Mariusz Brzozowski*

Pełnomocnik do spraw ochrony infrastruktury krytycznej. Wybrane zagadnienia

Streszczenie

Infrastruktura krytyczna warunkuje przetrwanie, dobrobyt i rozwój wszystkich obywateli. Podstawowym celem jej ochrony jest utrzymanie ciągłości świadczenia nadrzędnych dla państwa usług. Zrozumienie roli i odpowiedzialności poszczególnych uczestników systemu infrastruktury krytycznej przy koordynacji działań to fundament skuteczności i trwałości tego mechanizmu. Operatorzy infrastruktury krytycznej to osoby posiadające najlepszą wiedzę na temat specyfiki i funkcjonowania danego obiektu/instalacji/urządzenia/usługi, a także warunki do eliminacji zagrożeń oraz minimalizacji ich skutków. Niniejszy artykuł został poświęcony podmiotom wyznaczanym do ochrony infrastruktury krytycznej, tj. osobie odpowiedzialnej za utrzymywanie kontaktów oraz pełnomocnikowi do spraw infrastruktury krytycznej.

Słowa kluczowe: infrastruktura krytyczna, zagrożenie, ochrona obiektów infrastruktury krytycznej, pełnomocnik do spraw ochrony infrastruktury krytycznej, zarządzanie kryzysowe, Narodowy Program Ochrony Infrastruktury Krytycznej

* Mgr inż. Mariusz Brzozowski, Wydział Prawa i Administracji, Uniwersytet Warmińsko-Mazurski w Olsztynie, e-mail: mariuszbrzozowskirr@wp.pl.

Wstęp

Sytuacja międzynarodowa związana z napaścią Federacji Rosyjskiej (FR) na Ukrainę sprawiła, że w przestrzeni medialnej bardzo dużo miejsca poświęca się zagrożeniom infrastruktury krytycznej (IK). Podkreśla się, że trzeba ją chronić za wszelką cenę, ale niewiele mówi się o tym, jakie zadania wykonują poszczególne osoby odpowiedzialne za ochronę rzeczonej infrastruktury. Dlatego uwaga przekazu skupia się na zagrożeniach, a nie na realizowanych przedsięwzięciach. Wobec tego należałoby uwypuklić bieżące działania podejmowane przez podmioty, które mają w swoich zasobach IK oraz służby i instytucje odpowiedzialne za ich ochronę. Warto podkreślić jak dużą rolę odgrywają obecnie ustanowione w polskim prawodawstwie osoby odpowiedzialnej za utrzymywanie kontaktu ze strony operatorów infrastruktury krytycznej z podmiotami odpowiedzialnymi za ochrony IK. Zgodnie z aktualnie obowiązującymi regulacjami prawnymi taką funkcję pełnią pełnomocnik do spraw ochrony IK oraz tzw. osoba wskazana do kontaktów. W czasie aktualnego zagrożenia zewnętrznego są one najważniejsze w organizacji bezpieczeństwa IK. Podejmowane przez m.in. pełnomocnika działania, czyli reakcja na wystąpienie zdarzenia (przekazanie odpowiednim służbom informacji, skierowanie w odpowiednie miejsce sił i środków itp.) w chwili wystąpienia niebezpieczeństwa, będą decydowały o skali ewentualnych skutków negatywnych dla infrastruktury krytycznej.

Bezpieczeństwo infrastruktury krytycznej zaczyna urastać do rangi bezpieczeństwa narodowego, dostęp zaś do podstawowych usług pozostaje wymiernym aspektem bezpieczeństwa narodowego i obowiązkiem państwa względem jego obywateli[1].

Główny cel badań prezentowanych w niniejszym artykule dotyczy identyfikacji misji i zadań pełnomocnika do spraw ochrony infrastruktury krytycznej RP oraz tzw. osoby wskazanej do kontaktów, przedstawienia obowiązków i uprawnień wyżej wymienionych oraz określenia pożądanych zmian w tym zakresie uwzględniających najnowsze rozwiązania legislacyjne przyjęte na gruncie regionalnym (UE). Główny problem badawczy wyrażono w postaci pytania: Jaką funkcję spełnia obecnie pełnomocnik do spraw ochrony infrastruktury krytycznej RP i tzw. osoba wskazana do kontaktów oraz jakie są aktualne

1 Więcej zob. Uchwała nr 67 Rady Ministrów z 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022", M.P. 2013, poz. 377, s. 27–28.

potrzeby i priorytety w zakresie weryfikacji zadań wyżej wymienionych w kontekście najnowszych rozwiązań legislacyjnych przyjętych przez prawodawstwo unijne? Podczas prowadzenia badań wykorzystano metody teoretyczne, w tym analizę i syntezę literatury przedmiotu.

Dlaczego w IK monitoring, nadzór, kontrola i koordynacja działań są tak ważne?

Jednym z najpoważniejszych zagrożeń bezpieczeństwa międzynarodowego jest neoimperialna polityka władz z Kremla. Federacja Rosyjska notorycznie podważa aktualny ład międzynarodowy oparty na prawie międzynarodowym, co służy realizacji jej mocarstwowych dążeń oraz powiększania strefy wpływów. Usilnie próbuje udowodnić, że tworzone przez Zachód sojusze (zwłaszcza znienawidzone przez Rosję NATO) czy choćby ich kooperacja bilateralna to czyste mrzonki, które stwarzają pozory kolosa, ale tak naprawdę jego nogi pozostają gliniane. W ostatnim czasie Rosja podważa traktaty i porozumienia rozbrojeniowe.

