Akademia WSB
Dąbrowa Górnicza, Cieszyn, Olkusz, Żywiec, Kraków

Wydział Nauk Stosowanych

mgr Mariusz Staszczak

Bezpieczeństwo i odporności infrastruktury krytycznej w kontekście współczesnych zagrożeń

Autoreferat pracy doktorskiej napisanej pod kierunkiem:

dra hab. Zbigniewa Mikołajczyka, prof. ucz.

Promotor pomocniczy:
dr inż. Cezary Sochala

Dąbrowa Górnicza 2024

Spis treści

1. Przesłanki wyboru tematu pracy

Populacja Europy przywykła do życia w warunkach pokoju. Mamy zapewniony dostęp do mediów i szeregu usług publicznych. Standardem stało się korzystanie z dorobku techniki w postaci komputerów, telefonów mobilnych czy Internetu oraz wielu innych rozwiązań technologicznych. Wszystkie te standardy i udogodnienia uwarunkowane są funkcjonowaniem infrastruktury państwa[1], której kluczowymi elementami są urządzenia, instalacje i systemy wchodzące w skład infrastruktury krytycznej (IK). Z formalnego punktu widzenia, ochrona tej infrastruktury w Polsce stanowi element zarządzania kryzysowego.

Położenie geopolityczne Polski sprawia, że jest ona krajem buforowym NATO i UE. Przy tym, zasadniczym zagrożeniem bezpieczeństwa europejskiego pozostaje Federacja Rosyjska, która dysponuje znacznym potencjałem do prowadzenia działań zagrażających IK we wszystkich wymiarach i domenach jej funkcjonowania. Dość jednoznacznie dowodzą tego wydarzenia ostatnich dekad. Rosja nieustannie prowadzi działania sabotażowe, a także dokonuje ataków w cyberprzestrzeni. Są one wymierzone w funkcjonowanie infrastruktury krytycznej (elektrownie, sieci przesyłowe, koleje) państw NATO i UE. Rosja finansuje też grupy hakerskie w państwach trzecich, np. *UNC1151/Ghostwriter* czy *Digital Shadows/Conti*. Z raportu Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ang. *European Union Agency for Cybersecurity* – ENISA) wynika, że od wybuchu obecnej fazy wojny na Ukrainie wzrosło zagrożenie dla rządów, przedsiębiorstw i kluczowych sektorów, takich jak energetyka, transport, bankowość i infrastruktura cyfrowa. Raport *Microsoft* stwierdza z kolei, że w okresie luty – maj 2022 r. Rosja przeprowadziła cyberataki w 42 państwach (poza Ukrainą), których głównym celem były agencje rządowe (49%) oraz instytucje zarządzające infrastrukturą krytyczną (19%). Najczęściej atakowana była Polska (8% przypadków) i państwa bałtyckie (w sumie 14%). Mimo że państwa NATO prowadzą nasilone działania mające na celu zwiększenie fizycznej ochrony infrastruktury krytycznej, Rosja nadal ma potencjał do prowadzania ataków i działań sabotażowych Mogą na to wskazywać eksplozje rurociągów *Nord Stream 1* i *Nord Stream 2*. W tym celu, podobnie jak w cyberprzestrzeni,

[1] Infrastruktura państwa to część infrastruktury obejmująca obiekty, urządzenia stałe i instytucje usługowe niezbędne do należytego funkcjonowania produkcyjnych działów gospodarki oraz życia (w tym bezpieczeństwa) ludności kraju.

Rosja może posługiwać się obywatelami państw trzecich[2]. Poza atakami cybernetycznymi Rosjanie dokonują również ataków kinetycznych, których konsekwencjami są ciągłe awarie systemu energetycznego Ukrainy. Uszkodzeniom ulega większość elektrowni i elektrociepłowni. Zniszczone zostają obiekty służby zdrowia. Opisane ataki doprowadzają także do przerwy w dostawach ciepła i wody, gdyż wstrzymana zostaje praca elektrowni atomowych, cieplnych i wodnych, jak również do paraliżu transportu kolejowego.

Możliwe jest dalsze nasilenie cyberataków oraz aktów sabotażu i terrorystycznych wymierzonych w infrastrukturę krytyczną oraz teleinformatyczną, których celem będzie sparaliżowanie kluczowych usług w państwie. Tego rodzaju działania będą m.in. zwiększać poczucie zagrożenia wojennego i testować zdolności obronne państw członkowskich Unii Europejskiej i NATO. Istotne będzie też rozwijanie kompetencji społecznych i instytucjonalnych w zakresie reagowania na cyberzagrożenia, zwłaszcza związane z funkcjonowaniem infrastruktury krytycznej. Ataki na infrastrukturę lub sama groźba ich przeprowadzenia są nieodłącznym elementem strategii działań hybrydowych.

W obecnej sytuacji geopolitycznej w bezpośrednim otoczeniu Polski zagrożenia działaniami hybrydowymi, które mogą być wymierzone w polską infrastrukturę krytyczną – w postaci np. ataków cybernetycznych, terrorystycznych lub rozpoznania obiektów IK prowadzonych przez obce służby specjalne (w celu dokonania sabotażu lub dywersji) – są jak najbardziej realne.

W związku z powyższym celowym było podjęcie badań nad ochroną infrastruktury krytycznej w Polsce. W ich ramach dokonano przeglądu obecnie obowiązujących procedur w zakresie ochrony IK, zarówno w czasie pokoju, jak i wojny, a ponadto poddano analizie działania wiodących instytucji odpowiedzialnych za ochronę IK. Zidentyfikowano również najważniejsze zagrożeń, które odnoszą się do IK. Ponadto podjęto próbę zoptymalizowania obecnego sytemu ochroni IK w świetle postanowień dyrektywy CER[3].

[2] A.M. Dyner, *Działania hybrydowe Rosji przeciw państwom NATO i UE, „*Biuletyn PISM" R. 2022, nr 183 (2602). Strona internetowa: https://www.pism.pl/publikacje/dzialania-hybrydowe-rosji-przeciw-panstwom-nato-i-ue, dostęp: 14.02.2023 r.

[3] *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* (Tekst mający znaczenie dla EOG) PE/51/2022/REV/1, Dz.U. L 333, 27.12.2022, s. 164-198.

2. Cele pracy i hipotezy badawcze

Celem badań było poznanie uwarunkowań i doświadczeń w zakresie ochrony infrastruktury krytycznej w Polsce – w ujęciu współczesnym i perspektywicznym.

Badania zmierzały do rozwiązania głównego problemu badawczego (GPB), który został wyrażony pytaniem: W jakim zakresie obecny system ochrony infrastruktury krytycznej zapewnia odpowiedni poziom ochrony obiektów, instalacji i urządzeń i usług wchodzących w skład infrastruktury krytycznej w aspekcie ich zagrożeń?

