną zlokalizowaną na terytorium państw członkowskich, której zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie. To, czy wpływ jest istotny, ocenia się w odniesieniu do kryteriów przekrojowych. Obejmuje to skutki wynikające z międzysektorowych współzależności z innymi rodzajami infrastruktury[16]. Za wyznaczanie i ochronę EIK odpowiedzialne są państwa członkowskie, co pokazuje, że OIK zyskuje nowy wymiar aktywności, uwzględniający także konieczność nawiązywania międzynarodowej współpracy i ścisłych partnerstw.

Zjawisko współzależności może być także zauważone na wewnętrznym poziomie. IK jest częścią całościowej infrastruktury państwowej. Uznaje się, że ma ona wyjątkowo istotne znaczenie w porównaniu z innymi infrastrukturami i często jest chroniona w bardziej rygorystyczny sposób. Jednak oba rodzaje infrastruktur istnieją nie obok siebie w separacji, ale często także jako połączone systemy. Nie można zatem mieć pewności, że incydent jaki dotknie infrastrukturę nie będzie miał konsekwencji dla IK. Sprawia to kolejną trudność w zapewnianiu OIK.



Ryc. 2. Współzależność infrastruktury krytycznej

Źródło: Opracowanie własne

[16] Dyrektywa Rady 2008/114/WE, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:PL:PDF, dostęp 02.02.2013.

Ostatnim ze wskazanych tutaj trendów i wyzwań w zakresie OIK jest wzrastająca rola technologii teleinformatycznych, które coraz częściej warunkują sprawne funkcjonowanie infrastruktur. Uzależnienie IK od tych technologii otworzyło cały nowy katalog zagrożeń dla jej bezpieczeństwa i w jeszcze większym stopniu uwydatniło zjawisko współzależności.

Współpraca prywatno-publiczna w OIK

W wyniku procesów liberalizacji oraz deregulacji rynków duża część infrastruktury, także określanej jako krytyczna, znalazła się w rękach podmiotów prywatnych. Doprowadziło to do znaczących zmian w sposobie zapewniania OIK. Przede wszystkim podmioty publiczne nie są już w stanie samodzielnie prowadzić działań zmierzających do OIK i muszą w dużej mierze polegać na działaniach podmiotów prywatnych[17]. Eksperci wskazują, że to właśnie współpraca prywatno-publiczna jest aktualnie jednym z podstawowych i niezbędnych komponentów skutecznej OIK. Współpraca tego typu będzie w niniejszym artykule egzemplifikowana za pomocą partnerstwa publiczno-prywatnego (PPP) rozumianego jako „zorganizowane partnerstwo między publicznymi a prywatnymi podmiotami, które ustanawia wspólne obszary działania i cele i używa zdefiniowanych ról oraz metodologii pracy w celu ich osiągnięcia"[18]. Esencją tego typu współpracy jest „uzyskanie synergii dzięki wspólnemu innowacyjnemu wykorzystaniu zasobów i zastosowaniu zarządzania wiedzą wraz z optymalnym osiągnięciem celów wszystkich zaangażowanych stron, podczas gdy cele te nie mogłyby być osiągnięte w takim samym stopniu bez zaangażowania partnerów"[19].

Warunkiem wstępnym dla podjęcia współpracy między aktorami prywatnymi i publicznymi jest sytuacja, w której podzielają oni wspólny cel[20]. W kontekście IK jest to zapewnienie jej bezpieczeństwa. O ile z punktu widzenia podmiotów publicznych priorytet zapewnienia najwyższego możliwego stopnia OIK wydaje się bezdyskusyjny, o tyle nie jest to już tak oczywiste z perspektywy podmiotów prywatnych. Partnerów dzieli tutaj często odmienny sposób percepcji hierarchii interesów. Podmioty prywatne są zorientowane przede wszystkim na zysk i to jest ich główna motywacja. Często są one w stanie zaakceptować pewien poziom ryzyka, gdyż wydatki jakie musiałyby ponieść, by osiągnąć najwyższy poziom bezpieczeństwa, są wyższe niż potencjalne straty. Z punktu widzenia bezpieczeństwa publicznego, o który muszą dbać podmioty publiczne, taki tok rozumowania jest nieakcepto-

[17] *Protecting Ciritical Infrastructure...*, 32.

