WOJSKOWA AKADEMIA TECHNICZNA
im. Jarosława Dąbrowskiego

Rada Dyscypliny Naukowej
Nauki o Bezpieczeństwie

Cyberprzestrzeń i cyberbezpieczeństwo jako determinanty bezpieczeństwa narodowego Rzeczpospolitej Polskiej

Rozprawa doktorska

mgr inż. Marcin DĄBROWSKI

Promotor:
prof. dr hab. inż. Piotr ZASKÓRSKI
Promotor pomocniczy:
dr inż. Krzysztof LIDERMAN

W a r s z a w a 2025

SPIS TREŚCI

SPIS UŻYTYCH OZNACZEŃ I SKRÓTÓW

AAA – Authentication, Authorization, Accounting

ABW – Agencja Bezpieczeństwa Wewnętrznego

AI – Artificial Intelligence

AOB – Analiza Obszaru Badawczego

APT – Advanced Persistent Threat

BN – Bezpieczeństwo Narodowe

BBN – Biuro Bezpieczeństwa Narodowego

CBZC – Centralne Biuro Zwalczania Cyberprzestępczości

CIA – Confidentiality, Integrity Availability

CSIRT – Computer Emergency Response Team

DDoS – Distributed Denial-of-Service

DSRK RP – Długookresowa Strategia Rozwoju Kraju Rzeczypospolitej Polskiej

EDA – Europejska Agencja Obrony

ENISA – Agencja Unii Europejskiej ds. Cyberbezpieczeństwa

ICD – Informacyjna Ciągłość Działania

ISAC – Information Sharing and Analysis Center

ICT – Technologie Informacyjne i Komunikacyjne

KSC – Krajowy System Cyberbezpieczeństwa

KRRiT – Krajowa Rada Radiofonii i Telewizji

KRPC RP – Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczpospolitej Polskiej

KRD – Krajowa Rada ds. Dezinformacji

NASK – Naukowa Akademicka Sieć Komputerowa

NATO – Organizacja Traktatu Północnoatlantyckiego

MON – Ministerstwo Obrony Narodowej

MSWiA – Ministerstwo Spraw Wewnętrznych i Administracji

OIN – Ochrona Informacji Niejawnych

ON – Obrona Narodowa

OSINT – Open Source Intelligence

OSSB – Operator Strategicznej Sieci Bezpieczeństwa

PTI – Polskie Towarzystwo Informatyczne

RODO – General Data Protection Regulation

RP – Rzeczpospolita Polska

SBN – System Bezpieczeństwa Narodowego

SBN RP – Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej

SOC – Security Operations Center

SOP – System Obrony Państwa

SR SBN RP – Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej

SZR RP – Strategie Zintegrowanego Rozwoju Rzeczypospolitej Polskiej

SZK – System Zarządzania Kryzysowego

ŚSRK RP – Średniookresowa Strategia Rozwoju Kraju Rzeczypospolitej Polskiej

UE – Unia Europejska

ZK – Zarządzanie Kryzysowe

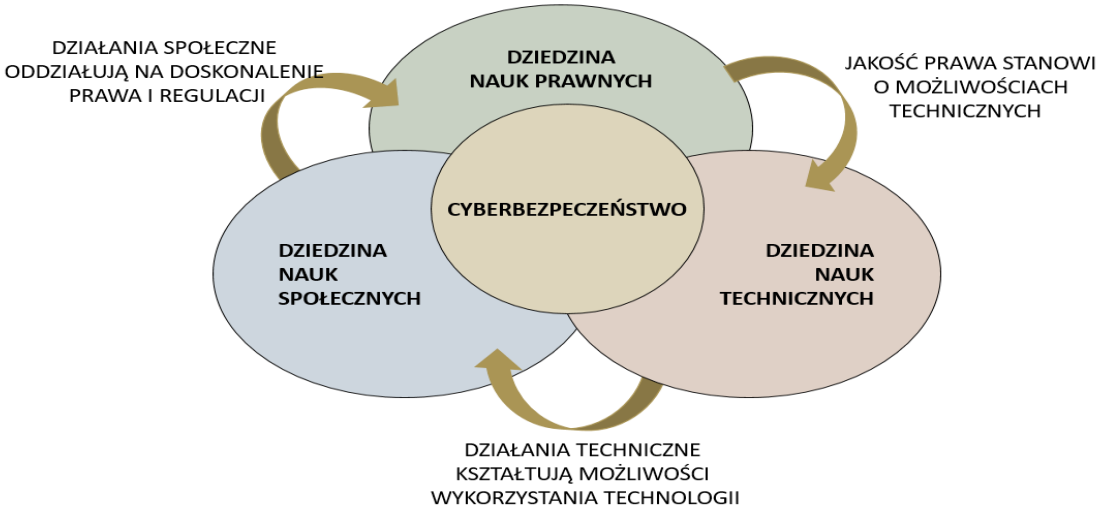
WSTĘP

Bezpieczeństwo narodowe (BN) jest kluczową wartością w wymiarze społecznym i indywidualnym, a ostatnie dwie dekady przyniosły wiele dynamicznych zmian w strategicznym bezpieczeństwie Polski i w środowisku międzynarodowym. Globalizacja i rewolucja informacyjna przyczyniły się do powiązania świata coraz ściślejszymi sieciami wzajemnych zależności[1]. Tuż obok szans pojawiły się nowe wyzwania, rodzaje ryzyka oraz zagrożenia dla bezpieczeństwa państwa i obywateli. Współczesne środowisko bezpieczeństwa jest coraz bardziej złożone i niepewne. Rosną interakcje polityczne, militarne, gospodarcze i społeczne w skali krajowej, regionalnej oraz globalnej. Wywiera to znaczący wpływ na główne kierunki transformacji Systemu Bezpieczeństwa Narodowego. Coraz większy wpływ na kształtowanie bezpieczeństwa ma cyfryzacja społeczeństwa, która jest jedną z najbardziej dynamicznych zmian w dziejach ludzkości. Rozpatrując aktualny stan techniki można pokusić się o stwierdzenie, że niemal w każdej dziedzinie życia społecznego obserwuje się rosnący trend cyfryzacji[2], który niesie ze sobą również pewnego rodzaju zagrożenia dla szeroko rozumianego bezpieczeństwa. Środowiskiem, w którym następuje gromadzenie, wymiana, analiza i przetwarzanie danych jest cyberprzestrzeń. Dzisiejsze działania zagrażające bezpieczeństwu państwa i obywateli zarówno militarne jak i niemilitarne zostały w dużym stopniu zdominowane właśnie przez aktywność w cyberprzestrzeni i z tego powodu istnieje uzasadniona potrzeba jej ochrony. Odpowiedzią na te zagrożenia jest powstanie nieustannie rozwijającej się dziedziny zwanej cyberbezpieczeństwem, łączącej osiągnięcia z zakresu informatyki, telekomunikacji, prawa i nauk społecznych w celu ochrony cyberprzestrzeni (Rys. 1). Rangę cyberbezpieczeństwa wśród pozostałych sektorów bezpieczeństwa podkreśla fakt powstania odosobnionych strategii wyznaczających kierunki rozwoju tego obszaru[3].

Jak już wspomniano ostatnie dwie dekady to czas nieustannego zwiększania roli cyberprzestrzeni i związanego z tym problemu zapewniania cyberbezpieczeństwa. Duży wpływ na rozwój cyberbezpieczeństwa miał „Incydent Estoński[4]" z 2007 roku oraz konflikt w Gruzji z 2008 roku, który zdobył miano „pierwszej cyberwojny", powodując

[1] Biała Księga, Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN Warszawa 2013 r. s. 3.
[2] Gajewski J., Paprocki W., Pieriegud J., Cyfryzacja gospodarki i społeczeństwa szanse i wyzwania dla sektorów infrastrukturalnych. Publikacja Europejskiego Kongresu Finansowego, Gdańsk 2016. s. 11.
[3] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2017-2022, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2019-2024,
[4] Incydent Estoński – pierwsze w historii masowe wykorzystanie ataków na systemy teleinformatyczne.

urzeczywistnienie obaw o wykorzystanie cyberprzestrzeni, jako środowiska do prowadzenia działań zbrojnych.



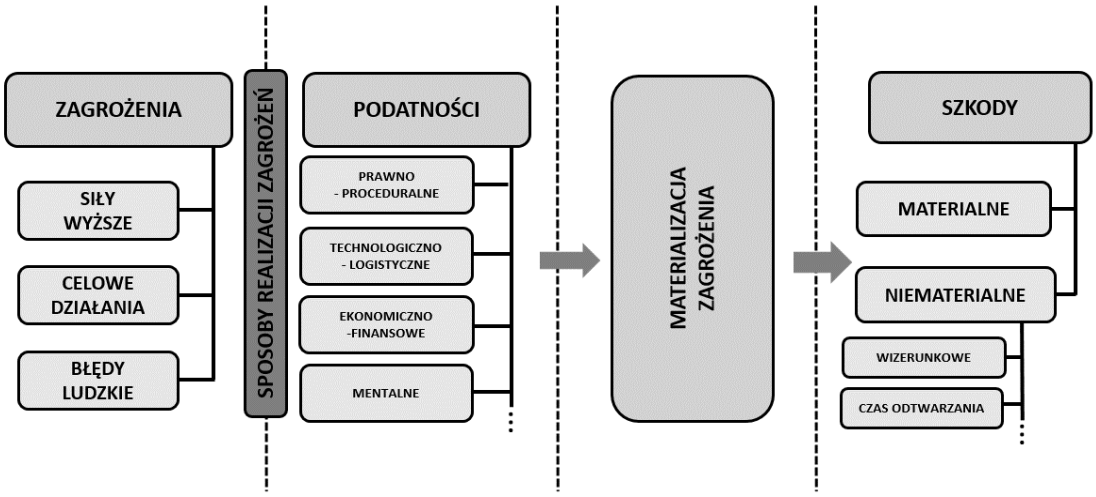
Rys. 1. Obszary nauk składające się na cyberbezpieczeństwo
Źródło: Opracowanie własne.

Wydarzenia te zainicjowały proces, w którym zaczęto na poważnie myśleć o tworzeniu struktur zdolnych do cyberobrony. Z tego też powodu powstał Krajowy System Cyberbezpieczeństwa (KSC) implementujący do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) tzw. Dyrektywę NIS[5] mającą na celu utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego funkcjonowania państwa. Dokumentem normatywnym regulującym działanie KSC jest ustawa[6], która w swym zakresie określa jej organizację, zadania oraz obowiązki podmiotów wchodzących w skład tego systemu. Jest to pierwsza kompleksowa regulacja w Polsce dotycząca całościowego ujęcia problemu bezpieczeństwa systemów teleinformatycznych w sektorze publicznym jak i prywatnym. Rozpatrując cyberbezpieczeństwo w ujęciu globalnym wskazane jest zwrócenie uwagi na fakt, że cyberprzestrzeń została sklasyfikowana jako V domena operacyjna Sił Zbrojnych. Należy przez to rozumieć, że jest środowiskiem, w którym mogą toczyć się działania zbrojne lub inne mające istotny wpływ na zapewnianie konstytucyjnego porządku państwa. Z tego tytułu zostały podjęte działania międzynarodowe na szczeblu NATO oraz EU w postaci współpracy państw członkowskich w zapewnianiu zdolności kolektywnej obrony poprzez podnoszenie gotowości oraz dostępności sił i środków w obszarze cyberbezpieczeństwa.

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa systemów informatycznych na terytorium Unii.
[6] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560.

System Bezpieczeństwa Narodowego składa się z sektorowych obszarów bezpieczeństwa. Jednym z nich jest bezpieczeństwo cyberprzestrzeni będące jednocześnie składową bezpieczeństwa informacji, które tak naprawdę jest ponaddziedzinowe, ponieważ dotyczy każdego sektora bezpieczeństwa państwa. Bezpieczeństwo informacji to praktyka ochrony informacji w głównej mierze poprzez ograniczanie ryzyka i zwykle obejmuje zapobieganie lub zmniejszanie prawdopodobieństwa nieautoryzowanego, niewłaściwego dostępu do danych lub niezgodnego z prawem wykorzystania informacji[7]. W dość dużym uproszczeniu bezpieczeństwo informacji można przedstawić jako politykę triady: dostępności, poufności i integralności danych. Cyberbezpieczeństwo w swej głównej mierze ma na celu ochronę zasobów informacyjnych przed nieuprawnionym wykorzystaniem. W konfrontacji z postępem technologicznym stanowi to poważne wyzwanie we współczesnym świecie. Każdy rozwój techniki niesie za sobą nie tylko korzyści, ale również nowe (nieznane) zagrożenia. Zgodnie z prawem Moore'a moc obliczeniowa komputerów podwaja się co 24 miesiące a co za tym idzie coraz trudniej jest utrzymać właściwy poziom dostępu do informacji (danych). Sytuacja ta powoduje, że co jakiś czas dochodzi do pewnych zdarzeń, na które System Bezpieczeństwa Narodowego nie jest przygotowany i może nastąpić utrata informacyjnej ciągłości działania (organu, państwa). Niezależnie od charakteru zdarzenia (militarne lub niemilitarne) warunkiem koniecznym do materializacji zagrożeń jest dopuszczenie do interakcji stałych elementów takich jak podatności i zagrożenia. Zagrożenia mogą wynikać z działania „sił wyższych" na które nie mamy wpływu, z błędów ludzkich oraz z celowych działań. Podatności są to luki, wady oraz słabości systemowe rozumiane jako braki i niedoskonałości całego systemu. Mogą one występować w infrastrukturze techniczno-technologicznej np. błędy w oprogramowaniu komputerowym lub wadliwa konstrukcja elektroniczno-mechaniczna oraz wady proceduralne typu błędne wytyczne, instrukcje, brak odpowiedniej komunikacji. Zagrożenia w połączeniu z podatnościami będą zatem prowadziły do materializacji zagrożeń a to z kolei będzie skutkowało szkodami[8] (rys. 2.).

[7] https://nflo.pl/slownik/bezpieczenstwo-informacji/ [dostęp: 31.07.2023 r.].
[8] https://uksw.edu.pl/images/artykuly/uniwersytet/RODO/Ryzyko-w-ochronie-danych-osobowych-AK-29.01.2018.pdf [dostęp: 01.08.2024 r.].



Rys. 2 Schemat materializacji zagrożenia.
Źródło: Opracowanie własne na podstawie diagramu autorstwa K. Liderman.

W współczesnym świecie, gdzie dominuje cyfryzacja procesów, systemów oraz procedur kluczowe jest utrzymanie informacyjnej ciągłości działania, ponieważ jej utrata niesie za sobą katastrofalne skutki zarówno w wymiarze materialnym jak i funkcjonalnym. Dlatego z punktu widzenia bezpieczeństwa istotnym atrybutem staje się ryzyko rozumiane jako miara stopnia zagrożenia a w tym przypadku utraty informacyjnej ciągłości działania. Należy mieć świadomość, że nie jest możliwe całkowite wyeliminowanie pewnych podatności oraz że nigdy żaden system nie osiągnie 100% bezpieczeństwa. Z tego też powodu ważna jest korelacja między zagrożeniem oraz prawdopodobieństwem jego wystąpienia oraz zrozumienie mechanizmu przyczynowo skutkowego co pozwala na wychwycenie luk, wad, słabości w obecnym systemie bezpieczeństwa państwa. Ponadto daje możliwość podjęcia czynności korygujących np. w postaci utworzenia koncepcji wzmacniania systemu bezpieczeństwa i jej implementacji.

Cyberbezpieczeństwem z poziomu krajowego należy zarządzać. Należy to realizować poprzez wykorzystanie oryginalnych metod i modeli obejmujących główne obszary zażądania cyberbezpieczeństwem. Wdrażanie i aktualizacja zabezpieczeń powinno dotykać jednocześnie[9]:

- pracowników, czyli ich kompetencji oraz struktur, w ramach których funkcjonują;
- procesów zapewniających eksploatacje i doskonalenie systemów zarządzania bezpieczeństwem informacji oraz zapewniających skuteczną reakcję na

[9] Syta J., 2025, Zarządzanie cyberbezpieczeństwem. Pracownicy, Procesy, Technologie, Wydawnictwo Naukowe PWN, ISBN: ·978-83-01-24182-7, s. 11.

cyberincydenty;

- technologii, czyli narzędzi, które wspomagają zmniejszanie prawdopodobieństwa cyberincydentów oraz ograniczanie ich skutków.

Oczywiście, stanowi to spore wyzwanie dla każdej organizacji natomiast biorąc pod uwagę stale zmieniający się krajobraz podatności i zagrożeń dotykających cyberprzestrzeń jest to konieczne do utrzymania wysokiego poziomu krajowego cyberbezpieczeństwa. Należy podkreślić, że współczesne zagrożenia przed jakimi stoi Rzeczpospolita Polska ulegają dynamicznym przekształceniom. Zmiany w systemie, który ma im się przeciwstawiać zachodzą powoli co wymusza wręcz ciągły proces monitorowania i analizy ryzyka wystąpienia tych zagrożeń poprzez aktualizację procedur lub zorientowanie na nowe kierunki. Natura każdego systemu sprawia, że nie jest on pozbawiony wad, dlatego tak ważne jest identyfikowanie zagrożeń i wprowadzanie działań usprawniających. Z punktu widzenia bezpieczeństwa zachodzi konieczność wzmocnienia ochrony oraz sprawności i efektywności systemów bezpieczeństwa państwa. Złożoność każdego systemu pokazuje jak wiele elementów składa się na nie i w sytuacjach mających znamiona kryzysu nie ma już czasu na tworzenie nowych struktur oraz wprowadzanie istotnych zmian, dlatego należy zrealizować to zawczasu tak aby każdy system był w stopniu maksymalnym pozbawiony podatności. Kluczowymi kompozycjami w Polsce z punktu widzenia bezpieczeństwa są:

- System Bezpieczeństwa Narodowego;
- System Obrony Państwa;
- System Zarządzania kryzysowego;
- Krajowy System Cyberbezpieczeństwa.

Istnieje jeszcze szereg systemów niższego szczebla, które są równie ważne w sytuacjach materializacji zagrożenia. Konstrukcje te ukierunkowane są branżowo lub sektorowo:

- System Ochrony Infrastruktury Krytycznej;
- System Ochrony Granicy Państwowej;
- System Przeciwpowodziowy;
- System Ochrony Informacji Niejawnych;
- System Bezpieczeństwa Międzynarodowego;
- Krajowy System Ratowniczo Gaśniczy;
- Krajowy System Elektromagnetyczny;

- Krajowy System Wykrywania Skażeń;
- inne.

Współcześnie wszystkie te systemy są mocno uzależnione od różnorodnych technologii informacyjnych i komunikacyjnych (ITC) a co za tym idzie są podatne na zagrożenia wykorzystujące cyberprzestrzeń do realizacji. Z tego też powodu zachodzi konieczność wzmocnienia poziomu krajowego cyberbezpieczeństwa tym samym eliminując podatności mające wysoki potencjał wykorzystania przez zagrożenia w ujęciu wszystkich konstrukcji bezpieczeństwa.

Tematyka rozprawy doktorskiej umiejscowiona jest w dziedzinie nauk społecznych, dyscyplinie nauk o bezpieczeństwie, w obszarze bezpieczeństwa państwa. Dysertacja porusza problematykę Systemu Bezpieczeństwa Narodowego, zarządzania ryzykiem, bezpieczeństwa informacji oraz informacyjnej ciągłości działania systemów. Praca składa się z wstępu, sześciu merytorycznych rozdziałów oraz zakończenia wraz z załącznikami. Realizacja rozprawy doktorskiej została zaplanowana tak aby zawartość poszczególnych rozdziałów profilowana była celami oraz problemami badawczymi i hipotezami szczegółowymi, które są obrazem dekompozycji hipotezy głównej.

W rozdziale pierwszym autor skupi się na problematyce podstawowych pojęć, gdzie zostanie przeprowadzona krytyczna analiza już istniejących definicji. Dodatkowo zostanie podjęta próba autorskiego zdefiniowania takich ich pojęć jak: cyberbezpieczeństwo oraz informacyjna ciągłość działania systemu. Celem dalszej części rozdziału będzie ustalenie miejsca, roli oraz rangi cyberbezpieczeństwa w systemach bezpieczeństwa państwa. Ponadto autor skupi uwagę na przedstawieniu struktury, zadań oraz korelacji z informacyjną ciągłością działania systemów wraz z analizą Krajowego Systemu Cyberbezpieczeństwa. Dodatkowym komponentem będzie w zakresie cyberbezpieczeństwa analiza porównawcza istniejących rozwiązań innych wybranych państw. W tym celu zostanie wykorzystana metoda analizy systemowej w ujęciu procesowym, która w szerszym kontekście zarządzania procesami pozwoli rozważać nad wdrożeniem pewnych rozwiązań stosowanych w innych krajach.

Celem drugiego rozdziału będzie przedstawienie metodyki badań. Wyeksponowane zostanie uzasadnienie podjęcia tematyki badań. W toku rozdziału zostanie dokonane ukierunkowania na obszar badawczy, którego dotyczy problematyka rozprawy. Ponadto zostanie przedstawione uszczegółowienie schematu badawczego poprzez ujednoznacznienie zarówno celów, problemów jak i hipotez badawczych wraz

z opisem doboru metod i technik wykorzystanych w badaniach. Końcowym etapem rozdziału będzie przegląd literatury co pozwoliło na przedstawienie zarówno aktualnego stanu wiedzy w danym obszarze jak i wskazanie miejsc, w których występują braki literaturowe.

W rozdziale trzecim zostaną wyeksponowane elementy materializacji zagrożeń i podatności mogące oddziaływać na System Bezpieczeństwa Narodowego i inne systemy bezpieczeństwa państwa. Na wstępie zostanie przeanalizowane studium przypadków zdarzeń, które wpisują się w obszar badawczy i w rzeczywistości miały poważne konsekwencje w wymiarze globalnym, ponieważ dotyczyły utraty informacyjnej ciągłości działania. Analiza przypadków zostanie przeprowadzona z zamiarem dochodzenia do źródeł niepowodzenia tych zdarzeń, przy czym szczególna uwaga będzie poświęcona zagrożeniom wykorzystującym celowe działania mające wpływ na dostępność, poufność, integralność zasobów informacyjnych. Następnie w celu zdiagnozowania aktualnych zagrożeń będą użyte dane statystyczne corocznie publikowane w raportach branżowych wyspecjalizowanych instytucji. Dodatkowo będą przeprowadzone badania w postaci wywiadów i wywiadów eksperckich mające na celu wyłonienie zagrożeń w kluczowych sektorach bezpieczeństwa państwa. Również na podstawie analizy dokumentów normatywnych oraz struktury systemów bezpieczeństwa państwa zostaną wyłonione wady, luki, oraz słabości systemowe. Będą one w nawiązaniu do klasycznego schematu materializacji zagrożeń traktowane jako podatności. Całościowy zbiór zagrożeń (elementów materializacji zagrożeń i sposobów realizacji zagrożeń) zostanie skonfrontowany z zdolnościami obronnymi Systemu Bezpieczeństwa Narodowego co pozwoli wyłonić szczątkowy katalog zagrożeń, na które obecny system nie jest przygotowany.

Rozdział czwarty dotyczył będzie zastosowania oceny ryzyka do prognozowania jakości decyzji modyfikujących System Bezpieczeństwa Narodowego. W tym celu zostanie przedstawiona między innymi kombinacja podatności z elementami materializacji zagrożeń. Zestawienie te pozwoli w przypadku braku podjęcia działań naprawczych wskazać oczekiwane straty. W dalszej części rozdziału zostanie zbadany stopień wykorzystania podatności przez elementy materializacji zagrożeń a uzyskane wyniki w zestawieniu tabelarycznym posłużą do oszacowania poziomu istotności dla każdej podatności. Przedmiotowe podatności zostaną poddane kategoryzacji oraz kompleksowej analizie obszaru przyczynowego ich powstania. Będą to to działania

niezbędne w celu dojścia do źródeł niepowodzenia tych podatności i wypracowania rozwiązań eliminacji ich podczas tworzenia koncepcji poprawy bezpieczeństwa. Kwintesencją rozdziału będzie utworzenie tabeli podatności względem poziomu istotności wraz z wskazaniem propozycji ich eliminacji w ujęciu obszarów doskonalenia takich jak wielkość infrastruktury, liczba potrzebnego personelu, zmiany w regulacjach prawnych oraz kosztu utworzenia i utrzymania.

W rozdziale piątym zostanie zaprezentowana koncepcja wzmacniania odporności państwa na zagrożenia wykorzystujące cyberprzestrzeń w aspekcie potrzeb skutecznego funkcjonowania systemów bezpieczeństwa państwa ze szczególnym uwzględnieniem ochrony zasobów informacyjnych. Podstawę opracowania koncepcji w obszarze cyberbezpieczeństwa stanowiły będą badania nad zagrożeniami, podatnościami i ryzykiem utraty ciągłości działania lub obniżenia poziomu bezpieczeństwa. W rozdziale tym będzie skupiony wysiłek na uwzględnieniu ograniczeń w obszarach doskonalenia, gdzie zostały przeanalizowane problemy prawno-proceduralne, ekonomiczno-finansowe, technologiczno-logistyczne, jak również mentalne i organizacyjne. Potencjalne rozwiązania powstaną na podstawie wyeksponowanych podatności, gdzie główny wysiłek będzie skupiony się na dwóch największych wyzwaniach w cyberbezpieczeństwie tj. sił i środków rozumianych jako finansowanie i potencjał ludzki. Wyakcentowany zostanie przede wszystkim problem kadrowy, ponieważ poziom rosnących zagrożeń powoduje zwiększające się zapotrzebowanie na wykwalifikowanych specjalistów w zakresie bezpieczeństwa w sektorze prywatnym, co stanowi swego rodzaju zagrożenie dla administracji państwowej. Jako jedno z rozwiązań zaproponowany zostanie krajowy program szkolenia ustawowego począwszy do poziomu wczesnoszkolnego. Uwaga zostanie skoncentrowana również na podniesieniu rangi cyberbezpieczeństwa na poziomie strategii oraz dokumentów normatywnych będących implementacją wytycznych dyrektyw europejskich NIS. Ponadto zostaną dołożone wysiłków na źródła pozyskiwania środków finansowych przeznaczonych na cyberbezpieczeństwo poziomu krajowego. Końcowym etapem projektu będzie analiza skuteczności krajowych podmiotów zajmujących się cyberbezpieczeństwem w celu zweryfikowania, które elementy należy zmienić, rozbudować lub utworzyć, aby utrzymać odpowiedni poziom cyberbezpieczeństwa. Każda z propozycji eliminacji podatności zostanie poddana analizie SWOT celem wyłonienia nie tylko zalet, ale przed wszystkim zagrożeń i słabych stron.

Celem rozdziału szóstego będzie implementacja koncepcji opartej na ochronie zasobów informacyjnych wraz z elementami strategii zarządzania organizacją podnoszącymi poziom bezpieczeństwa usług cyfrowych. Pierwszy etap obejmował będzie zaprojektowanie procesu wdrożeniowego poprzez ustalenie miarodajnych wskaźników, które definiowałyby wartość koncepcji pod względem kosztów wdrożenia i utrzymania, potrzeb rozbudowy infrastruktury, ilości dodatkowego personelu oraz zmian w regulacjach prawnych. W drugiej części zostaną zaprezentowane szczegółowe badania w postaci wywiadów (sondażu diagnostycznego) mających na celu ocenę utworzonej koncepcji pod kątem akceptacji wielkości sił i środków niezbędnych do realizacji przedmiotowych rozwiązań. Ilościowe zestawienie odpowiedzi z wywiadu pozwoli na jednoznaczną ocenę przedmiotowej koncepcji oraz wyeksponowanie słabych punktów koniecznych do dalszego przeanalizowania.

Całość dysertacji zostanie podsumowana zakończeniem, w którym zostanie dokonane obiektywne spojrzenie na całokształt przeprowadzonych badań, z jednoczesnym wskazaniem dalszych kierunków rozwoju prac związanych z podnoszeniem krajowego poziomu cyberbezpieczeństwa. Dysertacja będzie stanowiła kompleksowy przegląd systemów bezpieczeństwa państwa w ujęciu funkcjonalnym z jednoczesnym wskazaniem obszarów wymagających poprawy poprzez eliminację stwierdzonych podatności, które pod wpływem zagrożeń mogą prowadzić do paraliżu lub ustania ciągłości działania całego państwa.

ROZDZIAŁ I. DZIEDZINA PROBLEMU

1.1. Podstawowe pojęcia

Istotnym z punktu widzenia podjęcia próby rozwiązania jakiegokolwiek problemu jest prawidłowe określenie definicji fundamentalnych pojęć dla badanego obszaru. Podstawowym źródłem czerpania definicji powinny być literatura branżowa i dokumenty normatywne, przy czym do wiarygodnych źródeł należą Słownik Języka Polskiego, słowniki branżowe oraz regulacje prawne, które de facto zawierają oficjalne definicje. Należy tu wspomnieć, że również istnieją poboczne źródła takie jak Internet natomiast nie wszystkie definicje zamieszczone w sieci spełniają wymogi zasad konstrukcji definicji. Ponadto zasadna jest analiza anglojęzycznych definicji co pozwala zrozumieć jak dane pojęcia określane są w innych częściach świata. W niektórych przypadkach ustalenie definicji może być problematyczne, ponieważ istnieją pojęcia takie jak np. bezpieczeństwo lub cyberbezpieczeństwo itp., które są zbyt obszerne, aby mogły zostać przedstawione uniwersalnie a co za tym idzie można je zdefiniować tylko do konkretnej dziedziny. Należy przez to rozumieć, iż w przypadku braku odpowiedniej definicji dla danego pojęcia w wymienionych źródłach zasadnym jest dążenie do utworzenia definicji opartej na zasadach zgodnych z logiką definicji[10] w ujęciu konkretnego problemu badawczego. Poprawnie sformułowana definicja powinna składać się z trzech elementów takich jak:

- definiendum, stanowiąca jej człon definiowany;
- definiens, część definicji stanowiąca jej człon definiujący;
- łącznik definicyjny, znak równości: „jest", „to", „oznacza", „jest to", itp.

Konsekwencją tak przedstawionego podziału jest klasyczny schemat definicji, który można wyrazić zapisem „A jest to B mające cechę C", gdzie „B i C" to definiens w tym przykładzie złożone z rodzaju najbliższego „B" i różnicy gatunkowej „C", (łac. genus proximum et differentiam specificam[11]). Oczywiście zasadnym jest również podział definicji ze względu na przesłanki wyróżnienia, które przedstawiono w tabeli 1. Kryteria są swego rodzaju kategoriami definicji, gdzie do najczęściej spotykanych należy klasyfikacja rodzajowa, realna, charakteryzująca przedmiot, zjawisko przez podanie zespołu cech mu wyłącznie właściwych.

[10] Logikę definicji – należy rozumieć jako zbiór wytycznych i dobrych praktyk wykorzystywanych przy tworzeniu definicji.
[11] http://doktorat.xn--pook-11a.pl/SEP/15Z/Logika/logika_2.pdf [dostęp 21.11.2021].

Tab. 1. Kryteria definicji.

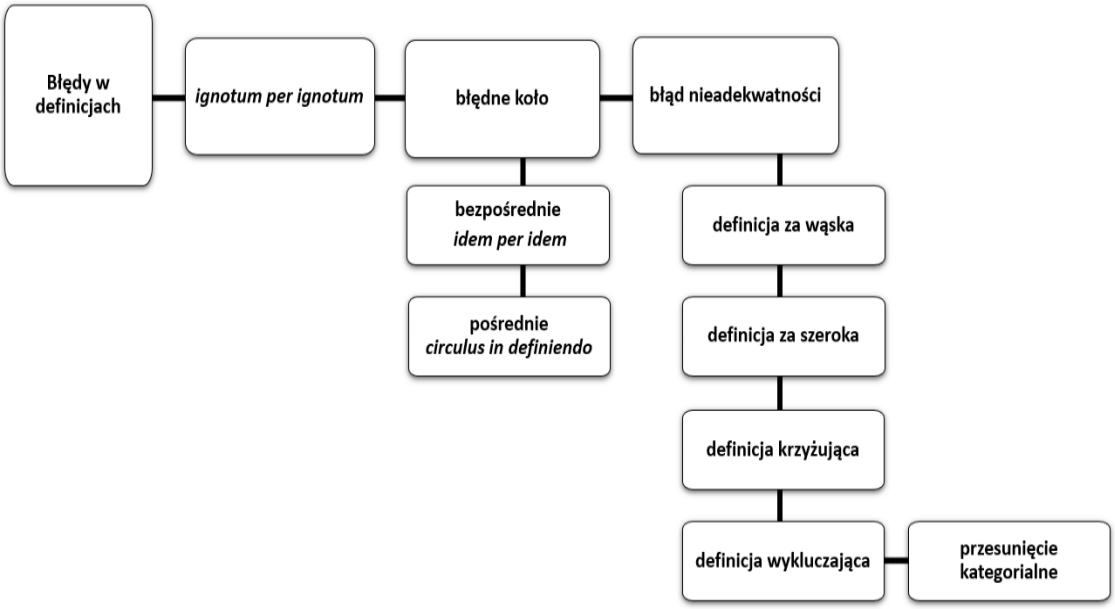
KRYTERIUM WYRÓŻNIENIA	WYSZCZEGÓLNIENIE
klasyfikacja rodzajowa	− definicja realna (charakteryzująca przedmiot-zjawisko przez podanie zespołu cech mu wyłącznie właściwych) − definicja nominalna (wyjaśniająca znaczenie wyrazów przez podanie wyrazów w nim równoznacznych)
klasyfikacja pojęciowa	− definicja realno-znaczeniowa (polegająca na wyjaśnieniu treści znaczeniowej wyrazu bez odwoływania się do jego budowy słowotwórczej) − definicja zakresowa (wskazująca na zakres desygnatów oznaczonych definiowanym wyrazem) − definicja klasyczna (określająca pojęcie przez wymienianie cech identyfikujących i różnicujących)
klasyfikacja zakresowa	− definicje cząstkowe-redukcyjne (podające tylko niektóre kryteria stosowalności danego wyrażenia, tylko warunek konieczny lub wystarczający) − definicje warunkowe (przez postulaty indukcyjne)
szczegółowa klasyfikacja rodzajowa definicji nominalnych i realnych	− definicja analityczna-sprawozdawcza (podająca przyjęte znaczenie definiowanego wyrażenia) − definicja syntetyczna-projektująca (podająca nowe znaczenie wyrażenia na mocy konwencji terminologicznej) − definicja regulująca (modyfikuje uściślająco istniejące określenie)
klasyfikacja według przejrzystości konstrukcji	− definicje wyraźne (odpowiadające wprost na pytanie „co to jest” − definicje w uwikłaniu
klasyfikacja rodzajowa definicji w uwikłaniu	− definicja przez postulaty − definicja indukcyjna − definicja przez abstrakcje

Źródło: Czaja S., Becla A., Wybrane informacyjne problemy definiowania zrównoważonego i trwałego rozwoju, ujęcie teoretyczne, s 18.

Nie bez znaczenia pozostaje fakt, że definicja może być obarczona błędem w swojej konstrukcji oraz znaczeniu, dlatego ważne jest, aby na etapie projektowania nowej definicji mieć świadomość jak tego uniknąć[12]. Na rysunku 2 zaprezentowano schemat możliwych błędów jakie mogą zaistnieć przy tworzeniu definicji. Niezależnie od rodzaju błędów należy zadbać, aby treść definicji była zgodna z prezentowanym wyrażeniem, ponieważ odnosząc się do pojęcia samej definicji, która brzmi „*Definicja - wypowiedź o określonej budowie, w której informuje się o znaczeniu pewnego wyrażenia przez wskazanie innego wyrażenia oddającego sens sformułowania*[13]*”* zasadnym jest, aby „wyrażenia” były dobierane według zasady „brzytwy Ockhama”.

[12] Czaja S., Becla A., Wybrane informacyjne problemy definiowania zrównoważonego i trwałego rozwoju, ujęcie teoretyczne, Uniwersytet Ekonomiczny we Wrocławiu, Optimum. Studia Ekonomiczne nr. 1 (79) 2016, s 17.

[13] https://pl.wikipedia.org/wiki/Definicja#Budowa_definicji. [dostęp: 21.11.2021].



Rys. 3. Schemat błędów w definicji.
Źródło: http://doktorat.xn--pook-11a.pl/SEP/15Z/Logika/logika_2.pdf [dostęp: 22.03.2021].

Rozwinięciem rysunku 3 jest tabela 2, która zawiera rodzaj, znaczenie oraz przykłady błędów. Uwzględnienie treści tej tabeli pozwoli na szczegółową selekcję i analizę definicji a w przypadku konieczności utworzenia własnej umożliwi zachowanie logicznej poprawności.

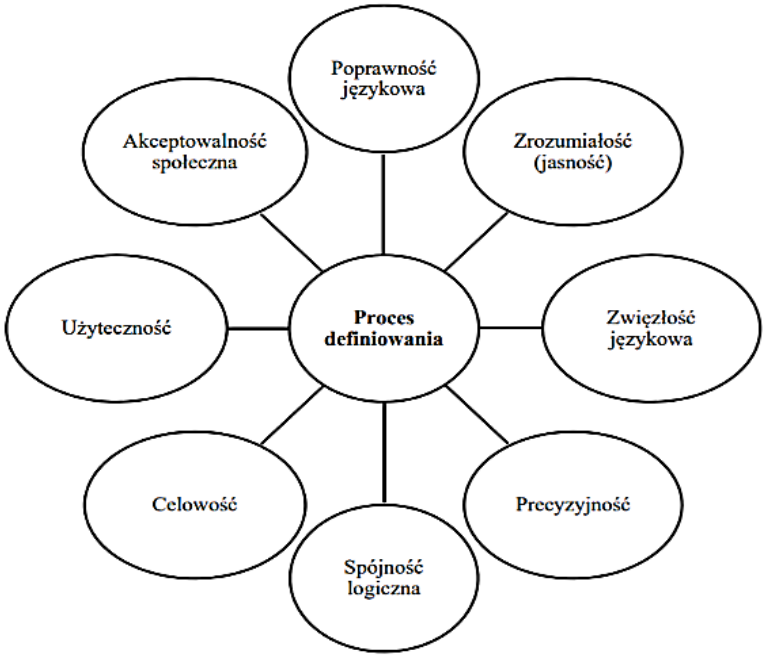
Tab. 2. Opis i znaczenie błędów definicji.

BŁĄD	ZNACZENIE	PRZYKŁAD
„ignotum per ignotum” nieznane przez nieznane	powstaje, gdy definiens jest niezrozumiały dla odbiorcy	„Izoleucyna to aminokwas egzogenny o rozgałęzionym łańcuchu węglowym”.
„idem per idem” to samo przez to samo	powstaje, gdy w definiensie pojawia się definiendum	„Organizacje społeczne, to organizacje zawodowe, samorządowe, spółdzielcze i inne organizacje społeczne”.
„circulus in definiendo” błędne koło pośrednie	powstaje, gdy w definiensie pojawiają się zwroty, które muszą być definiowane z użyciem definiendum	„Trybut to danina płacona w związku z uznaniem zwierzchności senioralnej zwierzchność senioralna to uznanie statusu lennika”.
za wąski	powstaje, gdy zakres definiensa jest węższy od zakresu definiendum	„Marynarz jest to osoba pływająca na statku handlowym”.
za szeroki	powstaje, gdy zakres defininens jest szerszy od definiendum	„Istnieją roślinożerne ssaki, niebędące krowami, np. owca”.
krzyżują się	takie w których powiedziano za dużo, jak i za mało, że jest za wąska i za szeroka	„Żołnierz to osoba pełniąca służbę wojskową w Polsce”.
wykluczają się	w których zakresy definiendum i definiensa się wykluczają	„Żołnierz to mężczyzna zarejestrowany w urzędzie pracy jako bezrobotny”.

błąd przesunięcia kategorialnego	powstaje, w sytuacji, w których definiendum i definiens należą do innych kategorii	„Sprawiedliwość to tyle, co wszystkie uczynki sprawiedliwe”.

Źródło: opracowanie własne http://doktorat.xn--pook-11a.pl/SEP/15Z/Logika/logika_2.pdf [dostęp: 21.11.2021 r.].

Znając przyczyny podstawowych błędów można wskazać dobrą praktykę tworzenia definicji, przy czym za dobrą uznaje się taką, która w pełni wyczerpuje znamiona badanego zjawiska zachowując przy tym swą niepodważalność. Pożądane cechy definicji zaprezentowano na rysunku 4.



Rys. 4. Pożądane cechy definicji.
Źródło: Czaja S., Becla A., Wybrane informacyjne problemy definiowania zrównoważonego i trwałego rozwoju, ujęcie teoretyczne, s 17.

Analizując cechy przedstawione na rysunku 4 można pokusić się o refleksje co do miarodajności tych elementów. O ile w definicji już istniejącej można poddać ją krytycznej analizie to w przypadku tworzenia nowej może okazać się to problematyczne, ponieważ np. to co dla „jednych” jest zrozumiałe, użyteczne i akceptowalne to nie musi być takie dla innych. Argument ten czyni definicję samą w sobie niejako „indywidualnie przyswajalną” i pozwala każdej osobie decydować o wyborze odpowiedniej definicji z zachowaniem przedstawionych kryteriów metodycznych. Zgodnie z prezentowanymi założeniami dla podstawowych pojęć realizacja wyboru definicji odbędzie się poprzez poddanie krytyce już istniejących a w przypadku braku spełniających wymagania formalne zostaną przedstawione definicje autorskie. Uwaga zostanie zwrócona na stopień mierzalności badanej materii, gdzie jak

już wspomniano, w przypadku definicji uniwersalnych problematyczna jest „namacalność" i postawienie pewnych granic obszaru, którego one dotyczą. Z tego też powodu czyni to definicje dość skomplikowanymi pod względem precyzji odniesienia a głównym kryterium będzie tu poza wykluczeniem błędów zrozumiałość, spójność logiczna, zwięzłość i akceptowalność społeczna. Zgodnie z przyjętymi wymogami analizie zostaną poddane definicje: bezpieczeństwa, cyberprzestrzeni, cyberbezpieczeństwa, ciągłości działania oraz informacyjnej ciągłości działania. Będą one zaczerpnięte z Słownika Języka Polskiego, regulacji prawnych (ustaw, norm), literatury tematycznej oraz sieci Internet. Dodatkowo analiza zostanie rozszerzona o anglojęzyczne definicje, przy czym zostaną one wyszukane w przeglądarce „Google" za pomocą przedmiotowych haseł. Źródła definicji zostały celowo dobrane w taki sposób, aby można było zaprezentować odmienność ich pochodzenia co pozwoli na wyeksponowanie ich różnorodności. Dla każdej przedstawionej definicji zostanie podane jej źródło pozyskania oraz komentarz co do zgodności z przedstawionymi wymogami logiki definicji, przy czym istotne jest wytłumaczenie podejścia przyczynowo skutkowego prezentowanej analizy krytycznej, ponieważ nie ma ona na celu negowania lub dyskredytacji jakiejkolwiek definicji a jedynie wspomóc proces wyboru tych definicji, które z punktu widzenia prowadzenia dalszych badań będą stanowiły punkt odniesienia. Dodatkowo należy również podkreślić, iż w większości prezentowane definicje nie zawierają błędnych twierdzeń natomiast cel, w którym zostały stworzone nie pozwala na ich użycie w przedmiotowych badaniach. Z tego powodu analiza krytyczna będzie stanowiła swego rodzaju odcinanie się od definicji, które nie mają zastosowania i przełożenia na tworzenie koncepcji poprawy Bezpieczeństwa Narodowego RP. Definiowanie problematycznych sformułowań wymaga odpowiedniego balansowania pomiędzy zgodnością konstrukcyjną treści oraz spójnością logiczną i wspomnianą już wcześniej akceptowalnością społeczną.

1.1.1. Bezpieczeństwo

Analiza definicji bezpieczeństwa odzwierciedla problematykę definiowania ponieważ tak szerokie pojęcie okazuje się trudne do przedstawienia za pomocą kilku zdań wyczerpując przy tym pełne jego znaczenie.

Definicja bezpieczeństwa nr 1

„Bezpieczeństwo to stan, w którym jednostka, grupa społeczna, organizacja, państwo nie odczuwa zagrożenia swego istnienia lub podstawowych interesów; sytuacja, w której występują formalne, instytucjonalne i praktyczne gwarancje ochrony”.

Źródło: Słownik Języka Polskiego.

Analizując tę definicję można dostrzec, że spełnia warunek konstrukcyjny, ponieważ nie dopatrzono się żadnego z błędów logiki definicji. Zawarte są jednak błędy merytoryczne. W jednej definicji występuje rozbieżność w takiej postaci, że raz jest to „*stan*” a raz „*sytuacja*”. Skoro bezpieczeństwo jest „*stanem*”, to narzuca się pytanie jakie są inne stany z bezpieczeństwem związane? Na pewno muszą być dwa: „*bezpiecznie*” i „*niebezpiecznie*” co nasuwa pytanie jakie są formalne warunki przejścia ze stanu do stanu? Traktując zapis całościowo wynika z niego, że „*bezpieczeństwo*” jest zależne od „*ochrony*” przy czym słowo „*gwarancje*” nic konkretnego nie wnosi, ponieważ termin gwarancja oznacza jedną z instytucji prawa zobowiązań zgodnie z polskim prawem handlowym.

Definicja bezpieczeństwa nr 2

„Bezpieczeństwo – teoria i praktyka zapewniania możliwości przetrwania (egzystencji) i realizacji własnych interesów przez dany podmiot, w szczególności poprzez wykorzystywanie szans (okoliczności sprzyjających), podejmowanie wyzwań, redukowanie ryzyk oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów”.

Źródło: Biuro Bezpieczeństwa Narodowego[14].

W stwierdzeniu tym można zaobserwować rozszerzenie niewiadomych w definiens takich jak „*możliwości przetrwania (egzystencji)*” czy „*wykorzystywanie szans (okoliczności sprzyjających)*” co należy do poprawnych praktyk budowania definicji. Jednak zauważalny jest termin *„teoria i praktyka”* co w ogólnym przekonaniu bardziej właściwy byłby do opisania definicji jako nauk o bezpieczeństwie, ponieważ definiując bezpieczeństwo wskazane jest uwzględnienie minimalnych granic namacalności tego pojęcia. Należy tu jednak podkreślić szerokie rozwinięcie znaczenia tej definicji oraz brak błędów logicznych co czyni, że definicja ta może być odpowiednia dla szerszego grona odbiorców.

[14] https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp 21.11.2021].

Definicja bezpieczeństwa nr 3

„Bezpieczeństwo to stan, który daje poczucie pewności i gwarancje jego zachowania oraz szanse na doskonalenie. Jest to jedna z podstawowych potrzeb człowieka. Odznacza się brakiem ryzyka utraty czegoś dla człowieka szczególnie cennego – życia, zdrowia, pracy, szacunku, uczuć, dóbr materialnych i dóbr niematerialnych".

Źródło: Bezpieczeństwo Narodowe Polski w XXI wieku[15].

Z przedstawionego sformułowania wynika, że w jakiś sposób można doskonalić „*pewność*" oraz pada ponownie termin „*gwarancje*". W definicji tej również nie jest jasne czy bezpieczeństwo jest „*stan*em" czy „*potrzebą*". Poza tym czego dotyczy ta „*potrzeba*"? Doskonalenia? Występuje błąd rozumienia istoty ryzyka wyrażonego poprzez słowa „*odznacza się brakiem ryzyka*". Nie da się ryzyka zredukować do zera, zawsze będzie jakieś ryzyko szczątkowe co w dalszej części dysertacji będzie przedmiotem badań. Zwrot „*życia*, *zdrowia, pracy, szacunku, uczuć, dóbr materialnych i dóbr niematerialnych*", jest zbytnim wydłużeniem, ponieważ samo wskazanie dóbr materialnych i niematerialnych powszechnie definiuje ich części składowe.

Definicja bezpieczeństwa nr 4

„Bezpieczeństwo stanowi jedną z najbardziej istotnych wartości dla człowieka. Zajmuje znaczącą pozycję wśród tzw. dóbr uniwersalnych, jak dobro, prawda czy sprawiedliwość i jest jedną z naczelnych potrzeb ludzi, wraz z potrzebami życia, zdrowia, wolności, godności, prywatności i godnego traktowania".

Źródło: Vademecum Bezpieczeństwa[16].

W tej definicji po raz kolejny użyto zbędnego rozszerzenia w fragmencie „*dóbr uniwersalnych, jak dobro, prawda czy sprawiedliwość lub naczelnych potrzeb ludzi, wraz z potrzebami życia, zdrowia*" ponieważ powszechnie wiadomo jakie są dobra uniwersalne i naczelne potrzeby ludzi. Definicja bardziej ta bardziej odnosi się do usytuowania bezpieczeństwa w teorii „piramidy Maslowa", przy czym nie wyczerpuje do końca znaczenia tego pojęcia. Godnym uwagi jest fakt, że odnosi się wyłącznie do „*wartości człowieka*" oraz „*naczelnych potrzeb ludzi*". Ponadto konstrukcja logiczna nie jest spełniona, ponieważ definicja ma w sobie błąd „za wąski" i zakres „definiensa" jest węższy od zakresu definiendum.

[15] Jakubczak R., Flis J. – Bezpieczeństwo Narodowe Polski w XXI wieku, Warszawa 2006, s. 6.
[16] https://depot.ceon.pl/ Vademecum_bezpieczenstwa.pdf [dostęp 21.11.2021].

Definicja bezpieczeństwa nr 5 (anglojęzyczna)

„Security is a state in which the risks and the threats resulting from them are minimized or eliminated”.

Tłumaczenie:

„*Bezpieczeństwo to stan, w którym ryzyka i wynikające z nich zagrożenia są minimalizowane lub eliminowane*”.

Źródło: Ladislav Hofreiter, About security in contemporary world[17].

Definicja jest zaczerpnięta z artykułu naukowego Uniwersytetu Żylińskiego na Słowacji. Autor jest przekonany, że ryzyko można wyeliminować co nie do końca jest prawdą. Natomiast minimalizacja ryzyka jest możliwa pozostaje tylko pytanie czy bezpieczeństwo jest tylko powiązane z pojedynczym stanem? Definicja w swej konstrukcji posiada błąd jest „za wąska” w stosunku do definiendum.

Prezentowana analiza definicji bezpieczeństwa wykazała, że próba zdefiniowania całościowo tego pojęcia jest obarczona błędami konstrukcyjnymi jak również trudno jest wyczerpać w pełni znaczenie tego pojęcia. W związku z tak przedstawioną sytuacją wskazane jest dążenie do utworzenia definicji bezpieczeństwa dla konkretnej dziedziny, obszaru, ponieważ nie jest możliwym znalezienie „złotego środka”, który byłby dopasowany w każdym kontekście. Nie oznacza to jednak, iż prezentowane definicje są nieużyteczne wręcz przeciwnie. Każda z definicji znajdzie swoje zastosowanie w konkretnym celu natomiast z punktu widzenia potrzeb prowadzonych badań najbardziej przystosowana jest definicja nr 5 łącząca w swej istocie bezpieczeństwo z ryzykiem, która po rozbudowaniu w dalszej części dysertacji będzie stanowiła punkt odniesienia dla rozwiązania problemu badawczego.

1.1.2. Cyberprzestrzeń

Definicja cyberprzestrzeni podobnie jak w przypadku bezpieczeństwa występuje w licznych źródłach literatury. Przykładowo według NATO cyberprzestrzeń jest środowiskiem takim samym jak ląd, woda, powietrze czy przestrzeń kosmiczna. W związku z czym wskazane jest, aby poszukiwana definicja odnosiła się poniekąd do praw fizycznych rządzących tym środowiskiem i wzajemnymi relacjami z otoczeniem. Innymi słowy wskazane jest znalezienie definicji, która sięga do korzeni zjawiska.

[17] https://civitas.edu.pl/wp-content/uploads/2015/03/Securitologia-1-21-2015_007-017.pdf s-7. [dostęp: 21.11.2021].

Definicja cyberprzestrzeni nr 1

„Cyberprzestrzeń – rozumie się przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570), wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami".

Źródło: Ustawa o stanie wyjątkowym[18].

Jest to definicja ustawowa, oficjalna. Jednak nie spełnia warunku przejrzystości oraz przyswajalności. Powoływanie się w definiens na oddzielne akty prawne powoduje wystąpienie błędu „ignotum per ignotum" czyli nieznane przez nieznane. Należy tu postawić pytanie, czy gdyby nie „*przestrzeń przetwarzania i wymiany informacji*" cyberprzestrzeń nie istniałaby? Należy podkreślić, że cyberprzestrzeń jako środowisko istniała już zanim powstały „*systemy teleinformatyczne*" co czyni definicję „za wąską".

Definicja cyberprzestrzeni nr 2

„Cyberprzestrzeń jest m.in. przestrzenią komunikacyjną tworzoną przez systemy powiązań internetowych. Pozwala jej użytkownikom na komunikację w sieci i nawiązywanie relacji w czasie rzeczywistym".

Źródło: Przegląd Teleinformatyczny[19].

W pierwszej części definicji „*Cyberprzestrzeń jest m.in. przestrzenią*" występuje klasyczny przykład „idem per idem" czyli to samo przez to samo. Dodatkowo słowo „*m.in.*" sugeruje, że jest jeszcze czymś innym tylko nie zostało wyjaśnione czym. Można podważyć zasadność tezy i zadać pytanie czy aby na pewno cyberprzestrzeń jest tylko do komunikowania się i tylko w czasie rzeczywistym? Zastanawiający jest też zwrot „*systemy powiązań internetowych*" co wskazuje na to, że poza Internetem cyberprzestrzeń nie istnieje.

Definicja cyberprzestrzeni nr 3

„Cyberprzestrzeń – pojęcie to oznacza wirtualny świat".

Źródło: Leksykon tematyczny, Zarządzanie IT[20].

[18] Ustawa z dnia 21 czerwca 2002 r. o stanie wyjątkowym, Dz.U. 2002 Nr 117 poz. 985, s. 1.
[19] Marczyk M., Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru. Przegląd Teleinformatyczny nr 1-2, (59) 2018, s. 59.
[20] Gogołek W., Cetera W., *Leksykon tematyczny. Zarządzanie, IT*, Wydawnictwo Wydziału Dziennikarstwa i Nauk Politycznych UW, Warszawa 2014, s. 246.

Stwierdzenie to również jest przykładem podręcznikowego „ignotum per ignotum" czyli nieznane przez nieznane. Dodatkowo nawet jeśli słowa wirtualny świat byłyby szerzej rozwinięte to czy na pewno tylko wirtualny świat?

Definicja cyberprzestrzeni nr 4

„Cyberprzestrzeń – cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami".

Źródło: Sienkiewicz P., Ontologia cyberprzestrzeni[21].

W definicji uwagę przyciąga przejrzystość, zwięzłość oraz poprawność językowa. Stanowi to przesłanki do twierdzenia, że definicja może być przyswajalna i akceptowalna dla ogółu społeczeństwa. Natomiast brakuje tu odniesienia do źródła istoty cyberprzestrzeni, które zastąpiono terminem „*cyfrowa przestrzeń*" co powoduje wystąpieniem błędu „ignotum per ignotum" czyli nieznane przez nieznane.

Definicja cyberprzestrzeni nr 5 (anglojęzyczna)

„Cyberspace – A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers".

Tłumaczenie:

„Cyberprzestrzeń – domena globalna w środowisku informacyjnym, składająca się z współzależnej sieci infrastruktur informatycznych i związanych z nimi zasobów danych, w tym Internetu, sieci telekomunikacyjnych, systemów komputerowych oraz wbudowanych procesorów i kontrolerów".

Źródło: Department of Defense Dictionary of Military and Associated Terms[22].

Definicja pochodzi z dokumentu JP 1-02 Ministerstwa Obrony USA i odnosi się do wyobrażanego środowiska, w którym informacje w cyfrowej postaci są udostępniane przez sieci komputerowe. Należy wziąć pod uwagę fakt, że jest to definicja o kontekście militarnym i jest utworzona językiem branżowym. Definicja po raz kolejny sugeruje jako by cyberprzestrzeń poza „*infrastrukturami informatycznymi Internetem, sieciami telekomunikacyjnymi, systemami komputerowymi*" nie istniała

[21] Sienkiewicz P., Ontologia cyberprzestrzeni, Zeszyty Naukowe, nr 13, Vol. 9, 2015, Warszawska Wyższa Szkoła Informatyki, s. 15.
[22] JP1_02 Department of Defense Dictionary of Military and Associated Terms 8 November 2010.

co jest niezgodne wobec głównego założenia, z którego wynika, że cyberprzestrzeń to środowisko.

Przedstawione definicje próbują wyjaśnić znaczenie słowa cyberprzestrzeń i należy zwrócić uwagę na to, że większość z nich to tylko nowa nazwa na coś co tak naprawdę nazwane już zostało np. Internet, sieci teleinformatyczne, sieci teletransmisyjne itd. Jak już przedstawiono pożądane jest znalezienie definicji zbliżonej do uniwersalnej, która sięga do źródła wspomnianego środowiska i nie skupia się tylko na stanie obecnym poprzez pryzmat wykorzystania cyberprzestrzeni. W tym celu przytoczono definicję, która spełnia przedstawione kryteria:

Definicja cyberprzestrzeni nr 6

„Cyberprzestrzeń – środowisko (na które składa się ląd, woda, powietrze, przestrzeń kosmiczna oraz pole elektromagnetyczne) i umieszczone w tym środowisku obiekty (w tym ludzie) posiadające zdolności kształtowania pola elektromagnetycznego i wykrywania jego zmian oraz magazynowania informacji o tych zmianach".

Źródło: Krzysztof Liderman, O istocie cyberprzestrzeni[23].

Konstrukcja definicji jest poprawna logicznie, przy czym nie stwierdzono żadnego błędu. Definicja odnosi się do istoty cyberprzestrzeni z próbą zaznaczenia namacalnych granic „*ląd, woda, powietrze, przestrzeń kosmiczna oraz pole elektromagnetyczne*". Treść definicji nie odnosi się do konkretnych systemów, Internetu, komunikowania się, sposobu wykorzystania cyberprzestrzeni co powoduje, że nie jest ona w żaden sposób ograniczona. W odróżnieniu od innych definicji widoczny jest brak operowania konkretnymi dziedzinami a jedynie fizyką zjawiska wyrażoną jako pole elektromagnetyczne połączone z środowiskiem, w którym ono występuje. Wszystkie zaprezentowane definicje traktują cyberprzestrzeń jako „tu i teraz" przy czym tak naprawdę cyberprzestrzeń istniała od zawsze natomiast do filozofów należy rozstrzygnięcie czy ludzkość ją odkryła czy wynalazła[24]? Należy zatem uznać, iż tak rozwinięty „definiens" wyczerpuje wszelkie przesłanki, aby uznać definicję za użyteczną w badaniach nad poprawą koncepcji bezpieczeństwa państwa.

[23] Liderman K., O istocie cyberprzestrzeni. Instytut Teleinformatyki i Cyberbezpieczeństwa WAT, s. 7.
[24] Liderman K., O istocie… dz. cyt., WAT, s. 3.

1.1.3. Cyberbezpieczeństwo

Zgodnie z logiką cyberbezpieczeństwo powinno być traktowane jako dziedzina mająca na celu zapobieganie i ochronę przed skutkami negatywnego wykorzystania cyberprzestrzeni. Zatem wskazane jest, aby zgodnie z etymologią tego słowa definicja nawiązywała do bezpieczeństwa w pośredniej lub bezpośredniej korelacji z cyberprzestrzenią. Ostatnia dekada spowodowała, że wraz z rosnącymi zagrożeniami definicja cyberbezpieczeństwa zyskała na popularności i prezentowane są rozmaite opisy tego twierdzenia.

Definicja cyberbezpieczeństwa nr 1

„*Cyberbezpieczeństwo – odporność systemów informacyjnych na wszelkie działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy*".

Źródło: Ustawa o krajowym systemie cyberbezpieczeństwa[25].

Jest to oficjalna definicja zawarta w ustawie. Uwagę przyciąga zwrot „*odporność systemów informacyjnych*" gdzie rodzi się pytanie jakie są miary odporności i co czyni system bardziej lub mniej odpornym. Kolejnym problemem tej definicji jest brak rozwinięcia na czym polegają pojęcia takie jak „*poufność, integralność, dostępność i autentyczność*" jedynie można zgadywać co autor miał na myśli. Definicję można zaliczyć jako posiadającą błąd „ignotum per ignotum".

Definicja cyberbezpieczeństwa nr 2

„Cyberbezpieczeństwo to zastosowanie technologii, procesów i kontroli w celu ochrony systemów, sieci, programów, urządzeń i danych przed atakami cybernetycznymi".

Źródło: Hackeru, Izraelski Instytut Szkoleniowy[26].

Definicja zaczerpnięta ze strony internetowej instytutu zajmującego się szkoleniem międzynarodowym z cyberbezpieczeństwa. Brakuje tu precyzji sformułowania takiego jak na czym polega „*atak cybernetyczny*"? Czy należy przez to rozumieć, że został przeprowadzony przez cybernetyków? Cyberprzestrzeń sama w sobie nie jest zagrożeniem a jedynie środowiskiem, w którym następuje materializacja zagrożeń. Analizując definicję nasuwają się kolejne pytania np. jeżeli tych „*technologii, procesów i kontroli w celu ochrony systemów, sieci, programów, urządzeń i danych przed atakami*

[25] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018 poz. 1560, s 2.
[26] https://hackeru.pl/cyberbezpieczenstwo-dla-poczatkujacych [dostęp 21.11.2021].

cybernetycznymi" nie będzie się stosowało to będzie mniej czy bardziej „cyberbezpiecznie?" Czy wszystkie te elementy muszą być stosowane łącznie? Definicja bardziej opisuje czynności stosowane w cyberbezpieczeństwie niż wyjaśnia istotę tego pojęcia.

Definicja cyberbezpieczeństwa nr 3

„*Cyberbezpieczeństwo – stan systemów informacyjnych oznaczający odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy informacyjne*".

Źródło: Departament Bezpieczeństwa i Zarządzania Kryzysowego[27].

Definicja ta bliska jest tej ustawowej. Niezbyt użyteczna, bo nie podano w jakich to stanach może znajdować się system informacyjny. Najprostszy zbiór takich stanów to zbiór dwuelementowy (działa, nie działa) natomiast to wymaga sformułowania uznawanych przez wszystkich interesariuszy kryteriów przejścia ze stanu do stanu. Poza tym co oznacza termin „*odporność*"? Jakie są miary „*odporności*"? Można zauważyć, że pojawia się problemem jak wyznaczyć „*dany poziom zaufania"*? zatem kolejny przykład nieznane przez nieznane.

Definicja cyberbezpieczeństwa nr 4

„*Cyberbezpieczeństwo RP – transsektorowy obszar bezpieczeństwa, obejmujący proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego elementów (struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej oraz będących w ich dyspozycji systemów teleinformatycznych i zasobów informacyjnych)*".

Źródło: Biuro Bezpieczeństwa Narodowego[28].

Definicja przedstawia klasyczne błędy. Po pierwsze nie da się postawić konkretnych granic cyberprzestrzeni i cyberbezpieczeństwa RP tzn. jakakolwiek miara by nie była stosowana (ilościowa czy jakościowa) to wynik będzie nieprecyzyjny. Kierując się tym tokiem myślenia to przykładowo system teleinformatyczny, który na terytorium RP uznawany jest za bezpieczny, to kilka metrów poza granicą państwa już nie będzie (i odwrotnie). Zachodzi więc uzasadniona potrzeba nietraktowania cyberbezpieczeństwa

[27] https://www.gov.pl/web/klimat/wspolpraca-krajowa [dostęp 21.11.2021 r.].
[28] https://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp 21.11.2021 r.].

poprzez pryzmat terytorialny. Po drugie, nie zdefiniowano terminu „*transsektorowości*" więc zaprezentowana definicja przedstawia nieznane przez nieznane.

Definicja cyberbezpieczeństwa nr 5

„*Cyberbezpieczeństwo – stanowi zespół zagadnień związanych z zapewnianiem ochrony w obszarze cyberprzestrzeni. Z pojęciem cyberbezpieczeństwa związana jest między innymi ochrona przestrzeni przetwarzania informacji oraz zachodzących interakcji w sieciach teleinformatycznych*".

Źródło: Encyklopedia Zarządzania[29].

W tej definicji dopatrzono się błędnego toku myślenia w postaci stawiania równości między bezpieczeństwem, a ochroną. Dodatkowo w zdaniu „z *pojęciem cyberbezpieczeństwa związana jest między innymi ochrona*" to ten zwrot między innymi oznacza, że są jakieś inne słowa związane z cyberbezpieczeństwem, które nie zostały wymienione w definicji co czyni ją za wąską.

Definicja cyberbezpieczeństwa nr 6 (anglojęzyczna)

„*Cybersecurity definition: Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure*".

Tłumaczenie:

„*Definicja cyberbezpieczeństwa: Strategia, polityka i normy dotyczące bezpieczeństwa i operacji w cyberprzestrzeni, które obejmują pełny zakres redukcji zagrożeń, zmniejszenie podatności, odstraszanie, międzynarodowe zaangażowanie, odpowiedź na incydenty, sprężystość i zasady odzyskiwania oraz działania, w tym operacje sieci komputerowej, zapewnienie informacji, egzekwowanie prawa, dyplomacja, wojskowe i wywiadowcze misje, ponieważ odnoszą się do bezpieczeństwa i stabilności globalnej infrastruktury informacyjnej i komunikacyjnej*".

Źródło: Internet[30], wyszukana za pomocą hasła „definition of cyber security".

[29] https://mfiles.pl/pl/index.php/Cyberbezpiecze%C5%84stwo [dostęp: 19.11.2021].
[30] https://niccs.cisa.gov/about-niccs/cybersecurity-glossary, Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review.

Definicja zaczerpnięta z dokumentu „White House Cyberspace Policy Review", która przedstawia sposób rozumowania cyberbezpieczeństwa za oceanem. Jest to interesujący przykład, ponieważ wprowadza nowy termin „*operacji w cyberprzestrzeni*". Godnym uwagi jest fakt, że definicja porusza szeroko pojętą problematykę jak np. „*egzekwowanie prawa, dyplomacja*" przy czym nie sprowadza cyberbezpieczeństwa tylko do bezpieczeństwa teleinformatycznego. Zastanawiający w tej definicji jest fragment „*obejmują pełny zakres redukcji zagrożeń*" i tu rodzi się pytanie jaki jest ten zakres i czy rzeczywiście ten „*pełen zakres zagrożeń*" jest możliwy do zredukowania? Kolejnym przykładem budzącym wątpliwość jest część odnosząca się do zakresu cyberbezpieczeństwa *„cyberbezpieczeństwo to strategia, polityka i normy dotyczące bezpieczeństwa i operacji w cyberprzestrzeni*". Czy aby na pewno cyberbezpieczeństwo możliwe jest do zapewnienia, przy wykorzystaniu tylko tych elementów? Ponownie przenosząc te elementy na inną płaszczyznę można by stwierdzić, że bezpieczeństwo państwa zależy tylko od norm, strategii i polityk co nie jest do końca prawdą.

Analiza przedstawionych definicji cyberbezpieczeństwa wskazuje, że są one obarczone „grzechem pierworodnym", ponieważ w żadnej z nich nie zostało poruszone nawiązanie do definicji bezpieczeństwa oraz cyberprzestrzeni. Jak już wspomniano połączenie tych obu pojęć w jedno pozwoli na uzyskanie jednolitej definicji, która będzie miała zastosowanie w dalszych badaniach nad koncepcją poprawy bezpieczeństwa państwa. W tym celu została utworzona definicja zgodna z opisywanymi założeniami.

Definicja cyberbezpieczeństwa nr 7 (autorska)

„Cyberbezpieczeństwo – nazwa oznaczająca, że na bezpieczeństwo nie wpływa negatywnie cyberprzestrzeń, która jest wykorzystywana do realizacji zagrożeń".

Dla tak przedstawionej definicji wyraźnie widać, że konstrukcja jest obarczona błędami (za krótka oraz nieznane przez nieznane) dlatego należy ją rozwinąć z uwzględnieniem pełnej definicji bezpieczeństwa i cyberbezpieczeństwa:

„Cyberbezpieczeństwo – nazwa oznaczająca, że na bezpieczeństwo (stan, w którym ryzyko i wynikające z nich zagrożenia są minimalizowane lub eliminowane) nie wpływa negatywnie cyberprzestrzeń (rozumiana jako środowisko, na które składa się ląd, woda, powietrze, przestrzeń kosmiczna oraz pole elektromagnetyczne posiadająca zdolności kształtowania pola elektromagnetycznego i wykrywania jego zmian oraz magazynowania informacji o tych zmianach), która jest wykorzystywana do realizacji zagrożeń".