Na podstawie wstępnych studiów literatury przedmiotu sformułowano następujące szczegółowe problemy badawcze (SPB):

1. W jakim stopniu system zarządzania kryzysowego determinuje sprawne funkcjonowanie ochrony IK?
2. Jak instytucje państwowe zajmujące się ochroną IK spełniają swoje funkcję?
3. Jakie zagrożenia w największym stopniu determinują ochronę IK?
4. W jakim zakresie obecne założenia teoretyczne spełniają wymagania ochrony IK podczas pokoju, kryzysu i wojny?
5. W jakim kierunku ewoluuje europejski i krajowy system ochrony IK?

Hipotezy badawcze

Na potrzeby procedury badawczej przyjęto wstępną hipotezę badawczą: System ochrony infrastruktury krytycznej w Polsce zapewnia w dużym stopniu ochronę obiektów, instalacji, urządzeń i usług wchodzącym w skład IK. Natomiast jeżeli dokonane zostaną zmiany organizacyjno-prawne, system ten w pełni umożliwi ochronę tej infrastruktury w przyszłości. W konsekwencji szczegółowym hipotezom badawczym (SHB) nadano następującą postać.

Hipoteza 1. Obecny system zarządzania kryzysowego zapewnia warunki do sprawnego funkcjonowania systemu ochrony IK poprzez uregulowania zawarte w ustawie o zarządzaniu kryzysowym na rzecz ochrony IK m.in. poprzez.:

a) ujmowanie zagrożeń dla IK w Krajowym Planie Zarządzania Kryzysowego;
b) ujmowanie zagrożeń dla IK w Raporcie o zagrożeniach bezpieczeństwa narodowego;
c) tworzenie Narodowego Programu Ochrony Infrastruktury Krytycznej;

d) konieczność sporządzania jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy;
e) wymóg tworzenia planów ochrony infrastruktury krytycznej;

Hipoteza 2. Zakresy odpowiedzialności instytucji biorących udział w procesie ochrony IK nie są właściwie określone i wymagają poszerzenia kompetencji m.in. o kontrolno-nadzorcze dla Rządowego Centrum Bezpieczeństwa w stosunku do operatorów IK.

Hipoteza 3. Na podstawie analizy przypadków oraz międzynarodowych uwarunkowań bezpieczeństwa do najpoważniejszych zagrożeń dla niezakłóconego funkcjonowania IK należy zaliczyć zagrożenia ze stronu obcych służb specjalnych, terrorystyczne, cybernetyczne, informacyjne, jak również te związane z użyciem bezzałogowych statków powietrznych;

Hipoteza 4. Obecnie w Polsce istnieją rozwiązania pozwalające na ochronę obiektów IK w czasie pokoju i wojny, a wynikają one m.in. z ustawy o zarządzaniu kryzysowym, ustawy ochronie osób i mienia, a także z ustawy o obronie Ojczyzny oraz aktów wykonawczych ww. ustaw. Jednakże są one stosowanie w ograniczonym stopniu;

Hipoteza 5. Największą zmianą w podejściu do ochrony IK determinuje wejście w życie dyrektywy CER, która wprowadza wiele nowych rozwiązań w zakresie IK. Zapisy powyższej dyrektywy powinny zostać zaimplementowane do polskiego prawodawstwa najpóźniej do 17 października 2024 r. Obecny projekt ustawy o ochronie ludności nie implementuje zapisów dyrektywy CER, natomiast ma być do niej dostosowywany.

3. Przebieg badań i struktura pracy

Według definicji Stefana Nowaka metody badawcze to przede wszystkim typowe, powtarzalne sposoby zbierania, opracowywania, analizy i interpretacji danych empirycznych, służące do uzyskania maksymalnie uzasadnionych odpowiedzi na stawiane w nich pytanie[4]. Natomiast Józef Pieter pojęcie metody rozumie szeroko i zalicza do niej wszystkie procesy, które zachodzą w trakcie badań naukowych od momentu powstania problemu do jego jakościowego i ilościowego opracowania wyników[5].

[4] Por. S. Nowak, *Metodologia badań społecznych,* Warszawa 1985, s.22.
[5] Por. J. Pieter, *Ogólna metodologia pracy naukowej*, Wrocław 1967, s. 70.

Organizacja procesu badawczego przebiegła według poniższego schematu:

- etap wstępny, w ramach którego dokonano wyboru tematu, następnie określono cel badań oraz ogólny problem badawczy jak również szczegółowe problemy badawcze, a następnie sformułowano do nich główną hipotezę badawczą oraz szczegółowe hipotezy badawcze, a także zweryfikowany został zakres badań w ujęciu przedmiotowym i podmiotowym oraz wybrane zostaną metody i techniki badawcze,
- etap zasadniczy polegał na przeprowadzeniu badań właściwych,
- etap końcowy polegał na opracowaniu zebranego w trakcie badań materiału, a następnie poddaniu go analizie w celu zweryfikowania przyjętych hipotez oraz pisemnego opracowania wyników badań.

W trakcie procesu badawczego wykorzystano różne metod i technik badawcze, a podstawowym kryterium ich doboru była racjonalizacja przebiegu badań, jak również możliwość uzyskania obiektywnych wyników. Prowadzenie badań odbywało się z zastosowaniem teoretycznych oraz empirycznych metod badawczych, które wykorzystane zostały właściwie do rozwiązań problemów.

Rozwiązanie podjętego problemu badawczego, jak również zweryfikowanie postawionej głównej hipotezy badawczej wymagało wykorzystania następujących metod badawczych:

- analizy, w tym: analizy literatury, analizy instytucjonalno-prawnej, historycznej, porównawczej, systemowej oraz analizy i konstrukcji logicznej; analizie zostały poddane rozwiązania prawne (ustawy, rozporządzenia, zarządzenia decyzje) i rozwiązania organizacyjne (strategie, systemy, relacje między systemami oraz ich elementami, procedury, a także wytyczne oraz inne dokumenty) związane z ochroną IK;
- syntezy dla łączenia w całość wyodrębnionych i zbadanych wcześniej elementów, dla uogólnienia faktów wynikających z zebranego materiału, między innymi do formułowania osądów dotyczących przedmiotu badań;
- wywiadu nieustrukturyzowanego z osobami, które mają doświadczenie w ochronie infrastruktury krytycznej, do ustalenia trendów i rozwiązań, także zagrożeń i wyzwań stojących prze operatorami infrastruktury krytycznej;
- badania ankietowego na potrzeby którego użyto narzędzia badawczego w postaci kwestionariusza ankiety. W przypadku wątpliwości pojawiających się w ankiecie

przeprowadzono również, w ramach doprecyzowania wywiad celowy (bezpośredni) z ekspertami z instytucji i służb zajmujących się problematyką ochrony infrastruktury krytycznej.