Ze względu na temat niniejszego artykułu nie chodzi o użycie siły militarnej czy aktywną antyzachodnią (w tym antypolską) propagandę. Należy skupić się na prowadzonych działaniach poniżej progu wojny (o charakterze hybrydowym), które oprócz tego, że niosą ryzyko wybuchu konfliktu na wielką skalę zagrażają właściwemu funkcjonowaniu państwa oraz zapewnieniu przetrwania (rozwoju) ludności cywilnej.

Jedną z form działań o charakterze hybrydowym jest wykorzystanie dostępnych sił i środków do zakłóceń w funkcjonowaniu IK, np. poprzez atak na jej elementy, w tym sieci łączności stacjonarnej i mobilnej będące fundamentem wymiany informacji, w tym w razie sytuacji kryzysowych.

Rozwój nowoczesnych technologii (zarówno cywilnych, jak i wojskowych) sprzyja wydłużaniu listy zagrożeń bezpieczeństwa. Wzrasta rola i realne wykorzystanie bezzałogowych i autonomicznych systemów, atrakcyjne okazuje się ingerowanie w systemy w sferze cyber, a także sięganie po bardziej drastyczne środki, np. systemy broni precyzyjnego rażenia.

To wszystko stanowi nie tylko prawdopodobne, lecz także jak najbardziej rzeczywiste niebezpieczeństwo dla IK, na którą składają się „[…] 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”[2]. Warto w tym miejscu przypomnieć, że są to systemy „[…] zaopatrzenia w energię, surowce energetyczne i paliwa; łączności; sieci teleinformatycznych; finansowe; zaopatrzenia w żywność; zaopatrzenia w wodę; ochrony zdrowia; transportowe; ratownicze; zapewniające ciągłość działania administracji publicznej; produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych”[3].

Zauważyć należy, że „[…] na sprawne i bezpieczne funkcjonowanie państwa wpływa niezakłócone działanie”[4] wyżej wymienionych systemów. „Za jej prawidłowe działanie i reagowanie na ewentualne zagrożenia odpowiadają przede wszystkim właściciele i posiadacze obiektów oraz wojewodowie i samorządy”[5], o czym więcej w dalszej części niniejszego artykułu.

Zagrożenia infrastruktury krytycznej mogą dotyczyć zabezpieczeń fizycznych, technicznych, osobowych, prawnych, ale i w sferze cybernetycznej. Zamierzone wrogie działania mogą mieć na celu nie tyle uszkodzenie czy zniszczenie, ile chociażby czasowe zakłócenie funkcjonowania. Może to być wyrazem stworzenia zagrożenia konkretnej funkcjonalności IK oraz ośmieszenia efektywności jej ochrony przez dane państwo. Akty dywersji, sabotaże nie są tylko częścią szpiegowskiej literatury. Stanowią planowe działania mające na celu zachwianie pozycji danego państwa (podmiotu) oraz jego wizerunku na arenie międzynarodowej.

W obecnej sytuacji – wykluczenie Federacji Rosyjskiej jako partnera strategicznego w dostawach surowców energetycznych – należy zachować szczególną czujność w kontekście niemilitarnych, ale spektakularnych ataków ze strony Kremla. Dotychczasowy potentat na rynku energetycznym nie ukrywa swojej złości, co jawnie pokazuje nieukrywane przez rosyjskie jednostki pływające zjawisko monitorowania i mapowania[6] przez nich posadowionych na dnie Bałtyku czy Morza Północnego elementów europejskiej morskiej IK[7].

2 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, Dz.U. 2022, poz. 261, z późn. zm., art. 3, pkt 2.

3 Ibidem.

4 A. Panasiuk, S. Sierański, *Ochrona obiektów infrastruktury krytycznej*, „Kontrola i Audyt” 2017, nr 1, s. 76–86.

5 Ibidem.

6 O tym w ostatnim czasie informowały media: gospodarskamorska.pl, Onet.pl, o2.pl, businessinsider.com.pl, rp.pl z 19 kwietnia 2023 roku, cytując słowa europejskich dziennikarzy i przedstawicieli służb specjalnych (Norwegia, Dania, Finlandia czy Szwecja).

7 Przez pojęcie „europejska infrastruktura krytyczna” należy rozumieć „[…] systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia i instalacje kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące

Nie należy zapominać o wydarzeniach z września 2022 roku, kiedy doszło do wybuchów na Nord Stream 1 i 2. Sabotaż, ataki terrorystyczne na morzu nie należą do częstych, niemniej jednak stanowią nie lada wyzwanie dla podmiotów odpowiedzialnych za zapewnienie bezpieczeństwa. Po wydarzeniach, które zbiegły się w czasie z oficjalnym otwarciem Baltic Pipe, rząd RP wprowadził wobec polskiej infrastruktury energetycznej mieszczącej się poza granicami Rzeczypospolitej Polskiej[8] drugi stopień alarmowy „Bravo"[9].

Reasumując, aktualna sytuacja bezpieczeństwa w regionie wraz z geostrategicznym położeniem Polski wymaga szczególnych wysiłków związanych z monitoringiem, nadzorem, kontrolą i koordynacją działań mających na celu ochronę ważnej z punktu widzenia bezpieczeństwa państwa infrastruktury.