Konstrukcja definicji została pozbawiona błędów logicznych oraz przedstawia pełne rozwinięcie definiensa, co pozwala uznać ją za akceptowalną. Dodatkowo, należy zwrócić uwagę, że definicja w początkowej części eksponuję rolę ryzyka jako względnej granicy pomiaru bezpieczeństwa co jest dość istotne z punktu widzenia miarodajności tej definicji.

1.1.4. Ciągłości działania

Pojęciem, które również zostało poddane analizie jest definicja ciągłości działania. Utrzymanie ciągłości działania jest ważnym elementem cyberbezpieczeństwa. Termin ten wywodzi się z zarządzania, ponieważ od niego w głównej mierze zależy sprawność i efektywność każdej organizacji w tym rozumianej również jako państwo.

Definicja ciągłości działania nr 1

„*Ciągłość działania – jest określana jako strategiczna i taktyczna zdolność instytucji do zaplanowania reagowania na incydenty oraz zakłócenia w funkcjonowaniu biznesowym instytucji w celu kontynuowania jej działalności na akceptowalnym, wcześniej ustalonym poziomie, ograniczania strat w przypadku wystąpienia incydentów lub innych zakłóceń”.*

Źródło: Instytut Technik Innowacyjnych[31].

Definicja niezbyt wyczerpująco przedstawia istotę ciągłości działania. Należy poddać rozważaniu wątpliwość czy tylko na „za*planowaniu*” polega ciągłość działania? Wdrażać tego co „*zaplanowano*” nie trzeba. Wskazane jest również rozwinięcie o jakich incydentach mówimy, bo przecież nie o tych, które zgodnie ze Słownikiem Języka Polskiego oznaczają „nieprzyjemne wydarzenia”. Kolejną wadą tej definicji jest „*działalności na akceptowalnym poziomie*” pomimo, że „*wcześniej ustalonym*” to nadal nie rozwinięto jakie czynniki decydują o akceptacji poziomu.

Definicja ciągłości działania nr 2

„Ciągłość działania – postulatywny stan odporności organizacji na zakłócenia”.

Źródło: Komisja Nadzoru Finansowego[32].

Pomimo, że długość definicji nie jest absolutnie wykładnikiem jej poprawności

[31] Białas A., Zarządzanie ciągłością działania oraz bezpieczeństwem informacji i innych zasobów w górnictwie, Instytut Technik Innowacyjnych EMAG, s. 52.

[32] Maderak K., Zapewnienie ciągłości działania, Departament Funduszy Inwestycyjnych i Funduszy Emerytalnych Warszawa, 2018, s. 9.

to czy tak złożony proces jak ciągłość działania można zdefiniować w sześciu słowach? Wątpliwości ulega zwrot „*postulatywny stan odporności*", ponieważ kto i na jakiej podstawie ustala te postulaty? Czyżby autor po raz kolejny miał na myśli, że zgodnie z SJP chodzi o żądanie, wniosek, propozycję, życzenie? Kolejnym godnym uwagi a przede wszystkim wyjaśnienia jest człon „*odporność organizacji na zakłócenia*" gdzie nie zdefiniowano o jakich zakłóceniach jest mowa. Tak jak wspomniano jednym zdaniem możemy opisać przedmiot natomiast niewskazane jest definiowanie zbioru działań podejmowanych przez organizację jakim jest ciągłość działania, ponieważ od razu powoduje to błąd konstrukcyjny.

Definicja ciągłości działania nr 3

„*Ciągłość działania – strategia zapewniająca wznowienie działalności i ciągłości działania w przypadku wystąpienia zakłócenia tej działalności w określonym Docelowym Czasie wznowienia (RTO) poprzez określenie odpowiednich Planów Ciągłości Biznesowej (BCP). Plany Ciągłości Działania definiowane są dla wcześniej określonych działalności krytycznych*".

Źródło: System BCM.

Definicja zaczerpnięta z system zarządzania ciągłością działania biznesu (BCMS) zgodnego z normami ISO 22301 i ISO 27031. Uwagę przyciąga tzw. zlepek definicji wyrażonych w skrótach np. „*RTO, BCP*" co czyni definicję obarczoną błędem „ignotum per ignotum" czyli nieznane przez nieznane. Na uwagę zasługuje również słowo „*strategia*", która jest utożsamiana z wizją i planistyką a nie konkretnymi działaniami w organizacji.

Definicja ciągłości działania nr 4

„Zarządzanie ciągłością działania – działania mające na celu utrzymanie ciągłości biznesu na założonym poziomie. W cyberbezpieczeństwie dotyczy dostępności zasobów informatycznych wspierających realizację krytycznych procesów biznesowych (infrastruktura, sieć, sprzęt, systemy, aplikacji, dane)".

Źródło: Portal GOV[33].

Definicja posiada kilka błędów. Po pierwsze „nieznane przez nieznane" na co wskazuje fragment „*w cyberbezpieczeństwie dotyczy*", gdzie cyberbezpieczeństwo nie jest w żaden sposób rozwinięte i pozostaje niewiadomą. Kolejny błąd to „idem per idem", czyli to

[33] https://www.gov.pl/web/baza-wiedzy/zapewnienie-ciaglosci-dzialania [dostęp: 01.02.2021].

samo przez to samo „*Zarządzanie ciągłością działania - działania mające na celu utrzymanie ciągłości.”* Należy pamiętać, że definicja powinna dążyć do uniwersalności dla wszystkich dziedzin a nie być inna dla cyberbezpieczeństwa inna dla biznesu i organizacji. Zauważalny jest brak zdefiniowania źródła istoty problemu a jedynie opisanie pewnej części.

Definicja ciągłości działania nr 5

„Ciągłość działania – jest to zapewnianie na drodze ustanowienia procesu i organizacji działania, że pewien uznawany za minimalny, niezbędny poziom działania operacyjnego zostanie zachowany nawet w warunkach krytycznego zakłócenia”.

Źródło: słownik pojęć[34].

W definicji tej użyto słów „*działania operacyjnego*” gdzie w odróżnieniu od innych definicji wymieniane są szczeble taktyczne i strategiczny. Pojęcie ciągłości działania powinno być zunifikowane niezależnie od rozpatrywanego poziomu. Zastanawiające jest pytanie jakie „*poziomy działania*” autor miał na myśli? Jak już wspomniano odróżnia się dwa poziomy akceptowalny oraz nieakceptowalny. Należy również zwrócić uwagę na słowo „*zapewnianie*” z którego nic nie wynika, ponieważ z nie jest to tożsame z realnymi działaniami.

Definicja ciągłości działania nr 6 (anglojęzyczna)

„Business Continuity is the development of strategies, plans and actions which provide protection or alternative modes of operation for those activities or business processes which, if they were to be interrupted, might otherwise bring about a seriously damaging or potentially fatal loss to the enterprise”.

Tłumaczenie:

„Ciągłość biznesowa to opracowywanie strategii, planów i działań, które zapewniają ochronę lub alternatywne tryby działania dla tych aktywności lub procesów biznesowych, które w przypadku ich przerwania mogłyby spowodować poważne szkody lub potencjalnie krytyczne straty dla przedsiębiorstwa”

Źródło: Business Continuity and Disaster Recovery Trends[35].

Ciągłość działania jest przedstawiona jako „*ciągłość biznesowa*” przy czym każdą organizację mającą na celu interes, przedsięwzięcie handlowe, produkcyjne czy

[34] http://www.2business.pl/index.php?page=ciaglosc-dzialania---slowniczek-pojec [dostęp: 08.08.2023].
[35] Business Continuity and Disaster Recovery Trends, Considerations, & Leading Practices November 13, 2014, Presented by: Jon Bronson - Los Angeles Trey MacDonald – Atlanta.

administracyjne można utożsamić z biznesem. Pozytywnym aspektem tej definicji jest to, że zakłada ona nie tylko „*ochronę*" systemu, ale i utrzymanie pewnych procesów jako „*alternatywne sposoby działania*" niezależne od siebie. Problematyczna natomiast jest część „*mogłyby spowodować poważne szkody lub potencjalnie krytyczne straty*" gdzie należałoby określić na jakiej podstawie i gdzie jest granica poważna szkody oraz krytycznej straty. Zachowanie ciągłości działania (biznesowej) wiąże się z „planem awaryjnym" organizacji w czasie wystąpienia zagrożenia. Zasadnym jest zatem określenie w definicji co ma być „utrzymane" w takiej sytuacji jakie parametry przedsiębiorstwa i na jakim poziomie tak aby możliwym było wyznaczenie punktu odniesienia względem celów z jednoczesnym ustaleniem granicy, po przekroczeniu której przedmiotowa ciągłość zostaje przerwana. W tym celu zaproponowana została definicja:

Definicja ciągłości działania nr 7

„Ciągłość działania organizacji – to zdolność organizacji do realizacji podstawowych zadań biznesowych na określonym poziomie jakości z przerwami nie dłuższymi niż dopuszczalne".

Źródło: Krzysztof Liderman[36].

Zdanie „*realizacji podstawowych zadań biznesowych*" utożsamia się z celami organizacji, przy czym w zależności od podmiotu będą one nieco się różniły od siebie. Zadania biznesowe muszą być realizowane na „*określonym poziomie jakości*", który może wyznaczyć odpowiedni certyfikat ISO lub zawarta umowa. Nie należy tego rozpatrywać jako nieznane przez nieznane, ponieważ wspomniane ISO jest rozumiane jako wyznacznik jakości a nie jako oddzielny dokument, do którego odnosi się definicja. Kolejnym parametrem determinującym ciągłość działania jest czas, który uwzględniono w zdaniu „*z przerwami nie dłuższymi niż dopuszczalne*" a wyznacznikiem „dopuszczalnego czasu" są wyniki analizy ryzyka. Należy zwrócić uwagę, że do realizacji tak pojmowanej „ciągłości działania" muszą być dostępne w wystarczającej ilości i na odpowiednim poziomie jakościowym zasoby takie jak: infrastrukturalne, ludzkie, informacyjne, które pozwolą oszacować przedmiotową ciągłość.

Nierozdzielną częścią strategii biznesowej każdej organizacji jest ciągłości działania, którą nie jest tak łatwo zdefiniować. Samo wyrażenie być może jest intuicyjne

[36] Liderman K., Bezpieczeństwo informacyjne. Nowe wyzwania". PWN. 2017, s. 239.

natomiast aby opisać je w sposób niepozostawiający możliwości do podważenia jest już problematyczne. Analiza definicji ciągłości działania nr 6 wykazała, że istotnym elementem ciągłości działania jest analiza ryzyka, ponieważ, to wskaźniki będące wynikiem tej analizy w głównej mierze tworzą miarodajne parametry do utrzymania „ciągłości" w organizacji.

1.1.5. Informacyjna ciągłości działania

Cyberbezpieczeństwo w głównej mierze dotyczy bezpieczeństwa zasobów informacyjnych, które są istotne z punktu widzenia utrzymania ciągłości działania danego podmiotu. W tym przypadku mowa o „informacyjnej ciągłości działania" (dalej w skrócie ICD), która jest jej newralgiczną częścią. Zasoby informacyjne w organizacji stanowią chronioną wartość nie tylko ze względu na regulacje prawne takie jak np. (RODO, OIN) ale przede wszystkim dlatego, że są to zasoby w krótkim czasie trudno odtwarzalne. Należy zatem uznać, że informacja jest równie ważna jak personel, narzędzia, materiały czy infrastruktura, ponieważ bez zasobów w postaci danych, wiedzy, technologii, komunikacji nie jest możliwym przeprowadzenie żadnego procesu w przedsiębiorstwie. Współczesne modele organizacji budowane w oparciu o procesy wskazują na potrzebę zwrócenia szczególnej uwagi na zasoby informacyjne, które w warunkach działania na globalnych rynkach nabierają strategicznego znaczenia. Dlatego jednym z podstawowych problemów zarządzania współczesną organizacją wydaje się kwestia zapewnienia ciągłości działania w wymiarze informacyjnym[37]. Należy przez to rozumieć, że zmieniły się priorytety bezpieczeństwa i dla każdej organizacji ważne staje się nie tylko operowane własnymi, bogatymi zasobami, ale również umiejętne minimalizowanie ryzyka zerwania biznesowej ciągłości działania w momencie utraty ciągłości informacyjnej w relacji z otoczeniem zewnętrznym[38]. Sytuacja ta wymusza poddanie szczególnej opiece zintegrowane systemy informatyczne zarządzania, które poprzez działania prewencyjne oraz minimalizację skutków materializacji zagrożeń są w stanie w dość krótkim czasie przejść na alternatywne rozwiązania. W przedsiębiorstwach komercyjnych utrata lub odcięcie od zasobów informacyjnych może spowodować przestój i „wypadnięcie" z obiegu, co z pewnością wykorzysta konkurencja. Zatem realnym staje się powiedzenie,

[37] Szwarc K., Zaskórski P., Identyfikacja zagrożeń dla ciągłości działania organizacji, WAT, Studia Bezpieczeństwa Narodowego, 2012, Tom R. 2, Nr 3, s. 215.
[38] Zaskórski P., Zarządzanie organizacją w warunkach ryzyka utraty informacyjne ciągłości działania, WAT, 2011, s. 145.

że szeroko pojęta informacja jest walutą obecnych czasów i powinna być chroniona jak najwyższe dobro.

Z tak zaprezentowanym postrzeganiem definicja informacyjnej ciągłości działania w swej istocie powinna nawiązywać do zasobów informacyjnych, które bezpośrednio przekładają się na utrzymanie ciągłości działania organizacji oraz do alternatywnych procesów rozumianych jako plan awaryjny dostępu i wykorzystania informacji. Należy tu wspomnieć, że pomimo rangi jaką pełni ICD w organizacji problematyczne jest doszukanie się jej definicji w różnych źródłach co można tłumaczyć tym, że ten istotny element „biznesowy" jest niezauważalny lub niedoceniany. W ogólnym rozumieniu ICD traktowana powinna być jako zdolność organizacji do reagowania na zagrożenia mające wpływ na zasoby informacyjne. Chodzi o to, aby tam, gdzie to możliwe szybko przywrócić normalne warunki działania a tam, gdzie to niemożliwe przejść do zaplanowanego sposobu zastępczego wykonywania zadań.

Autorska definicja informacyjnej ciągłości działania

„Informacyjna ciągłość działania – to zdolność podmiotu do realizacji statutowych zadań w warunkach zakłóconego operowania zasobami informacyjnymi z uwzględnieniem alternatywnych procesów, które mogą zostać wdrożone w sytuacji zaistnienia interakcji przejawów zagrożenia z podatnością przy użyciu sił i środków oraz w czasie niepowodującym obniżenia efektywności danego podmiotu".

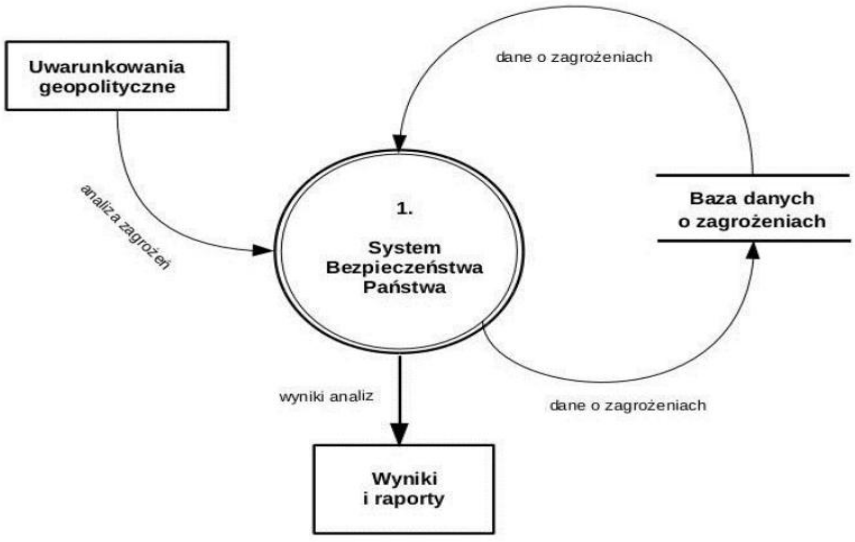
W definicji celowo użyto zwrotu „*to zdolność podmiotu*" ponieważ ICD jest stanem do którego dany podmiot dąży zatem nie należy jej traktować jako stałego elementu przypisanego do organizacji. Również świadomie zamiast terminu wystąpienia zagrożeń użyto sformułowania „*zaistnienia interakcji przejawów zagrożenia z podatnością*" ponieważ utrata ICD zależna jest nie tylko od zaistnienia sytuacji niekorzystnej, ale też od wszelkiego rodzaju podatności co w dalszej części badań będzie szczegółowo omówione. Należy zwrócić uwagę na część zdania „*przy użyciu sił i środków oraz w czasie niepowodującym obniżenia efektywności*" gdzie z punktu widzenia ICD zasadnym jest, aby wszelkie działania mające na celu przywrócenie normalnego stanu organizacji nie powodowały zaburzenia „trójkąta wymiarów projektu[39]" na który składa się zakres-koszt-czas. Z tego samego powodu należy przyjąć za słuszne podejście, że nie wszystkie działania „naprawcze" są możliwe do wdrożenia,

[39] Zaskórski P., Ewaluacja projektów, "Zeszyty Naukowe Wyższej Szkoły Informatyki w Warszawie", 2012, nr 8, s. 36.

ponieważ zbyt duże odstępstwa w którymś z wymiarów spowodują wręcz przeciwny skutek dla ciągłości biznesowej i przełożą się na utratę płynności finansowej lub podważą renomę organizacji. Niezależnie od punktu widzenia cyberbezpieczeństwo jest ściśle związane z informacyjną ciągłością działania, która ma kluczowy wpływ na funkcjonowanie każdej organizacji, rozumianej również jako państwo.

1.2. System bezpieczeństwa państwa

W bezpieczeństwie Polski kluczową rolę odgrywa system bezpieczeństwa państwa definiowany jako *„całość sił (podmiotów), środków oraz zasobów przeznaczonych przez państwo do realizacji zadań w dziedzinie bezpieczeństwa odpowiednio do tych zadań zorganizowana (w podsystemy i ogniwa) utrzymywana i przygotowywana*[40]*”.* Innymi słowy jest to zbiór wszystkich systemów bezpieczeństwa w kraju. Należy zwrócić uwagę na fakt, że system bezpieczeństwa państwa często jest błędnie mylony z Systemem Bezpieczeństwa Narodowego. Różnica jest następująca otóż system bezpieczeństwa państwa jest to ogół wszystkich systemów bezpieczeństwa w kraju natomiast System Bezpieczeństwa Narodowego jest jego głównym systemem. Zatem w systemie bezpieczeństwa państwa istnieje wiele systemów a SBN jest tym najważniejszym.



Rys. 5. Diagram kontekstowy systemu bezpieczeństwa państwa.
Źródło: https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-c67752ef-9df6-4c83-87fb-8fe3c517e13c/c/ZNPSl_OiZ_2017_100_Spustek__Paluch.pdf [dostęp: 03.04.2025].

[40] Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013, s. 36.

Do głównych zadań systemu bezpieczeństwa państwa zgodnie z grafiką (Rys. 5), należy analiza zagrożeń, tworzenie bazy danych o zagrożeniach oraz raportowanie wyników analiz. Natomiast w przypadku materializacji zagrożeń mających znamiona kryzysu uruchamiany jest odpowiedni podsystem do monitorowania, reagowania i przywracania stanu normalnego w państwie[41]. W systemie bezpieczeństwa państwa wyróżnia się kluczowe systemy w ujęciu zagrożeń wykorzystujących cyberprzestrzeń do realizacji. Należą do nich:

- System Bezpieczeństwa Narodowego;
- Krajowy System Cyberbezpieczeństwa;
- System Zarządzania Kryzysowego;
- System Obrony Państwa.

Każdy z wymienionych systemów posiada w swej strukturze systemy/podsystemy niższego szczebla, które wykonują zadania adekwatne do ich przeznaczenia. Próba skatalogowania wszystkich systemów i podsystemów jest trudna do realizacji, ponieważ nie istnieje jeden uniwersalny wskaźnik, za pomocą którego można je zinwentaryzować. W dysertacji na potrzeby badań przyjęto wskaźnik „operacyjności" do stopniowania ważności systemów co zostało omówione szczegółowo w podrozdziale 1.5.

Prezentowane systemy bezpieczeństwa państwa współcześnie są silnie uzależnione od technologii cyfrowych. Biorąc pod uwagę kierunek obecnych zagrożeń cyberbezpieczeństwo staje się kluczowym elementem do utrzymania zdolności ochronnych. Blokowanie, kradzież czy nieuprawniony dostęp do zasobów informacyjnych są to zagrożenia, które mogą nie tylko zniwelować wysiłki podczas funkcjonowania systemu, ale mogą być wykorzystane przeciwko własnym siłom i środkom. Aby można było w pełni wykorzystać zaplanowany potencjał głównych systemów wobec zagrożeń muszą być spełnione pewne warunki, do których należą:

- dobrze skonstruowane prawo pozwalające w pełni wykorzystać możliwości systemu;
- odpowiednia ilość i jakość infrastruktury adekwatna do rozmiarów zagrożeń;
- odpowiednia ilość i jakość specjalistów zapełniająca wszystkie wakaty;
- wystarczające środki finansowe niepowodujące cięć pozwalające się rozwijać.

[41] Spustek H., Paluch A., 2017, Struktura systemu bezpieczeństwa narodowego polski. Uniwersytet Opolski, Zeszyty naukowe politechniki śląskiej, seria: organizacja i zarządzanie z. 100 Nr kol. 1972, s. 109.

Chcąc zapewnić prawidłowe funkcjonowanie każdego systemu należy dążyć do utrzymania powyższych czterech elementów na zaplanowanym (akceptowalnym) poziomie.

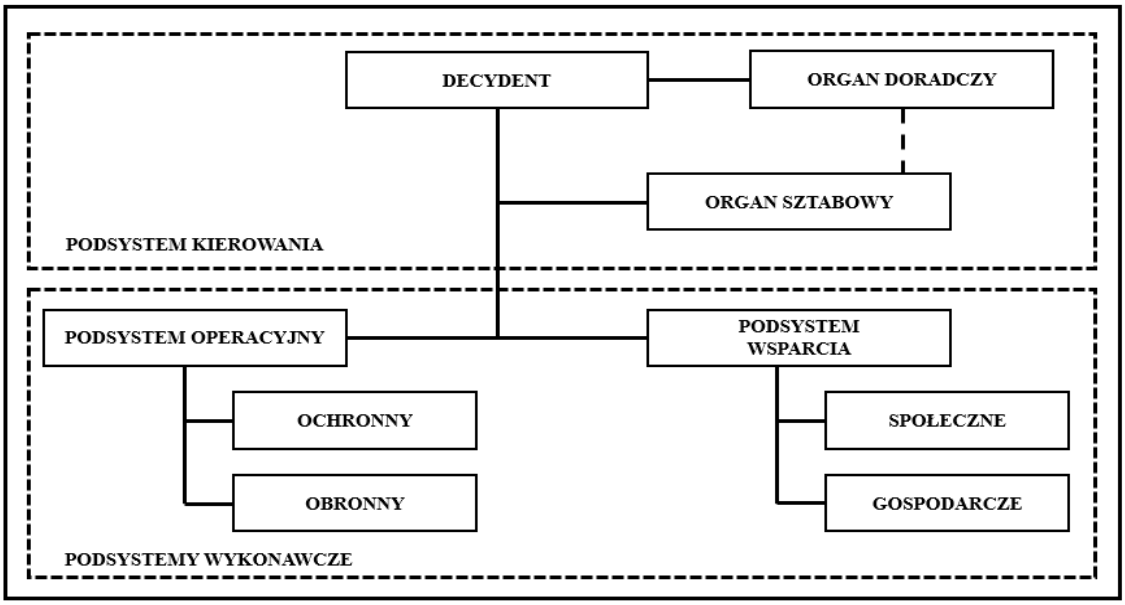
1.2.1. System Bezpieczeństwa Narodowego

System Bezpieczeństwa Narodowego (SBN) został zdefiniowany jako: *„System obejmujący siły, środki i zasoby przeznaczone do realizacji zadań w obszarze bezpieczeństwa narodowego odpowiednio zorganizowane utrzymywane i przygotowywane*[42]*”.* Zgodnie ze strategią rozwoju SNB ma na celu przygotowanie i wykorzystanie sił oraz środków będących w dyspozycji państwa do przeciwdziałania zagrożeniom godzącym w przetrwanie narodu i państwa, integralność terytorialną, niezależność polityczną i suwerenność, sprawne funkcjonowanie instytucji państwa oraz rozwój społeczno-gospodarczy[43]. W dużym uproszczeniu można powiedzieć, że system ten jest przeciwstawny do zagrożeń zarówno wewnętrznych jak i zewnętrznych a jedną z miar jego efektywności jest zdolność adaptacji do współczesnych niebezpieczeństw. Obserwacja i analiza SBN wskazuje, że zmiany w tym systemie zachodzą z pewnym opóźnieniem w stosunku do ewolucji zagrożeń co wymusza wręcz ciągły proces monitorowania i analizy ryzyka wystąpienia niekorzystnych zmian w środowisku bezpieczeństwa poprzez aktualizację procedur lub zorientowanie na nowe kierunki. Należy tu wspomnieć, że natura każdego systemu a w tym SBN sprawia, że nie jest on pozbawiony niedoskonałości, dlatego tak ważne jest identyfikowanie luk, wad, słabości i wprowadzanie działań usprawniających szczególnie w tak kluczowym obszarze jakim jest bezpieczeństwo. Aby stworzyć koncepcję poprawy bezpieczeństwa państwa należy dokonać wnikliwego przeglądu struktury całego systemu oraz przeanalizować główne kierunki działań wraz z szczegółowym wyeksponowaniem zadań dla tego systemu.

Podstawową kwestią jednocześnie problematyczną jest fakt, że polskie prawo nie reguluje funkcjonowania SBN[44]. Występuje brak jednolitego aktu prawnego co powoduje, że działania podejmowane przez organy czy podmioty mają charakter sektorowy lub transsektorowy oraz rozproszony. Szczegółowo rzecz ujmując SBN nie stanowi samodzielnie funkcjonującej struktury państwowej. Jak w każdym dużym

[42] https://zpe.gov.pl/a/system-bezpieczenstwa-narodowego---ogolna-charakterystyka/D10Rhn2ZnC [dostęp: 06.08.2024].
[43] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022, s 13.
[44] Kołodziejczak M., Wymiar prawny systemu kierowania bezpieczeństwem narodowym RP., Studenckie Zeszyty Naukowe 2019, Vol. XXII, nr 42., s. 93

systemie tak i w skład SBN wchodzą podsystemy (Rys. 6). Głównym komponentem SBN jest podsystem kierowania, który tworzą organy władzy publicznej i kierownicy jednostek organizacyjnych. Organy te wykonują zadania związane z bezpieczeństwem kraju oraz dowodzeniem Siłami Zbrojnych RP[45]. Podsystem wykonawczy tworzą siły i środki będące w jurysdykcji właściwych ministrów kierujących działami administracji rządowej, organów centralnych, wojewódzkich, samorządu terytorialnego oraz innych instytucji i podmiotów państwowych odpowiedzialnych za realizację ustawowo określonych zadań[46]. Podsystem ten swe cele statutowe realizuje poprzez instytucje operacyjne jak i wspierające. Współbieżnie do systemów wsparcia w SBN biorą udział jeszcze organizacje pozarządowe (non-profit, ang. non-government organization NGO).



Rys. 6. Podsystemy w Systemie Bezpieczeństwa Narodowego.
Źródło: opracowanie własne.

Co ważne są to organizacje skupiające wysiłek na rzecz wybranego interesu, przy czym nie działają w celu osiągnięcia zysku. W odróżnieniu od organów publicznych podobnie jak przedsiębiorcy są prywatne i powstają z inicjatywy ich założycieli (najczęściej prywatnych osób fizycznych) ale w odróżnieniu od przedsiębiorstw podobnie jak władze publiczne działają w interesie publicznym a nie prywatnym. Charakterystyczną cechą organizacji pozarządowych jest więc brak powiązań z władzą publiczną i bywają nazywane często trzecim sektorem obok sektora publicznego i prywatnego. Godnym uwagi jest liczba organizacji tego typu w Polsce, gdzie przykładowo wg. statystyk w 2023

[45] Zaskórski P., Ewaluacja projektów, "Zeszyty Naukowe Wyższej Szkoły Informatyki w Warszawie", 2012, nr 8, s.14.
[46] Tamże, s. 14.

r. aktywnie działalność prowadziło 98 tys. rejestrowych organizacji non-profit. Całościowe podejście do bezpieczeństwa państwa jest procesem złożonym i z tego też powodu zostały wyodrębnione poszczególne dziedziny do których zaliczono obronę ochronę społeczną i gospodarczą (Rys. 7).

KIEROWANIE BEZPIECZEŃSTWEM NARODOWYM	DZIEDZINY BEZPIECZEŃSTWA NARODOWEGO															
	OBRONA			OCHRONA			SPOŁECZNE					GOSPODARCZA				
	SEKTORY BEZPIECZEŃSTWA NARODOWEGO															
	DYPLOMATYCZNY	MILITARNY	WYWIADOWCZY	KONTRWYWIADOWCZY	PRAWA I PORZĄDKU PUBLICZNEGO	RATOWNICTWA	KULTUROWY	EDUKACYJNY	SOCIALNY	DEMOGRAFICZNY	MIGRACYJNY	FINANSOWY	ENERGETYCZNY	TRANSPORTOWY	INFRASTRUKTURY KRYTYCZNEJ	ŚRODOWISKA NATURALNEGO
	TRANSSEKTOROWE OBSZARY BEZPIECZEŃSTWA (CYBERBEZPIECZEŃSTWO, BEZPIECZEŃSTWO ANTYTERRORYSTYCZNE)															
PODMIOTY BEZPIECZEŃSTWA NARODOWEGO REALIZUJĄCE ZADANIA STRATEGICZNE (OPERACYJNE - WSPIERAJĄCE)																
PREZYDENT, RADA MINISTRÓW	MSZ … MON MSW	MON … MSW MSZ	AW SWW	ABW SKW	MSW Policja SG SOP MS SW MAC CBA Prokura.	MSW PSP OCK … MAC MŚ	MKiDN MEN … OP	MNiSZW MEN … MKiDN uczelnie szkoły	MPiPS … MZ OP	MPiPS … MZ OP	UDSC … MAC MSW	MF … MG MRiRW MSP MRR MTBiGM	MG … MSP	MTBiGM … MG MSP	MTBiGM … MG MSP	MŚ … OP

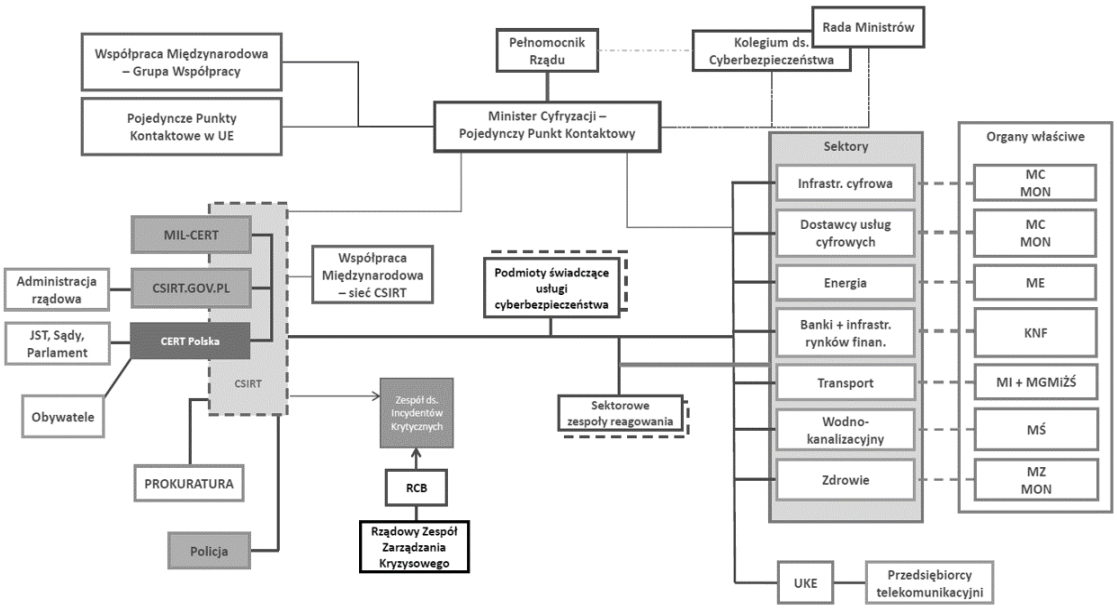
Rys. 7. Dziedziny bezpieczeństwa i sektory w Systemie Bezpieczeństwa Narodowego. Źródło: opracowanie własne na podstawie SBN RP.

Każdej z tych dziedzin przyporządkowano sektory oraz podmioty realizujące określone w dokumentach normatywnych zadania na rzecz bezpieczeństwa. Analizując dziedziny BN można zauważyć, że istnieją tzw. transsektorowe obszary bezpieczeństwa, które w swym spektrum odpowiedzialności przenikają wszystkie pozostałe gałęzie (branże) i są z nimi ściśle powiązane. Najbardziej obszernym jest cyberbezpieczeństwo również rozumiane jako bezpieczeństwo systemów teleinformatycznych, które jest szczególnym wyzwaniem, ponieważ materializacja zagrożeń w tej sferze w sposób bezpośredni jak i pośredni generuje zagrożenia w innych sektorach bezpieczeństwa.

1.1.2. Krajowy System Cyberbezpieczeństwa

W Polsce w ubiegłej dekadzie zaczęto na poważnie myśleć o tworzeniu struktur zdolnych do cyberobrony. Z tego też powodu powstał Krajowy System Cyberbezpieczeństwa (KSC) implementujący do polskiego porządku prawnego

dyrektywę Parlamentu Europejskiego i Rady (UE) tzw. Dyrektywę NIS[47] mającą na celu utworzenie efektywnego systemu bezpieczeństwa teleinformatycznego funkcjonowania państwa (Rys. 8). Dokumentem normatywnym regulującym jest ustawa[48], która w swym zakresie określa organizację Krajowego Systemu Cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu. Jest to pierwsza kompleksowa regulacja w Polsce dotycząca szerszego ujęcia problemu bezpieczeństwa systemów teleinformatycznych w sektorze publicznym jak i prywatnym. W skonsolidowanej strukturze istotną rolę odgrywają Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT[49]), które odpowiedzialne są za koordynację oraz reagowanie na te incydenty rozumiane jako pojedyncze zdarzenie lub serie zdarzeń związanych z bezpieczeństwem informacji w cyberprzestrzeni.



Rys. 8. Struktura Krajowego Systemu Cyberbezpieczeństwa.
Źródło: Departament Bezpieczeństwa i Zarządzania Kryzysowego, Ministerstwo Energii.

Godnym uwagi jest fakt, że do czasu wejścia w życie ustawy o KSC podmioty i organizacje rządowe miały inny charakter tj. nie stanowiły jednolitego systemu a jedynie były to dziedzinowe instytucje zajmujące się bezpieczeństwem teleinformatycznym. Zmiany jakie zachodzą współcześnie w środowisku cyberprzestrzeni zmuszają do ciągłej aktualizacji systemu cyberbezpieczeństwa i tak w chwili obecnej realizowany jest proces wdrożenia nowelizacji ustawy o KSC, która w swej zawartości wprowadza zmiany

[47] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wspólnego poziomu bezpieczeństwa systemów informatycznych na terytorium Unii.
[48] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560.
[49] CSIRT (ang. Computer Security Incident Response Team).

strukturalne całego systemu. W tym przypadku zmiany również są podyktowane wejściem w życie Dyrektywy NIS II, wdrożonej przez Komisję Europejską.

Podstawową zmianą w „nowej" strukturze KSC będzie utworzenie przeznaczonych zespołów CSIRT przez organy właściwe dla każdego z 11 sektorów, które będą nadzorowane przez wiodący CSIRT NASK. W porównaniu do poprzedniej struktury w nowej uwzględniono m.in. administrację publiczną, sektor żywności, telekomunikację, ścieki, przemysł, zarządzanie odpadami i przestrzeń kosmiczną oraz rozszerzono zakres infrastruktury cyfrowej. Ulegną również zmianie wymagania od dostawców usług cyfrowych w tym kluczowych oraz zostanie położony większy nacisk na większe zarządzanie ryzykiem co przełoży się na podniesienie poziomu utrzymania informacyjnej ciągłości działania w państwie. Nowością będzie również wprowadzenie odpowiedzialności kierownictwa firmy za zarządzanie ryzykiem w zakresie cyberbezpieczeństwa. Zaproponowano ustanowienie Europejskiej sieci zarządzania kryzysowego w cyberprzestrzeni (European Cyber Crises Liaison Organisation Network, EU-CyCLONe), której zadaniem będzie koordynacja zarządzania incydentami wielkiej skali na poziomie Unii Europejskiej[50]. W wyniku zmian powstanie kolejny CSIRT INT podległy Agencji Wywiadu, który ma wspierać obsługę incydentów zgłaszanych przez jednostki podległe Ministrowi Spraw Zagranicznych (w tym placówki zagraniczne RP)[51]. Działania w zakresie cyberbezpieczeństwa będą wspierać ISAC (Information Sharing and Analysis Center) centra wymiany i analiz informacji tworzone jako oddolne i dobrowolne inicjatywy sektorowe lub dziedzinowe, które mogą działać w formie partnerstwa publiczno-prywatnego (PPP). Ich zadaniem będzie analiza informacji o potencjalnych zagrożeniach i podatnościach oraz wymiana informacji a także dzielenie się najlepszymi praktykami z otoczeniem.

Obecnie Krajowy System Cyberbezpieczeństwa jest cały czas wystawiany na próbę poprzez ingerencję wrogich podmiotów. Jest on atakowany w sposób niemalże ciągły co z operacyjnego punktu widzenia czyni go bardziej newralgicznym niż System Obrony Państwa czy System Zarządzania Kryzysowego, dlatego tak ważne jest eliminowanie w nim wszelkich podatności. Pomimo usilnych starań z należytą starannością wprowadzania znowelizowanej ustawy twórcy nie uniknęli błędów. Istnieją obszary, które nie są regulowane przez ustawę oraz takie, które po implementacji

[50] Biuletyn Polskiego Towarzystwa Informatycznego, nr 4/2021, ISSN 2719-8472, s. 30.
[51] Tamże, s. 30.

dokumentu wygenerują szereg dodatkowych podatności systemowych. Wyniki szczegółowej analizy projektu nowelizacji ustawy przedstawiono w rozdziale III. Dodatkowo należy wziąć pod uwagę, że KSC powinien zrzeszać wszystkie krajowe organy odpowiedzialne za cyberbezpieczeństwo a w rzeczywistości tak nie jest. Mowa tu o Centralnym Biurze Zwalczania Cyberprzestępczości podlegającym pod Policję (MSWiA), które nie jest w tym systemie i wejście w życie nowelizacji ustawy tego stanu rzeczy nie zmieni.

1.2.3. System Zarządzania Kryzysowego

Ważną rolę w zapewnieniu bezpieczeństwa państwa pełni Zarządzanie Kryzysowe (ZK), które zostało zdefiniowane 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 kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej*[52]*”*. W skład Systemu Zażądania Kryzysowego wchodzą liczne podsystemy. W tym miejscu należy również zaznaczyć jak ważną rolę w zapewnieniu bezpieczeństwa pełnią niemieszczące się w ogólnej klasyfikacji współbieżne z SZK systemy wsparcia bezpieczeństwa państwa do których należą m.in.:

- system ochrony infrastruktury krytycznej;
- system ochrony granicy państwowej;
- system przeciwpowodziowy;
- system ochrony informacji niejawnych;
- system bezpieczeństwa międzynarodowego;
- Krajowy System Ratowniczo-Gaśniczy;
- Krajowy System Elektroenergetyczny;
- Krajowy System Wykrywania Skażeń i Alarmowania;
- inne.

System Zarządzania Kryzysowego jest elementem Systemu Bezpieczeństwa Narodowego. Wynika to z faktu, że zapewnia obywatelom ochronę przed zagrożeniami

[52] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym. Dz.U. 2007 nr 89 poz. 590.

związanymi z występowaniem klęsk żywiołowych oraz katastrof spowodowanych zarówno siłami natury jak i działalnością człowieka.

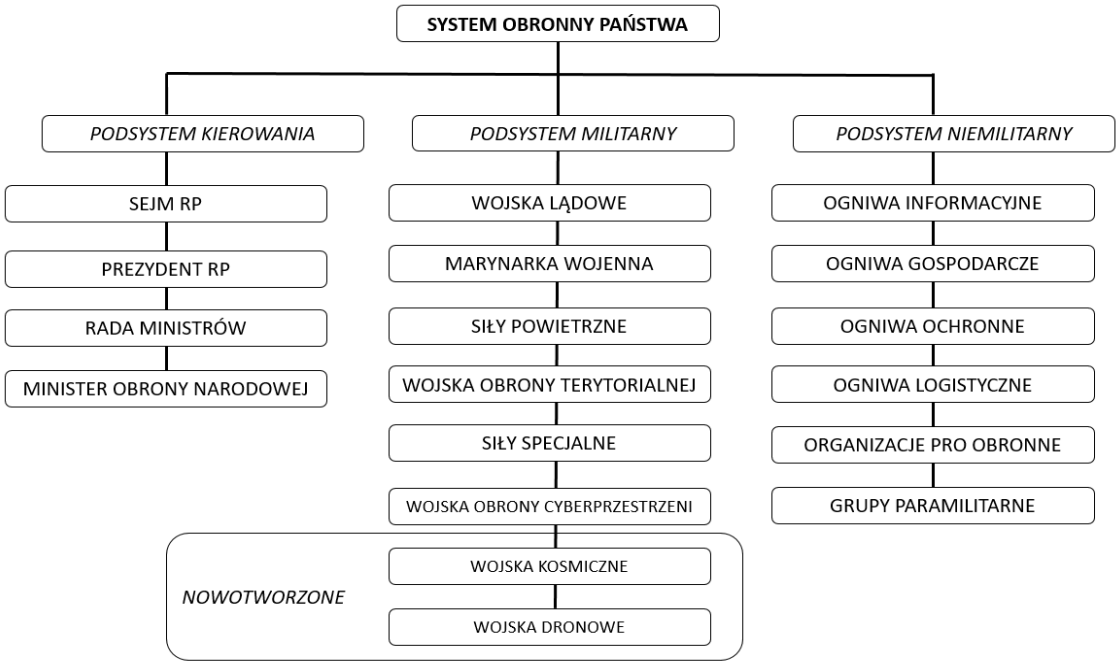
Szczebel administracyjny	Organ zarządzania kryzysowego	Organ opiniodawczo-doradczy	Centrum Zarządzania Kryzysowego
Krajowy	Rada Ministrów, Prezes Rady Ministrów	Rządowy Zespół Zarządzania Kryzysowego	Rządowe Centrum Bezpieczeństwa
Resortowy	Minister kierujący działem administracji rządowej, Kierownik organu centralnego	Zespół Zarządzania Kryzysowego (ministerstwa, urzędu centralnego)	Centrum Zarządzania Kryzysowego (ministerstwa, urzędu centralnego)
Wojewódzki	Wojewoda	Wojewódzki Zespół Zarządzania Kryzysowego	Wojewódzkie Centrum Zarządzania Kryzysowego
Powiatowy	Starosta powiatu	Powiatowy Zespół Zarządzania Kryzysowego	Powiatowe Centrum Zarządzania Kryzysowego
Gminny	Wójt, Burmistrz, Prezydent miasta	Gminny Zespół Zarządzania Kryzysowego (Miejski Zespół Zarządzania Kryzysowego	Mogą być tworzone (nie ma obowiązku utworzenia) gminne (miejskie) centra zarządzania kryzysowego

Rys. 9. Szczeble w Zarządzaniu Kryzysowym.
Źródło: Walczak W., 2009, Zarządzanie kryzysowe − rola i zadania organów administracji państwowej, Katedra Zarządzania SWSPiZ w Łodzi, Tom X, Zeszyt 8/2009. s. 99.

Obecnie działalność systemu oparta jest o szczeble administracyjne co w głównej mierze determinuje ilość użytych sił i środków w zależności od rozmiaru kryzysu. Niezależnie od szczebla administracyjnego (Rys. 9) działalność zarządzania kryzysowego opiera się o zasoby informacyjne, które stanowią bieżące pomiary jak i archiwalne dane. Zarządzanie kryzysowe jest szczególnie podatne na zagrożenia wykorzystujące cyberprzestrzeń do realizacji, ponieważ paraliż informacji w tym zasobów może mieć katastrofalne skutki w toku działań naprawczych. Jako przykład braku odpowiedniego poziomu cyberbezpieczeństwa w SZK może posłużyć współczesny konflikt ukraińsko-rosyjski. Otóż po rozpoczęciu inwazji na Ukrainę okazało się, że duża część systemów w tym dedykowanych do Zarządzania Kryzysowego Ukrainy miała zaimplementowane tak zwane „Backdoory" czyli tylne furtki dostępu w oprogramowaniu lub sprzęcie. W konsekwencji przeciwnik nie tylko mógł paraliżować działania tego systemu, ale również mógł być w posiadaniu istotnych zasobów informacyjnych, które wykorzystywał do pogłębiania kryzysu.

1.2.4. System Obrony Państwa

Słownik terminów z zakresu bezpieczeństwa narodowego definiuje System Obronny Państwa (SOP) jako: *„skoordynowany wewnętrznie zbiór elementów ludzkich, materiałowych i organizacyjnych zapewniających możliwości przeciwstawienia się zagrożeniom wojennym, zgodnie z celami i zamiarem obrony". Tworzą go podsystemy: kierowania, militarny oraz niemilitarny. Jego strukturę przedmiotową tworzą zadań w ramach przygotowań obronnych w czasie pokoju, a także w czasie zagrożenia i wojny*[53]". Innymi słowy SOP jest podstawowym systemem niższego szczebla Systemu Bezpieczeństwa Narodowego i jest przeznaczony do zapewnienia bezpieczeństwa militarnego oraz zachowania potencjału państwa do efektywnego reagowania na zewnętrzne kryzysy polityczno-militarne. System ten również posiada w swej strukturze liczne podsystemy (Rys. 10), które ze względu na specyfikę są podatne z punktu widzenia cyberbezpieczeństwa.



Rys. 10. Struktura Systemu Obronnego Państwa.
Źródło: opracowanie własne.

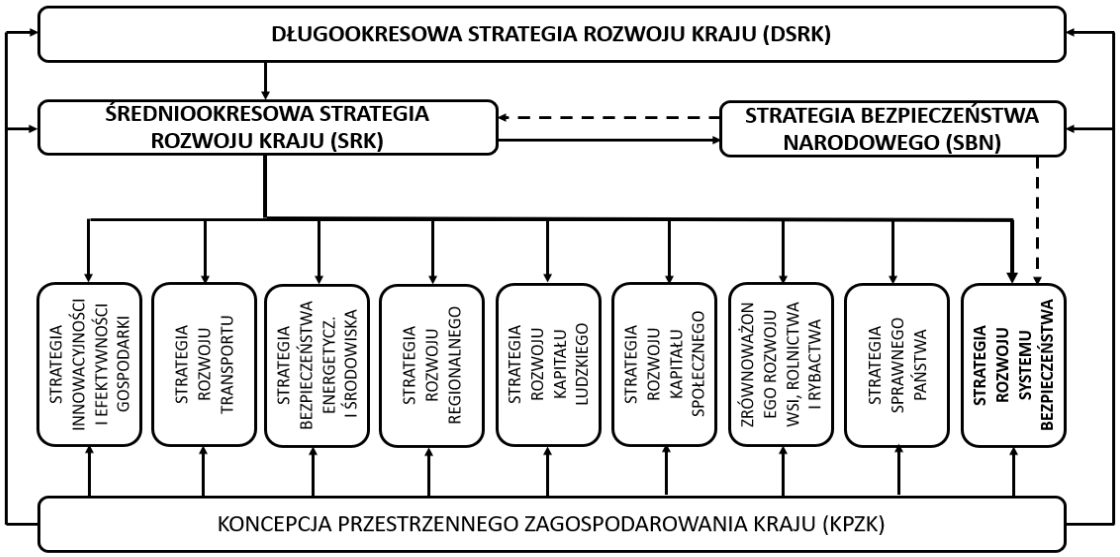
Należy mieć na uwadze, że cyberprzestrzeń oficjalnie jest kolejną domeną, w której mogą toczyć się działania zbrojne, a większość rozwiniętych państw wykształciła w swej strukturze podmioty dedykowane do działań ofensywnych i defensywnych w tym zakresie. Tu jako przykładem można się posłużyć konfliktem rosyjsko-gruzińskim, który

[53] Łepkowski W., 2009, Słownik terminów z zakresu bezpieczeństwa narodowego, Akademia Obrony Narodowej; Wyd. 4, Warszawa, s. 169.

przybrał miano pierwszej cyberwojny. Obecnie panuje powszechnie powiedzenie, że kolejną wojnę światową stoczą matematycy i jest w tym dużo prawdy, ponieważ nie będzie przesadą, jeżeli stwierdzimy, że współcześnie przeciwnik z dostępem do sprzętu teleinformatycznego i sieci potrafi sparaliżować dostawy logistyczne dla batalionu czołgów. To nad wyraz pokazuje jakimi narzędziami i jakimi technikami prowadzone są obecnie konflikty zbrojne. Z tego powodu System Obronny Państwa musi posiadać wysokie zdolności obrony cybernetycznej. Ponadto system powinien posiadać wyszkoloną kadrę z odpowiednimi kompetencjami, która dysponuje sprzętem z „górnej półki" a przede wszystkim posiadać zdolności prawne do prowadzenia działań w pełnym spektrum działań tzn. (defensywno-ofensywne).

1.3. Dokumenty strategiczne kreujące wizję systemu bezpieczeństwa państwa

Ukierunkowane działania mające zapewnić odpowiedni poziom bezpieczeństwa na szczeblu krajowym realizowane są na podstawie strategii, które ze względu na swój zasięg i obszerność zajmują odpowiednie miejsce w hierarchii dokumentów narodowych (Rys. 11). Najwyższym dokumentem, który przedstawia długoterminową wizję rozwoju państwa jest Długookresowa Strategia Rozwoju Kraju 2030 (DSRK RP) Trzecia fala nowoczesności, przy czym stosowana jest zamiennie z inną nazwą Strategia Polska 2030.



Rys. 11. Miejsce DSRK, SBN i SRSBN w hierarchii strategii.
Źródło: Kowalewski M., Aspekty bezpieczeństwa narodowego Rzeczpospolitej Polskiej, s. 178.

Jest to strategia określająca główne trendy, wyzwania i scenariusze rozwoju społeczno-gospodarczego oraz kierunki przestrzennego zagospodarowania kraju, z uwzględnieniem

zasady zrównoważonego rozwoju, obejmującym okres 20 lat[54]. Cele rozwojowe DSRK RP uszczegóławiane są za pośrednictwem strategii zintegrowanych a przede wszystkim przez Średniookresową Strategię Rozwoju Kraju 2020 (SRK RP), która bezpośrednio wywiera wpływ na kształtowanie Strategii Bezpieczeństwa Narodowego RP[55] (SBN RP). Niezależnie od tego dokumentu powstał kolejny, który w swej istocie prezentuje prognozy rozwoju samego Systemu Bezpieczeństwa Narodowego. Mowa tu Strategii Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej[56] (SR SBN RP). Pomimo, że wizja obu dokumentów powinna być spójna to nie należy utożsamiać ich ze sobą jako zamienne. Jest o istotne, ponieważ pierwszy dokument przedstawia BN jako ukierunkowaną dziedzinę działalności państwa, natomiast w drugim opisano rozwój samego systemu a to już nie jest tożsame.

Dokumenty normatywne związane z systemem bezpieczeństwa państwa w ujęciu cyberbezpieczeństwa zostały poddane wnikliwej analizie, której celem było wyeksponowanie wad, luk, słabości systemu z poziomu dokumentacji. Zestawienie i dokonanie porównania dokumentów ze stanem obecnym pozwoliło w szerszym kontekście wskazać rozwiązania systemowe które powinny zostać wprowadzone podczas transformacji systemu. Wobec zebranej w literaturze wiedzy należy podkreślić, że System Bezpieczeństwa Narodowego wraz z innymi kluczowymi systemami, pomimo dynamicznie zmieniającego się otoczenia nadal pozostaje w strukturze niezmiennej co świadczy o braku należytego monitorowania tych systemów w konfrontacji z aktualnymi zagrożeniami. W efekcie takiego stanu rzeczy każdy system staje się niewydolny lub niezdolny do przeciwstawienia się współczesnym zagrożeniom i z holistycznego punktu widzenia wpływa to na poziom bezpieczeństwa państwa polskiego. Biorąc pod uwagę rodzaj zagrożeń wykorzystujących cyberprzestrzeń można wywnioskować, że ranga obszaru bezpieczeństwa jakim jest cyberbezpieczeństwo jest opisana w dokumentach strategicznych lapidarnie i umieszczona zbyt nisko w hierarchii całego systemu bezpieczeństwa państwa. Ma to swoje konsekwencje w postaci przeznaczanych na ochronę, obronę cyberprzestrzeni sił i środków oraz niskie uświadomienie społeczne o tego rodzaju zagrożeniach wśród obywateli i decydentów.

[54] Długookresowa Strategia Rozwoju Kraju-Polska 2030. s. 12.
[55] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020 r.
[56] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022 r.

1.4. Zasoby informacyjne w systemie bezpieczeństwa państwa

Zasoby informacyjne w systemach bezpieczeństwa państwa takich jak SBN, KSC, SZK, SOP oraz konstrukcjach niższego szczebla są kluczowym elementem tych systemów, ponieważ to dzięki nim możliwe jest podejmowanie jakichkolwiek działań. Zasoby rozumiane jako zbiór danych, informacji, wiedzy oraz infrastruktury IT, wykorzystywane są na każdym szczeblu zarządzania od planowania poprzez zapobieganie, przygotowanie, reagowanie aż do usuwania skutków zagrożeń. Jednym z ważniejszych problemów choćby w procesie Zarządzania Kryzysowego jest podejmowanie decyzji w odpowiednim czasie z użyciem wiarygodnych informacji, które obecnie przekazywane są współcześnie za pomocą urządzeń elektronicznych połączonych w sieć[57]. Decyzje te muszą być poparte rzetelnymi informacjami z zachowaniem bezpieczeństwa danych co wskazuje jak istotna jest ochrona samych systemów teleinformatycznych, które wspierają wszelkie procesy. Pozytywną cechą systemów teleinformatycznych jest to, że dają możliwość szkolenia poprzez wielokrotne odtwarzanie różnych wariantów działań, sytuacji, zachowań i efektów podejmowania decyzji co z pewnością podnosi zdolności do przeciwdziałania i minimalizacji skutków zagrożeń[58]. Ilość danych oraz informacji przetwarzana w tych systemach jest olbrzymia. Warto wspomnieć tu o dziedzinowych podsystemach, które sprzężone są z SZK. Praktycznie każdy rodzaj służb czy administracji państwowej posiada narzędzia do monitorowania i gromadzenia informacji na temat określonych parametrów, do których przykładowo należą:

- stacje hydrologiczne do pomiaru pogody i stanu wód;
- stacje sieci obserwacyjno-badawcze wód podziemnych;
- stacje obserwacji naziemnej do monitorowania pożarów;
- stacje PMS do wczesnego wykrywania skażeń chemicznych;
- stacje ASS-500 do ciągłego poboru próbek aerozoli z powietrza;
- stacje IMGW, do pomiarów określonych elementów meteorologicznych;
- system ARAKIS do wykrywanie incydentów w systemach teleinformatycznych;
- system do powiadamiania i wymiany informacji w sytuacjach awaryjnych;
- system EURDEP do wymiany danych o wartościach promieniowania gamma;

[57] Domański P., Systemy wsparcia informatycznego w Systemie Zarządzania Kryzysowego na szczeblu wojewódzkim, Rocznik Bezpieczeństwa Morskiego, rok 2016, s. 234.

[58] Zaskórski P., Dąbrowski M., 2022, Bezpieczeństwo cyberprzestrzeni jako determinanta sprawności zarządzania w sytuacjach kryzysowych. ISBN 978-83-8270-094-7 s. 15-16.

- systemy wewnętrzne monitorowania infrastruktury krytycznej;
- inne.

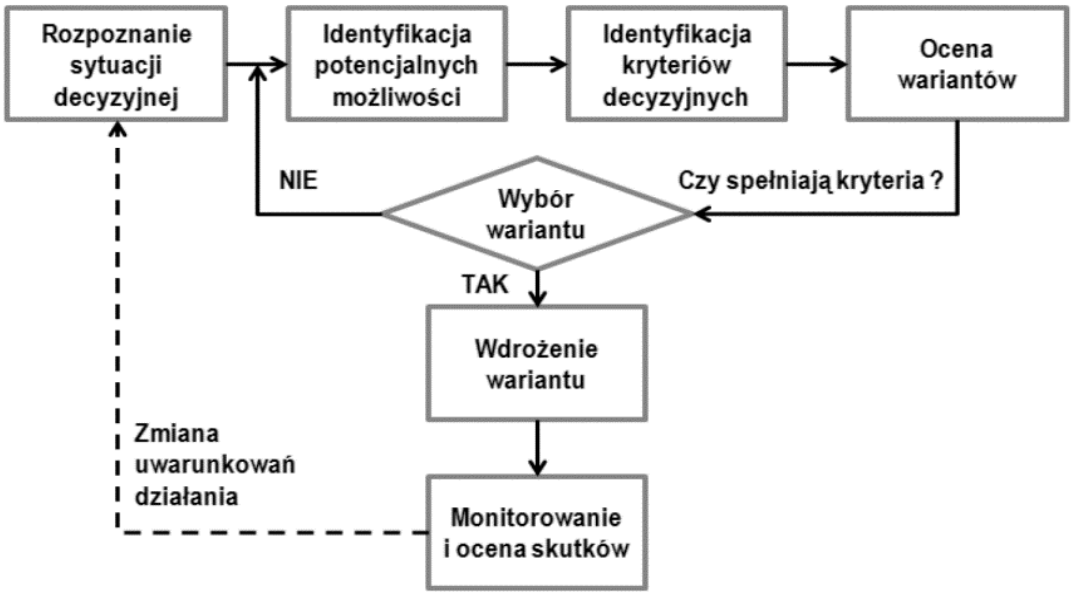
Przedstawione systemy odzwierciedlają tylko cześć z wszystkich zbiorów natomiast pozwala to urealnić wyobrażenie jak wielka ilość danych jest gromadzona i przetwarzana na potrzeby wszystkich systemów odpowiedzialnych za bezpieczeństwo państwa. Problematyczne jest zatem zachowanie poufności, integralności oraz dostępności tych danych, ponieważ istnieją zagrożenia takie jak działania hybrydowe, terrorystyczne, cyberwywiad w przypadku których celem może być nie tylko kradzież i paraliż zasobów, ale również wykorzystanie ich przeciwko organom co będzie miało znacznie większe skutki.

System bezpieczeństwa państwa we współczesnym państwie, powinien być zintegrowany ze wszystkimi możliwymi podsystemami generującymi dane geoprzestrzenne, rozpoznawcze, informacyjne, pomiarowe z uwzględnieniem baz danych archiwalnych na których można prognozować przebieg sytuacji wraz z możliwymi wariantami rozwoju. Ilość danych wprowadzanych do systemu nie powinna stanowić problemu a wręcz przeciwnie należy uznać je jako pożądane dobro, które w sprzężeniu z systemami gromadzenia i analizy wielkich kolekcji danych np. Big Data[59] wniesie możliwość modelowania pewnych zjawisk czy korygowania błędów ludzkich. W dalszej perspektywie rozwoju np. w Zarządzaniu Kryzysowym coraz częściej będą wykorzystywane numeryczne modele terenu, analizy zależności logicznych zdarzeń oraz ich skutków czy prognozy rozwoju sytuacji kryzysowych, w których symulacyjnie istnieje możliwość podejmowania decyzji w warunkach zbliżonych do realiów[60]. Działania takie wpływają na zwiększenie wyszkolenia obsady i odpowiedniego doboru sił i środków do rozmiaru rzeczywistego zagrożenia. Zwalczanie sytuacji zagrożenia w ujęciu systemowym polega przede wszystkim na procesie decyzyjnym, w którym informacja i zasoby stanowią podstawę sprawności i efektywności podjętych działań przez organy do tego przeznaczone. Na każdym etapie procesu należy dążyć do synergicznego połączenia danych archiwalnych z informacją bieżącą co skutkuje, że na podstawie doświadczeń i rzetelnej oceny stanu faktycznego wypracowywane są prawidłowe decyzje. Zatem informacja sama w sobie powinna być traktowana jako zasób

[59] Big data - termin odnoszący się do dużych, zmiennych i różnorodnych zbiorów danych, których przetwarzanie i analiza są trudne, ale jednocześnie wartościowe.

[60] Zaskórski P., Dąbrowski M., Bezpieczeństwo cyberprzestrzeni jako determinanta sprawności zarządzania w sytuacjach kryzysowych. ISBN 978-83-8270-094-7 s. 16.

determinujący ciągłość działania zarządzania sytuacją kryzysową[61]. W przeciwnym razie jej utrata może skutkować paraliżem wszelkich działań lub zastosowaniem nieadekwatnych sił i środków a co za tym idzie zwiększeniem zasięgu zagrożenia, strat ludzkich, materialnych oraz kosztów związanych z przywracaniem należytego stanu.



Rys. 12. Etapy procesu decyzyjnego.
Źródło: Opracowanie Krzysztof Szwarc.

Należy zwrócić uwagę, że zgodnie z grafiką (Rys. 12) odcięcie od informacji na każdym z etapów procesu decyzyjnego obarczone będzie wysokim ryzykiem niepowodzenia działań. Z tego powodu dążenie do utrzymania zasobów informacyjnych w systemach bezpieczeństwa państwa jest szczególnie ważnym wyzwaniem i powinno być ukierunkowane na zachowanie cech bezpieczeństwa informacji, czyli tzw. „triady CIA[62]". Wszystkie systemy teleinformatyczne wykorzystywane w konstrukcjach bezpieczeństwa posiadają określone podatności, które mogą być wykorzystywane przez „cyberzagrożenia". Połączenie tak dużej ilości podsystemów w spójną całość wymaga ciągłego monitorowania stanu samego systemu przyjmując, że ogólna niezawodność systemu jest pochodną niezawodności elementarnej, czyli wszystkich elementów tworzących dany system[63]. Przyczyny skutków niepowodzeń należy doszukiwać się w następujących zasadniczych zagrożeniach:

[61] Szwarc K., Uwarunkowania ciągłości działania Systemu Zarządzania Kryzysowego, Studia Bezpieczeństwa Narodowego R. 4, Nr 5, WAT 2014, s. 214.
[62] CIA triad - od angielskich odpowiedników tych pojęć. C-poufności I-integralność i A-dostępność.
[63] Szwarc K., Uwarunkowania ciągłości działania Systemu Zarządzania Kryzysowego, Studia Bezpieczeństwa Narodowego R. 4, Nr 5, WAT 2014, s. 208.

- siły natury (pożar, powódź, trzęsienie ziemi, epidemia, itd.);
- błędy ludzkie i działania w według błędnych lub niewłaściwych procedur;
- celowe działania z zamiarem wyrządzenia szkud przez ludzi;
- awarie sprzętu teleinformatycznego;
- awarie oprogramowania;
- awarie infrastruktury towarzyszącej np. zasilanie, klimatyzacja, ogrzewanie.

W związku z tym w systemach każdego szczebla należy dążyć do podejmowania zabezpieczeń przed powyższymi zagrożeniami poprzez wdrażanie przedsięwzięć technicznych i organizacyjnych, które zostały zaprezentowane w tabeli 3.

Tab. 3. Przedsięwzięcia organizacyjne i techniczne.

TECHNICZNE	Kopie bezpieczeństwa (zapasowe)
	System kontroli dostępu (fizycznego i logicznego)
	Ośrodek zapasowy (przetwarzania danych, biznesowy)
	Rezerwa sprzętowa (komputery i urządzenia sprzętowe)
	Zapasowa infrastruktura usługowa (łącza, zasilanie, łączność, woda, gaz)
ORGANIZACYJNE	Wdrożone plany zapewniania ciągłości działania
	Przećwiczona kryzysowa organizacja pracy
	Efektywne szkolenia
	Właściwa eksploatacja sprzętu, oprogramowania i obiektów infrastruktury
	Użytkownik sprzętu spełniający odpowiednie standardy jakościowe

Źródło: Opracowanie Krzysztof Liderman.

Należy również zweryfikować czy już wdrożone środki są nadzorowane i cyklicznie monitorowane na każdym szczeblu. Niezależnie od podjętych zabezpieczeń istnieje dodatkowa grupa ryzyka związana z infrastrukturą sprzętową. Jako poważne źródło zagrożeń należy traktować samo pochodzenie elementów infrastruktury cyfrowej, ponieważ podzespoły które są produkcji firm należących do obcych krajów w szczególności potentatów technologicznych takich jak Rosja, Chiny czy USA mogą powodować utajony wyciek zasobów. Realizując zadania ustawowe, interesariusze, w głównej mierze dysponują systemem powiązań informacyjnych wewnątrz organizacji pochodzących z różnej klasy, marki urządzeń a biorąc pod uwagę, że coraz popularniejsze stają się ataki typu „Backdoor" to może nastąpić wyciek danych. Umieszczenie luki przez producenta w oprogramowaniu daje możliwość dostania się do baz danych przez osoby do tego nieuprawnione bez oczywistych śladów włamań do systemu. Mając na uwadze powyższe argumenty należy uznać, iż zasoby informacyjne w systemach każdego szczebla powinny stanowić szczególną wartość i należy dołożyć wszelkich starań, aby je

chronić. Obecny stan ochrony zasobów informacyjny w podmiotach państwowych jest na średnim poziomie co jest konsekwencją niewystarczających nakładów finansowych na wprowadzenie nowych sprawdzonych technologii oraz brakiem odpowiednio wykształconych kadr w administracji państwowej. W związku z powyższym koncepcja poprawy bezpieczeństwa powinna być ugruntowana na zwiększeniu środków na cyberbezpieczeństwo i pozyskiwaniem wyspecjalizowanego personelu.

1.5. Analiza porównawcza systemów cyberbezpieczeństwa wybranych państw

Przeglądając zadania i strukturę KSC warto przyjrzeć się jak podchodzą do cyberbezpieczeństwa decydenci z innych państw europejskich. W tym celu zostało zaprezentowane zbiorcze zestawienie sfer państwowych objętych systemem ochrony cybernetycznej i formuła zapewniania tej ochrony. W tabeli 4 przedstawiono główne cele wynikające ze strategii cyberbezpieczeństwa takich państw jak: Wielka Brytania, Francja, Niemcy, Szwajcaria i Polska. Dodatkowo w poniższym zestawieniu uwzględniono sfery: gospodarczą, publiczną i administracyjno-polityczną. Analiza porównawcza wymienionych sfer w konfrontacji z Polską wykazuje na współbieżne cele, przy czym wszystkie kraje dążą do scentralizowanej struktury Krajowego Systemu Cyberbezpieczeństwa. Każde z wymienionych państw jako determinanty cyberbezpieczeństwa wskazuje ochronę elementów infrastruktury krytycznej, tworzenie odpornych na zagrożenia systemów teleinformatycznych z jednocześnie narastającą cyfryzacją gospodarki oraz ochroną zasobów informacyjnych. Omawiane państwa w swej strukturze posiadają funkcjonalne instytucje cywilne, militarne oraz naukowo-badawcze, przy czym zachowany jest podział na realizowane zadania. Istotnym wyzwaniem przed jakimi stoją prawie wszystkie państwa europejskie jest zjawisko dezinformacji. Warto wspomnieć, że tylko w samej EU toczą się prace nad kilkoma projektami mającymi na celu eliminację dezinformacji pod różną postacią. Powstają organizacje, które w swej strukturze stowarzyszają pasjonatów z całego świata, którzy za punkt honoru biorą sobie walkę z manipulacją mediami i dostępem do rzetelnych informacji. Współcześnie rozwijane są również programy komputerowe, które wspierają proces zautomatyzowania wychwytu dezinformacji w sieci. Niestety algorytmy stosowane w nich muszą być znacznie bardziej rozbudowane, ponieważ proces

odróżniania dezinformacji od wiarygodnych informacji jest skomplikowany[64]. Ponadto tworzone są warunki prawne do wprowadzania tego typu rozwiązań.