Na potrzeby badania ankietowego oraz wywiadu wykorzystane zostały narzędzia w postaci kwestionariusza ankiety oraz wywiadu, co pozwoliło osiągnąć cel badawczy i zweryfikować założoną hipotezę roboczą; w jego części informacyjnej ankietowani zostali poinformowani o charakterystyce zagadnienia oraz celu badań; pytania będą miały zarówno charakter otwarty, jaki i zamknięty, a sposób odpowiedzi na zadane w ankiecie pytania pozwalał na zachowanie anonimowości udzielanych odpowiedzi; umożliwiono też udzielnie odpowiedzi z podaniem danych osobowych.

W celu osiągnięcia złożonego procesu badawczego wykorzystane zostały następujące materiały źródłowe:

- prace badawcze, referaty i publikacje naukowe;
- dostępna literatura przedmiotu;
- Internet;
- opracowania historyczne;
- inne opracowania i materiały źródłowe w zależności od potrzeb;
- wywiady z ekspertami.

Celem badania opinii respondentów było poznanie opinii dotyczącej funkcjonowania systemu infrastruktury krytycznej poprzez ekspertów, którzy w zakresie pracy zawodowej lub naukowej zajmują się w szczególności ochroną infrastruktury krytycznej. Badaniem objęto również ekspertów posiadających ugruntowaną wiedzę z zakresu działalności o tożsamych lub analogicznym charakterze w stosunku do ochrony IK: ochrony obiektów podlegających obowiązkowej ochronie oraz zagadnień związanych z przygotowaniem obiektów infrastruktury krytycznej na czas wojny. W związku z tym w badaniu udział wzięły zarówno osoby ze środowiska naukowego, jak i praktycy z instytucji cywilnych i wojskowych. Pytania skierowane do ekspertów odnosiły się do szeroko rozmienianego sytemu ochrony IK, a w szczególności będą dotyczyły:

- próby zidentyfikowania najważniejszych zagrożeń dla obiektów IK, a w konsekwencji wyzwań w zakresie ochrony obiektów, instalacji i urządzeń oraz usług wchodzących w skład IK,
- oceny sprawności działania instytucji odpowiedzialnych za ochronę IK,

- dokonania przeglądu rozwiązań prawno-organizacyjnych na czas pokoju oraz wojny zapewniających ochronę obiektów, instalacji i urządzeń wchodzących w skład IK oraz porządnych kierunków ich doskonalenia,
- zidentyfikowania konieczności ustanowienia nowych rozwiązań organizacyjnych w postaci np. aktów prawnych, które w istotnym stopniu wpłyną na podniesienie poziomu bezpieczeństwa IK,
- uszeregowania systemów IK najbardziej podatnych na działania mogące prowadzić do ich uszkodzenia,
- gradacji zagrożeń dla IK, które w chwili obecnej charakteryzują się największym prawdopodobieństwem wystąpienia,
- wyłonienia instytucji, która po implementacji zapisów dyrektywy CER powinna odgrywać pierwszoplanowe znacznie w ochronie IK.

Badanie realizowane zostało poprzez przesłanie ankiety ekspertom za pomocą poczty elektronicznej, a w przypadku konieczności doprecyzowania zagadnień lub rozbieżności przeprowadzono rozmowy z ekspertami w ramach wywiadu.

W procesie badawczym udział wzięło dwudziestu ekspertów. Wytypowanych ekspertów podzielić można na grupy obejmujące:

- sześciu żołnierzy (w tym dwóch byłych) zajmujących się w swojej pracy zawodowej m.in. kwestiami zarządzania kryzysowego;
- cztery osoby zwiane są bezpośrednio z pracą naukowo-dydaktyczną dotyczącą kwestii poruszanych w rozprawie;
- dwie osoby zajmujące się kwestiami zarządzania kryzysowego oraz ochrony IK na szczeblu starostwa powiatowego;
- sześć osób (w tym trzy piastują stanowiska kierownicze) zajmujących się kwestiami zarządzania kryzowego oraz ochrony IK w ministerstwach i urzędach centralnych (w tym jedna z nich jest ekspertem w zakresie ochrony osób i mienia, a kolejna ekspertem w zakresie zagrożeń militarnych);
- jedną osobę będącą funkcjonariuszem Policji;
- jedną osobę będącą funkcjonariuszem Państwowej Straży Pożarnej.

Powyżsi eksperci dobierani byli z możliwe wszystkich działów administracji publicznej. Przyjęto założenie, że będą to osoby reprezentujące wszystkie możliwe podmioty zajmujące się bezpośrednio lub pośrednio ochroną infrastruktury krytycznej, w związku z czym do badań zaproszono ekspertów podejmujących zawodowo

problematykę zarządzania kryzysowego, w tym ochrony infrastruktury krytycznej reprezentujących m.in. Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Obrony Narodowej, Dowództwo Generalne Rodzajów Sił Zbrojnych, Wojska Obrony Terytorialnej, Rządowe Centrum Bezpieczeństwa, Straż Pożarną, Policję, Żandarmerię Wojskową. Ponadto oprócz osób zawodowo zajmujących się ochroną IK, w badaniach wzięli udział również przedstawiciele środowisk naukowych reprezentujący m.in. Akademię Sztuki Wojennej oraz Akademię Policji w Szczytnie.

Praca rozpoczyna się od rozdziału o charakterze metodologicznym. W rozdziale tym dokonano wprowadzenia w problematykę, uzasadniono potrzebę podjęcia badań nad nią, określono przedmiot i cele badań, główny problem badawczy i problemy szczegółowe, główną hipotezę badawczą i hipotezy szczegółowe, a także opisano ich organizację i przebieg. Przedstawiono w nim również metody, techniki i narzędzia badawcze wykorzystane w trakcie prowadzenia badań.

Rozdział drugi zawiera rozważania teoretyczne na temat przedmiotu pracy. Przedstawiono w nim funkcjonujący obecnie w Polsce od 2007 r. system zarządzania kryzysowego na szczeblu centralnym, wojewódzkim oraz samorządowym. Zaprezentowano również system ochrony infrastruktury krytycznej oraz opisano wchodzący w jego skład Narodowy Program Ochrony Infrastruktury Krytycznej. Wyodrębniono także podrozdział opisujący mechanizm sporządzania planów ochrony infrastruktury krytycznej.

Kolejny rozdział prezentuje analizę instytucjonalnego sytemu bezpieczeństwa infrastruktury krytycznej. Dokonano w nim przeglądu najważniejszych instytucji odpowiadających za bezpieczeństwo IK, a ponadto omówiono system antyterrorystyczny RP, w tym system stopni alarmowych i stopni alarmowych CRP, oraz przedstawiono kwestie związane z krajowym systemem cyberbezpieczeństwa.