Pełnomocnik do spraw ochrony infrastruktury krytycznej RP i tzw. osoba wskazana do kontaktów – charakterystyka ogólna na podstawie obowiązujących regulacji prawnych

Właściciele oraz posiadacze samoistni i zależni obiektów, instalacji, urządzeń i usług IK (tzw. operatorzy IK)[10] zostali zobligowani do ochrony wyżej wymie-

zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, wyznaczone w systemach, o których mowa w pkt 2 lit. a i h [a) zaopatrzenia w energię, surowce energetyczne i paliwa, b) łączności, c) sieci teleinformatycznych, d) finansowe, e) zaopatrzenia w żywność, f) zaopatrzenia w wodę, g) ochrony zdrowia, h) transportowe], w zakresie energii elektrycznej, ropy naftowej i gazu ziemnego oraz transportu drogowego, kolejowego, lotniczego, wodnego śródlądowego, żeglugi oceanicznej, żeglugi morskiej bliskiego zasięgu i portów, zlokalizowane na terytorium państw członkowskich Unii Europejskiej, których zakłócenie lub zniszczenie miałoby istotny wpływ na co najmniej dwa państwa członkowskie" – zob. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym…, art. 3, pkt 2a.

8 Gazociąg Baltic Pipe, podwodny kabel wysokiego napięcia prądu stałego SwePol.

9 Drugi stopień alarmowy można wprowadzić w razie zaistnienia zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, ale konkretny cel ataku nie został zidentyfikowany.
Prezes Rady Ministrów podpisał zarządzenia, które do 31 maja 2023 roku przedłużyły obowiązywanie trzech stopni alarmowych:
– trzeciego stopnia alarmowego CRP (3 stopień „Charlie-CRP") na całym terytorium RP – zarządzenie nr 18 z 24 lutego 2023 roku;
– drugiego stopnia alarmowego (2 stopień „Bravo") na całym terytorium RP – zarządzenie nr 19 z 24 lutego 2023 roku;
– drugiego stopnia alarmowego (2 stopień „Bravo") dla polskiej infrastruktury energetycznej poza granicami RP – zarządzenie nr 20 z 24 lutego 2023 roku.

10 Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, Dz.U. 2010, nr 83, poz. 541, par. 1.

nionych elementów, zwłaszcza w zakresie przygotowania i realizacji planów IK[11]. Sposób tworzenia, aktualizacji oraz struktura wyżej wymienionych planów, a także warunki i tryb uznania spełnienia obowiązku posiadania planu odpowiadającego wymogom planu ochrony IK zostały określone w rozporządzeniu Rady Ministrów z 30 kwietnia 2010 roku.

W gestii operatorów IK leży również obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami właściwymi do ochrony infrastruktury krytycznej oraz pełnomocnika do spraw ochrony infrastruktury krytycznej. Naturalnym zabiegiem, zgodnie z oczekiwaniem potencjalnego Czytelnika, jest w tym miejscu zdefiniowanie i rozróżnienie tych dwóch podmiotów.

Zgodnie z ustawą o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, w sektorze energetycznym[12], w odróżnieniu od pozostałych sektorów wchodzących w skład infrastruktury krytycznej, ustanowiono instytucję pełnomocnika do spraw ochrony infrastruktury krytycznej.

Podmiot ten jest powoływany (i odwoływany) przez zarząd spółki[13], w porozumieniu z ministrem właściwym do spraw aktywów państwowych oraz dyrektorem Rządowego Centrum Bezpieczeństwa (RCB)[14]. Pełnomocnik jest pracownikiem spółki monitorującym jej działalność w zakresie m.in.: rozporządzania składnikami mienia, rozwiązania spółki, zmiany przedmiotu

11 Plany te powinny zawierać np.: charakterystykę danego obiektu IK, specyfikę rzeczywistych i możliwych zagrożeń, opcjonalne scenariusze wdrażane w razie wystąpienia sytuacji kryzysowej (kryzysu).

12 Ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, Dz.U. 2020, poz. 2173, z późn. zm., art. 6, ust. 8.

13 Podmiot prowadzący działalność w sektorze energii elektrycznej, ropy naftowej oraz paliw gazowych, którego mienie (obiekty, instalacje i urządzenia) zostało ujawnione w jednolitym wykazie obiektów IK, zgodnie z kryteriami przyjętymi w Narodowym Programie Ochrony Infrastruktury Krytycznej. Należy zaznaczyć, że nie każdy strategiczny obiekt należy do infrastruktury krytycznej. Więcej zob. *Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity: uchwała nr 210/2015 Rady Ministrów z dnia 2 listopada 2015 r. w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej, z uwzględnieniem uchwały nr 116/2020 Rady Ministrów z dnia 13 sierpnia 2020 r. zmieniającej uchwałę w sprawie przyjęcia Narodowego Programu Ochrony Infrastruktury Krytycznej*, s. 13–14, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej [dostęp: 20.05.2023].