Tab. 4. Zbiorcze zestawienie sektorów państwowych cyberbezpieczeństwa.

Państwo	Sfera gospodarcza	Sfera publiczna	Sfera administracyjno-polityczna
W.ielka Brytania	Zapewnienie możliwości funkcjonowania firm i instytucji finansowych, prowadzących działalność lub posiadających aktywa na terytorium Królestwa	Zapewnienie funkcjonowania systemów i sieci umożliwiających swobodne i bezpieczne korzystanie z systemów teleinformatycznych i zasobów Internetu przez społeczeństwo	Prowadzenie działań systemowych, ukierunkowanych na ochronę państwowych zasobów informatycznych i sieci teleinformatycznych
Francja	Zapewnienie ochrony teleinformatycznej infrastruktury krytycznej, w tym małych i średnich przedsiębiorstw i zasobów będących własnością obywateli		Utrzymanie systemów łączności pomiędzy wszystkimi strukturami władzy wykonawczej i systemu zarządzania kryzysowego, zwłaszcza możliwości przesyłu informacji niejawnych
Republika Federalna Niemiec	Zapewnienia możliwości bezpiecznego funkcjonowania sieciowych systemów informacyjnych, wpływających na obszary życia gospodarczego oraz umożliwiających rozwój społeczno-gospodarczy	Zapewnienie bezpieczeństwa sieciom i bazom danych instytucji publicznych	Budowa federalnej sieci informatycznej dla urzędów federalnych i państw związkowych
Konfederacja Szwajcarska	Zwiększenie odporności infrastruktury krytycznej oraz sektorów usług finansowych i bankowego na zagrożenia generowane w cyberprzestrzeni oraz przeciwdziałanie i ograniczenie konsekwencji działań przestępczych i wrogich w cyberprzestrzeni, zwłaszcza cyberprzestępczości, cyberszpiegostwa i sabotażu cybernetycznego		
Polska	Niwelowanie możliwości oddziaływania na sektory gospodarcze pełniące istotne funkcje w państwie	Niwelowanie możliwości wykradzenia lub wykorzystania danych publicznych i wrażliwych	Niwelowanie możliwości oddziaływania na sektory gospodarcze pełniące istotne funkcje w państwie

Źródło: System bezpieczeństwa cybernetycznego państw europejskich, s. 67.

Przykładem jest tu Francja, która bardzo mocno dyscyplinuje informacje podczas wyborów[65]. Wprowadzono ustawę o zwalczaniu manipulowania informacją. Dokument ten został utworzony z obawy na dezinformację, która może wpłynąć na wynik wyborów prezydenckich w 2018 roku. Ustawa określa sankcje karne i finansowe za naruszanie przepisów. Przykładowo jest to rok więzienia i 75 tys. EUR kary za celowe wprowadzanie w błąd, które mogłoby wpłynąć na uczciwość wyborów[66]. Ponadto wprowadza nowe narzędzia walki z rozpowszechnianiem fałszywych informacji w okresie wyborczym. Dodatkowo w celu egzekwowania kar powołano sądy, które w trybie 24 godzinnym

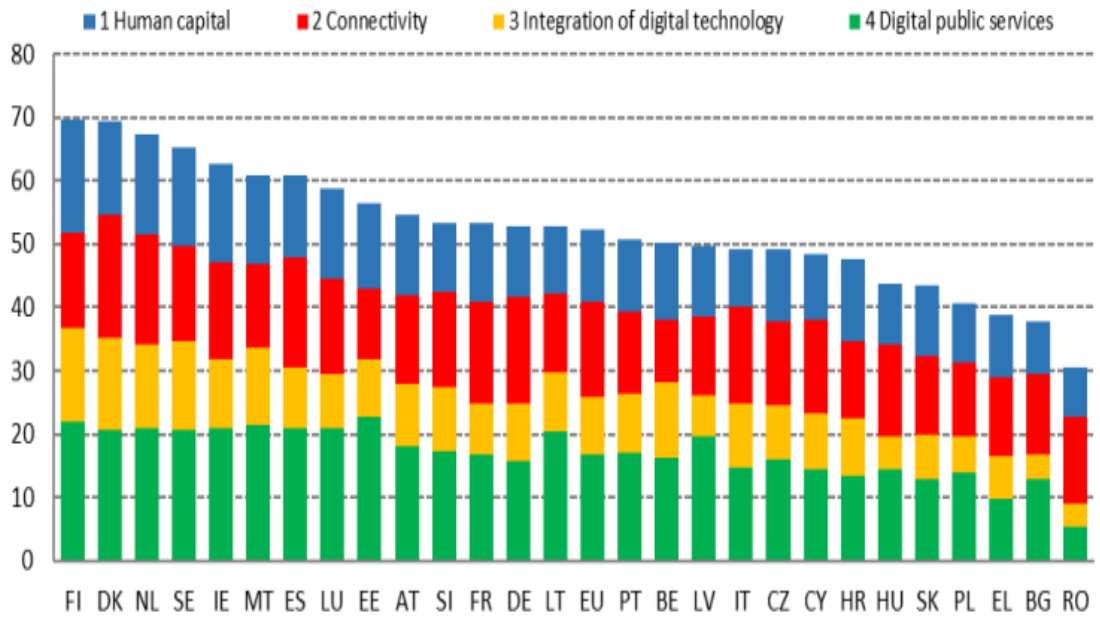
[64] Dąbrowski M., Wyzwania i zagrożenia dla bezpieczeństwa Europy środkowo-wschodniej. Dezinformacja w działaniach hybrydowych. ISBN 978-83-67138-76-5, 2021, s. 74.
[65] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037847559 [dostęp: 23.11.2022 r.].
[66] Tamże, s. 70.

orzekają o treściach manipulacyjnych i mogą wydać zakaz rozpowszechniania tych treści.

Kolejnym przykładem godnym naśladowania są Stany Zjednoczone Ameryki, ponieważ już w latach 90 utworzono tam ISAC, czyli Centra Wymiany i Analizy Informacji dla każdego sektora infrastruktury krytycznej[67]. Organizacją zrzeszającą zespoły ISAC ze wszystkich sektorów jest Narodowa Rada ISAC (National Council of ISAC, NCI). Do jej obowiązków należy wzmacnianie współpracy i wymiana informacji międzysektorowych. Obecnie w Stanach Zjednoczonych działa ponad 20 organizacji ISAC. Ponadto w Europie również funkcjonują lub są tworzone ISAC poziomu europejskiego. W odróżnieniu od USA europejskie centra są bardziej sformalizowane i skoncentrowane na trzech kierunkach: krajowym, sektorowym i międzynarodowym. Przykładowo w Belgi przy Centrum Cyberbezpieczeństwa funkcjonuje sieć ISAC, która jest skupiona na różnych sektorach gospodarki, gdzie za pomocą wspólnej platformy poszczególne centra wymieniają się informacjami o incydentach. W Holandii Narodowe Centrum Cyberbezpieczeństwa jest punktem centralnym dla ISAC utworzonych w sektorach krytycznych. Poza wymianą informacji o incydentach odbywają się regularne spotkania budujące zaufanie i sprzyjające wymianie dobrych praktyk. W Finlandii Narodowe Centrum Cyberbezpieczeństwa działa jako punkt koordynacji i wymiany informacji o incydentach pomiędzy administracją publiczną a ISAC w sektorach krytycznych[68].

Ważną informacją monitorującą stan cyberbezpieczeństwa danego państwa jest weryfikacja na podstawie Indeksu Gospodarki Cyfrowej i Społeczeństwa Cyfrowego DESI (Rys. 13) realizowana przez Komisję Europejską od 2014 roku. Indeks ten pozwala analizować wskaźniki kluczowe dla obszarów cyfrowych i wspierać proces podejmowania decyzji politycznych w zakresie kierunków rozwoju. Na podstawie przedstawionego wykresu można wywnioskować, że Polska zajmuje miejsce daleko w tyle w stosunku do Holandii, Finlandii czy Danii, które w 2022 roku były liderami cyberbezpieczeństwa w Europie. Porównując wskaźniki pierwszej trójki z wynikiem Polski widoczny jest deficyt kapitału ludzkiego a to właśnie ten czynnik jest motorem napędowym pozostałych wskaźników. Wynika to między innymi z niekompletnego systemu edukacji z zakresu cyberbezpieczeństwa w Polsce.

[67] https://cyberpolicy.nask.pl/isac-centra-wymiany-analizy-informacji/ [dostęp: 03.11.2023].
[68] Tamże.



Rys. 13. Zestawienie Indeksu DESI z 2022 roku.
Źródło: https://ec.europa.eu/newsroom/dae/redirection/document/88764 [dostęp: 22.03.2023].

Potwierdzeniem tego faktu może być analiza duńskiej Strategii Cyberbezpieczeństwa i Bezpieczeństwa Informacji na lata 2018-2021[69], która w swej treści zakłada wspólne działania zainicjowane w ramach całego systemu edukacji. Działalność ta skoncentrowana jest na podnoszeniu świadomości wyzwań związanych z bezpieczeństwem wśród dzieci, młodzieży oraz nauczycieli[70]. Należy przez to rozumieć, że wiodące w cyberbezpieczeństwie państwo stawia na kształtowanie świadomości najmłodszych pokoleń co w perspektywie czasu indukuje tych ludzi do rozwijania zdolności w kierunku branży IT oraz eliminuje popełnianie w przyszłości błędów przez osoby wyedukowane. Polska strategia cyberbezpieczeństwa w części „Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli" również zakłada, że edukacja powinna być osiągalna na jak najwcześniejszym etapie, lecz niestety jest to realizowane bez większych efektów. Dzieciom i młodzieży należy umożliwić dostęp do usług cyfrowych w związku z czym zasadnym byłoby utworzenie w strukturze KSC organu wdrażającego i kontrolującego kształcenie na poziomie obowiązku ustawowego. Rozwiązanie to jest konieczne, ponieważ pozostawienie kształcenia niewyspecjalizowanym kierunkowo nauczycielom będzie przynosiło niewłaściwe skutki.

[69] https://www.wojsko-polskie.pl/aszwoj/u/8a/10/8a10c049-b55b-4559-b59a-dca6c4db61f8/dania.pdf [dostęp: 22.03.2021].
[70] Tamże, s. 25.

Podejście do cyberbezpieczeństwa przez wiodące w tej dziedzinie państwa może wnieść do krajowego systemu wiele solidnych rozwiązań. Po pierwsze dążenie do utworzenia szkolenia na jak najniższym poziomie przełoży się na podniesienie poziomu świadomości oraz motywowanie ludzi do rozwoju w tym kierunku. Idąc dalej zasadne jest utworzenie wiodącego ISAC w pełni dotowanego z budżetu państwa tak aby koordynowało resztę centrów składających się z podmiotów partnerstwa-publiczno-prywatnego. Istnieje uzasadniona potrzeba walki z dezinformacją poprzez utworzenie specjalistycznego na szczeblu krajowym organu monitorującego przestrzeń informacyjną z jednoczesną współpracą w tym kierunku z organizacjami europejskimi. Przykład Francji jest dowodem na to, że istnieją już metody walki z dezinformacją. Zastosowanie istniejących rozwiązań z innych państw posiada jedną pożądaną cechę mianowicie są to koncepcje już sprawdzone więc zminimalizowane jest prawdopodobieństwo wdrożenia pomysłu o niewiadomych skutkach.

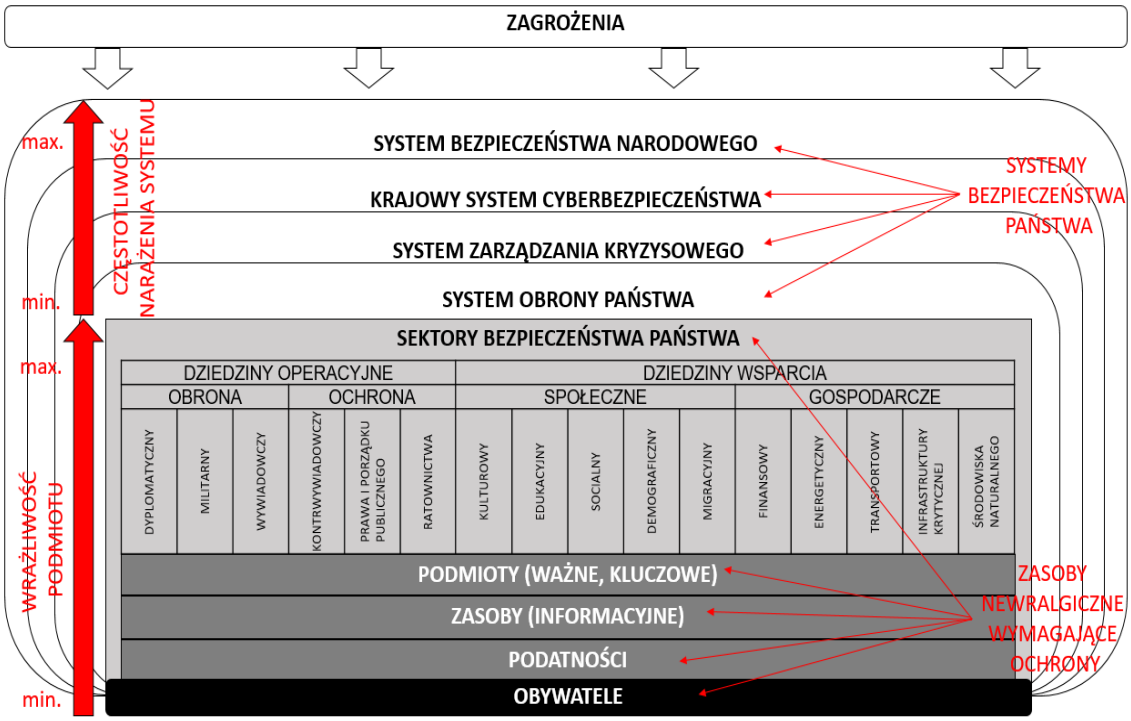
1.6. Podsumowanie rozdziału

Nie jest możliwym co wykazano w początkowej części rozdziału ustalenie jednoznacznej definicji bezpieczeństwa natomiast należy rozpatrywać je w konkretnym kontekście wraz z ukierunkowaniem na obszary, których ma dotyczyć. Podobnie rzecz wygląda z innymi definicjami kluczowymi z punktu widzenia badanego obszaru. Bezpieczeństwo Narodowe zależy od wielu czynników, przy czym obecne czasy wyraźnie podkreślają jak bardzo newralgiczna jest cyberprzestrzeń wraz z bezpieczeństwem informacji. Z całą pewnością jest to pokłosie czwartej rewolucji przemysłowej w której obecnie żyjemy a która jednocześnie stanowi swego rodzaju paradygmat ostatnich dekad. Na szczeblu krajowym istnieje system, którego głównym zadaniem jest przeciwdziałanie wszelkim rodzajom zagrożeń. Mowa tu o Systemie Bezpieczeństwa Narodowego, który w swej istocie stanowi podstawowy mechanizm ochronny kraju. System powstał w oparciu o sektory bezpieczeństwa oraz wieloletnie doświadczenia. Natomiast, aby być skutecznym i efektywnym musi on być cyklicznie dostosowywany do nowych często nie do końca znanych wyzwań. System ten w swej strukturze zawiera liczne podsystemy, gdzie biorąc pod uwagę operacyjność rozumianą jako częstotliwość konfrontacji z zagrożeniami to Krajowy System Cyberbezpieczeństwa współcześnie wiedzie prym pod względem narażenia na ataki wrogich podmiotów. Należy wyraźnie podkreślić, że szerokorozumiane cyberbezpieczeństwo przenika przez

wszystkie systemy bezpieczeństwa w państwie. Z tego też powodu w koncepcji poprawy bezpieczeństwa państwa analizie podlegał będzie nie tylko sam System Bezpieczeństwa Narodowego i jego główne podsystemy jakimi są SKZ, SOP, KSC. Takie działanie ma na celu podejście holistyczne tak aby w pełni zdiagnozować przedmiotową problematykę. Aby zobrazować przestrzeń badawczą przedstawiono autorski schemat struktury Systemu Bezpieczeństwa Narodowego (Rys. 14), który w swej istocie zawiera hierarchię podsystemów pod względem intensyfikacji działań ochronnych i obronnych oraz wpływu materializacji zagrożeń na struktury państwa w ujęciu cyberbezpieczeństwa. Należy uznać, że najsłabszym ogniwem w systemie jest człowiek a w ujęciu państwa - obywatel. Na potrzeby egzystencji i rozwoju obywateli zostały powołane podmioty (w tym ważne i kluczowe), które zapewniają wszelkie usługi m.in. poprzez szerokorozumiane łańcuchy dostaw. Wszystkie te podmioty zawierają zasoby informacyjne, które powinny być traktowane jako najwyższe dobro i powinny być szczególnie chronione. Dodatkowo wszystkie wymienione obiekty (obywatele, podmioty, zasoby) posiadają podatności, które w połączeniu z zagrożeniami mogą skutkować materializacją zagrożeń. Aby do tego nie doszło obiekty te chronione są przez System Obrony Państwa, System Zarządzania Kryzysowego i Krajowy System Cyberbezpieczeństwa, czyli główne składowe Systemu Bezpieczeństwa Narodowego. Analiza obecnej struktury SBN w konfrontacji z przedstawionymi argumentami wskazuje na ponowne dostosowanie tego systemu do współczesnych zagrożeń. Przypomina to odwieczną walkę „miecza i tarczy", które muszą być stale ulepszane, aby zachować przewagę nad przeciwnikiem. Z tego też powodu istnieje uzasadniona potrzeba zdefiniowania na nowo pojęcia tego systemu jednocześnie nadając mu odpowiedni „charakter" tak aby odzwierciedlić rzeczywistą funkcję w państwie. Aktualizacja systemu wraz z koncepcją poprawy bezpieczeństwa państwa będzie zatem czynnością, która jest pożądania. Zdefiniowanie na nowo całości systemu proponowane jest w następujący sposób:

Definicja autorska Systemu Bezpieczeństwa Narodowego:

„System Bezpieczeństwa Narodowego - jest to zbiór wzajemnie skorelowanych obiektów oraz zbiór relacji pomiędzy nimi, które poprzez realizację statutowych zadań w wszystkich dziedzinowych obszarach bezpieczeństwa pełnią funkcję prewencyjną, zwalczającą i minimalizującą skutki zagrożeń zarówno wewnętrznych jak i zewnętrznych".



Rys. 14. Schemat Systemu Bezpieczeństwa Narodowego wraz hierarchią podsystemów.
Źródło: Opracowanie własne.

Wedle tak przedstawionej definicji można założyć, że dojrzałość systemu wobec zagrożeń stanowi o odporności całego państwa we wszystkich dziedzinach bezpieczeństwa. W ujęciu współczesnych zagrożeń to właśnie system Krajowy System Cyberbezpieczeństwa należy zdefiniować jako główny podsystem SNB, ponieważ jest on narażony na ataki niemalże w sposób ciągły w przeciwieństwie do Systemu Zarządzania Kryzysowego, którego użycie (oprócz monitorowania) jest sporadyczne. Jeszcze rzadziej dochodzi do naruszenia Systemu Ochrony Państwa, wobec czego tak zaprezentowana hierarchia wydaje się logiczna.

Przeprowadzona analiza dokumentów, weryfikacja literatury i struktury SBN wyraźnie wskazuje, że współcześnie bezpieczeństwo państwa powinno być ukierunkowane na zagrożenia w cyberprzestrzeni w związku z czym zasadnym jest, aby wprowadzić zmiany, które uczynią SBN bardziej odpornym w tym spektrum zagrożeń. Ponadto należy wziąć pod uwagę, że pojedyncza jednostka osobowa z punktu widzenia zwykłego obywatela jako podstawowe zagrożenia upatruje w konfliktach zbrojnych, przestępczości, ochronie zdrowia itp. W związku z tym wskazane jest założenie, że osoby te nie dostrzegą jak istotne jest współcześnie cyberbezpieczeństwo a co za tym idzie cały ciężar odpowiedzialności w tej materii spoczywa na państwie. Analiza dostępnej literatury i dokumentów normatywnych również wykazała, że nie zawsze

w sposób jasny i zrozumiały przedmiotowa problematyka jest poruszana i eksponowana. Dodatkowo zakres „cyberzagrożeń" jest tak duży, że aby uzyskać pełen obraz sytuacyjny należy połączyć ze sobą wielką liczebnie ilość rozproszonej wiedzy. Z przeprowadzonej analizy dokumentacji można wywnioskować, że ranga cyberbezpieczeństwa nie jest wystarczająco doceniana w związku z czym należy dołożyć wszelkich starań, aby ten stan rzeczy zmienić. Zmiany te powinny obejmować nie tylko dokumenty i regulacje prawne, ale również strukturę, infrastrukturę, oraz całokształt postrzegania społecznego zagrożeń w cyberprzestrzeni. Wynika z tego również, że Informacyjna Ciągłość Działania państwa jako organizacji staje się determinantem bezpieczeństwa kraju, przy czym kierunki współczesnych zagrożeń ewidentnie wskazują na konieczność ochrony zasobów informacyjnych wszelkich systemów teleinformatycznych. Aby wprowadzić działania usprawniające System Bezpieczeństwa Narodowego wraz z podsystemami należy wzmocnić ochronę zasobów informacyjnych. Można tego dokonać poprzez dostosowanie podmiotów państwowych do współczesnych zagrożeń, zaktualizowanie regulacji prawnych oraz prowadzenie działań uświadamiających społeczeństwo. Wobec czego do zrealizowania przedmiotowego celu wymagana jest ingerencja nie tylko w główny system (SBN) i podsystem (KSC, SZK, SOP), ale również pozostałe podsystemy niższego szczebla, które w pewnych obszarach posiadają podatności, które mogą mieć wpływ na materializację zagrożeń w cyberprzestrzeni.

ROZDZIAŁ II. PODSTAWY METODOLOGICZNE

2.1. Uzasadnienie podjęcia badań

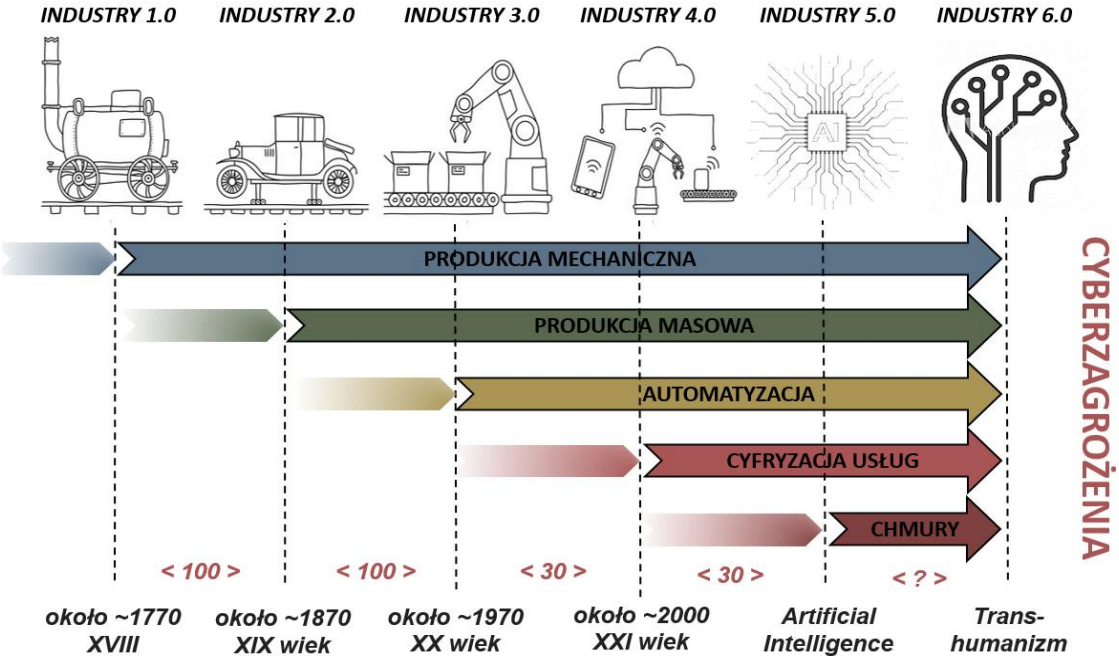
Cyfryzacja jako ciągły proces konwergencji rzeczywistego i wirtualnego świata staje się głównym motorem innowacji i zmian nie tylko w sferze militarnej ale i w większości gałęzi życia społecznego. Kluczowymi czynnikami napędzającymi rozwój gospodarki cyfrowej w tym możliwości doskonalenia systemów bezpieczeństwa, ale ze świadomością powstania nowych zagrożeń są:

- Internet rzeczy (ang. Internet of Things - IoT);
- Internet wszechrzeczy (ang. Internet of Everything - IoE);
- wszechobecna łączność (ang. hyperconnectivity);
- aplikacje i usługi bazujące na chmurze obliczeniowej (ang. cloud computing);
- analityka bardzo dużych zbiorów wielopostaciowych danych nieustrukturalizowanych (ang. big data Analytics - BDA);
- bardzo duże zasoby danych działające jako usługa (ang. Big Data as a Service BDaaS);
- automatyzacja (ang. automation) oraz robotyzacja (ang. robotisation);
- wielokanałowe modele dystrybucji produktów i usług (ang. multi-channel).

Z punktu widzenia obywatela istnieje uzasadniona potrzeba zapewnienia ciągłości działania w świadczeniu „usług cyfrowych" w rozumieniu zapisów ustawy[71] oraz zapewnieniu niezakłóconego dostępu do „usług kluczowych" mających istotne znaczenie dla utrzymania ciągłości działania infrastruktury krytycznej. Infrastruktura ta obejmuje takie sektory jak: energię, transport, bankowość i infrastrukturę rynków finansowych, ochronę zdrowia, uzdatnianie wody i wszechobecną infrastrukturę cyfrową. Długookresowe następstwa zastosowania przełomowych technologii cyfrowych składających się na istotę obecnej czwartej rewolucji przemysłowej (Rys. 15) tzw. Industry 4.0 (I4.0) należą do najważniejszych wyzwań ludzkości[72]. Dodatkowo należy sobie uświadomić w jakim stopniu technologie informatyczne a w szczególności cyberprzestrzeń są wykorzystywane w celu usprawnienia działalności państwa oraz zapewnienia jego bezpieczeństwa w różnych wymiarach. Zatem można postawić pytanie czy w dzisiejszym świecie można funkcjonować bez techniki cyfrowej? Otóż nie ponadto

[71] Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną Dz. U. 2002 Nr 144 poz. 1204.
[72] Wieczorek P., Czwarta rewolucja przemysłowa, Wizja przemysłu nowej generacji - perspektywa dla Polski, Państwo i społeczeństwo, Nr 3/maj-czerwiec/2018.

pewne jest, że ludzkość zmierza ku kolejnej piątej rewolucji (I5.0), którą będzie zdominowana przez sztuczną inteligencję (AI) w głównej mierze bazującą na technologiach kognitywnych[73].

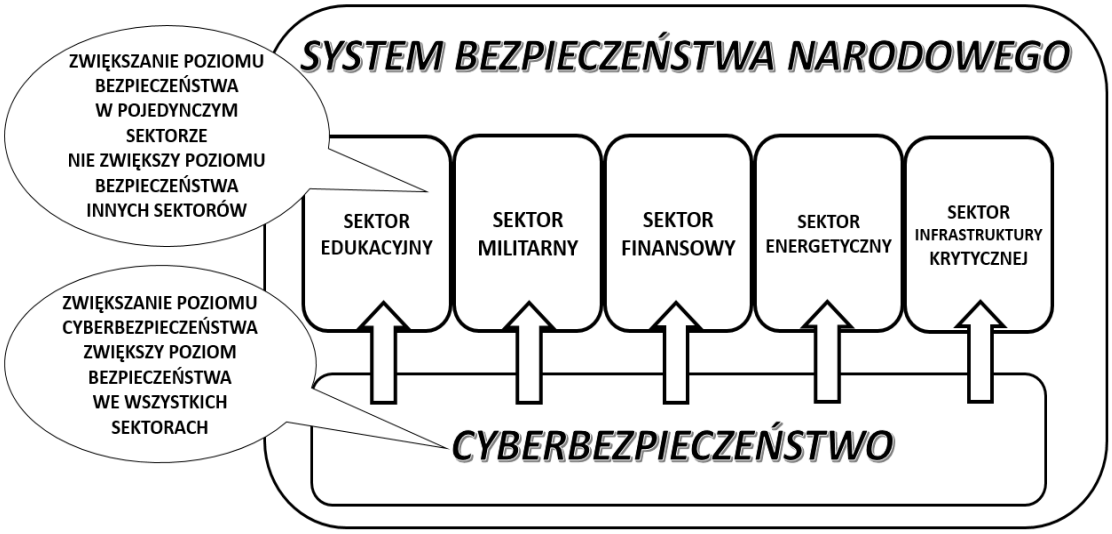


Rys. 15. Fazy rozwoju rewolucji przemysłowych z ekspozycją roli cyberprzestrzeni.
Źródło: Opracowanie własne.

Nie jest jednoznacznie określone, kiedy to nastąpi jednak według niektórych ekspertów rewolucja ta już trwa. Coraz liczniejsze grupy badaczy zaliczają powstające na bazie technologii cyfrowej inteligentne fabryki do zjawisk piątej rewolucji przemysłowej. Ponadto istnieją poglądy, że opisywana rewolucja I5.0 jest tylko eksplikacją czwartej[74]. Analiza przedziałów czasowych pomiędzy kolejnymi rewolucjami wskazuje na gwałtowne przyśpieszenie po trzeciej rewolucji (od 1 do 3 średnio około 100 lat) co skutkowało powstaniem I4.0 już po niespełna 30 latach od poprzedniej. Przełomowe były tu lata 70 XX wieku, ponieważ był to rozkwit technologii informatycznych. Zgodnie z prawem Moore'a[75], który dowiódł empirycznie, że moc obliczeniowa komputerów co 18 miesięcy podwaja się (ostatecznie po korekcji co 24) przełożyło się to właśnie na przyśpieszenie czwartej rewolucji. Kierując się tymi przesłankami należy wnioskować, że od czasu nadejścia I4.0 minęło ponad 20 lat i obecnie jest to początek rewolucji sztucznej inteligencji, gdyż postęp technologii cyfrowej rośnie w skali logarytmicznej.

[73] Automatyzacja kognitywna wykorzystuje różne algorytmy i podejścia technologiczne wywodzące się z obszaru sztucznej inteligencji.
[74] Furmanek W., Piąta rewolucja przemysłowa. Eksplikacja pojęcia, „Edukacja-Technika-Informatyka" 2018, nr 2/24, s. 276, https://doi.org/10.15584/eti. [dostęp: 03.05.2023].
[75] Gordon Earle Moore (ur. w 1929 w San Francisco) współzałożyciel korporacji Intel.

Niezależnie od technologii jaką ludzkość obecnie dysponuje istnieje kolejny ważny powód, dla którego zasadnym jest skupienie uwagi na transsektorowym cyberbezpieczeństwie. Rozważając problematykę zwiększenia poziomu bezpieczeństwa narodowego warto przyjrzeć się relacjom między sektorami bezpieczeństwa. Z grafiki (Rys. 16) wynika, że podniesienie poziomu cyberbezpieczeństwa warunkuje zwiększeniem bezpieczeństwa w każdym sektorze co przekłada się całościowo na poprawę bezpieczeństwa państwa, przy czym zależność ta nie działa odwrotnie. Posługując się przykładem można przedstawić to w następujący sposób:



Rys. 16. Newralgiczne obszary Systemu Bezpieczeństwa Narodowego.
Źródło: Opracowanie własne na podstawie struktury Systemu Bezpieczeństwa Narodowego.

„Usprawniając system cyberbezpieczeństwa poprzez wprowadzenie separacji lub segmentacji sieci teleinformatycznej w elektrowni zwiększamy bezpośrednio poziom bezpieczeństwa sektora infrastruktury krytycznej oraz ciągłość działania systemu energetycznego mający istotny wpływ na funkcjonowanie pozostałych sektorów. Natomiast zwiększając potencjał w sektorze np. militarnym poprzez utworzenie i wyposażenie dodatkowego batalionu pancernego w czołgi zwiększamy bezpieczeństwo tylko tego sektora nie zwiększając bezpieczeństwa innych sektorów a wręcz przeciwnie dokładamy dodatkowe obciążenie poprzez zwiększenie elementów posiadających odpowiednie podatności”.

Ten przykład powinien zobrazować rolę i znaczenie cyberbezpieczeństwa w całym Systemie Bezpieczeństwa Narodowego a w szczególności informacyjnej ciągłości działania w aspekcie zapewniania bezpieczeństwa w cyberprzestrzeni co jest przedmiotem dalszych badań.

2.2. Przegląd literatury

Analiza dostępnej literatury z zakresu cyberbezpieczeństwa w ujęciu bezpieczeństwa państw wskazuje na problematykę niezauważalności lub niedoceniania istoty informacyjnej ciągłości działania w tworzeniu Systemu Bezpieczeństwa Narodowego odpornego na zagrożenia. Wykorzystana w przygotowywaniu niniejszej dysertacji literatura przedmiotu nie jest obszerna. Jest to spowodowane tym, że od wejścia w życie dokumentów, które są kluczowe dla omawianych zagadnień upłynął krótki czas.

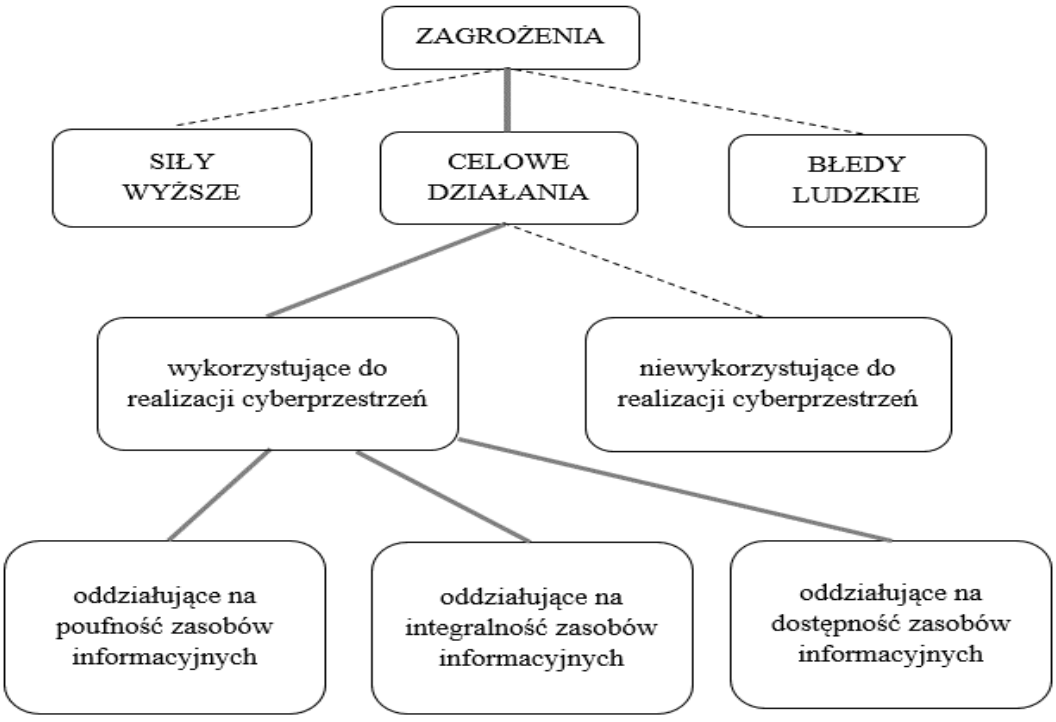
Na uwagę zasługuje książka autorstwa Mariana Kowalewskiego „Aspekty bezpieczeństwa narodowego Rzeczypospolitej polskiej" w której to dość szczegółowo i obszernie została przedstawiona struktura aktualnych dokumentów strategicznych. Kolejnym dziełem, bez którego dysertacja nie mogłaby powstać, jest „Bezpieczeństwo Informacyjne. Nowe wyzwania", autorstwa Krzysztofa Lidermana, które w sposób kompleksowy wyczerpuje wiedzę z zakresu przedmiotowej tematyki. Kolejną pozycją, która znalazła zastosowanie w toku pisania rozprawy jest „Internet Rzeczy - Problemy cyberbezpieczeństwa" autorstwa Jerzego Krawca oraz „Cyberbezpieczeństwo - podejście systemowe" tego samego autora. W Internecie dostępnych jest wiele artykułów dotyczących zagrożeń, ataków oraz „cyberbezpieczeństwa", jednak wiele z nich zawiera błędy merytoryczne takie jak zbytnie używanie nowomowy z przedrostkiem „cyber" bez ukazywania prawdziwego źródła zagrożenia. Kluczową pozycją a jednocześnie najważniejszą która wpisuje się w tematykę dysertacji, jest „Zarządzanie organizacją w warunkach utraty informacyjnej ciągłości działania" pod redakcją Piotra Zaskórskiego. Literatura ta w sposób wielowymiarowy opisuje problematykę zarządzania organizacją (rozumianą również jako państwo) w warunkach zagrożeń dla bezpieczeństwa informacyjnego z jednoczesnym wyeksponowaniem rozwiązań systemowych i proceduralnych.

Ponadto w dysertacji dokonano analizy wielu dokumentów normatywnych począwszy od Strategii Bezpieczeństwa Narodowego, Strategii Rozwoju Systemu Bezpieczeństwa Narodowego, Strategii Cyberbezpieczeństwa, po ustawy takie jak Ustawa o Krajowym Systemie Cyberbezpieczeństwa, Ustawa o Zarządzaniu Kryzysowym, Ustawa o świadczeniu usług drogą elektroniczną, Prawo Telekomunikacyjne oraz Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne.

Dodatkowo cennym źródłem wiedzy okazały się dane statystyczne szeroko prezentowane w rocznikach „Cert Polska" wydawanych przez CSIRT NASK oraz „Raporty o stanie bezpieczeństwa cyberprzestrzeni RP" redagowane przez zespół CSIRT GOV Agencji Bezpieczeństwa Wewnętrznego. Informacje zawarte w broszurach pozwoliły na wyeksponowanie kierunków, rodzajów, technik i metod wykorzystywanych we współczesnych zagrożeniach bezpieczeństwa informacyjnego.

2.3. Przedmiot i podmiot badań

W rozprawie przyjęto założenie, że przedmiotem pracy będzie analiza obecnego Systemu Bezpieczeństwa Narodowego, celem wychwycenia luk, wad, słabości i zidentyfikowania zagrożeń, na które obecny system bezpieczeństwa państwa jest nieprzygotowany. Dla osiągnięcia zamierzonego celu pracy przyjęto ograniczenia zawężające się do celowych działań wykorzystujących do realizacji cyberprzestrzeń (Rys. 17).



Rys. 17. Schemat obszaru zainteresowania.
Źródło: opracowanie własne.

W zakresie podmiotowym zgodnie z istotną dla tematu pracy Dyrektywą NIS[76] w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci

[76] Dyrektywa NIS została przyjęta 6 lipca 2016 r. Jest pierwszym europejskim prawem w zakresie cyberbezpieczeństwa. Dyrektywa nakłada na państwa członkowskie szereg obowiązków, obliguje je do powołania konkretnych instytucji oraz wprowadzenia mechanizmów współpracy. W Polsce jej zapisy realizuje ustawa o krajowym systemie cyberbezpieczeństwa z 28 sierpnia 2018 roku.

i systemów informatycznych na terytorium Unii dysertacja dotyczy podmiotów wskazanych bezpośrednio w dokumencie, które wymagały identyfikacji na poziomie krajowym i zostały określone w Ustawie o Krajowym Systemie Cyberbezpieczeństwa jako podmioty tego systemu. Dotyczy to również podmiotów, które w trakcie rozprawy mogą zostać zidentyfikowane jako istotne dla badanych zagadnień.

Temat pracy jest ograniczony ramami czasowymi i przestrzennymi. Obejmuje on okres od 2018 roku do 2025 roku[77] ze względu na specyfikę badanego zagadnienia. Do tego czasu instytucje państwowe zajmujące się cyberbezpieczeństwem miały inny wymiar i charakter działań. Należy jednak zaznaczyć, że w dysertacji przytoczono incydenty teleinformatyczne, które wydarzyły się na przestrzeni ostatnich dwóch dekad celem analizy przyczynowo skutkowej. W rozprawie skoncentrowano się na krajowych rozwiązaniach z uwzględnieniem środowiska międzynarodowego w tym Unii Europejskiej z uwagi na transgraniczny charakter zagrożeń badanego obszaru. Ponadto za przykłady przedstawiono incydenty, które zaistniały w USA, Gruzji, ponieważ ze względu na skutki oraz rozmiar były one kluczowe podczas analizy zakresu zagrożeń.

2.4. Cele: główny i szczegółowe badań

Głównym celem badań jest identyfikacja luk, wad, słabości w Systemie Bezpieczeństwa Narodowego i opracowanie na podstawie jej wyników koncepcji zwiększenia poziomu bezpieczeństwa państwa, przy czym główny cel badań jest kompozycją celu poznawczego i utylitarnego.

Cel poznawczy: Identyfikacja zagrożeń dla Systemu Bezpieczeństwa Narodowego oraz ocena ich wpływu na poziom bezpieczeństwa. Wyszukiwanie luk, wad i słabości na podstawie wyników badań polegających na wywiadach, wywiadach eksperckich z respondentami, którzy przyczynią się do identyfikacji rodzaju zagrożeń w dziedzinowych sektorach bezpieczeństwa państwa ze szczególnym uwzględnieniem analizy ryzyka utraty informacyjnej ciągłości działania.

Cel utylitarny: Opracowanie koncepcji wzmocnienia Systemu Bezpieczeństwa Narodowego, której podstawowym elementem będzie wskazanie sposobów eliminacji lub ograniczenia wykrytych podatności. Podstawą koncepcji będzie przegląd elementów

[77] 2018 rok – wejście w życie ustawy o Krajowym Systemie Cyberbezpieczeństwa.

systemu bezpieczeństwa państwa i zdefiniowanie zbioru zdarzeń generujących ryzyko utraty informacyjnej ciągłości działania.

Ponadto w rozprawie postawiono cele szczegółowe profilowane poszczególnymi rozdziałami dysertacji do których należą:

1) Ustalić miejsce cyberbezpieczeństwa w Systemie Bezpieczeństwa Narodowego i związek z informacyjną ciągłością działania (ICD) tego systemu.
2) Przedstawić zakres, problemy, hipotezy i metody badawcze.
3) Wskazać jakie zagrożenia wykorzystujące cyberprzestrzeń mogą wpływać na ICD.
4) Dokonać ewaluacji czynników ryzyka utraty ICD.
5) Opracować koncepcję wzmacniania Systemu Bezpieczeństwa Narodowego w aspekcie przeciwdziałania realizacji zagrożeń dla ICD.
6) Ocenić możliwości wdrożenia i praktycznego zastosowania opracowanej koncepcji.

2.5. Problem główny i szczegółowe

Główny problem badawczy ma odpowiedzieć na pytanie jakie luki, wady, słabości występują w obecnym Systemie Bezpieczeństwa Narodowego i w jaki sposób można ograniczać skutki ich wykorzystania do nieuprawnionych działań w celu podniesienia poziomu bezpieczeństwa państwa?

Ponadto w rozprawie w formie pytań przedstawiono problemy szczegółowe, które zostaną rozwiązane w poszczególnych rozdziałach dysertacji a należą do nich:

1) Jaki wpływ na poziom bezpieczeństwa państwa i jego ciągłość działania ma cyberbezpieczeństwo?
2) Jakie badania należy podjąć w celu opracowania koncepcji poprawy bezpieczeństwa państwa?
3) Jaki wpływ na bezpieczeństwo państwa mają zagrożenia wykorzystujące cyberprzestrzeń?
4) Jakie podatności wpływają na utratę ICD państwa i jakie są ich obszary przyczynowe?
5) W jaki sposób można poprawić aktualny stan bezpieczeństwa państwa z uwzględnieniem ryzyka utraty cyberbezpieczeństwa?
6) Jakie są możliwości wdrożenia opracowanej koncepcji i jakie warunki muszą być

spełnione, aby skutecznie ją zaimplementować?

2.6. Hipotezy: główna i szczegółowe

Główna hipoteza obszaru badań zakłada, że w cyberprzestrzeni występuje szereg zagrożeń dla bezpieczeństwa narodowego, które wymagają stosownych odpowiedzi ze strony instytucji państwa w szczególności eliminacji podatności obniżających odporność państwa na cyberzagrożenia. System Bezpieczeństwa Narodowego wymaga dostosowania obecnych instytucji, regulacji prawnych oraz poziomu sił i środków do współczesnych zagrożeń wykorzystujących do materializacji cyberprzestrzeń.

Ponadto w pracy dokonano weryfikacji założeń, które przedstawiono jako hipotezy szczegółowe a należą do nich twierdzenia takie jak:

1) Dominującym elementem bezpieczeństwa państwa jest zdolność do zachowania informacyjnej ciągłości działania wszystkich kluczowych instytucji państwa.
2) Zachowanie ciągłości działania Systemu Bezpieczeństwa Narodowego determinowana jest zdolnością utrzymania informacyjnej ciągłości działania.
3) Zastosowanie oceny ryzyka jest elementem niezbędnym do prognozowania jakości decyzji modyfikujących System Bezpieczeństwa Narodowego.
4) Wyeliminowanie wad, luk i słabości może być podstawą do opracowania koncepcji poprawy bezpieczeństwa państwa i zapewniania jego ciągłości działania.
5) Opracowana koncepcja jest możliwa do implementacji i praktycznego zastosowania po spełnieniu określonych warunków organizacyjno-prawnych i społeczno-ekonomicznych.

2.7. Metody, techniki i narzędzia badawcze

W dysertacji przyjęto, że do realizacji celów oraz rozwiązania problemów badawczych zasadne będzie zastosowanie komplementarnych metod teoretycznych i empirycznych. Wykorzystane zostaną różne metody, techniki i narzędzia, gdzie w tym przypadku wiodącą metodą będą wywiady oraz wywiady eksperckie polegające na zebraniu opinii i poglądów bezpośrednio od wybranych respondentów oraz ekspertów w zakresie cyberbezpieczeństwa. Badania będą podzielone na dwie części. Pierwsza obejmuje wywiad wstępny z respondentami celem uzyskania informacji o zagrożeniach (Rozdział III). Druga cześć będzie wywiadem eksperckim końcowym

podsumowywującym jakość utworzonej koncepcji poprawy bezpieczeństwa (Rozdział VI). W obu przypadkach wykorzystanym narzędziem będzie kwestionariusz wywiadu a następnie zostanie dokonana analiza zebranych odpowiedzi.

W ramach przygotowania do wprowadzenia w dziedzinę problemu dokonano krytycznej analizy istniejących definicji podstawowych pojęć oraz uzupełniono je autorskimi definicjami. Dodatkowo w toku rozprawy przeanalizowano dokumenty normatywne na poziomie krajowym takie jak Strategia Bezpieczeństwa Narodowego, Strategia Rozwoju Systemu Bezpieczeństwa Narodowego oraz kluczowe regulacje prawne z perspektywy badanych zagadnień, czyli m.in. ustawy o Krajowym Systemie Cyberbezpieczeństwa.

W celu dokonania wglądu w rodzaje zagrożeń przeprowadzono studium przypadków zdarzeń, które miały poważne konsekwencje i w znacznym stopniu przyczyniły się do utraty informacyjnej ciągłości działania organizacji. W studium przypadków dominowały zdarzenia, które odbiły się głośnym echem na arenie międzynarodowej do których należały:

- Sytuacji Estonii w czasie „cyber-incydentu" z 2007 roku jako przykład paraliżu teleinformatycznego państwa.
- Ataki teleinformatyczne wspierających konflikt w Gruzji z 2008 roku jako przykład pierwszej nazwanej mianem „cyber-wojny".
- Wyciek wojskowej bazy danych JIM w Polsce z 2022 roku jako przykład podatności systemów teleinformatycznych.
- Wymuszenie okupu w USA podczas „cyber-ataku" na rurociąg paliwowy Colonial Pipeline z 2021 roku jako przykład ataku na infrastrukturę krytyczną.

Zdarzenia te zostały wyeksponowane w sposób przyczynowo skutkowy tak aby konsekwentnie można było odnieść się do źródła ich niepowodzenia a także wyeksponować ich następstwa i skutki.

Istotne z punktu widzenia pozyskiwania danych o zagrożeniach okazały się statystyki cyberbezpieczeństwa, które przedstawiono celem analizy kierunków, metod oraz technik generowania zagrożeń. Dane statystyczne ze względu na transgraniczny charakter obejmują zarówno krajowe raporty o stanie cyberbezpieczeństwa jak i poziomu Unii Europejskiej. Analiza statystyk połączona z odpowiedziami na wywiad ekspercki pozwoli na utworzenie zbioru zagrożeń, który został skonfrontowany z zdolnościami Systemu Bezpieczeństwa Narodowego celem wyłonienia tych zagrożeń, na które obecny

system jest nieprzygotowany. Pozwoli to na utworzenie katalogu zagrożeń resztkowych dla których została podjęta próba opracowana koncepcji poprawy bezpieczeństwa państwa z jednoczesną eliminacją podatności. Zagrożenia zostały poddane analizie celem dokonania wstępu do szacowania ryzyka prawdopodobieństwa ich wystąpienia oraz ustalenia poziomu istotności podatności z którymi korelują. Celem dekompozycji podatności na czynniki pierwsze przedstawiono je przy pomocy modelu romboidalnego co pozwoliło na analizę obszaru przyczynowego powstania ich.

Badania nad opracowaną koncepcją również wymusiły analizę dokumentów normatywnych pod kątem możliwości wdrożenia pewnych rozwiązań naprawczych. Działania te miały na celu zweryfikowanie w jakim stopniu oraz w jakim zakresie opracowana koncepcja jest możliwa do implementacji z uwzględnieniem ograniczeń i możliwości prawno-proceduralnych, finansowo-ekonomicznych, techniczno-logistycznych oraz mentalnych i organizacyjnych. Uzupełnieniem implementacji są badania ankietowe ukierunkowane do respondentów reprezentujących kluczowe instytucje zajmujące się cyberbezpieczeństwem co pozwoliło na uzyskanie odpowiedzi na pytanie czy opracowana koncepcja spotka się z akceptacją w środowisku dziedzinowych ekspertów.

Reasumując metody i narzędzia badawcze wykorzystane w pracy przedstawiono syntetyczne zestawienie z podziałem na teoretyczne i empiryczne:

- *teoretyczne*: analiza systemowa, synteza, indukcja i dedukcja, komparatystyka, analiza literatury, metoda analizy i krytyki piśmiennictwa, metoda analizy i konstrukcji logicznej, metoda badania dokumentów.
- *empiryczne*: ankiety, sondaż diagnostyczny, wywiad, wywiad ekspercki, analiza SWOT, model romboidalny.

Na podstawie wyodrębnionych celów, problemów i hipotez badawczych dokonano określenia zmiennych zależnych i niezależnych w celu ustalenia czynników wpływających na poprawę istniejących rozwiązań dzięki opracowanej koncepcji poprawy bezpieczeństwa:

- *zmienne zależne*: cyberbezpieczeństwo, zdolność reagowania na incydenty, ryzyko wystąpienia zagrożenia, zasoby organizacji, ciągłość działania.
- *zmienne niezależne*: cyberprzestrzeń, doświadczenie, zdolności, kwalifikacje, aktywności, zasoby, kultura i system, wartości, funkcjonalność, użyteczność, efektywność, niezawodność, jakość.

2.8. Organizacja i przebieg badań

Proces badawczy w pracy rozpoczął się od momentu analizy kluczowych pojęć mających istotny wpływ na obszar badawczy. Definicje bezpieczeństwa, cyberprzestrzeni, cyberbezpieczeństwa, ciągłości działania, w tym informacyjnej ciągłości działania, poddano analizie krytycznej celem wyłonienia tych definicji, które nie zawierają w swej konstrukcji błędu logicznego oraz w sposób jednoznaczny przybliżają tematykę rozprawy. Te definicje to:

Bezpieczeństwo:

„*Bezpieczeństwo to stan, w którym ryzyka i wynikające z nich zagrożenia są minimalizowane lub eliminowane*".

Cyberprzestrzeń:

„Cyberprzestrzeń - środowisko (na które składa się ląd, woda, powietrze, przestrzeń kosmiczna oraz pole elektromagnetyczne) i umieszczone w tym środowisku obiekty (w tym ludzie) posiadające zdolności kształtowania pola elektromagnetycznego i wykrywania jego zmian oraz magazynowania informacji o tych zmianach".

Cyberbezpieczeństwo:

„Cyberbezpieczeństwo - nazwa oznaczająca, że na bezpieczeństwo (stan, w którym ryzyko i wynikające z nich zagrożenia są minimalizowane lub eliminowane) nie wpływa negatywnie cyberprzestrzeń (rozumiana jako środowisko, na które składa się ląd, woda, powietrze, przestrzeń kosmiczna oraz pole elektromagnetyczne posiadająca zdolności kształtowania pola elektromagnetycznego i wykrywania jego zmian oraz magazynowania informacji o tych zmianach), która jest wykorzystywana do realizacji zagrożeń".

Ciągłość działania;

„Ciągłość działania organizacji - to zdolność organizacji do realizacji podstawowych zadań biznesowych na określonym poziomie jakości z przerwami nie dłuższymi niż dopuszczalne".

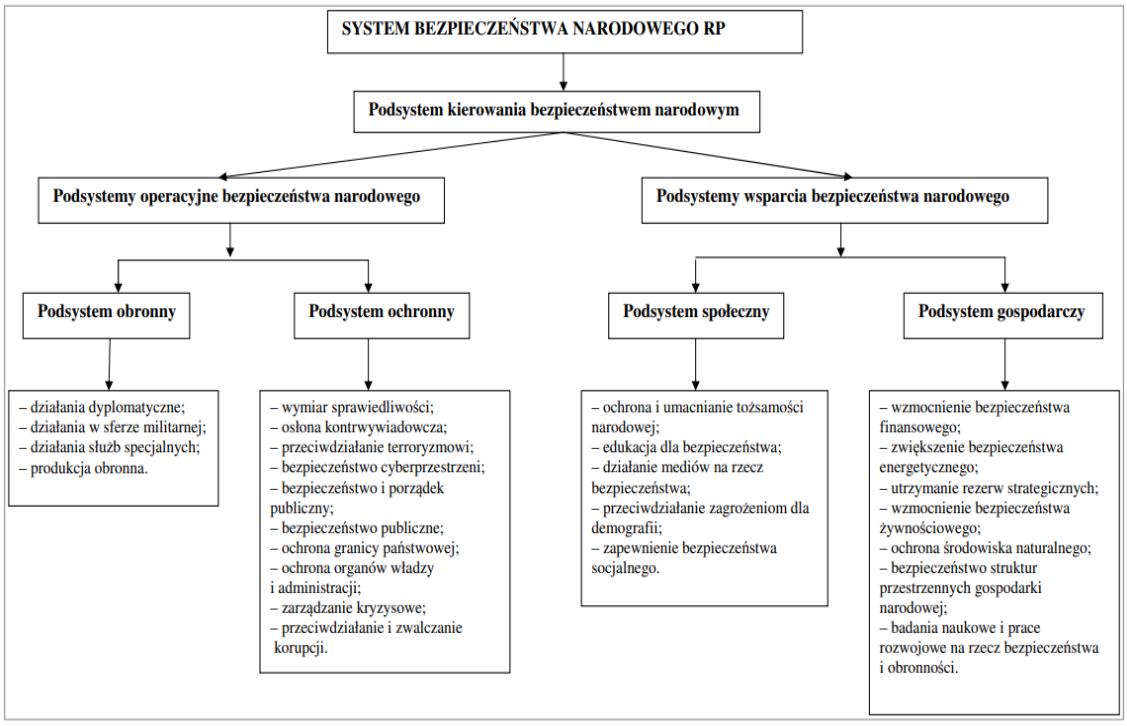
Informacyjna ciągłość działania;

„Informacyjna ciągłość działania – to zdolność podmiotu do realizacji statutowych zadań w warunkach zakłóconego operowania zasobami informacyjnymi z uwzględnieniem alternatywnych procesów, które mogą zostać wdrożone w sytuacji zaistnienia interakcji przejawów zagrożenia z podatnością przy użyciu sił i środków oraz w czasie niepowodującym obniżenia efektywności danego podmiotu".

Definicje te stanowią podstawę modelu Systemu Bezpieczeństwa Narodowego, którego postać graficzna jest pokazana na rysunku 14 (Rozdział I). System ten został zdefiniowany w następujący sposób:

„System Bezpieczeństwa Narodowego – jest to zbiór wzajemnie skorelowanych obiektów oraz zbiór relacji pomiędzy nimi, które poprzez realizację statutowych zadań w wszystkich dziedzinowych obszarach bezpieczeństwa pełnią funkcję prewencyjną, zwalczającą i minimalizującą skutki zagrożeń zarówno wewnętrznych jak i zewnętrznych".

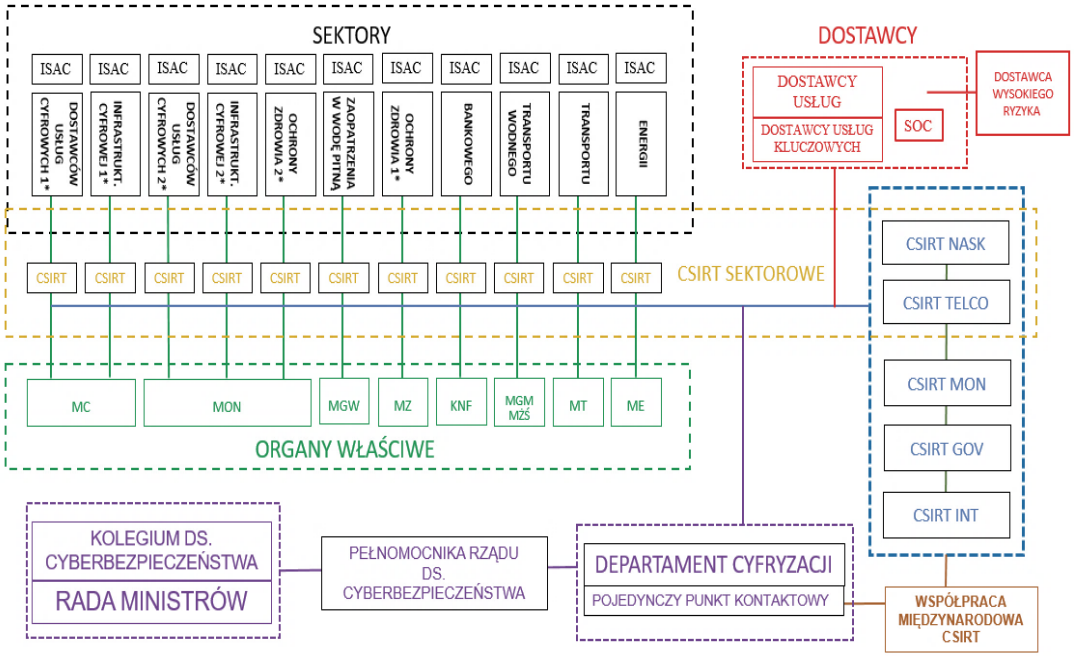
Wzorując się definicjami wybranych pojęć w toku pracy nastąpiła detekcja wad, luk i słabości w obecnym systemie bezpieczeństwa państwa, wobec czego analizie i modyfikacji został poddany klasyczny model Systemu Bezpieczeństwa Narodowego wraz z podsystemami, których schemat prezentowany jest na rysunku 18.



Rys. 18. Model Systemu Bezpieczeństwa Narodowego wraz z podsystemami.
Źródło: https://bibliotekanauki.pl/articles/120095.pdf s. 72 [dostęp: 13.08.2024].

Jak ustalono w rozdziale pierwszym kluczową role w SBN wobec narastających zagrożeń stanowi podsystem odpowiedzialny za bezpieczeństwo cyberprzestrzeni, czyli Krajowy System Cyberbezpieczeństwa, którego zdekomponowana postać została przedstawiona na grafice (Rys. 19). To właśnie ten system przejął ciężar obrony państwa, ponieważ współcześnie to zdecydowana większość zagrożeń wykorzystuje do materializacji cyberprzestrzeń. W związku z czym tworzenie koncepcji poprawy bezpieczeństwa

państwa w toku badań skoncentrowane jest w głównej mierze na tym systemie. Należy jednak uznać holistyczne podejście do bezpieczeństwa i zaznaczyć, że nie tylko ten system jest odpowiedzialny za cyberbezpieczeństwo. Istotne jest tutaj zrozumienie, że największe szanse powodzenia ataku są wtedy, kiedy celem wrogich działań jest jakaś wada, luka, słabość, czyli szerokorozumiana podatność. Mając na uwadze powyższe to w każdej dziedzinie w każdym obszarze istnieją podatności, które mogą być potencjalnym celem ataków teleinformatycznych wrogich podmiotów.



Rys. 19. Struktura Krajowego Systemu Cyberbezpieczeństwa w wersji znowelizowanej.
Źródło: Opracowanie własne na podstawie Biuletyn PTI nr 4/2021, ISSN 2719-8472, s. 29-33.

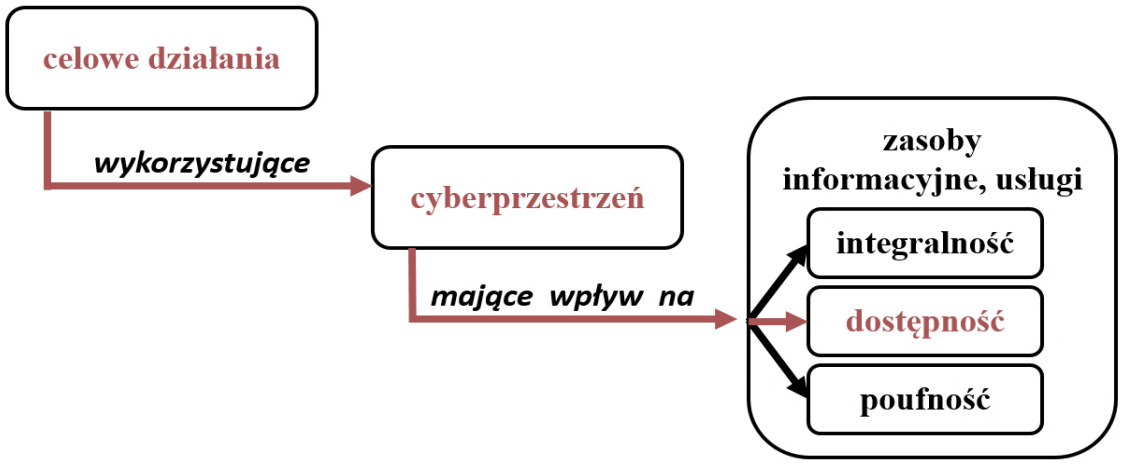
W celu wyeksponowania podatności dokonano również analizy dokumentacji normatywnej takiej jak strategie: SBN, SSRK, DSRK, SR SBN, Ustawa o KSC, co zaowocowało ustaleniem obszarów, które w połączeniu z zdiagnozowanymi zagrożeniami będą wyznaczały ryzyko materializacji zagrożeń. Przy wykorzystaniu metody „desk reserach" zestawiono dane statystyczne sposobów realizacji zagrożeń z ostatnich kilku lat celem wychwycenia kierunków ataków, które będą kluczowe jako prognoza na kolejne lata. Kolejnym krokiem było sporządzenie kwestionariuszu wywiadu oraz wywiadu eksperckiego, który zawierał 8 pytań (załącznik nr 1) dotyczących nowych kierunków rozwoju przyszłych zagrożeń jak i również propozycji minimalizacji skutków ich materializacji. Analiza przedstawionych statystyk wraz z wywiadem, który został skierowany do przedstawicieli każdego z szesnastu sektorów Systemu Bezpieczeństwa Narodowego oraz instytucji zajmujących się

cyberbezpieczeństwem pozwoliła na utworzenie zbioru zagrożeń, który został skonfrontowany z obecnymi możliwościami przeciwdziałania SBN. W konsekwencji powstał szczątkowy zbiór sposobów realizacji zagrożeń na który obecny system nie jest przygotowany dając jednocześnie podwaliny do utworzenia koncepcji poprawy bezpieczeństwa państwa. Zagrożenia zbioru resztkowego zostały poddane ewaluacji ryzyka co pozwoliło na oszacowanie prawdopodobieństwa ich wystąpienia oraz wskazaniu istotności podatności. Wyeksponowane podatności zostały poddane próbie eliminacji poprzez wdrożenie działań naprawczych w wyniku czego powstała koncepcja poprawy bezpieczeństwa państwa. Badania nad implementacyjnością opracowanej koncepcji polegały wykorzystaniu analizy SWOT dla każdego z proponowanych rozwiązań celem wyłonienia nowych zagrożeń wskazania mocnych stron oraz uwzględnieniu szans. Procedura ta pozwoliła na zweryfikowane czy istnieją uwarunkowania do wprowadzenia w życie przedmiotowych zmian z uwzględnieniem ograniczeń finansowo-ekonomicznych, techniczno-logistycznych oraz prawno-proceduralnych i mentalnych. W ostatnim etapie badań opracowano sondaż diagnostyczny celem zweryfikowania słuszności wdrożenia koncepcji.

ROZDZIAŁ III. IDENTYFIKACJA ZAGROŻEŃ BEZPIECZEŃSTWA NARODOWEGO RZECZPOSPOLITEJ POLSKIEJ

3.1. Zagrożenia wykorzystujące cyberprzestrzeń i wpływające na utratę informacyjnej ciągłości działania państwa – studium przypadków

Istnieje wiele rodzajów klasyfikacji zagrożeń, gdzie do najogólniejszego, ze względu na stosunek do obszaru państwa, należą wewnętrzne i zewnętrzne. Dodatkowo, można wyróżnić podział ze względu na podmiotowość – zagrożenia ekologiczne, ekonomiczne, energetyczne, fizyczne, teleinformatyczne, kulturowe, militarne, polityczne, socjalne i społeczne. Taka klasyfikacja poniekąd wynika z opisu nazw sektorów prezentowanych w Strategiach Bezpieczeństwa Narodowego.



Rys. 20. Schemat badanych zagrożeń.
Źródło: opracowanie własne.

Głównym celem badań dysertacji, jest wychwycenie zagrożeń, dla obecnego systemu bezpieczeństwa państwa, mających wpływ na poziom krajowego cyberbezpieczeństwa oraz utrzymanie informacyjnej ciągłość działania państwa. Główny nacisk położony jest na działania celowe wrogich podmiotów wykorzystujących cyberprzestrzeń do wpływu na poufność, integralność i dostępność zasobów informacyjnych oraz usług (Rys. 20). Należy zaznaczyć, że główna uwaga zostanie skupiona na zagrożeniach mających kluczowy wpływ na „dostępność" zasobów, ponieważ analiza danych statystycznych wskazuje ten rodzaj ataków teleinformatycznych jako najczęstsze źródło niepowodzenia. W celu zrozumienia jakiego rodzaju incydenty mieszczą się w przedstawionym przedziale oraz jak bardzo poważne skutki niesie za sobą materializacja tych zagrożeń dokonano przeglądu studium przypadku zdarzeń, w których doszło do utraty ciągłości działania na dużą skalę.

Sytuacja Estonii w czasie „cyberincydentu" z 2007 roku[78].

Estonia doświadczyła jako pierwszy kraj w historii Europy zmasowanego ataku na swą infrastrukturę teleinformatyczną. Według źródeł wywiadowczych napastnicy powiązani byli z władzami Federacji Rosyjskiej. W wyniku trzytygodniowej fali ataków zostały zablokowane serwery i strony prawie wszystkich mediów. Sytuacja była na tyle poważna, że NATO wysłało swoich najlepszych ekspertów ds. cyberterroryzmu do Tallina, aby zbadali sprawę i pomogli Estończykom wzmocnić ich cyberobronę. Według dziennika „The Guardian" głównymi celami były serwery i strony internetowe:

- prezydencja estońska i jej parlament;
- prawie wszystkie ministerstwa rządowe w kraju;
- partie polityczne;
- trzy z sześciu dużych organizacji informacyjnych w kraju;
- dwa największe banki;
- firmy specjalizujące się w komunikacji.