Rozdział czwarty skupia się na przeglądzie współczesnych zagrożeń, na które mogą być obecnie podatne obiekty, urządzenia i instalacje wchodzące w skład infrastruktury krytycznej. Na podstawie powyższego przeglądu poddano analizie zagrożenia, które mogą wystąpić w stosunku do IK, a ich działanie może prowadzić do dysfunkcji obiektów, instalacji i urządzeń wchodzących w skład IK strony. Szczegółowo zostały opisane zagrożenia mogące wystąpić ze strony obcych służb specjalnych, terrorystyczne, występujące w cyberprzestrzeni, informacyjne oraz związane z użyciem bezzałogowych statków powietrznych. Scharakteryzowano też wybrane przypadki

ataków na ukraińską IK oraz kwestie uszkodzeń gazociągów Nord Stream 1 i Nord Stream 2.

Rozdział piąty poświęcony został rozwiązaniom wzmacniającym ochronę IK, przewidzianym na czas pokoju, zewnętrznego zagrożenia państwa oraz wojny. Opisano w nim szczegółowo procedury wynikające z ustawy o ochronie osób i mienia oraz przepisy dotyczące obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, jak również przedstawione zagadnienie militaryzacji.

Rozdział szósty przedstawia planowane rozwiązania z zakresu infrastruktury krytycznej, które muszą zostać wdrożone do polskiego porządku prawnego poprzez implementację zapisów dyrektywy CER dotyczącej odporności podmiotów krytycznych. Zaprezentowane zostały również nowe rozwiązanie dla infrastruktury krytycznej, które przewiduje projekt ustawy o ochronie ludności oraz o stanie klęski żywiołowej.

Rozprawę zamyka zakończenie, które zawiera wnioski zebrane po analizie wszystkich rozdziałów pracy, a także ocenę osiągniętego celu i założeń badawczych. Rozdział zawiera również prezentację wniosków z weryfikacji hipotez – wyników końcowych z przeprowadzonych badań.

Uzupełnieniem rozprawy jest bibliografia, w której zawarto zestawienie materiałów źródłowych wykorzystanych w toku procesu badawczego, oraz załączniki, wśród których znalazły się: kwestionariusz ankiety/wywiadu z ekspertami, a także streszczenie wyników badań ich opinii.

4. Wyniki badań w kontekście hipotez badawczych

W aspekcie pierwszej szczegółowej hipotezy badawczej potwierdzono, że obecnie obowiązujący system zarządzania kryzowego w Polsce daje możliwość przygotowania się na sytuacje kryzysowe, a w przypadku ich wystąpienia – na reagowanie na nie oraz na odbudowę zniszczonej infrastruktury krytycznej. W ramach ustawy o zarządzaniu kryzysowym istnieją określone procedury i wykonywane są cyklicznie dokumenty planistyczne, które pozwalają na odpowiednie funkcjonowanie systemu ochrony IK. Do powyższych dokumentów należy zaliczyć: Krajowy Plan Zarządzania Kryzysowego, Raport o zagrożeniach bezpieczeństwa narodowego, Narodowy Program Ochrony Infrastruktury Krytycznej, Wykaz przedsięwzięć i procedur systemu zarządzania kryzysowego z uwzględnieniem zobowiązań wynikających z członkostwa w Organizacji Traktatu Północnoatlantyckiego, Plany ochrony

infrastruktury krytycznej. Natomiast w opinii autora, jak również z wyników przeprowadzonych badań wynika, że należy wybrać z NPOIK najważniejsze zapisy dotyczące kwestii bezpieczeństwa, tzw. minimalne zabezpieczenia, które musi spełniać każdy obiekt IK, i przenieść je do rangi np. rozporządzenia w sprawie planów ochrony IK lub nawet zawrzeć je ustawie o zarządzaniu kryzysowym. Zasadnym byłoby także dokonanie gradacji ważności systemów IK oraz przeprowadzenie ich podziału na kategorie ważności. Wynika to z faktu, że nie każdy obiekt IK musi stosować wszystkie wyśrubowane zapisy NPOIK, a mógłby je stosować w jakiejś części. W związku z tym zasadny wydaje się podział obiektów IK na kategorie i dopasowanie do każdej kategorii minimalnych wymagań dotyczących zapewnienia im bezpieczeństwa.

Uzyskane wyniki badań pozwoliły również na potwierdzenie drugiej hipotezy, w której wskazano, że zakresy odpowiedzialności instytucji biorących udział w procesie ochrony IK nie są do końca właściwie określone i wymagają poszerzenia kompetencji m.in. o kontrolno-nadzorcze dla Rządowego Centrum Bezpieczeństwa w stosunku do operatorów IK. Należy stwierdzić, że RB spełnia swoją funkcję, ale uprawnienia tej instytucji są mocno ograniczone i nie przystają do dzisiejszych oczekiwań w dobie gwałtownych kryzysów w rejonie Europy Środkowo-Wschodniej, jak również zamieniających się uwarunkowań prawnych wynikających z prawa unijnego. RCB jest przede wszystkim instytucją zajmującą się przekazywaniem i gromadzeniem informacji dotyczących sytuacji kryzysowych, brak jej uprawnień kontrolno-nadzorczych w stosunku operatorów IK. Zapisy dyrektywy CER jasno wskazują, że podmiot krytyczny niewywiązujący się ze swoich obowiązków, który dorowadził do zakłócenia usługi kluczowej, zostanie ukarany. Obecnie nie ma takich możliwości, gdyż zgodnie z zapisami NPOIK funkcjonuje podejście bezsankcyjne do operatorów IK. Wypełniając przepisy dyrektywy, należy powołać podmiot, który będzie uprawiony do dokonywania kontroli, audytów i nakładania kard administracyjnych. W chwili obecnej w Polsce nie ma instytucji posiadającej takich uprawnień, więc należy powołać nową instytucję lub poszerzyć uprawniania RCB. W chwili obecnej najszybszym sposobem na podniesienia rangi RCB do miana naczelnego organu administracji rządowej (obecnie RCB posiada status jednostki budżetowej) byłyby postawienie na jej czele ministra bez teki, który jest jedocześnie członkiem rządu w randze ministra, a nie kieruje żadnym resortem, tylko zajmuje się wykonywaniem zdań powierzonych przez premiera. Minister tzw. zadaniowy jest zarówno naczelnym organem administracji rządowej, jak i częścią organu kolegialnego, czyli Rady Ministrów.