[18] ENISA, *Cooperative Models for Effective Public Private Partnerships. Good Practice Guide*, 2011, s. 12, tłum. własne.

[19] M. Dunn Cavelty, M. Suter, *Public Private Partnerships are no silver bullet...*, International Journal of Critical Infrastructure Protection, Zurich 2009, doi: 10.1016/j.ijcip.2009.08.006, Center for Security Studies, s. 2.

[20] Ibidem, s. 2.

wany, a bezpieczeństwo należy traktować jako jedno z najważniejszych zadań bez wyjątku. Jest zatem bardzo istotne, aby uzmysławiać podmiotom prywatnym, jak bardzo istotną rolę społeczną pełnią i że bezpieczeństwo jest wspólną odpowiedzialnością jaką dzielą z podmiotami z sektora publicznego. Należy także budować głębokie wzajemne zrozumienie dla często odmiennej percepcji interesów.

Argumentem, który zwiększa szansę na przekonanie podmiotów prywatnych do większego zaangażowania w zapewnianie bezpieczeństwa, jest koncepcja odwróconego efektu „jazdy na gapę". Według tej koncepcji infrastruktura stanowi niejako system naczyń połączonych, w którym bardzo często awaria lub zniszczenie jednego elementu wpływa na funkcjonowanie kolejnego. Istnieje sytuacja, w której podmioty nie inwestują w działania służące podnoszeniu bezpieczeństwa infrastruktury, ale są beneficjentem działań podejmowanych w tym zakresie przez inne podmioty. Mogą one wtedy uznać, ze nie warto angażować wielu środków w obronę, gdyż zrobią to za nich inni. Jednak sytuacja ta może mieć odwrotne skutki. Wystarczy, że jeden element, będący „słabym ogniwem" w systemie wzajemnie połączonego organizmu, znajdzie się w niebezpieczeństwie i sytuacja ta może kosztować innych olbrzymie straty. Podmioty prywatne muszą mieć świadomość, że ich decyzje mają znaczenie nie tylko społeczne, ale także mogą okazać się dla nich samych bardzo istotne, również z punktu widzenia ich komercyjnego interesu. Z tej przyczyny należy podkreślać, że wspólne działania oraz poczucie współodpowiedzialności leży w interesie wszystkich. Sektor publiczny musi być uwrażliwiony na rynkową orientację podmiotów prywatnych i podchodzić do działań związanych z bezpieczeństwem, mając na uwadze ten właśnie aspekt. W tym kontekście należy podkreślić, że planowanie i wdrażanie wszystkich inicjatyw publiczno-prywatnych zorientowanych na OIK musi być w największym stopniu efektywne i uwzględniające konieczność dbania o ponoszone koszy.

Powody, dla których przedstawiciele sektora prywatnego i publicznego decydują się na współpracę w zakresie OIK, mogą być różne i mogą być odmienne dla obu typów podmiotów. Dla przedstawiciela sektora publicznego przyczyną może być np. uzmysłowienie sobie, że to podmioty prywatne posiadają najlepsze możliwości, narzędzia lub wiedzę ekspercką rozwiązującą dany problem. Sektor prywatny może przykładowo dostrzec, że dany problem, lub możliwość jego najlepszego rozwiązania, wykracza poza granice organizacji. Dla podmiotów prywatnych istotne może być także to, że poprzez udział we wspólnych inicjatywach z sektorem państwowym mogą one wpływać na polityki publiczne[21], mogą także w partycypacji dostrzegać źródło prestiżu. Istnieje także szereg powodów, które mogą być dostrzeżone wspólnie przez obu partnerów w takim samym stopniu. Przykłady takich wspólnych powodów to: dostrzeżenie duplikacji wysiłków na rzecz zapewniania bezpieczeństwa infrastruktury, zidentyfikowanie niewystarczającej wymiany informacji, która jest

[21] ENISA, *Cooperative Models for Effective Public Private Partnerships. Good Practice Guide*, s. 18.

konieczna do podejmowania właściwych działań[22], czy w końcu chęć osiągnięcia oszczędności kosztów, wynikająca z synergii działań.