Zdarzenia spowodowały społeczną panikę, ponieważ świadomość obywateli i rządu o cyberwojnie była względnie niska. Nikt nie zdawał sobie sprawy ze skali problemu oraz jak długo to potrwa. Obywatele rozwiniętego państwa niebędącego w stanie wojny nagle stracili dostęp do informacji, środków finansowych, rozrywki i innych usług teleinformatycznych. Obawy społeczne były zasadne, ponieważ mało kto był w stanie uwierzyć w niewidzialnego wroga co powodowało dezorientacje obywateli, która podsycana była zniekształconymi informacjami o stanie faktycznym. Dodatkowo należy podkreślić to, że Estonia na owe czasy posiadała jedne z najlepiej rozwiniętych systemów teleinformatycznych w Europie środkowo-wschodniej co nie uchroniło państwa przed atakami. Sytuacja wymusiła na estońskich służbach mobilizację nie tylko państwowych instytucji, ale również prywatnych firm zajmujących się cyberbezpieczeństwem celem próby opanowania sytuacji[79]. Dość szybko okazało się, że jedynym sposobem niwelującym ataki jest całkowite odcięcie od usług informatycznych niemalże wszystkich użytkowników państwa a w efekcie izolując kraj od reszty świata.

Komentarz – incydent estoński jest przykładem jak w skali państwa może być sparaliżowana infrastruktura krytyczna, która doprowadziła do utraty informacyjnej ciągłości działania.

[78] https://www.theguardian.com/world/2007/may/17/topstories3.russia [dostęp: 22.02.2023].
[79] M. Dąbrowski, Wyzwania i zagrożenia dla bezpieczeństwa Europy środkowo-wschodniej. Dezinformacja w działaniach hybrydowych. ISBN 978-83-67138-76-5, s. 185.

Zdarzenia z tamtego okresu wpisują się w teorię pierścieni Wardena[80], który to opisał jakimi metodami można zneutralizować przeciwnika bez użycia sił zbrojnych. Kluczowe znaczenie miało tu przeprowadzenie pierwszy raz w historii ataków na zmasowaną skalę powodując dezorientację władz oraz paraliż instytucji państwowych. Należy zwrócić uwagę na fakt, że Estonia w tamtych latach była w czołówce liderów pod względem cyberbezpieczeństwa a stopień rozwoju państwa w tym zakresie był na zaawansowanym poziomie, jednak to nie uchroniło bałtyckiego państwa przed katastrofalnymi skutkami materializacji zagrożenia.

Ataki teleinformatyczne wspierające konflikt w Gruzji z 2008 roku[81].

Sytuacja w Gruzji nazywana mianem pierwszej „cyberwojny" była przełomowym wydarzeniem, ponieważ to właśnie wtedy na masową skalę do wspierania działań zbrojnych wykorzystano cyberprzestrzeń. Konflikt zbrojny między siłami zbrojnymi Gruzji a separatystami z republik Osetii Południowej i Abchazji oraz wojskami interwencyjnymi Federacji Rosyjskiej (FR) poniekąd wywołany był działaniami hybrydowymi (podobnie jak na Ukrainie w 2014 roku) poprzez dezinformację społeczeństwa i podsycanie ruchów prorosyjskich. Gruzja to kraj, który obok Estonii chyba najbardziej doświadczył skutków ataków na systemy teleinformatyczne. Infrastruktura IT został zaatakowana w tym samym czasie, kiedy rosyjskie wojska zbliżyły się na kilkadziesiąt kilometrów do Tbilisi. Celem padły strony serwisów rządowych w tym ambasad USA, Wielkiej Brytanii i innych państw. Ucierpiały systemy bankowe poprzez ataki DDoS. Podmienianie były witryny internetowe w połączeniu z sfałszowanymi komunikatami BBC i CNN, preparowano zainfekowane strony, które w rzeczywistości infekowały komputery i propagowały dalsze ataki. Zastosowano również próbę znieważenia prezydenta Gruzji M. Saakaszwilego w której podmieniono zawartość strony prezydenckiej i treść portalu zastąpiono pokazem slajdów ze zdjęciami Adolfa Hitlera. Działania te spowodowały, że operatorzy usług teleinformatycznych z wówczas jedynym gruzińskim CSIRT[82] nie byli w stanie powstrzymywać ataków. Jak później wykazało dochodzenie, pomimo że konflikt rozpoczął się w sierpniu to przygotowania do głównego ataku na infrastrukturę teleinformatyczną trwały już od marca 2008 roku. Analiza po wydarzeniach doprowadziła do ustalenia, że za skoordynowanymi atakami stoi Serwis StopGeorgia.ru (Georgia, czyli Gruzja) przy

[80] Koncepcja Johna A. Wardena opiera się na założeniu, że „wróg jest systemem" złożonym z pięciu koncentrycznych okręgów takich jak siły zbrojne, populacja, infrastruktura, procesy, przywództwo.
[81] https://www.cybsecurity.org/pl/gruzja-rosja-konflikt-w-cyberprzestrzeni/ [dostęp: 28.04.2023].
[82] CSIRT – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego.

użyciu RBN - Russina Business Network[83], która słynie z podobnych procederów w przestępczym podziemiu rosyjskiego Internetu.

Komentarz – pomimo, że konflikt w Gruzji był jednym z najkrótszych w historii wojen a siły gruzińskie liczebnie nie odbiegały od wielkości sił FR wraz separatystami to koncepcja połączenia działań regularnych z paraliżem informacyjnym okazała się druzgocząco skuteczną techniką operacyjną i znacznie przechyliła szalę zwycięstwa na korzyść wrogiego podmiotu. Opisywane zdarzenia są przykładem synergii, czyli operacji połączonych co należy rozumieć jako scalenie klasycznych operacji wojskowych z operacjami w cyberprzestrzeni, obecnie V domeną sił zbrojnych. Skutki owego incydentu miały szerokie odbicie w społeczeństwie uniemożliwiając obywatelom zdobywanie informacji o zaistniałych zdarzeniach co uruchomiło napęd rozwijający działalność propagandową i dezinformacyjną. Niemniej uderzająca była również kwestia zablokowania możliwości prezentowania gruzińskiego stanowiska i wydarzeń z kraju na arenie międzynarodowej co opóźniało wszelką pomoc i wsparcie międzynarodowe dla Gruzji. Biorąc pod uwagę skuteczność zastosowanej taktyki istnieje dość duże prawdopodobieństwo wspierania w przyszłych operacjach wojskowych działaniami o podobnym charakterze. Z tego też powodu zachodzi uzasadniona konieczność utrzymywania i rozwijania organów odpowiedzialnych za prowadzeniu działań obronnych cyberprzestrzeni w Polsce na szczebli krajowym.

Wymuszenie okupu w USA cyberatakiem *na rurociąg Colonial Pipeline[84].*

Atak na rurociąg Colonial Pipeline miał miejsce w 2021 roku. Wrogie podmioty z grupy „Dark Side" wstrzymały pracę ropociągów o długości prawie dziewięciu tysięcy kilometrów oraz zdobyły 100 GB poufnych danych, których użyto jako karty przetargowej podczas żądania okupu. Dodatkowo przy pomocy techniki „ransomware[85]" zblokowano systemy teleinformatyczne poprzez szyfrowanie danych co spowodowało wstrzymanie 45% dostaw paliwa do wschodniej części kraju. Sytuacja utrzymująca się sześć dni powodowała realne zagrożenie wstrzymania ruchu lotniczego oraz drastyczny wzrost cen dla konsumentów komercyjnych. W wyniku poważnych strat oraz utrudnień w komunikacji dla całego wschodniego wybrzeża USA operator rurociągu próbując

[83] Dąbrowski M., Wyzwania i zagrożenia dla bezpieczeństwa Europy środkowo-wschodniej. Dezinformacja w działaniach hybrydowych. ISBN 978-83-67138-76-5, s. 188.

[84]https://biznesalert.pl/hakerzy-colonial-pipeline-cyberatak-polityka-bezpieczenstwo-cyberprzestrzen/ [dostęp: 21.02.2023].

[85] Ransomware to rodzaj złośliwego oprogramowania, którego celem jest blokowanie systemów komputerowych, poprzez szyfrowanie danych.

zapobiec całkowitej kompromitacji zapłacił okup w wysokości 5 mln dolarów w krypto walucie. Dodatkowo operator nie podjął w odpowiednim czasie działań mających na celu współpracy z organami ścigania. Zapłacenie okupu przez konsorcjum paliwowe świadczyło o niskiej skuteczności lub o ewentualnym braku możliwości działania prewencyjnego w tej sytuacji.

Komentarz – przykład paraliżu infrastruktury krytycznej mający istotny wpływ na ciągłość działania państwa (ruch lotniczy, drogowy). Biorąc pod uwagę blokadę systemów teleinformatycznych należy uwzględnić również ustanie informacyjnej ciągłości działania. Ponadto zdarzenie to jest przykładem jak potężne mocarstwo jakim są Stany Zjednoczone potrafi być bezsilne wobec małej grupy wykwalifikowanych wrogich podmiotów. Opóźniona współpraca z państwowymi organami i próba ukrycia incydentu doprowadziła nie tylko do strat finansowych, ale również wizerunkowych całego państwa. Następstwem tego zdarzenia było wprowadzenie regulacji prawnych mających na celu obowiązek niezwłocznego zgłaszania do organów państwowych incydentów celem natychmiastowej interwencji. Porównując to zdarzenie z krajowymi realiami należy podkreślić fakt, że w Polsce istnieje duża liczba infrastruktury krytycznej, która może być potencjalnym celem wrogiego podmiotu a czasowy paraliż którejś z nich spowodowałby utratę ciągłości działania kluczowych gałęzi przemysłu lub pozbawił znacznej części kraju dostępu do usług niezbędnych do funkcjonowania społeczeństwa.

Wyciek wojskowej bazy danych JIM w Polsce z 2022 roku[86].

Jednolity Indeks Materiałowy[87] (JIM) jest to baza danych, która wspiera system logistyczny polskich Sił Zbrojnych. Zawiera ona wszelkie informacje na temat części zapasowych, kategorii uzbrojenia, rodzaju sprzętu oraz zapotrzebowania na nie. Ujawnione dane zawierały ponad 1 mln 700 tyś. rekordów, z których można przeanalizować jakimi środkami rażenia dysponuje każda jednostka organizacyjna w kraju. Jak stwierdzili eksperci baza zawiera stan zasobów armii aktualny do września 2022 roku. W ujawnionych bazach wymienione są także rodzaje oprogramowania z którego korzysta wojsko oraz wykaz zakupionych przez nie licencji. Osobą odpowiedzialną za wyciek był najprawdopodobniej jeden z pracowników działu

[86] https://wiadomosci.onet.pl/kraj/gigantyczny-wyciek-danych-z-wojska-ponad-17-mln-pozycji-w-internecie/1mknjtf [dostęp: 28.04.2023].

[87] Baza Jednolitego Indeksu Materialnego, Baza danych oficjalnie wprowadzona decyzją nr 69/MON z 19 lutego 2007 roku w sprawie wdrażania i użytkowania jednolitego indeksu materiałowego w Siłach Zbrojnych RP.

informatycznego Inspektoratu Wsparcia Sił Zbrojnych, instytucji, która odpowiada za zakupy dla wojska oraz magazynowanie sprzętu i części zamiennych. Dochodzenie w sprawie dowiodło, że pracownik stworzył autorski program, do którego skopiował dane z niejawnych wojskowych systemów celem łatwiejszej ich analizy.

Komentarz – W przedstawionym incydencie wyeksponowano jak bardzo newralgiczne w systemach teleinformatycznych są zasoby informacyjne. Można pokusić się o stwierdzenie, że to co przez operacje trwające latami wywiad wrogiego państwa próbuje zdobyć zostało udostępnione w postaci jednej bazy danych w ciągu jednego dnia. W tym przypadku ewidentnie przyczyną było naruszenie poufności zasobów informacyjnych natomiast do ustalenia pozostaje czy był to błąd ludzki czy celowe działania. Należy mieć świadomość, że w Polsce zasoby informacyjne mające często postać baz danych niejawnych informacji występują w każdego rodzaju systemach teleinformatycznych eksploatowanych w administracji państwowej. Z tego też powodu powinny być traktowane jako kluczowe dobro i należy je szczególnie chronić przed nieautoryzowanym dostępem.

Prezentowane studium przypadków to tylko niektóre z zdarzeń jakie mogą spowodować utratę informacyjnej ciągłości działania podmiotu (organizacji, państwa). Należy zwrócić uwagę, że do podobnych zdarzeń dochodzi cyklicznie w całej Polsce z tą różnicą, że skala oraz straty są nieporównywalnie mniejsze czego dowodem są statystyki organów odpowiedzialnych za cyberbezpieczeństwo. Niemniej jednak na podstawie prezentowanych przypadków można wywnioskować, że niepodejmowanie jakichkolwiek działań mających charakter prewencyjny prowadzi do katastrofalnych wręcz strat dla całego państwa i obywateli.

3.2. Luki, wady i słabości wpływające na bezpieczeństwo - analiza dokumentów

W podrozdziale tym dokonano analizy dokumentów normatywnych mających kluczowe znaczenie dla funkcjonowania Systemu Bezpieczeństwa Narodowego oraz systemów niższego szczebla. Dokumenty te są o tyle istotne, ponieważ pokazują zależność pomiędzy wizją ogólnego bezpieczeństwa państwa a cyberbezpieczeństwem gdzie biorąc pod uwagę jak ważne jest prawo w bezpieczeństwie teleinformatycznym tego rodzaju analiza jest konieczna. Dokumentami tymi są:

- Strategia Bezpieczeństwa Narodowego (SBN);[88]
- Strategia Rozwoju Systemu Bezpieczeństwa Narodowego (SR SBN);[89]
- Ustawa o Zarządzaniu Kryzysowym (ZK);[90]
- Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC);[91]
- Projekt nowelizacji ustawy o KSC (w toku od 2020).[92]

Ponadto przeanalizowano zapisy stanowiące o roli i randze cyberbezpieczeństwa w strukturach państwa, adekwatności struktury oraz prawnego uwarunkowania podmiotów odpowiedzialnych za cyberbezpieczeństwo. Wszelkie elementy budzące wątpliwości skatalogowano w trzech kategoriach takich jak luki, wady, słabości. Stwierdzono nie tylko braki prawne, proceduralne, infrastrukturalne, ale również wadliwe elementy systemu lub takie, których sprawność i efektywność jest na niskim poziomie a co za tym idzie mogą być podatne na zagrożenia. Prezentowane kategorie w dalszej części badań będą traktowane jako podatności systemu. Podatności przedstawiono w formie podpunktów wymagających usprawnienia poprzez ujęcie ich w koncepcji poprawy bezpieczeństwa i należą do nich:

- słabości:[93]
  - niskie zainteresowanie interesariuszy publicznymi konsultacjami nowelizacji ustawy o KSC (tzw. NIS2);
  - niewystarczająca ilość i jakość regulacji prawnych dotyczących dezinformacji;
  - niski poziom współpracy pomiędzy podmiotami odpowiedzialnymi za cyberbezpieczeństwo;
  - niski poziom nakładów (finansowania) podmiotów odpowiedzialnych za cyberbezpieczeństwo;
- wady:[94]

[88] https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf. [dostęp: 28.04.2023].
[89] https://www.bbn.gov.pl/ftp/dok/01/strategia_rozwoju_systemu_bezpieczenstwa_narodowego_rp_2022.pdf. [dostęp: 28.04.2023].
[90] https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20070890590/U/D20070590Lj.pdf. [dostęp: 28.04.2023].
[91] https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf. [dostęp: 28.04.2023].
[92] https://orka.sejm.gov.pl/Druki9ka.nsf/0/C974DE0E6799563DC12589E40030360D/%24File/3457-ustawa.docx. [dostęp: 28.04.2023].
[93] Słabości – rozumiane jako funkcjonujące rozwiązania, lecz na niskim poziomie efektywności.
[94] Wady – rozumiane jako rozwiązania, które nie spełniają wymagań.

- wskazanie Operatora Strategicznej Sieci Bezpieczeństwa (OSSB) jako jedynego w postaci jednoosobowej spółki;
- marginalne powiązanie Strategii Cyberbezpieczeństwa z krajowymi Strategiami;
- różnorodność pochodzenia eksploatowanego sprzętu teleinformatycznego oraz eksploatacja urządzeń pochodzących od producentów uznanych za „dostawców wysokiego ryzyka"

– luki[95]:

- brak sprzężenia instytucji Centralnego Biura Zwalczania Cyberprzestępczości z Krajowym Systemem Cyberbezpieczeństwa;
- brak właściwego do wagi zagadnienia wyeksponowania roli cyberbezpieczeństwa w Strategii Rozwoju Systemu Bezpieczeństwa Narodowego;
- brak regulacji prawnych dotyczących działalności Centrów Wymiany i Analizy Informacji;
- brak satysfakcjonującego poziomu ukompletowania kadr odpowiedzialnych za cyberbezpieczeństwo w administracji państwowej.

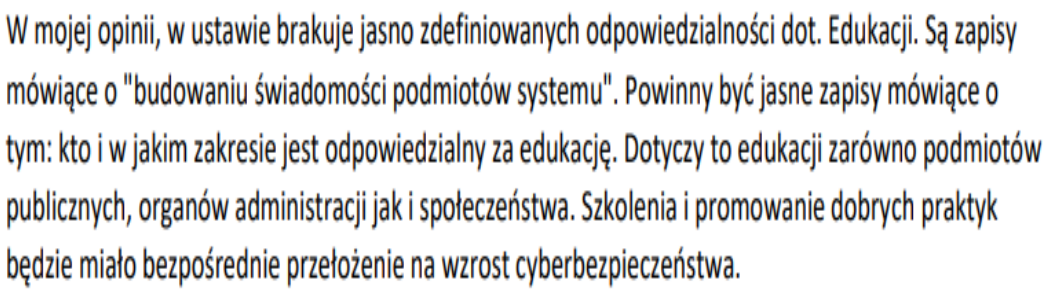
W celu szczegółowego rozwinięcia prezentowanych podatności dokonano ich opisu z jednoczesną próbą w sposób lapidarny wskazania rozwiązania przedmiotowego problemu.

„Niskie zainteresowanie interesariuszy publicznymi konsultacjami nowelizacji ustawy o KSC (tzw. NIS2)"

Przegląd projektu nowelizacji Krajowego Systemu Cyberbezpieczeństwa a właściwie samego procesu jego wdrażania budzi pewne wątpliwości. Mianowicie zwyczajowo każdy projekt nowej ustawy poddawany jest konsultacjom międzyresortowym oraz publicznym, gdzie każdy z interesariuszy (instytucje i podmioty gospodarcze) ma prawo (również we własnym interesie) do przeanalizowania i wniesienia poprawek oraz ewentualnie wyrażenia swoich problemów związanych z wdrażanymi przepisami. Analiza zbioru pism dostępnych w biuletynie informacji publicznych wykazała, iż stanowiska organów, które ze względu na swą podmiotowość powinny być dość żywotnie zainteresowane cyberbezpieczeństwem

[95] Luki - rozumiane jako braki.

wyrażają brak uwag co do proponowanych zmian w projekcie[96]. Oczywiście nie ma w tym nic złego, że jest pełna aprobata natomiast należy zwrócić uwagę, że zmiana tak ważnej ustawy zdarza się raz na kilka lat lub więcej związku z czym konsultacje jest to czas, gdzie należy wręcz zaakcentować problemy cyberbezpieczeństwa w danej organizacji i próbować je przekazać do wiadomości decydentów z jednoczesnym wyeksponowaniem ich na tle zapisu projektu[97]. Mowa tu o takich instytucjach jak Służba Ochrony Państwa (SOP), Krajowa Rada Radiofonii i Telewizji (KRRiT) dla których cyberbezpieczeństwo jest kluczowym elementem. Dodatkowo nie stwierdzono w wykazie pism odpowiedzi głównych interesariuszy wchodzących w skład nowej struktury KSC podmiotów odpowiedzialnych za gospodarkę wodną oraz transportu co może świadczyć o braku zainteresowania lub brakiem osób z odpowiednimi kwalifikacjami do analizy i zdiagnozowania przedmiotowej problematyki. Stwierdzono natomiast liczne petycje (interpretowane jako odwołania i skargi) od podmiotów będących bezpośrednio w kręgu tzw. „dostawców wysokiego ryzyka" takich jak „Huawei" i „ZTE" oraz osób cywilnych, które „doradzają" w sprawach państwowych, gdzie jedna z uwag została zaprezentowana w grafice (Rys. 21).



Rys. 21. Tekst zawarty w „petycji" od prywatnej osoby.
Źródło: https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html [dostęp: 12.04.2022].

Merytoryka treści odzwierciedla słuszne zaniepokojenie i realną potrzebę wprowadzenia odpowiedniego systemu edukacji. Jednakże przesłanie „gołego" tekstu bez podpisu, podania afiliacji, daty, czy bez zachowania „kultury biurowej" i stylistyki ogólnie przyjętej świadczy wyłącznie o swego rodzaju frustracji pewnego obywatela i prawdopodobnie takie „pseudo pismo" nie będzie rozpatrywane wśród poważnych wypowiedzi podmiotów zainteresowanych.

[96] https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-zamowien-publicznych.html [dostęp: 05.04.2024].

[97] Proces konsultacji publicznych ma na celu uwzględnienie wszelkich potencjalnych zastrzeżeń zgłaszanych przez strony zainteresowane danym projektem.

„Niewystarczająca ilość i jakość regulacji prawnych dotyczących dezinformacji"

W ustawie o Krajowym Systemie Cyberbezpieczeństwa zarówno jak i w projekcie jej nowelizacji nie zaobserwowano poważniejszej wzmianki o coraz większym problemie dezinformacji wśród mediów tradycyjnych i społecznościowych. Współczesne wydarzenia na świecie wyraźnie pokazują jak bardzo destrukcyjna na społeczeństwo może być dezinformacja, którą można porównać do Broni Masowego Rażenia. Nie jest to przesadą, ponieważ spełnia pewne kryteria (niesie poważne skutki, oddziałuje psychologiczne a nawet może zagrażać życiu i zdrowiu wielkiej liczbie osób), przy czym takie kryteria spełniają również „cyberataki[98]". W Polsce istnieją stowarzyszenia takie jak np. Demagog, które świadczą usługi walki z dezinformacją natomiast należałoby rozważyć utworzenie w strukturze KSC „oficjalnego" ośrodka na wzór Europejskiego Obserwatorium Mediów Cyfrowych (w którym również Polska uczestniczy). Takie działanie miałoby na celu skuteczną walkę z dezinformacją szczególnie w czasie istotnych wydarzeń, takich jak wybory lub okresy napięć społecznych wywołanych zagrożeniami epidemii czy konfliktu zbrojnego. Rozwiązaniem tego problemu może być zastosowanie tak zwanego modelu francuskiego szerzej opisanego w podrozdziale 1.3.2, który polega na utworzeniu na szczeblu krajowym rady ds. dezinformacji oraz skuteczne szybkie sankcjonowanie decyzji tej rady przez wytypowane sądów 24 godzinnych.

„Niski poziom współpracy między podmiotami odpowiedzialnymi za cyberbezpieczeństwo"

Coraz bardziej zauważalnym problemem jest niski poziom współpracy mającej na celu wspólne działania na rzecz utrzymania wysokiego poziomu cyberbezpieczeństwa. Należy przez to rozumieć sytuację, w której dany podmiot (najczęściej środowiska akademickie) próbują uzyskać informację o rzeczywistym stanie cyberbezpieczeństwa poprzez realizację metod badawczych takich jak wywiady, wywiady eksperckie, ankiety lub sondaże diagnostyczne a w konsekwencji często nie uzyskują wiarygodnych i rzetelnych odpowiedzi z organów właściwych. Taki stan rzeczy powoduje paraliż procesu naprawczego lub wdrażania rozwiązań systemowych dla przedmiotowej problematyki co w rezultacie przekłada się na poziom bezpieczeństwa. Przedstawiony problem należy do kategorii mentalnych, ponieważ nie ma żadnego oficjalnego zakazu udzielania informacji publicznie dostępnych to jednak instytucje zasłaniają się

[98] Przykład: 2017 rok, atak na sieć szpitali NHS w Wielkiej Brytanii wywołany poprzez złośliwe oprogramowanie typu ransomware (WannaCry), gdzie około 20 tyś. pacjentów zostało odciętych od usług medycznych.

wrażliwością tych, że informacji. Sytuacja skutkuje w niektórych przypadkach brakiem możliwości prowadzenia badań nad podniesieniem poziomu bezpieczeństwa co samo w sobie jest podatnością. Należy zatem poważnie podejść do partnerstwa cywilno-publicznego i stosowania dobrych praktyk akademickich, ponieważ to właśnie środowiska akademickie posiadają odpowiedni potencjał i zdolności do prowadzenia badań nad poprawą bezpieczeństwa i wdrażaniem nowych zbadanych rozwiązań.

„Niski poziom finansowania podmiotów odpowiedzialnych za cyberbezpieczeństwo".

Problem najbardziej dotkliwy ze wszystkich, ponieważ pozostałe problemy wywodzą się od niego. Finansowanie cyberbezpieczeństwa na poziomie krajowym wymaga poważnego przeanalizowania dlatego, że stale rosnące zagrożenia wymagają zwiększania środków finansowych zarówno na utrzymanie odpowiednio wykształconej kadry, instytucji oraz badań nad nowymi technologiami. Z punktu widzenia skali zagrożeń wskazane jest utworzenie specjalnego funduszu na utrzymanie cyberbezpieczeństwa realizowanego nie tylko z budżetu państwa, ale również z podatku jakim jest choćby opłata radiowo-telewizyjna, która jest ściśle powiązana z korzystaniem z usług cyfrowych na odpowiednim poziomie. Pomimo, że tworzenie kolejnego podatku jest z natury rzeczy nieakceptowalne społecznie to ta celowa opłata RiTV powinna być przeznaczona na pokrycie usług związanych również z cyberbezpieczeństwem. W przeciwnym razie niski stan finansowania cyberbezpieczeństwa będzie odbijał się na ilości i jakości personelu odpowiedzialnego za bezpieczeństwo.

„Wskazanie Operatora Strategicznej Sieci Bezpieczeństwa (OSSB) jako jedynego w postaci jednoosobowej spółki".

Istotną wadą jaką reprezentuje nowelizacja ustawy o KSC jest wskazanie w obecnej formie Operatora Strategicznej Sieci Bezpieczeństwa (OSSB). Zakłada się, że ma to być jednoosobowa spółka Skarbu Państwa będąca jednocześnie operatorem telekomunikacyjnym[99]. Operator OSSB będzie świadczył usługi na rzecz istotnych instytucji państwowych takich jak policja, wojsko, rząd, infrastruktura krytyczna, sądownictwo, ośrodki władzy samorządowe. W związku z czym zasadnym jest, aby nadzorowany przez rząd operator strategiczny, który ma przejąć kontrolę nad Internetem i telefonią komórkową nie był jedynym. Jest to istotne, ponieważ istnieje duże prawdopodobieństwo, że będzie on celem ataków teleinformatycznych a co za tym idzie

[99] Interpelacja nr 29249 do Prezesa Rady Ministrów, Ministra Cyfryzacji w sprawie zmian w ustawie o krajowym systemie cyberbezpieczeństwa.

zachodzi realne ryzyko paraliżu tego operatora. Spowodowanie strat u OSSB pozbawi tym samym operatorów (podwykonawców) świadczenia usług w tym obszarze co przełoży się na blokadę całej administracji państwowej. Jak już opisywano kluczowe dla ciągłości działania są przedsięwzięcia organizacyjne i techniczne, które w swej treści nawiązują do zapasowej infrastruktury usługowej a w tym przypadku zapasowego operatora strategicznego. Ponadto zgodnie z wszelkimi standardami jednoosobowa spółka, która jest zaproponowana nie jest najlepszym rozwiązaniem dla tego typu instytucji, ponieważ rodzi to problemy natury niezależności i upolitycznienia tego organu. W związku z czym wskazane byłoby w tym przypadku kierować się nadmiarowością systemu lub silnym zapleczem badawczo-rozwojowym.

„Marginalne powiązanie Strategii Cyberbezpieczeństwa z krajowymi Strategiami"

Kolejnymi słabościami jakie można dostrzec w toku analizy dokumentów normatywnych jest marginalne traktowanie zagrożeń cyberprzestrzeni w strategiach różnego poziomu. Jak zakładają twórcy dokumentu „Strategia Rozwoju Systemu Bezpieczeństwa Narodowego", dokument ten jest w pełni sprzężony z Zintegrowanymi Strategiami Rozwoju, przy czym nie jest powiązany z Strategią Cyberbezpieczeństwa. Jest to dość dyskusyjny problem, ponieważ jeżeli dokument odpowiadający za rozwój Systemu Bezpieczeństwa Narodowego jest ściśle powiązany np. ze Strategią Rozwoju Wsi a nie jest powiązany z Strategią Cyberbezpieczeństwa to świadczy o tym, że dokument nie wykorzystuje w pełni swojego potencjału kreowania wizji pełnego spektrum zagrożeń dla SBN. Ponadto stwierdzono urwaną ciągłość przejścia hierarchii zagrożeń z dokumentu wyższego szczebla, na niższy lub równoległy. Ponieważ budowa cyberbezpieczeństwa rozpoczyna się od solidnego wypracowania dokumentacji planistycznej, strategicznej oraz regulacji prawnych, trzeba zachować logiczny ciąg pomiędzy dokumentami. Należy przez to rozumieć, że Strategia Bezpieczeństwa Narodowego, która w 2020 roku doczekała się nowelizacji i treść dokumentu w o wiele mocniejszym stopniu eksponuje rolę cyberbezpieczeństwa w stosunku do poprzedniej wersji to nadal cyberbezpieczeństwo w dokumentach niższego szczebla jest traktowane przedmiotowo. Przyczyną takiego stanu rzeczy jest data publikacji dokumentów i brak ich aktualizacji. Należy tutaj zaznaczyć, że godne uwagi jest traktowanie cyberbezpieczeństwa na szczeblu Unii Europejskiej, gdzie obecnie powstaje dużo dokumentów i regulacji prawnych nakazujących wprowadzanie zmian państwom członkowskim w zakresie podniesienia rangi przedmiotowego cyberbezpieczeństwa.

„Różnorodność pochodzenia eksploatowanego sprzętu teleinformatycznego oraz eksploatacja urządzeń pochodzących od producentów uznanych za „dostawców wysokiego ryzyka”

Administracja państwowa dysponuje ogromną rzeszą zasobów IT niezbędnych do prawidłowej realizacji wszelkich procesów. Każdy pracownik korzysta z różnorodnego sprzętu komputerowego czy urządzeń mobilnych wyposażonych w licencjonowane oprogramowanie. Niesie to za sobą konsekwencje w postaci konieczności rozbudowy zaplecza logistycznego celem utrzymania zasobów IT na odpowiednim poziomie. Dodatkowo należy gromadzić informacje na temat posiadanego wyposażenia oraz monitorować jego cykl życia gwarantując sprawne działanie sprzętu, aktualność systemów oraz bezpieczeństwo danych. Zjawiskiem dość często praktykowanym jest celowe, maksymalne przedłużanie resursu sprzętu IT, ponieważ w magazynach zalegają materiały eksploatacyjne pasujące wyłącznie do danego typu urządzenia. Dość dużym problemem jest eksploatacja sprzętu teleinformatycznego od producentów uznanych niebawem za „dostawców wysokiego ryzyka”. Zdecydowana większość sprzętu będąca na wyposażeniu organów państwowych pochodzi z Rosji, Chin i USA. Są to państwa rozwinięte technologicznie, które oferują produkty elektronicznej infrastruktury cyfrowej często unikalnych rozwiązań, których nie można zastąpić krajowymi bezpiecznymi produktami. Współczesne zagrożenia dość mocno eksponują trend tworzenia tak zwanych „Backdoor” w oprogramowaniu, poprzez które może nastąpić nieautoryzowany dostęp. Luki te występują w oprogramowaniu a biorąc pod uwagę, że producenci niechętnie dzielą się kodami źródłowymi swoich produktów to nigdy nie wiadomo co jest zaszyte w „software i hardware” większości urządzeń cyfrowych. Problem jest dotkliwy, ponieważ nie ma możliwości wymiany całego eksploatowanego sprzętu na ten rodzimej produkcji. Jest to wręcz nierealne pod względem logistycznym, finansowym oraz technologicznym. Prawdopodobnie problem ten będzie rozwiązywany sukcesywnie przez długie lata natomiast trzeba mieć świadomość, że technologicznie jako państwo nie jesteśmy w stanie produkować całego asortymentu produktów, które są obecnie eksploatowane. Jest to słabość, której nie można zaradzić w krótkim przedziale czasowym, ponieważ obecne zdolności produkcyjne są ograniczone a jedynym rozwiązaniem tego problemu są inwestycje w nowe technologie i krajowy, sprawdzony przemysł elektroniczny co sukcesywnie wyprze „obcą” technologię z rynku.

„Brak sprzężenia instytucji Centralnego Biura Zwalczania Cyberprzestępczości z Krajowym Systemem Cyberbezpieczeństwa”

Skoro w strukturze KSC wyszczególniono organ właściwy jakim jest Ministerstwo Obrony Narodowej (MON) wraz sektorami odpowiedzialności w ramach cyberbezpieczeństwa to czy obecnie tworzone Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) podlegające pod Ministerstwo Spraw Wewnętrznych i Administracji (MSWiA) nie powinno też zostać sprzężone z systemem? Biorąc pod uwagę, że przestępstwa teleinformatyczne są coraz bardziej powszechne i stanowią integralną część negatywnej działalności w cyberprzestrzeni to wręcz zasadnym jest ustanowienie miejsca tego biura wraz z wzajemnymi powiązaniami z pozostałą częścią systemu. Włączenie CBZC do Krajowego Systemu Cyberbezpieczeństwa pozwoli na lepszą współpracę pomiędzy organami właściwymi do spraw cyberbezpieczeństwa uniknięcie przerzucania odpowiedzialności między instytucjami. Ponadto pozwoli na ujednolicenie procedur i odciążenie CSIRT-ów w sprawach, którym nadano już charakter postępowania prokuratorskiego co znacznie podniesie sprawność obsługiwanych incydentów teleinformatycznych. Dodatkowo należy zbadać czy CBZC w obecnej postaci jest wystarczającym organem wobec dynamicznie rosnącej cyberprzestępczości.

„Brak właściwego do wagi zagadnienia wyeksponowania roli cyberbezpieczeństwa w Strategii Rozwoju Systemu Bezpieczeństwa Narodowego”

Strategia Rozwoju Systemu Bezpieczeństwa Narodowego jest dokumentem z 2013 roku i prezentuję wizję rozwoju SBN na okres do 2022 roku w związku z czym jest już „po terminie”. Ponieważ dokument tworzony był ponad dekadę temu nie stwierdzono w nim należytego podejścia do cyberbezpieczeństwa godnego wyzwaniom współczesnych czasów. Biorąc pod uwagę jak bardzo w ostatniej dekadzie zagrożenia cyberprzestrzeni ewaluowały należy rozpocząć pracę nad nowelizacją strategii, która jest powiązana z nowymi (zaktualizowanymi) dokumentami. Obecna strategia nawiązuje jeszcze do Polityki Ochrony Cyberprzestrzeni RP, którą zastąpiła Strategia Cyberbezpieczeństwa na lata 2019-2024 oraz Strategii Obronności Rzeczypospolitej Polskiej roku 2009 roku, którą zastąpiła Strategia Bezpieczeństwa Narodowego z 2020 roku. W związku z czym zachodzi konieczność utworzenia nowelizacji przedmiotowej strategii, która będzie godnie eksponowała współczesne zagrożenia wykorzystujące cyberprzestrzeń celem urealnienia tak naprawdę jedynego dokumentu, który w sposób całościowy opisuje wizję Systemu Bezpieczeństwa Narodowego.

„Brak regulacji prawnych dotyczących działalności Centrów Wymiany i Analizy Informacji"

Kolejną luką jaką można odnaleźć w projekcie o KSC są Centra Wymiany i Analizy Informacji (ang. ISAC), które bazują na partnerstwie między podmiotami prywatnymi i publicznymi, gdzie zazwyczaj są one jednostkami non-profit. Oczywiście koncepcja jest jak najbardziej słuszna natomiast z założenia są to podmioty, które nie podlegają sztywnym uregulowaniom prawnym. W szczególności brak jest przepisów, które określałyby sposób ich finansowania czy zarządzania nimi. W związku z czym źródłem finansowania może być prywatna dotacja co w jakimś stopniu lobbuje działalność ISAC. Obecnie w USA działa 25 sektorowych ISAC zrzeszonych w National Council of ISACs (NCI[100]) czyli organizacje koordynującą, stworzoną w celu maksymalizacji przepływu informacji między podmiotami prywatnymi a władzami, przy czym w projekcie nowelizacji KSC nie został wskazany wiodący ISAC co może przełożyć się na „chaos" hierarchiczny i niezdrową rywalizację zamiast współpracy (synergii). Zgodnie z założeniami wg stanu na 2023 rok szacunki ministerstwa właściwego ds. cyfryzacji przewidują w ramach „Partnerstwa dla Cyberbezpieczeństwa" funkcjonowanie 11 podmiotów ISAC, a z kolejnymi 18 trwają ustalenia warunków współpracy[101]. Tak duża liczba podmiotów równorzędnych wymusza wręcz zgodnie ze standardami zarządzania wyznaczenie organu koordynującego.

„Brak satysfakcjonującego poziomu ukompletowania kadr odpowiedzialnych za cyberbezpieczeństwo w administracji państwowej"

Ściśle powiązany problem z niskim poziomem finansowania cyberbezpieczeństwa jest to brak odpowiedniej ilości i jakości wyspecjalizowanych kadr. Przyczyną takiego stanu rzeczy jest konkurencyjność na cywilnym rynku pracy, gdzie stawki na stanowiskach znacznie odbiegają od tych w administracji państwowej. Pomimo wprowadzenia rozporządzenia[102] mającego wyrównać stopień zarobków pomiędzy rynkiem cywilnym a administracją państwową to nadal problem nie jest rozwiązany. Przede wszystkim brak jest ścisłych wytycznych kto i na jakich zasadach dodatek ten otrzymuje, gdzie niektórzy

[100] NASK, ISAC (Centra Wymiany i Analizy Informacji) w kontekście sektorowych centrów cyberbezpieczeństwa, s. 4.
[101] Projekt z dnia 7 września 2020 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych, s. 48.
[102] Rozporządzenie Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa. Dz.U. 2022 poz. 131.

kierownicy jednostek organizacyjnych wprowadzają dodatkowe wytyczne niepoparte żadnymi regulacjami oraz obostrzenia celowo pozbawiając pracowników tego świadczenia. Mowa tu o organizowaniu dodatkowych egzaminów wewnętrznych, których zdawalność jest znikoma, pomimo że w rozporządzeniu mowa jest tylko o posiadaniu certyfikatu jako podstawy do przyznania świadczenia. W związku z czym nie jest w pełni wykorzystywane wsparcie mające na celu zachęcenia i pozostawienia na stanowisku administracji państwowej osób wykwalifikowanych. Należy zatem uznać, że ogólna globalna tendencja wskazuje na braki w tego typu specjalistach, wobec czego należy podjąć kroki wspierające, zachęcające oraz ułatwiające kształcenie osób w preferowanym kierunku jak również egzekwować rozwiązania mające na celu zachęcić specjalistów do pozostania na stanowisku w administracji państwowej.

Problemy tutaj przedstawione wynikające z analizy dokumentów normatywnych struktury SBN oraz dostępnych informacji zawartych w literaturze oraz Internecie są nieliczne i prezentowane tylko powierzchownie. Należy również mieć świadomość, że będąc w połowie 2025 roku, jeżeli przeanalizujemy zapisy samej Strategii Cyberbezpieczeństwa RP na lata 2019-2024 to nasuwa się konkluzja, że żaden z pięciu celów szczegółowych w niej zawartych nie został w pełni zrealizowany[103]. W związku z czym zasadnym jest podniesienie dyskusji nie tylko na temat tworzenia dobrego prawa i dokumentów planistycznych, ale również egzekwowaniu ich treści w bieżącej działalności państwa polskiego.

3.3. Dane statystyczne zagrożeń w cyberprzestrzeni.

Statystyki cyberbezpieczeństwa między innymi mają na celu ekspozycję danych w postaci tabelarycznej, które zawierają informację na temat rodzaju incydentów, kategorii oraz sektorów branżowych na które są przeprowadzane ataki. W Polsce organami odpowiedzialnymi za obsługę incydentów są tzw. CSIRT (Computer Security Incident Response Team) gdzie do głównych poziomu krajowego należą:

- CSIRT NASK[104] utrzymywany przez Państwowy Instytut Badawczy NASK;

[103] https://portal.pti.org.pl/wp-content/uploads/2024/03/8_cyber-raporty.pdf [dostęp: 09.05.2024].

[104] CSIRT NASK – prowadzony jest przez Naukową i Akademicką Sieć Komputerową, Państwowy Instytut Badawczy. Jako jednostka badawcza prowadzi szereg różnych projektów. Jednym z najistotniejszych projektów prowadzonych przez instytucję w chwili obecnej jest projekt SiSSDeN w ramach europejskich programów badawczych Horizon 2020, którego celem jest poprawa stanu cyberbezpieczeństwa europejskich instytucji i użytkowników końcowych poprzez rozwój świadomości sytuacyjnej oraz współdzielenie użytecznych informacji o zagrożeniach.

- CSIRT GOV[105] utrzymywany przez Agencję Bezpieczeństwa Wewnętrznego;
- CSIRT MON[106] utrzymywany przez Ministerstwa Obrony Narodowej.

Do prezentowanego grona należałoby włączyć jeszcze Centralne Biuro Zwalczania Cyberprzestępczości (CZBC), które jako jednostka organizacyjna Policji obsługuje incydenty związane z przestępczością internetową. Oprócz wymienionych instytucji szczebla krajowego są jeszcze podmioty sektorowe realizujące zadania związane z obsługą incydentów takie jak np. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego polskiego sektora finansowego (CSIRT KNF) lub zespoły CERT funkcjonujące przy operatorach telefonii komórkowej oraz inne z tą różnicą, że podmioty te nie publikują oficjalnych danych. Statystyki tworzą wszystkie instytucje szczebla krajowego w cyklicznych raportach o stanie cyberbezpieczeństwa uwzględniając branżowe incydenty. Godnym zauważenia jest fakt, że niezależnie od kontekstu zagrożeń niemalże wszystkie instytucje kreujące dane statystyczne wskazują na dwie podstawowe przyczyny niezadawalającego stanu cyberbezpieczeństwa. Pierwsza to brak należytego finansowania cyberbezpieczeństwa a druga to brak wystarczającej liczby odpowiednio wyszkolonych kadr w tym zakresie co wskazano także w poprzednim podrozdziale. Oczywiście istnieje oczywista korelacja pomiędzy tymi potrzebami, ponieważ to głównie poziom zarobków w administracji publicznej jest główną przyczyną tak niskiego poziomu ukompletowania stanowisk związanych z cyberbezpieczeństwem. W celu zweryfikowania jakie są dominujące kierunki zagrożeń oraz które sektory branżowe są najbardziej narażone na ataki dokonano przeglądu danych statystycznych.

CERT NASK publikuje coroczny raport o nazwie „CERT Polska[107]", w którym znajdują się zestawienia zdarzeń zgłoszonych do tej instytucji. W Tab. 5 przedstawiono zestawienie incydentów od 2013 do 2024 roku, z podziałem na charakter zagrożenia. Na podstawie raportu CERT Polska można wywnioskować, że w ostatnich latach a w szczególności po 2019 roku ataki na usługi

[105] CSIRT GOV – jednym z jego podstawowych zadań jest rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej.

[106] CSIRT MON do zadań należy koordynacja obsługi incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane, w tym podmioty, których systemy teleinformatyczne lub sieci teleinformatyczne objęte są jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej oraz przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, w stosunku do których organem organizującym i nadzorującym wykonywanie zadań na rzecz obronności państwa.

[107] Raporty roczne działalności CERT Polska z lat 2013-2024.

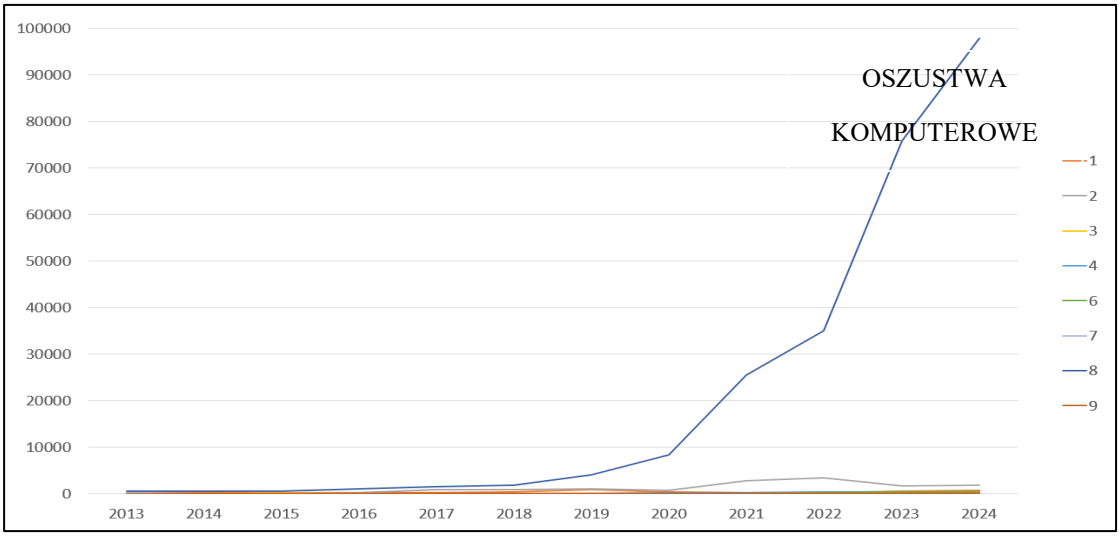
handlowe, oszustwa komputerowe oraz złośliwe oprogramowanie są dominującymi zagrożeniami w cyberprzestrzeni. Taki stan rzeczy jest prawdopodobnie podyktowany pandemią COVID19, gdzie społeczność w znacznym stopniu przestawiła się na pracę i naukę zdalną a tym samym zwiększyła się intensyfikacja zakupów w sieci co indukowało ten rodzaj zagrożeń. Natomiast na podstawie danych branżowych należy rozumieć, iż sektory takie jak media, energetyka, infrastruktura cyfrowa, bankowość, handel, usługi pocztowe są szczególnie narażone na wszelkiego rodzaju ataki.

Tab. 5. Zestawienie incydentów z lat 2013-2024.

LP	Incydent \ rok	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
1	Obraźliwe i nielegalne treści	160	370	146	237	185	431	812	371	311	308	584	775
2	Złośliwe oprogramowanie	320	98	142	211	854	862	969	746	2847	3409	1650	1891
3	Gromadzenie informacji	46	98	270	65	157	101	95	60	27	31	29	26
4	Włamania do systemów	11	13	10	54	118	125	160	317	247	384	418	447
5	Próby włamań do systemów	30	36	76	109	262	153	77	174	127	121	205	179
6	Dostępność zasobów ataki DDOS	30	69	35	45	53	49	57	121	148	175	385	426
7	Atak na bezpieczeństwo Informacji	33	25	89	45	28	46	41	68	55	39	59	62
8	Oszustwa komputerowe	589	613	611	1069	1439	1878	4086	8310	25472	35009	75917	97995
9	Inne	0	40	77	91	52	25	102	42	33	49	56	14

Źródło: opracowanie własne na podstawie raportów CERT.

Dane zawarte w tabeli 5 przedstawione w graficzny sposób na wykresie (Rys. 22).



Rys. 22. Wykres graficzny danych z tabeli 5
Źródło: opracowanie własne.

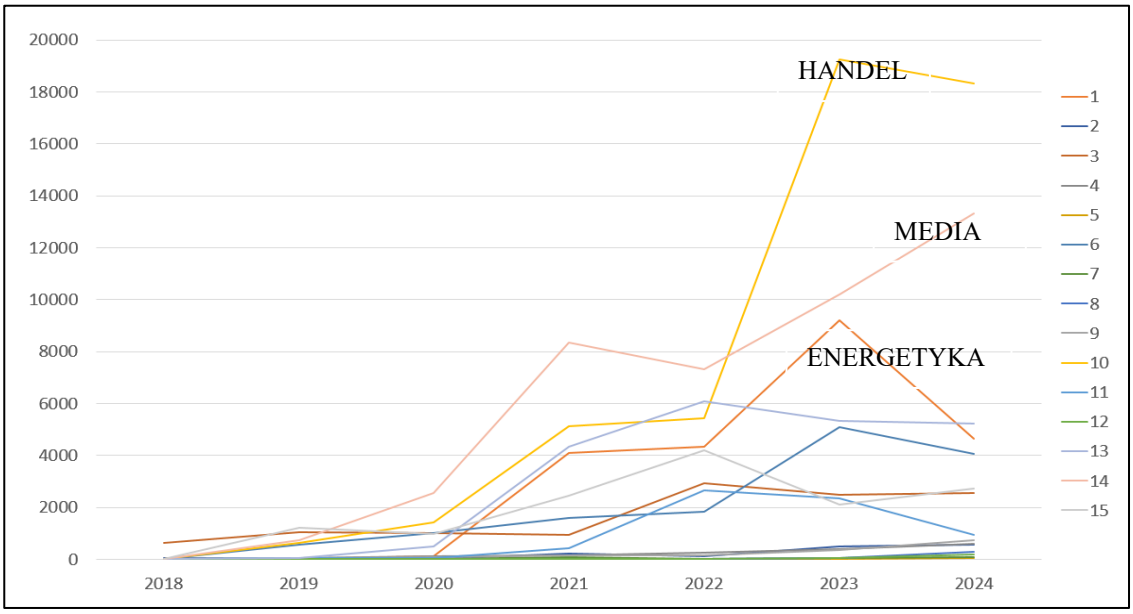
Zestawienie incydentów w przedziale czasowym od 2018 do 2024 roku z podziałem na sektory dziedzinowe zostało przedstawione w Tab. 6.

Tab. 6. Zestawienie incydentów w sektorach branżowych z lat 2018 – 2024.

LP	Sektor \ rok	2018	2019	2020	2021	2022	2023	2024
1	Energetyka	20	28	101	4084	4320	9196	4632
2	Transport	51	61	29	220	111	492	565
3	Bankowość	643	1057	1008	947	2944	2481	2544
4	Służba zdrowia	13	53	112	150	251	405	604
5	Wodociągi	2	5	9	18	9	13	59
6	Infrastruktura cyfrowa	29	550	1016	1606	1821	5101	4055
7	Budownictwo	bod	31	29	89	24	61	68
8	Kultura i dziedzictwo nar.	bod	9	7	11	30	62	292
9	Oświata i wychowanie	bod	62	71	142	167	354	733
10	Handel hurtowy i detaliczny	bod	624	1437	5125	5438	19253	18324
11	Produkcja	bod	46	57	421	2650	2353	956
12	Logistyka i dystrybucja	bod	19	27	18	15	64	184
13	Poczta i usługi kurierskie	bod	49	500	4338	6093	5319	5216
14	Media	bod	748	2568	8339	7329	10191	13322
15	Osoby fizyczne	bod	1212	959	2464	4214	2105	2735

Źródło: opracowanie własne na podstawie raportów CERT.

Dane zawarte w tabeli 6 przedstawione w graficzny sposób na wykresie (Rys. 23).



Rys. 23. Wykres graficzny danych z tabeli 6.
Źródło: opracowanie własne.

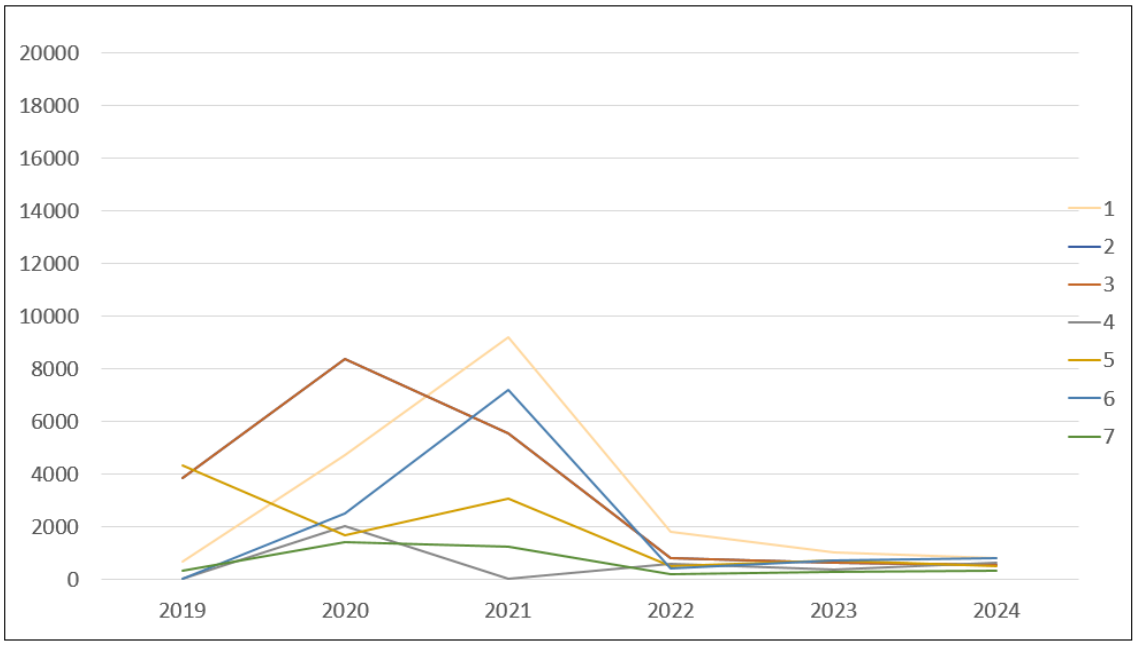
CSIRT GOV Agencji Bezpieczeństwa Wewnętrznego publikuje coroczny raport o stanie bezpieczeństwa cyberprzestrzeni RP[108]. Ze względu na specyficzny obszar, który zespół monitoruje statystyki dotyczą ataków na organy państwowe. W tabeli nr. 7 przedstawiono liczbę incydentów wg sektorów zgłoszonych przez podmioty krajowego systemu cyberbezpieczeństwa. Niestety dostęp do wyników poniżej 2019 roku jest niemożliwy, ponieważ gromadzone dane miały inny charakter w związku z czym analiza będzie dotyczyła ostatnich sześciu lat.

Tab. 7. Liczba incydentów wg sektorów z lat 2019 – 2024.

LP	Sektor \ rok	2019	2020	2021	2022	2023	2024
1	Infrastruktura krytyczna	685	4714	9196	1798	1022	783
2	Urząd	3837	8356	5563	809	629	559
3	Pozostałe	3206	4714	644	650	910	391
4	Organ państwowy	*b.d.*	2039	*b.d.*	599	380	627
5	Ministerstwo	4336	1656	3056	503	736	501
6	Instytucja	*b.d.*	2518	7203	400	725	817
7	Służby	341	1400	1237	200	274	313

Źródło: opracowanie własne na podstawie raportów rocznych CSIRT GOV.

Dane zawarte w tabeli 7 przedstawione w graficzny sposób na wykresie (Rys. 24).



Rys. 24. Wykres graficzny danych z tabeli 7.
Źródło: opracowanie własne.

[108] https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [dostęp: 01.02.2024].

W zestawieniu incydentów z okresu 2019-2024 z podziałem na sektory (Tab. 7) wyniki są niejednoznaczne i brak w nich logicznego trendu. Należy to rozumieć jako wahania ilości incydentów, które są wzrostowe lub malejące w następujących po sobie latach. Przyczyn takiego stanu rzeczy może być wiele. Istnieje podejrzenie, że w głównej mierze pandemia COVID19 przyczyniła się do takiego stanu rzeczy. Ponadto do prawdopodobnych przyczyn należą również uwarunkowania polityczne, stopień rozbudowy ochrony danego sektora czy też sytuacją w relacjach stosunków międzynarodowych. Potwierdzeniem tej tezy może być zestawienie rozkładu źródeł ataków na sieci, która również przedstawia niejednoznaczne dane w zależności od badanego roku. W tabeli 8 przedstawiono czołówkę 5 państw wg źródeł incydentów w przedziale czasowym 2017-2024 rok.

Tab. 8. Rozkładu źródeł ataków na sieci.

LP	2017	2018	2019	2020	2021	2022	2023	2024
1	CHINY (35%)	CHINY (22%)	ROSJA (22%)	ROSJA (22%)	ROSJA (25%)	USA (28%)	USA (25%)	USA (21%)
2	USA (17%)	USA (19%)	USA (13%)	USA (16%)	USA (15%)	ROSJA (18%)	ROSJA (18%)	POLSKA (9%)
3	POLSKA (15%)	ROSJA (13%)	NIDERLANDY (12%)	POLSKA (12%)	CHINY (7%)	CHINY (14%)	NIDERLANDY (13%)	FINLANDIA (8%)
4	ROSJA (7%)	POLSKA (12%)	POLSKA (10%)	CHINY (4%)	W. BRYTANIA (7%)	NIDERLANDY (7%)	BUŁGARIA (13%)	ROSJA (6%)
5	FRANCJA (5%)	W. BRYTANIA (9%)	CHINY (8%)	NIDERLANDY (4%)	NIDERLANDY (5%)	NIEMCY (7%)	CHINY (8%)	IZRAEL (5%)

Źródło: opracowanie własne na podstawie raportów rocznych CSIRT GOV.

Analiza danych statystycznych wyraźnie wskazuje, że istnieją trzy państwa, z których to cyklicznie dokonywane są ataki na rządowe systemy teleinformatyczne. Należą do nich Federacja Rosyjska, Chiny oraz Stany Zjednoczone Ameryki, przy czym w tabeli w nawiasach wpisano wartość procentową państwa w wszystkich atakach z danego roku. Zaskakujący jest fakt, że Stany Zjednoczone Ameryki jako główny sojusznik Polski znajdują się podium tego rankingu. Godnym omówienia jest również rola Polski w tabeli, ponieważ po 2020 roku znika ona z zestawienia i nieujęta jest nawet w rozszerzonej dziesiątce źródeł ataków aż do 2024 roku. Prawdopodobnej przyczyny takiego stanu rzeczy należy upatrywać w konsekwencjach pandemii COVID-19 gdzie wrogie podmioty skupiały się na innej działalności.

Należy jednak mieć na uwadze, że prezentowane dane nie są w 100% miarodajne, ponieważ do ich stworzenia użyto odmiennie zdefiniowanych wskaźników. O wiele większa wiarygodność prezentowanych danych byłaby w momencie, gdyby do ich skatalogowania użyto tej samej nomenklatury i jednakowych wartości klasyfikacyjnych. Rozwiązania przedmiotowej problematyki upatruje się w wejściu do polskiego porządku prawnego implementacji Dyrektywy NIS II, w postaci nowelizacji ustawy o KSC. Spowoduje to ujednolicenie we wszystkich państwach członkowskich Unii Europejskiej wskaźników definiujących parametry dla każdego zagrożenia lub podatności i dlatego posłużono się również danymi z instytucji ENISA.

Istotnym z punktu widzenia informacji jest również coroczny raport Threat Landscape[109] przygotowany przez Agencję UE ds. Cyberbezpieczeństwa (ENISA[110]) według którego w roku 2024 zdefiniowano prognozy ośmiu głównych zagrożeń wykorzystujących do realizacji cyberprzestrzeń z podziałem na kategorie takie jak:

Ransomware – przejęcie kontroli nad czyimiś danymi i żądanie okupu.

Komentarz – W 2024 r. ataki typu ransomware nadal były jednym z głównych cyberzagrożeń. Stają się coraz bardziej złożone. Według ankiety cytowanej przez ENISĘ przeprowadzonej pod koniec 2023 i w 2024 r. ponad połowa respondentów lub ich pracowników miała styczność z atakami ransomware. Z danych opracowanych przez agencję wynika, że średnia wartość okupu zapłaconego w atakach ransomware podwoiła się z 71 000 euro w 2019 do 150 000 euro w 2020 roku. Szacuje się, że w 2023 r. globalne szkody wywołane przez ataki tego typu osiągnęły wartość 18 miliardów euro, czyli 57 razy więcej niż w 2015 roku[111].

Malware – złośliwe oprogramowanie szkodzące systemowi.

Komentarz – złośliwe oprogramowanie (Malware) to m.in. wirusy, robaki, konie trojańskie i oprogramowanie szpiegujące. W 2020 i na początku 2021 r. liczba incydentów związanych ze złośliwym oprogramowaniem globalnie spadła z powodu

[109] ENISA Threat Landscape 2024 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 [dostęp: 02.05.2025].

[110] ENISA - Agencja Unii Europejskiej ds. Cyberbezpieczeństwa odpowiedzialna za zapewnienie wysokiego i efektywnego poziomu bezpieczeństwa w sieciach i systemach informatycznych w Unii Europejskiej. Utworzona 15 marca 2004 roku na mocy Rozporządzenia (WE) nr 460/2004 Parlamentu Europejskiego i Rady pod nazwą Europejska Agencja Bezpieczeństwa Sieci i Informacji (European Network and Information Security Agency) służy jako centrum doradztwa państwom członkowskim Unii Europejskiej w kwestiach związanych z szeroko rozumianym bezpieczeństwem w Internecie oraz przyczynia się do rozwoju społeczeństwa informacyjnego.

[111] https://www.europarl.europa.eu/news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia [dostęp: 07.11.2023].

pandemii COVID-19 jednak znacznie wzrosła pod koniec 2021 r. gdy ludzie zaczęli wracać do biur. Wzrost liczby incydentów związanych ze złośliwym oprogramowaniem przypisuje się również tzw. cryptojackingowi (potajemnemu wykorzystywaniu komputera ofiary do nielegalnego wydobywania krypto walut) oraz złośliwemu oprogramowaniu atakującemu tzw. Internet rzeczy czyli urządzenia podłączone do Internetu takie jak routery lub kamery. Według ENISA w samym pierwszym półroczu 2022 r. było więcej ataków na Internet rzeczy niż w poprzednich czterech latach[112].

Socjotechnika – wykorzystywanie błędu ludzkiego w celu uzyskania dostępu.

Komentarz – ataki wykorzystujące socjotechnikę to nakłanianie ofiar podstępem do otwierania złośliwych dokumentów, plików lub wiadomości e-mail, odwiedzania stron internetowych i udzielania w ten sposób nieautoryzowanego dostępu do systemów lub usług. Najczęstszym atakiem tego rodzaju jest Phishing (poprzez e-mail) lub Smishing (poprzez SMS-y). Według badań cytowanych przez ENISĘ prawie 60% naruszeń cyberbezpieczeństwa w Europie na Bliskim Wschodzie i w Afryce zawiera element socjotechniki. Główne organizacje, pod które podszywały się wrogie podmioty wykorzystujące Phishing, należały do sektora finansowego i technologicznego. Przestępcy coraz częściej atakują również giełdy i właścicieli krypto walut[113].

Zagrożenia danych – uzyskanie nieautoryzowanego dostępu do danych i ujawnienia ich.

Komentarz – żyjemy w gospodarce coraz bardziej opartej na danych tj. wytwarzamy ogromne ilości danych, które są niezwykle ważne m.in. dla przedsiębiorstw i sztucznej inteligencji co czyni je ważnym celem dla cyberprzestępców. Zagrożenia dla danych głównie dzieli się na naruszenia bezpieczeństwa danych (zamierzone ataki wrogiego podmiotu) oraz wycieki danych (niezamierzone ujawnienie danych). Najczęstszą motywacją takich ataków pozostają pieniądze. Tylko w 10% przypadków motywem było szpiegostwo.

Zagrożenia dostępności – uniemożliwianie użytkownikom dostępu do danych lub usług.

Komentarz – ataki typu DoS, DDoS są jednymi z najbardziej krytycznych zagrożeń dla systemów informatycznych. Ich zakres i złożoność są coraz większe. Jedną z powszechnych form ataku a zarazem techniką jest przeciążenie infrastruktury sieciowej i uniemożliwienie dostępu do systemu. Ataki typu „odmowa usługi" coraz częściej

[112] ENISA Threat Landscape 2022 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport [dostęp: 07.11.2023].

[113] ENISA Threat Landscape 2024 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 dostęp: 07.06.2025].

uderzają w sieci komórkowe i podłączone urządzenia. Są często używane w wojnie rosyjsko-ukraińskiej. Celem ataków były również strony internetowe związane z COVID-19 np. dotyczące szczepień[114].

Zagrożenia dla dostępności – zagrożenia dla dostępności Internetu.

Komentarz – Takie zagrożenia obejmują fizyczne przejmowanie i niszczenie infrastruktury internetowej co zaobserwowano na okupowanych terytoriach ukraińskich od czasu rosyjskiej inwazji a także aktywne cenzurowanie serwisów informacyjnych lub mediów społecznościowych[115]. Należy jednak zaznaczyć, że fizyczne niszczenie infrastruktury cyfrowej jest dość trudne, ponieważ większość serwerów, za pomocą których odbywa się ruch sieciowy jest strzeżona i przechowywana poza dostępem osób postronnych. Należy uwzględnić, że niszczenie fizyczne infrastruktury w przypadku usług sieciowych wymaga zaangażowania o wiele większych sił niż w przypadku przejęcia zdalnego, zablokowania lub szyfrowania ruchu sieciowego.

Dezinformacja – rozpowszechnianie mylnych informacji.

Komentarz – Dezinformacja jest bronią używaną od czasów starożytnych a jej archetypem jest koń trojański, który z pozoru nieszkodliwy w istocie niszczy tych, którzy go przyjmą. Należy przyjąć, że informacja to inaczej formowanie i urabianie świadomości, a jeśli dokonywana jest w złej wierze staje się dezinformacją, manipulacją służącą do tego, aby podstępem zmusić ludzi do działań, które przynoszą im szkodę i których sami z siebie by nie podjęli[116]. Wrogie podmioty wykorzystują dezinformację w połączeniu z rozwijającymi się technologiami, aby dotrzeć do jak najliczniejszej grupy społeczeństwa. Celem kampanii wymierzonych w obywateli jest sianie strachu i niepewności. Rosnące wykorzystanie mediów społecznościowych i mediów internetowych doprowadziło również do nasilenia kampanii rozpowszechniających Fakenews, czyli informacji wprowadzających w błąd oraz technologii Deepfake co oznacza, że możliwe jest teraz tworzenie fałszywych nagrań audio, wideo lub zdjęć, które są prawie nie do odróżnienia od prawdziwych. Boty udające prawdziwych ludzi mogą zakłócać działanie społeczności internetowych zalewając je fałszywymi komentarzami[117].

---

[114] Tamże.

[115] ENISA Threat Landscape 2024 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 dostęp: 07.06.2025].

[116] Vladimir Volkoff, *Krótka historia dezinformacji. Od konia trojańskiego do Internetu.* wydawnictwo

[117] ENISA Threat Landscape 2024 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 [dostęp: 02.06.2025].

Zagrożenia dla łańcucha dostaw – ataki na relacje między organizacjami a dostawcami. Komentarz – Organizacje stają się coraz bardziej podatne na takie ataki ze względu na coraz bardziej trudne do nadzorowania złożone systemy, których używają oraz rosnącą liczbę dostawców. Należy zwrócić uwagę, że w tym przypadku zagrożeniem jest „wrogi podmiot", który wykonuje atak na pewien specyficzny cel – łańcuchy dostaw. Jest to dość szerokie spektrum przyczynowe, ale głównym motorem indukującym te zagrożenie są działania wynikające z celowego wykorzystania pewnych technologii do złych zamiarów takich jak przerwanie ciągłości działania dostaw poprzez awarie serwerowni, wycieki danych, blokowanie dostępu lub szyfrowanie danych[118].

Prezentowane prognozy zagrożeń są wynikiem analizy tylko za lata 2022-2024 r. natomiast biorąc pod uwagę trendy rozwojowe z całą pewnością w następnych latach będą one tylko potęgowane poprzez dynamiczny rozwój technologii, oprogramowania i socjotechniki.