14 Ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych…, art. 5, ust. 1.

przedsiębiorstwa, przeniesienia siedziby za granicę[15]. Odpowiada za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony IK, a także ma prawo do uczestniczenia w posiedzeniach zarządu spółki oraz żądania od jej organów wszelkich dokumentów, informacji oraz wyjaśnień dotyczących spraw wskazanych powyżej[16]. Ponadto do zakresu jego zadań należy: 1) zapewnienie ministrowi właściwemu do spraw aktywów państwowych oraz ministrowi właściwemu do spraw energii informacji dotyczących dokonania przez organy spółki czynności prawnych (sprzeciw wobec podjętej przez zarząd spółki uchwały, m.in. rozporządzania składnikami mienia, rozwiązania spółki, zmiany przedmiotu przedsiębiorstwa spółki, przeniesienia siedziby spółki za granicę; przyjęcia planu rzeczowo finansowego, planu działalności inwestycyjnej lub wieloletniego planu strategicznego[17]); 2) przygotowywanie dla zarządu spółki oraz rady nadzorczej spółki informacji nt. ochrony IK; 3) zapewnienie zarządowi spółki doradztwa w zakresie funkcjonującej w spółce IK; 4) monitorowanie działalności spółki w zakresie ochrony IK; 5) przekazywanie informacji o IK dyrektorowi RCB (na wniosek ww.); 6) przekazywanie oraz odbieranie informacji o zagrożeniu IK we współpracy z dyrektorem RCB[18].

Ponadto do obowiązków pełnomocnika do spraw ochrony infrastruktury krytycznej należy przygotowanie dla zarządu spółki oraz rady nadzorczej raportu o stanie ochrony IK. Dokument jest sporządzany co kwartał bądź na żądanie zarządu spółki lub rady nadzorczej[19].

Powinien to być zbiór informacji traktujących o ochronie infrastruktury krytycznej dotyczących ochrony fizycznej, technicznej, prawnej, osobowej, teleinformatycznej oraz planów odbudowy i przywracania infrastruktury krytycznej do funkcjonowania[20].

Jeżeli raport jest niekompletny, zawiera nieścisłości bądź nie do końca ukazuje stan faktyczny kwestii w nim zawartych, to pełnomocnik do spraw ochrony infrastruktury krytycznej jest zobligowany, na wezwanie ministra właściwego do spraw aktywów państwowych albo ministra właściwego do spraw

15 Ibidem, art. 5, ust. 2.
16 Ibidem, art. 5, ust. 1, 5.
17 Jeżeli wykonanie takiej uchwały stanowiłoby, oczywiście realne zagrożenie funkcjonowania, ciągłości działania, a także integralności infrastruktury krytycznej.
18 Ibidem, art. 5, ust. 2.
19 Ustawa z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych…, art. 6, ust. 3.
20 Ibidem.

energii lub dyrektora RCB, do uzupełnienia raportu, co jest obwarowane stosownym zakresem i terminem[21].

Pełnomocnik do spraw ochrony IK sporządza również sprawozdanie kwartalne z wykonanych obowiązków, które składa ministrowi właściwemu do spraw aktywów państwowych, ministrowi właściwemu do spraw energii oraz dyrektorowi RCB[22].

Należy zauważyć, że sektor energetyczny, w przeciwieństwie do innych sektorów (np. sektora lotniczego), nie podlega regulacjom szczególnym, które odnosiłyby się do jego bezpieczeństwa. Dlatego w tej materii należy posługiwać się ogólnymi przepisami regulującymi kwestię ochrony infrastruktury krytycznej, takimi jak: 1) ustawa z 26 kwietnia 2007 roku o zarządzaniu kryzysowym wraz ze sporządzanym na jej podstawie Narodowym Programem Ochrony Infrastruktury Krytycznej; 2) ustawa z 22 sierpnia 1997 roku o ochronie osób i mienia; 3) ustawa z 18 marca 2010 roku o szczególnych uprawnieniach ministra właściwego do spraw aktywów państwowych oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych; 4) ustawa z 10 kwietnia 1997 roku – Prawo energetyczne.

W pozostałych sektorach wchodzących w skład infrastruktury krytycznej ustanowiono „osobę wskazaną do kontaktów". Zazwyczaj jest to osoba odpowiedzialna za ochronę w danym obiekcie infrastruktury krytycznej. Do jej obowiązków należy utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony IK. Powinna „[...] odbierać/przekazywać informacje o zagrożeniach dla danej IK i mieć techniczne możliwości realizacji tego zadania w trybie 24-godzinnym. Powinna również posiadać możliwie największą wiedzę o infrastrukturze krytycznej operatora i jej funkcjonowaniu"[23].

Wyznaczanie takiej osoby na stanowisko odbywa się na podstawie zapisu ustawy o zarządzaniu kryzysowym stanowiącym, że operatorzy IK mają obowiązek wyznaczyć, w terminie 30 dni od dnia otrzymania informacji o ujęciu obiektu w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład IK z podziałem na systemy, osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami właściwymi w sprawie ochrony infrastruktury krytycznej[24].

21 Ibidem, ust. 4.
22 Ibidem, ust. 5.
23 *Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity*, s. 16–17.
24 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym..., art. 6, ust. 5a.

Nie można również zapominać o wprowadzonej 5 lipca 2018 roku ustawie o krajowym systemie cyberbezpieczeństwa. Określa ona m.in. organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w jego skład[25].

Ze względu na ważność cyberbezpieczeństwa dla infrastruktury krytycznej z dużą dozą prawdopodobieństwa można powiedzieć, że operatorzy infrastruktury krytycznej zostali również uznani za operatorów usług kluczowych.

Ustawa przewiduje w tym zakresie zwolnienie operatora IK, który posiada zatwierdzony plan ochrony infrastruktury krytycznej, z obowiązku opracowania dokumentacji wymienionej w przedmiotowej ustawie. Jednocześnie wprowadzono zmiany do ustawy z 26 kwietnia 2007 roku o zarządzaniu kryzysowym. Zgodnie z nimi operatorzy infrastruktury krytycznej, którzy są jednocześnie operatorami usług kluczowych, powinni uwzględnić w planach ochrony infrastruktury krytycznej dokumentację dotyczącą cyberbezpieczeństwa jej systemów informacyjnych. Szczegółowe postanowienia dotyczące tej dokumentacji znajdują się w rozporządzeniu Rady Ministrów.

