Studia i Materiały. Miscellanea Oeconomicae
Rok 21, Nr 4/2017, tom I
Wydział Prawa, Administracji i Zarządzania
Uniwersytetu Jana Kochanowskiego w Kielcach

Zarządzanie kryzysowe i bezpieczeństwo

Michał Wiśniewski[1], **Tadeusz Krupa**[2]

KIERUNKI ROZWOJU ZARZĄDZANIA BEZPIECZEŃSTWEM INFRASTRUKTURY KRYTYCZNEJ

Streszczenie: Artykuł prezentuje syntezę wiedzy na temat zarządzania bezpieczeństwem IK w świetle praktyki oraz przepisów obowiązujących w Polsce i UE. W artykule zwrócono uwagę na związek pojęć bezpieczeństwo narodowe, zarządzanie kryzysowe oraz IK. Zaobserwowano rozbieżności terminologiczne prowadzące do odmiennego postrzegania IK mającego wpływ na jej identyfikację oraz sposób klasyfikacji. W podsumowaniu zawarto kierunki rozwoju zarządzania bezpieczeństwem IK.

Słowa kluczowe: Infrastruktura Krytyczna, Europejska Infrastruktura Krytyczna, funkcjonalności krytyczne, zarządzanie kryzysowe, bezpieczeństwo narodowe, ochrona infrastruktury krytycznej

Wprowadzenie

Rozwój cywilizacyjny i postęp techniczny dostarczają rozwiązań, które umożliwiają efektywne działanie państwa oraz komfortowe funkcjonowanie społeczeństwa. Obserwowany postęp dotyczy całości otoczenia człowieka, co prowadzi do coraz większego uzależniania się ludności od szeroko rozumianej infrastruktury, zapewniającej niezbędne funkcjonalności, np. systemu: energetycznego, łączności, opieki zdrowotnej, dostaw żywności i wody, itp. Częścią tej infrastruktury jest tzw. infrastruktura krytyczna (IK). Ze względu na ważny interes społeczny obserwowana jest duża dynamika prac prowadzonych nad systemem pojęć zdolnym

[1] Mgr inż. Michał Wiśniewski, Wydział Zarządzania, Politechnika Warszawska.
[2] Prof. dr hab. inż. Tadeusz Krupa, Wydział Zarządzania, Politechnika Warszawska.

opisać IK oraz metodami jej ochrony[3]. Działania te doprowadziły do rozbieżności w sposobie identyfikacji IK oraz dotyczących celu jej ochrony.

Uzasadnieniem podjęcia badań w obszarze zarządzania bezpieczeństwem IK jest również wzrost liczby systemów uznawanych za IK. Systemy IK nie są od siebie odizolowane i nieustannie na siebie oddziałują tworząc sieć zależności[4]. Dlatego awarie występujące w jednym systemie IK mogą, w wyniku „efektu domina" lub innych modelowych zbieżności (np. tzw. efekt „dziur w serze"), negatywnie wpływać na poprawność funkcjonowania innych systemów. Rozszerzająca się lista systemów IK determinuje tym samym wzrost stopnia skomplikowania procesu, co w konsekwencji ogranicza jakość procesów zarządzania bezpieczeństwem IK.

Istnieje więc uzasadniona potrzeba analizy osiągnięć w obszarze zarządzania bezpieczeństwem IK oraz opracowanie systemu pojęć i metod działania możliwych do zastosowania w przypadku większości kluczowych systemów IK. Stąd celem artykułu jest analiza stanu wiedzy oraz próba określenia kierunków rozwoju zarządzania bezpieczeństwem współczesnych IK.

Opracowanie jest wynikiem prac przeprowadzonych w ramach uczestnictwa w projekcie rozwojowym NCBiR pt. Wysokospecjalistyczna platforma wspomagająca planowanie cywilne i ratownictwo w administracji publicznej RP oraz jednostkach organizacyjnych KSRG umowa nr DOB – BIO7/11/02/2015 na wykonanie projektów w zakresie badań naukowych i projektów rozwojowych na rzecz obronności i bezpieczeństwa państwa, przez konsorcjum: Politechnika Warszawska (Wydział Zarządzania), Medcore sp. z o.o.

Bezpieczeństwo narodowe

Pojęcie IK nierozerwalnie wiąże się z zagadnieniem zarządzania kryzysowego i pojęciem bezpieczeństwa narodowego. Związek ten widać w przyjętej w Polsce definicji zarządzania kryzysowego określanego jako „działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowej, usuwaniu ich skutków oraz odtwarzaniu zasobów IK"[5]. Sytuacja kryzysowa to „sytuacja wpływająca negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołująca znaczne ograniczenia w działaniu właściwych organów administracji

---

[3] **Metodyki** – 2008 r. National Risk Assessment Method Guide; 2008 r. National Risk Register; 2009 r. Working with scenarios, risk assessment and capabilities In the National Safty and Security Strategy of Netherlands; 2010 r. A Framework for Major Emergrncy Management, A Guide to Risk Assessment In Major Emergency Management; 2011 r. Method of Risk Analysis for Civil Protection; 2012 r. Guide to Risk and Vulenerability Analyses; 2013 r. All Hazards Risk Assessment Methodology Guidelines. **Opracowania naukowe** – Lidwa, 2012; Atlas, 2013; Kyriakides, Polycarpou, 2015; Skomra, 2015; Macaulty, 2016; Kosieradzka, Zawiła-Niedźwiecki, 2016.