Przeprowadzone badania pozwoliły również na zweryfikowanie trzeciej hipotezy, w której potwierdzono, że na terytorium Polski istnieje zwiększone zagrożenie wystąpieniem zdarzenia o charakterze terrorystycznym, jednak jego celu nie da się dokładnie określić, a także innymi zagrożeniami w postaci cyberataków lub rozpoznania obiektów IK przez obce służby specjalne. W związku z tym jest to czas szczególny dla operatorów IK, którzy powinni wdrożyć w życie wszystkie przewidziane na tę okoliczność procedury m.in. wynikające z aktów wykonawczych do ustawy antyterrorystycznej i zacieśnić współpracę ze służbami odpowiadającymi za zapewnienie bezpieczeństwa IK. Powyższa współpraca powinna opierać się na współdziałaniu w zakresie wymiany informacji nt. cyberataków wymierzonych w IK oraz najlepszych praktyki ich odparcia, analizy ryzyka i podatności, w celu identyfikacji punktów narażonych na atak. Należy dokonać właściwych zabezpieczeń IK przed penetracją w celu rozpoznania przed atakiem dywersyjnym. Powyższe skłania również do refleksji nad odpowiedzią na pytanie, jakiego rodzaju zagrożenia możemy się spodziewać oraz jakie obiekty IK mogą być celem ataku. Obecnie działania, których jesteśmy świadkami, przede wszystkim mają charakter wywiadowczy. Są prowadzone przez służby specjalne Rosji i Białorusi, które aktywnie rozpoznają obiekty IK, o czym świadczą zatrzymania dokonywane przez polskie służby. Równoległe do zagrożeń fizycznych i osobowych, poważne zagrożenia dla systemów IK stanowią cyberataki. Według wydanego w przez CSIRT GOV Raportu o stanie cyberbezpieczeństwa RP, w 2021 r. najczęściej atakowanym sektorem była infrastruktura krytyczna. Analizując współczesne zagrożenia dla systemów i obiektów IK, można wytypować trzy fazy ataku na obiekt IK. W pierwszej napastnik dokonuje testowania sytemu bezpieczeństwa danego obiektu poprzez np. rozpoznanie dronem. Najprostszą formą sprawdzenia sytemu IT jest przesłanie e-maila z zainfekowaną zwartością, a następnie sprawdzenie reakcji ochrony na robienie zdjęć obiektu itp. Kolejną fazą jest już próba sabotażu wobec obiektu poprzez świadomą ingerencję. Natomiast ostatnią fazą jest już atak kinetyczny na obiekt IK.

Próba zweryfikowania czwartej szczegółowej hipotezy badawczej również zakończyła się powodzeniem, gdyż potwierdzono, że w Polsce istnieją rozwiązania prawne dotyczące ochrony IK na czas pokoju, a są to tzw. ochrona obowiązkowa, która wynika z ustawy o ochronie osób i mienia, oraz ochrona infrastruktury krytycznej, o której mowa w ustawie o zarządzaniu kryzysowym są przygotowywane i prowadzone są czasie pokoju. Natomiast na czas wojny jest to Szczególna ochrona obiektów, która jest przygotowywana w trakcie pokoju, a prowadzona będzie w przypadku ogłoszenia

mobilizacji oraz w czasie wojny. Obecnie obowiązujące przepisy dotyczące ochrony IK w czasie pokoju wynikają z ustawy o ochronie osób i mienia oraz ustawy o zarzadzaniu kryzysowym. Powyższe regulacje zapewniają prowadzenie działań ochronnych w obiektach IK zarówno w czasie pokoju, jak również w przypadku wystąpienia sytuacji kryzysowej. Jednak w przypadku zewnętrznego zagrożenia bezpieczeństwa państwa i w czasie wojny nie mają zastosowania. Konkludując, żeby obiekty IK miały zapewniony odpowiedni poziom bezpieczeństwa w czasie wojny, niezbędne jest ich umieszczenie w wykazie obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa. Gdyby znaleziono wspólny mianownik dotyczący tego, jaka jest ta koncepcja ochrony wszystkich tych grup powyższych obiektów, można by było doprowadzić do zebrania wszelkich przepisów dotyczących ich ochrony i wydać na ich podstawie jeden akt prawny, który będzie dotyczył ochrony tych obiektów w czasie pokoju oraz wojny.

Na potwierdzenie piątej hipotezy szczegółowej należy wskazać, że wejście w życie dyrektywy CER zmieni przede wszystkim sposób wyłaniania infrastruktury krytycznej z obecnie obowiązującego podejścia obiektowego na podejście usługowe. Oznacza to, że nie będzie konieczności włączania całego obiektu do wykazu IK, ale będzie możliwość umieszczenia w nim pojedynczej usługi, która jest krytyczna dla danego operatora IK. Zgodnie z zapisami dyrektywy CER prace nad jej wdrożeniem należy rozpocząć od wyłonienia usług kluczowych, a kolejno ustalić operatorów tych usług. Każdy operator będzie zobowiązany do przeprowadzenia analizy ryzyka, a gdy zakres zakłóceń dla danej usługi będzie przekraczał określone normy, taki operator zostanie wskazany jako krytyczny. Operatorzy uznani za krytycznych będą musieli wskazywać infrastrukturę, za pomocą której realizują usługę kluczową. W kontekście nowych przepisów należy również zwrócić uwagę na odejście od zasady bezsankcyjnego podejścia do operatorów IK, ponieważ dyrektywa zakłada nakładanie kar dla zarządców IK, którzy nie wywiązali się z zapewnienia właściwej ochrony zarządzanych przez siebie podmiotów krytycznych wchodzących w skład IK. Idąc dalej, dyrektywa nakłada również obowiązek zlecania i prowadzenia audytów. Powyższe niewątpliwie oznacza, że należy powołać nowy organ lub nadać uprawnienia już działającej instytucji do przeprowadzania kontroli i możliwości nakładania kar administracyjnych na operatorów IK, którzy nie dopełnili obowiązków. W tym miejscu należy zaznaczyć, że obecnie Rządowe Centrum Bezpieczeństwa, w którym znajduje się wydział ochrony infrastruktury krytycznej koordynujący kwestie związane z ochroną IK, nie posiada takich uprawnień. Kolejną kwestią, która jest swoistym novum w ochronie IK, a została ona uregulowana

w przepisie art. 10, jest wsparcie państw członkowskich dla podmiotów krytycznych. Określone ramy tej pomocy są dość szerokie i dotyczą nawet przekazania zasobów finansowych. Według opinii RCB podmioty krytyczne będą mogły liczyć na wsparcie finansowe ze strony państwa, jeśli będzie to uzasadnione bezpieczeństwem publicznym. Takie wsparcie nie będzie traktowane jako niedozwolona pomoc publiczna[6]. Należy zauważyć, że w chwili obecnej państwo nie ma obowiązku wsparcia finansowania ochrony operatorów IK. Rozwiązanie dotyczące wsparcia operatorów IK przez państwa należy ocenić pozytywnie, szczególnie w obliczu ciągłych prób destabilizacji rynku energetycznego UE, którego przykładem mogą być choćby działania sabotażowe wobec gazociągów Nord Stream 1 oraz Nord Stream 2.