3.4. Badania nad zagrożeniami Systemu Bezpieczeństwa Narodowego.

W celu przeprowadzenia badań nad rodzajami zagrożeń czynność tą podzielono na dwa etapy. Pierwszy obejmował zdobycie wiedzy na temat świadomości sytuacyjnej zagrożeń cyberbezpieczeństwa głównych interesariuszy Systemu Bezpieczeństwa Narodowego. Drugi etap polegał na zebraniu informacji na temat zagrożeń bezpieczeństwa spośród wyspecjalizowanych instytucji zajmujących się wyłącznie cyberbezpieczeństwem. W toku realizacji pierwszego etapu sporządzono kwestionariusz wywiadu skierowany do 16 respondentów z dziedzin reprezentujących sektory bezpieczeństwa (Tabela 9). Kwestionariusz (załącznik nr. 1) składał się z 8 otwartych pytań, w których rzecznicy prasowi wybranych instytucji mieli wyrazić swoje opinie na temat zagrożeń oraz zidentyfikować zagrożenia występujące w sektorach, w których są zatrudnieni. W wyniku przeprowadzonego badania odpowiedzi na wywiad udzieliło tylko 4 instytucje z czego Agencja Wywiadu oraz Służba Kontrwywiadu Wojskowego odmówiły pisemnie udzielania wywiadu, ponieważ po wnikliwej analizie pytań zawartych w kwestionariuszu stwierdzono, że odpowiedzi mogłyby zaszkodzić bezpieczeństwu tychże instytucji.

[118] ENISA Threat Landscape 2024 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 [dostęp: 02.06.2025].

Tab. 9. Zestawienie odpowiedzi na wywiad ekspercki.

LP	SEKTOR BEZPIECZEŃSTWA PAŃSTWA	INSTYTUCJA DO KTÓREJ KIEROWANO WYWIAD	CZY UDZIELONO WYWIADU
1	DYPLOMATYCZNY	Ministerstwo Spraw Zagranicznych	TAK
2	MILITARNY	Dowództwo Operacyjne Rodzaju Sił Zbrojnych	NIE
3	WYWIADOWCZY	Agencja Wywiadu	NIE
4	KONTRWYWIADOWCZY	Służba Kontrwywiadu Wojskowego	NIE
5	PRAWA I PORZĄDKU PUBLICZNEGO	Komenda Główna Policji	NIE
6	RATOWNICTWA	Komenda Główna Państwowej Straży Pożarnej	NIE
7	KULTUROWY	Ministerstwo Kultury i Dziedzictwa Narodowego	NIE
8	EDUKACYJNY	Ministerstwo Edukacji i Nauki	NIE
9	SOCIALNY	Ministerstwo Rodziny i Polityki Społecznej	NIE
10	DEMOGRAFICZNY	Ministerstwo Rodziny i Polityki Społecznej	NIE
11	MIGRACYJNY	Urząd do Spraw Cudzoziemców	NIE
12	FINANSOWY	Ministerstwo Finansów	NIE
13	ENERGETYCZNY	Urząd Regulacji Energetyki	NIE
14	TRANSPORTOWY	Ministerstwo Infrastruktury	NIE
15	INFRASTRUKTURY KRYTYCZNEJ	Rządowe Centrum Bezpieczeństwa	NIE
16	ŚRODOWISKA NATURALNEGO	Ministerstwo Klimatu i Środowiska	TAK

Źródło: opracowanie własne na podstawie informacji zwrotnej.

Natomiast w wywiadach na które zdołano uzyskać odpowiedzi respondenci wspólnie, jako główną przyczynę możliwości realizacji zagrożeń wskazują następujące podatności:

- niski poziom wiedzy kadr wszystkich szczebli w zakresie cyberzagrożeń;
- brak szkoleń z zakresu cyberbezpieczeństwa;
- braki wykwalifikowanych pracowników z zakresu cyberbezpieczeństwa.

Ponadto zgodnie z kompetencjami respondenci wskazali jako główne źródła zagrożeń:

- *sektor dyplomatyczny (Ministerstwo Spraw Zagranicznych)* jako główne zagrożenia upatruje w częstym ujawnianiu informacji w przestrzeni Internetowej co świadczy o braku koordynacji działań i braku wiedzy dyplomatów na temat zagrożeń. Natomiast jako poprawę stanu obecnego wskazuje konieczność utworzenia sprawnych interdyscyplinarnych zespołów analitycznych wspierających instytucje państwowe w zakresie cyberbezpieczeństwa.
- *sektor środowiska naturalnego (Ministerstwo Klimatu i Środowiska)* wyraża obawy o podatności w systemach zdalnego sterowania wykorzystywanych w przemyśle. Materializacja zagrożeń w tego typu systemach może ewaluować w postaci zatrucia środowiska naturalnego (np. wyciek substancji toksycznych). Ponadto w cyberprzestrzeni kreowane są fałszywe informacje, które wprowadzają obywateli w błąd. Dotyczy to podszywania się pod instytucje zaufania

publicznego, które dostarczają obywatelom informacji nt. chociażby jakości powietrza czy wód.

W pozostałych 12 przypadkach rzecznicy prasowi odmawiali udzielenia wywiadu z następujących przyczyn:

- nie czuli się kompetentni do wypowiedzi na temat zagrożeń cyberbezpieczeństwa (*co jest nieuzasadnione, ponieważ Rzecznik Prasowy jest to funkcja, która zobowiązuje do odpowiadania na wszelkie pytania dotyczące instytucji a każda instytucja posiada specjalistów od bezpieczeństwa teleinformatycznego*).
- uważali, że specyfika działalności ich sektorów bezpieczeństwa jest wolna od zagrożeń cyberbezpieczeństwa (*co świadczy o niskiej a nawet zerowej świadomości sytuacyjnej zagrożeń w cyberprzestrzeni*).
- nieuzasadniony brak chęci współpracy (*co świadczy o niskich kompetencjach respondenta lub nonszalanckim podejściu do kreatora wywiadu*).

Podsumowanie zebranych w ramach ankietowania informacji (bez podziału pomiędzy respondentów) jest następujące:

1. Wskazane zagrożenia:
   a) zbyt częste ujawnianie informacji wrażliwych w przestrzeni Internetowej przez wysokich rangą przedstawicieli władz państwowych;
   b) chęci celowej ingerencji wrogich podmiotów w systemy infrastruktury krytycznej;
   c) działania dezinformacyjne.
2. Wskazane podatności:
   a) brak wiedzy kadr specjalistycznych;
   b) brak szkoleń dla kadr specjalistycznych;
   c) niska odporność społeczeństwa na dezinformacyjne.
3. Wskazane działania zabezpieczające:
   a) konieczność utworzenia sprawnych interdyscyplinarnych zespołów analitycznych wspierających instytucje państwowe w zakresie cyberbezpieczeństwa;
   b) walka z dezinformacją.

Analizując ilość braków odpowiedzi oraz ich przyczyny należy uznać tę sytuację jako słabość systemową, ponieważ wspólne dążenie do poprawy bezpieczeństwa powinno być

priorytetowym zadaniem wszystkich odpytywanych instytucji. W rzeczywistości brak zainteresowania niemalże doprowadzono do utraty ciągłości działania procesu naprawczego.

W toku realizacji drugiego etapu badań przeznaczonego dla wyspecjalizowanych w zakresie cyberbezpieczeństwa instytucji wywiad ekspercki skierowano do przedstawicieli takich instytucji jak:

1. Naukowa i Akademicka Sieć Komputerowa CSIRT NASK.
2. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV.
3. Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni CSIRT MON.

Kwestionariusz wywiadu (załącznik nr 1) składał się 8 pytań, które odnosiły się do rodzaju zagrożeń jakie wiążą się z cyberprzestrzenią. W tym miejscu należy wyjaśnić pewną zbieżność. Instytucje w których przeprowadzono wywiad są to podmioty, z których zbierano dane statystyczne natomiast zakres pytań w wywiadzie zawierał informację o krokach i czynnościach usprawniających oraz szczegółowych informacji na temat zagrożeń dla tych instytucji w zakresie cyberbezpieczeństwa. Niestety również w tym przypadku badania nie zostały zrealizowane do końca, ponieważ instytucje odmówiły udzielania odpowiedzi kierując się dbaniem o poufność danych. W związku z czym wyeksponowanie zagrożeń odbyło się z pominięciem informacji zbieranych na podstawie wywiadów eksperckich. Analiza całościowa badania pozwala jednoznacznie wskazać, że metoda badawcza polegająca na wywiadach w tym przypadku zawiodła co nie oznacza, że nie dostarczyła żadnych informacji a wręcz przeciwnie. Jest to słabość systemowa którą należy uwzględnić podczas tworzenia koncepcji poprawy bezpieczeństwa.

Reasumując szczegółowa analiza zarówno studium przypadków danych statystycznych jak również szczątkowych informacji z wywiadów pozwoliła na wyeksponowanie kluczowych kierunków zagrożeń, które w obecnych czasach wpływają na bezpieczeństwo kraju i mogą poważnie oddziaływać na informacyjną ciągłość działania państwa. Na tej podstawie utworzono tabelę zbioru sposobów realizacji zagrożeń (Tab. 10), która w połączeniu z analizą dokumentów zawartą w podrozdziale 3.2 prezentuje potencjalne spektrum materializacji zagrożeń.

Tab. 10. Zbiór sposobów realizacji zagrożeń wraz z analizą danych statystycznych.

	analiza danych statystycznych			sposoby realizacji zagrożeń - metody, techniki, narzędzia -			
LP	*najczęściej atakowane sektory*	*najczęściej atakowane cele*	*główne lokalizacje wrogich podmiotów*	*złośliwe oprogramowanie*	*cyber-przestępczość*	*dezinformacja*	*utrudniony dostęp do usług*
1	media	infrastruktura krytyczna	USA	Malware	oszustwa komputerowe	Fakenews	DoS, DDoS
2	energetyka	urzędy	Rosja	Backdoor	kradzieży danych	Deepfake	niszczenie infrastruktury cyfrowej
3	infrastruktura cyfrowa	ministerstwa	Chiny	Ransomware	obraźliwe treści	Propaganda	zagrożone łańcuchy dostaw
4	bankowość, handel, usługi pocztowe	służby, instytucje	Francja, Niemcy, Niderlandy, W. Brytania	Socjotechniki	-	-	-

Źródło: Opracowanie własne.

Prezentowane sposoby realizacji zagrożeń (w szczególności kierunki) są współbieżne z odpowiedziami jakie wyrazili respondenci podczas badań ankietowych. Dzieje się tak, ponieważ w obu przypadkach została wskazana dezinformacja oraz ingerencja w infrastrukturę cyfrową w związku z czym dążenie do wyeliminowania wad, luk, słabości w systemie SBN podatnych na tego typu sposoby realizacji zagrożeń są priorytetem.

Należy jednak wziąć pod uwagę, że obecny System Bezpieczeństwa Narodowego jest w stanie zneutralizować niektóre działania wrogich podmiotów. Dlatego należy dokonać analizy porównawczej zdolności obronnych systemu z opisanymi wcześniej sposobami działania wrogich podmiotów (przede wszystkim ataków wykorzystujących cyberprzestrzeń) aby otrzymać resztkowy zbiór wrogich działań na który obecny system nie jest przygotowany. Pozwoli to zbudować na tej podstawie koncepcję poprawy bezpieczeństwa państwa.

3.5. Odporność Systemu Bezpieczeństwa Narodowego na cyberzagrożenia

Z punktu widzenia cyberbezpieczeństwa w struktury Systemu Bezpieczeństwa Narodowego wchodzą nie tylko Krajowy System Cyberbezpieczeństwa, ale i również instytucje oraz podmioty branżowe takie jak np. CBZC, które w tym wypadku podlega pod Policję a nie należy do KSC. Mając to na uwadze zasadnym jest zbadanie czy istnieją w SBN podmioty, które posiadają zdolności obronne wobec opisanych sposobów

realizacji zagrożeń. Analiza systemowo-proceduralna przedstawiona w tym rozdziale pozwoli na identyfikację działań, na które obecny system nie jest przygotowany. W tym przypadku kryterium podziału na państwa źródła ataków, zostanie uznane jako drugorzędne. Oczywiście należy wziąć pod uwagę, że geolokalizacja wrogiego podmiotu jest istotna w przypadku skutecznego ścigania sprawców cyberprzestępstw. Kluczowe znaczenie ma tutaj informacja czy z takim krajem jest podpisana umowa o ekstradycję oraz czy państwo świadczy pomoc prawną itd. W końcu nie bez znaczenia jest również informacja o lokalizacji źródeł ataków z punktu widzenia polityki zagranicznej, ponieważ prowadzenie dialogu biznesowego z tym krajem będzie obarczone większym ryzykiem. Ponadto celem uproszczenia analizy podział ze względu na organizację oraz cel zostanie również uznany za drugorzędny. Należy przez to rozumieć, że mniejsze znaczenie będzie miało w tym przypadku czy obiektem ataku jest instytucja czy ministerstwo, branża energetyczna czy finansowa, ponieważ wpływa to na rozmiar skutków oraz wizerunek organizacji natomiast nie jest wyznacznikiem zdolności obronnych. Jako przeciwstawnym argumentem do powyższych założeń można posłużyć się tezą, która mówi, że *„cały system jest tak silny jak silne jest jego najsłabsze ogniwo”* wobec czego w toku przeprowadzonej komparacji zostaną wychwycone najsłabsze ogniwa. W związku z czym należy uznać, że celem analizy jest zweryfikowanie zdolności ochronnych Systemu Bezpieczeństwa Narodowego jako całości wobec zdefiniowanych dotychczas sposobów realizacji zagrożeń. Dodatkowo geolokalizacja źródła i cele ataków nie będą brane pod uwagę z jednoczesnym uznaniem kluczowej roli metod, technik oraz narzędzi wykorzystywanych do materializacji zagrożeń.

Cyberprzestępczość – (oszustwa komputerowe, kradzieże danych, obraźliwe treści) w skład których wchodzą szeroko pojęte działania mające na celu osiągnięcie korzyści przez wrogi podmiot. Działania te polegają na wyłudzeniach, kradzieży krypto walut i pieniędzy, kradzieże tożsamości cyfrowej lub szantaż za pośrednictwem sieci. Jest to specyficzna grupa przestępstw, która ukierunkowana jest w głównej mierze na osoby fizyczne rzadziej podmioty. Można więc zastosować tu podział ze względu na rozmiar przestępstwa, gdzie wyróżnia się pojedynczych oszustów, grupę oszustów i zorganizowane grupy przestępcze prowadzące działania na wielką skalę. Podstawowym organem zajmującym się zjawiskiem oszustw komputerowych są wyspecjalizowane komórki policji takie jak Centralne Biuro Antykorupcyjne, Centralne Biuro Zwalczania Cyberprzestępczości, Agencja Bezpieczeństwa Wewnętrznego. Organy policji rozsiane są w delegaturach w całym kraju, gdzie zazwyczaj są to placówki wojewódzkie.

Aby precyzyjnie stwierdzić czy prezentowane siły i środki są wystarczające do zagrożeń związanych z oszustwami komputerowymi należałoby dysponować szczegółowymi statystykami dotyczącymi ilością zgłoszonych incydentów w stosunku do zakończonych pozytywnie postępowań karnych. Niemniej jednak nie ulega wątpliwości, że w systemie bezpieczeństwa państwa istnieją organy odpowiedzialne i zdolne do przeciwstawienia się zagrożeniu jakim jest cyberprzestępczość.

Wnioski – jak pokazują dane statystyczne z zakresu cyberprzestępstwa oszustwa komputerowe są współcześnie plagą i wykazują trend rosnący w związku z czym współczesne zdolności systemu bezpieczeństwa państwa nie są wystarczające do przeciwstawienia się im. Wobec czego istnieje pewna słabość, którą trzeba poprawić, oddzielną kwestią jest również sytuacja kadrowa instytucji zwalczających ten rodzaj przestępstw.

Złośliwe oprogramowanie (Malware, Ransomware, Backdoor, Socjotechniki) – Malware i ransomware są to fragmenty kodu i programy wspomagające osiągnięcie celów przez wrogie podmioty je wykorzystujące. Pomocna w ich implementacji jest socjotechnika, którą często wrogie podmioty stosują w celu uzyskania dostępu do zasobów. Zatem dwa podstawowe elementy wykorzystywane do realizacji swoich celów to specjalnie spreparowane do tego oprogramowanie, czyli narzędzie, drugie to podatności będące błędami lub niedopatrzeniem twórców oprogramowania eksploatowanego przez atakowany obiekt. Dodatkowo istnieje możliwość stworzenia celowego nieuprawnionego dostępu do zasobów poprzez zaprojektowanie „Backdoor-a", czyli tylnej furtki w oprogramowaniu na etapie produkcji, o której wie tylko twórca oprogramowania. Są to bardzo groźne narzędzia, ponieważ konsekwencją ich użycia będzie wyciek i zaszyfrowanie danych celem okupu lub zablokowanie dostępu. Najlepszą formą zapobiegania jest położenie dużego nacisku na szkoleniu, informowaniu i nauczaniu o tzw. higienie cyfrowej. Postępowanie wg ściśle określonych norm i przestrzeganie zasad bezpieczeństwa pozwoli na uniknięcie zdecydowanej większości zagrożeń z tej grupy. Natomiast szkolenie nie może się ograniczać do wybranej grupy pracowników powinno ono obejmować całe społeczeństwo i aby mogło być realizowane należy utworzyć narodowy program nauczania wspomnianej już „higieny cyfrowej". Kolejnym sposobem na zwalczanie tego typu narzędzi jest dostarczanie i wdrażanie konstrukcji oraz oprogramowania sprawdzonego, przebadanego i z pominięciem nabycia od „dostawców wysokiego ryzyka".

Wnioski – współczesne zdolności systemu bezpieczeństwa państwa wskazują na słabość w konfrontacji ze zjawiskiem złośliwego oprogramowania, ponieważ zarówno podatności jak i nowotworzone narzędzia wrogich podmiotów wymagają specjalistycznej wiedzy do ich rozpoznania. Dodatkowo krajowe zdolności w dziedzinie tworzenia i wdrażania rozwiązań konstrukcyjnych i oprogramowania nie są na tyle rozbudowane, aby zaspokoić wszystkie potrzeby w administracji państwowej w tym infrastruktury krytycznej.

Dezinformacja (Fakenews, Deepfake, propaganda). Rozwój techniki w dobie mediów społecznościowych w znacznym stopniu ułatwia manipulację informacją, która celowana jest w społeczeństwo lub precyzyjnie wybrane grupy społeczne. O skuteczności dezinformacji świadczy fakt, że rządy wszystkich rozwiniętych państw dokładają starań, aby ją zwalczać, ponieważ na poważnie może zagrozić demokracji. Zjawisko takie jak „Fakenews[119]" trwale wpisało się w media społecznościowe oraz media klasyczne. Ponadto coraz częstszym zjawiskiem jest „Deepfake[120]", które przy pomocy stale rozwijającej się sztucznej inteligencji potrafi tworzyć realistyczne obrazy, które w realnym świecie nigdy nie miały miejsca. Szczególnym zagrożeniem z tej sfery jest propaganda, która tworzona jest w celu uwierzytelnienia szkodliwej narracji pokazując ją jako dobro. Podstawową i problematyczną kwestią jest zdefiniowanie co jest propagandą a co prawdą. Ponieważ to co dla jednego jest kłamstwem dla drugiego będzie prawdą. Niezależnie od strony, na którą patrzymy należy wskazać, że na szczeblu krajowym nie ma żadnej instytucji zajmującej się problematyką propagandy oraz walką z „Fakenews". Istnieją jedynie stowarzyszenia „Fact-hecking[121]" takie jak „Demagog[122]", które w swym statucie mają walkę z nieprawdziwymi informacjami wraz z weryfikowaniem ich. Ponieważ są to organizacje non-profit spektrum ich działań będzie uzależnione od kierunku ich

[119] Fakenews – nieprawdziwa lub częściowo nieprawdziwa wiadomość, często o charakterze sensacyjnym, publikowana w mediach z intencją wprowadzenia odbiorców w błąd w celu osiągnięcia korzyści finansowych, politycznych lub prestiżowych.

[120] Deepfake – technika obróbki obrazu, polegająca na łączeniu obrazów twarzy ludzkich przy użyciu technik sztucznej inteligencji.

[121] Fact-chacking – proces, który ma na celu zweryfikowanie informacji, polegający na dokładnym sprawdzaniu faktów w wiarygodnych źródłach, konfrontowania możliwie licznych potwierdzeń w opracowaniach lub dokumentach na piśmie lub w formie materiałów audio-wideo, a także w wypowiedziach autorytetów posiadających wiedzę i powszechnie uznaną wiarygodność w dziedzinie, której dotyczy weryfikowana informacja. Celem fact-checkingu jest promowanie prawdziwości i poprawności informacji.

[122] Stowarzyszenie Demagog – najstarsza w Polsce organizacja non-profit zajmująca się fact-checkingiem i walką z fałszywymi informacjami i dezinformacją.

finansowania. Mając na uwadze specyfikę zagrożenia należy stworzyć warunki do utworzenia przykładowo krajowej rady do spraw dezinformacji, która miałaby status instytucji mającej na celu obiektywne weryfikowanie i zapobieganie propagowaniu fałszywych informacji.

Wnioski – współczesne zdolności Systemu Bezpieczeństwa Narodowego wskazują na luki w walce z dezinformacją, propagandą jak i pokrewnymi zjawiskami. Istnieje uzasadniona konieczność zinstytucjonalizowania działalności antydezinformacyjnej natomiast aby to uczynić należy również wprowadzić odpowiednie regulacje prawne. Biorąc pod uwagę, że technologie Deepfake oraz Fakenews są wykorzystywane w działaniach hybrydowych poniżej progu wojny oraz w samym konflikcie zbrojnym to zdolności krajowe w tym zakresie stanowią obecnie tylko organizacje Fact-checkingowe. Niestety jest to zdecydowanie za mało, aby przeciwstawić się tego typu działaniom czego dowodem jest obecna sytuacja na granicy Polsko-Białoruskiej i wojna na Ukrainie.

Utrudniony dostęp do usług (DoS, DDoS, niszczenie infrastruktury cyfrowej, zagrożone łańcuchy dostaw). Celem tego typu ataku jest paraliż danej usługi tak aby żaden użytkownik nie mógł z niej skorzystać. Powody tych działań mogą być różne i mieć motywację religijną, polityczną, operacyjną sił zbrojnych lub praktyką stosowaną w celu obniżenia potencjału konkurencji. Należy wspomnieć, że w przypadku ataku DoS, DDoS istnieją specjalistyczne oprogramowania, które za pomocą algorytmów heurystycznych potrafią przewidzieć dynamicznie zwiększający się ruch sieciowy na serwerach i blokować go z odpowiednią przepustowością lub przekierowywać. Niemniej jednak są to rozwiązania, które są w toku badań i wymagają jeszcze udoskonalenia. W związku z czym jak dotąd w przypadku ataku DOS, DDOS najskuteczniejszą formą obrony jest odłączenie hosta od sieci. Kolejnym zagrożeniem w tej kategorii jest niszczenie fizyczne infrastruktury cyfrowej przy której następuje trwała utrata dostępu do usług. Zagrożona w tym przypadku jest również infrastruktura krytyczna, która jest ściśle powiązana z dostawami w takich gałęziach jak energetyka, petrochemie czy telekomunikacja. Zniszczenie lub blokowanie infrastruktury wpływa na zdolność świadczenia usług oraz wszelkich procesów logistycznych czego przykładem może być opisany na początku rozdziału incydent z „*Colonial Pipline*”. Blokowanie dostępu do usług jest zatem ściśle powiązane z szerokorozumianymi atakami na łańcuchy dostaw. W odpowiedzi na ten sposób realizacji zagrożenia dąży się do umieszczania infrastruktury cyfrowej w miejscach odseparowanych od osób nieupoważnionych.

Dodatkowo instytucje państwowe odpowiedzialne za cyberbezpieczeństwo stale monitorują cyberprzestrzeń w domenie infrastruktury krytycznej co znacznie zmniejsza prawdopodobieństwo mechanicznego uszkodzenia infrastruktury. Takie działania jednak nie zmniejszają ryzyka zdalnego dostępu i szyfrowania (w tym niszczenia) infrastruktury cyfrowej co obecnie jest dużym problemem. Należy uznać, że jeszcze bardziej problematyczne będzie utrzymanie infrastruktury cyfrowej w czasie konfliktu zbrojnego, ponieważ to właśnie infrastruktura krytyczna będzie celem wzmożonych ataków teleinformatycznych oraz działań kinetycznych takich jak rażenie taktycznymi rakietami lub ingerencja grup dywersyjnych czego przykładem jest obecny konflikt na Ukrainie.

Wnioski – współczesne zdolności systemu bezpieczeństwa państwa pomimo stałego monitoringu wskazują na brak odporności w konfrontacji z tego typu zagrożeniem zarówno w czasie pokoju jak i działań zbrojnych. Jedynym sposobem zachowania ciągłości dostępu do usług jest dążenie do nadmiarowości i alternatywnych systemów działania oraz zwiększenia zdolności operacyjnych instytucji odpowiedzialnych za monitorowanie infrastruktury cyfrowej w państwie.

3.6. Podsumowanie rozdziału

Przedstawione w rozdziale badania metodą „desk research", które obejmowały analizę studium przypadków, danych statystycznych, uzyskanych wywiadów eksperckich pozwoliły na zbudowanie pewnego obrazu zagrożeń i podatności dla Systemu Bezpieczeństwa Narodowego w ujęciu cyberbezpieczeństwa. Studium przypadków prezentuje skalę strat materialnych i niematerialnych w wymiarze całego państwa spowodowanych nieuprawnionym dostępem do zasobów informacyjnych przez wrogi podmiot. Analiza opisanych zdarzeń nakłania do refleksji na temat jak bardzo poważne skutki może nieść za sobą materializacja zagrożeń w cyberprzestrzeni. Pełnego wglądu w powagę tego rodzaju zagrożeń dostarczają dane statystyczne gromadzone przez krajowe instytucje odpowiedzialne za cyberbezpieczeństwo. Należy jednak zaznaczyć, iż pomimo sprecyzowanych wytycznych w dyrektywie NISII, to istnieje pewien brak zgodności pomiędzy kategoryzacją poszczególnych incydentów w danych statystycznych między instytucjami. W związku z czym oprócz istotności incydentów należałoby sprecyzować pewnego rodzaju ramy, które pozwoliłyby na jednolitą kategoryzację zdarzeń teleinformatycznych między instytucjami. Mowa tu przede wszystkim o jasno sprecyzowanych różnicach pomiędzy np. „atakiem na bezpieczeństwo informacji",

a „gromadzeniem informacji", które traktowane są przez CERT Polska jako oddzielne incydenty. Problematyczne jest również pozyskiwanie informacji formalną drogą, poprzez wywiady eksperckie o bieżącym stanie zagrożeń w poszczególnych sektorach działalności państwa. W chwili obecnej wszelkie instytucje niechętnie dzielą się informacjami a to z kolei utrudnia prowadzenie badań nad poprawą bezpieczeństwa co samo w sobie jest podatnością. Niemiej jednak z uzyskanych wywiadów można wywnioskować, że istnieje uzasadniona potrzeba podnoszenia świadomości na temat zagrożeń w cyberprzestrzeni dla kadry w administracji państwowej oraz pozostałej części społeczeństwa.

Przeprowadzona analiza wskazała zarówno źródła, metody, narzędzia i techniki oraz sposoby realizacji zagrożeń przez wrogie podmioty (celowe działania) jak również podatności występujące w Systemie Bezpieczeństwa Państwa. Należy mieć świadomość, iż obecny system posiada pewne zdolności obronne, przy czym dynamicznie zmieniające się środowisko zagrożeń w cyberprzestrzeni wymaga jego aktualizacji i zorientowania na nowe kierunki min. poprzez eliminację stwierdzonych podatności. Przedstawiona w rozdziale analiza pozwala wyeksponować i uporządkować opisane sposoby realizacji zagrożeń w sposób tabelaryczny (Tab. 11) tak aby można było rozpocząć pracę nad koncepcją poprawy bezpieczeństwa państwa.

Tab. 11. Zestawienie sposobów realizacji zagrożeń i obszarów oddziaływania.

SPOSOBY REALIZACJI ZAGROŻEŃ	INSTYTUCJE WIODĄCE W SBN	PODMIOTY WSPIERAJĄCE POZARZĄDOWE	KIERUNEK ZAGROŻEŃ	SYSTEMY BEZPIECZEŃSTWA PAŃSTWA	OBSZAR BEZPIECZEŃSTWA I ODDZIAŁYWANIA
Cyberprzestępczość	POLICJA, CBZC, CBA, ABW	-	wewnętrzne i zewnętrzne	SBN, KSC	cyberbezpieczeństwo, porządek publiczny
Złośliwe oprogramowanie	CSIRT MON, GOV, NASK	start-upy, prywatne podmioty	wewnętrzne i zewnętrzne	SBN, KSC, SOP	cyberbezpieczeństwo, społeczeństwo, bezpieczeństwo państwa
Dezinformacja	-	prywatne podmioty factcheckingowe	wewnętrzne i zewnętrzne	SBN, KSC, SOP	cyberbezpieczeństwo, społeczeństwo, bezpieczeństwo państwa, porządek publiczny
Utrudniony dostęp do usług	CSIRT MON, GOV, NASK	start-upy, prywatne podmioty	wewnętrzne i zewnętrzne	SBN, KSC, SZK, SOP	cyberbezpieczeństwo, społeczeństwo, bezpieczeństwo państwa

Źródło: Opracowanie własne.

W tabeli wyraźnie widać, że istnieje luka w postaci braku instytucji państwowej odpowiedzialnej za dezinformację. Brak jest również podmiotów prywatnych odpowiedzialnych za cyberprzestępczość, natomiast jest to wyłącznie domena organów państwowych. Oczywiście podchodząc do zagadnienia z biznesowego punktu widzenia jest to obszar do zagospodarowania, ponieważ przy obecnym poziomie oszustw komputerowych popyt na usługi odzyskiwania utraconego mienia jest stale rosnący[123]. W celu dokonania całościowego zestawienia czynników mających wpływ na materializację zagrożeń przedstawiono w sposób uporządkowany (Tab. 12) podatności stwierdzone w podrozdziale 3.2. Podatności te są konsekwencją stwierdzonych luk, wad i słabości, które zostały wyłonione na podstawie analizy dokumentów strategicznych, regulacji prawnych oraz projektu ustawy o nowelizacji Krajowego Systemu Cyberbezpieczeństwa.

Tab. 12. Zdiagnozowane podatności systemowe.

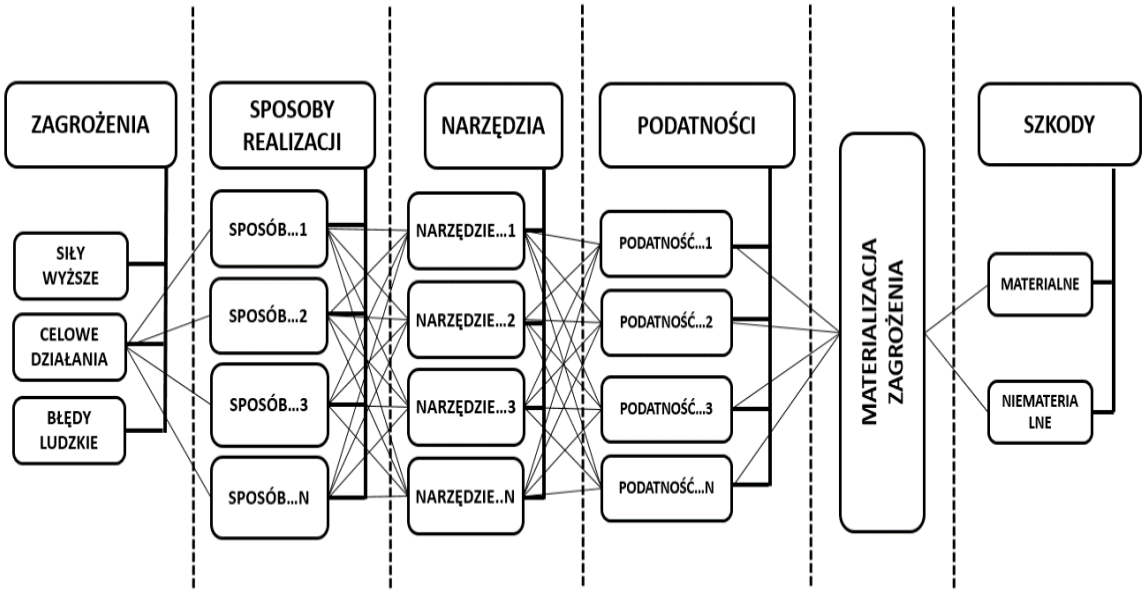
SŁABOŚCI SYSTEMOWE	WADY SYSTEMOWE	LUKI SYSTEMOWE
1. Niewystarczająca ilość i jakość regulacji prawnych dotyczących dezinformacji; 2. Niski poziom finansowania podmiotów odpowiedzialnych za cyberbezpieczeństwo; 3. Zwiększenie liczby instytucji odpowiedzialnych za walkę z oszustwami komputerowymi 4. Niski poziom współpracy miedzy podmiotami odpowiedzialnymi za cyberbezpieczeństwo; 5. Niskie zainteresowanie interesariuszy publicznymi konsultacjami nowelizacji ustawy o KSC	1. Wskazanie Operatora Strategicznej Sieci Bezpieczeństwa (OSSB) jako jedynego, w postaci jednoosobowej spółki; 2. Marginalne powiązanie Strategii Cyberbezpieczeństwa z krajowymi Strategiami; 3. Eksploatacja sprzętu teleinformatycznego producentów uznanych za „dostawców wysokiego ryzyka;	1. Brak właściwego do wagi zagadnienia wyeksponowania roli cyberbezpieczeństwa w Strategii Rozwoju Systemu Bezpieczeństwa Narodowego; 2. Brak regulacji prawnych dotyczących działalności ISAC 3. Brak satysfakcjonującego poziomu ukompletowania kadr odpowiedzialnych za cyberbezpieczeństwo w administracji państwowej. 4. Brak sprzężenia instytucji Centralnego Biura Zwalczania Cyberprzestępczości z Krajowym Systemem Cyberbezpieczeństwa; 5. Brak ustawowego kształcenia najmłodszych użytkowników Cyberprzestrzeni;

Źródło: Opracowanie własne.

Zdiagnozowane podatności mogą mieć różny charakter co zostanie szczegółowo skatalogowane w kolejnym rozdziale niemniej jednak są to elementy, których wyeliminowanie w znaczący sposób poprawi bezpieczeństwo całego systemu bezpieczeństwa państwa. Należy pamiętać, że aby zminimalizować ryzyko wystąpienia materializacji zagrożenia należy podjąć wysiłki w dwóch kierunkach, tj. prowadzić działania prewencyjne przeciw zagrożeniom (siły wyższe, błędy ludzkie, celowe działania) lub wyeliminować podatności co z punktu widzenia nakładów sił

[123] Istnieją biura detektywistyczne, które podejmują się zadań odzysku utraconego mienia z cyberprzestępstw, natomiast są to sporadyczne przypadki.

i środków oraz przewidywalności jest o wiele bardziej możliwe do zrealizowania. Na grafice (Rys. 25) przedstawiającej model graficzny przyczyn i skutków wyraźnie widać, że eliminacja podatności spowoduje ustanie ciągu zdarzeń prowadzących do materializacji zagrożeń.



Rys. 25. Model graficzny przyczyn i skutków materializacji zagrożeń.
Źródło: Opracowanie własne.

Wobec czego główny nacisk w tworzeniu koncepcji poprawy bezpieczeństwa państwa położony będzie na eliminację stwierdzonych podatności.

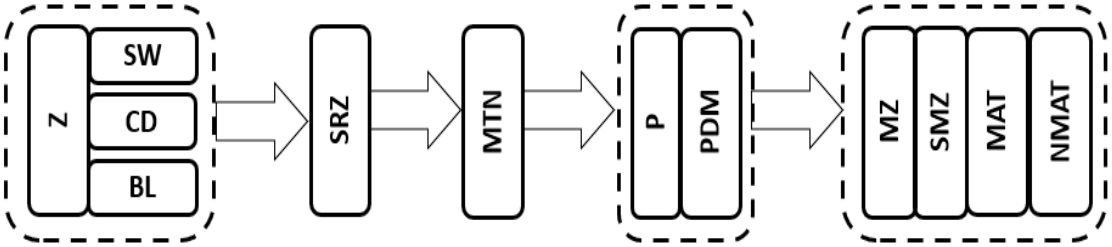
ROZDZIAŁ IV. ANALIZA RYZYKA W USPRAWNIANIU SYSTEMU BEZPIECZEŃSTWA NARODOWEGO

Analiza ryzyka wiąże się zawsze z podjęciem jakiejś decyzji. Natomiast decyzja ta nie zawsze ma charakter otwarty tzn. może wynikać z kontekstu działania. Należy przez to rozumieć, że zasadne jest przedstawienie w jakim celu realizowana jest analiza ryzyka i do czego potrzebne będą jej wyniki. Podczas tworzenia koncepcji poprawy bezpieczeństwa państwa analiza ryzyka (jako całościowy proces) ma dać odpowiedź na pytanie jakie będą oczekiwane straty przy założeniu, że nie zostaną podjęte żadne działania naprawcze. Dodatkowo analiza ryzyka powinna wspomóc w podjęciu decyzji o wyborze najlepszej jakości rozwiązań i to jest rzeczywisty powód przeprowadzania analizy ryzyka.

Na wstępie zostanie przedstawione jakie wskaźniki zostaną uzyskane i będę służyć do szacowanie ryzyka. W tym rozdziale zachodzi konieczność operowania długimi terminami bliskoznacznymi oraz mogącymi powodować niezrozumienie w interpretacji w związku z czym celem wykluczenia pomyłki zostaną one wyjaśnione wraz z podaniem ich skrótów oraz zależnościami między nimi. W nawiązaniu do grafiki nr 25 (podrozdział 3.6), aby nastąpiła materializacja zagrożenia musi nastąpić pewien ciąg przyczynowo skutkowy następujących po sobie elementów. Mając dane wejściowe takie jak: podatności, podmioty, zagrożenia, sposoby realizacji zagrożeń, metody, narzędzia i techniki wykorzystywane do realizacji zagrożeń oraz skutki materializacji zagrożeń to za pomocą graficznego modelu (Rys. 26) został przedstawiony schemat prezentujący jakie zależności zachodzą w tym procesie. Składowymi całego procesu będą przedstawione poniżej elementy takie jak:

- (Z) zagrożenia;
- (SW) siły wyższe;
- (CD) celowe działania;
- (BL) błędy ludzkie;
- (SRZ) sposoby realizacji zagrożenia;
- (MTN) metody, techniki, narzędzia;
- (P) podatności;
- (PDM) podmioty;
- (MZ) materializacja zagrożenia;
- (SMZ) skutki materializacji zagrożenia;

- (MAT) materialne;
- (NMAT) niematerialne.



Rys. 26. Schemat poglądowy: jakie zależności zachodzą podczas materializacji zagrożeń.
Źródło: opracowanie własne.

Zrozumienie prezentowanego ciągu zdarzeń pozwoli na wychwycenie jakiego rodzaju wskaźniki możemy uzyskać szacując ryzyko. Zostaną oszacowane takie wskaźniki jak:

- oczekiwane straty w przypadku braku podjęcia działań naprawczych, uzyskane w wyniku zestawienia podmiotów/systemów/obywateli z podatnościami;
- stopień narażenia podmiotu przez podatności, uzyskany w wyniku zestawienia podmiotów/systemów/obywateli z podatnościami;
- prawdopodobieństwo wystąpienia zagrożenia, uzyskane w wyniku zestawienia podatności z elementami materializacji zagrożenia;
- stopień wykorzystania podatności przez elementy materializacji zagrożeń, uzyskane w wyniku zestawienia podatności z elementami materializacji zagrożenia.

Prezentowane wskaźniki zaspokoją potrzebę oszacowania strat oraz wspomogą dalsze działania poprzez podjęcie decyzji o wyborze najlepszej jakości rozwiązań.

4.1. Istota zarządzania ryzykiem oraz jego miary

Zarządzanie ryzykiem to systematyczne stosowanie polityki, procedur i praktyki zarządzania do zadań ustalania kontekstu ryzyka jego identyfikowania, analizowania, wyznaczania, postepowania z ryzykiem oraz monitorowania i komunikowania ryzyka (definicja za PN-IEC 62198). Podstawowe elementy tego procesu można przedstawić w formie graficznej (Rys. 27).

Rys. 27. Podstawowe elementy zarządzania ryzykiem.
Źródło: Opracowanie własne na podstawie K. Liderman, Bezpieczeństwo informacyjne.

Zgodnie z ideą analiza ryzyka ma dać odpowiedź na pytanie jaki poziom istotności mają poszczególne zagrożenia i jaka jest możliwość ich materializacji przy założeniu określonego i niezmiennego w czasie oceny stanu środowiska. Aby uzyskać taką odpowiedź należy znać zbiór zagrożeń, sposoby ich realizacji i podatności umożliwiające konkretna realizację, możliwości (prawdopodobieństwa) tych realizacji oraz szkody wywołane przez te realizacje i szacunkowe straty, które wtedy powstają. W przedmiotowym problemie badawczym analiza pozwoli prognozować jakie szkody zostaną poniesione w przypadku pozostawienia stanu obecnego bez wprowadzania koncepcji poprawy bezpieczeństwa, przy czym oszacowanie rzeczywistych strat może okazać się niemożliwe. Kolejnym zastosowaniem ryzyka jest wykazanie czy i jak istotna poprawa odporności Systemu Bezpieczeństwa Narodowego nastąpi po wdrożeniu proponowanej koncepcji tzn. wartość ryzyka w tym przypadku można uznać za wskaźnik trafności (jakości) decyzji dotyczących modyfikacji SBN.

Zgodnie z grafiką (Rys. 27) podstawowym elementem identyfikacji jest ustalenie środowiska i zakresu analizy ryzyka co zostało w minimalnym stopniu uczynione w poprzednich rozdziałach. Ponieważ zagrożenia i podatności związane z SBN zostały już zidentyfikowane (patrz rozdz. 3.2 i rozdz. 3.3) to można przejść do szacowania ryzyka. Szacowanie ryzyka powinno być realizowane poprzez skonfrontowanie zagrożeń z podatnościami co w efekcie pozwoli na stworzenie mapy ryzyka. Z kolei mapa ryzyka

wymaga oszacowanej możliwości (wyrażonej prawdopodobieństwem lub oceną opisową) zajścia określonego zdarzenia i wartości szkód (strat) które wtedy wystąpią. Aby to uczynić należy przyjąć nieliczne, ale istotne kryteria porównawcze np.: w przypadku określania możliwości wystąpienia zagrożeń przyjmuje się zgodnie z literaturą[124], że podstawą do wyliczania stanowi informacja o częstości wystąpienia w przeszłości danego zagrożenia. Jeśli mowa o konsekwencjach materializacji zagrożeń, to rozpatruje je jako szkody oraz wynikające z nich straty. Jako szkody należy wziąć pod uwagę nie tylko straty materialne, ale także niematerialne, które mogą okazać się trudno policzalne. Do najczęściej branych pod uwagę szkód podczas szacowania ryzyka stosuje się straty:

- finansowe;
- fizyczne;
- czas potrzebny do przywrócenia stanu normalnego funkcjonowania;
- wizerunkowej organizacji (np. spadek liczby odbiorców usługi);
- życie i zdrowie ludzkie.

Mając na uwadze zależność pomiędzy szkodami a stratami można wywnioskować, że miarą ryzyka są oczekiwane straty.

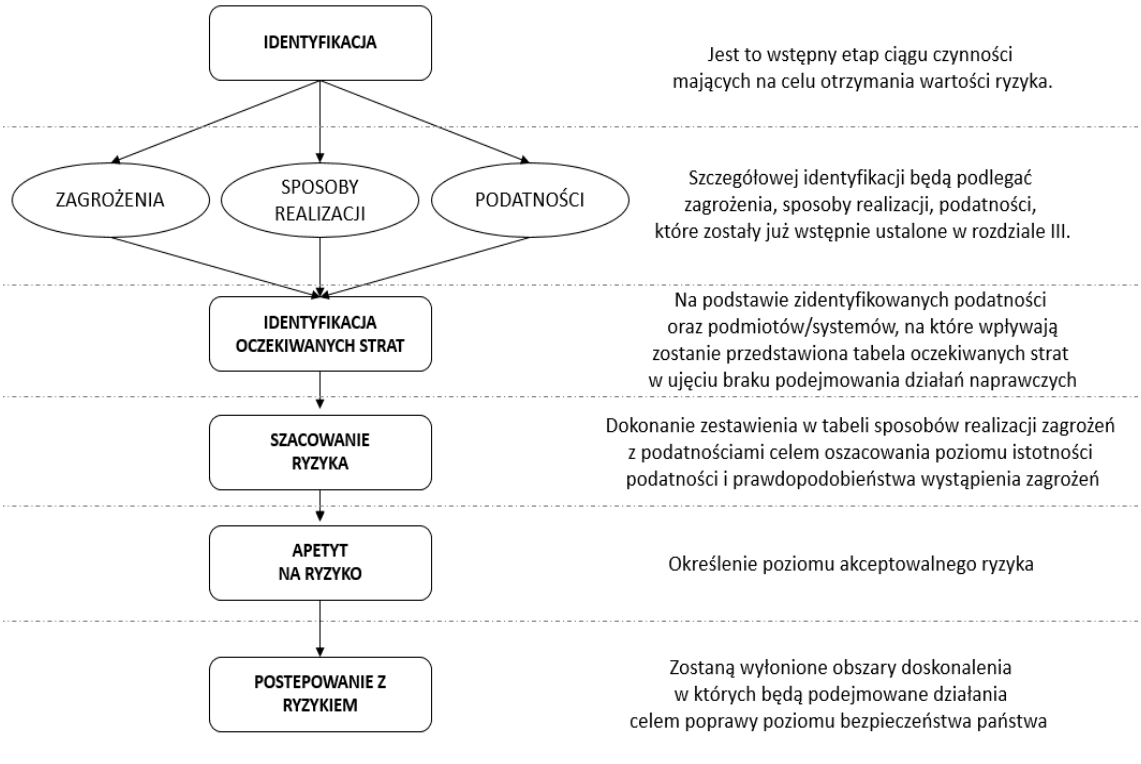
Nie jest możliwe wyeliminowanie wszystkich sposobów realizacji zagrożeń oraz nie wszystkie stwierdzone podatności muszą zostać zminimalizowane. Dzieje się tak, ponieważ ich szkodliwość stwierdzona w wyniku szacowania ryzyka może okazać się znikoma w stosunku do nakładów poniesionych na działania minimalizujące. Kolejnym problemem jaki się wyłania, jest precyzyjny dobór kryteriów porównawczych materializacji zagrożeń uwzględniających kontekst i okoliczności wystąpienia danego zagrożenia. Należy przez to rozumieć, że przy użyciu tych samych technik i narzędzi inne skutki będzie miał nieautoryzowany dostęp do systemu operacyjnego użytkownika domowego (osoby prywatnej) a inne skutki będą w przypadku przejęcia kontroli nad systemem sterowania w elektrowni. Wobec powyższego przyjęto na potrzeby analizy ryzyka kryteria incydentu, czyli zdarzenia, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo ustalone w ustawie o Krajowym Systemie Cyberbezpieczeństwa do których należą:

[124] PN-ISO/IEC 27005/2010 Technika informatyczna. Techniki bezpieczeństwa. Zarządzanie ryzykiem w bezpieczeństwie informacji.

- incydent krytyczny. Incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT;
- incydent poważny. Incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej,
- incydent istotny. Incydent, który ma istotny wpływ na świadczenie usługi cyfrowej.

Przedstawione poziomy incydentów będą wykorzystane jako wskaźniki służące do nadawania priorytetów podczas tworzenia koncepcji poprawy stanu obecnego.

W celu uporządkowania procesu zarządzania ryzykiem przedstawiono schemat postępowania (Rys. 28) wraz z komentarzem na poziomie ogólności według którego w rozdziałach V i VI, zostanie dokonany logiczny ciąg przyczynowo skutkowy dalszych działań. W schemacie blokowym postepowania wprowadzono dodatkowy element jakim jest apetyt na ryzyko.



Rys. 28. Schemat blokowy metody postępowania.
Źródło: Opracowanie własne.

Termin ten jest przedmiotem sporów w naukach o zarządzaniu i jest obszernie definiowany natomiast skutkiem tych definicji jest wielkość ryzyka (lub jego poziom),

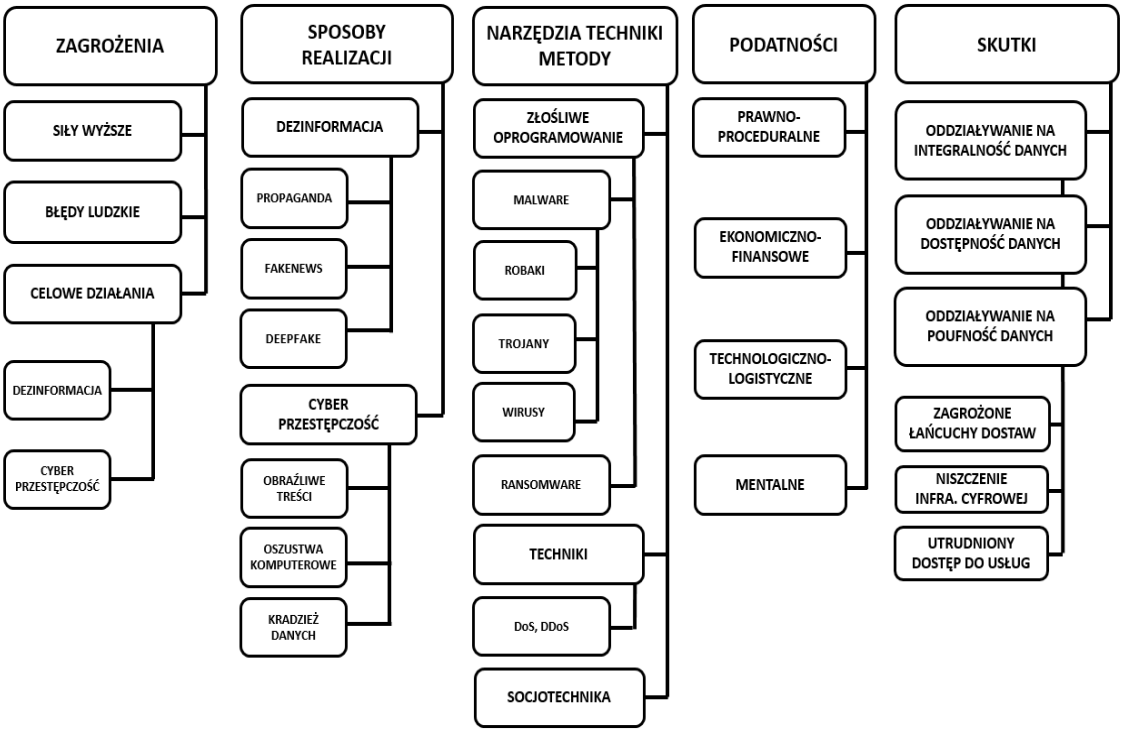
którą organizacja akceptuje[125]. Zatem czynności wykonane na tym etapie pozwolą zdefiniować ryzyko, które państwo polskie z punktu widzenia bezpieczeństwa jest gotowe podjąć w trakcie realizacji swoich celów.

4.2. Identyfikacja zagrożeń i podatności

Przedstawione w rozdziale III zagrożenia, sposoby realizacji, metody, techniki i narzędzia wykorzystywane do realizacji zagrożeń należy uporządkować w kategorie zgodne z ich znaczeniem np.:

- złośliwe oprogramowanie jest to narzędzie (do realizacji zagrożeń);
- cyberprzestępczość jest to zagrożenie (celowe działanie ludzi);
- dezinformacja to sposób realizacji zagrożenia (celowe działanie ludzi);
- utrudniony dostęp do usług jest to skutek realizacji zagrożenia.

Końcowa postać elementów składających się na ryzyko zdiagnozowanych w rozdziale III przybierze postać zgodną z schematem (Rys. 29). Należy zaznaczyć, że prezentowane elementy nie są wszystkimi możliwymi klasyfikacjami mogącymi wystąpić w toku materializacji zagrożeń.



Rys. 29. Kategoryzacja zagrożeń, sposobów, metod, technik, narzędzi.
Źródło: opracowanie własne na podstawie danych z rozdziału III.

[125] Korombel A., Apetyt na ryzyko - próba uporządkowania terminologii, Towarzystwo Naukowe Organizacji i Kierownictwa (TNOiK), Przegląd Organizacji, Nr 4 (927), 2017, s. 47-53.

Na schemacie zaprezentowano ułożone w sposób logiczny zdiagnozowane w rozdziale III elementy otrzymane na podstawie danych statystycznych raportów CSIRT NASK, CSIRT GOV oraz uzyskanych odpowiedzi na wywiady w tym wywiady eksperckie. Podobnie rzecz wygląda z podatnościami zidentyfikowanymi na etapie analizy dokumentacji, które w głównej mierze mają podłoże prawno-proceduralne, ekonomiczno-finansowe, technologiczno-logistyczne oraz mentalne.

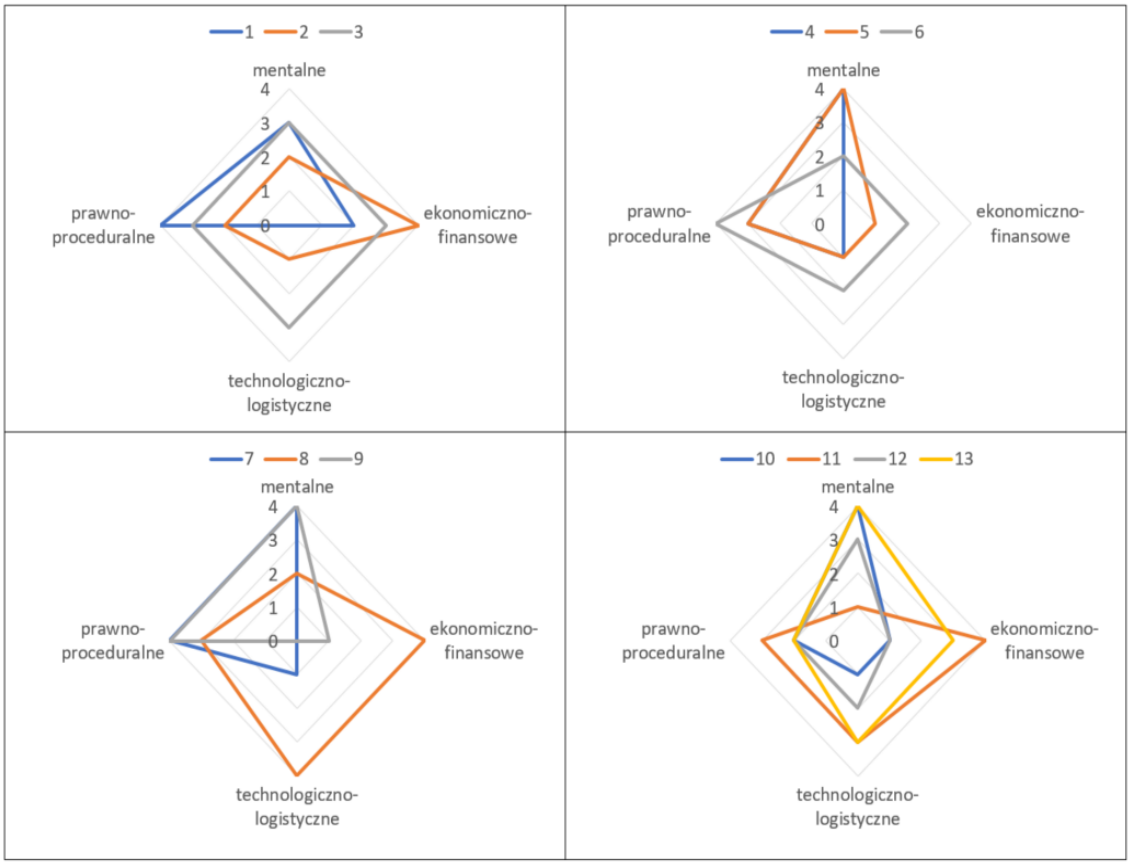
Tab. 13. Konkretyzacja podatności.

<table>
<tr><th>OBSZAR / PODATNOŚĆ</th><th>prawno-proceduralne</th><th>ekonomiczno-finansowe</th><th>technologiczno-logistyczne</th><th>mentalne</th></tr>
<tr><td>słabości systemowe</td><td>Niewystarczająca ilość i jakość regulacji prawnych dotyczących dezinformacji; 1</td><td>Niski poziom finansowania podmiotów odpowiedzialnych za cyberbezpieczeństwo; 2</td><td>Zbyt mała zdolność operacyjnych instytucji odpowiedzialnych za walkę z oszustwami komputerowymi 3</td><td>Niskie zainteresowanie interesariuszy publicznymi konsultacjami nowelizacji ustawy o KSC 4
Niski poziom współpracy miedzy podmiotami odpowiedzialnymi za cyberbezpieczeństwo; 5</td></tr>
<tr><td>wady systemowe</td><td>Wskazanie Operatora Strategicznej Sieci Bezpieczeństwa (OSSB) jako jedynego, w postaci jednoosobowej spółki; 6
Marginalne powiązanie Strategii Cyberbezpieczeństwa z krajowymi Strategiami; 7</td><td>.</td><td>Eksploatacja sprzętu teleinformatycznego producentów uznanych za „dostawców wysokiego ryzyka; 8</td><td></td></tr>
<tr><td>luki systemowe</td><td>Brak właściwego do wagi zagadnienia wyeksponowania roli cyberbezpieczeństwa w Strategii Rozwoju Systemu Bezpieczeństwa Narodowego; 9
Brak regulacji prawnych dotyczących działalności ISAC 10</td><td>Brak satysfakcjonującego poziomu ukompletowania kadr odpowiedzialnych za cyberbezpieczeństwo w administracji państwowej. 11</td><td>Brak sprzężenia instytucji Centralnego Biura Zwalczania Cyberprzestępczości z Krajowym Systemem Cyberbezpieczeństwa; 12</td><td>Brak ustawowego kształcenia najmłodszych użytkowników Cyberprzestrzeni w zakresie higieny cyfrowej. 13</td></tr>
</table>

Źródło: opracowanie własne na podstawie analizy dokumentów zawartej w rozdziale III.

Dokonana w ten sposób konkretyzacja (Tab. 13) pozwala na logiczne poukładanie podatności poprzez przypisanie ich do głównego źródła przyczynowego. W tabeli również poszczególne podatności oznaczono numerami (w kwadratach na dole po prawej stronie) tak aby wykorzystać numerację w dalszych analizach. Należy jednak zaznaczyć, że szczegółowo rzecz ujmując prezentowane podatności nie mają tylko jednego źródła pochodzenia, z którego wynikają. W większości są to splątane ze sobą przyczyny, wobec czego celem zobrazowania całościowego podejścia do źródeł ich powstania dokonano przedstawienia ich za pomocą modelu romboidalnego. Do realizacji modelu romboidalnego (Rys. 30) użyto następującej wartości skali:

- brak powiązania (0), należy rozumieć jako brak punktu powiązania podatności z obszarem przyczynowym;
- lekkie powiązanie (1), należy rozumieć jako niewielkie (brzegowe) powiązanie podatności z obszarem przyczynowym;
- średnie powiazanie (2), należy rozumieć jako połowiczne powiązanie podatności z obszarem przyczynowym;
- mocne powiązanie (3), należy rozumieć jako przeważające powiązanie podatności z obszarem przyczynowym;
- bardzo mocne powiązanie (4), należy rozumieć jako całkowite powiązanie podatności z obszarem przyczynowym;



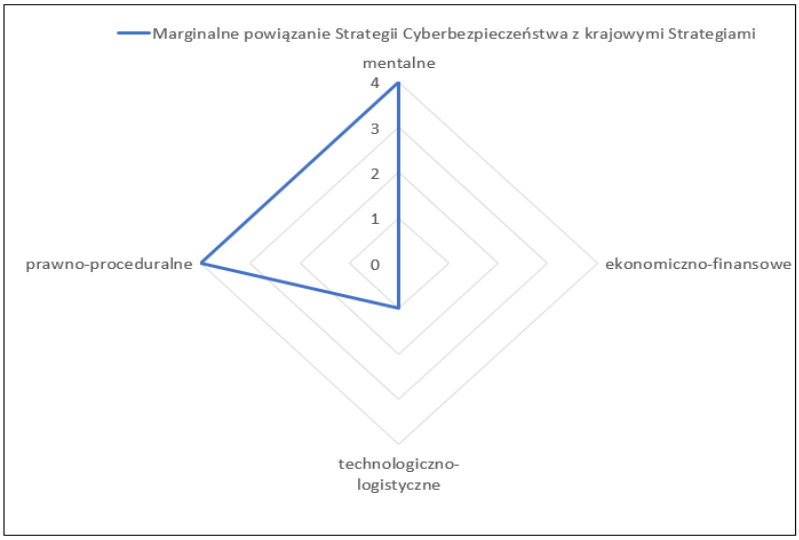
Rys. 30. Modele romboidalne płaszczyzn przyczynowych podatności.
Źródło: opracowanie własne na podstawie Tab. 13.

- PRZYKŁAD -

Zaprezentowano schemat odczytu wartości zapisanych w modelu i jako przykład posłużono się podatnością nr 7 (Tab. 13), która dotyczy „Marginalne powiązanie Strategii Cyberbezpieczeństwa z krajowymi Strategiami". Zgodnie z diagramem oraz wartością skali ustalono, że poziom zależności tej podatności od przyczyn jest następujący:

- prawno-proceduralne (4), całkowite powiązanie;
- technologiczno-logistyczne (1), niewielkie powiązanie;
- ekonomiczno-finansowe (0), brak powiązania;
- mentalne (4), całkowite powiązanie.

Przy pomocy tej metody zrealizowano zestawienie modelu romboidalnego z rysunku 30, natomiast postać graficzna z pojedynczą podatnością nr 7 będzie wyglądała następująco:



Rys. 31. Model romboidalne płaszczyzn przyczynowych podatności nr. 7.
Źródło: opracowanie własne.

- KONIEC PRZYKŁADU -

Przedstawienie na modelu romboidalnym (Rys. 30) zidentyfikowanych podatności będzie uwzględnione przy tworzeniu koncepcji poprawy bezpieczeństwa w kolejnym rozdziale.

4.3. Wskazanie oczekiwanych strat

Wstępną częścią szacowania ryzyka jest analiza oczekiwanych strat przy założeniu, że nie zostaną podjęte żadne przedsięwzięcia naprawcze stanu obecnego. W tym celu dla każdej z wyłonionych podatności zostanie przeprowadzona prognoza ewentualnych skutków i następstw w przypadku braku ich usunięcia. Na potrzeby analizy użyty zostanie model Systemu Bezpieczeństwa Narodowego (Rys. 14, rozdział 1.6), który przedstawia zależności i hierarchię pomiędzy systemami bezpieczeństwa państwa oraz podmiotami. Do realizacji analizy oczekiwanych strat została stworzona trójstopniowa skala, która pokazuje trzy poziomy istotności podatności:

- niski (1) oddziałuje na znikomym poziomie. W praktyce oznacza, że dana podatność nie wpływa na działalność podmiotu/systemu/obywateli w sposób zakłócający normalne funkcjonowanie w konsekwencji nieusunięcia podatności, istnieje prawdopodobieństwo wystąpienia incydentu istotnego;
- średni (2) oddziałuje na średnim poziomie. W praktyce oznacza, że dana podatność wpływa na działalność podmiotu/systemu/obywateli w sposób mogący zakłócać normalne funkcjonowanie w konsekwencji nieusunięcia podatności, istnieje prawdopodobieństwo wystąpienia incydentu poważnego;
- wysoki (3) oddziałuje na wysokim poziomie. W praktyce oznacza, że dana podatność ma potencjał paraliżujący na podmiot/system/obywateli i zakłóca normalne funkcjonowanie w konsekwencji nieusunięcia podatności, istnieje prawdopodobieństwo wystąpienia incydentu krytycznego.

Dodatkowo w wyniku zestawienia podatności z podmiotami/systemami/obywatelami można przeanalizować stopnień narażenia podmiotu na wszystkie stwierdzone podatności i w tym celu utworzono trójstopniową skalę zgodnie z:

- niskie (1), narażenie podmiotu/systemu/obywateli dla wszystkich podatności zostało uznane jako niskie;
- średnie (2), narażenie podmiotu/systemu/obywateli dla wszystkich podatności zostało uznane jako średnie;
- wysokie (3), narażenie podmiotu/systemu/obywateli dla wszystkich podatności zostało uznane jako wysokie.

Należy zaznaczyć, że analiza skutków nieusunięcia podatności jest bardzo problematyczna. Dzieje się tak, ponieważ trudno jest przewidzieć przy pomocy jakiego sposobu realizacji nastąpi materializacja zagrożeń, jaki byt[126] (podmiot, system lub obywatel) będzie celem ataku lub jakie konsekwencje będzie miało błędnie skonstruowane prawo. Z tego też powodu w analizie (Tab. 14) zakładany jest wariant uwzględniający najpoważniejsze skutki jakie mogą wystąpić dla danej podatności. Dalej została przedstawiona szczegółowa analiza zawartości, której wyniki są podstawą do wprowadzenia odpowiednich miar w pola tabeli. Przy czym należy zaznaczyć, że analiza jest subiektywna, ale wsparta wynikami wywiadów i danych statystycznych zawartych w rozdziale III, które można uznać za element obiektywny.

[126] Celowo ustawiono w jednym szeregu podmioty, systemy i obywateli, ponieważ wszystkie te „byty" posiadają podatności, które mogą być wykorzystane do materializacji zagrożenia.

Tab. 14. Tabela oczekiwanych strat.

LP.	PODMIOTY I SYSTEMY / PODATNOŚCI	SYSTEMY BEZPIECZEŃSTWA PAŃSTWA				ZASOBY NEWRALGICZNE WYMAGAJĄCE OCHRONY					SUMA
		SYSTEM BEZPIECZEŃSTWA NARODOWEGO	KRAJOWY SYSTEM CYBERBEZ.	SYSTEM ZARZĄDZANIA KRYZYSOWEGO	SYSTEM OBRONY PAŃSTWA	SEKTORY BEZPIECZEŃSTWA PAŃSTWA	PODMIOTY (WAŻNE, KLUCZOWE)	ZASOBY INFORMACYJNE	PODATNOŚCI (INNE)	OBYWATELE	
1	Niewystarczająca ilość i jakość regulacji prawnych dotyczących dezinformacji	3	3	3	3	3	2	2	1	3	23
2	Niski poziom finansowania podmiotów odpowiedzialnych za cyberbezpieczeństwo	3	3	3	3	3	3	3	3	3	27
3	Zbyt mała zdolność operacyjnych instytucji odpowiedzialnych za walkę z oszustwami komputerowymi	3	3	2	2	3	3	3	3	3	25
4	Niskie zainteresowanie interesariuszy publicznymi konsultacjami nowelizacji ustawy o KSC	2	3	1	1	3	2	2	2	1	17
5	Niski poziom współpracy miedzy podmiotami odpowiedzialnymi za cyberbezpieczeństwo	2	3	3	3	2	2	3	3	1	22
6	Wskazanie Operatora Strategicznej Sieci Bezpieczeństwa (OSSB) jako jedynego	2	2	2	2	2	2	2	1	1	16
7	Marginalne powiązanie Strategii Cyberbezpieczeństwa z krajowymi Strategiami	2	2	2	2	2	2	2	1	1	16
8	Eksploatacja sprzętu teleinformatycznego producentów uznanych za „dostawców wysokiego ryzyka	2	2	3	3	2	2	3	3	1	21
9	Brak właściwego do wagi zagadnienia wyeksponowania roli cyberbezpieczeństwa w Strategii RSBN	3	3	3	3	2	2	3	2	1	22
10	Brak regulacji prawnych dotyczących działalności ISAC	2	3	3	2	2	2	3	2	1	20
11	Brak satysfakcjonującego poziomu ukompletowania kadr w administracji państwowej	3	3	3	3	3	3	3	3	3	27
12	Brak sprzężenia instytucji CBZC z Krajowym Systemem Cyberbezpieczeństwa	1	2	1	1	2	2	2	2	2	15
13	Brak ustawowego kształcenia najmłodszych użytkowników Cyberprzestrzeni	1	1	1	1	1	1	2	3	3	14
SUMA		29	33	30	29	30	28	33	29	24	

Źródło: opracowanie własne na podstawie Tab. 13.