[4] S. Korzeniowska, *Cyberbezpieczeństwo infrastruktury Krytycznej*, LSW – Leśnodorski Ślusarek i Wspólnicy, s. 19-20, www.lsw.com.pl, (29.08.2016).

[5] Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 Nr 89 poz. 590), art. 2.

publicznej ze względu na nieadekwatność posiadanych sił i środków”[6]. Przytoczone definicje zarządzania kryzysowego i sytuacji kryzysowej wskazują na konieczność przygotowania planów reakcji na zdarzenia niepożądane, których wystąpienie może wpływać na bezpieczeństwo narodowe.

Bezpieczeństwo narodowe w literaturze przedmiotu definiowane jest przez wielu autorów:

- W. Stankiewicz uważa bezpieczeństwo narodowe za „stan równowagi między zagrożeniem wywołanym możliwością zaistnienia konfliktu a potencjałem obronnym”[7];
- C. Rutkowski definiuje bezpieczeństwo narodowe jako „stan świadomości społecznej, w którym istniejący poziom zagrożeń, dzięki posiadanym zdolnościom obronnym, nie budzi obaw o zachowanie (osiągnięcie) uznanych wartości”[8].

Przytoczone definicje akcentują konieczność obrony państwa przed zagrożeniami militarnymi „czyli użyciem lub groźbą użycia siły militarnej przez podmiot prawa międzynarodowego”[9]. Tymczasem kryzys gospodarczy i finansowy ostatnich lat silnie uwidocznił konieczność szerszego podejścia do zagadnienia bezpieczeństwa narodowego i zarządzania kryzysowego. Współcześnie bezpieczeństwo narodowe musi być rozpatrywane na trzech poziomach[10]:

- bezpieczeństwa zewnętrznego (niepodległość i integralność terytorialna),
- bezpieczeństwa wewnętrznego (ład i porządek wewnątrz państwa),
- trwałego i zrównoważonego rozwoju (stabilny rozwoju społeczno-gospodarczy kraju i ochrona środowiska).

Zmiany w rozumieniu i interpretacji pojęcia bezpieczeństwa narodowego dotyczą przesuwania się punktu ciężkości z zagrożeń militarnych na zagrożenia niemilitarne w tym zagrożenia naturalne i terrorystyczne. Zagrożenia niemilitarne definiuje się jako „zagrożenia obejmujące taki splot zdarzeń w stosunkach międzynarodowych, w których z dużym prawdopodobieństwem może nastąpić ograniczenie lub utrata warunków do niezakłóconego bytu i rozwoju państwa, ewentualnie naruszenie jego suwerenności w wyniku zastosowania wobec niego przemocy niezbrojnej”[11]. Natomiast zagrożenia naturalne to „zagrożenia, których istota wynika z działań sił natury: geologicznych, hydrologicznych, endemicznych”[12].

Zmiana charakteru zagrożeń determinuje redefinicję pojęcia bezpieczeństwo narodowe, które należy rozumieć jako jedno z „podstawowych dziedzin aktywności

---

[6] *Ibidem*, art. 3, pkt 1.

[7] W. Stankiewicz, *Bezpieczeństwo narodowe a walki niezbrojne*, *Studium*, Warszawa 1991, s. 76.

[8] C. Ruktowski, *Bezpieczeństwo i obronność: strategie – koncepcje – doktryny*, Warszawa 1995, s. 30.

[9] AON, *Słownik terminów z zakresu bezpieczeństwa narodowego – wydanie szóste,* Akademia Obrony Narodowej, Warszawa 2008, s. 176.

[10] U. Kąkol, M. Kisilowski, G. Kunikowski, A. Uklańska, *Diagnoza planowania cywilnego w procesie przygotowań obronnych*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego,* Fundacja Gospodarki i Administracji Publicznej, Kraków 2016, s. 53-63.

[11] AON, *Słownik..., op.cit.*, s. 176.

[12] *Ibidem*, s. 176.

państwa, mające zapewnić rozwój i swobodę realizacji interesów narodowych w konkretnych warunkach bezpieczeństwa, poprzez podejmowanie wyzwań, wykorzystywanie szans, redukowanie ryzyka oraz przeciwdziałanie wszelkiego rodzaju zagrożeniom dla jego interesów"[13]. Pojęcie zagrożenia należy tu rozumieć jako „sytuację, w której pojawia się prawdopodobieństwo powstania stanu niebezpiecznego dla otoczenia. Przyjmując za podstawę dziedziny i obszary, w których może wystąpić zagrożenie, wyróżnia się zagrożenia militarne i niemilitarne"[14]. Z przytoczonej definicji wynika, że państwo chcąc zapewnić bezpieczeństwo obywatelom musi zgromadzić odpowiednie siły i środki w odpowiedzi na zagrożenia, których wystąpienie mogłoby doprowadzić do sytuacji kryzysowej.