Recepta na udane PPP

Istnieje wiele elementów jakie należy rozważyć przy projektowaniu i wdrażaniu w życie wspólnych działań prywatno-publicznych. Poniżej zaprezentowane zostaną rekomendacje oraz dobre praktyki zwiększające szansę na osiągnięcie zamierzonych efektów.

Zanim podejmie się decyzje o powołaniu do życia wspólnych inicjatyw publiczno-prywatnych należy upewnić się, że nie istnieją grupy, które już pracują nad podobnymi lub tożsamymi zagadnieniami. Problem duplikacji często zniechęca podmioty do angażowania się w pracę. Jeśli zidentyfikowano takie inicjatywy, podmiot inicjujący współpracę powinien w pierwszej kolejności rozważyć możliwość wsparcia już działających grup i wstrzymać się od powoływania do życia nowych projektów[23].

Kolejnym, a zarazem jednym z najważniejszych elementów warunkujących sprawnie funkcjonującą i spełniającą swoje zadania współpracę prywatno-publiczną, jest właściwe zidentyfikowanie problemu, który chce się rozwiązać, lub kwestii, którą chce się podjąć. Dobrze określony cel, dla którego organizuje się współpracę, w znaczący sposób ułatwia dobranie odpowiednich narzędzi prowadzących do jego osiągnięcia i właściwe zaprojektowanie całej inicjatywy[24]. Należy zatem dokonać kompleksowej analizy sytuacji wraz z rzetelną oceną potrzeb. Są trzy główne strategie inicjowania współpracy. W pierwszym scenariuszu jest ona wynikiem inicjatywy oddolnej – dana społeczność bądź podmiot prywatny rozpoznaje problem i zwraca się do podmiotu publicznego z inicjatywą rozpoczęcia wspólnych działań. Druga możliwość to odgórne inspirowanie współpracy. W takim wypadku to podmiot publiczny zaprasza sektor publiczny do współdziałania, dostrzegając, że istnieją kwestie, które winny zostać rozwiązane we współpracy. Często jest to także wynikiem odpowiednich zapisów umieszczonych w konkretnym dokumencie, obligującym sektor publiczny do zaangażowania w działanie przedstawicieli prywatnych. W końcu możliwa jest także kombinacja dwóch powyższych kategorii[25].

Kolejna korzyść, wynikająca z dobrej i precyzyjnej identyfikacji celu jaki chce się osiągnąć poprzez współpracę, to możliwość ewaluacji podjętych działań. Jest to bardzo istotne, daje bowiem szansę na ocenę wartości i użyteczności całej inicjatywy, co szczególnie dla podmiotów prywatnych ma olbrzymie znaczenie. Dzięki ewaluacji podmioty mają możliwość dostrzeżenia plusów swojego zaangażowania.

---

[22] Ibidem, s. 19.

[23] Ibidem, s. 51

[24] Ibidem, s. 17.

[25] ENISA, *Cooperative Models for Effective Public Private Partnerships. Deskop Research Report*, 2011, s. 21.

Warto podkreślić, że w trakcie trwania inicjatywy należy nieustannie zadawać sobie pytanie na temat aktualności założonych celów i zadań jakie były powodem, dla którego zawiązano współpracę. Tylko w ten sposób można zapewnić zachowanie celowości i wartości prowadzonych działań[26].

W końcu prawidłowe określenie celu determinuje także długość trwania współpracy i jej charakter. W tym kontekście możemy mówić o:

- trwałych grupach – grupy te powoływane są, aby rozwiązywać dany problem długofalowo,
- grupach roboczych – powołanych do rozwiązania konkretnej sytuacji problemowej,
- grupach szybkiego reagowania – zazwyczaj trwają bardzo krótki okres czasu, mierzony nawet w godzinach. Powoływane są, aby poradzić sobie z danym zdarzeniem lub zidentyfikowanym słabym punktem[27].

Drugą i jedną z najważniejszych rekomendacji dotyczących budowania efektywnej współpracy prywatno-publicznej jest konieczność takiego zaprojektowania działań, by aktywna partycypacja wszystkich podmiotów we wspólnych działaniach prowadziła do osiągnięcia jasno określonych korzyści i wartości. Współpraca musi przynosić zysk (rozumiany nie tylko w kategoriach ekonomicznych) dla wszystkich zaangażowanych podmiotów, zarówno prywatnych, jak i publicznych[28]. Istnienie korzyści wynikających ze współpracy i możliwość wyraźnego ich dostrzeżenia i zaobserwowania jest olbrzymią motywacją do podejmowania dalszych działań i do pogłębiania współpracy.