Dokonanie zestawienia podatności z podmiotami/systemami/obywatelami (patrz Tab. 14) w efekcie pozwoliło na zobrazowanie strat przy założeniu, że nie będą wprowadzone żadne działania naprawcze. Natomiast jak najszybsze usunięcie lub zminimalizowanie omawianych podatności wpłynie pozytywnie na następujące elementy takie jak:

- zmniejszenia kosztów poniesionych strat;
- podniesienia świadomości społecznej;
- zmniejszenia liczby użytkowników podatnych na zagrożenia;
- zbudowaniu mocniejszego potencjału obronnego;
- indukowanie do rozwoju w dziedzinie cyberbezpieczeństwa;
- powstrzymania migracji kadr do sektora prywatnego;
- zbudowania solidnego prawa;
- podniesienia wydatków publicznych na cyberbezpieczeństwo.

Przeprowadzona analiza pozwoliła wyeksponować, że niskie straty będzie miała tylko podatność „brak ustawowego kształcenia najmłodszych użytkowników cyberprzestrzeni”

natomiast największy stopień narażenia podmiotów przez podatności będą występowało w przypadku podmiotów:

- Krajowego Systemu Cyberbezpieczeństwa;
- zasobów informacyjnych.

Należy pamiętać, że kluczowe znaczenie ma również czas, ponieważ każde działania usprawniające, które jak najszybciej zostaną wprowadzone poprzez koncepcję poprawy bezpieczeństwa będą przyczyniały się do minimalizacji użycia sił i środków w przyszłości.

Tab. 15. Tabela prognozowanych szkód oraz stopień narażenia podmiotów.

OCZEKIWANE STRATY	WYNIK	PODATNOŚCI
NISKIE	9 - 14	• Brak ustawowego kształcenia najmłodszych użytkowników Cyberprzestrzeni
ŚREDNIE	15 - 20	• Niskie zainteresowanie interesariuszy publicznymi konsultacjami nowelizacji ustawy o KSC • Wskazanie operatora strategicznej sieci bezpieczeństwa (OSSB) w postaci jednoosobowej spółki • Marginalne powiązanie rangi cyberbezpieczeństwa w krajowych Strategiach • Brak regulacji prawnych dotyczących działalności ISAC • Zwiększenie instytucji odpowiedzialnych za walkę z oszustwami komputerowymi i sprzężenie z KSC
WYSOKIE	21 - 27	• Niewystarczająca ilość i jakość regulacji prawnych dotyczących dezinformacji • Niski poziom finansowania podmiotów odpowiedzialnych za cyberbezpieczeństwo • Zbyt mała zdolność operacyjnych instytucji odpowiedzialnych za walkę z oszustwami komputerowymi • Niski poziom świadomości o zagrożeniach w cyberprzestrzeni personelu w administracji państwowej • Eksploatacja sprzętu teleinformatycznego producentów uznanych za dostawców wysokiego ryzyka • Brak właściwego do wagi zagadnienia wyeksponowania roli cyberbezpieczeństwa w Strategii RSBN • Brak satysfakcjonującego poziomu ukompletowania kadr w administracji państwowej

STOPIEŃ NARAŻENIA PODMIOTU PRZEZ PODATNOŚCI	WYNIK	PODMIOTY
NISKI	13 - 21	
ŚREDNI	22 - 30	• System Bezpieczeństwa Narodowego • System Zarządzania Kryzysowego • System Obrony Państwa • Sektory Bezpieczeństwa Państwa • Podmioty (ważne, kluczowe) • Podatności (inne) • Obywatele
WYSOKI	31 - 39	• Krajowy System Cyberbezpieczeństwa • Zasoby Informacyjne

Źródło: opracowanie własne na podstawie Tab. 14.

Szczegółowa analiza zawartości tabeli 14 i 15.

„Niewystarczająca ilość i jakość regulacji prawnych dotyczących dezinformacji”

Dezinformacja jest zjawiskiem, któremu sprzyja rozwój technologii cyfrowych zwłaszcza „Social-mediów”. Biorąc pod uwagę jak bardzo społeczeństwo jest obyte technologiczne z cyfryzacją to zjawisko dezinformacji będzie tylko się potęgować. Z punktu widzenia statystyki przeciętny obywatel nie czyta już gazet czy nie ogląda telewizji a źródłem wiedzy dla niego jest Internet oraz media społecznościowe w których informacje są w niewielkim stopniu kontrolowane. Brak konkretnych

rozwiązań mających na celu kontrolę dezinformacji niesie za sobą poważne konsekwencje społeczne. Kraje wschodnie (min. Rosja, Białoruś) utrzymują wyspecjalizowane organizacje np. APT 28, APT 29 zajmujące się tworzeniem dedykowanych tzn. mających na celu trafienia w konkretną grupę społeczną kampanii dezinformacyjnych przeciwko państwu polskiemu. Natomiast w kraju nie istnieje żadna oficjalna i celowa instytucja odpowiedzialna za walkę z dezinformacją i zjawiskami pokrewnymi. W związku z czym, w wyniku nasilenia omawianych kampanii przeciw państwu polskiemu zagrożony może być porządek publiczny poprzez podsycanie wszelkiego rodzaju zamieszek, strajków, buntu itp.

Należy zauważyć, że dezinformacja często jest potęgowana w chwilach niepewności, kiedy w państwie zaistnieją wydarzenia wymuszające uruchomienie któregoś z systemów bezpieczeństwa państwa. Ponadto dezinformacja najbardziej destrukcyjnie oddziałuje na obywateli. Na podstawie powyższej argumentacji oraz wyników ankietowania zamieszczonego w załączniku przyjmuje się, że istotność podatności jest na poziomie średnim.

„*Niski poziom finansowania podmiotów odpowiedzialnych za cyberbezpieczeństwo”*

Zagrożenia wykorzystujące cyberprzestrzeń będą systematycznie ewoluowały a co za tym idzie nakłady finansowe na cyberbezpieczeństwo również muszą się rozwijać w odpowiednim tempie. Oczywiście należy tu wyjaśnić, że nie ma górnej kwoty, która byłaby wystarczająca do inwestowania w bezpieczeństwo. Jednak należy dążyć do uzyskania poziomu zaspokojenia potrzeb wynikających z rozbudowy Krajowego Systemu Cyberbezpieczeństwa, prowadzenia badań w tym kierunku oraz utrzymania szkolnictwa, celem poprawy świadomości społeczeństwa. Ponadto nie bez znaczenia jest problem pozyskiwania wyspecjalizowanych kadr w administracji państwowej co jest ściśle powiązane z wysokością zarobków. Brak należytego wynagradzania pracowników będzie skutkował przejściem ich do sektora prywatnego co przełoży się na jakość bezpieczeństwa państwa. Dodatkowo niedofinansowanie instytucji wpłynie na brak rozwoju a to z kolei przejawia się zacofaniem wobec postępującego otoczenia.

Niski poziom finansowania cyberbezpieczeństwa zatem będzie miało kluczowe znaczenie we wszystkich sferach funkcjonowania zarówno państwa jak i systemów podmiotów i obywateli. Na podstawie powyższej argumentacji oraz wyników ankietowania zamieszczonego w załączniku przyjmuje się, że istotność podatności jest na poziomie wysokim.

„Zbyt mała zdolność operacyjna instytucji odpowiedzialnych za walkę z oszustwami komputerowymi”

Zgodnie z statystykami oszustwa komputerowe są plagą współczesnych czasów. Brak zwiększenia zdolności operacyjnych instytucji odpowiedzialnych za walkę z cyberprzestępczością będzie skutkowało poważnymi stratami z budżetu państwa a to z kolei będzie wpływało na zmniejszenie dostępnych środków na finansowanie cyberbezpieczeństwa w związku z czym tworzy się błędne koło. Należy zaznaczyć, że Centralne Biuro Zwalczania Cyberprzestępczości w toku swojej działalności tylko za 2023 rok „odzyskało” 450 mln zł, gdzie część z tych pieniędzy zaspokoi roszczenia pokrzywdzonych a część trafi z powrotem do budżetu.

Wnioski jakie się nasuwają wyraźnie pokazują, że skala cyberprzestępstw znacznie przewyższa zdolności operacyjne organów odpowiedzialnych za walkę z nimi a to z kolei oddziałuje na obywateli oraz systemy bezpieczeństwa zasoby oraz generuje dodatkowe podatności. Na podstawie powyższej argumentacji oraz wyników ankietowania zamieszczonego w załączniku przyjmuje się, że istotność podatności jest na poziomie wysokim.

„Niskie zainteresowanie interesariuszy publicznymi konsultacjami nowelizacji ustawy o KSC”

Główni interesariusze, którzy powinni być zainteresowani wprowadzaniem korzystnych zmian nie wnoszą uwag do projektu co będzie skutkowało przekładaniem swoich problemów na kolejne lata. Biorąc pod uwagę, że zmiana prawnych zapisów odbywa się raz na kilka lub kilkanaście lat działania o takim charakterze są zaprzepaszczoną szansę na poprawę bezpieczeństwa. Skutkiem takiego postępowania jest wprowadzenie znowelizowanych przepisów, które nie do końca wyczerpują swój potencjał korygujący. Jako źródło problemu należy upatrywać brak odpowiednio wykwalifikowanych kadr oraz brak odpowiedniej wiedzy z zakresu cyberbezpieczeństwa co skutkuje unikaniem podejmowania działań w kierunku poprawy stanu obecnego w przedmiotowej dziedzinie.

Problem ten będzie oddziaływał w głównej mierze nie tylko na system cyberbezpieczeństwa, ale również i sektory bezpieczeństwa państwa, ponieważ brak pewnych rozwiązań będzie generował kolejne podatności oraz wpłynie na podmioty i zasoby tych podmiotów. Na podstawie powyższej argumentacji oraz wyników

ankietowania zamieszczonego w załączniku przyjmuje się, że istotność podatności jest na poziomie średnim.

„*Niski poziom współpracy między podmiotami odpowiedzialnymi za cyberbezpieczeństwo”*

Jest to problem, w którym cierpią dwie strony, czyli środowiska akademickie oraz instytucje, które są obiektem badań. W wyniku stosowania tego rodzaju polityki wymiany informacji utracony zostaje potencjał naprawczy. Biorąc pod uwagę ogólnoświatowy trend powstawania „Think tank[127]”, które biorą czynny udział w rozwiązywaniu problemów spraw publicznych krajowe realia wskazują na odcinanie się od wszelkiej pomocy starając się nie dzielić problemami. Skutkiem takiego postępowania jest nie tylko spowolniony rozwój organizacji, ale również zawężone pole badawcze osób zajmujących się różnego rodzaju problematyką. W tym przypadku źródłem problemu również jest niski stan świadomości na temat zagrożeń w cyberprzestrzeni. O ile dbanie o poufne informacje w każdej organizacji (administracji państwowej) jest jak najbardziej wskazane to znikoma świadomość problematyki powoduje zaniechanie działań mających na celu współpracę.

Ten złożony problem ma bezpośredni wpływa na zdolności systemów bezpieczeństwa państwa oraz na poziom bezpieczeństwa podmiotów i zasobów, przy jednocześnie niskim znaczeniu dla obywateli. Na podstawie powyższej argumentacji oraz wyników ankietowania zamieszczonego w załączniku przyjmuje się, że istotność podatności jest na poziomie wysokim.

„Wskazanie Operatora Strategicznej Sieci Bezpieczeństwa (OSSB) jako jedynego, w postaci jednoosobowej spółki”

Strategiczna Sieć Bezpieczeństwa tak jak infrastruktura krytyczna nie powinna być zarządzana przez jednoosobowego decydenta. Biorąc pod uwagę fakt, że jednoosobowa spółka to specyficzna forma prowadzenia działalności, w której istnieje tylko jeden wspólnik, który jednocześnie jest jedynym udziałowcem to właśnie ta jedna osoba ma pełną kontrolę nad zarządzaniem i decyzjami podejmowanymi w spółce. W związku z czym zachodzi obawa o jej upolitycznienie. Skutki jakie się biorą z takiego stanu rzeczy będą miały charakter stworzenia pośrednika, który niewiele wnosi natomiast

[127] Think tank (z ang. dosłownie „zbiornik myśli”) – niezależny komitet doradczy, z założenia o charakterze organizacji non-profit, zajmujący się badaniami i analizami dotyczącymi spraw publicznych.

ma być finansowany za to, że jest pośrednikiem. Ponieważ została wytypowana do tego celu firma, która ma jedynie 5% udział w rynku telekomunikacyjnym w kraju zaburzy to dotychczasowy ład biznesowy pośród operatorów, ponieważ nadanie uprawnień strategicznego operatora spowoduje, że firma ta stanie się monopolistą na pewnego rodzaju usługi. Dla porównania firma „Exatel", która jest rekomendowana jako OSSB zatrudnia obecnie około 450 pracowników i nie posiada zaplecza badawczo-rozwojowego oraz CSIRT-u, przy czym na przykład spółka „Polkomtel" zatrudnia 160 tyś osób[128] i posiada w pełnym spektrum rozbudowane zapiecze logistyczne do utrzymania sieci strategicznej. W związku z czym różnica jest znacząca.

Tworzenie strategicznej sieci bezpieczeństwa wydaje się zbyt newralgicznym przedsięwzięciem, aby była zarządzana poprzez tak mało rozbudowaną strukturę. Kluczowe tu jest zapewnienie realnego bezpieczeństwa podmiotom korzystającym z usług takiego operatora. O ile spółka spełni swoje ustawowe wymogi w czasie pokoju to w przypadku wystąpienia kryzysu nie będzie miała wystarczającego zaplecza do utrzymania zasobów. Ponadto praktyka pokazuje, że nakazy administracyjne korzystania z usług określonego podmiotu powodują zwiększenie kosztów tych usług z jednoczesnym obniżeniem ich jakości podobnie jak w przypadku monopolistów. Na podstawie powyższej argumentacji oraz wyników ankietowania zamieszczonego w załączniku przyjmuje się, że istotność podatności jest na poziomie średnim.

„Marginalne powiązanie Strategii Cyberbezpieczeństwa z krajowymi Strategiami"

Do realizacji zadań cyberbezpieczeństwa niezbędne są dobrze skonstruowane dokumenty o charakterze wizji rozwoju a w następnej kolejności będące implementacją tych strategii regulacje prawne. W wyniku nieładu w dokumentach strategicznych powstaje nie do końca poprawnie sformowane prawo, gdzie w tym przypadku skutkiem jest niedocenienie roli i rangi cyberbezpieczeństwa w podstawowej działalności państwa polskiego. Skutki tego problemu będą takie same jak w przypadku braku nowelizacji Strategii Rozwoju SBN gdzie obecny stan rzeczy powoduje marginalne traktowanie cyberbezpieczeństwa. Dodatkowo biorąc pod uwagę obecne czasy (Industry 5.0) sytuacja powoduje niedocenienie zagrożeń wykorzystujących cyberprzestrzeń a to z kolei wpływa na świadomość społeczną i środki przeznaczane na ochronę.

[128] https://bank.pl/watpliwosci-zwiazane-z-powolaniem-operatora-strategicznej-sieci-bezpieczenstwa/ [dostęp: 23.05.2024].

Brak uporządkowania i utrzymania rangi cyberbezpieczeństwa we wszystkich dokumentach strategicznych oddziałuje na niemal każdy system i podmioty w państwie. Dodatkowo społeczeństwo nie będzie dostrzegało skali zagrożeń, dopóki decydenci nie nakreślą ich w dokumentach normatywnych. Na podstawie powyższej argumentacji oraz wyników ankietowania zamieszczonego w załączniku przyjmuje się, że istotność podatności jest na poziomie średnim.

„Eksploatacja sprzętu teleinformatycznego od producentów uznanych za „dostawców wysokiego ryzyka"

Problem jest o tyle złożony, że prawdziwych skutków eksploatacji sprzętu teleinformatycznego od producentów uznanych za „dostawców wysokiego ryzyka" możemy nigdy nie poznać. Wyobraźmy sobie sytuację, w której system teleinformatyczny wykorzystywany na potrzeby wsparcia działań o charakterze Zarządzania Kryzysowego jest pochodzenia od „dostawców wysokiego ryzyka" i posiada w sobie „Backdoor". Pomimo że przetwarzane w nim informacje mają charakter jawny to sama informacja o siłach i środkach oraz metodach ich wykorzystania ma niezwykle istotne znaczenie dla obcych służb. Takie informacje w niepowołanych rękach w przypadku wystąpienia sytuacji kryzysowej mogą sparaliżować działania przywracające normalny stan. Są to niezwykle wrażliwe dane i należy mieć 100% pewność, że elementy sprzętowe systemu są z zaufanego źródła i są sprawdzone poprzez odpowiednie akredytacje i audyty.

Obierając najmniej optymistyczny scenariusz to eksploatacja sprzętu teleinformatycznego od producentów uznanych za „dostawców wysokiego ryzyka" jest poważnym problemem. O ile sytuacja ta nie dotyczy obywateli to ma kolosalne znaczenie w systemach bezpieczeństwa państwa i toruje drogę do paraliżu podmiotów realizujących zadania na rzecz obrony państwa. Na podstawie powyższej argumentacji oraz wyników ankietowania zamieszczonego w załączniku przyjmuje się, że istotność podatności jest na poziomie wysokim.

„Brak właściwego do wagi zagadnienia wyeksponowania roli cyberbezpieczeństwa w Strategii Rozwoju SBN"

Skutki tego problemu są takie same jak w przypadku marginalnego połączenia Strategii Cyberbezpieczeństwa z krajowymi Strategiami. W związku z czym oba przypadki można uznać za jedną podatność.

Przyjmuję się na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych, że istotność podatności jest na poziomie wysokim.

„*Brak regulacji prawnych dotyczących działalności ISAC”*

Szczegółowo rzecz ujmując mowa tu o regulacjach dotyczących finansowania i kontroli. Brak konkretnych regulacji może mieć poważne skutki, ponieważ ISAC są dotowane poprzez darowizny, dotacje, subwencje. Z tego też powodu każdy z „darczyńców” może chcieć mieć wgląd w to jak wydatkowane są środki, które przekazał a co za tym idzie może wejść w posiadanie informacji o działalności operacyjnej ISAC. Kolejnym problemem powołania w obecnej formie ISAC jest brak zhierarchizowanej struktury co skutkowało będzie rywalizacją o finanse (dotacje) zamiast współpracy. Należy podkreślić fakt, że państwa członkowskie UE dążą do kontroli działalności i normalizacji zasad finansowania własnych ISAC. Za przykład może posłużyć czysto hipotetyczny wyciek danych operacyjnych z ISAC Kolej, który odpowiedzialny jest po części za infrastrukturę krytyczną. Zagrożenie jakie mogą popłynąć z takiego stanu rzeczy w wariancie najmniej optymistycznym mogą generować nie tylko straty z tytułu utraty wizerunku, ale też doprowadzić do ujawnienia newralgicznych w skali państwa zasobów informacyjnych. W związku z przedmiotowym problemem to nie tylko systemy bezpieczeństwa będą zagrożone, ale również życie i zdrowie obywateli.

Na podstawie powyższej argumentacji oraz wyników ankietowania zamieszczonego w załączniku przyjmuje się, że istotność podatności jest na poziomie średnim.

„*Brak satysfakcjonującego poziomu ukompletowania kadr w administracji państwowej”*

Jest to kluczowy problem tuż obok finasowania i ściśle z nim powiązany. Obecne stawki jakie wykwalifikowany specjalista może uzyskać w administracji państwowej są około 2-3 razy niższe niż te, które można otrzymać w sektorze prywatnym. Konsekwencją jest przechodzenie (uciekanie) personelu do podmiotów prywatnych. Wskutek tego w administracji państwowej pozostają osoby mniej wyspecjalizowane co przekłada się na jakość działań w cyberprzestrzeni. Ponadto dotkliwe są obecne braki kadrowe co powoduje, że ilość zadań przeznaczonych na jedną osobę jest

intensyfikowana. Cyberbezpieczeństwo jest dziedziną bezpieczeństwa w której to jakość i ilość specjalistów świadczy o zdolnościach obronnych państwa.

Problematyka jest poważna i oddziałująca na wszystkie systemy oraz podmioty w państwie. Dodatkowo z punktu widzenia obywateli jakość oraz ilość kadr odpowiedzialnych za cyberbezpieczeństwo ma również kluczowe znaczenie. Na podstawie powyższej argumentacji oraz wyników ankietowania zamieszczonych w załączniku przyjmuje się, że istotność podatności jest na poziomie wysokim.

„Brak sprzężenia instytucji CBZC z Krajowym Systemem Cyberbezpieczeństwa"

Oprócz potrzeby podwojenia instytucji odpowiedzialnej za walkę z cyberprzestępczością istnieje uzasadniona potrzeba włączenia CBZC do struktur Krajowego Systemu Cyberbezpieczeństwa. Potrzeba ta wynika z ujednolicenia struktury KSC oraz podziału zadań pomiędzy poszczególnymi instytucjami. Skutkiem pozostawienia stanu obecnego bez przedmiotowych działań może być brak ściśle zdefiniowanego podziału między pracą operacyjną CBZC i CSIRT. Obecnie CBZC, które w swym statucie ma wpisaną walkę z cyberprzestępczością i operuje w cyberprzestrzeni funkcjonuje poza strukturą KSC co samo w sobie jest przedmiotem do dyskusji.

Słabość ta jest najmniej dotkliwa pod względem oddziaływania na systemy, podmioty i obywateli natomiast jest konieczna, aby uporządkować strukturalnie Krajowy System Cyberbezpieczeństwa. Przyjmuję się na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych, że istotność podatności jest na poziomie średnim.

„Brak ustawowego kształcenia najmłodszych użytkowników Cyberprzestrzeni"

Pomimo, że kształcenie ustawiczne najmłodszych użytkowników cyberprzestrzeni było przedmiotem wielu dyskusji to do tej pory nie powstał żaden konkretny program gotowy do wdrożenia w życie. Skutkiem takiego stanu rzeczy jest brak przygotowania najmłodszych użytkowników do zgodnej z przeznaczeniem i normami eksploatacji technologii cyfrowych. Taka sytuacja powoduje przede wszystkim brak podnoszenia świadomości społecznej na zagrożenia cyberprzestrzeni. Dodatkowo nie indukuje w uczniach pasji do cyberbezpieczeństwa gdzie biorąc pod uwagę, że młodzi ludzie na tym etapie planują już swoje ukierunkowanie zawodowe to nie mają szans zapoznać się z tą dziedziną wiedzy. Jest to luka, której efekty będą

widoczne w następnym pokoleniu o ile nic się nie zmieni. Problem ten będzie potęgowany i docelowo będzie oddziaływał stopniowo na wszystkie systemy i podmioty.

Niemniej jednak oceniając stan obecny przyjmuję się na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych, że istotność podatności jest na poziomie niskim.

Posługując się w ten sposób zdefiniowaną terminologią oraz wskaźnikami można w miarę czytelnie przedstawić dalsze czynności realizowane w tym etapie.

4.4. Szacowanie i ocena ryzyka

Zestawienie wyłonionych elementów składowych materializacji zagrożeń (ESMZ) a w szczególności sposobów realizacji zagrożeń (SRZ), metod, technik, narzędzi (MTN) oraz skutków materializacji zagrożeń (SMZ) z podatnościami pozwoli uzyskać informację na temat jakie jest prawdopodobieństwo wystąpienia danego ryzyka wobec wskazanych podatności oraz jaki jest poziom istotności każdej z podatności w konkretnym stanie rzeczywistości. W tym celu dokonano kolejnego zestawienia zaprezentowanego w tabeli 16 gdzie użyto następujących poziomów otrzymanych na podstawie istotności podatności względem składowych materializacji zagrożenia:

- niska (1) istotność podatności wobec elementów materializacji zagrożenia, co należy rozumieć, że EMZ znikomo oddziałują na podatność;
- średnia (2) istotność podatności wobec elementów materializacji zagrożenia, co należy rozumieć, że EMZ połowicznie oddziałuje na podatność;
- wysoka (3) istotność podatności wobec elementów materializacji zagrożenia, co należy rozumieć, że EMZ znacznie oddziałuje na podatność;

Prezentowana trójstopniowa skala jakościowa również w tym przypadku oparta jest na subiektywnej ocenie. W tym miejscu należy podkreślić fakt, że elementy składowe materializacji zagrożeń będą istniały niezależnie od tego czy wyeliminujemy podatności czy nie. Z kolei w celu ustalenia prawdopodobieństwa oddziaływania elementu materializacji zagrożenia z podatnościami użyto następującej trójstopniowej skali:

- niskie (1) prawdopodobieństwo oddziaływania podatności z elementami materializacji zagrożenia jest niskie, co należy rozumieć, że interakcja EMZ z podatnością jest mało prawdopodobna;

- średnie (2) prawdopodobieństwo oddziaływania podatności z elementami materializacji zagrożenia jest średnie, co należy rozumieć, że interakcja EMZ z podatnością jest możliwa;
- wysokie (3) prawdopodobieństwo oddziaływania podatności z elementami materializacji zagrożenia jest wysokie, co należy rozumieć, że interakcja EMZ z podatnością jest bliska pewności.

Dodatkowo istotność podatności wobec elementów materializacji zagrożenia będzie miała wpływ na oczekiwane straty a łatwość wykorzystania podatności będzie miała wpływ na częstość realizacji zagrożenia. Wobec czego istnieje uzasadniona potrzeba identyfikacji tych wartości celem pełnego zobrazowania obecnej sytuacji.

Tab. 16. Możliwość realizacji zagrożeń.

PODATNOŚCI / ELEMENTY MATERIALIZACJI ZAGROŻENIA		1	2	3	4	5	6	7	8	9	10	11	12	13	PRAWDOPODOBIEŃSTWO
METODY, NARZĘDZIA, TECHNIKI WYKORZYSTYWANE DO MATERIALIZACJI ZAGROŻEŃ															
ZŁOŚLIWE OPROGRAMOWANIE	MALWARE	1	3	3	1	2	1	1	1	1	2	3	2	3	24
	RANSOMWARE	1	3	3	1	2	1	1	1	1	2	3	2	3	24
BACKDOOR		1	3	3	1	2	1	1	3	1	2	3	2	3	26
DOS, DDOS		1	3	1	2	2	3	1	2	1	3	3	2	1	25
SOCJOTECHNIKI		2	3	2	1	2	1	1	2	1	2	3	2	3	25
SPOSOBY REALIZACJI ZAGROŻEŃ															
DEZINFORMACJA	FAKENEWS	3	3	3	2	3	2	2	2	2	2	3	2	3	32
	DEEPFAKE	3	3	3	2	3	2	2	2	2	2	3	2	3	32
	PROPAGANDA	3	3	3	2	3	2	2	2	2	2	3	2	3	32
CYBER PRZESTĘPCZOŚĆ	OSZUSTWA KOMPUTEROWE	1	3	3	1	2	2	1	1	2	2	3	2	3	26
	KRADZIEŻY DANYCH	1	3	3	2	2	1	2	1	2	2	3	2	3	27
	OBRAŹLIWE TREŚCI	2	3	3	1	3	1	2	1	2	1	3	3	3	28
SKUTKI MATERIALIZACJI ZAGROŻEŃ															
DOSTĘPNOŚĆ INTEGRALNOŚĆ POUFNOŚĆ	NISZCZENIE INFRA. CYFROWEJ	1	3	1	1	1	2	2	3	2	1	3	1	2	23
	ZAGROŻONE ŁAŃCUCHY DOSTAW	2	3	3	2	3	2	2	2	2	2	3	2	2	30
	UTRUDNIONY DOSTĘP DO USŁUG	2	3	3	2	2	2	2	2	2	1	3	1	2	27
STOPIEŃ WYKORZYSTANIA PODATNOŚCI PRZEZ EMZ		24	42	37	21	32	23	22	25	23	26	42	27	37	

Źródło: opracowanie własne na podstawie.

Z przedstawionej tabeli (Tab. 16) można pozyskać informację na temat istotność podatności oraz prawdopodobieństwa wystąpienia składowych materializacji zagrożeń co zostało przedstawione w tabeli nr. 17. Przeprowadzona analiza pozwoliła wyeksponować, że najbardziej prawdopodobnymi do realizacji są elementy dezinformacji tj. Fakenews, Deepfake oraz propaganda. Natomiast największy stopień

wykorzystania podatności przez elementy materializacji zagrożenia będą miały podatności:

- niski poziom finansowania podmiotów odpowiedzialnych za cyberbezpieczeństwo;
- zbyt mała zdolność operacyjnych instytucji odpowiedzialnych za walkę z oszustwami komputerowym;
- brak satysfakcjonującego poziomu ukompletowania kadr odpowiedzialnych za cyberbezpieczeństwo w administracji państwowej;
- brak ustawowego kształcenia najmłodszych użytkowników Cyberprzestrzeni w zakresie higieny cyfrowej.

W związku z czym prezentowane problemy muszą zostać rozwiązane poprzez eliminację podatności na pierwszym miejscu.

Tab. 17. Stopień narażenia podatności na EMZ oraz prawdopodobieństwo wystąpienia składowych materializacji zagrożeń.

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	WYNIK	ELEMENTY SKŁADOWE MATERIALIZACJI ZAGROŻEŃ
NISKIE	13 - 21	
ŚREDNIE	22 - 30	Malware, Ransomware, Backdoor, DoS, DDoS, socjotechniki, oszustwa komputerowe, kradzieży danych, obraźliwe treści, niszczenie infrastruktury cyfrowej, zagrożone łańcuchy dostaw, utrudniony dostęp do usług
WYSOKIE	31 - 39	fakenews, deepfake, propaganda

STOPIEŃ WYKORZYSTANIA PODATNOŚCI PRZEZ ELEMENTY MATERIALIZACJI ZAGROŻEŃ	WYNIK	PODATNOŚCI
NISKI	14 - 23	• Niskie zainteresowanie interesariuszy publicznymi konsultacjami nowelizacji ustawy o KSC • Wskazanie Operatora Strategicznej Sieci Bezpieczeństwa (OSSB) jako jedynego • Marginalne powiązanie Strategii Cyberbezpieczeństwa z krajowymi Strategiami • Brak właściwego do wagi zagadnienia wyeksponowania roli cyberbezpieczeństwa w Strategii RSBN
ŚREDNI	24 - 33	• Niewystarczająca ilość i jakość regulacji prawnych dotyczących dezinformacji • Niski poziom współpracy miedzy podmiotami odpowiedzialnymi za cyberbezpieczeństwo • Eksploatacja sprzętu teleinformatycznego producentów uznanych za „dostawców wysokiego ryzyka • Brak regulacji prawnych dotyczących działalności ISAC • Brak sprzężenia instytucji CBZC z Krajowym Systemem Cyberbezpieczeństwa
WYSOKI	34 - 42	• Niski poziom finansowania podmiotów odpowiedzialnych za cyberbezpieczeństwo • Zbyt mała zdolność operacyjnych instytucji odpowiedzialnych za walkę z oszustwami komputerowymi • Brak satysfakcjonującego poziomu ukompletowania kadr w administracji państwowej • Brak ustawowego kształcenia najmłodszych użytkowników Cyberprzestrzeni

Źródło: opracowanie własne na podstawie Tab. 16.

Przedstawiona została szczegółowa analiza zawartości, której wyniki są podstawą do wprowadzenia odpowiednich miar w pola tabeli, przy czym należy zaznaczyć, że analiza jest również subiektywna.

Szczegółowa analiza zawartości tabeli 16 i 17.

Malware – jest złośliwym oprogramowaniem, które wg statystyk wiedzie prym jako narzędzie służące do realizacji zagrożenia. Wrażliwymi podatnościami będą tu braki

prawno-proceduralne. Natomiast kluczowe znaczenie będzie tu miało finansowanie, poziom kadr, uświadamianie obywateli oraz operacyjność podmiotów odpowiedzialnych za Cyberbezpieczeństwo. Najbardziej narażone będą podatności związane z finansowaniem i ukompletowaniem kadr oraz mające bezpośredni wpływ na technologię.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że stopień oddziaływania techniki ataku względem wszystkich podatności jest na poziomie średnim.

Ransomware – jest złośliwym oprogramowaniem, które blokuje/szyfruje dostęp do zasobów informacyjnych. Narzędzie wykorzystuje podobnie podatności jak Malware. Zgodnie z raportami organizacji zajmujących się Cyberbezpieczeństwem jest najczęściej stosowanym narzędziem do wymuszania okupu lub działań o charakterze sabotażowym, dywersyjnym lub walki ideologicznej. Najbardziej narażone będą podatności związane z finansowaniem i ukompletowaniem kadr oraz mające bezpośredni wpływ na technologię.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że stopień oddziaływania techniki ataku względem wszystkich podatności jest na poziomie średnim.

Backdoor – jest luką w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania. Istnieje uzasadnione podejrzenie skojarzenia tego oprogramowania z podatnością eksploatacji sprzętu ITC od „dostawców wysokiego ryzyka". Ponadto jako luka w oprogramowaniu będzie oddziaływała w stopniu podobnym na podatności tak jak Malware i Ransomware. Najbardziej narażone będą podatności proceduralno-prawne oraz technologiczno-logistyczne natomiast mentalne i ekonomiczno-finansowe nieco mniej.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że stopień oddziaływania luki w oprogramowaniu jaką jest Backdoor względem wszystkich podatności jest na poziomie średnim.

DoS, DDoS – jest to technika ataku na systemy teleinformatyczne, powodująca przeciążenie serwerów i jest względnie łatwa do implementacji. Do przeprowadzenia ataku służą najczęściej komputery nad którymi przejęto kontrolę przy użyciu specjalnego oprogramowania (różnego rodzaju tzw. boty i Trojany). Na dany sygnał komputery

zaczynają jednocześnie atakować system ofiary zasypując go fałszywymi próbami skorzystania z usług jakie oferuje. Technika ta jest klasycznym przykładem ingerowania w dostępność zasobów informacyjnych. Podatności prawno-proceduralne wobec techniki będą najbardziej odporne natomiast ekonomiczno-finansowe oraz technologiczno-logistyczne są najmniej odporne.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że stopień oddziaływania techniki ataku względem wszystkich podatności jest na poziomie średnim.

Socjotechniki – jest to zbiór technik wykorzystywanych w celu wprowadzenia ofiary w błąd. Analiza dotychczas poznanych socjotechnik pozwala na stwierdzenie, że wyobraźnia wrogich podmiotów nie ma granic. Najmniej odporne podatności to te które mają składową mentalności na wyższym poziomie oraz zawierają niedoprecyzowane błędy proceduralno-prawne. Natomiast podatności ekonomiczno-finansowe oraz technologiczno-logistyczne będą odporne w stopniu średnim.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że stopień oddziaływania socjotechnik wykorzystywanych podczas wrogich działań względem wszystkich podatności jest na poziomie średnim.

Utrudniony dostęp do usług – jest to konsekwencja materializacji zagrożeń, która wg statystyk jest jednym z najbardziej dotkliwych skutków, ponieważ wypływa bezpośrednio na dostępność zasobów informacyjnych. Przyczyną powstania mogą być wszystkie wymienione sposoby realizacji zagrożeń oraz narzędzia, metody i techniki, wobec czego interakcja z podatnościami będzie wypadkową wszystkich oddziaływań.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że konsekwencje w postaci utrudnionego dostępu do usług podczas wrogich działań, będą dotyczyły wszystkich podatności są na poziomie średnim.

Zagrożone łańcuchy dostaw-usług – jest to kolejna konsekwencja materializacji zagrożeń, która wg statystyk jest jednym z najbardziej dotkliwych skutków, ponieważ w skali globalnej powoduje gigantyczne straty. Przyczyną powstania mogą być wszystkie wymienione sposoby realizacji zagrożeń oraz narzędzia, metody i techniki, wobec czego interakcja z podatnościami będzie wypadkową wszystkich oddziaływań.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że konsekwencje w postaci przerwania ciągłości w łańcuchu dostaw w wyniku wrogich działań będą dotyczyły wszystkich podatności i są na poziomie średnim.

Niszczenie infrastruktury cyfrowej – jest to rzadko spotykana konsekwencja materializacji zagrożeń jednak bardzo dotkliwa. Szczególnie realna podczas stanów nadzwyczajnych takich jak konflikt czy sytuacje kryzysowe. Przyczyną powstania może być fizyczne lub zdalne uszkodzenie infrastruktury tak jak to miało podczas wykorzystania programu Stuxnet[129]. Podatności składające się z przyczyn technologiczno-logistycznych, ekonomiczno-finansowych będą narażone w wyższym stopniu natomiast szczególnie wrażliwą podatnością będzie eksploatacja sprzętu pochodzącego od dostawców wysokiego ryzyka.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że konsekwencje w postaci niszczenia infrastruktury cyfrowej podczas wrogich działań będą dotyczyły wszystkich podatności na poziomie średnim.

Propaganda – jako element dezinformacji powszechnie spotykany w otaczających nas mediach i życiu codziennym. Jest szczególnym elementem, ponieważ jak wszystkie składowe propagandy oddziałuje niemal na wszystkie podatności w stopniu średnim i wysokim a co za tym idzie potrafi wykorzystać wszystkie kategorie podatności.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że propaganda będzie oddziaływała z wszystkimi podatnościami na poziomie wysokim.

Fakenews – jest to element dezinformacji powszechnie spotykany w otaczających nas mediach i życiu codziennym. Należy przyznać, że Fakenews oddziałuje z podobną siłą jak propaganda na wszystkie podatności.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że Fakenews będzie oddziaływało z wszystkimi podatnościami na poziomie wysokim.

[129] Stuxnet – działający w systemie Windows robak komputerowy, po raz pierwszy wykryty w czerwcu 2010. Stuxnet atakował głównie sterowniki PLC, konwertery częstotliwości zmieniając częstotliwość prądu, jaki one wysyłały, co doprowadzało do przyspieszenia pracy wirówek gazowych wzbogacających uran a w konsekwencji ulegały one zniszczeniu.

Deepfake – szczegółowo rzecz ujmując jest to bliźniacze zjawisko do Fakenews, więc będzie rozpatrywane niemal identycznie.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych, przyjmuje się, że Deepfake będzie oddziaływało z wszystkimi podatnościami na poziomie wysokim.

Oszustwa komputerowe – jedne z najdotkliwszych działań w cyberprzestępczości powodujące olbrzymie straty finansowe w skali całego państwa. Oszustwa będą korelowały z podatnościami natury proceduralno-prawnej będą miały wpływ na poziom kadr odpowiedzialnych za cyberbezpieczeństwo i wielkość nakładów finansowych na walkę z przestępczością cyfrową. Nie bez znaczenia pozostają tu podatności o wysokiej składowej mentalności takie jak niski poziom współpracy oraz świadomość użytkowników technologii cyfrowych.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych, przyjmuje się, że oszustwa komputerowe będą oddziaływały z wszystkimi podatnościami na poziomie średnim.

Kradzieży danych – działania cyberprzestępcze zazwyczaj polegające na wyłudzeniu danych oraz wykorzystania ich do wrogich zamiarów. Konsekwencją tego typu działań są próby zaciągnięcia kredytu na ofiarę lub zakup nielegalnych przedmiotów. Kradzież danych będzie miała silny wpływ na podatności proceduralno-prawne oraz mentalne w ujęciu uświadamiania obywateli.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych, przyjmuje się, że kradzież danych będzie oddziaływała z wszystkimi podatnościami na poziomie średnim.

Obraźliwe treści – to mieszana forma cyberprzestępczości z elementami dezinformacji. Jest szczególnie niebezpieczna w przypadku nastoletnich obywateli, ponieważ zdarzają się przypadki samookaleczeń lub samobójstw spowodowanych tzw. „hejtem" w sieci lub dyskredytacją kogoś w oczach innych.

Na podstawie powyższej argumentacji, wyników ankietowania zamieszczonego w załączniku oraz danych statystycznych przyjmuje się, że obraźliwe treści będą oddziaływały z wszystkimi podatnościami na poziomie średnim.

4.5. Apetyt na ryzyko

Wprowadzenie czynności określenia apetytu na ryzyko wymusza zastosowanie podziału na poziomy ryzyka takie jak:

- krytyczne ryzyko, którym należy definitywnie zarządzać;
- tolerowane ryzyko, które możemy zaakceptować, ale tylko w szczególnych warunkach;
- akceptowalne ryzyko, które dopuszczamy.

W przypadkach budzących wątpliwości ryzyko tolerowane powinno podlegać wnikliwszej analizie opartej na dodatkowych wskaźnikach. Jednak ze względu na to, że zamiarem przedmiotowej dysertacji jest w stopniu maksymalnym dążyć do poprawy bezpieczeństwa to priorytetem będzie usunięcie wszystkich stwierdzonych podatności.

Należy zaznaczyć, że w rozdziale VI podczas implementacji przedmiotowej koncepcji poprawy bezpieczeństwa będzie realizowana również analiza ryzyka po wprowadzeniu utworzonych zmian. Wówczas możliwym będzie skonfrontowanie zestawienia obu analiz ryzyk i dalsze rozstrzyganie nad akceptowalnym poziomem ryzyka jakie państwo polskie jest w stanie zaakceptować. W chwili obecnej przyjmuje się, że apetytem na ryzyko jest stopień akceptacji oraz implementacji przyjętych rozwiązań. Ponieważ sytuacja wymaga konieczności wprowadzenia jakichkolwiek działań naprawczych to rozwiązania których nie uda się zaimplementować będą wpisane w apetyt na ryzyko.

4.6. Postępowanie z ryzykiem

Jak wspomniano na początku rozdziału istnieje kilka metod postępowania z ryzykiem[130]. Najczęściej stosowane rozwiązania to:

- kontrola (redukcja ryzyka), wprowadza się działania kontrolne w celu zmniejszenia prawdopodobieństwa jego wystąpienia;
- unikanie ryzyka, polega na zaniechaniu wszelkich działań, które to ryzyko generują;
- transfer (przeniesienie ryzyka), zleca się określone czynności związane z ryzykiem podmiotowi zewnętrznemu (outsourcing);

[130] Liderman K., Bezpieczeństwo… dz. cyt. s. 87.

- retencja, akceptacja ryzyka oznacza, że godzimy się z ryzykiem przyjmując, że koszt postępowania z ryzykiem jest większy niż szkody, które by to spowodowało.

Ponieważ założenie jest takie, aby nie dopuścić do materializacji zagrożeń w związku z czym w tym przypadku metodą będzie dążenie do minimalizacji ryzyka poprzez eliminację stwierdzonych podatności (tzw. unikanie ryzyka). Oczywiście może się zdarzyć sytuacja (podatność), której nie da się usunąć lub zminimalizować wtedy rozpatrywane będą inne przedstawione metody.

Na podstawie dotychczas przeprowadzonych w rozdziale analiz przedstawiona zostanie kolejność czynności realizacji procesu naprawczego zgodnie z wagą istotności podatności. Aby stworzyć warunki do eliminacji podatności należy uwzględnić pewne obszary doskonalenia. Poprzez obszary doskonalenia należy rozumieć działania, do których należą:

- utworzenie (przekształcenie) infrastruktury;
- wzmocnienie kapitału ludzkiego;
- utworzenie lub modyfikacja prawa;
- pozyskanie nakładów finansowe;
- utworzenie programu rozwoju.

Na podstawie zebranych danych (Tab. 15) ujęto w tabeli 18 zdiagnozowane podatności wraz z propozycją przygotowanych dla nich rozwiązań oraz jednoczesnym zaznaczeniem obszaru doskonalenia, który jest konieczny do implementacji. W tym miejscu należy wyjaśnić pewne ułatwienia, które zastosowano, ponieważ scalono „bliźniacze" podatności w jedno tak jak to miało miejsce w przypadku:

1. *„Marginalne powiązanie Strategii Cyberbezpieczeństwa z krajowymi Strategiami" i „Brak właściwego do wagi zagadnienia wyeksponowania roli cyberbezpieczeństwa w Strategii Rozwoju Systemu Bezpieczeństwa Narodowego".*
2. *„Brak sprzężenia instytucji CBZC z Krajowym Systemem Cyberbezpieczeństwa" i „Zbyt mała zdolność operacyjnych instytucji odpowiedzialnych za walkę z oszustwami komputerowymi".*
3. *„Niski poziom współpracy między podmiotami odpowiedzialnymi za cyberbezpieczeństwo" i „Niskie zainteresowanie interesariuszy publicznymi konsultacjami nowelizacji ustawy o KSC".*

Prezentowane podatności mają podobną przyczynowość oraz wymagają podjęcia tych samych działań naprawczych w związku z czym w szerszym kontekście można je rozpatrywać jako jedną podatność. Zabieg ten pozwoli na zmniejszenie ilości podatności z pełnym zachowaniem wyeliminowania skutków ich następstw. Przykładowo połączone problemy z punktu 3 wskazują jako źródło ich powstawania niewystarczający poziom wiedzy o cyberbezpieczeństwie osób pełniących służbę/pracę w podmiotach administracji państwowej. Podniesienie poziomu świadomości oraz elementarnej wiedzy z zakresu cyberbezpieczeństwa przełoży się na poprawę współpracy oraz intensywniejsze zaangażowanie w sprawy dotyczące przedmiotowej problematyki.

Tab. 18. Propozycji eliminacji podatności wraz z obszarem doskonalenia.

Lp.	Wykaz podatności (propozycja eliminacji)	obszary doskonalenia				
		Wielkość infrastrukt.	Liczba personelu	Regulacje prawne	Koszty utworzenia	Utrzymanie miesięczne
1	Brak ustawowego kształcenia najmłodszych użytkowników cyberprzestrzeni. (narodowy program kształcenia ustawowego z ustanowieniem przedmiotu higiena cyfrowa)	NIE	NIE	*TAK*	*TAK*	*TAK*
2	Eksploatacja sprzętu teleinformatycznego producentów uznanych za dostawców wysokiego ryzyka. (programu rozwoju badań nad tworzeniem własnych zdolności technologicznych)	NIE	NIE	*TAK*	*TAK*	*TAK*
3	Wskazanie operatora strategicznej sieci bezpieczeństwa (OSSB) w postaci jednoosobowej spółki. (propozycja realizacji zadania OSSB przez NASK-PIB)	*TAK*	*TAK*	*TAK*	*TAK*	*TAK*
4	Brak regulacji prawnych dotyczących działalności ISAC. (zaproponowanie modelu amerykańskiego polegającego na usankcjonowaniu centrów)	NIE	NIE	*TAK*	NIE	*TAK*
5	Marginalne powiązanie rangi cyberbezpieczeństwa w krajowych Strategiach. (podniesienie rangi i znaczenia cyberbezpieczeństwa w dokumentach strategicznych)	NIE	NIE	*TAK*	NIE	*TAK*
6	Niski poziom świadomości o zagrożeniach w cyberprzestrzeni personelu w administracji państwowej. (utworzenie narodowego programu szkolenia z cyberbezpieczeństwa w administracji państwowej)	NIE	NIE	*TAK*	NIE	*TAK*
7	Niewystarczająca ilość i jakość regulacji prawnych dotyczących dezinformacji. (propozycja utworzenia na szczeblu krajowym instytucji odpowiedzialnej za dezinformację)	*TAK*	NIE	*TAK*	*TAK*	*TAK*
8	Zwiększenie instytucji odpowiedzialnych za walkę z oszustwami komputerowymi i sprzężenie z KSC. (propozycja utworzenia kolejnego biura CZBC i włączenie do struktur KSC)	*TAK*	*TAK*	*TAK*	*TAK*	NIE
9	Brak satysfakcjonującego poziomu ukompletowania kadr w administracji państwowej. (rozbudowa rozporządzenia KPRM w sprawie świadczeń teleinformatycznych)	NIE	TAK	*TAK*	*TAK*	*TAK*
10	Niski poziom finansowania podmiotów odpowiedzialnych za Cyberbezpieczeństwo. (zamiana abonamentu RiTV na podatek cyberbezpieczeństwa)	NIE	NIE	*TAK*	TAK	*TAK*

Źródło: opracowanie własne.

Obszary doskonalenia, które brano pod uwagę są niezbędne do wykluczenia przedmiotowych podatności. Niektóre propozycje eliminacji wymagają utworzenia lub przekształcenia w ujęciu instytucjonalnym obecnej infrastruktury. Prawie wszystkie podatności, aby je wyeliminować wymagają pozyskania nakładów finansowych oraz wzmocnienia kapitałem ludzkim. Biorąc pod uwagę nienajlepszą kondycję kadrowo-finansową Funduszu Cyberbezpieczeństwa jest to poważne wyzwanie wymagające

nieszablonowych rozwiązań. Podstawą do poprawienia stanu obecnego jest dobrze skonstruowane prawo oraz nadanie w strukturach systemu bezpieczeństwa państwa odpowiedniej rangi cyberbezpieczeństwa adekwatnej do rodzaju zagrożeń w cyberprzestrzeni. Biorąc pod uwagę współczesny rozwój techniki cyfrowej będący następstwami następujących po sobie rewolucji przemysłowych w szczególności rozwój Sztucznej Inteligencji cyberbezpieczeństwo powinno mieć charakter nie tylko transsektorowy, ale przede wszystkim ponaddziedzinowy.

Wszelkie niezbędne elementy konieczne do utworzenia koncepcji poprawy bezpieczeństwa zostały uzyskane w związku z czym następnym etapem będzie tworzenie samej koncepcji opartej na eliminacji podatności wraz z oszacowaniem sił i środków ujętych w obszarach doskonalenia. Koncepcja realizowana będzie od eliminacji najmniej istotnych podatności. Takie podejście pozwoli zająć się tworzeniem rozwiązań najbardziej istotnych na końcu. Biorą pod uwagę, że są to problemy dotyczące pozyskiwania kadr i środków finansowych zajmując się nimi na końcu będzie można uwzględnić również potrzeby wynikające z przedmiotowej koncepcji.

4.7. Podsumowanie rozdziału

Podstawowym elementem jaki należy uczynić podczas analizy ryzyka jest ustalenie w jakim celu jest to robione. W tym przypadku analiza miała na celu przynieść odpowiedź na pytanie - jakie skutki mogą zaistnieć przy założeniu, że nie zostaną podjęte żadne działania naprawcze? Przedstawione zestawienia kluczowych czynników mających wpływ na ryzyko pozwoliły przedstawić w formie skali poziomy:

- oczekiwane straty w przypadku braku podjęcia działań naprawczych;
- stopień narażenia podmiotu przez podatności;
- prawdopodobieństwo wystąpienia zagrożenia;
- stopień wykorzystania podatności przez elementy materializacji zagrożeń.

Dodatkowo zdiagnozowanie przyczyn stwierdzonych podatności pozwoliło na określenie obszarów doskonalenia i eliminacji tych podatności. W przygotowywanej koncepcji poprawy bezpieczeństwa państwa precyzyjne można wyznaczyć, które obszary muszą zostać uwzględnione a to z kolei przełoży się na jakość rozwiązań. Dopełnieniem szacowania ryzyka będzie ponowny przegląd ryzyka po wprowadzeniu zmian, wobec czego porównanie po implementacji analizy ex-post z analizą ex-ante będzie stanowiło |o efektywności proponowanych zmian.

W toku podejmowanych działań związanych z szacowaniem ryzyka stwierdzono, że konieczne jest utworzenie lub przekształcenie obecnych instytucji, które realizują zadania na rzecz cyberbezpieczeństwa i zorientować je na nowe kierunki zagrożeń. Istnieje uzasadniona potrzeba utworzenia programu pozyskiwania wyspecjalizowanych kadr do walki z zagrożeniami w cyberprzestrzeni. Zarówno dokumenty szczebla strategicznego jak i regulacje prawne muszą być stworzenie lub zmodyfikowane do poziomu adekwatnego współczesnym wyzwaniom przed jakimi stoi System Bezpieczeństwa Narodowego wraz z podsystemami w ujęciu cyberbezpieczeństwa. Aby móc zrealizować prezentowane założenia należy nie tylko zapewnić, ale również zwiększyć poziom obecnego finansowania zadań ochronnych w cyberprzestrzeni. Problem jest złożony, ponieważ cyberbezpieczeństwo jest obszarem bezpieczeństwa wymagającym znacznych nakładów finansowych. Ponadto należy również do kosztów oszacować potencjalne straty finansowe jakie niesie za sobą długoterminowy brak podejmowania działań. Tworzenie projektu koncepcyjnego poprawy bezpieczeństwa państwa odbędzie się poprzez przedstawienie działań naprawczych dla każdej podatności, obejmując przedmiotowe obszary doskonalenia oraz poddaniu każdego pomysłu będącego rozwiązaniem problemu analizie SWOT co pozwoli na wychwycenie potencjalnych źródeł nowych nieznanych zagrożeń.

ROZDZIAŁ V. KONCEPCJA WZMACNIANIA ODPORNOŚCI PAŃSTWA NA ZAGROŻENIA WYKORZYSTUJĄCE CYBERPRZESTRZEŃ

5.1. Założenia i ograniczania koncepcji

Głównym celem tego rozdziału jest utworzenie koncepcji wzmacniania odporności państwa. Koncepcja ta musi zawierać kompleksowe rozwiązania. Należy przez to rozumieć, że konieczne jest podjęcie szeregu działań. Nie tylko minimalizacji wykorzystania podatności przez zagrożenia, ale również eliminacji płaszczyzn przyczynowych powstawania tych podatności zgodnie z grafiką nr 30 (rozdział 4.2). Rozwiązania zaproponowane w koncepcji w wymiarze ogólnym mają na celu:

- usprawnienie funkcjonowanie systemów bezpieczeństwa państwa;
- zwiększenie bezpieczeństwa obywateli w cyberprzestrzeni;
- podniesienie ogólnej świadomość obywateli o zagrożeniach w cyberprzestrzeni.
- wzmocnienie ochrony zasobów informacyjnych przed nieupoważnionym dostępem;
- utrzymanie ciągłości działania świadczenia usług cyfrowych;
- zmniejszenie poziomu ogólnokrajowej cyberprzestępczości.

W wymiarze społecznym cele szczegółowe koncepcji będą bezpośrednio związane z ochroną i bezpieczeństwem zasobów informacyjnych o potencjale (siły i środki, procedury i plany działania itp..) oraz będą oddziaływały na podsystemy:

- system obronnego państwa;
- system ochrony infrastruktury krytycznej;
- system ochrony granicy państwowej;
- system przeciwpowodziowy;
- system ochrony informacji niejawnych;
- system bezpieczeństwa międzynarodowego;
- krajowy system ratowniczo-gaśniczy;
- krajowy system elektroenergetyczny;
- krajowy system wykrywania skażeń i alarmowania;
- inne.

Należy zaznaczyć, że przedstawione systemy będą wykorzystywane w zarówno w zarządzaniu kryzysowym jak i w działaniach militarnych. Oczywiście powyższe cele nie będą osiągnięte z dniem utworzenia i wdrożenia koncepcji będzie to długi proces, ale

konieczny, który z perspektywy czasu będzie przynosił namacalne efekty. Należy zwrócić uwagę, że wymienione cele są ze sobą ściśle skorelowane przez co należy rozumieć, że mają one na siebie wpływ bezpośredni oraz pośredni. Rozwinięcie wizji celu pozwoli na dostrzeżenie wspólnych obszarów działania:

Usprawnienie funkcjonowania systemów bezpieczeństwa państwa – jest to element konieczny do prawidłowego, niezakłóconego funkcjonowania państwa polskiego. Tak jak opisano w rozdziale I system ten powinien być cyklicznie aktualizowany i ukierunkowany na nowe zagrożenia tak aby w pełni wykorzystać swój potencjał. Podniesienie skuteczności i efektywności systemów w tym podsystemów pozwoli na wzmocnienie ciągłości działania we wszystkich obszarach bezpieczeństwa państwa.

Zwiększenie bezpieczeństwa obywateli w cyberprzestrzeni – jednym z zadań państwa polskiego jest zwiększanie bezpieczeństwa obywateli w cyberprzestrzeni. Należy przez to rozumieć, że to właśnie państwo poprzez tworzenie regulacji prawnych, procedur, instytucji/podmiotów czy produktów/usług powinno działać na rzecz ochrony obywatela. Krajowy system cyberbezpieczeństwa jako centralny system zrzesza podmioty odpowiedzialne za bezpieczeństwo. Podnoszenie zdolności tego systemu bezpośrednio przełoży się na bezpieczeństwo obywateli. Dodatkowo należy podkreślić istotę bezpieczeństwa produktów ITC gdzie z punktu widzenia technologii jest to dość obszerny temat. Dzieje się tak, ponieważ obejmuje on przestrzeń od tworzenia bezpiecznych już produktów/usług aż po etap życia produktu i wycofania z eksploatacji.

Podnoszenie ogólnej świadomość obywateli o zagrożeniach w cyberprzestrzeni – jak powszechnie wiadomo czynnik ludzki jest najsłabszym elementem w łańcuchu bezpieczeństwa informacji[131]. Biorąc pod uwagę, że bezpieczeństwo informacji w cyberbezpieczeństwie jest kluczowym obszarem to należy dążyć do zwiększania wysiłków na podnoszenie świadomości obywateli o zagrożeniach w cyberprzestrzeni. Bezpieczeństwo obywateli w cyberprzestrzeni można podzielić na dwa kierunki. Pierwszy to ogólnospołeczne uświadamianie obywateli o zagrożeniach wykorzystujących cyberprzestrzeń do realizacji. Drugi to kształtowanie wiedzy osób

[131] Skulska J. 2021, Człowiek jako najsłabsze ogniwo bezpieczeństwa informacyjnego, Nowoczesne Systemy Zarządzania Instytut Organizacji i Zarządzania Zeszyt 16 (2021), nr 1 (styczeń-marzec) ISSN 1896-9380, s. 107.

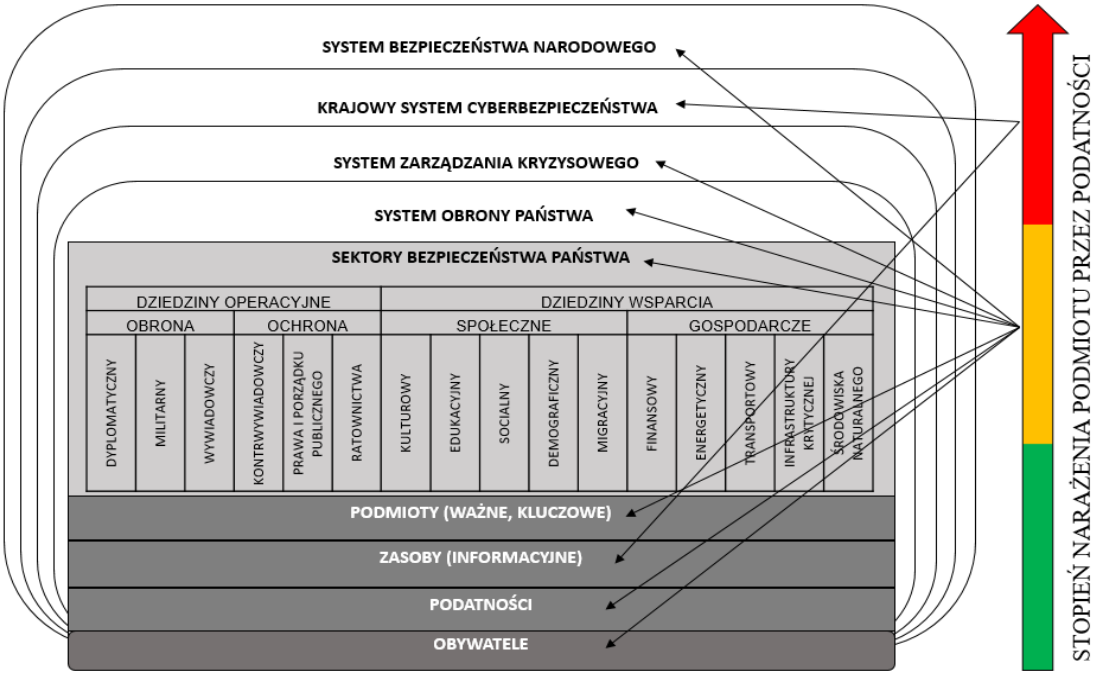
zajmujących stanowiska w administracji państwowej na temat higieny cyfrowej i bezpiecznego przetwarzania danych w zasobach informacyjnych.

Wzmocnienie ochrony zasobów informacyjnych przed nieupoważnionym dostępem – ochrona zasobów informacyjnych jest współcześnie kluczowym zadaniem. Dzieje się tak, ponieważ prawie wszystkie gałęzie gospodarki oraz dziedziny bezpieczeństwa funkcjonują wykorzystując nowoczesne zdobycze techniki oparte na technologiach cyfrowych. Nieuprawniony dostęp do zasobów informacyjnych w systemach teleinformatycznych podmiotów ważnych lub kluczowych może skutkować powstaniem trudno odnawialnych strat. Co gorsze, może nastąpić paraliż tej instytucji w momencie, kiedy będzie ona najbardziej potrzebna np. w okresie zimowym blokada lokalnych zasobów informatycznych elektrowni wchodzącej w skład krajowego systemu elektroenergetycznego.

Utrzymanie ciągłość działania świadczenia usług cyfrowych – współcześnie wszelkie usługi logistyczne w dużej mierze realizowane są poprzez technologie cyfrowe. Doświadczenia z „incydentu estońskiego", konfliktu w Gruzji czy konfliktu na Ukrainie pokazują jak bardzo kluczowe jest utrzymanie ciągłości działania w łańcuchu dostaw. W sytuacjach kryzysowych paraliż systemu finansowego, energetycznego, logistycznego pogłębiany będzie poprzez niespokojne nastroje społeczne wynikające z przerw w dostawach wszelkich dóbr. Należy dążyć do wypracowania alternatywnych procedur, szlaków, podwykonawców tak aby utrzymać ciągłość działania usług z przerwami nie większymi niż zaplanowano.

Zmniejszenie poziomu ogólnokrajowej cyberprzestępczości – tak jak opisano w rozdziale 3 cyberprzestępczość jest rosnącym trendem nie tylko w Polsce, ale i na świecie. Dołożenie starań do budowy narzędzi systemowych jest wskazane po to, aby zatrzymać dalszy rozrost przestępczości tego typu. W obecnym systemie zauważalny jest brak odpowiedniej ilości instytucji oraz sił i środków, aby ten problem zminimalizować lub utrzymać na jednolitym poziomie.

Mając na uwadze kierunek realizacji przedstawionych celów można przedstawić koncepcję poprawy bezpieczeństwa państwa. Model operacyjny (zmodyfikowany) SBN utworzony w podrozdziale 1.6 z naniesionymi wynikami analizy z podrozdziału 4.5 przedstawiono na grafice (Rys. 32). Model prezentuje zestawienie stopnia narażenia podmiotów względem stwierdzonych podatności (zgodnie z kolorami: czerwony największe zagrożenia, zielony najmniejsze).



Rys. 32. Zmodyfikowany model SBN z zidentyfikowanymi obszarami doskonalenia. Źródło: opracowanie własne.

Dla tak zdefiniowanych stopni narażenia systemów/podmiotów/obywateli należy sukcesywnie i skutecznie rozpocząć proces eliminacji stwierdzonych podatności. Zgodnie z rozdziałem IV ustalono pięć obszarów doskonalenia do których należą:

1. Rozbudowa niezbędnej infrastruktury.
2. Pozyskanie wyspecjalizowanej kadry.
3. Zmiana niezbędnych regulacji prawnych.
4. Wstępne koszty utworzenia.
5. Koszty cykliczne utrzymania.

Jako podstawę koncepcji przyjęto identyfikację dostępnych rozwiązań problemu z podaniem argumentów przemawiających za słusznością danego rozwiązania. Całość została poparta analizą SWOT celem zidentyfikowania ukrytych zagrożeń i słabych stron oraz wyeksponowania szans i mocnych stron. Kolejność omawiania działań naprawczych będzie przypadkowa, ponieważ przyjęto założenia, że bez względu na wyniki szacowania ryzyka, eliminacji zostaną poddane wszystkie stwierdzone podatności. Oszacowanie potrzeb obszarów doskonalenia niezbędnych do realizacji koncepcji zostanie zrealizowane w rozdziale VI dotyczącym implementacji. Oczywiście należy mieć świadomość, że na tym etapie nie jest możliwe precyzyjne wyliczenie podanych wskaźników. Z tego też powodu będą to przedziały wartości poparte argumentacją wynikającą z analogicznych zdarzeń i projektów.

5.2. Tworzenie krajowych zdolności technologicznych

Wychodząc naprzeciw problematyce eksploatacji technologii od dostawców zakwalifikowanych jako „dostawcy wysokiego ryzyka" w pierwszej kolejności należy wyjaśnić w czym tkwi sam problem. W projekcie nowelizacji Ustawy o Krajowym Systemie Cyberbezpieczeństwa utworzono instytucję „dostawcy wysokiego ryzyka" jako próbę eliminacji pewnej klasy zagrożeń. Wprowadzenie postępowania administracyjnego mającego na celu uznania podmiotu za dostawcę wysokiego ryzyka uzasadnione jest potrzebą ochrony bezpieczeństwa państwa i porządku publicznego[132]. Postępowanie w sprawie uznania dostawcy za dostawcę wysokiego ryzyka miałoby być wszczynane przez ministra ds. informatyzacji z urzędu lub na wniosek z powodu zaistnienia następujących przesłanek[133]:

1. Zagrożeń bezpieczeństwa narodowego o charakterze ekonomicznym, wywiadowczym i terrorystycznym. Ponadto zagrożeń dla realizacji zobowiązań sojuszniczych i europejskich jakie stanowi dostawca sprzętu i oprogramowania z uwzględnieniem informacji o zagrożeniach uzyskanych od państw członkowskich lub organów UE lub NATO.
2. Prawdopodobieństwa z jakim dostawca sprzętu lub oprogramowania znajduje się pod kontrolą państwa spoza terytorium UE lub NATO.
3. Trybu, zakresu i rodzaju powiązań dostawcy sprzętu lub oprogramowania z podmiotami określonymi w unijnym rozporządzeniu w sprawie środków ograniczających w celu zwalczania cyberataków zagrażającymi Unii lub jej państwom członkowskim.
4. Liczby i rodzajów wykrytych podatności i incydentów dotyczących typów produktów ICT lub rodzajów usług ICT lub konkretnych procesów ICT dostarczanych przez dostawcę sprzętu lub oprogramowania oraz sposobu i czasu ich eliminowania.
5. Trybu i zakresu w jakim dostawca sprzętu lub oprogramowania sprawuje nadzór nad procesem wytwarzania i dostarczania sprzętu lub oprogramowania dla wspomnianych wcześniej podmiotów będących odbiorcami produktów usług lub procesów ICT w szczególności zarządzających infrastrukturą krytyczną.

[132] https://www.parp.gov.pl/component/content/article/85058:krajowy-system-cyberbezpieczenstwa-zmiany-w-funkcjonowaniu-i-ich-wplyw-na-rynek-ict [dostęp: 04.02.2024].
[133] Art. 66a. Projektu ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw.

6. Treści wydanych rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa dotyczących sprzętu lub oprogramowania danego dostawcy.

Opierając się na powyższych przesłankach w projekcie proponuje się wprowadzenie mechanizmu pozwalającego na uznanie określonego dostawcy sprzętu lub oprogramowania dla szczególnego rodzaju podmiotów gospodarczych i społecznych za dostawcę wysokiego ryzyka. Oczywiście, przedstawiony opis jest procesem uznania podmiotu za dostawcę wysokiego ryzyka. Natomiast zgodnie z ujętą słabością w kręgu zainteresowań pozostają takie podatności jak „Backdoor" czyli tworzenie celowych „furtek" w oprogramowaniu (Hardware, Software) pozwalających na nieuprawniony dostęp do systemu przez nieautoryzowane podmioty. Należy zdawać sobie sprawę, że obecnie choćby tylko infrastrukturze krytycznej działa wiele produktów od producentów, którzy w niedalekiej przyszłości na podstawie zapisów ustawowych zostaną uznani właśnie za takich dostawców. Pomimo że oficjalnie jeszcze przepisy te nie weszły w życie (ma to nastąpić w drugiej połowie 2025 roku) to należy uznać, że dalsza eksploatacja tych systemów jest wysoce ryzykowna.