W uproszczeniu potencjał obronny przed zagrożeniami militarnymi stanowią siły zbrojne państwa. Natomiast potencjałem obronnym przed zagrożeniami niemilitarnymi jest IK państwa, która odpowiada za dostępność funkcjonalności i zasobów niezbędnych do reakcji na zagrożenia niemilitarne. Jednocześnie należy zauważyć, że IK sama jest podatna na zagrożenia. Stąd konieczne jest wdrożenie procedur ochrony IK.

Przedstawione refleksje jasno wskazują na związek pojęć bezpieczeństwo narodowe, zarządzanie kryzysowe i infrastruktura krytyczna oraz fundamentalne znaczenie IK w dla bezpieczeństwa obywateli i stabilności rozwoju gospodarczego.

Podsumowując dotychczasowe rozważania dotyczące IK należy zauważyć, że IK:
- jest konieczna do funkcjonowania państwa, gospodarki i społeczeństwa,
- to instalacje, maszyny, budynki, systemy i instytucje usługowe,
- pełni zróżnicowane funkcje gospodarcze i społeczne,
- wpływa na bezpieczeństwo państwa i obywateli.

Infrastruktura krytyczna

Dotychczas świadomie nie podano definicji IK, ponieważ jej rozumienie nie jest jednolite, co zilustrowano na przykładzie definicje stosowanej w Polsce i UE.

W Polsce termin IK[15] został zdefiniowany i wprowadzony do prawnego systemu pojęciowego na mocy ustawy u o zarządzaniu kryzysowym. Zasoby oraz obiekty zaliczone do IK realizują zróżnicowane zadania wspomagające funkcjonowanie państwa oraz społeczeństwa. Realizowane przez IK zadania mogą stanowić kryterium grupowania obiektów uznanych za IK w systemy. Polska IK jest podzielona na jedenaście systemów krytycznych[16].

Identyfikacja obiektów IK w Polsce odbywa się na podstawie kryteriów systemowych i przekrojowych, które zostały zdefiniowane przez dyrektora Rządowego Centrum Bezpieczeństwa i opublikowane w Narodowym Programie Ochrony Infrastruktury Krytycznej (NPOIK). Kryteria systemowe charakteryzują ilościowo

---

[13] *Ibidem*, s.17.
[14] *Ibidem*, s.172-173.
[15] Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 Nr 89 poz. 590), art. 3, pkt 2.
[16] *Ibidem*, art. 3, pkt 2.

lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi, których spełnienie może spowodować zaliczenie do IK. Kryteria te przedstawione są dla każdego z systemów IK i stanowią niejawny załącznik do NPOIK. Kryteria przekrojowe opisują parametry odnoszące się do skutków zniszczenia bądź zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi[17]:

- ofiary w ludziach,
- skutki finansowe,
- konieczność ewakuacji,
- utratę usługi,
- czas odbudowy,
- efekt międzynarodowy,
- unikatowość.

W pierwszym etapie wyznaczania IK wykorzystuje się kryteria sektorowe na podstawie, których wstępnie przypisuje się analizowany obiekt do jednego z systemów IK. W ramach etapu drugiego weryfikowane jest czy obiekt wpisuje się w ustawową definicję IK. Przez co należy rozumieć sprawdzenie:

- Czy obiekt jest kluczowy dla bezpieczeństwa państwa i jego obywateli?
- Czy warunkuje sprawne funkcjonowanie administracji publicznej, przedsiębiorców i instytucji?

Jeśli obiekt przejdzie pozytywnie etap drugi w ramach etapu trzeciego jest oceniany w kategoriach wyznaczonych przez kryteria przekrojowe. Na tym etapie obiekt zostaje zakwalifikowany jako IK w przypadku, gdy zostaną spełnione dwa z siedmiu kryteriów przekrojowych.

W polskim systemie prawnym nie istnieje akt normatywny obnoszący się bezpośrednio do zagadnienia ochrony IK. Przywoływany NPOIK jest aktem o charakterze planistycznym wyznaczającym ogólne założenia i cele jakie należy w tym obszarze osiągnąć. Nie precyzuje on jednak metod i technik jakimi uczestnicy procesu zarządzania bezpieczeństwem IK mogliby się posługiwać przygotowując plan działań mający zabezpieczyć IK przed zagrożeniami. Wskazuje on jednak zestaw praktyk rekomendowanych dla podmiotów zajmujących się ochroną IK.