Proces badań zmierzał do zweryfikowania przyjętej głównej hipotezy badawczej, która został wyrażony pytaniem: *W jakim zakresie obecny system ochrony infrastruktury krytycznej zapewnia odpowiedni poziom ochrony obiektów, instalacji i urządzeń i usług wchodzących w skład infrastruktury krytycznej w aspekcie ich zagrożeń?* Na podstawie wyników przeprowadzonych badań należy stwierdzić, że w znacznej mierze obecny system spełnia wymogi zapewnia odpowiedniego poziom ochrony IK, ale ciągle musi być udoskonalany, a dodatkowo w obliczu postanowień dyrektywy CER dotyczącej odporności podmiotów krytycznych powyższy system musi zostać znacząco przebudowany. Przesłankami, które przemawiają za tym, że obecny system ochrony IK daje rękojmię zachowania poziomu ochrony IK zapewniającego jej sprawne działanie, jest choćby fakt funkcjonowania ustawy o zarzadzaniu kryzysowym, na mocy której wydawane są dokumenty planistyczne zapewniającego ochronę IK. Obecny system oczywiście nie jest pozbawiony słabych stron, takich jak choćby bezsankcyjne podejście do niewypełnienia zapisów NPOIK. W obowiązującym porządku prawnym funkcjonuje zbyt wiele aktów prawnych zawierających problematykę ochrony infrastruktury krytycznej, przez co operatorzy są zmuszeni do wykonywania wielu planów ochrony IK, np. wynikających z ustawy o zarzadzaniu kryzysowym, ustawy o ochronie osób i mienia, ustawy o obronie ojczyzny czy ustawy o krajowym systemie cyberbezpieczeństwa. Mnogość aktów powoduje rozmycie odpowiedzialności za ochranę IK. W związku z tym konieczne wydaje się powołanie zespołu roboczego na szczeblu ponadresortowym, który podejmie prace nad powstaniem nowego aktu

[6] Por. *Dyrektywa CER – dyrektywa o odporności podmiotów krytycznych*. Strona internetowa: https://www.gov.pl/web/rcb/dyrektywa-cer--dyrektywa-o-odpornosci-podmiotow-krytycznych, dostęp: 30.05.2023 r.

prawnego, konsolidującego ochronę IK w czasie pokoju oraz wojny. Celowe jest powołanie instytucji w randze centralnego organu administracji rządowej, która będzie koordynować kwestie ochrony IK. Instytucja ta musi posiadać szerokie uprawnienia do nadkładania kar w drodze decyzji administracyjnych, jak również do kontroli operatorów IK w drodze audytu. Musi również posiadać odpowiednie zatrudnienie gwarantujące właściwą realizację zadań w zakresie ochrony IK, żeby móc dokonywać uzgodnień planów IK nie tylko w formie korespondencyjnej, lecz także porównań zapisów zawartych w planach IK ze stanem faktycznym. Dobitnym przykładem, który świadczy o tym, że system IK znacznej mierze zapewnia odpowiedni poziom bezpieczeństwa obiektom IK, lecz nie w pełni, jest wypowiedź byłego dyrektora RCB, który podczas posiedzenia sejmowej podkomisji stałej do spraw zarządzania kryzysowego 7 marca 2023 r. stwierdził, że na 125 operatorów IK, 85% z nich ma zatwierdzony plan ochron IK.

5. Wnioski z badań

Przeprowadzone badania dotyczyły szeroko rozumianej problematyki ochrony infrastruktury krytycznej w Polsce. Na podstawie przeprowadzonych badań sformułowano następujące wnioski.

Po pierwsze obecnie ukształtowany system zarządzania kryzysowego w RP oraz główna jego funkcja związana w praktyce z przygotowaniem i reagowaniem na sytuacje kryzysowe odnosi się do podejmowania działań w odpowiedzi na zagrożenia niemilitarne (naturalne, techniczne oraz spowodowane intencjonalną działalnością człowieka). Ustawa o zarządzaniu kryzysowym powstała w związku z koniecznością wypełnienia luki pomiędzy stanami funkcjonowania państwa czasu pokoju i czasu wojny oraz w uzupełnieniu konstytucyjnych stanów nadzwyczajnych i stała się elementem prawodawstwa ingerującego w obszar bezpieczeństwa powszechnego. Jednym z ważnych elementów systemu ochrony IK jest obowiązek sporządzania przez operatorów planów Ochrony IK, które w swojej zawartości wyczerpują wiele elementów w zakresie prowadzenia ochrony IK. Ten obowiązek poszerza świadomość operatorów o ważności ochrony IK. Co należy podkreślić, w obecnym systemie ochrony IK brak przepisów prawnych nakładających obowiązek czy ujednolicających poziom zabezpieczenia obiektów. Narodowy Program Ochrony Infrastruktury Krytycznej oraz dobre praktyki i rekomendacje są tylko dokumentami pomocniczymi i mają formę

wskazówek. Kryteria, które mają służyć jej wyodrębnieniu[7] nie są na tyle precyzyjne, że pozwalają na jej właściwe wyselekcjonowanie. Konieczne jest jednak w tym miejscu zaznaczenie, że kryteria te służą jedynie wyodrębnieniu infrastruktury krytycznej w skali ogólnopaństwowej – szczebla krajowego – która służy jego sprawnemu funkcjonowaniu. Pomija się w tym względzie infrastrukturę krytyczną poziomu wojewódzkiego, powiatowego czy gminnego.

Po drugie do 2014 r. (inwazja Rosji) największymi zagrożeniami infrastruktury krytycznej były zagrożenia obszaru środowiskowego, zagrożenia obszaru technologicznego oraz zagrożenia obszaru danych i sieci, natomiast obecnie najważniejszym zagrożeniem jest zagrożenie obszaru czynnika ludzkiego (terroryzm, kradzież, niezadowolenie obywateli lub pracowników, nieświadome, szkodliwe działanie wynikające z niewiedzy, brak polityki bezpieczeństwa oraz nierealistyczne regulacje prawne lub luki prawne, brak wykwalifikowanej kadry menadżerskiej oraz brak szkoleń i ćwiczeń zgrywających wiele podmiotów odpowiedzialnych za bezpieczeństwo narodowe oraz brak kampanii uświadamiającej zagrożenia). Do głównych zagrożeń w obecnych uwarunkowaniach międzynarodowych należałoby zaliczyć przede wszystkim działania dywersyjno-sabotażowe (np. działanie inspirowanej przez Federację Rosyjską siatki monitorujących ruch na lotnisku w Rzeszowie-Jasionce i na szlakach kolejowych), co jest związane z zaangażowaniem Polski w pomoc wojskową Ukrainie. Nie należy wykluczyć przeprowadzenia kinetycznych ataków (być może nawet pod fałszywą flagą) wymierzonych w obiekty IK. Prowadzenie działań od wewnątrz jest równie istotne, co działania zewnętrzne.