Jako rozwiązanie tego problemu zalecane jest zinwentaryzowanie i zidentyfikowanie w infrastrukturze krytycznej (docelowo w pozostałych gałęziach) wszelkich niezbędnych do należytego jej funkcjonowania systemów pochodzących od producentów uznanych za dostawców wysokiego ryzyka i zastąpienie ich zaufanymi produktami. W tym miejscu pojawiają się pewne ograniczenia mianowicie dostępność technologii uznawanej za względnie bezpiecznej. Jednym z rozwiązań jest zdobywanie technologii od tak zwanej „zaufanej strony trzeciej tylko kto ma nią być, skoro nasz największy sojusznik (USA) jest w ścisłej czołówce państw źródeł ataków? Tak przedstawiony problem wymusza wdrożenia tylko jednego rozwiązania mianowicie utworzenia własnych krajowych zdolności technologicznych i sukcesywne zastępowanie „obcych" systemów. Aby to zrealizować, w pierwszej kolejności należałoby przeanalizować krajowe zdolności. Mowa tu o środowisku akademickim i wyszczególnieniu instytutów, katedr i zakładów specjalizujących się w informatyce, automatyce i cybernetyce. Wówczas można byłoby utworzyć organ mający właściwości konsorcjum dofinansowane przez państwo celem prowadzenia badań wdrożeniowych, mających na celu zastąpienie systemów nową sprawdzoną technologią. Przedmiotowe rozwiązanie z punktu widzenia zdolności jest osiągalne. Należy wsiąść pod uwagę, że

Polska myśl techniczna jest ceniona w świecie a Polscy inżynierowie uznawani za solidnie wykształconych, często zajmujących kluczowe stanowiska w korporacjach technologicznych na całym świecie. Jako kraj posiadamy odpowiednie kwalifikacje oraz zasoby i potencjał, aby prowadzić badania w tym zakresie i być samowystarczalnymi. Cały projekt wraz z wykonaniem wiąże się z nakładami finansowymi oraz czasem potrzebnym na prowadzenie badań i testowaniem technologii. Jednakże za systemy kupowane z innych źródeł też musimy zapłacić często zawyżone ceny z tytułu zakupy u monopolisty. W celu zweryfikowania zasadności proponowanego rozwiązania, propozycje poddano analizie SWOT (Tab. 19).

Tab. 19. Analiza SWOT utworzenia konsorcjum badawczo-wdrożeniowego.

WEWNĘTRZNE			ZEWNĘTRZNE		
kod	1 - niski 2 - średni 3 - wysoki	MOCNE STRONY (S)	kod	1 - niski 2 - średni 3 - wysoki	SZANSE (O)
S1	3	• duży poziom bezpieczeństwa systemów	O1	2	• unikatowe rozwiązania - pozyskanie rozwojowej technologii będącej konkurencyjną w przyszłości
S2	2	• zmniejszony problem z serwisem i naprawami przez krajowe firmy			
S3	3	• uniezależnienie technologiczne	O2	2	• rozwój krajowej myśli technicznej
S4	1	• zmniejszone koszty utrzymania	O3	1	• dofinansowanie wybranych uczelni
S5	1	• zdobywanie wiedzy i doświadczenia	O4	1	• umacnianie krajowej gospodarki
5	10	*SUMA*	4	6	*SUMA*
kod	1 – niski 2 - średni 3 - wysoki	SŁABE STRONY (W)	kod	1 - niski 2 - średni 3 - wysoki	ZAGROŻENIA (Z)
W1	2	• względnie długi okres oczekiwania na wdrożenie rozwiązań	Z1	2	• brak wiedzy i doświadczenia na temat rozwiązań konstrukcyjnych
W2	1	• brak doświadczenia przy projektowaniu podobnych urządzeń			
2	3	*SUMA*	1	2	*SUMA*

Źródło: opracowanie własne.

Na podstawie analizy SWOT wyłoniono jako dominujące kategorie zarówno mocne strony jak i szanse. W związku z czym można uznać propozycję utworzenia konsorcjum technologicznego składającego się z odpowiednich instytucji jako zasadną i niegenerującą dodatkowych zagrożeń. Proponowane rozwiązanie w postaci stworzenia warunków do projektowania, produkcji i wdrażania własnej myśli technologicznej jest korzystną alternatywą wobec nabywania technologii od dostawców wysokiego ryzyka lub zastępowania ich produktami zaufanej strony trzeciej. Podstawowym a zarazem najważniejszym parametrem jest zapewnienie bezpieczeństwa na wymaganym poziomie co pozwoli uzyskać tylko własna technologia. Ponadto nie bez znaczenia jest utrzymywanie rozwoju technologii w kraju. Jest to istotne, ponieważ przełoży się na

wsparcie gospodarki wzbogacenie doświadczenia oraz rozwoju dziedzin nauki i co najważniejsze uniezależni krajowy przemysł i infrastrukturę krytyczną od dostawców wysokiego ryzyka. Wdrożenie w życie i uzyskanie własnych (krajowych) zdolności wytwarzania kluczowych systemów i produktów ITC pozwoli na zwiększenie bezpieczeństwa w newralgicznych sieciach teleinformatycznych wykorzystywanych w niemal całym systemie bezpieczeństwa państwa.

5.3. Wzmocnienie roli cyberbezpieczeństwa na poziomie strategii

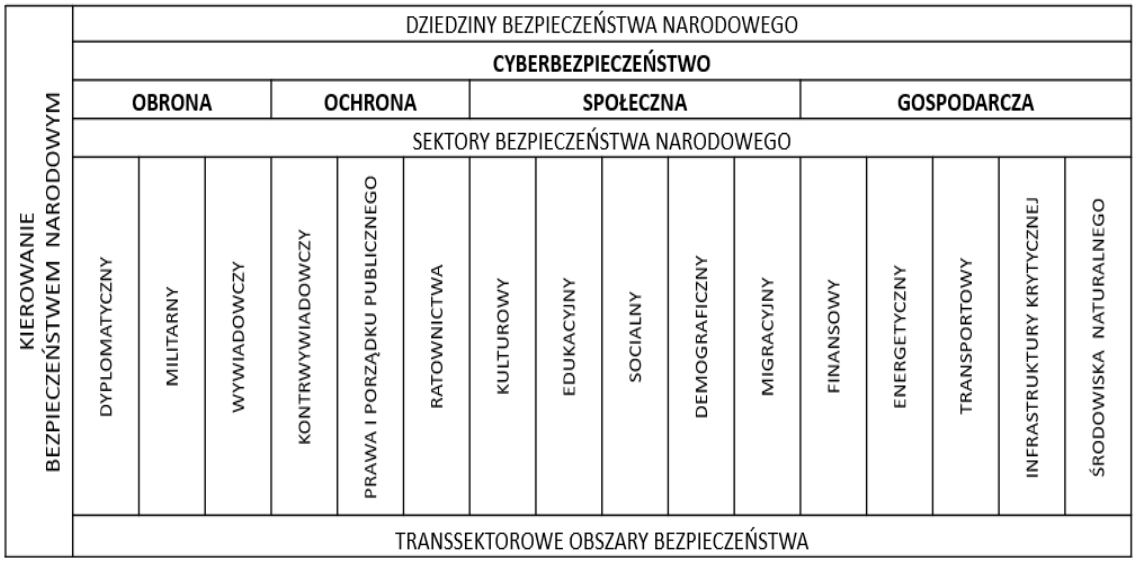
Podstawą niektórych podatności są zdezaktualizowane dokumenty poziomu strategicznego. Nowelizacja Strategii Rozwoju Systemu Bezpieczeństwa Narodowego powinna nastąpić jak najszybciej, ponieważ jak przewidywali jej autorzy jest to dokument obowiązujący przez 10 lat, a więc do końca 2023 roku. W związku z czym w celu utrzymania płynnego przejścia pomiędzy poziomem dokumentów (Rys 33.) należy zadbać o ich terminową aktualizację.

Rys. 33. Miejsce SR SBN RP w hierarchii dokumentów strategicznych.
Źródło: Strategia Rozwoju Systemu Bezpieczeństwa Narodowego. s. 6.

Strategia SR SBN bezpośrednio podległa pod strategię SBN i powinna zachować utrzymanie roli i rangi cyberbezpieczeństwa tak jak to zostało wyeksponowane w znowelizowanej Strategii Bezpieczeństwa Narodowego z 2020 roku. Zmiany jakie nastąpiły w strategii w pełni wpisują się w potrzeby wyłonione na podstawie analizy dokumentów, której wyniki przedstawiono w niniejszej rozprawie (rozdz. III). Zmiany te spełniają wymogi odpowiedniej ekspozycji przedmiotowego cyberbezpieczeństwa

jako kluczowego czynnika bezpieczeństwa[134]. Ponadto zwrócono uwagę, że wrogie podmioty coraz częściej wykorzystują dezinformację do wpływania na opinię publiczną. Dodatkowo został położony nacisk na uświadamianie społeczne o zagrożeniach cyberprzestrzeni oraz na rozwijaniu krajowych zdolności w obszarze testowania, badania, oceny i certyfikacji rozwiązań i usług z obszaru cyberbezpieczeństwa. W przeciwieństwie do wyższego szczebla Strategia Rozwoju Systemu Bezpieczeństwa Narodowego zawiera zapisy które informują, że w zestawieniu dokumentów wdrożeniowych SRSBN RP wykorzystywana była Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej z 2013 roku. Dokument ten został zastąpiony przez Krajowe Ramy Polityki Cyberbezpieczeństwa RP w 2017 roku. Świadczy to o tym, że strategia powołuje się na nieaktualne zapisy i dokumenty, które są wręcz kluczowe dla omawianej problematyki. Mało tego jako główne działania z zakresu cyberbezpieczeństwa strategia wskazuje przyjęcie do użytku tejże Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej[135] a przecież od 2018 roku obowiązuje Strategia Cyberbezpieczeństwa[136], która również straciła swą moc w 2024 roku. W związku z czym strategia SR SNB w stosunku do strategii SBN nie ma nic wspólnego z płynnością utrzymania cyberbezpieczeństwa. Dodatkowo w celu 4 przedmiotowej strategii nawiązującej do „Zwiększenia integracji polityk publicznych z polityką bezpieczeństwa" nie ma mowy o żadnym dokumencie odnoszącym się do cyberbezpieczeństwa a przecież strategia SBN jasno wskazuje tą dziedzinę jako główny współczesny kierunek zagrożeń. W związku z powyższym należy uznać, że dokument wyższego szczebla tj. strategia SBN na wysokim poziomie eksponuję rolę i rangę cyberbezpieczeństwa natomiast dokument niższego szczebla SR SBN (Rys. 23) niweluje te działania niemalże całkowicie, marginalizując sprawę. Z tego też powodu należy zaktualizować dokument z odpowiednim wyeksponowaniem roli i rangi cyberbezpieczeństwa. Potrzeba zmiany SR SBN jest oczywista, ponieważ na podstawie tej strategii będą budowane inne dokumenty niższego szczebla więc błędy będą powielane. W aktualizacji strategii SR SNB należy przede wszystkim zmienić rangę transsektorowego cyberbezpieczeństwa na ponaddziedzinową co w przełożeniu na schemat użyty w Białej Księdze[137] będzie przedstawiał się jak na (Rys. 34).

[134] Strategia Bezpieczeństwa Narodowego RP 2020. s. 20.
[135] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022. s. 20
[136] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.
[137] Biała Księga Bezpieczeństwa Narodowego RP. s. 19.



Rys. 34. Propozycja podniesienia rangi cyberbezpieczeństwa w Systemie Bezpieczeństwa Narodowego. Źródło opracowanie własne na podstawie Strategii Rozwoju Systemu Bezpieczeństwa Narodowego 2013.

Działania takie pozwolą o dbałość na pierwszym miejscu o cyberbezpieczeństwo niezależnie od dziedziny czy sektora bezpieczeństwa.

Tab. 20. Powiązanie SR SBN RP z zintegrowanymi strategiami.

SR SBN RP	Zintegrowane strategie rozwoju								inne
CELE	Strategia innowacyjności i efektywności gospodarki	Strategia rozwoju kapitału ludzkiego	Strategia rozwoju transportu	Bezpieczeństwo energetyczne i środowisko	Sprawne Państwo	Strategia rozwoju kapitału społecznego	Krajowa strategia rozwoju regionalnego	Strategia zrównoważonego rozwoju wsi, rolnictwa i rybactwa	**Strategia Cyberbezpieczeństwa RP**
Kształtowanie stabilnego międzynarodowego środowiska bezpieczeństwa	X		X	X	X	X			**X**
Umocnienie zdolności państwa do obrony	X	X			X	X			**X**
Rozwój odporności na zagrożenia bezpieczeństwa narodowego			X	X	X			X	**X**
Zwiększenie integracji polityk publicznych z polityką bezpieczeństwa			X	X	X	X	X		**X**
Tworzenie warunków do rozwoju zintegrowanego systemu bezpieczeństwa narodowego					X				**X**

Źródło: Opracowanie własne na podstawie SR SBN RP[138].

Istotnym etapem tworzenia obecnej strategii było ukierunkowanie jej na zgodność ze Zintegrowanymi Strategiami Rozwoju. Oczywiście powinno być na odwrót, ale biorąc pod uwagę, że strategie ZSR są przewidywane na dłuższy okres to nie ma możliwości ich zmiany, a jedynym rozwiązaniem skorelowania ich jest dopasowanie poprzez treść SR SBN. W związku z powyższym schemat powiązań pomiędzy przedmiotowymi dokumentami powinien być jak na (Tab. 20). Godnym uwagi jest fakt,

[138] Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022. s. 9.

że w obecnej chwili dokumenty strategiczne Zintegrowanych Strategii Rozwoju w swej treści wskazują cyberbezpieczeństwo jako kluczowe ogniwo ich działalności, przy czym nie mają nawiązania do żadnego dokumentu powiązanego z cyberbezpieczeństwem. Na podstawie przedstawionych argumentów propozycja uporządkowania treści strategii została poddana analizie SWOT (Tab. 21.).

Tab. 21. Analiza SWOT ujednolicenia dokumentów szczebla strategicznego.

WEWNĘTRZNE			ZEWNĘTRZNE		
kod	1 - niski 2 - średni 3 - wysoki	MOCNE STRONY (S)	kod	1 - niski 2 - średni 3 - wysoki	SZANSE (O)
S1 S2 S3 S4	3 2 2 1	• zwiększenie rangi cyberbezpieczeństwa • integracja strategii różnego szczebla • zachowanie hierarchii zagrożeń w dokumentach • Spowodowanie, że nie zostanie utracona ciągłość przepływu informacji między szczeblami dokumentów	O1 O2	2 2	• zwiększenie świadomości na postrzeganie zagrożeń w cyberprzestrzeni • dokumenty niższego szczebla będą również mocniej akcentowały rangę cyberbezpieczeństwa
4	8	*SUMA*	2	4	*SUMA*
kod	1 – niski 2 - średni 3 - wysoki	SŁABE STRONY (W)	kod	1 - niski 2 - średni 3 - wysoki	ZAGROŻENIA (Z)
W1	2	• postępowanie odwrotne tj. dopasowanie głównego dokumentu do strategii, gdzie powinno się dopasować strategię do głównego dokumentu			
1	2	*SUMA*	0	0	*SUMA*

Źródło: Opracowanie własne.

Analiza SWOT pokazała, że zarówno mocne strony jak i szanse są dominujące. Nie stwierdzono zagrożeń w związku z czym należy uznać propozycję ujednolicenia roli i rangi cyberbezpieczeństwa w strategiach jako słuszną.

Konkluzja jaka płynie z ujednolicenia rangi cyberbezpieczeństwa jest następująca. Strategia Bezpieczeństwa Narodowego jest dokumentem wyższego szczebla, który w sposób należyty oraz oczekiwany uwzględnia i eksponuje zagrożenia w cyberprzestrzeni. Wskazane jest, aby dokument niższego szczebla jakim jest Strategia Rozwoju Systemu Bezpieczeństwa Narodowego utrzymał rangę znaczenia cyberprzestrzeni podczas wytyczania kierunków rozwoju Systemu Bezpieczeństwa Narodowego co pozwoli zachować płynność istoty zagrożeń pomiędzy dokumentami różnego szczebla. Nie ulega wątpliwości, że SR SBN musi zostać jak najszybciej zaktualizowana, ponieważ tak ważny system jakim jest System Bezpieczeństwa Narodowego powinien być cyklicznie i terminowo unowocześniany otwierając się na nowe lub zmienione trendy w działaniach wrogich podmiotów.

5.3.1. Regulacje w sprawie centrów wymiany i analizy informacji (ISAC)

W rozdziale pierwszym została poruszona kwestia centrów wymiany i analizy informacji, gdzie opisywane były rozwiązania cyberbezpieczeństwa stosowane w innych państwach. Na uwagę zasługuje rozwiązanie tego problemu stosowane w Stanach Zjednoczonych Ameryki, które regulują prawnie działalność tych centrów oraz zhierarchizowały te instytucje. Skoro funkcjonują one w USA bez większych problemów to nic nie stoi na przeszkodzie, aby zapożyczyć te rozwiązania i zastosować w kraju. Zgodnie ze statutem tych instytucji ISAC to centra wymiany wiedzy i doświadczeń dotyczących incydentów cyberbezpieczeństwa w danym sektorze gospodarki[139]. Organizacje mają wspólny cel niezależnie od obszaru prawnego ich działania. Wiąże się to również z znaczeniem funkcjonalnym więc dostosowanie przepisów amerykańskich nie powinno stanowić większej przeszkody do wdrożenia. ISAC z założenia są to organizacje typu partnerstwa publiczno-prywatnego (PPP), które bardzo dobrze sprawdzają się zwłaszcza w obszarze cyberbezpieczeństwa. Wartą uwagi jest informacja, że z założenia przedmiotowe centra nie są formalnie finansowane co oznacza konieczność zastanowienia się na jakie zasadzie one funkcjonują, skoro nie otrzymują żadnych dochodów. Pytanie jest o tyle poważne, że należy się zastanowić, czy jeżeli zgłosi się do tej organizacji sponsor lobbujący pewne zachowania to czy nie będzie to stanowiło pokusy wobec braku alternatywnych źródeł finansowania. W związku z czym, jeżeli proponowane ISAC w projekcie nowelizacji ustawy o KSC zakłada współpracę typu PPP to należy w jakiś sposób rozważyć ich utrzymanie przynajmniej na poziomie samych podstawowych wydatków tak aby wykluczyć prawdopodobieństwo ingerencji tak zwanych „sponsorów wysokiego ryzyka" w ich działalność. Rozwiązaniem problemu może być utworzenie wiodącego ISAC na wzór National Council of ISACs (NCI z USA[140]) czyli organizacji naczelnej, która zrzesza podległe organizacje i sprawuje funkcje koordynująco-kontrolną. Wiodący ISAC w takim przypadku musi być w pełni lub częściowo dotowany przez państwo celem sprawowania nadzoru nad podległymi organizacjami, które mogą utrzymywać się z datków za swoją działalności. Pomysł został poddany analizie SWOT (Tab. 22) celem wyłonienia ewentualnych zagrożeń jakie mogą zaistnieć.

[139] https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Poradnik-NASK-na-temat-tworzenia-ISAC.pdf [dostęp: 28.05.2024].
[140] https://www.nationalisacs.org/ [dostęp: 03.02.2024].

Tab. 22. Analiza SWOT zhierarchizowania ISAC.

WEWNĘTRZNE			ZEWNĘTRZNE		
kod	1 - niski 2 - średni 3 - wysoki	MOCNE STRONY (S)	kod	1 - niski 2 - średni 3 - wysoki	SZANSE (O)
S1 S2 S3 S4	3 1 2 2	• zwiększenie kontroli w ISAC • ustrukturyzowanie ISAC • transparentne zasady finansowania • możliwość kierowania odgórnie każdym poszczególnym ISAC	O1 O2	2 2	• wprowadzenie zdrowej rywalizacji zamiast konkurencyjności wśród ISAC • wspólne szkolenia, większa wymiana wiedzy i doświadczeń • możliwość migracji specjalistów między poszczególnymi centrami
4	8	*SUMA*	2	4	*SUMA*
kod	1 - niski 2 - średni 3 - wysoki	SŁABE STRONY (W)	kod	1 - niski 2 - średni 3 - wysoki	ZAGROŻENIA (Z)
W1	3	• Koszty związane z utrzymaniem wiodącego ISAC			
1	3	*SUMA*	0	0	*SUMA*

Źródło: Opracowanie własne.

Przeprowadzona w tym przypadku analiza pozwoliła wyłonić mocne strony i szanse jako dominujące, przy czym nie stwierdzono zagrożeń. Słabą stroną jest finansowanie. Należy więc uznać zhierarchizowanie centrów ISAC za właściwy pomysł jako eliminację stwierdzonej luki. Konkluzja jest następująca: Centra powstaną niezależnie od przedmiotowej koncepcji. Należy jednak zauważyć, że w przypadku tworzenia tak specyficznych instytucji co jest w Polsce swego rodzaju nowością zasadne jest wspieranie się sprawdzonymi i dobrze funkcjonującymi rozwiązaniami. Jak pokazuje historia ewentualne zmiany w toku funkcjonowania pociągają dodatkowe koszty oraz generują nieznane problemy w związku z czym należy poważnie przeanalizować zhierarchizowanie centrów zanim powstaną.

5.3.2. Narodowy, długoterminowy program uświadamiania społecznego

Pożądany jest pomysł, który rozwiąże problem niskiej współpracy pomiędzy instytucjami oraz zwiększy poziom zainteresowania wdrażaniem dokumentacji dotyczącej cyberbezpieczeństwa. Taki stan można osiągnąć tylko poprzez szkolenie i uświadamianie pracowników administracji państwowej o istocie problematyki zagrożeń w cyberprzestrzeni. Zidentyfikowane i opisane w rozdziale III sposoby realizacji zagrożeń w głównej mierze wykorzystują błędy ludzkie a wszelkie sposoby socjotechniki ukierunkowane są na słabości oraz brak odpowiedniej wiedzy. Dlatego celem minimalizacji zagrożeń kluczowe jest podniesienie świadomości całego społeczeństwa.

Wyszklony pracownik to taki, który ma wiedzę o zagrożeniach i nie unika działań mających na celu poprawę bezpieczeństwa zarówno własnego jak i instytucji, w której pracuje/służy. Warto podkreślić, że już istnieją kampanie cyberbezpieczeństwa[141], które obecnie możemy zaobserwować we wszystkich massmediach. Jednak jak pokazują statystyki nadal ogromna liczba osób jest podatna na oszustwa komputerowe, socjotechnikę, propagandę czy to co jest już globalnym problemem – dezinformację. Miejscem, w którym uczy się ludzi jest oczywiście szkoła trzeba mieć jednak świadomość, że część społeczeństwa dawno temu zakończyła edukację w związku z czym zachodzi konieczność sięgnięcia po inne metody. Innym miejscem, w którym ludzie się szkolą jest ich praca. Każdy pracownik przed objęciem stanowiska pracy musi przejść 8 godzinne szkolenie BHP. Jest to warunek konieczny, przy czym raz na 4 lata zachodzi potrzeba ponownego podejścia do jednodniowego kursu i zaliczenia egzaminu z tej tematyki. Pomysłem, który może wyjść naprzeciw zaistniałej sytuacji w cyberbezpieczeństwie jest obowiązkowe szkolenie z podstaw higieny cyfrowej. Rozwiązane to wymaga odpowiednich regulacji prawnych oraz akceptacji środowiska pracodawców, ale biorąc pod uwagę szczytność zakładanego celu nie przewiduje się w tym problemu.

Tab. 23. Harmonogram 8 godzinnego szkolenia.

Lp.	Temat zajęć	czas
1	wprowadzenie z przedstawieniem regulacji oraz sankcji prawnych	1 godz.
2	omówienie zagrożeń - „ransomware” oparte na przykładach (studium przypadków) wraz z sposobami ochrony	1 godz.
3	omówienie zagrożeń - „malware” oparte na przykładach (studium przypadków) wraz z sposobami ochrony	1 godz.
4	omówienie zagrożeń - „phishing”, oparte na przykładach (studium przypadków) wraz z sposobami ochrony	1 godz.
5	omówienie zagrożeń - „socjotechniki” oparte na przykładach (studium przypadków) wraz z sposobami ochrony	1 godz.
6	przedstawienie ogólnodostępnych statystyk cyberzagrożeń wraz z omówieniem statystyki dotyczące oszustw komputerowych, wyłudzeń, szyfrowania danych	1 godz.
7	zapoznanie i zachęcenie do stosowania dobrych praktyk polegających na stosowaniu menadżera haseł, silnych haseł, częstych zmian haseł, zapoznania z polityką bezp.	1 godz.
8	test wiedzy zakończony zaliczeniem lub nie	1 godz.

Źródło: Opracowanie własne.

To właśnie pracodawcy biorąc pod uwagę własny interes mogą dążyć do takiej formy nauczania a ponieważ przełoży się to na jakość współpracy w zakresie cyberbezpieczeństwa. Propozycja wprowadzenia obowiązkowego szkolenia powinna

[141] Kampanie prowadzone są za pomocą plakatów, filmów wideo, animacji, klipów, poradników oraz reportaży.

w swym zakresie obejmować podstawową ogólnodostępną wiedzę na temat sposobów, technik i metod realizacji zagrożeń w cyberprzestrzeni. Przykładowy plan szkolenia został zamieszczony w tabeli 23. Pozostaje problem kto miałby prowadzić to szkolenie. W większych organizacjach występują funkcje inspektora bezpieczeństwa teleinformatycznego lub informatyków, gdzie nie stanowi to problemu. W małych firmach za szkolenie odpowiadałby pracodawca lub wyznaczony przez niego pracownik. Program szkolenia[142] byłby ogólnodostępny na stronach Ministerstwa Cyfryzacji co rozwiązałoby problem dystrybucji materiałów szkoleniowych. Wyniki analizy SWOT przedmiotowej propozycji są prezentowane w tabeli 24.

Tab. 24. Analiza SWOT propozycji obowiązkowego szkolenia z higieny cyfrowej.

WEWNĘTRZNE			ZEWNĘTRZNE		
kod	1 - niski 2 - średni 3 - wysoki	MOCNE STRONY (S)	kod	1 - niski 2 - średni 3 - wysoki	SZANSE (O)
S1	3	• masowe zwiększenie cyberbezpieczeństwa w firmach i organizacjach	O1	3	• Uchronienie pracowników przed byciem ofiarą oszustwa
S2	2	• podnoszenie przez pracodawców kwalifikacji i stanu wiedzy pracowników	O2	3	• coraz bardziej świadome zagrożeń społeczeństwo
S3	2	• zmniejszanie ryzyka utraty ICD w organizacji	O3	3	• obniżenie trendu oszustw komputerowych i innych zagrożeń
3	7	*SUMA*	3	9	*SUMA*
kod	1 - niski 2 - średni 3 - wysoki	SŁABE STRONY (W)	kod	1 - niski 2 - średni 3 - wysoki	ZAGROŻENIA (Z)
W1	2	• brak wyszkolonych osób do prowadzenia szkolenia w małych firmach	Z1	2	• Pracodawcy małych firm nie będą się stosowali do szkolenia
1	2	*SUMA*	1	2	*SUMA*

Źródło: Opracowanie własne.

Dokonana analiza również i w tym przypadku wskazuje mocne strony i szanse jako dominujące. Konkluzja jest następująca: system szkolenia w postaci 8 godzinnego obowiązkowego kursu raz w roku w znacznym stopniu poprawi bezpieczeństwo teleinformatyczne w miejscach pracy a to z kolei przełoży się na jakość współpracy między podmiotami. Metoda pozwoli na systematyczne uświadamianie społeczeństwa (ludzi pracujących na etacie) w przedziale wiekowym 18-65 lat. Program szkoleniowy byłby ogólnie dostępny, przy czym do samego programu stworzono by metodyczne instrukcje nauczania. Tak zrealizowane szkolenie prawdopodobnie przyniesie lepsze

[142] Program szkolenia składałby się z instrukcji, opisu metodyki oraz samych treści szkoleniowych, których wdrożenie nie stanowiłoby większego problemu.

efekty niż obecne kampanie cyberbezpieczeństwa. Z czasem poziom wyszkolenia pracowników w administracji państwowej osiągnie etap, w który współpraca i wymiana informacji na temat zagrożeń w cyberprzestrzeni nie będzie stanowiła problemu.

5.3.3. Narodowy długoterminowy program szkolnictwa ustawowego.

Zgodnie z przysłowiem „Czego Jaś się nie nauczy tego Jan nie będzie umiał". Szkolenie uczniów w wieku wczesnoszkolnym jest jak najbardziej wskazane. Biorąc pod uwagę, że obecnie dzieci wczesnoszkolne są przypisywane do klas o profilu np.: matematycznym, programistycznym, algorytmicznym to nic nie stoi na przeszkodzie, aby w tym wieku wprowadzić obowiązkowy przedmiot bezpieczeństwa korzystania z sieci. Należy mieć świadomość, że jest to wiek, w którym dzieci zaczynają eksplorację Internetu co w przypadku braku nadzoru stanowi zagrożenie. Problem jest o tyle poważny, że dzieci pozostawione samym sobie z technologią cyfrową czerpią wiedzę i inspiracje z sieci co samo w sobie nie jest złą praktyką natomiast treści umieszczane w Internecie pozostawiają wiele do życzenia. W odróżnieniu od zaproponowanego szkolenia dla dorosłych dzieci powinny być ukierunkowane w sposób ciągły a przedmiotem jaki powinien być wprowadzony jest przykładowo higiena cyfrowa. Przedmiot ten powinien być wprowadzeniem do zajęć informatycznych oraz ich uzupełnieniem. Nacisk kładziony powinien być na wyrobienie u dzieci prawidłowych nawyków (wzorców) zachowania w sieci. Ponadto należy poruszyć tematykę nie tylko zasad bezpiecznego korzystania z Internetu, ale również uczniowie powinni być zapoznawani z zjawiskami takimi jak socjotechnika, Fakenews, Deepfake oraz wszelkie konsekwencje „hejtu" w sieci. Jako porównanie pomysłu do obecnego toku nauczania może służyć fakt, że dzieci w tym wieku uczone są zasad i przepisów ruchu drogowego na przedmiocie takim jak technika więc nic nie stoi na przeszkodzie, aby uczyć ich zasad korzystania z Internetu na przedmiocie z Informatyki. Proponowany pomysł został poddany analizie SWOT - zobacz tab. 25.

Wyniki analizy jednoznacznie wskazują, że szanse i mocne strony definitywnie przeważają słabe strony nie generując zagrożeń. W związku z czym propozycja wprowadzenia dodatkowego przedmiotu jakim będzie higiena cyfrowa jest jak najbardziej zasadna.

Tab. 25. Analiza SWOT wprowadzenia wczesnoszkolnego przedmiotu higiena cyfrowa.

WEWNĘTRZNE			ZEWNĘTRZNE		
kod	1 - niski 2 - średni 3 - wysoki	MOCNE STRONY (S)	kod	1 - niski 2 - średni 3 - wysoki	SZANSE (O)
S1 S2 S3	2 2 2	• masowe zwiększenie cyberbezpieczeństwa w najmłodszych użytkowników sieci • wsparcie rodziców w wychowaniu w reżimie cyfrowym • wsparcie w innych zakresach bezpieczeństwa dzieci takich np. jak ochrona nieletnich w sieci	O1 O2 O3	2 2 2	• zwiększenie świadomości młodego pokolenia będzie przynosiło profity w przyszłości • zmniejszenie statystyk wykorzystywania nieletnich w sieci • zmniejszenie liczby pacjentów placówek leczenia uzależnień od Internetu
3	6	*SUMA*	3	6	*SUMA*
kod	1 - niski 2 - średni 3 - wysoki	SŁABE STRONY (W)	kod	1 - niski 2 - średni 3 - wysoki	ZAGROŻENIA (Z)
W1	2	• Przygotowanie kadry nauczycielskiej na nowy przedmiot			
1	2	*SUMA*	0	0	*SUMA*

Źródło: Opracowanie własne.

Kształcenie dzieci w ramach dodatkowego przedmiotu edukacji wczesnoszkolnej nie wnosi żadnych dodatkowych obciążeń ze strony środowiska szkolnego, ponieważ prawie każda szkoła zatrudnia nauczycieli od informatyki. Pomysł ten w połączeniu z propozycją szkolenia dorosłych ludzi z zakresu cyberbezpieczeństwa omawiany w poprzednim podrozdziale powoduje, że niemal cały przekrój społeczeństwa będzie podlegała uświadamianiu wykluczając jedynie emerytów, rencistów oraz bezrobotnych.

5.4. Zwiększenie liczby instytucji odpowiedzialnych za cyberbezpieczeństwo

Projekt koncepcyjny poprawy bezpieczeństwa zakłada utworzenie organów i instytucji, które będą podnosiły poziom krajowego cyberbezpieczeństwa. Przy tworzeniu projektu wymagane są rozważania nad rozbudową biura CBZC i utworzeniu instytucji odpowiedzialnej za dezinformację oraz powołaniem Operatora Strategicznej Sieci Bezpieczeństwa. Wiąże się to z olbrzymimi nakładami zarówno finansowymi, potrzebami kadrowymi oraz rozbudową istniejących instytucji. W większości proponowanych rozwiązań zarówno nakłady finansowe jak i stan osobowy może okazać się trudny do oszacowania. W związku z czym w pierwszej kolejności założono wykorzystanie obecnych zdolności państwa w tym zakresie. Przedstawione rozwiązania będą jedynie propozycjami, które są konieczne do prawidłowego funkcjonowania państwa i w istocie projektu koncepcyjnego zakłada się, że personel oraz środki finansowe są wystarczające do tego, aby można było wprowadzić przedmiotowe

rozwiązania. Pozyskanie środków finansowych oraz wyspecjalizowanych kadr zostanie poddane wnikliwej analizie w końcowym etapie rozdziału**.**

5.4.1. Tworzenie instytucji Operatora Strategicznej Sieci Bezpieczeństwa

Strategiczna Sieć Bezpieczeństwa jest pomysłem, który tworzony jest od 2018 roku a jego zalążki stanowiły projekty o kryptonimach „KWARC" i „CATEL". Miały to być systemy niejawnej łączności mobilnej i stacjonarnej dedykowane dla łączności rządowej. Obecna (kolejna) wersja nowelizacji ustawy o KSC (grudzień 2024) odrzuciła projekt OSSB. Niemniej jednak z punktu widzenia bezpieczeństwa państwa sieć łączności rządowej jest jak najbardziej konieczna i w końcu będzie musiała być zrealizowana. Wobec czego należy rozważyć czy w obecnej formie projektu OSSB i jego realizacja dla tak newralgicznej sieci jest zasadna. Zakłada się, że Operator Strategicznej Sieci Bezpieczeństwa będzie wyznaczany w drodze zarządzenia przez Prezesa Rady Ministrów spośród podmiotów spełniających łącznie następujące warunki[143]:

- będących jednoosobową spółką Skarbu Państwa;
- będących przedsiębiorcą telekomunikacyjnym;
- posiadających infrastrukturę telekomunikacyjną niezbędną do realizacji zadań;
- posiadających środki techniczne i organizacyjne zapewniające bezpieczne przetwarzanie danych w sieci telekomunikacyjnej;
- posiadających świadectwo bezpieczeństwa przemysłowego.

Wobec powyższego jako OSSB będzie wybrana jedna z obecnych już spółek, która przekształci się w konsorcjum. Spółka będzie świadczyła usługi w zakresie[144]:

- oferowania odpłatnych usług telekomunikacyjnych na warunkach hurtowych;
- udostępniania odpłatnie usług telekomunikacyjnych na rzecz OSSB, w celu świadczenia przez niego usług telekomunikacyjnych i innych usług służących zapewnieniu realizacji zadań na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego;

[143] https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa [dostęp: 04.02.2024].

[144] https://www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-telekomunikacyjne-poprzedni-tytul-projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-ustawy-prawo-telekomunikacyjne-oraz-ustawy-ordynacja-podatkowa2 [dostęp: 06.02.2024].

- zapewnienia pokrycia całego terytorium kraju zasięgiem sieci hurtowej oraz zapewnienia szczególnego poziomu bezpieczeństwa w interesie publicznym, w zakresie sieci oraz usług.

W związku z powyższym zachodzą pewne wątpliwości, które można wyrazić za pomocą następujących pytań:

1. Czy spółka wyłoniona jako jedna z obecnie działających na polskim ryku, która nabędzie tak wielkie uprawnienia nie będzie kuszona, aby je wykorzystać do nieczystej rywalizacji z konkurencją w swojej działalności komercyjnej (niezwiązanej z OSSB)?
2. Czy jednoosobowa spółka nie sprawi podejrzenia jako podatnej na upolitycznienie lub lobbowanie w jakimś kierunku?
3. Czy musi to być spółka Skarbu Państwa?
4. Jak bardzo musi być rozbudowana infrastruktura spółki, skoro projekt zakłada utworzenie 330 masztów przeznaczonych pod OSSB?

Odpowiedź nr 1. na tak postawione pytanie można odpowiedzieć zapisem, że spółka ta w chwili stania się OSSB traci możliwość działalności komercyjnej co zwiększy jej bezpieczeństwo jak strategicznego operatora. Pytanie kolejne jakie się rodzi czy istnieje spółka na polskim rynku, która zgodzi się na ten warunek.

Odpowiedź nr 2. jednoosobowa spółka nawet w strukturze administracji państwowej jest niewskazana choćby ze względu na decyzyjność tak newralgicznej sieci. Owszem ma ona rację bytu, ale tylko w momencie, kiedy spółka jest utworzona w wyniku komercjalizacji przedsiębiorstwa państwowego na prywatną co w polskim prawie ma miejsce. Natomiast tym wypadku występuje działanie odwrotne.

Odpowiedź nr 3. odpowiadając na te pytanie należy przeanalizować pewne zależności, które wynikają z celu powołania samej instytucji. OSSB staje się dostawcą usług dla większości podmiotów administracji rządowej i samorządowej, wobec czego świadczy usługi, które wchodzą w zakres bezpieczeństwa i obronności. Co odpowiada na pytanie, że musi być to spółka mająca korzenie i kapitał krajowy w związku z czym wskazane jest, aby to była spółka Skarbu Państwa lub instytucja krajowa.

Odpowiedź nr 4. następnie wymaga się, aby miała własną niezależną i rozbudowaną infrastrukturę co zawęża krąg spółek. Pomimo, że projekt KSC zakłada wybudowanie 330 masztów w miejscach trudnodostępnych to sieć tej spółki musi już funkcjonować, wobec czego wymagana jest kompletna infrastruktura.

Reasumując na podstawie prezentowanej analizy przedstawiono własną propozycję Operatora Strategicznej Sieci Bezpieczeństwa. Biorąc pod uwagę, że:

- projekt zakłada rozbudowę 330 masztów co stanowi część infrastruktury;
- operator strategiczny powinien być szczególnie chroniony;
- powinien mieć doświadczone zaplecze z zakresu cyberbezpieczeństwa;
- powinien być niezależny i nie mieć konkurencji;
- posiadać świadectwo bezpieczeństwa przemysłowego.

Przedmiotem rozważań będzie propozycja rozbudowy NASK-PIB jako operator OSSB. Choć pomysł wydaje się kontrowersyjny to należy rozpatrywać go w kategoriach przede wszystkim zdolności, doświadczenia, wiedzy, bezpieczeństwa i braku powiązania z konkurencją i rynkiem spółek. Oczywiście dostosowanie NASK do roli operatora wiąże się z nakładami na infrastrukturę i tworzenie dodatkowych oddziałów, ale pozostaje poza wpływami lobbystycznymi. Biorąc pod uwagę ścisłą współpracę między NASK a Agencją Bezpieczeństwa Wewnętrznego, świadczone usługi będą na najwyższym z możliwych poziomie bezpieczeństwa. Dla tak zaprezentowanego pomysłu zostanie sporządzona analiza SWOT (Tab. 26) celem wyłonienia zagrożeń i szans.

Tab. 26. Analiza SWOT utworzenia OSSB z zasobów NASK-PIB.

WEWNĘTRZNE			ZEWNĘTRZNE		
kod	1 - niski 2 - średni 3 - wysoki	MOCNE STRONY (S)	kod	1 - niski 2 - średni 3 - wysoki	SZANSE (O)
S1	3	• wysoki poziom bezpieczeństwa usług	O1	2	• operator strategicznej sieci zależny tylko od administracji rządowej
S2	1	• brak konkurencyjności			
S3	2	• brak podatności na działania lobbystyczne	O2	2	• usług telekomunikacyjne na warunkach hurtowych
S4	2	• duże doświadczenie i ciągły rozwój badań			
S5	1	• posiadanie niezbędnych certyfikatów	O3	2	• brak powiązań z operatorami wysokiego ryzyka
S6	2	• wykluczenie jednoosobowej spółki			
S7	2	• realizacja zadań na rzecz obronności	O4	2	• transparentność instytucji
7	13	*SUMA*	4	8	*SUMA*
kod	1 - niski 2 - średni 3 - wysoki	SŁABE STRONY (W)	kod	1 - niski 2 - średni 3 - wysoki	ZAGROŻENIA (Z)
W1	2	• koszt utworzenia pełnej infrastruktury	Z1	2	• zwiększenie zapotrzebowania na wyspecjalizowane kadry
1	1	*SUMA*	1	2	*SUMA*

Źródło: Opracowanie własne.

Szanse i mocne strony definitywnie przeważają zagrożenia. Dodatkowo NASK na chwilę obecną jest operatorem akademickiej sieci to utworzenie na podstawie zasobów instytucji kolejnego zaufanego i sprawdzonego operatora nie stanowi przeszkód.

W związku z przeprowadzoną analizą można zaryzykować stwierdzenie, że tak poważny operator jakim ma być OSSB musi pochodzić spoza środowiska operatorów komercyjnych oraz musi posiadać zdolności do ciągłych badań nad siecią wprowadzając nowatorskie rozwiązania. W tym przypadku kluczowym jest uzyskanie odpowiedniego stopnia bezpieczeństwa sieci a te warunki spełnia NASK-PIB. Pomimo, że wymaga to dużych nakładów finansowych oraz zmiany w ustawie „Prawo Telekomunikacyjne", celem dostosowania NASK do tej roli to wszelkie standardy bezpieczeństwa jakie są wymagane w tym przypadku zostaną zachowane.

5.4.2. Organy odpowiedzialne za walkę z dezinformacją

Współcześnie dezinformacja stała się globalnym zagrożeniem uznawanym przez badaczy jako mająca realny wpływ na demokrację państw. Zgodnie z teorią dezinformacji wg Vladimira Volkoffa[145] można wyszczególnić następujące pojęcia:

- klient, osoba lub grupa, która zyskuje na operacji dezinformacji;
- agent, wykonawca zleconej dezinformacji, działa poprzez agentów wpływu;
- wsporniki, wydarzenia będące podstawą akcji dezinformacyjnej, nie muszą być prawdziwe, ważne, aby wywoływały jednoznaczne skojarzenia;
- przekaźniki, media;
- temat przewodni;
- pudła rezonansowe, kiedyś media niezwiązane z agentami wpływu, a obecnie dzięki rozwojowi Internetu także osoby prywatne; ich zadaniem jest nieświadome stwarzanie szumu medialnego;
- grupa docelowa do której kierowane są działania dezinformacyjne.

Celem kampanii dezinformacyjnej jest wytworzenie w grupie docelowej określonego poglądu na wskazany temat a także zdyskredytowanie argumentów przeciwników „klienta". Dezinformacja szerzej rozumiana jako informacje celowo wprowadzające w błąd (manipulacja informacją) definiowana jest na szczeblu europejskim[146] nieco inaczej. Dodatkowo do tej grupy można zaliczyć Fakenews (fałszywe informacje)

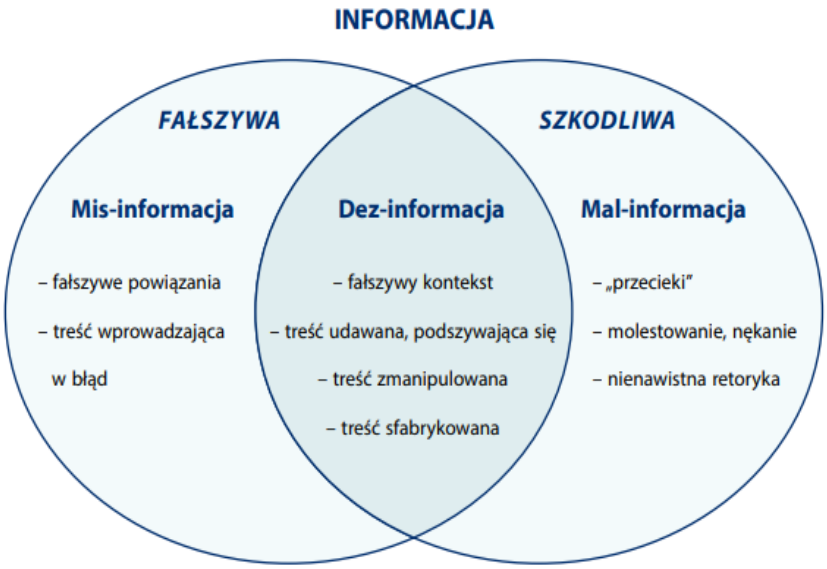
[145] Vladimir Volkoff – ur. 7 listopada 1932 w Paryżu, zm. 14 września 2005 w Bourdeilles; francuski pisarz, autor min. Dezinformacja: oręż wojny, Traktat o dezinformacji. Od Konia Trojańskiego do Internetu.

[146] Krajowa Rada Radiofonii i Telewizji, Fakenews dezinformacja online, próby przeciwdziałania tym zjawiskom z perspektywy instytucji międzynarodowych oraz wybranych państw UE, w tym Polski, Warszawa 2020. s. 11.

i Deepfake (fałszywe obrazy). Według raportu Rady Europy[147] z listopada 2017 r. istnieją trzy kategorie nieładu informacyjnego (information disorder):

- mis-informacja występuje, gdy rozpowszechniane informacje są nieprawdziwe, ale nie zostały stworzone z zamiarem wyrządzenia szkody;
- dezinformacja występuje, gdy fałszywe informacje są tworzone i rozpowszechnianie świadomie z zamiarem wyrządzenia krzywdy lub szkody;
- mal-informacja występuje, gdy rozpowszechniane informacje są oparte na faktach, ale powstały w celu wyrządzenia krzywdy lub szkody następuje to często poprzez upublicznianie informacji prywatnych.

Dla tak uporządkowanych definicji następuje zależność pomiędzy nimi zgodnie z rysunkiem 35. Wobec rosnącego problemu w niemalże całej Europie trwają prace nad opracowaniem regulacji prawnych oraz algorytmami służącymi do automatycznego wychwytu zmanipulowanych treści. W Polsce pomimo tworzenia nowelizacji ustawy o KSC problematyka dezinformacji jest marginalna.



Rys. 35. Zależność między Mis-Dezinformacja-Mal.
Źródło: Wardle, Derakhshan, Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, 2017.

Przyczyny takiego stanu rzeczy można doszukiwać się choćby w tym, że instytucja, która powinna być żywotnie zainteresowana przedmiotową problematyką mowa tu o Krajowej Radzie Radiofonii i Telewizji nie wnosi żadnych poprawek do projektu. Przy czym wskazane jest, aby to właśnie ta instytucja rozpoczęła proces walki z dezinformacją.

[147] 6 Claire Wardle, Hossein Derakhshan, Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe report, DGI (2017)09.

Przyglądając się działaniom państw europejskich w walce z dezinformacją na uwagę zasługuje Francja, która wprowadziła rygorystyczny zakaz propagowania dezinformacji w okresie poprzedzającym wybory w 2018 roku. Realizowane było to poprzez wprowadzenie ustawy[148] z której wynikała możliwość wszczynania postępowań przez specjalnie do tego utworzone 24-godzinne sądy, gdzie główną karą za naruszanie przepisów były sankcje karne i finansowe. Przykładowo był to rok więzienia i 75 tys. euro kary za „celowe wprowadzanie w błąd, które mogłoby wpłynąć na uczciwość wyborów". Oczywiście aby kazus francuski mógł zastosować zaimplementowany w Polsce należy powołać biegłych do definiowania co jest dezinformacją a co nie. I tu pojawia się główny problem a mianowicie to co dla jednej osoby będzie informacją dla drugiej może już być dezinformacją. W związku z czym należy powołać instytucje taką jak np. „Krajowa Rada ds. Dezinformacji (KRD)", która będzie rozstrzygała co do wartości informacji pojawiających się w przestrzeni medialnych. Oczywiście aby rada miała rację bytu musi składać się z krajowych autorytetów w danej dziedzinie i nie może być upolityczniona. W związku z czym wskazane jest, aby jej członkowie pochodzili z środowiska akademickiego. W Polsce istnieje na szczeblu krajowym Polska Akademia Nauk (PAN)[149], która w swym zakresie statutowym spełnia warunki do funkcjonowania takiej rady. Biorąc pod uwagę, że PAN zrzesza naukowców z niemalże każdej dziedziny jest najbardziej kompetentnym organem w tym zakresie. Utworzenie KRD oraz regulacji prawnych sankcjonujących dezinformację rozpocznie proces walki z dezinformacją w kraju.

Propozycja zostanie poddana analizie SWOT (Tab. 27) celem zweryfikowania czy jest zasadna. Z analizy można wyczytać, że pomysł utworzenia KRD wraz z regulacjami w sprawie dezinformacji jest słuszny. Jako zagrożenie uznać należy wzrost obaw społecznych w niektórych kręgach o paraliż informacyjny lub tworzenie propagandy, gdzie można przyjąć, że będzie to marginalna część społeczeństwa. Krajowa Rada ds. Dezinformacji utworzona z nieetatowej grupy autorytetów z Państwowej Akademii Nauk byłaby najbardziej uznawaną społecznie ze wszystkich możliwych do realizacji a zadaniem KRD byłoby walka z kampaniami dezinformacyjnymi oraz wspieranie sądów w ramach biegłych ekspertów dziedzinowych.

[148] LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information [dostęp: 23.01.2024].

[149] PAN – Polska Akademia Nauk, państwowa instytucja naukowa realizująca działania służące rozwojowi, promocji, integracji i upowszechnianiu nauki oraz przyczyniająca się do rozwoju edukacji i wzbogacania kultury narodowej.

Tab. 27. Analiza SWOT utworzenia instytucji odpowiedzialnej za dezinformację.

WEWNĘTRZNE			ZEWNĘTRZNE		
kod	1 - niski 2 - średni 3 - wysoki	MOCNE STRONY (S)	kod	1 - niski 2 - średni 3 - wysoki	SZANSE (O)
S1	3	• walka z dezinformacją	O1	2	• oczyszczenie przestrzeni medialnej z manipulacji informacją
S2	2	• wzmocnienie racji stanu			
S3	2	• uspokojenie nastroi społecznych podczas ważnych wydarzeń	O2	2	• wzmocnienie Polski na arenie międzynarodowej
S4	1	• zyski do budżetu z kar finansowych	O3	2	• wzmocnienie pozycji autorytetów dziedzinowych
S5	2	• bezpieczniejsza sieć cyfrowa			
S6	2	• walka z hybrydowymi zagrożeniami	O4	2	• stopniowe eliminowanie teorii spiskowych
			O5	2	• odbudowanie zaufania dziennikarskiego
6	12	*SUMA*	5	8	*SUMA*
kod	1 - niski 2 - średni 3 - wysoki	SŁABE STRONY (W)	kod	1 - niski 2 - średni 3 - wysoki	ZAGROŻENIA (Z)
W1	2	• wymagane usprawnienie sądownictwa	Z1	2	• wzrost obaw społecznych w niektórych kręgach o paraliż informacyjny i tworzenie propagandy
1	2	*SUMA*	1	2	*SUMA*

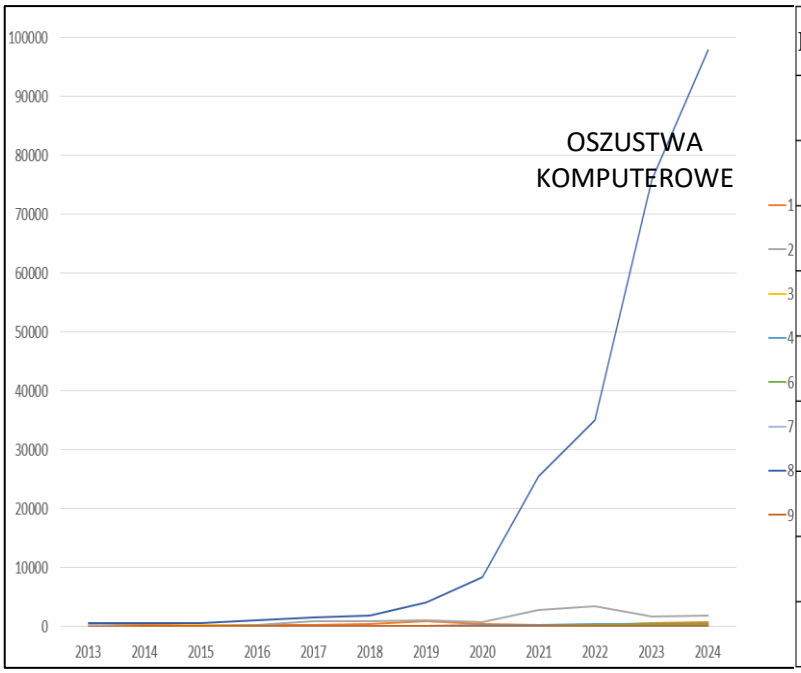
Źródło: Opracowanie własne.

Okres pandemii COVID-19 oraz konflikt ukraiński wyraźnie pokazują jak bardzo duża jest potrzeba utworzenia tego typu gremium celem rozwiania wszelkich wątpliwości negatywnie oddziaływujących na społeczeństwo. Prezentowane rozwiązane wpłynie również na środowisko dziennikarskie, gdzie obecnie stosowane są złe praktyki związane z dezinformacją.

5.4.3. Rozbudowa Centralnego Biura Zwalczania Cyberprzestępczości

W Polsce od 2022 roku funkcjonuje z sukcesami Centralne Biuro Zwalczania Cyberprzestępczości. Pomimo, że formacja jest dość młoda to ma już na koncie poważne sukcesy, które są licznie w mediach ogłaszane. Niestety statystyki dotyczące oszustw komputerowych mają dynamiczny trend wzrostowy co świadczy o niewystarczającym potencjale pojedynczego biura wobec skali zagrożeń. Kolejnym zauważalnym problemem jest działalność CBZC poza strukturą Krajowego Systemu Cyberbezpieczeństwa. Pomimo, że formacja jest częścią Policji to nie stoi nic na przeszkodzie wpiąć ją w ten system, gdzie analogią może być CSIRT GOV, Agencji Bezpieczeństwa Wewnętrznego, który hierarchicznie podlega również pod MSWiA. Wpięcie CBZC do systemu KSC rozwiąże problemy, które stanowią o ilości zgłoszeń przekazywanych do biura. W chwili obecnej wszystkie oszustwa mające charakter przestępczy są właśnie zgłaszane do CBZC, gdzie również niektóre incydenty

z CSIRT-ów mające podłoże przestępcze tam trafiają czyniąc tą instytucję nie wydolną. W związku z czym zalecana jest ścisła współpraca pomiędzy instytucjami i aby to uczynić wskazane jest wprowadzenie CBZC do KSC.



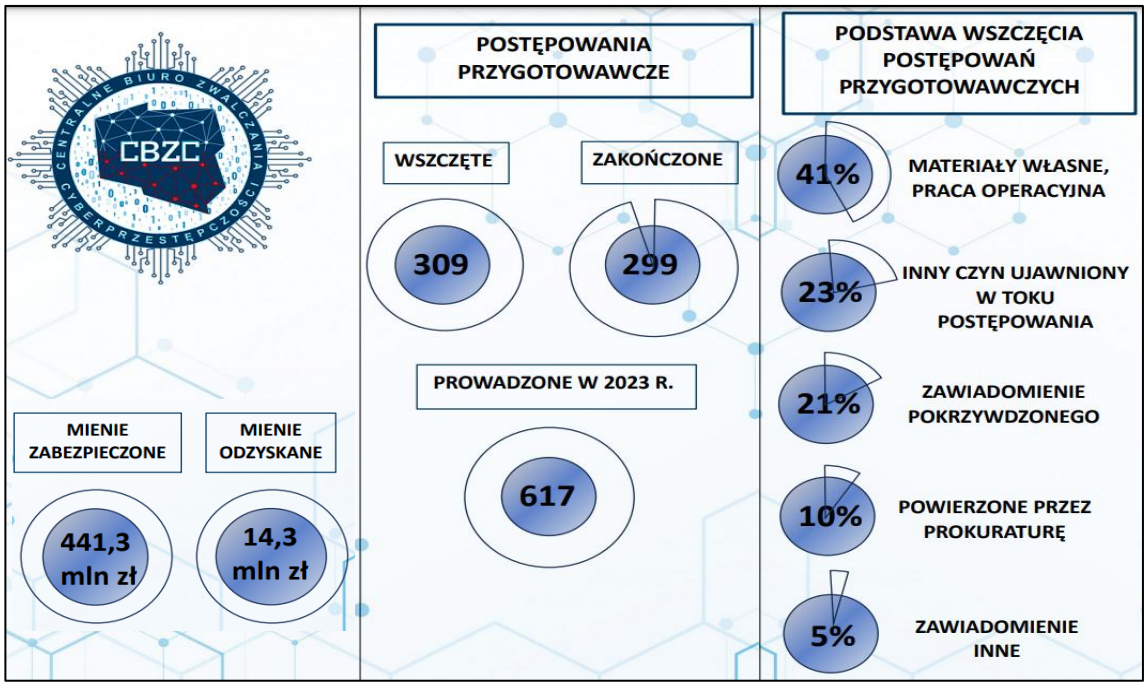
LP	Incydent \ rok
1	Obraźliwe i nielegalne treści
2	Złośliwe oprogramowanie
3	Gromadzenie informacji
4	Włamania do systemów
5	Próby włamań do systemów
6	Dostępność zasobów ataki DDOS
7	Atak na bezpieczeństwo Informacji
8	Oszustwa komputerowe
9	Inne

Rys. 36. Dane statystyczne ilości oszustw komputerowych.
Źródło: opracowanie własne na podstawie raportu CERT polska.

Godnym uwagi jest fakt, że CBZC powstało w 2021 roku, przy czym zdolność operacyjną uzyskało w 2022 roku więc dane statystyczne tego biura obejmują jedynie 2023 rok. Problem oszustw komputerowych wszelkiej maści ma poważniejsze podłoże. Mianowicie zgodnie z grafiką (Rys. 36) ilość tych zdarzeń według danych statystycznych na koniec 2022 roku wynosiła 35 tysięcy a w 2024 prawie 10 tyś. Dane statystyczne CBCZ[150] za rok 2023 pokazują, że biuro realizowało tylko 1,2 tysięcy postępowań (Rys. 37). W związku z tak prezentowanymi danymi można przeliczyć, że aby zająć się wszystkimi zgłoszeniami potrzebna jest zdolność operacyjna 29 takich biur co nie jest możliwe do zrealizowania. Natomiast zasadne jest rozważenie jednego dodatkowego biura w celu ustabilizowania trendu rosnącego oszustw komputerowych. Wiąże się to z olbrzymimi nakładami finansowymi, bo obecne biuro kosztowało 48 mln[151] zł, ale biorąc pod uwagę „zyski" czyli ilość środków zabezpieczonych i odzyskanych (łącznie 455 mln) to wydaje się to być zwrotna inwestycja. Oczywiście w tym wypadku należy oddzielić finanse

[150] Wyniki Statystyczne Centralnego Biura Zwalczania Cyberprzestępczości za 2023 rok. s. 2.
[151] https://kielce.wyborcza.pl/kielce/7,47262,29464437,wybuduja-nowa-siedzibe-dla-specow-od-cyberprzestepczosci-kosz.html [dostęp 02.02.2024].

z budżetu oraz prywatne straty natomiast uwzględniając, że środki w budżecie są z podatków, które wszyscy płacimy zachodzi zatem logiczny ciąg samo zarabiania przez siebie CBZC.



Rys. 37. Dane statystyczne ilości postępowań prowadzonych przez CBZC.
Źródło: opracowanie własne na podstawie raportu CBZC.

W związku z tak przedstawionym problemem w celu weryfikacji jakości i oceny propozycji zostanie przedstawiona analiza SWOT (Tab. 28).

Tab. 28. Analiza SWOT propozycji rozbudowy CBZC.

WEWNĘTRZNE			ZEWNĘTRZNE		
kod	1 - niski 2 - średni 3 - wysoki	MOCNE STRONY (S)	kod	1 - niski 2 - średni 3 - wysoki	SZANSE (O)
S1	3	• wzmocnienie walki z przestępczością komputerową	O1	2	• wzmocnienie zaufania do działań policji
S2	3	• zwiększenie liczby rekompensat dla pokrzywdzonych	O2	2	• znaczna minimalizacja oszustw komputerowych
S3	2	• wzajemne wsparcie poprzez wpięcie CBZC do struktury KSC	O3	2	• zwiększenie liczebności policji co przełoży się na bezpieczeństwo
S4	2	• delegowanie z CSIRT większej części spraw	O4	2	• zwiększenie pozycji kraju na arenie międzynarodowej
S5	1	• możliwość migracji kard pomiędzy biurami			
5	11	*SUMA*	4	8	*SUMA*
kod	1 - niski 2 - średni 3 - wysoki	SŁABE STRONY (W)	kod	1 - niski 2 - średni 3 - wysoki	ZAGROŻENIA (Z)
W1	2	• koszt utworzenia biura 48 mln (zgodnie z inflacją ok. 60 mln) • długi czas budowy	Z1	3	• zwiększenie zapotrzebowania na wykwalifikowane kadry w administracji publicznej
1	2	*SUMA*	1	3	*SUMA*

Źródło: Opracowanie własne.

Analiza wskazała zasadność mocnych stron i szans, przy czym należy zauważyć, że generowane są słabe strony i zagrożenia, które utożsamiane są z dwoma głównymi problemami cyberbezpieczeństwa. Celowo wskazano na budowę kolejnego biura, ponieważ obecne zostało zaprojektowane tak, że nie ma możliwości rozbudowania go do akceptowalnego poziomu.

Tworzenie kolejnego Biura Zwalczania Cyberprzestępczości jest pomysłem dość poważnym i należy przeanalizować to na poziomie kierownictwa MSWiA i uzgodnień międzyresortowych. Wstępna analiza oraz przedstawione argumenty wydają się być zasadne, aby na poważne rozważyć ten proces. Biorąc pod uwagę, że w każdym województwie CBZC ma swoje delegatury wskazane jest, aby rozbudować którąś z nich. W zależności od potrzeb można rozważyć rozbudowę wszystkich delegatur w jakimś stopniu tak aby poprawić efektywność całej instytucji.

5.5. Siły i środki w cyberbezpieczeństwie

Zmierzając do końca koncepcji poprawy bezpieczeństwa należy zająć się najbardziej istotnymi sprawami, które generują zagrożenia w cyberbezpieczeństwie. Mowa tu o środkach finansowych oraz zwiększeniu liczby wyspecjalizowanych kadr szczególnie w administracji państwowej. W zakresie potencjału ludzkiego cały czas panuje tendencja odchodzenia specjalistów do sektora prywatnego ze względu na zarobki. Obecnie rynek „cywilny" proponuje nawet 2-3 krotność wynagrodzenia[152] w zależności od specjalizacji. Jest to naturalne, że jeżeli osoba wykształci się za własne pieniądze (co w Polsce jest drogie) to będzie zmierzała do uzyskania jak największego wynagrodzenia za swą pracę a pobudki patriotyczne będą traktowane marginalnie. W związku z czym tylko realne wyrównanie zarobków w administracji państwowej pozwoli przyciągnąć i utrzymać odpowiednią liczbę wyspecjalizowanych pracowników.

Na realizację i utrzymanie każdego z proponowanych w koncepcji rozwiązań potrzebne są środki finansowe. Ponadto problemem jest to, że codzienna „walka" w cyberprzestrzeni nie jest widoczna dla opinii publicznej w związku z czym zarówno elity polityczne jak i społeczeństwo nie są przekonane co do skali zagrożeń. Konsekwencją takiego stanu rzeczy jest niskie finansowanie cyberbezpieczeństwa. Prezentowana koncepcja ma na celu nie tylko eliminację podatności, ale również

[152] Ekspert cyberbezpieczeństwa w administracji publicznej może liczyć na około 6 tyś. zł miesięcznie, gdzie w korporacji na tym samym stanowisku i z tym samym wykształceniem oraz kursami otrzyma od przedział 12 do 25 tysięcy miesięcznie.

podniesienie rangi cyberbezpieczeństwa oraz ogólnospołeczne uświadamianie co ostatecznie będzie dążyło do zrozumienia problematyki zagrożeń i zwiększenia nakładów finansowych na cyberbezpieczeństwo.

5.5.1. Pozyskiwanie wykwalifikowanych pracowników

Dla większości gałęzi administracji państwowej pozyskiwanie wyszkolonych pracowników jest problemem. Ponadto coraz większy kryzys w tym zakresie przechodzą służby mundurowe, które również stanowią trzon cyberbezpieczeństwa w kraju. Wszystko spowodowane jest katastrofalną wręcz przepaścią pomiędzy uposażeniem na etacie w administracji państwowej a stawkami proponowanymi w dużych korporacjach. Pomysłem jaki już funkcjonuje i miał naprawić sytuację jest Rozporządzenie w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa[153]. Dokument ten opisuje stawki dodatku w zależności od posiadanych uprawnień i stażu pracy w zakresie „cyber" gdzie z urzędu taki dodatek powinien zostać wypłacony pracownikom po spełnieniu warunków. Niestety tak nie jest. Kierownicy jednostek organizacyjnych często z sobie tylko wiadomych powodów narzucają kryteria w postaci przystąpienia do dodatkowych egzaminów, które są z natury trudno zdawalne, ponieważ nie jest określony ich zakres a treść zależy tylko od prowadzącego. Pomimo, że nie ma oficjalnej regulacji do stosowania tego typu praktyk to takie działania niosą skutek przeciwstawny do zamierzonego. Powoduje to ubywanie wyspecjalizowanych kadr do prywatnych pracodawców co stwarza olbrzymią lukę w administracji państwowej.

Rozwiązaniem tego problemu jest wydanie zaktualizowanego rozporządzenia w którym kierownicy jednostek organizacyjnych będą obligatoryjnie zmuszani do wypłacania dodatkowych świadczeń pracownikom spełniającym zawarte w treści dokumentu wymagania. W przeciwnym razie sytuacja będzie przypominała przykład z prawem jazdy, które kierowca w firmie zdobył państwowym egzaminem a pracodawca co miesiąc egzaminuje go z przepisów ruchu drogowego uzależniając od tego jego wypłatę. Jest to sytuacja nie do przyjęcia. W związku z czym zaproponowana zostanie nowelizacja rozporządzenia w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa z rygorem wykonywalności

[153] Rozporządzenie Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa. Dz.U. 2022 poz. 131.

dla kierowników jednostek organizacyjnych. Analiza SWOT (Tab. 29) pozwoli bliżej przyjrzeć się wadom i zaletom.

Tab. 29. Analiza SWOT nowelizacji rozporządzenia w sprawie dodatków „cyber".

WEWNĘTRZNE			ZEWNĘTRZNE		
kod	1 - niski 2 - średni 3 - wysoki	MOCNE STRONY (S)	kod	1 - niski 2 - średni 3 - wysoki	SZANSE (O)
S1	2	• przyciągnięcie specjalistów do administracji państwowej	O1	2	• zwiększenie prestiżu pracy w administracji państwowej
S2	2	• zwiększenie szans pozostania w administracji pracujących już specjalistów	O2	2	• większa motywacja i wydajność pracowników administracji państwowej
S3	3	• zwiększenie cyberbezpieczeństwa jednostki organizacyjnej	O3	2	• stopniowe uzupełnianie kadr odpowiedzialnych za cyberbezpieczeństwo
3	7	*SUMA*	3	6	*SUMA*
kod	1 - niski 2 - średni 3 - wysoki	SŁABE STRONY (W)	kod	1 - niski 2 - średni 3 - wysoki	ZAGROŻENIA (Z)
W1	2	• większe wydatki na cyberbezpieczeństwo			
1	2	*SUMA*	0	0	*SUMA*

Źródło: Opracowanie własne.

Wszystkie przesłanki wskazują na zasadność dopracowania regulacji, przy czym oprócz wydatków nie generują żadnych zagrożeń. Należy zatem uznać, iż narzędzie do rozwiązania problemu braku wyspecjalizowanych kadr w administracji państwowej odpowiedzialnych za cyberbezpieczeństwo już istnieje, lecz jest tylko nieumiejętnie wykorzystywane. Należy wymusić zmianę mentalności ludzi zwłaszcza odpowiedzialnych za organizację jednostek i instytucji. Zarówno wykształcenie jak i specjalistyczne kursy, które nie należą do najłatwiejszych i najtańszych a które pracownik ukończył zasługują na uznanie poprzez odpowiednie wynagrodzenie. Dodatkowo nikt nie będzie podejmował pracy na zaniżonych stawkach zwłaszcza że rynek cywilny jest nienasycony tego typu specjalistami.