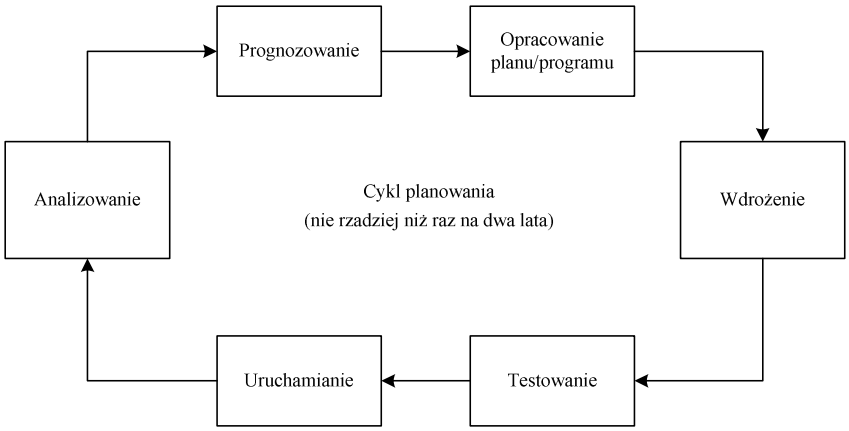
Pojęcie ochrony IK również zostało zdefiniowane w ustawie o zarządzaniu kryzysowym, która obecnie jest podstawą prawną działań podejmowanych w celu zabezpieczenia IK. Ochrona IK rozumiana jest jako „wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania i integralności IK w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtwarzania tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie”[18]. Realizacja tak zdefiniowanej ochrony IK wymaga identyfikacji zagrożeń i oceny ryzyk jakie są determinowane rozpoznanymi zagrożeniami.

---

[17] *Narodowy Program Ochrony Infrastruktury Krytycznej*, RCB, Warszawa 2015, s. 13.

[18] Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590), art. 3, pkt 2.

Obecnie ze względu braku dedykowanych metod i narzędzi zarządzania bezpieczeństwem IK w Polsce ochrona IK jest realizowana w ramach procesu planowania cywilnego[19]. Planowanie cywilne jest realizowane w tzw. cyklu planowania, który został zobrazowany na rysunku 1.



Rysunek 1. Schemat cyklu planowania cywilnego
Źródło: Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590).

Ustawa o zarządzaniu kryzysowym doprowadziła w Polsce do konsolidacji wielu przepisów określających obowiązki podmiotów odpowiedzialnych za zarządzanie bezpieczeństwem IK w jednym akcie prawnym. Jednak jej uchwalenie nie oznacza, że akty prawne stosowane przed 26 kwietnia 2007 r. tracą moc i można je pomijać.

Należy tu wspomnieć o innych terminach określających urządzenia, instalacje i usługi uznawane za niezbędne do funkcjonowania państwa i jego obywateli. Obok pojęcia IK można w literaturze przedmiotu znaleźć odwołania do pojęć:

- Infrastruktura państwa „to główne obiekty, instalacje i urządzenia stałe, wraz z instytucjami usługowymi utrzymujące je w sprawności technicznej, niezbędne do funkcjonowania produkcyjnych działów gospodarki oraz życia (w tym bezpieczeństwa) ludności kraju”[20];
- Infrastruktura bezpieczeństwa to „całokształt obiektów, urządzeń, instalacji oraz instytucji zapewniających ich sprawność techniczną i utrzymanie, które są podstawą funkcjonowania systemu bezpieczeństwa państwa”[21];
- Obszary, obiekty, urządzenia, transporty podlegające obowiązkowej ochronie to „elementy ważne dla obronności, interesu gospodarczego państwa,

[19] *Ibidem*, art. 3, pkt 4.
[20] AON, *Słownik…*, *op.cit*., s. 56.
[21] *Ibidem*, s. 52.

bezpieczeństwa publicznego i innych ważnych interesów państwa podlegają obowiązkowej ochronie przez specjalistyczne uzbrojone formacje ochronne lub odpowiednie zabezpieczenia techniczne”[22];

– Infrastruktura publiczna to „dobra publiczne majce charakter dóbr podstawowych o strategicznym znaczeniu dla całej gospodarki i społeczeństwa, umożliwiającej przemieszczanie mediów (energii, pojazdów, wody, informacji), osób i rzeczy, udostępniane bezpłatnie lub za odpłatnością, częściową, pozostające w gestii władz publicznych (państwowych lub lokalnych), na których spoczywa obowiązek tworzenia infrastruktury i utrzymania jej w odpowiednim stanie”[23].

Bez względu na nazewnictwo, działania związane z ochroną IK wykraczają poza granice państw. Coraz większego znaczenia nabiera współpraca w ramach wspólnot narodowych i działania zmierzające do zabezpieczenia infrastruktur wpływających na funkcjonowanie więcej niż jednego państwa. Podejmowane inicjatywy bazują na międzynarodowych przepisach, mających zapewnić ciągłość funkcjonowania obiektów IK w uwarunkowaniach powiązań globalnych przedsięwzięć, minimalizujących zagrożenia systemów IK, przede wszystkim dzięki wzajemnemu informowaniu i ostrzeganiu[24]. Polska IK nie jest wyjątkiem od tej reguły, czego przykładem jest system zaopatrzenia w energię, surowce energetyczne i paliwa. System ten zaliczany jest do tzw. Europejskiej Infrastruktury Krytycznej (EIK).

EIK definiowana jest jako „IK zlokalizowana na terytorium państw członkowskich, której zakłócenie lub zniszczenie ma istotny wpływ na co najmniej dwa państwa członkowskie UE”[25]. Obecnie EIK jest identyfikowana w dwóch sektorach.