Sformalizowana współpraca prywatno-publiczna może mieć różną strukturę i sposób organizacji. Podział ról i decyzja dotycząca tego, kto sprawuje jakie funkcje (kto jest liderem grupy, kto koordynatorem itd.), może mieć znaczący wpływ na to, w jaki sposób funkcjonowała będzie współpraca[29]. Należy zatem, przed rozpoczęciem prac, dokonać kompleksowej analizy i wyboru strategii tego, jak zaplanować prace grupy. Można wyróżnić przynajmniej trzy sposoby podziału ról[30]:

- PPP, w którym jeden z członków jest liderem i zarządza pracą grupy. Może nim być zarówno podmiot prywatny, jak i publiczny.
- PPP, w którym rolę lidera pełni specjalnie do tych celów powołane ciało.
- PPP, w którym wszyscy członkowie mają takie same zobowiązania i prawa. Czasami w tym modelu występuje również kadencyjne sprawowanie tej funkcji lidera.

---

[26] Ibidem, s. 20.

[27] ENISA, *Cooperative Models for Effective Public Private Partnerships. Good Practice Guide*, s. 18.

[28] Ibidem.

[29] Ibidem, s. 18.

[30] ENISA, *Cooperative Models for Effective Public Private Partnerships. Deskop Research Report*, s. 17.

Jak wskazują Myriam Dunn Cavelty oraz Manuel Suter, w ostatnim czasie na znaczeniu zyskuje trend takiego organizowania współpracy między podmiotami publicznymi oraz prywatnymi w zakresie OIK, w którym te pierwsze coraz rzadziej zajmują się faktycznym kierowaniem pracami grup i monitorowaniem działań, a bardziej skupiają się na koordynowaniu działań i identyfikacji instrumentów, które motywują członków do wypełniania określonych zadań. Według tego podejścia większą wartość mają formy współpracy, które są oparte na mechanizmach samoregulacji oraz samoorganizacji[31]. Takie rozwiązanie daje zaangażowanym podmiotom większe poczucie pewności i buduje zaufanie. Ponadto prowadzi do większej elastyczności prowadzenia prac i lepszego dostosowania się do zmieniającej się sytuacji oraz okoliczności.

PPP można także podzielić ze względu na sposób partycypacji. Wtedy możemy mówić między innymi o:

- uczestnictwie na zasadzie płatnego członkostwa,
- członkostwie obowiązkowym, np. determinowanym istniejącymi odpowiednimi przepisami,
- partycypacji na zasadzie wolontariatu – podmioty zostają członkami danego PPP dobrowolnie[32].

Jeśli podmiot publiczny decyduje się na zaproszenie podmiotów prywatnych do współpracy na zasadzie członkostwa nieobligatoryjnego, musi podjąć odpowiednie działania, zachęcające podmioty do zaangażowania się w prace. Istnieje cała gama zachęt, jakie można zaoferować członkom współpracy, i korzyści jakie mogą osiągnąć dzięki aktywnemu zaangażowaniu się w poszczególne inicjatywy, np.[33]:

- chęć redukowania ryzyka związanego z narażeniem na niebezpieczeństwa. Zaangażowanie się we wspólne prace może prowadzić do osiągnięcia lepszej ochrony, wyższego poziomu bezpieczeństwa i lepszej odporności, co jest jedną z najważniejszych korzyści podjęcia współpracy,
- oszczędności wynikające z synergii wspólnych działań podejmowanych wraz z podmiotem publicznym w ramach rozwiązania danego problemu,
- możliwość uzyskania dostępu do informacji, które członkom prywatnym, w ramach współpracy, przekazuje podmiot publiczny,
- możliwość uzyskania dostępu do wiedzy, którą można nabyć dzięki uczestnictwu w projekcie,
- możliwość uniknięcia konieczności aplikowania regulacji, do wprowadzenia których podmiot byłby zobligowany w razie nieuczestniczenia w pracach,
- wspomniana wcześniej możliwość wpływania na kreowanie polityki i rozwiązań publicznych, a także wyznaczanie kierunków działań.