Powyższe oznacza konieczność ciągłego dostosowywania obowiązujących u operatora infrastruktury krytycznej procedur, w tym także opracowywania dodatkowej dokumentacji zgodnej z przepisami ustawy oraz rzeczonego rozporządzenia. Również i w tym zakresie ważną rolę odgrywają pełnomocnicy do spraw ochrony infrastruktury krytycznej, a także osoby wskazane do kontaktów.

Pełnomocnik do spraw ochrony infrastruktury krytycznej RP i tzw. osoba wskazana do kontaktów – zmiany w planowanej ustawie o ochronie ludności oraz o stanie klęski żywiołowej

„Sprawne funkcjonowanie państwa w dużej mierze jest zależne od poprawnego realizowania zadań przez odpowiednie podmioty administracji, które muszą być wykonywane nie tylko według ściśle określonych kompetencji i poziomu odpowiedzialności, ale także niezależnie od częstotliwości, istoty i charakteru wszelkich wyzwań i zagrożeń”[26].

25 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018, poz. 1560, art. 1.

26 G. Sobolewski, *Ochrona infrastruktury bezpieczeństwa państwa* [w:] *Ochrona infrastruktury bezpieczeństwa państwa*, red. G. Sobolewski, B. Michailiuk, I. Denysiuk, Warszawa 2019, s. 25.

Bardzo ważne dla funkcjonowania każdego systemu, a bezpieczeństwa w szczególności, są podstawy prawne[27].

Należy zwrócić uwagę, że aktualnie jest procedowany projekt z 31 sierpnia 2022 roku ustawy o ochronie ludności oraz o stanie klęski żywiołowej. Z dniem wejścia w życie rzeczonej ustawy traci moc m.in. ustawa o zarządzaniu kryzysowym, jednakże część jej przepisów została przeniesiona do aktualnie procedowanego projektu, w tym przepis ustanawiający osobę wskazaną do kontaktu. Planowana jest regulacja wskazanego przepisu w następującym brzmieniu: „Operator infrastruktury krytycznej wyznacza, w terminie 30 dni od dnia otrzymania informacji [o ujęciu obiektów, urządzeń, instalacji lub usług w wykazie obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, z uwzględnieniem podziału na poszczególne systemy], osobę odpowiedzialną za utrzymywanie kontaktów z Policją, Agencją Bezpieczeństwa Wewnętrznego oraz innymi właściwymi organami administracji publicznej”[28]. Należy nadmienić, że w wielokrotnie modyfikowanym projekcie nie wymieniono pełnomocnika do spraw infrastruktury krytycznej[29].

Wojna w Ukrainie wyraźnie pokazuje strategię realizowaną przez rosyjskiego agresora. Polega ona głównie na eliminacji sektora energetycznego, co ma doprowadzić do dysfunkcji państwa. Należy podkreślić znaczenie w ochronie IK zarówno pełnomocników do spraw ochrony IK, jak i osób wskazanych do kontaktów. W zaistniałej sytuacji osobom tym są stawiane szczególne zadania związane z sytuacją geopolityczną RP – jej trudnym położeniem na mapie świata oraz stosunkiem Federacji Rosyjskiej do Rzeczypospolitej Polskiej, co z racji bliskości prowadzonych przez rosyjskiego agresora działań wojennych nie pozostaje bez znaczenia.

Konstatując, należy wyraźnie podkreślić ciężar odpowiedzialności, jaki spoczywa na omawianych w niniejszym artykule podmiotach, ze względu na ich rolę w identyfikacji i monitorowaniu zagrożeń infrastruktury bezpieczeństwa państwa, od której uzależnione są: byt, przetrwanie i rozwój ludności cywilnej RP.

27 C. Guźniczak, S. Stempiński, *Zarządzanie kryzysowe. Doskonalenie procedur reagowania na przykładzie Gminy Miasta Szczecin*, Toruń 2021, s. 7.

28 Ustawa o ochronie ludności oraz o stanie klęski żywiołowej (projekt z dnia 8 listopada 2022 r.), art. 122, https://www.zpp.pl/storage/library/2022-11/5f2c5aa776a92ae03abd39d5097f45c1.pdf [dostęp: 25.05.2023].

29 Projektowanie ustawy mającej na celu uporządkowanie spraw związanych z obroną cywilną i ochroną ludności w RP to proces trwający od 2009 roku.

Pełnomocnik do spraw ochrony infrastruktury krytycznej RP i tzw. osoba wskazana do kontaktów – zmiany w innowacyjnych rozwiązaniach legislacyjnych UE (CER EU)

Od 2004 roku Rzeczpospolita Polska jest państwem członkowskich Unii Europejskiej. Przynależność do tak istotnej struktury ponadnarodowej wiąże się z wieloma korzyściami, ale i zobowiązaniami. Jednym z tych drugich jest to, że jako członek UE jest zobligowana do implementacji do polskiego porządku prawnego stanowionych unijnych rozwiązań legislacyjnych.