Tabela 1. Wykaz sektorów Europejskiej Infrastruktury Krytycznej

Sektor	**Podsektor**	
Energia	Energia elektryczna	Infrastruktura i urządzenia do wytwarzania i przesyłania energii elektrycznej w odniesieniu do dostaw energii elektrycznej;
	Ropa naftowa	Produkcja, rafinacja, przetwarzanie, magazynowanie i przesyłanie rurociągami ropy naftowej;
	Gaz	Produkcja, rafinacja, przetwarzanie, magazynowanie i przesyłanie rurociągami gazu; Terminale skroplonego gazu ziemnego (LNG);
Transport	Transport drogowy;	
	Transport kolejowy;	
	Transport lotniczy;	
	Transport wodny;	
	Żegluga oceaniczna, żegluga morska bliskiego zasięgu i porty;	

Źródło: Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania EIK oraz oceny potrzeb w zakresie jej ochrony.

[22] Ustawia z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. 1997 nr 114 poz. 740), art. 5, pkt 1.

[23] K. Brzozowska, *Finansowanie inwestycji infrastrukturalnych przez kapitał prywatny na zasadzie Project finance,* Warszawa 2009, s. 18.

[24] A. Tyburska, M. Nalepski, *Ochrona infrastruktury krytycznej,* Szczytno 2008, s. 22.

[25] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania EIK oraz oceny potrzeb w zakresie jej ochrony, art. 2b.

Oprócz terminu EIK w prawodawstwie UE funkcjonuje definicja IK[26] różniąca się od definicji przyjętej w Polsce. Różnica w pojmowaniu IK przez prawodawstwo Polskie i UE skutkuje m.in. odmienną listą systemów IK[27], co zilustrowano w tabeli 2.

Tabela 2. Porównanie wykazu EIK i Polskiej IK

Europejska IK	IK Polski
– energia, – przemysł jądrowy, – technologie informacyjno-komunikacyjne, – woda, – żywność, – zdrowie, – sektor finansowy, – transport, – przemysł chemiczny, – przemysł kosmiczny, – infrastruktura badawcza.	– system zaopatrzenia w energię, surowce energetyczne i paliwa, – system łączności, – system sieci teleinformatycznych, – system finansowy, – system zaopatrzenia w żywność, – system zaopatrzenia w wodę, – system ochrony zdrowia, – system transportowy, – system ratowniczy, – system zapewniający ciągłość działania administracji publicznej, – system produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Źródło: opracowanie własne na podstawie ibid., art. 2b i Ustawa z dnia 26 kwietnia 2007, *op.cit*., art. 3, pkt 2.

Ponadto Unijny Mechanizm Ochrony Ludności (UMOL), wyróżniona dodatkowy sektor IK, który nazwano *systemem ochrony dziedzictwa narodowego*.

W przypadku EIK pojęcie ochrony IK definiowane jest „jako wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania i integralności IK w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczania i neutralizacji ich skutków”[28]. W przypadku tej definicji również widać rozbieżności rozumienia terminu ochrona IK. W polskiej definicji akcentuje się dodatkowo szybkie odtwarzanie uszkodzonej lub zniszczonej IK. Może to prowadzić do innego ukierunkowania planów ochrony IK, które skupią się na odbudowie IK, co pozwoli przywrócić jej funkcjonalności. W unijnej definicji ochrony IK nie ma fragmentu sugerującego odtworzenie IK, co otwiera możliwość podejmowania działań zmierzających do udostępnienia funkcjonalności uszkodzonej lub zniszczonej IK na innych dostępnych zasobach.

EIK wyznaczana jest na podstawie kryteriów przekrojowych i sektorowych. Europejskie kryteria sektorowe charakteryzują ilościowo lub podmiotowo parametry (funkcyjne) infrastruktury, która po ich spełnieniu może zostać zaliczona jako

[26] *Ibidem*, art. 2b.

[27] R. Radziejewski, *Ochrona infrastruktury krytycznej – teoria a praktyka,* PWN, Warszawa 2014, s. 46-47.

[28] Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania EIK oraz oceny potrzeb w zakresie jej ochrony, art. 2e.

IK. W przypadku unijnej definicji kryteriów sektorowych należy zwrócić uwagę, że podkreślają one znaczenie funkcji IK, co nie występuje w polskich przepisach. Europejskie kryteria przekrojowe odnoszą się do rozmiaru strat wynikających z zakłócenia lub zniszczenia IK, które podzielono na[29]:

- kryterium ofiar w ludziach – liczba ofiar śmiertelnych lub liczba rannych,
- kryterium skutków ekonomicznych – wielkość strat ekonomicznych,
- kryterium skutków społecznych – wpływ na zaufanie opinii publicznej, cierpienia fizyczne i zakłócenia codziennego funkcjonowania.

Procedura wyznaczania EIK jest wskazana w zapisach Dyrektywy Rady 2008/114/WE z 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania EIK oraz oceny potrzeb w zakresie jej ochrony. Zapisy dyrektywy pozostawiają państwom członkowskim UE znaczącą swobodę w kwestii wyznaczania EIK. Stwierdza się, że „Komisja Europejska wraz z państwami członkowskimi opracowuje wytyczne w sprawie stosowania kryteriów przekrojowych i sektorowych oraz ustala przybliżone progi, które mają być stosowane do rozpoznawania EIK"[30]. Ponadto kraje członkowskie mogą stosować krajowe kryteria wyznaczania IK w celu wskazania EIK.