Po trzecie obecne rozwiązania związane z ochroną IK wymagają zmian systemowych, a przede wszystkim ujednolicenia i usprawnienia całego procesu ochrony i obrony obiektów, urządzeń i obszarów istotnych dla bezpieczeństwa państwa i zabezpieczenia funkcjonowania ludności cywilnej oraz usług dostarczanych tym podmiotom. Kluczową kwestią wydaje się być ujednolicenie problematyki, która jest zawarta m.in. w ustawie o zarządzaniu kryzysowym, ustawie o ochronie osób i mienia, przepisach wydanych na podstawie ustawy o obronie Ojczyzny. Ochrona IK w czasie pokoju nie jest tożsama z jej ochroną i obroną w czasie wojny. Ochrona infrastruktury

[7] Chcę podkreślić, że w mojej ocenie, z legalistycznego punktu widzenia, kryteria wyodrębniania zawarte w art. 6a ustawy *o zarządzaniu kryzysowym* odnoszą się do Europejskiej Infrastruktury Krytycznej. Natomiast w ocenie Rządowego Centrum Bezpieczeństwa, co znalazło odzwierciedlenie w *Narodowym Programie Infrastruktury Krytycznej*, kryteria te mają zastosowanie również do wyodrębniania krajowej infrastruktury krytycznej.

krytycznej nie mieści się w pojęciu zarządzania kryzysowego. Wypracowane dotychczas rozwiązania obejmujące problematykę szczególnej ochrony, po dokonaniu uporządkowania w obszarze legislacyjnym, powinny znaleźć zastosowanie w odniesieniu do obiektów infrastruktury bezpieczeństwa narodowego[8], zarówno w stanie stałej gotowości obronnej państwa, jak i w sytuacji zewnętrznego zagrożenia bezpieczeństwa państwa, w tym spowodowanego działaniami terrorystycznymi, a także zbrojnej napaści na terytorium RP, w razie szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego oraz w innych sytuacjach określonych w aktach normatywnych wydanych przez organy właściwe w sprawach obronności i bezpieczeństwa państwa. Ich ochrona powinna być prowadzona przez zmilitaryzowane w tym celu jednostki we wszystkich czterech kategoriach, tj. obronności, gospodarki i transportu, bezpieczeństwa cywilnego oraz innych ważnych interesów i zasobów państwa[9].

Po czwarte ustawa o zarządzaniu kryzysowym nie rozróżnia ochrony IK w czasie pokoju i w czasie wojny. Z formalno-prawnego punktu widzenia, jeżeli obiekt IK nie znalazł się w wykazie obiektów szczególnie ważnych dla bezpieczeństwa lub obronności państwa, to nie zostanie objęty działaniami ochronnymi i obronnymi prowadzonymi przez jednostki zmilitaryzowane oraz Siły Zbrojne RP, o których mowa w ustawie o obronie Ojczyzny. Biorąc pod uwagę powyższe, należy stwierdzić, że obecne rozwiązania wprowadzone ustawą o obronie Ojczyzny pozwalają na zapewnienie ochrony i obrony obiektów IK, pod warunkiem ich uwzględnienia w wykazie, o którym mowa powyżej. Należy zaznaczyć, że pojęcie IK nie występuje bezpośrednio w ustawie o obronie ojczyzny, natomiast zawiera ona pojęcie obiektów podlegających szczególnej ochronie. Porównując obiekty podlegające szczególnej ochronie, należy zwrócić uwagę, że w większości są to tożsame obiekty, które możemy sklasyfikować jako IK. Należałoby zastanowić się nad rozwiązaniem, już przyjętym w ustawie o ochronie osób i mienia, która zawiera zapis wskazujący, że wszystkie obiekty znajdujące się w wykazie IK są jednocześnie obiektami podlegającymi obowiązkowej ochronie, i przyjąć zapis, że obiekty znajdujące się na wykazie IK są jednocześnie obiektami podlegającymi szczególnej ochroni

Po piąte IK ze względu na swoją ważną specyfikę mogłaby być w ogóle wyseparowana z zarządzania kryzysowego i rzeczywiście rozprowadzona odrębnym

[8] Pojęcie to rozwijam w odpowiedzi na dalsze pytania.
[9] Por. R. Wróbel, *System ochrony infrastruktury bezpieczeństwa narodowego*, s. 305.

aktem prawnym o randze ustawy. Natomiast obecnie należy skupić się bardziej – w przypadku ewentualnej zmiany zapisów dotyczących ochrony IK – na wprowadzeniu mechanizmów sprawdzających operatorów IK, w takim zakresie, w jakim ten operator dba o bezpieczeństwo IK, z uwzględnieniem tych przypadków, które dotyczą dysfunkcji IK, np. na przestrzeni ostatniego roku, dwóch czy pięciu lat.

Po szóste należy również pamiętać, że ustawa o działaniach antyterrorystycznych wprowadziła do ustawy o ochronie osób i mienia zmianę, zgodnie z którą do obszarów, obiektów i urządzeń „podlegających obowiązkowej ochronie" należą: obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi ujęte w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej. W omawianym zagadnieniu wskazanie to jest niezwykle istotne, gdyż wprowadza chaos w aktualnym porządku prawnym. Zastosowany przez ustawodawcę zabieg przypisujący jedną ze zdefiniowanych legalnie kategorii pojęciowych – infrastruktura krytyczna – do drugiej – „obiekt podlegający obowiązkowej ochronie" – budzi uzasadnione wątpliwości. Zastanawia również przyjęcie takiego założenia, tym bardziej, że – jak zostało wskazane powyżej – kategoria „obiektów podlegających obowiązkowej ochronie" z punktu widzenia przedmiotu ochrony jest kategorią węższą. Zauważyć również trzeba, że ustawa o ochronie osób i mienia odnosi się do urządzeń, obiektów, obszarów i transportów, podczas gdy ustawa o zarządzaniu kryzysowym wskazuje, że IK tworzą systemy, w skład których wchodzą powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi. Wprowadzenie tej zmiany legislacyjnej budzi również zastrzeżenia od strony praktycznej, ponieważ zakres ochrony w przypadku IK, a w szczególności procedura uzgadniania planu ochrony oraz zakres form ochrony, są dużo bardziej rozbudowane. Dlatego też zasadne jest wprowadzenie regulacji prawnych mających charakter unifikujący. Postulowanym kierunkiem jest wprowadzenie jednej kategorii pojęciowej „infrastruktura bezpieczeństwa narodowego". Tym samym zasadna jest unifikacja obecnie funkcjonujących kategorii pojęciowych: „infrastruktura krytyczna", „obiekty podlegające obowiązkowej ochronie", „obiekty podlegające szczególnej ochronie".

Po siódme podsumowując wyniki badań ankietowych, systemy infrastruktury krytycznej, które zdają się być najbardziej narażone na działania mające na celu ich uszkodzenie to według respondentów systemy zaopatrzenia w energię, surowce energetyczne i paliwa (zdecydowanie tak - 85%), sieci teleinformatyczne (zdecydowanie

tak - 65%), łączność (zdecydowanie tak - 30%)[10].Z kolei systemy, które zdają się być najmniej narażone, to zaopatrzenie w żywność, zaopatrzenie w wodę oraz transportowe.