Komisja Europejska (KE) niejednokrotnie podkreślała potrzebę zapewnienia stosownego poziomu bezpieczeństwa infrastruktury krytycznej w państwach członkowskich. Pod koniec 2022 roku przyjęła nową dyrektywę Parlamentu Europejskiego i Rady w sprawie odporności podmiotów krytycznych (tzw. dyrektywa CER). Warto nadmienić, że jest ona spójna z niedawno przyjętą dyrektywą NIS 2 w sprawie bezpieczeństwa cybernetycznego.

Dyrektywa CER dotyczy dziesięciu sektorów, tj.: energii, transportu, bankowości, infrastruktury rynku finansowego, zdrowia, wody pitnej, ścieków, infrastruktury cyfrowej, administracji publicznej i przestrzeni kosmicznej[30].

Wskazano w niej m.in.: „Chociaż pewne środki istniejące na poziomie unijnym, takie jak europejski program ochrony infrastruktury krytycznej, i krajowym mają na celu wspieranie ochrony infrastruktury krytycznej w Unii, należy zrobić więcej, aby lepiej przygotować podmioty będące operatorami takiej infrastruktury do reagowania na ryzyko dla ich funkcjonowania, które mogłoby prowadzić do zakłóceń w świadczeniu usług kluczowych”[31]. Podkreślono, że „[...] należy również zrobić więcej, aby lepiej przygotować takie podmioty na dynamiczny krajobraz zagrożeń obejmujący m.in. ewolucję zagrożeń hybrydowych i terrorystycznych, i na rosnące współzależności między infrastrukturą a sektorami”[32].

Jeżeli więcej wymaga się od operatorów IK, to także większe oczekiwania będą od osób, którym powierzono zadania „osoby wskazanej do kontaktów”

30 Wcześniej obowiązująca 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 (Dz. Urz. UE 2008, L 345/75) dotyczyła wyłącznie energii i transportu.

31 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE, Dz. Urz. UE 2022, L 333/165.

32 Ibidem.

oraz pełnomocnika ds. ochrony IK. Profesjonalizm, znajomość specyfiki danego obiektu/instalacji/urządzenia/usługi, umiejętność wskazania zmian służących wzmocnieniu ich ochrony, weryfikacja zabezpieczeń i dążenie do udoskonalenia systemów ochrony jest sprawdzana podczas audytów. I tutaj pojawia się ważny problem, brakuje bowiem skutecznych metod weryfikacji, czy wskazane podczas kontroli nadzoru niedomagania zostały uwzględnione. To z kolei wynika z braku narzędzi w tym obszarze.

W efekcie przeprowadzonych w 2016 roku działań wynikających z zadań ustawowych Najwyższa Izba Kontroli (NIK) ujawniła wiele nieprawidłowości u skontrolowanych operatorów infrastruktury krytycznej, m.in.:

– „nie obejmowano ochroną fizyczną wszystkich obiektów infrastruktury krytycznej powiązanych ze sobą funkcjonalnie i niezbędnych do zapewnienia bezpieczeństwa funkcjonowania infrastruktury krytycznej,

– część terenów, na których znajdowały się obiekty infrastruktury krytycznej, nie była właściwie zabezpieczona przed wejściem osób nieuprawnionych, a w dużej części obszarów brakowało monitoringu wizyjnego,

– wejścia do niektórych obiektów nie spełniały norm bezpieczeństwa i nie były objęte systemem kontroli dostępu, a bramy wjazdowe nie były wyposażone w zapory zabezpieczające przed wtargnięciem,

– u większej części skontrolowanych podmiotów odpowiedzialnych za ochronę infrastruktury krytycznej nie wprowadzono rozwiązań na wypadek wystąpienia zdarzeń sabotażu lub wyrządzenia szkód przez pracowników na terenie obiektów infrastruktury krytycznej,

– we wszystkich skontrolowanych podmiotach nie wyodrębniono kluczowego, ze względu na przestrzeganie zasad bezpieczeństwa infrastruktury krytycznej, personelu,

– w znaczącej większości podmioty te nie określały też procedur umożliwiających sprawdzenie wybranego oferenta wykonującego usługi dla operatora infrastruktury krytycznej pod kątem jakości wykonywanych usług czy też zachowania poufności wykonywanych prac”[33].

Powyższe to przykład, który potwierdza, że wykrywanie deficytów bezpieczeństwa infrastruktury krytycznej ma miejsce, ale na ich wskazaniu zwykle się kończy, brak jest bowiem systemu nakazowego, obwarowanego sankcjami w razie niepodjęcia zalecanych działań.

33 *NIK o bezpieczeństwie infrastruktury krytycznej*, https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-obiektow-infrastruktury-krytycznej.html [dostęp: 1.06.2023].

To ma się zmienić w myśl zapisów zawartych w nowej dyrektywie CER. Zaostrzają one wymagania od podmiotów uznanych za krytyczne dotyczące przeprowadzania ocen ryzyka i sprawozdawczości. Co ważne (i w ocenie piszącego zbyt długo wyczekiwane), dyrektywa CER wprowadza możliwości nadzoru i kontroli (audytu) oraz sankcyjność. Otóż, do oceny, czy podmioty zidentyfikowane przez państwa członkowskie jako podmioty krytyczne wypełniają obowiązki ustanowione w dyrektywie, państwa członkowskie mają zapewnić właściwym organom uprawnienia i środki do „[…] przeprowadzania kontroli na miejscu w zakresie infrastruktury krytycznej oraz budynków i terenów wykorzystywanych przez podmiot krytyczny do świadczenia usług kluczowych oraz prowadzenia zdalnego nadzoru nad środkami stosowanymi przez podmioty krytyczne, także przeprowadzania lub zlecania audytów dotyczących podmiotów krytycznych”[34].