Całości procedury identyfikacji EIK składa się z dwóch etapów: rozpoznania i wyznaczenia EIK. Etap rozpoznania realizowany jest na poziomie jednostek UE natomiast etap wyznaczenia realizowany jest przez kraj członkowski na terenie, którego potencjalna EIK jest zlokalizowana. W przypadku etapu wyznaczania EIK państwo członkowskie, na którego terytorium zlokalizowana jest potencjalna EIK, prowadzi rozmowy z państwami, na które potencjalna EIK może mieć wpływ. Rozmowy mają potwierdzić lub zanegować przypuszczalny wpływ EIK na systemy zainteresowanego państwa i ustalić ich natężenie. Po osiągnięciu porozumienia państwo, na terenie którego znajduje się potencjalna EIK nadaje jej status EIK. Następnie informuje Komisję Europejską o liczbie EIK w danym sektorze. Wykaz EIK znany jest tylko państwom, na które jej awaria ma wpływ.

Dyrektywa w sprawie rozpoznawania i wyznaczania EIK oraz oceny potrzeb w zakresie jej ochrony jest konsekwencją wdrożenia Europejskiego Programu Ochrony IK (EPOIK). W EPOIK podkreślono, że „skuteczna ochrona IK wymaga komunikacji, koordynacji i współpracy na poziomie krajowym i UE pomiędzy wszystkimi zainteresowanymi stronami: operatorami IK, organami regulacji, organizacjami zawodowymi i stowarzyszeniami branżowymi, we współpracy ze wszystkimi poziomami władz państwowych oraz ogółem społeczeństwa"[31]. Należy zauważyć, że mimo zbliżonych definicji IK oraz ochrony IK istnieją rozbieżności wpływające na wykaz systemów uznawanych za IK.

[29] *Ibidem*, art. 3.
[30] *Ibidem*, art. 3, pkt. 2.
[31] R. Radziejewski, *op.cit.*, s. 44.

Tabela 3. Zestawienie sektorów IK w wybranych państwach

Sektor	Państwo						
	Austria	Finlandia	Holandia	Szwecja	Wielka Brytania	Niemcy	Polska
System kontroli ruchu powietrznego				x			
Bankowość i finanse	x	x		x	x		x
Rząd/służby		x		x	x		
Telekomunikacja	x	x		x	x	x	x
Energia/elektryczność	x	x	x	x	x	x	x
Służby ratownictwa	x	x			x		x
Żywość/rolnictwo		x			x	x	x
Materiały niebezpieczne						x	x
Służba zdrowia	x	x	x		x	x	x
Przemysł obronny/zakłady produkcyjne		x					
Media	x	x		x	x		
Sprawiedliwość/stosowanie prawa					x		
Obrona militarna/siły zbrojne/ instalacje wojskowe	x						
Dostawa gazu i ropy							x
Policja	x	x			x		
Poczta	x						
Administracja publiczna	x	x			x	x	x
Bezpieczeństwo porządek publiczny					x	x	
Gospodarka odpadami					x		x
Bezpieczeństwo socjalne/opieka	x	x					
Transport/logistyka/dystrybucja	x	x	x		x	x	x
Usługi komunalne	x						
Dostawy wody	x	x			x	x	x

Źródło: W. Wójtowicz, *Bezpieczeństwo infrastruktury krytycznej,* Departament Polityki Obronnej MON, Warszawa 2006, s. 51.

Analiza danych zebranych w Tabeli 2 wskazuje, że katalog systemów IK w poszczególnych krajach nie jest tożsamy. Rozbieżności w wykazie systemów uznawanych za krytyczne to nie jedyny przykład różnic w pojmowaniu ochrony IK. Prowadzi to do wniosku, że sprawna realizacja założeń EPOIK wymaga stosowania wspólnego systemu pojęciowego i integralnych metod działania w zakresie rozpoznawania zagrożeń, na które podatna jest IK, przewidywania scenariuszy zdarzeń niekorzystnych i wskazywania modeli zabezpieczeń przed rozpoznanymi zagrożeniami. Obecnie stosowane przepisy prawne, zarówno UE jak i narodowe nie dostarczają jednolitego systemu pojęciowego i nie wskazują metod jakimi mają się posługiwać uczestnicy procesu zarządzania bezpieczeństwem IK planujący i realizujący ochronę IK.

Potrzeby metodyczne zarządzania bezpieczeństwem infrastruktury krytycznej

Analizując polskie oraz unijne postrzeganie IK można dojść do wniosku, że mimo różnic w definicyjnych IK akcentowane są słowa „niezbędność" i „podstawa". W obu przypadkach IK pojmowana jest w sposób systemowy „oznaczający układ powiązanych ze sobą elementów, mających określoną budowę, stanowiących całość i realizujących funkcjonalności wynikające z funkcji elementów składowych systemu oraz powiązań między nimi"[32]. Efektywność funkcjonowania systemu zależy od ustalonych powiązań występujących między elementami IK i poziomu dostępności funkcji realizowanych przez elementy systemu. Rozpoznanie powiązań oraz ustalenie poziomu funkcjonalności pozwala na określenie zbioru możliwych stanów w jakich system może się znajdować. Analiza tego zbioru pozwala na wskazanie stanów pożądanych, w których poziom realizowanych funkcjonalności zapewnia bezpieczne działanie instytucji państwowych i społeczeństwa. Możliwe jest również wskazanie stanów, niepożądanych. Zbiory stanów pożądanych, niepożądanych i pośrednich stanowią przestrzeń funkcjonowania systemu. Posiadając narzędzia do rejestracji stanów systemu IK możliwe jest śledzenie zmian zachodzących w systemie i przewidywanie sekwencji stanów prowadzących do sytuacji kryzysowych[33].