---

[31] M. Dunn Cavelty, M. Suter, *Public Private Partnerships...*, s. 1.

[32] ENISA, *Cooperative Models for Effective Public Private Partnerships. Deskop Research Report*, s. 18.

[33] ENISA, *Cooperative Models for Effective Public Private Partnerships. Good Practice Guide*, s. 37.

Współpraca prywatno-publiczna może być tworzona jako sformalizowana forma współdziałania, angażująca członków z jednego państwa (krajowe partnerstwa), angażująca członków z różnych państw europejskich (europejskie partnerstwa), zrzeszająca podmioty z całego świata (partnerstwa międzynarodowe)[34]. Decydując się na wybór jednego z powyższych modeli współpracy należy pamiętać, że rozmiar grupy współpracującej oraz jej charakter (narodowy lub transnarodowy) mogą generować pewne obawy przed zaangażowaniem i zmniejszać chęć partycypacji w pracach.

Ostatnim, bardzo istotnym elementem, wpływającym na skuteczność działań powoływanej współpracy, jest zaangażowanie w daną inicjatywę właściwych podmiotów, ale także wybranych z nich właściwych ludzi i oddelegowanych specjalistów[35]. Tylko poczucie pracy z „właściwymi" ludźmi, posiadającymi odpowiednią wiedzę i doświadczenie, sprawia, że inicjatywa ma szansę być efektywna i nie będzie tylko markowaniem działań.

Wskazuje się także wiele przykładów pokazujących, że dużą wartość niesie tworzenie specjalnych grup strategicznych angażujących w prace przedstawicieli podmiotów z najwyższego szczebla zarządu. Jedną z pozytywnych konsekwencji takiego zaangażowania jest lepsze rozumienie przez kierownictwo problemów przed jakimi stoi firma i większe wsparcie dla działań związanych z budowaniem bezpieczeństwa[36].

Zaufanie podstawą PPP

Jednym z najważniejszych elementów udanej współpracy publiczno-prywatnej jest zbudowanie wzajemnego zaufania. Wszystkie zaangażowane strony muszą być pewne swoich intencji, zaangażowania i bezpieczeństwa interesów. Dotyczy to między innymi zapewniania bezpieczeństwa informacji, co może być rozumiane dwojako. Po pierwsze, podmioty muszą być pewne, że mogą polegać na informacji jaką przekazuje im druga strona. Wiarygodność jest tutaj fundamentalna. Po drugie, podmioty muszą mieć absolutne przekonanie, że ujawnienie partnerowi ważnych informacji nie odbije się negatywnie na ich interesie, np. informacja nie wycieknie, nie wpłynie niekorzystnie na dobre imię podmiotu. Ilustracją może być tutaj sytuacja, w której firmy mogą mieć opory przed przekazywaniem partnerom konkretnych informacji, np. o atakach cybernetycznych, których stali się ofiarą, w obawie przed utratą zaufania klientów, jeśli informacje o incydencie wycieką do przestrzeni publicznej.

[34] ENISA, *Cooperative Models for Effective Public Private Partnerships. Deskop Research Report*, s. 20.

[35] ENISA, *Cooperative Models for Effective Public Private Partnerships. Good Practice Guide*, s. 27.

[36] Ibidem, s. 26.

Jak pokazano powyżej, sposób organizacji współpracy publiczno-prywatnej może być zaprojektowany na wiele sposobów. Może mieć charakter narodowy lub międzynarodowy, grupy mogą skupiać członków z tych samych sektorów, mogą też być międzysektorowe[37]. Istnieje wiele argumentów za i przeciw wyborowi jednego z tych dwóch typów działań, jednak badania empiryczne przeprowadzone przez ENISA wskazują, że pierwszy wskazany typ współpracy sprzyja budowaniu zaufania między partnerami[38]. Dodatkową korzyścią takiego rozwiązania jest to, że sektorowo zorganizowana współpraca umożliwia członkom skupienie się na specjalistycznych problemach charakterystycznych dla danego sektora, niosąc dla nich większą wartość dodaną i większą gwarancję rozwiązania ważnych dla nich kwestii[39].