Państwa członkowskie zostały wskazane jako te, które „[…] ustanawiają przepisy dotyczące sankcji mających zastosowanie w przypadku naruszeń przepisów krajowych przyjętych na podstawie […] dyrektywy i podejmują wszelkie niezbędne środki w celu zapewnienia ich wykonywania”[35]. Podkreślono, że „[…] przewidziane sankcje muszą być skuteczne, proporcjonalne i odstraszające”[36].

Postulowane regulacje są ukierunkowane na zwiększenie odporności i poziomu bezpieczeństwa podmiotów wchodzących w skład IK państw członkowskich Unii Europejskiej. Nie bez przyczyny propozycja ma formę dyrektywy – ma to umożliwić uwzględnienie krajowych specyfik, współzależności sektorowych i transgranicznych. Projekt nowych unijnych ram odnoszących się do odporności IK obejmuje m.in. opis obowiązków właściwych organów, w tym wskazywanie podmiotów krytycznych.

Zapisy zawarte w przywołanym dokumencie powinny znaleźć odzwierciedlenie i rozwinięcie w polskich regulacjach prawnych.

W najnowszej „Strategii bezpieczeństwa narodowego RP” z 2020 roku w punkcie 2.7 wskazano wprost jako jeden z celów: „[…] zwiększyć odporność na zagrożenia przede wszystkim w zakresie: ciągłości rządzenia i funkcjonowania państwa, skutecznych dostaw energii, niekontrolowanego przepływu osób i relokacji ludności, gromadzenia, ochrony oraz zagospodarowania

34 Dyrektywa z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych…, art. 21.
35 Ibidem, art. 22.
36 Ibidem.

zasobów żywności i wody, zdolności do postępowania w przypadku wystąpienia zdarzeń o charakterze masowym, odpornych sieci telekomunikacyjnych i systemów teleinformatycznych, systemów informowania i ostrzegania ludności oraz wydolnego systemu transportowego"[37]. Punkt 2.8 nakazuje „[…] wdrożyć model ochrony infrastruktury krytycznej, polegający na zapewnieniu jej ciągłości działania oraz świadczonych przez nią usług"[38]. W przywołanym dokumencie strategicznym w punkcie 2.12 zalecono „[…] kontynuować wzmocnienie kontrwywiadowczego zabezpieczenia organów państwowych i infrastruktury krytycznej, adekwatnie do nasilającej się aktywności obcych służb wywiadowczych – zarówno w sferze wojskowej, jak i cywilnej"[39].

Słusznie zauważa Witold Skomra[40]: „[…] infrastrukturę krytyczną wyodrębniliśmy ponad 10 lat temu. W międzyczasie zmieniły się zagrożenia, kierunki dostaw gazu, ropy, węgla. Elementy składające się na łańcuch dostaw są dziś zupełnie inne niż 10 lat temu. W zasadzie należałoby zacząć wyznaczać infrastrukturę krytyczną od początku, zmieniając kryteria"[41]. Podobnie, w ocenie piszącego, należałoby podejść do jej zabezpieczenia, odpowiedzialności za nią, a zwłaszcza w kontekście nadzoru i kontroli tego rodzaju działań w celu weryfikacji ich efektywności, zbadania wiedzy, zaangażowania i możliwości stosownych podmiotów. Poprawa bezpieczeństwa rzeczywistych i cybernetycznych systemów IK, zdaniem piszącego, jest możliwa pod warunkiem wprowadzenia wyważonej sankcyjności. Taki zapis pojawił się w dyrektywie CER, co już zostało wcześniej zasygnalizowane.

Wprowadzając zmiany w przepisach dotyczących infrastruktury krytycznej, warto zastanowić się nad przyjęciem takich regulacji, które nie ograniczałyby osoby do kontaktu przed podejmowaniem trudnych decyzji w chwili zagrożenia. Dlatego odpowiedzialność nie może paraliżować działań.

37 *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, Warszawa 2020, s. 16.
38 Ibidem.
39 Ibidem.
40 Ekspert w dziedzinie zarządzania kryzysowego, szef Wydziału Ochrony Infrastruktury Krytycznej w Rządowym Centrum Bezpieczeństwa.
41 Cyt. za: D. Mikołajczyk, *Ustawa o ochronie ludności sprzeczna z unijną wizją odporności infrastruktury krytycznej*, https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/ustawa-o-ochronie-ludnosci-sprzeczna-z-unijna-wizja-odpornosci-infrastruktury-krytycznej [dostęp: 11.06.2023].

Zakończenie

Napaść zbrojna Federacji Rosyjskiej na niepodległą Ukrainę – państwo sąsiadujące z Polską i przez nią mocno wspierane – oraz obserwowane zabiegi Rosjan skupiających swoje wysiłki na uderzeniach w IK sprawiają, że należy powiedzieć wprost, że ochrona polskiej i europejskiej infrastruktury krytycznej stanowi jedno z głównych zadań stojących przed RP. Pozostaje też nie lada wyzwaniem dla państwa polskiego.