Sekwencję stanów systemu można pojmować jako „sekwencję zdarzeń inicjowaną przez wystąpienie pierwszego z nich, w której każde kolejne zdarzenie powoduje wystąpienie następnego. Efekt domina jest bezpośrednią przyczyną rozprzestrzeniania się zdarzeń kryzysowych oraz eskalacji ich skutków"[34]. Umiejętność obserwacji stanów systemu IK umożliwia zarządzanie bezpieczeństwem, zgodnie zasadą, że da się zarządzać tym co można zmierzyć.

Wiedza dotycząca powiązań między elementami systemu oraz poziomu funkcjonalności umożliwia podjęcie próby przewidzenia konsekwencji zakłócenia, awarii, utraty funkcjonalności fragmentu IK w stosunku do elementów zależnych. Wiedza ta jest konieczna aby zarządzać bezpieczeństwem IK jednak nie jest wystarczająca. Skuteczne zarządzanie bezpieczeństwem IK wymaga również wiedzy dotyczącej zagrożeń na jakie podatna jest IK. Dopiero połączenie wiedzy dotyczącej podatności na zagrożenia oraz wiedzy o organizacji systemu IK daje możliwość poszukiwania skutecznych metod ochrony IK.

Z przedstawionych rozważań wyłaniają się założenia dla procesu zarządzania bezpieczeństwem IK. Powinien on bazować na obserwacji funkcjonalności uznanych za podstawowe dla funkcjonowania państwa i społeczeństwa, które można nazwać krytycznymi. Wskazanie funkcjonalności pozwoli na rozpoznanie zasobów, które je realizują. Idąc dalej, wiedza o zasobach i ich funkcjach umożliwi

---

[32] Z. Bubnicki, *Podstawy informatycznych systemów zarządzania*, Wrocław 1993, s. 28.

[33] K. Maj, T. Krupa, *The Management Method Preventing a Crisis Situation in an Electrical Energy Utility.* Foundation of Management, vol. 2, nr 2, 2010, s. 37-50.

[34] A. Kosieradzka, J. Zawiła-Niedźwiecki (red.), *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym,* edu-Libri, Kraków 2016, s. 361.

wskazanie powiązań elementów systemu. Dzięki czemu odwzorowany zostanie model struktury analizowanego fragmentu IK. Wiedza o zasobach realizujących funkcjonalności krytyczne pozwoli na identyfikację zagrożeń, na które podatne są zasoby. Posiadając listę zagrożeń możliwe będzie wskazanie zestawu zabezpieczeń, których zastosowanie pozwoli osiągnąć lub utrzymać pożądany stan całego systemu. Proces zarządzania bezpieczeństwem bazujący na powyższych założeniach nazwano zarządzaniem sytuacyjnym bezpieczeństwem IK[35].

W związku z powyższym zasadną wydaje się hipoteza, że ochrona samych obiektów uznanych za IK jest niewystarczająca i należy w procesie zarządzania bezpieczeństwem IK kłaść nacisk przede wszystkim na ciągłość działania IK czyli utrzymanie dostępności funkcjonalności realizowanych przez zasoby uznane za krytyczne oraz szybkie odtwarzanie tej dostępności w przypadku uszkodzenia lub zniszczenia IK. Postawioną hipotezę zdaje się potwierdzać Komisja Europejska w dokumencie *Access to Essential Services*[36], w którym zaleca się zmianę kryteriów identyfikacji IK, na uwzględniające dostępności funkcji krytycznych.

Podsumowanie

Podsumowując artykuł należy zauważyć, że nastąpiła zmiana wiodącej kategorii zagrożeń wpływających na bezpieczeństwo narodowe i powodujących sytuacje kryzysowe z zagrożeń militarnych na niemilitarne.

Właściwa reakcja na sytuacje kryzysowe sprowadza się do rozpoznania zagrożeń, przygotowania planów reakcji na zagrożenia i zaangażowania odpowiednich sił i środków we właściwym czasie i miejscu, co wymaga skutecznej i efektywnej komunikacji i koordynacji na poziomie krajowym i UE pomiędzy wszystkimi zainteresowanymi stronami.

Efektywna komunikacja między podmiotami zaangażowanymi w proces zarządzania bezpieczeństwem IK jest zakłócana przez różne pojmowanie IK czego przykładem jest prawodawstwo UE i Polski. Zróżnicowane definiowanie IK skutkuje ogólnymi przepisami prawnymi i brakiem rekomendacji metodycznych w obszarze sporządzania poszczególnych części planów ochrony IK.