Po ósme podsumowując wyniki badań ankietowych, respondenci wskazali, że zagrożeniami, które są najbardziej prawdopodobne do wystąpienia w stosunku do infrastruktury krytycznej to cyberataki (zdecydowanie tak - 85%), kampanie dezinformacyjne (zdecydowanie tak – 55), użycie bezzałogowych statków powietrznych (zdecydowanie tak – 50%), działalność obcych służb specjalnych (zdecydowanie tak – 30%), zamach terrorystyczny (zdecydowanie tak – 15%).

Po dziewiąte podczas przeprowadzonych badań ankietowani odpowiadali na pytanie, jaka instytucja powinna być odpowiedzialna za ochranę infrastruktury krytycznej po wejściu w życie dyrektywy CER. Według respondentów najwłaściwszą instytucją pozostaje niezmiennie Rządowe Centrum Bezpieczeństwa, na drugim miejscu uplasowała się Agencja Bezpieczeństwa Wewnętrznego (zdecydowanie tak - 30%), natomiast na trzecim miejscu respondenci wskazali konieczność utworzenia nowej instytucji (zdecydowanie tak - 20%) odpowiadającej *sensu stricto* za ochronę IK.

6. Kierunki dalszych badań

Rezultatem rozprawy jest ocena obecnego systemu ochrony infrastruktury krytycznej w Polsce. Powyższa ocena umożliwiła zaproponowanie rozwiązań służących zwiększaniu zapewnienia bezpieczeństwa infrastruktury krytycznej w Polsce. Najważniejsze kierunki zmian, jakie należy wykonać w opinii respondentów, to:

- określenie organu odpowiedzialnego za całościowy nadzór nad problematyką utrzymywania IK w kraju,
- określenie terminów obowiązkowych ćwiczeń organów i elementów instytucji zaangażowanych w ochronę IK,
- zwiększenie środków finansowych z budżetu państwa na budowę, utrzymywanie i zabezpieczenie prawidłowego funkcjonowania IK, w tym zadań związanych z jego ochroną,
- możliwość nakładania kar finansowych na operatorów IK,
- instytucja lub instytucje nadzorujące IK muszą mieć status organu,

[10] Wyniki badań ankietowych opracowane zostały na podstawie skali Likerta.

- postulowane byłoby wyłączenie rozwiązań dotyczących ochrony infrastruktury krytycznej, jak również instytucji pełnomocnika do spraw ochrony infrastruktury krytycznej do odrębnego aktu prawnego,
- niezbędne jest również uregulowanie relacji między instytucjami odpowiedzialnymi za ochronę IK/obiektów podlegających obowiązkowej ochronie: Policja, ABW oraz RCB,
- zintensyfikowane szkolenia personelu odpowiedzialnego za realizację zadań z obszaru ochrony IK oraz prowadzenie, nie koniecznie kontroli, lecz wizyt roboczych na terenie obiektów. Mogą się one przyczynić do lepszego zrozumienia zagadnień, a przez to podnieść poziom ochrony obiektów.

W lipcu 2024 r. do uzgodnień międzyresortowych trafił projektu ustawy o zmianie ustawy o zarządzaniu kryzysowym oraz niektórych innych ustaw, w którym ujęto rozwiązania zawarte w dyrektywie CER mające na celu zapewnić ciągłości świadczenia usług kluczowych realizowanych w sektorach lub podsektorach wskazanych w dyrektywie CER. W zawiązku z powyższym zasadnym będzie kontynuowanie badań pod kątem implementowania przepisów ww. ustawy przez operatorów IK.

7. Wartość dodana pracy

Przedmiotem badań były założenia teoretyczne i doświadczenia praktyczne ochrony IK w Polsce w latach 2007 - 2023. W ramach powyższego w kontekście naukowym dokonano identyfikacji wyzwań i zagrożeń bezpieczeństwa dla infrastruktury krytycznej. Przeprowadzono również ocenę sprawności działania głównych instytucji państwowych zajmujących się ochroną IK. Ponadto dokonano przeglądu procedur zapewniających bezpieczeństwo IK w czasie pokoju, kryzysu oraz wojny. Określono również kierunki doskonalenia systemu ochrony infrastruktury krytycznej.

Autor niniejszej pracy ma nadzieję, że przedstawione w dysertacji wyniki badań będą stanowiły materiał porównawczy dla osób zajmujących się bezpieczeństwem infrastruktury krytycznej, a wnioski pozwolą na zweryfikowanie procedur zapewniających bezpieczeństwo IK w czasie pokoju oraz wojny.

8. Plan pracy

Wykaz Skrótów

Wstęp

ROZDZIAŁ I METODOLOGICZNE PODSTAWY BADAŃ

1.1. Sytuacja problemowa

1.2. Przedmiot, cele badań oraz problemy badawcze i hipoteza robocza

1.3. Metody, narzędzia i techniki badawcze

1.4. Założenia i ograniczenia badawcze

ROZDZIAŁ II INFRASTRUKRUTRA KRYTYCZNA W POLSCE I JEJ OCHRONA

2.1. Zarys systemu zarządzania kryzysowego

- 2.1.1. Zarządzanie kryzysowe na poziomie krajowym
- 2.1.2. Zarządzanie kryzysowe na poziomie resortowym
- 2.1.3. Zarządzanie kryzysowe na poziomie rządowej administracji terenowej
- 2.1.4. Zarządzanie kryzysowe na poziomie administracji samorządowej

2.2. Infrastruktura krytyczna jak element zarządzania kryzysowego

- 2.2.1. Europejska Infrastruktura Krytyczna
- 2.2.2. Ochrona infrastruktury krytycznej w prawie polskim
- 2.2.3. Identyfikacja infrastruktury krytycznej
- 2.2.4. Zadania i obowiązki operatorów infrastruktury krytycznej

2.3. Narodowy Program Ochrony Infrastruktury Krytycznej

- 2.3.1. Identyfikacja infrastruktury krytycznej według Narodowego Programu Ochrony Infrastruktury Krytycznej z 2020 r.
- 2.3.2. Zapewnienie bezpieczeństwa IK
- 2.3.3. Współpraca w ochronie infrastruktury krytycznej

2.4. Plany ochrony infrastruktury krytycznej

2.5. Wnioski

ROZDZIAŁ III ELEMENTY INSTYTUCJONALNEGO SYSTEMU OCHRONY INFRASTRUKTURY KRYRTYCZNEJ

3.1. Rządowe Centrum Bezpieczeństwa

- 3.1.1. Zadania Rządowego Centrum Bezpieczeństwa
- 3.1.2. Rola RCB w zakresie ochrony infrastruktury krytycznej
- 3.1.3. Krajowy Plan Zarządzania Kryzysowego
- 3.1.4. Współpraca z administracją publiczną
- 3.1.5. Współpraca z biznesem