W związku z wojną rosyjsko-ukraińską od 2022 roku, a co za tym idzie koniecznością wzmocnienia bezpieczeństwa energetycznego w rezultacie zintensyfikowanych działań o charakterze szantażu energetycznego wiele państw zadeklarowało wprost bądź pośrednio rezygnację z surowców energetycznych oferowanych przez Rosję. Uwzględniając sytuację geopolityczną, specyfikę systemu energetycznego RP i planowanych nowoczesnych rozwiązań oraz wskazane wyżej zapotrzebowanie na energię również z innych państw, Polska ma nadzieję wykorzystać szansę wybicia się na jednego z głównych graczy w łańcuchu dostaw surowców energetycznych dla regionu. Stąd też należy mieć na uwadze zagrożenie zrealizowanych i planowanych na tym gruncie inwestycji.

Należy podkreślić, że istota ochrony infrastruktury krytycznej polega nie tylko na zapewnieniu jej ochrony przed rzeczywistymi i możliwymi zagrożeniami, lecz także na tym, żeby ewentualne uszkodzenia czy zakłócenia w jej funkcjonowaniu były możliwie jak najkrótsze, żeby nie pociągały za sobą kolejnych strat w gospodarce RP i bezpieczeństwie jej obywateli.

„W Polsce, podobnie jak i w innych krajach, działająca sprawnie i w sposób niezakłócony infrastruktura krytyczna ma coraz większy wpływ na obywateli, struktury administracji i gospodarkę”[42]. Dlatego ochrona infrastruktury krytycznej powinna być procesem mającym na celu ochronę ciągłości świadczenia danej usługi oraz możliwie szybkie jej odtworzenie w razie awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie, a także głównym zadaniem operatora IK, państwo zaś powinno ograniczać się do pełnienia funkcji koordynująco-nadzorującej. Należy mieć na uwadze, że jakakolwiek ingerencja czy wsparcie są możliwe wówczas, gdy likwidacja skutków

42 *Narodowy Program Ochrony Infrastruktury Krytycznej – tekst jednolity*..., s. 4.

zaistniałego zdarzenia przekracza możliwości (siły i środki) określonego właściciela/posiadacza samoistnego i zależnego obiektu/instalacji/urządzeń/usług[43].

Stąd też kierowniczą rolę powinna odgrywać kompatybilna współpraca podmiotów, które są rzeczywiście (zobligowane ustawowo) odpowiedzialne za podjęcie działań ukierunkowanych na zminimalizowanie ryzyka zakłócenia funkcjonowania IK. Ważnymi ogniwami w tym łańcuchu są pełnomocnicy ds. ochrony infrastruktury krytycznej oraz tzw. osoby wskazane do kontaktów.

Należy mieć na uwadze, że to człowiek stanowi najbardziej kruche ogniwo użytkowania IK – czy to jako operator czy jako użytkownik. Dlatego warto sobie zdawać sprawę z ważności poruszanego w niniejszym artykule tematu oraz konieczności nadzoru nad wykonywaniem ustawowych obowiązków ochrony infrastruktury krytycznej i kontroli ich realizacji.

Przyjmowane na terytorium RP rozwiązania prawne powinny uwzględniać kontekst obecności Polski w Unii Europejskiej. Uzupełnienie w ustawie o zarządzaniu kryzysowym zapisów na temat europejskiej infrastruktury krytycznej pokazuje, że wyzwania stojące przed operatorami IK mają wymiar ponadnarodowy. Należy mieć na uwadze jak ważne jest zapewnienie bezpieczeństwa łańcucha dostaw i jakie niepożądane wielosektorowe i transgraniczne skutki gospodarcze i społeczne może nieść jego zakłócenie.

Bibliografia

Guźniczak C., Stempiński S., *Zarządzanie kryzysowe. Doskonalenie procedur reagowania na przykładzie Gminy Miasta Szczecin*, Toruń 2021.

Mikołajczyk D., *Ustawa o ochronie ludności sprzeczna z unijną wizją odporności infrastruktury krytycznej*, https://infosecurity24.pl/bezpieczenstwo-wewnetrzne/ustawa-o-ochronie-ludnosci-sprzeczna-z-unijna-wizja-odpornosci-infrastruktury-krytycznej [dostęp: 11.02.2023].

NIK o bezpieczeństwie infrastruktury krytycznej, https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-obiektow-infrastruktury-krytycznej.html [dostęp: 1.02.2023].

Panasiuk A., Sierański S., *Ochrona obiektów infrastruktury krytycznej*, „Kontrola i Audyt" 2017, nr 1.

Sobolewski G., *Ochrona infrastruktury bezpieczeństwa państwa* [w:] *Ochrona infrastruktury bezpieczeństwa państwa*, red. G. Sobolewski, B. Michailiuk, I. Denysiuk, Warszawa 2019.

43 Zob. Uchwała Nr 67 Rady Ministrów z dnia 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022", M.P. 2013, poz. 377, załącznik, s. 24.

The Plenipotentiary for Critical Infrastructure Protection. Selected Issues

Abstract

Critical infrastructure determines the survival and well-being of all citizens. The main purpose of its protection is to maintain the continuity of providing key services for the state. The mission and responsibility of CI participants, coordination of activities are very important things. Understanding this is the basis for the effectiveness and sustainability of this system. CI operators are people with the best knowledge about the specifics and functioning of critical infrastructure items (facility/installation/device/service). They also have the conditions to eliminate threats and reduce their negative effects. In this article provides space for entities designated to protect CI, i.e. the person responsible for maintaining contacts and the plenipotentiary for critical infrastructure.

Key words: critical infrastructure (CI), threat, protection of critical infrastructure items, plenipotentiary for critical infrastructure, crisis management, The National Programme for Critical Infrastructure Protection