Zaobserwowano także, że na zaufanie wpływa sposób komunikowania się i prowadzenia interakcji między podmiotami zaangażowanymi we współpracę. Sprzyjającymi okolicznościami są nie za duże grupy uczestników, w których reprezentanci podmiotów mają możliwość spotykania się twarzą w twarz. Budowanie personalnych relacji jest wskazywane jako kluczowe dla osiągnięcia zaufania. Jest to szczególnie istotne, jeśli współpraca dotyczy wymiany ważnych i często poufnych informacji[40].

Podsumowanie

Rozważania podjęte w niniejszym artykule miały na celu ukazanie problemów, wyzwań i aktualnych trendów w obszarze związanym z OIK. Charakter współczesnych międzynarodowych relacji i procesy zachodzące wewnątrz państw znacząco wpływają na sposoby zapewniania bezpieczeństwa najważniejszych infrastruktur. Globalizacja, prywatyzacja, współzależność to tylko wybrane okoliczności jakie wymuszają stosowanie nowych praktyk i nowych strategii. Tradycyjny sposób definiowania IK oraz sposób postrzegania niebezpieczeństw jej grożących ewoluował. W OIK zaangażowane są coraz to nowe podmioty, także międzynarodowe, co jest sytuacją nową i niosącą wiele wyzwań.

Kolejnym, jednym z najważniejszych elementów skutecznej OIK jest powoływanie do życia współpracy prywatno-publicznej. Decyzja o stworzeniu tego typu inicjatyw musi zostać poprzedzona głęboką refleksją związaną z celami, dla których tworzy się współpracę. Nie mniej ważne jest dalsze zaprojektowanie prac. Decyzje, przed jakimi stoją uczestnicy współpracy prywatno-publicznej, rekomendacje i sposoby organizowania inicjatyw pokazane w tym artykule miały na celu zasygnalizowanie kluczowych elementów. Każdy z nich wymaga bardziej kompleksowego

[37] ENISA, *Cooperative Models for Effective Public Private Partnerships. Deskop Research Report*, s. 20.

[38] ENISA, *Cooperative Models for Effective Public Private Partnerships. Good Practice Guide*, s. 23.

[39] Ibidem.

[40] Ibidem, s. 35.

rozwinięcia i osobnego potraktowania. Podkreślić tutaj należy jednak, że wszystkie aktywności podjęte w ramach wspólnych prac nad OIK muszą mieć na uwadze, i być szczególnie uczulone na nieustanne budowanie zaufania pomiędzy zaangażowanymi stronami. Jest to absolutnym fundamentem i warunkiem osiągnięcia sukcesu.

Bibliografia

Dunn Cavelty M., Suter M., *Public Private Partnerships are no silver bullet...*, International Journal of Critical Infrastructure Protection, Zurich 2009.

Dyrektywa Rady 2008/114/WE, w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:PL:PDF, dostęp 02.02.2013.

ENISA, *Cooperative Models for Effective Public Private Partnerships. Good Practice Guide*, 2011.

ENISA, *Cooperative Models for Effective Public Private Partnerships. Deskop Research Report*, 2011.

Renda A. (red.), *Protecting Critical Infrastructure in the EU. CEPS Task Force Report*, Centre for European Policy Studies 2010.

Rządowe Centrum Bezpieczeństwa, *Infrastruktura Krytyczna*, www.rcb.gov.pl.

Skomra W., *Ochrona infrastruktury krytycznej w systemie zarządzania kryzysowego*, Rządowe Centrum Bezpieczeństwa, www.powiat-wloszczowa.pl.

Umbach F., *Critical Energy Infrastructure At Risk of Cyber Attack*, KAS International Report 9/2012.

Wójtowicz W., *Bezpieczeństwo infrastruktury krytycznej*, Warszawa 2006.

Contemporary challenges of protecting the critical infrastructure

Abstract

The article analyzes the problem of protecting the critical infrastructure. It discusses current trends of ensuring its security and the way of identifying threats. Particular attention is paid to the issues of public-private cooperation which is the key component of actions influencing the security of critical infrastructure. The article also presents the main challenges that efficient private-public cooperation must face as well as best practices and recommendations.

Key words: security, infrastructure, protection