Metodyczne podejście do procesu zarządzania bezpieczeństwem IK powinno uwzględniać: funkcjonalności krytyczne; zasoby, które je realizują; zagrożenia, na które podatne są zasoby oraz zabezpieczenia przed rozpoznanymi zagrożeniami. Pozwoli to na lepsze zaspokojenie potrzeb społeczności uzależnionej od usług dostarczanych przez IK.

W związku z powyższym można wskazać trzy główne kierunki rozwoju zarządzania bezpieczeństwem IK:

1. Dalsza koncentracja działań zabezpieczających na zagrożeniach niemilitarnych.

---

[35] M. Wiśniewski, *Concept of Situational Management of Safety Critical Infrastructure of State*, Foundations of Management, volume 08, annual 16, 2016, s. 297-310.

[36] Access to Essentional Services, www.ec.europa.eu/priorities/publications/access-essential-services-european-pillar-social-rights_en, (15.12.2016).

2. Zmiana kryteriów wyznaczania IK na uwzględniające dostępność funkcjonalności IK.
3. Opracowanie systemu pojęć i metod zarządzania bezpieczeństwem IK możliwych do stosowania w dowolnym systemie IK.

Bibliografia:

Źródła literaturowe

Altas R., *21st Century Security and CPTED – Desining for Critical Infrastructure protection and crime prevention,* CRC Press, London – New York 2013.

AON, *Słownik terminów z zakresu bezpieczeństwa narodowego – wydanie szóste,* Akademia Obrony Narodowej, Warszawa 2008.

Brzozowska K., *Finansowanie inwestycji infrastrukturalnych przez kapitał prywatny na zasadzie Project finance,* Warszawa 2009.

Bubnicki Z., *Podstawy informatycznych systemów zarządzania*, Wrocław 1993.

Kąkol U., Kisilowski M., Kunikowski G., Uklańska A., *Diagnoza planowania cywilnego w procesie przygotowań obronnych*, [w:] *Współczesne koncepcje zarządzania publicznego. Wyzwania modernizacyjne sektora publicznego.* Fundacja Gospodarki i Administracji Publicznej, Kraków 2016.

Kosieradzka A., Zawiła-Niedźwiecki J. (red.), *Zaawansowana metodyka oceny ryzyka w publicznym zarządzaniu kryzysowym,* edu-Libri, Kraków 2016.

Kyriakides E., Polycarpou M., *ntellignet monitoring, control and security of critical infrastructure systems,* Springer, Berlin – Heidelberg 2015.

Lidwa W., Krzeszowski W., Więcek W., Kamiński P., *Ochrona infrastruktury krytycznej,* AON, Warszawa 2012.

Macaulty T., *Critical Infrastructure – Understandin its compnent parts, vulnerabilities, operating risk and interdependencies,* London – New York 2016.

Maj K., Krupa T., *The Management Method Preventing a Crisis Situation in an Electrical Energy Utility,* Foundation of Management, vol. 2, nr 2, 2010.

Radziejewski R., *Ochrona infrastruktury krytycznej – teoria a praktyka,* PWN, Warszawa 2014.

Ruktowski C., *Bezpieczeństwo i obronność: strategie – koncepcje – doktryny*, Warszawa 1995.

Skomra W. (red.), *Metodyka oceny ryzyka na potrzeby systemu zarządzania kryzysowego RP,* Warszawa 2015.

Stankiewicz W., *Bezpieczeństwo narodowe a walki niezbrojne*, *Studium*, Warszawa 1991.

Tyburska A., Nalepski M., *Ochrona infrastruktury krytycznej,* Szczytno 2008.

Wiśniewski M., Concept of Situational Management of Safety Critical Infrastructure of State. *Foundations of Management*, vol. 08, annual 16, 2016.

Wójtowicz W., *Bezpieczeństwo infrastruktury krytycznej,* Departament Polityki Obronnej MON, Warszawa 2006.

Akty prawne

Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie jej ochrony.

NPOIK 2015, Narodowy Program Ochrony Infrastruktury Krytycznej, RCB, Warszawa.

Ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym (Dz.U. 2007 nr 89 poz. 590).

Ustawie z dnia 22 sierpnia 1997 r. o ochronie osób i mienia (Dz.U. 1997 nr 114 poz. 740).

Źródła internetowe
Access to Essentional Services, www.ec.europa.eu/priorities/publications/access-essential-services-european-pillar-social-rights_en, (15.12.2016).
Korzeniowska S., *Cyberbezpieczeństwo infrastruktury Krytycznej*, LSW – Leśnodorski Ślusarek i Wspólnicy, www.lsw.com.pl, (29.08.2016).

Abstract

Development directions for critical infrastructure security management

This manuscript presents a synthesis of knowledge about of safety management of CI on the context of practices and regulations in Poland and the EU. The manuscript focuses on the relation of terms of national security, crisis management and CI. The differences in terminology were observed, which lead to different perceptions of CI. It affects to its identification and classification manner. The summary contains directions for development of safety management of CI.

Keywords: Critical Infrastructure, European Critical Infrastructure, emergency management, national security, protection of critical infrastructure, essential services