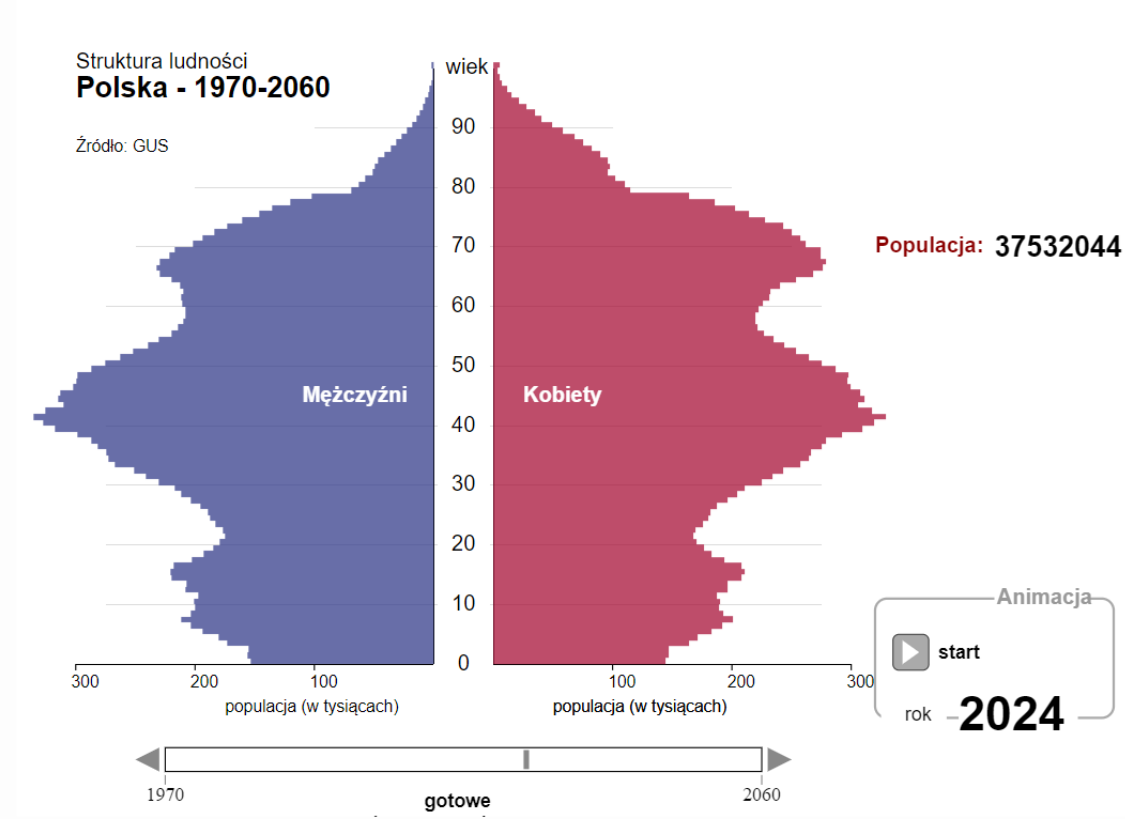
Tworzenie stałego zespołu specjalistów w administracji państwowej wymaga odpowiedniego ich wynagradzania. Skoro ustawodawca przewidział pewną formę świadczeń dla osób spełniających warunki to czemu nie jest to narzędzie wykorzystywane w pełni. To właśnie kierownicy jednostek organizacyjnych powinni walczyć o to, aby ich zespoły cyberbezpieczeństwa, wymagające tak specjalistycznej wiedzy i umiejętności były ukompletowane.

5.5.2. Pozyskiwanie środków finansowych na cyberbezpieczeństwo.

Najważniejszy problem z zakresu cyberbezpieczeństwa to oczywiście środki finansowania. Należy zwrócić uwagę, że i tak w ostatnich latach sytuacja diametralnie się poprawiła. Przede wszystkim trzeba wziąć pod uwagę ilość powołanych instytucji do realizacji cyberbezpieczeństwa, które pochłonęły setki milionów złotych oraz środki finansowe przeznaczane na ich utrzymanie, które są realizowane z budżetu państwa. Godnym uwagi jest fakt, że obecnie przy tak wielkich zagrożeniach jakie realizowane są w cyberprzestrzeni nie ma żadnych podatków dedykowanych i obciążających portfel podatnika. Należy wziąć pod uwagę, że wprowadzanie jakiegokolwiek podatku byłoby nieakceptowalne społecznie. Cyberbezpieczeństwo dotyczy nie tylko administracji państwowej to problem nas wszystkich (całego społeczeństwa). Obecnie wskazane jest utrzymanie nie tylko dostępu do usług, ale przede wszystkim zapewnienia właściwego bezpieczeństwa tych usług. W Polsce istnieje podatek, który jest ściśle powiązany z usługami cyberprzestrzeni z tym, że jest on niewłaściwie egzekwowany. Mowa tu o opłacie radiowo-telewizyjnej, której skuteczność sciągania jest na bardzo niskim poziomie. Większość społeczeństwa korzysta z klasycznych mediów (radio, telewizja) poprzez usługi sieciowe w związku z czym opłata radiowo-telewizyjna jest omijana. Wobec czego należy poddać transformacji ten rodzaj opłaty i zamienić go w opłatę od bezpieczeństwa usług w cyberprzestrzeni.

Według danych KRRiT na koniec 2022 roku opłaty uregulowało jedynie 828 tys. zobowiązanych (34,7 proc.), w tym 589 tys. gospodarstw domowych i 239 tys. abonentów instytucjonalnych. Świadczy to o tym, że po pierwsze opłata nie jest egzekwowana. Po drugie zarówno stacje radiowe i telewizyjne wystarczająco zarabiają na reklamach, lokowaniu produktów, kontraktach licencyjnych do tego stopnia, że są w stanie same się z tego utrzymać. Wobec czego opłata zwana abonamentem powinna zostać przekształcona w opłatę bezpieczeństwa cyberprzestrzeni, gdzie prawie każdy obywatel korzysta z urządzeń wpiętych w sieć. W chwili obecnej abonament radiowo-telewizyjny miesięcznie od odbiornika wynosi 27,30 zł za telewizor i 8,70 zł za radio. W Polsce jest 38 mln obywateli, gdzie po odjęciu osób poniżej 5 roku życia oraz emerytów, którzy nie są z technologią cyfrową zapoznani można oszacować, że będzie to populacja rzędu 31 mln (zgodnie z szacunkami GUS[154] Rys. 38).

[154] https://stat.gov.pl/obszary-tematyczne/ludnosc/ludnosc/ludnosc-piramida/ [dostęp: 02.05.2025]



Rys. 38. Struktura ludności w Polsce 2024 rok.
Źródło: https://stat.gov.pl/obszary-tematyczne/ludnosc/ludnosc/ludnosc-piramida/ [dostęp: 11.02.2024].

Co za tym idzie, gdyby każdy obywatel uprawniony (poza dziećmi do 5 lat i emerytami) uiścił opłatę w wysokości części obecnego abonamentu np. 10 zł to miesięcznie, byłoby to 310 mln zł do przeznaczenia na cyberbezpieczeństwo. Należy w tym przypadku zaznaczyć, że dzieci powyżej lat 5 są również użytkownikami cyberprzestrzeni w związku z czym opłata byłaby naliczana jak w przypadku odbioru domowych śmieci, gdzie podstawą jest ilość członków rodzin bez względu na wiek.

Reasumując z opłaty zastępującej abonament radiowo-telewizyjny w wysokości 10 zł od osoby w skali roku byłoby można przeznaczyć 3,72 miliarda złotych na wzmocnienie cyberbezpieczeństwa w kraju. Warunkiem jest akceptacja społeczna opłaty i sprawny system egzekucji poprzez włączenie tych opłat do rozliczania w rocznym zeznaniu podatkowym PIT. Dla porównania czteroosobowa rodzina mająca w domu telewizor i radio co jest poniekąd standardem zgodnie z obowiązującymi zasadami musi opłacić 432 zł abonamentu radiowo-telewizyjnego rocznie. Gdzie po zamianie opłaty na proponowaną wyniosłoby to 480 zł rocznie w związku z czym można uznać te opłaty jako podobnej wysokości. Oczywiście można by wliczyć w to zniżki dla wielodzietnych rodzin, rencistów, weteranów, kombatantów, w tym ulgi uczniowskie, studenckie tak jak to odbywa się na obecnych zasadach. Problemem stałoby się jedynie przekonanie

społeczeństwa do słuszności opłat a raczej celu jaki będą zasilały. W celu sprawdzenia jakości rozwiązania zostanie poddane ono analizie SWOT (Tab. 30).

Tab. 30. Analiza SWOT przekształcenia abonamentu RiTV.

WEWNĘTRZNE			ZEWNĘTRZNE		
kod	1 - niski 2 - średni 3 - wysoki	MOCNE STRONY (S)	kod	1 - niski 2 - średni 3 - wysoki	SZANSE (O)
S1 S2 S3 S4	3 3 3 3	• wzmocnienie cyberbezpieczeństwa • wyrównanie płac dla specjalistów cyberbezpieczeństwa • rozbudowa bezpieczeństwa komercyjnych usług i dostępu do usług • zmniejszenie cyberprzestępczości	O1 O2 O3	3 2 2	• rozwiązanie problemu niewystarczającego finansowania cyberbezpieczeństwa w kraju • wzmocnienie roli cyberbezpieczeństwa w społeczeństwie • równomierne rozłożenie kosztów utrzymania cyberbezpieczeństwa w śród obywateli
4	12	*SUMA*	3	7	*SUMA*
kod	1 - niski 2 - średni 3 - wysoki	SŁABE STRONY (W)	kod	1 - niski 2 - średni 3 - wysoki	ZAGROŻENIA (Z)
W1	2	• egzekwowanie opłat	Z1	2	• przekonanie społeczeństwa o słuszności opłaty
1	2	*SUMA*	1	2	*SUMA*

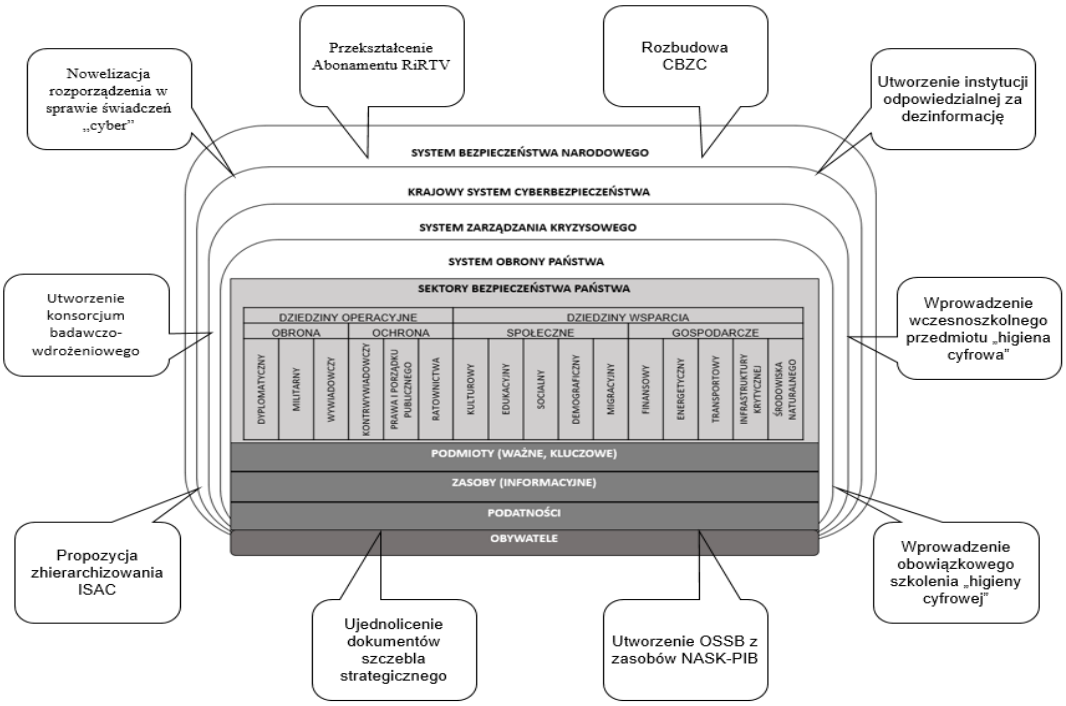
Źródło: Opracowanie własne.

Wszystkie przesłanki wskazują na zasadność wdrożenia przedstawionej opłaty przy założeniu, że podniesienie rangi oraz znaczenia cyberbezpieczeństwa wśród obywateli będzie sukcesywnie rosło. Dodatkowo opłata będzie pierwszą w historii państwa, gdzie obywatel płaci bezpośrednio za swoje bezpieczeństwo. Egzekwowanie można wymusić regulacjami prawnymi poprzez uwarunkowanie, że kto nie uiszcza opłat ten nie może się ubiegać o odszkodowanie lub zadośćuczynienie na drodze prawnej za szkody powstałe w wyniku działań w cyberprzestrzeni w związku z czym opłata byłaby również swego rodzaju koniecznym warunkiem dochodzenia swoich praw.

5.6. Podsumowanie rozdziału

Pomimo że cyberprzestrzeń istnieje od zarania dziejów ludzkość dopiero stosunkowo od niedawna nauczyła się wykorzystywać ją jako medium, w tym do materializacji zagrożeń. Kolejne lata, dekady a nawet wieki, będą tylko rozwijać zagrożenia wykorzystujące cyberprzestrzeń w związku z czym tak bardzo ważna jest eliminacja podatności, która temu sprzyja. Pozbycie się wad, luk, słabości stwierdzonych na podstawie rozdziału III wymaga zastosowania pewnych rozwiązań, które w głównej

mierze pociągają za sobą zmiany w regulacjach prawnych. Ponadto wymagają utworzenia programów rozwoju, tworzeniu dodatkowej infrastruktury a co za tym idzie wzmocnienia nakładów finansowych i kadrowych w sferze cyberbezpieczeństwa. Wszystkie te przedsięwzięcia (Rys. 39) wymagają jeszcze jednego mianowicie akceptacji społecznej. To właśnie świadomość społeczna o zagrożeniach determinuje środki mogące przeciwstawić się im. Tak jak już wspomniano mentalność jest sferą zachowania, której nie zmieni żadna regulacja prawna. Natomiast jest duża szansa, że jeśli zmienimy rangę cyberbezpieczeństwa wśród dokumentów takich jak strategie, wprowadzimy nauczanie zarówno w pracy jak i szkołach, utworzymy instytucje odpowiedzialne za ład informacyjny to świadomość społeczna ulegnie znacznemu polepszeniu.



Rys. 39. Propozycje eliminacji stwierdzonych podatności na tle operacyjnego modelu SBN. Źródło: opracowanie własne.

Wszelkie działania na korzyść cyberbezpieczeństwa wymagają odpowiednich nakładów w postać sił i środków finansowych, przy czym społeczeństwo nie jest przekonane do płacenia odpowiedniej kwoty na walkę z niewidzialnym wrogiem. Realnie rzecz biorąc wystarczy wdrażać zmiany w Systemie Bezpieczeństwa Narodowego, które idą wraz z postępem technologicznym. Ponadto należy ukierunkowywać ten system na nowe zagrożenie, jednocześnie eliminując rozwiązania, które są nieadekwatne, przestarzałe lub niespełniające swoich statutowych zadań. Świadomość społeczna jest na niskim poziomie i zachodzi konieczność jej podniesienia w granicach możliwości. Żeby tego dokonać wystarczy eksponować w większym stopniu katastrofalne skutki materializacji zagrożeń.

Należy tu wspomnieć, że większość incydentów które miały miejsce głównie w sektorze bankowym były ukrywane przed społeczeństwem w obawie przed utratą wizerunku a takie zachowania nie tylko sprzyjają agresorom, ale i niwelują rzeczywisty poziom zagrożenia. Sytuacja przypomina jeszcze niedawne pojmowanie konfliktu zbrojnego przez Polaków, gdzie sytuacja po 28 lutym 2022 roku nagle uświadomiła obywatelom, że zagrożenie jest jak najbardziej realne, bo dzieje się w bezpośrednim sąsiedztwie. Dlatego podejmując nawet te niepopularne decyzje takie jak np. zmiana abonamentu na opłatę cyberbezpieczeństwa należy dać do zrozumienia społeczeństwu, że zagrożenia cyberprzestrzeni są na tyle poważne, że państwo potrzebuje wsparcia własnych obywateli, aby wyjść naprzeciw dynamicznie rozwijającym się zagrożeniom.

ROZDZIAŁ VI. IMPLEMENTACYJNOŚĆ OPRACOWANEJ KONCEPCJI

Przed przystąpieniem do implementacji opracowanej koncepcji ważna jest identyfikacja wskaźników, za pomocą których zostanie dokonana ocena skutków implementacji ze szczególnym uwzględnieniem:

- rodzaju rozwiązywanego problemu,
- rekomendowanych rozwiązań, w tym planowanych narzędzi interwencji oraz oczekiwanych efektów,
- sposobów rozwiązań podobnych problemów w innych krajach w szczególności krajach członkowskich UE,
- podmiotów, na które oddziałuje przedmiotowy projekt,
- informacji związanych z zakresem projektu,
- wpływu proponowanych rozwiązań na sektor finansów publicznych,
- wpływu proponowanych rozwiązań na konkurencyjność gospodarki i przedsiębiorczość oraz na rodzinę, obywateli i gospodarstwa domowe,
- wpływu na rynek pracy oraz na inne obszary,
- wpływu na regulacje prawne i potrzebę ich aktualizacji,
- sposobu i czasu ewaluacji efektów projektu wg przyjętych mierników.

Uwzględnienie tych kluczowych aspektów pozwala na obiektywizację oceny możliwości poprawy bezpieczeństwa państwa wg zaproponowanej koncepcji. Ocena skutków wdrożenia tej koncepcji będzie zatem wynikiem analizy szczegółowych ocen i wskazań eksperckich (załącznik nr 8) oraz autooceny wg wskazanych w badaniu konsekwencji wdrożenia proponowanych rozwiązań.

6.1. Warunki i ograniczenia dla implementacji koncepcji

Implementacja opracowanej koncepcji wymaga akceptacji zarówno decydentów jak i społeczeństwa. Aby to uzyskać należy zdefiniować w sposób ilościowy lub jakościowy nieliczne, ale istotne kryteria porównawcze, które pozwolą oszacować jakie siły i środki należy zaangażować do realizacji koncepcji. W związku z czym tak jak to opisano w poprzednich rozdziałach (III i IV) będą brane pod uwagę takie wskaźniki jak:

- wielkość wkładu finansowego początkowego obliczona na podstawie analogicznych przedsięwzięć;

- wielkość wkładu finansowego cyklicznego na utrzymanie obliczona na podstawie analogicznych przedsięwzięć;
- ilość wykwalifikowanych specjalistów do pozyskania obliczona na podstawie analogicznych przedsięwzięć;
- ilość zmian w dokumentach prawnych obliczona na podstawie istniejących regulacji prawnych;
- ilość oraz wielkość niezbędnej infrastruktury obliczona na podstawie potencjalnych braków.

Utrzymując założenie, że realizacja koncepcji byłaby możliwa przy wykorzystaniu obecnych zdolności państwa (siły i środki) to podstawowym ograniczeniem jest czas w jakim zostanie ona wprowadzona. Jest to bezpośredni czynnik determinujący zasadność wprowadzenia koncepcji. Mowa tu w szczególności o rozwiązaniu polegającym na nowelizacji dokumentacji szczebla strategii, które są cyklicznie tworzone. Aby zrealizować te rozwiązanie należałoby rozpocząć pracę nad kluczowymi dla Systemu Bezpieczeństwa Narodowego dokumentami jednocześnie ściśle je ze sobą powiązując. Ponadto należy mieć świadomość, że implementacja koncepcji nie przyniesie natychmiastowych efektów poprawy obecnego stanu bezpieczeństwa. Na większość rezultatów będzie trzeba poczekać nawet latami tak jak w przypadku wprowadzania długoterminowych programów szkolenia i uświadamiania społeczeństwa. Z biznesowego punktu widzenia jest to rodzaj inwestycji, w którą trzeba dużo włożyć i długo czekać na zyski. Niemniej jednak zmiany, które niesie za sobą koncepcja są konieczne do wprowadzenia, ponieważ ich brak będzie potęgował rozmiary skutków materializacji zagrożeń w skali całego państwa zarówno w wymiarze materialnym jak i niematerialnym. Istnieje jeszcze jedna przesłanka przemawiająca za koniecznością implementacji przedmiotowej koncepcji. Mianowicie współczesne trendy państw europejskich oraz z innych regionów świata wykazują ciągły rozwój podnosząc poziom swojego cyberbezpieczeństwa. W związku z czym pozostawanie na stałym poziomie będzie tak naprawdę cofaniem się w stosunku do rozwijających się nacji.

W celu szczegółowego zbadania potrzebnych funduszy, liczby personelu, dodatkowej infrastruktury, zmiany regulacji prawnych, czyli podstawowych parametrów koncepcji, każde rozwiązanie w niej zawarte zostanie oszacowane pod kątem wskaźników, które rozwinięto w tabeli 31.

Tab. 31. Wskaźniki niezbędne do oszacowania sił i środków.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś – 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln – 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln – 50 mln)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne na podstawie rozdziału V.

W tym momencie należy wyjaśnić, że szczegółowe wartości tych wskaźników zostaną oszacowane w pewnych przedziałach, ponieważ nie jest możliwe dokładne (precyzyjne) wyliczenie żadnego z tych parametrów na tym etapie. Do określenia przybliżonych wyliczeń przydatna będzie metoda komparacji istniejących już rozwiązań, zdarzeń, praktyk oraz wgląd w bieżące wydatki na cyberbezpieczeństwo.

6.2. Szacowanie kluczowych wskaźników opracowanej koncepcji

Tworzenie krajowych zdolności technologicznych.

Przede wszystkim należy zinwentaryzować systemy (produkty ITC) eksploatowane w administracji państwowej a w szczególności w systemie zarządzania kryzysowego i infrastrukturze krytycznej, które pochodzą od producentów uznanych w niedalekiej przyszłości za „dostawców wysokiego ryzyka". Mowa tu o oprogramowaniu niezbędnym do funkcjonowania systemów sterowania, procesorach, serwomechanizmach, sterownikach logicznych i wszelkich urządzeniach posiadających zdolność magazynowania, transmisji i dystrybucji danych. Kolejnym etapem będzie powołane konsorcjum składającego się z instytucji będących w zasobach środowiska akademickiego i opracowanie planów badawczo-wdrożeniowych oraz rozwiązań konstrukcyjnych technologii, wykorzystywanych do utrzymania ciągłości działania newralgicznych systemów. Zaprojektowany i przebadany system, który zostanie

przetestowany będzie sukcesywnie wdrażany. Pozwoli to na pozbycie się technologii wysokiego ryzyka z infrastruktury krytycznej. Oczywiście nie tylko uczelnie posiadają zdolności do realizacji tego typu przedsięwzięć. Obecnie istnieją dość mocno rozwinięte Start-upy[155], które świadczą tego typu usługi, lecz ze względów ekonomicznych zaleca się wykorzystanie do tego celu zasobów środowiska akademickiego. Tabela 32 prezentuje wskaźniki potrzeb niezbędnych do wdrożenia tego rozwiązania.

Tab. 32. Środki do utworzenia konsorcjum badawczo-wdrożeniowego.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś - 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln - 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln - 50 mln)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne.

Infrastruktura – nie jest wymagana, ponieważ konsorcjum składałoby się z istniejących zakładów, katedr, instytutów, wydziałów akademickich wykorzystując biura i całe zaplecze badawcze będące w zasobach tych instytucji.

Liczba personelu – dodatkowa nie jest wymagana, ponieważ skład naukowy stanowiliby pracownicy akademiccy będący zatrudnieni na etatach w macierzystych uczelniach.

Zmiany regulacji prawnych – konsorcjum nie wymaga zmian prawnych, ponieważ ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce[156] w art. 60 zakłada współpracę międzyuczelnianą i tworzenie zespołów naukowo-badawczych. Istnieje konieczność utworzenia pewnych umów, które konsolidowałyby współpracę międzyuczelnianą. W zależności od ilości instytucji przewiduje się utworzenie od 2 do 5 umów i porozumień.

[155] Start-up – nowo utworzone przedsiębiorstwo lub tymczasowa organizacja poszukująca modelu biznesowego, który zapewniłby jej zyskowny rozwój. Istnieje wiele definicji start-upów. Podmioty zaliczane do tej kategorii są najczęściej związane z technologiami informacyjnymi i komunikacyjnymi (ICT) oraz sektorami high tech.

[156] Dz. U. 2018 poz. 1668.

Koszty utworzenia – nie są wymagane, ponieważ tak jak w przypadku infrastruktury konsorcjum składałoby się istniejących instytucji i zasobów wchodzących w ich skład.

Utrzymanie miesięczne – prace naukowo-wdrożeniowe są wysokobudżetowe i zazwyczaj określane poprzez granty przewidziane na całość projektu. W zależności od rozmiaru konsorcjum i ilości prac badawczych prowadzonych jednocześnie można poprzez metodę komparacji istniejących programów ustalić przedział miesięcznego utrzymania[157].

Rozwiązanie polegające na utworzeniu konsorcjum badawczo-wdrożeniowego obarczone jest dość dużymi kosztami utrzymania, ponieważ badania nad nowymi technologiami są kosztowne. Porównanie przedsięwzięcia do istniejącego programu naukowo-badawczego pozwoliło na określenie przedziału miesięcznych wydatków jakie są konieczne do realizacji rozwiązania.

Wzmocnienie roli cyberbezpieczeństwa na poziomie strategii

Problem polegający na niejednolitym i niespójnym eksponowaniu roli cyberbezpieczeństwa w strategiach jest istotny, ponieważ treść wizji przedmiotowych dokumentów determinuje potrzeby aktów niższego szczebla takich jak ustawy czy rozporządzenia. Istotą problemu jest brak zachowania w hierarchii dokumentów należytego płynnego przejścia, zachowującego adekwatny do zagrożeń poziom rangi cyberbezpieczeństwa. Problem wynika z wprowadzania strategii w różnych okresach, gdzie obecnie niektóre z nich straciły swoją aktualność. Mowa tu o Strategii Rozwoju Systemu Bezpieczeństwa Narodowego, która powstała w 2013 roku i zakładała wizję przedmiotowego systemu na 10 lat, a więc do 2023 roku. Brak prac nad aktualizacją dokumentu powoduje, że najważniejszy system państwa jest pozbawiony wizji dalszego rozwoju. Dodatkowo, dokument został przystosowany do korelacji z Zintegrowanymi Strategiami Rozwoju, a nie nawiązuje do Strategii Cyberbezpieczeństwa RP, co jest z punktu widzenia bezpieczeństwa bardzo istotne. Wobec czego należy rozpocząć pracę nad nowelizacją strategii oraz mocniejszym wyeksponowaniu rangi cyberbezpieczeństwa, adekwatnym do współczesnych zagrożeń we wszystkich dokumentach, które powinny utrzymywać hierarchiczną zgodność ze sobą. Natomiast, zgodnie z opisem problemu w rozdziale V należy dążyć do wyniesienia roli cyberbezpieczeństwa do rangi ponaddziedzinowej, ponieważ cyberbezpieczeństwo

[157] Jako porównanie posłużono się konkursem programu NEON skupiającym się na finansowaniu prac badawczo-rozwojowych dotyczących obszaru Przemysłu 4.0 i sztucznej inteligencji. Kwota dofinansowania wynosi 8 000 000,00 PLN na badania trwające około dwóch lat.

przenika każdą dziedzinę i każdy sektor bezpieczeństwa. Tabela 33 przedstawia nakłady niezbędne do realizacji założonego celu.

Tab. 33. Środki na wzmocnienie roli cyberbezpieczeństwa w strategiach.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś – 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln – 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln – 50 mln)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne.

Infrastruktura – nie jest wymagana, ponieważ tworzenie dokumentów strategicznych realizowane jest w instytucjach istniejących.

Liczba personelu - nie jest wymagana, ponieważ tworzenie dokumentów strategicznych realizowane jest przez personel istniejących już instytucji.

Zmiany regulacji prawnych – dokumentami, które należy zaktualizować są:

- Strategie w których minął czas wizji dokumentu:
  - Strategia Rozwoju Systemy Bezpieczeństwa Narodowego RP;
  - Strategia Cyberbezpieczeństwa RP (obecnie trwa projekt nowelizacji 2025).
- Dokumenty do mocniejszego wyeksponowania rangi cyberbezpieczeństwa:
  - Długookresowa Strategia Rozwoju Kraju;
  - Średniookresowa Strategia Rozwoju Kraju;
  - Strategia Bezpieczeństwa Narodowego RP (obecnie trwa projekt nowelizacji 2025).

Koszty utworzenia – nie są wymagane żadne wstępne koszty. Tworzenie dokumentacji szczebla strategicznego jest wpisane w obowiązki osób będących na etacie w przeznaczonych do tego instytucjach.

Utrzymanie miesięczne – nie jest wymagane, ponieważ kosztem utworzenia dokumentów jest pensja osób odpowiedzialnych za ich realizację.

Ujednolicenie, podniesienie rangi cyberbezpieczeństwa oraz zachowanie płynności przejścia między dokumentami różnego szczebla będzie miało nieoceniony wpływ na kształtowanie regulacji prawnych. Ponadto przełoży się to na akceptację społeczeństwa do zwiększania środków na cyberbezpieczeństwo, ponieważ wyeksponowanie zagrożeń cyberbezpieczeństwa na odpowiednim poziomie w dokumentach rangi strategii spowoduje zwiększenie świadomości społecznej.

Regulacje w sprawie centrów wymiany i analizy informacji (ISAC)

Centra wymiany i analizy informacji, czyli tzw. ISAC nie posiadają jasno sprecyzowanych zasad finansowania i działają na zasadzie dotowania i sponsorowania przez podmioty prywatne. W związku z czym zachodzi uzasadniona obawa, że podmiot prywatny, który jest sponsorem będzie mógł w ramach audytu finansowego mieć wgląd w dane wrażliwe przetwarzane w ISAC. Szczególna obawa zachodzi w przypadku centrów świadczących usługi na rzecz infrastruktury krytycznej[158]. Dodatkowo brak hierarchii w tym środowisku spowoduje, że centra nie będą współpracować, lecz rywalizować min. o źródła finansowania. W związku z czym utworzenie nadrzędnego ISAC dotowanego po części z budżetu państwa spowoduje, że działania pomiędzy centrami będą skoordynowane. Dodatkowo będzie rosła współpraca między nimi oraz zwiększy się transparentność finansowania z jednoczesnym sprawowaniem nadzoru. Takie postępowanie obecnie z powodzeniem funkcjonuje w Stanach Zjednoczonych Ameryki. Niezbędne środki do realizacji celu przedstawiono w tabeli 34.

Tab. 34. Środki potrzebne do utworzenia wiodącego ISAC.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś – 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln – 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln – 50 mln)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne.

[158] Ustawa zakłada utworzenie sektorowych ISAC dla energii, transportu, służby zdrowia, infrastruktury cyfrowej, finansowej.

Infrastruktura – nie jest wymagana, ponieważ wiodący ISAC będzie wybrany jako jeden z istniejących podmiotów, wobec czego infrastruktura będzie już przygotowana.
Liczba personelu – dodatkowa nie jest wymagana, ponieważ wiodący ISAC będzie wybrany jako jeden z istniejących podmiotów, wobec czego personel będzie już zatrudniony.

Zmiany regulacji prawnych – wymagana będzie zmiana zapisów w projekcie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa[159]. W art. 1 oraz rozdziale 5 a dotyczącą funkcjonowania ISAC. Dodatkowo będzie wymagane będzie utworzenie regulacji i wytycznych w sprawie finansowania oraz działalności bieżącej przedmiotowych organizacji.

Koszty utworzenia – nie są wymagane, ponieważ wiodący ISAC będzie wybrany jako jeden z istniejących podmiotów, w związku z czym nie są wymagane żadne nakłady początkowe.

Utrzymanie miesięczne – działalność wiodącego ISAC powinna być po części dotowana. Pozwoli to na utrzymanie kontroli nad całym sektorem centrów wymiany i analizy danych. Wysokość świadczeń powinna być uzależniona od rozmiaru organizacji. Przewiduje się refundację połowy miesięcznych kosztów utrzymania wiodącego centra tj. w przedziale od 100 tyś - 500 tyś na miesiąc[160].

Szczegółowe rekomendacje co do utworzenia ISAC zakładają dowolną strukturę[161]. W zależności od rodzaju sektora gospodarki w którym działają podmioty te mogą mieć różną wielkość. Zaleca się, aby wiodący ISAC został wybrany spośród centr, które sprawują nadzór cyberbezpieczeństwa w infrastrukturze krytycznej, czyli spośród ISAC Kolej, ISAC Lot lub ISAC sektora energetycznego itp.

Narodowy długoterminowy program uświadamiania społecznego.

Narodowy długoterminowy program uświadamiania społecznego, powinien przybrać formę szkoleń wstępnych i cyklicznych podczas zatrudniania pracownika w administracji państwowej. Szkolenie powinno być realizowane tak samo jak stanowiskowe BHP. Działania te spowodują, że po upływie pewnego czasu zdecydowana

[159] Dz. U. 2018 poz. 1560.
[160] Przedmiotowa wartość dotacji z budżetu państwa powinna zaspokoić około 50% kosztów miesięcznego utrzymania centra. Biorąc pod uwagę strukturę przeciętnego ISAC, który składa się z grupy kilkunastu lub kilkudziesięciu specjalistów koszt będzie mieścił się w przedziale 100-500 tyś zł na miesiąc.
[161] https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/Poradnik-NASK-na-temat-tworzenia-ISAC .pdf [dostęp: 20.06.2024].

większość pracowników sektora państwowego uzyska świadomość na temat zagrożeń, sposobów ich realizacji jak również skutków. Szkolenie tego typu w dużym stopniu przyczyni się do zmniejszenia ryzyka materializacji zagrożeń, ponieważ zdecydowana większość cyberataków wykorzystuje socjotechnikę polegającą na zmuszeniu ofiary do podjęcia pewnych działań. W związku z czym uświadamianie kadr jest wymogiem koniecznym, a propozycja wprowadzenia ustawowego szkolenia z cyberbezpieczeństwa będzie stopniowo podnosiła wiedzę i kompetencje zwiększając bezpieczeństwo organizacji. W tabeli 35 oszacowano środki niezbędne do wprowadzenia szkoleń.

Tab. 35. Środki potrzebne do wprowadzenia szkoleń z cyberbezpieczeństwa.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś – 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln – 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln – 50 mln / mc)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne.

Infrastruktura – nie jest wymagana, ponieważ szkolenia będą prowadzone w macierzystych zakładach pracy.

Liczba personelu – dodatkowa nie jest wymagana, ponieważ każda państwowa instytucja ma na etacie informatyków, którzy mogą takie szkolenia przeprowadzić.

Zmiany regulacji prawnych – wymagana będzie zmiana zapisów ustawie z dnia 26 czerwca 1974 r. Kodeks pracy[162], rozdział X, dotyczący służby bezpieczeństwa i higieny pracy oraz wdrożenia ogólnodostępnej strony internetowej wraz z materiałami instruktażowymi do pobrania.

Koszty utworzenia – nie są wymagane, ponieważ instruktorzy (informatycy) szkolący będą na etacie instytucji. Koszt utworzenia materiałów szkoleniowych również nie jest wymagany i powinien być realizowany poprzez obsadę Ministerstwa Cyfryzacji w ramach zadań służbowych.

[162] Dz. U. 1974 Nr 24 poz. 141.

Utrzymanie miesięczne – nie są wymagane koszty miesięcznego utrzymania, można jedynie rozważyć dodatki służbowe dla osób funkcyjnych prowadzących szkolenia.

Utworzone podręczniki, tablice poglądowe czy zestawy egzaminacyjne sprawdzające poziom wiedzy powinny być cyklicznie aktualizowane i zamieszczone na specjalnie przeznaczonej do tego stronie internetowej. Tak aby każdy z instruktorów i szkolonych miał bezpośredni dostęp do bezpłatnego materiału szkoleniowego.

Narodowy długoterminowy program szkolnictwa ustawowego.

Narodowy długoterminowy program szkolnictwa ustawowego wraz narodowym długoterminowy program uświadamiania społecznego powinny zaspokoić potrzebę podnoszenia świadomości społecznej z zakresu cyberbezpieczeństwa w państwie. Wprowadzenie do szkół obowiązkowego przedmiotu higieny cyfrowej zwiększy bezpieczeństwo przede wszystkim najmłodszych użytkowników sieci. Obecnie problem nieumiejętnego korzystania z sieci jest bardzo mocno poruszany medialnie, gdzie zarówno nielegalne i obraźliwe treści oraz tzw. hejt w skrajnych przypadkach może doprowadzić dziecko do depresji a w konsekwencji nawet samobójstwa. W związku z czym szkoła jest podstawowym miejscem, gdzie należy młodzież uczyć z zakresu bezpiecznego posługiwania się technologią cyfrową. Koszty będą porównywalne jak w przypadku wprowadzenia szkolenia w miejscach pracy (Tab. 36).

Tab. 36. Środki wymagane do wprowadzenia przedmiotu higiena cyfrowa.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś – 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln – 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln – 50 mln)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne.

Infrastruktura – nie jest wymagana, ponieważ przedmioty będą prowadzone w macierzystych szkołach.

Liczba personelu – dodatkowa nie jest wymagana, ponieważ każda szkoła ma na etacie nauczycieli, którzy mogą takie mogą takie przedmioty poprowadzić.
Zmiany regulacji prawnych – wymagana będzie zmiana zapisów w ustawie z dnia 14 grudnia 2016 r. Prawo oświatowe[163] oraz wdrożenie systemu konspektów do prowadzenia zajęć.
Koszty utworzenia – nie są wymagane, ponieważ nauczyciele mają pensum ściśle uzależnione od ilości godzin dydaktycznych. Pozostaje jedynie koszt utworzenia i dystrybucji podręczników do przedmiotu, ale to może być zrealizowane z funduszu ministerialnego.
Utrzymanie miesięczne – nie są wymagane koszty miesięcznego utrzymania można jedynie rozważyć dodatek dla każdego nauczyciela chcącego przejść kurs kwalifikacyjny.

Wprowadzenie higieny cyfrowej do programu wczesnoszkolnego może również zaindukować młode osoby do rozwijania się w tym kierunku w przyszłości.

Tworzenie instytucji Operatora Strategicznej Sieci Bezpieczeństwa.

Nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa w związku z koniecznością implementacji do polskiego porządku prawnego Dyrektywy NIS2 zakłada wprowadzenie instytucji Operatora Strategicznej Sieci Bezpieczeństwa. Biorąc pod uwagę, że niezależnie od tego kto będzie tym operatorem infrastruktura w postaci obiektów i masztów z nadajnikami musi powstać, wobec czego zmiana wyboru operatora nie generuje dodatkowych kosztów. Utworzenie z Naukowej Akademickiej Sieci Komputerowej operatora OSSB nie zaburzy w żaden sposób rynku przedsiębiorców telekomunikacyjnych oraz przyczyni się do niezależności tego podmiotu wobec lobbystów. Nie bez znaczenia pozostaje tu doświadczenie i własny C-SIRT oraz zaplecze badawczo naukowe. Koszt wyboru NASK na operatora strategicznej sieci wiąże się z angażowaniem następujących sił i środków (Tab. 37).

Infrastruktura – jest wymagana do utworzenia miejsc pracy dla ilości 50-200 osób. Oprócz samego obiektu należy wziąć pod uwagę również wyposażenie miejsc pracy.
Liczba personelu – szacunkowo obsługa strategicznej sieci bezpieczeństwa wymaga około 50-200 osób.

[163] Dz. U. 2017 poz. 59.

Tab. 37. Środki na utworzenie OSSB.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś – 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln – 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln – 50 mln)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne.

Zmiany regulacji prawnych – na tym etapie wymagane są zmiany w nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa[164], dział III o strategicznej sieci bezpieczeństwa oraz ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[165] art. 2. Należy jeszcze mieć na uwadze, że zachodzi potrzeba utworzenia programów rozwoju i innych dokumentów regulujących funkcjonowanie OSSB.

Koszty utworzenia – są wymagane w przedziale 1 mln - 10 mln z tytułu utworzenia miejsc pracy dla personelu tj. obsługi i kadry kierowniczej.

Utrzymanie miesięczne – przewiduje się nakłady rzędu 500 tyś - 1 mln zł miesięcznie z tytułu działalności bieżącej (utrzymanie infrastruktury oraz wypłaty).

Prezentowane wyliczenia stosowane w przypadku OSSB nie do końca mają rację bytu, ponieważ operator ten niezależnie od wyboru musi powstać. W związku z czym zmiana wyboru operatora nie wiąże się z dodatkowymi kosztami a przedstawione koszty nie powinny być brane pod uwagę przy zestawieniu sił i środków całego projektu.

Organy odpowiedzialne za walkę z dezinformacją.

W Europie plan działania przeciwko dezinformacji został ogłoszony 5 grudnia 2018 roku. Dokument ten określa kluczowe działania, które mają stanowić odpowiedź na problem dezinformacji. Komisja Europejska wskazuje w nim kroki, które powinny zostać zrealizowane przez unijne instytucje oraz państwa członkowskie. Dlatego propozycja

[164] Dz. U. 2018 poz. 1560.
[165] Dz. U. 2004 Nr 171 poz. 1800.

utworzenia Krajowej Rady ds. Dezinformacji jest zasadna. Założenie jest takie, aby radę tworzyli członkowie będący autorytetami, posiadającymi wiedzę i powszechnie uznaną wiarygodność w danej dziedzinie. Z tego też powodu zaleca się, aby byli to zasłużeni naukowcy z Polskiej Akademii Nauk. Skład rady powinien być ściśle powiązany z ilością dziedzin nauki[166] (8) tak aby każdą dziedzinę reprezentował po trzech uczonych. Pozwoli to utworzyć kolegium o możliwości udzielenia trzech odmiennych stanowisk w danej sprawie. Krajowa rada miałaby za zadanie wystosowywanie oficjalnego stanowiska w sprawach, do których przejawiają się odmienne poglądy mające znamiona dezinformacji. Koszty utworzenia rady zawiera tabela 38.

Tab. 38. Środki do walki z dezinformacją.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś – 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln – 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln – 50 mln)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne.

Infrastruktura – nie jest wymagana, ponieważ miejscem (siedzibą) Krajowej Rady ds. Dezinformacji będzie Polska Akademia Nauk.

Liczba personelu – nie jest wymagana, ponieważ Krajową Radę ds. Dezinformacji będą tworzyli uczeni z Polskiej Akademii Nauk.

Zmiany regulacji prawnych – na tym etapie wymagane są zmiany w ustawie z dnia 30 kwietnia 2010 r. o Polskiej Akademii Nauk[167], rozdział 3 o organach akademii.

Koszty utworzenia – nie są wymagane, ponieważ nie będzie tworzona dodatkowa infrastruktura z wyposażeniem oraz ma potrzeby pozyskania ekspertów.

[166] Dziedziny – nauk humanistycznych, nauk inżynieryjno-technicznych, nauk medycznych i nauk o zdrowiu, nauk rolniczych, nauk społecznych, nauk ścisłych i przyrodniczych, nauk teologicznych, sztuki.

[167] Dz. U. 2010 Nr 96 poz. 619.

Utrzymanie miesięczne – przewiduje się nakłady rzędu 20 tyś-100 tyś zł miesięcznie z tytułu działalności rady, w zależności od ilości spotkań roboczych[168].

Krajowa Rada ds. Dezinformacji, utworzona z autorytetów wchodzących w skład Polskiej Akademii Nauk cieszyłaby się społecznym uznaniem i stanowiłaby rzetelne źródło wiedzy. Biorąc pod uwagę, że uczestnictwo w przedmiotowym gremium stanowiłby dodatkowe honorarium zaleca się utworzenie odpowiednich wytycznych, które precyzowałyby odpowiednie wymagania rekrutacyjne tak aby w radzie zasiadali jedynie ludzie z jak najbogatszym dorobkiem naukowym.

Rozbudowa Centralnego Biura Zwalczania Cyberprzestępczości.

Dane statystyczne cyberprzestępczości wskazują na konieczność rozbudowy Centralnego Biura Zwalczania Cyberprzestępczości tak aby zaspokoić konieczność obsługi większej liczby przestępstw. Ważny w tym momencie jest fakt, że pieniądze odzyskane w wyniku działalności biura wracają do pokrzywdzonych oraz budżetu państwa. W związku z profilem działalności CBZC istnieje uzasadniona konieczność włączenia tej instytucji do Krajowego Systemu Cyberbezpieczeństwa co przełoży się na lepszy transfer ludzi, wiedzy i doświadczenia. Budowa obecnego biura kosztowała 48 mln zł, przy czym za lata 2022-2023 mienie odzyskane w wyniku działalności tego biura to 455 mln zł. W związku z czym stosując prostą matematykę można pokusić się o stwierdzenie, że biuro zwróciło się prawie dziesięciokrotnie. Rozbudowa instytucji przy założeniu, że podwojone zostaną zasoby pochłonie dość duże środki (tab. 39) natomiast w toku działalności biura środki te zwrócą się.

Tab. 39. Zasoby potrzebne na rozbudowę CBZC.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś – 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln – 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln – 50 mln)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne.

[168] Spotkania rady realizowane będą w zależności od potrzeby wypracowania stanowiska w danej sprawie.

Infrastruktura – jest wymagana, przy czym zaleca się utworzenie bliźniaczej infrastruktury w stosunku do istniejącego biura. Realizacja tego zadania powinna odbyć się poprzez rozbudowę jednej z ekspozytur regionalnych biura.
Liczba personelu – jest wymagana taka sama liczba pracowników jak w obecnym biurze, przy czym podział etatów na komórki wewnętrzne może być modyfikowany.
Zmiany regulacji prawnych – na tym etapie wymagane są zmiany w ustawie z dnia 17 grudnia 2021 r. o zmianie niektórych ustaw, w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości[169], cały art. 1 we wszystkich punktach. Natomiast nie ma potrzeby zmiany ustawy z dnia 6 kwietnia 1990 r. o Policji[170], ponieważ została ona już zmieniona pod kątem statutu działalności CBZC.
Koszty utworzenia – ponieważ będzie to bliźniacze biuro w stosunku do istniejącego to koszt (2018) będzie wynosił 48 mln plus inflacja co daje łącznie około 50 mln zł.
Utrzymanie miesięczne – będzie wynosiło tyle samo co obecnego biura, przy czym należy pamiętać, iż instytucja ta zarabia na siebie poprzez wpłaty odzyskanego mienia do budżetu państwa.

Drastycznie rosnący trend cyberprzestępstw w tym oszustw przy użyciu sprzętu teleinformatycznego wskazuje, że aby całkowicie wyeliminować ten rodzaj zagrożeń należałoby utworzyć 29 takich oddziałów przy uwzględnieniu „mocy przerobowej" istniejącego biura. Ilość środków, które są odzyskiwane poprzez działalność CBZC jest wystarczająca, aby zaspokoić potrzeby wdrożenia nie tyko przedmiotowej koncepcji, ale również innych organizacji realizującej zadania na rzecz cyberbezpieczeństwa.

Pozyskiwanie wyspecjalizowanego kapitału ludzkiego.

Istnieje już rozwiązanie tego problemu natomiast jest ono realizowane w sposób niewłaściwy. Mowa tu o doprecyzowaniu i konsekwentnym stosowaniu zapisów z rozporządzenie w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa. Obecnie z powodu niedoprecyzowania wytycznych dodatki te nie są wypłacane a kierownicy jednostek organizacyjnych stosują praktyki nieujęte w dokumencie, aby zminimalizować wypłacanie tych dodatków przy jednoczesnym pobieraniu go przez własne osoby. Rozporządzenie w swej treści przewiduje jakie kursy, dyplomy i certyfikaty uprawniają do otrzymania przedmiotowego świadczenia wraz z góry przewidzianą kwotą

[169] Dz. U. z 2021 r. poz. 1882 i 2333.
[170] Dz. U. 1990 Nr 30 poz. 179.

uzależnioną od stażu pracy w obrębie cyberbezpieczeństwa. Koniecznej zmianie muszą ulec:

- utożsamianie opisu karty stanowiska służbowego z zadaniami realizowanymi w ramach cyberbezpieczeństwa i wykazem zadań z rozporządzenia;
- określenie jasnych zasad przyznawania dodatku tak aby kierownicy jednostek organizacyjnych nie mieli podstaw prawnych do stosowania praktyk mających na celu uzależnianie wypłat świadczeń od dodatkowego egzaminu, który jest nieadekwatny w stosunku do realizowanych zadań.

Przykładem tego typu praktyk jest egzaminowanie pracowników pomimo posiadania przez nich ujętych w rozporządzeniu kursów i certyfikatów. Egzamin ten często zawiera pytania, które nie są w kompetencjach pracowników. Na przykład administrator sieci, który posiada dyplom Cisco CNNA oraz ukończony kurs Certified Ethical Hacking jest egzaminowany pytaniami z zakresu informatyki kwantowej lub zakresu znajomości danych statystycznych poszczególnych zagrożeń w odległych regionach świata. W związku z powyższym stosowanie tego typu praktyk ma na celu uniemożliwić poprzez dodatkowy egzamin, który z założenia jest niezdawalny, wypłatę świadczeń jak najmniejszej grupie pracowników. Przy czym sami kierownicy są zwalniani z brania udziału w egzaminach[171].

Tab. 40. Środki potrzebne do doprecyzowanie rozporządzenia.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś – 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln – 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln – 50 mln / mc)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne.

[171] Opis na podstawie doświadczeń autora podczas pracy w jednej z instytucji podlegającej po Komendanta Głównego Policji.

Wobec powyższych argumentów zaleca się doprecyzowanie rozporządzenia do akceptowalnych wytycznych tak aby pracownik, który przeszedł kurs z certyfikowaniem zakończony egzaminem nie musiał poddawany być dodatkowemu egzaminowi z góry ułożonego pod nie zdawalność. Koszty utworzenia rozwiązania zawarte są w tabeli 40.

Infrastruktura – nie jest wymagana, ponieważ zmianie ulega jedynie jeden dokument w postaci rozporządzenia.

Liczba personelu – nie jest wymagana, ponieważ doprecyzowanie rozporządzenia realizowane będzie przez zespół autorki tworzący przedmiotowy dokument.

Zmiany regulacji prawnych – zmianie podlega Rozporządzenie Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego, dla osób realizujących zadania z zakresu cyberbezpieczeństwa[172]. Zmiany w szczególności będą precyzowały:

- jasny proces przyznawania świadczeń;
- wprowadzenie trybu odwoławczego dla pracownika;
- tworzenie kart opisu stanowiska służbowego z realnymi zadaniami opisanymi w rozporządzeniu;
- konsekwencje prawne dla kierowników JO za stosowanie praktyk mających na celu wyjście poza ramy prawne przy przyznawaniu świadczeń.

Koszty utworzenia – nie są wymagane, ponieważ poprawa rozporządzenia będzie realizowana w ramach zadań służbowych osób uprawnionych.

Utrzymanie miesięczne – poprawa rozporządzenia pociągnie za sobą większą liczbę pracowników z przyznanym świadczeniem natomiast od momentu wprowadzenia rozporządzenia działania te są już wkalkulowane w budżet cyberbezpieczeństwa.

Wprowadzenie do świadczeń nowych zasad będzie kosztowne, ale taki był zamysł przedmiotowego rozporządzenia. Nie ma innej możliwości przyciągnięcia wykwalifikowanego specjalisty do administracji państwowej niż zapewnienie mu wynagrodzenia na równi lub zbliżonego z rynkiem „cywilnym". Z biegiem czasu przy sprawiedliwym przyznawaniu przedmiotowych świadczeń praca w administracji państwowej (pracownicy cywilni w formacjach mundurowych) zdobędzie na atrakcyjności.

[172] Dziennik Ustaw Rzeczypospolitej Polskiej Warszawa, dnia 20 stycznia 2022 r. Poz. 131

Pozyskiwanie środków finansowych na cyberbezpieczeństwo.

Propozycja zmiany abonamentu radiowo-telewizyjnego na abonament cyberbezpieczeństwa wydaje się słusznym pomysłem. Abonament pełniłby rolę tzw. ochrony cyberbezpieczeństwa. To oznacza, że każda osoba, która go opłaca ma prawo czynić roszczenia w przypadku, kiedy padnie ofiarą ataku teleinformatycznego. Przy takim założeniu jak obecnie obowiązuje np. w przypadku opłat za gospodarowanie odpadami. Oczywiście naliczanie nie powinno obejmować osób co do których orzeczono o niezdolności do samodzielnej egzystencji lub wobec których ustalono o[173]:

- zaliczeniu do I grupy inwalidów;
- całkowitej niezdolności do pracy;
- znacznym stopniu niepełnosprawności;
- trwałej lub okresowej całkowitej niezdolności do pracy w gospodarstwie rolnym;
- które otrzymują świadczenie pielęgnacyjne lub specjalny zasiłek opiekuńczy;
- niewidome, których ostrość wzroku nie przekracza 15%;
- które ukończyły 60 lat oraz mają prawo do emerytury;
- spełniające kryteria dochodowe, określone w ustawie z dnia 28 listopada 2003 roku o świadczeniach rodzinnych;
- które mają prawo do korzystania ze świadczeń pieniężnych z tytułu ustawy z dnia 12 marca 2004 roku o pomocy społecznej;
- bezrobotne;
- posiadające prawo do zasiłku przedemerytalnego;
- inwalidów wojennych i wojskowych;
- kombatantów będących inwalidami wojennymi lub wojskowym;
- członków rodzin pozostałych po kombatantach będących inwalidami wojennymi lub wojskowym;
- osób posiadających status weterana poszkodowanego.

Przy założeniu, że co roku począwszy od 2024 roku jest przeznaczane na fundusz cyberbezpieczeństwa 250 mln złotych z budżetu państwa[174] to dodatkowa kwota w postaci 3,72 mld rocznie (310 mln x 12) w znacznym stopniu podnosi wartość całego funduszu. Oczywiście z budżetu państwa odejdą wpłaty na abonament RiTV, przy czym

[173] Wytyczne pochodzą z regulacji o abonamencie RiTV.
[174] https://www.gov.pl/web/baza-wiedzy/wiecej-pieniedzy-na-fundusz-cyberbezpieczenstwa [dostęp: 20.06.2024].

obecnie skuteczność ściągalności tego podatku jest marginalna. Istotne jest również zastosowanie odpowiedniego mechanizmu motywacyjnego dla osób regularnie płacących przedmiotowy podatek. Jak już wspomniano należy uwzględnić system ubezpieczeń na okoliczność cyberprzestępstwa, gdzie osoba nie regulująca cyklicznie podatku nie ma możliwości ubiegania się o odszkodowanie lub innych roszczeń z tego tytułu oraz nie zakupi technologii ICT dla gospodarstwa domowego bez wylegitymowania się cyklicznie opłacanym podatkiem. Zyski z przedmiotowego podatku będą wystarczające, aby pokrywać koszty ubezpieczenia. Szczegółowy wykaz potrzeb prezentowany jest w tabeli 41.

Tab. 41. Koszt utworzenia abonamentu cyberbezpieczeństwa.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagana	nie są wymagane zmiany	nie są wymagane nakłady	nie są wymagane nakłady
2	niskie nakłady dla (1 - 20 osób)	wymagana w niskim stopniu (1 - 20 osób)	wymagane zmiany w niskim stopniu (1 - 2 dokument)	nakłady są wymagane w niskim stopniu (10 tyś - 100 tyś)	nakłady są wymagane w niskim stopniu (0 - 20 tyś / mc)
3	średnie nakłady dla (20 - 50 osób)	wymagana w średnim stopniu (20 - 50 osób)	wymagane zmiany w średnim stopniu (2 - 5 dokumenty)	nakłady są wymagane w średnim stopniu (100 tyś – 1 mln)	nakłady są wymagane w średnim stopniu (20 tyś - 100 tyś / mc)
4	duże nakłady dla (50 - 200 osób)	wymagana w dużym stopniu (50 - 200 osób)	wymagane zmiany w wysokim stopniu (5 - 10 dokumentów)	nakłady są wymagane w wysokim stopniu (1 mln – 10 mln)	nakłady są wymagane w wysokim stopniu (100 tyś - 500 tyś / mc)
5	bardzo duże nakłady dla (200 - 1000 osób)	wymagana w bardzo wysokim stopniu (200 - 1000 osób)	wymagane zmiany w bardzo wysokim stopniu (10 - 20 dokumentów)	nakłady są wymagane w bardzo wysokim stopniu (10 mln – 50 mln)	nakłady są wymagane w bardzo wysokim stopniu (500 tyś - 1 mln / mc)

Źródło: opracowanie własne.

Infrastruktura – nie jest wymagana, zadanie to może realizować Poczta Polska tak jak dotychczas lub przez Internet.

Liczba personelu – zniesienie abonamentu RiTV i egzekwowanie abonamentu cyberbezpieczeństwa realizowane będzie siłami już zaangażowanymi z Poczty Polskiej.

Zmiany regulacji prawnych – zmianie musi ulec ustawa z dnia 29 grudnia 1992 r. o Radiofonii i Telewizji[175], art. 6 oraz rozdział 4 dotyczący regulacji abonamentu. Należy również stworzyć regulamin opłat.

Koszty utworzenia – nie są wymagane koszty utworzenie przedmiotowego rozwiązania.

Utrzymanie miesięczne – utrzymanie miesięczne będzie takie samo jak w przypadku pobieranie abonamentu RiTV, przy czym w celu podniesienia skuteczności egzekucji zaleca się outsourcing firm windykacyjnych.

[175] Dz. U. z 2017 r. poz. 1414, 2111, z 2018 r. poz. 650, 915, 1717.

Abonament cyberbezpieczeństwa jako podatek byłby wysoko opłacalny. Biorąc pod uwagę, że nie będzie to kwota znacznie przewyższająca abonament RiTV to może być przyjęta z uznaniem społecznym. Obecnie abonament opłaca statystycznie 1/3 uprawnionych Polaków, przy czym jego egzekwowanie jest na bardzo niskim poziomie. Przy najmniej optymistycznych szacunkach, nawet gdyby ściągalność nowego abonamentu była na tym samym poziomie, to i tak daje to sumę 1,25 mld rocznie.

Rozwiązania, które zaprezentowano w rozdziale wymagają pewnych nakładów finansowych oraz osobowych. Zestawienie tych potrzeb przedstawiono w tabeli 42. Z tabeli wynika, że koszt wdrożenia przedstawionych rozwiązań wyniesie do 60 mln zł, a utrzymanie miesięczne to ponad 3 mln zł. Nie są to małe kwoty natomiast biorąc pod uwagę, że rozwiązanie zakłada rozbudowę biura CBZC oraz wprowadzenie abonamentu cyberbezpieczeństwa to generowane będą zyski roczne w postaci około 450 mln zł za walkę z cyberprzestępcami i około 3,1 mld zł z tytułu abonamentu co łącznie pozwala uzyskać 3,5 mld zł do budżetu państwa. Jest to kwota, która zaspokoi zarówno wdrożenie rozwiązań jak i ich utrzymanie oraz zapewni środki do pozyskania specjalistycznej kadry w administracji państwowej poprzez bezproblemowe wypłacanie świadczenia teleinformatycznego.

Tab. 42. Zestawienie środków niezbędnych do realizacji działań naprawczych.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagany	2 - 5 dokumentów	nie są wymagane	100 tyś - 500 tyś / mc
2	nie jest wymagana	nie jest wymagany	5 - 10 dokumentów	nie są wymagane	nie są wymagane
3	nie jest wymagana	nie jest wymagany	1 - 2 dokumentów	nie są wymagane	100 tyś - 500 tyś / mc
4	nie jest wymagana	nie jest wymagany	1 - 2 dokumentów	nie są wymagane	nie są wymagane
5	nie jest wymagana	nie jest wymagany	1 - 2 dokumentów	nie są wymagane	nie są wymagane
6	50 - 200 osób	50 - 200 osób	2 - 5 dokumentów	1 mln - 10 mln	500 tyś - 1 mln / mc
7	nie jest wymagana	nie jest wymagany	1 - 2 dokumentów	nie są wymagane	20 tyś - 100 tyś / mc
8	200 - 1000 osób	200 - 1000 osób	1 - 2 dokumentów	10 mln – 50 mln	500 tyś - 1 mln / mc
9	nie jest wymagana	nie jest wymagany	1 - 2 dokumentów	nie są wymagane	nie są wymagane
10	nie jest wymagana	nie jest wymagany	1 - 2 dokumentów	nie są wymagane	nie są wymagane
S	**250 - 1200 osób**	**250 - 1200 osób**	**16 - 34 dokumenty**	**11 mln - 60 mln**	**1,22 mln - 3,10 mln**

Źródło: opracowanie własne.

6.3. Badania eksperckie w zakresie użyteczności, funkcjonalności, realizowalności opracowanej koncepcji

W celu weryfikacji jakości proponowanych rozwiązań zostały one poddane ocenie poprzez pytania zawarte w wywiadach eksperckich. Ekspertami byli respondenci (szefowie, dowódcy) wyspecjalizowanych komórek administracji państwowej zajmujących się cyberbezpieczeństwem, instytucji wchodzących w skład Krajowego Systemu Cyberbezpieczeństwa oraz Systemu Bezpieczeństwa Narodowego. Wywiad przeprowadzony na kanwie kwestionariusza (załącznik nr 7) przedstawia dla każdej podatności opis problemu wraz z podaniem rozwiązania i szczegółowe wyliczenia wskaźników z obszaru doskonalenia. Respondenci ocenili każde z proponowanych rozwiązań w pięciostopniowej skali:

1 – proponowane rozwiązanie oceniam w stopniu niedostatecznym;
2 – proponowane rozwiązanie oceniam w stopniu miernym;
3 – proponowane rozwiązanie oceniam w stopniu dostatecznym;
4 – proponowane rozwiązanie oceniam w stopniu dobrym;
5 – proponowane rozwiązanie oceniam w stopniu bardzo dobrym.

Zaproponowana w ten sposób konstrukcja wywiadów pozwoliła na ilościową analizę jakości rozwiązań zawartych w przedmiotowej koncepcji.

Tab. 43. Zestawienie odpowiedzi respondentów na wywiad ekspercki.

EKSPERT / SYTUACJA PROBLEMOWA Z ROZWIĄZANIEM	nr. 1	nr. 2	nr. 3	nr. 4	nr. 5	nr. 6	nr. 7	nr. 8	nr. 9	nr. 10	SUMA PKT.
nr. 1	4	5	5	4	4	5	5	4	5	4	**45**
nr. 2	5	5	4	5	3	4	5	5	3	5	**44**
nr. 3	5	4	3	5	4	5	5	5	4	5	**45**
nr. 4	4	5	4	4	5	4	4	4	3	5	**42**
nr. 5	3	4	4	5	4	4	3	5	5	4	**41**
nr. 6	5	5	4	5	3	4	3	5	4	4	**42**
nr. 7	4	4	5	4	4	4	4	4	4	5	**42**
nr. 8	4	3	5	4	4	5	5	4	5	4	**43**
nr. 9	5	4	4	5	5	5	5	5	5	5	**48**
nr. 10	5	5	5	5	5	4	5	5	5	4	**48**
OCENA CAŁOŚCIOWA KONCEPCJI	**4**	**4**	**4**	**5**	**4**	**4**	**4**	**5**	**4**	**4**	**4,2 (4) 82%**

Źródło: opracowanie własne na podstawie kwestionariuszy wywiadów.

Wypełnione i zebrane wywiady zostały przedstawione w tabeli 43, celem całościowego wglądu w wyniki. W tabeli przedstawiono rozkład ocen względem problemów i ich rozwiązań zgodnie z kolejnością analiz zawartych w podrozdziale 6.2 oraz przypisanym numerem respondenta od 1 do 10 (łącznie 10 ekspertów). Respondenci pozostali anonimowi[176] a ich dane ze względu na RODO są w dyspozycji autora rozprawy. Po dokonaniu analizy na podstawie całościowego zestawienia można wywnioskować, jaki rozkład ocen zaistniał podczas opiniowania przez respondentów:

- najniżej oceniane rozwiązanie to - nr 5 (szkolenie uczniów - 41 pkt na 50);
- najwyżej oceniane rozwiązania to - nr 9, 10 (kadry, finanse - 48 pkt na 50);
- średnia arytmetyczna z ocen - 4,2 (max 5,0);
- procent całościowy (akceptacji) - 82%. (max 100%);
- ocena ogólna w pięciostopniowej skali - 4 (akceptacja w stopniu dobrym).

Wobec tak przedstawionych wyników należy uznać, że całokształt koncepcji spotkał się z uznaniem i ogólną akceptacją, ponieważ został oceniony w pięciostopniowej skali na ocenę 4. Oczywiście respondenci mieli pewne pomysły oraz rekomendowali modyfikacje w zaproponowanych rozwiązaniach stwierdzonych problemów jednak nie wszystkie uwagi miały uzasadnienie. Uwagi ekspertów wraz z komentarzami przedstawiono w formie punktów i w głównej mierze dotyczyły:

1) *Rekomendacja* - Ekspert zarekomendował, aby podczas implementacji rozwiązania mającego na celu wdrażanie narodowego programu szkolnictwa ustawowego dopełnić starań o zweryfikowanie czy obecnie w ramach zajęć z informatyki na etapie szkoły podstawowej nie ma działu jakim jest higiena cyfrowa, ponieważ będzie to zdublowaniem materiału do nauczania.
   Komentarz - Sprawdzono. Obecnie w szkołach na poziomie edukacji podstawowej (nauki wczesnoszkolnej) nie ma oficjalnie w programie elementów higieny cyfrowej ani innego przedmiotu wypełniającego znamiona przedmiotowych treści. Uwaga wniesiona przez eksperta nic nie zmienia w koncepcji.
2) *Rekomendacja* - Ekspert podał wątpliwość zasadność włączenia CBZC do Krajowego Systemu Cyberbezpieczeństwa.
   Komentarz - Jako uzasadnienie użyto argumentów mających na celu uświadomienie potrzeby wzmocnienia transferu wiedzy, umiejętności oraz kadr

[176] Anonimizacja respondentów została przeprowadzona w celu utrzymania obecnych kanonów prowadzenia wywiadów eksperckich w tym RODO oraz na życzenie samych ekspertów.

pomiędzy instytucjami. Ponadto instytucje powinny mieć możliwość wzajemnego wsparcia w przypadku wystąpienia zagrożenia na wielką skalę. Dodatkowo to kierowniczy personel CBZC sam inicjował rozmowy na ten temat w Komendzie Głównej Policji. Wobec czego uwaga wniesiona przez eksperta nie ma realnego uzasadnienia i nie powinna mieć wpływu na całościową koncepcję.

3) *Rekomendacja* - Ekspert zwrócił uwagę, że obecne oraz nowotworzone centra wymiany i analizy danych (ISAC) podlegają sprawdzeniu przez służby specjalnie oraz instytucje do tego powołane a co za tym idzie nie ma potrzeby sprawować nad nimi kontroli.

   Komentarz - Należy mieć na uwadze, że docelowo ma powstać około dwadzieścia kilka centrów a to dla służb specjalnych oraz instytucji, które obecnie są przeciążone zadaniami będzie stanowiło poważny problem, ponieważ każde z centr będzie sponsorowane przez kilka lub kilkanaście podmiotów. W związku z czym prezentowane rozwiązanie w postaci kontroli ISAC poprzez wyłonienie wiodącego Centra jest jak najbardziej słuszne a przedmiotowa uwaga wniesiona przez eksperta powinna być uzgodniona na szczeblu decyzyjnym. Na chwilę obecną uwaga nie zmienia nic w koncepcji.

4) *Rekomendacja* - Ekspert wyraził wątpliwości co do możliwości wdrożenia we wszystkich strategiach jednolitej rangi cyberbezpieczeństwa, ponieważ dokumenty powstają cyklicznie w różnych odstępach czasowych i nie ma możliwości zmiany ich w jednym czasie. Ponadto nie wszystkie strategie poziomu krajowego wymagają wysokiego poziomu cyberbezpieczeństwa.

   Komentarz - Uwaga jest słuszna, przy czym zmiana wszystkich dokumentów strategicznych w jednym czasie nie była intencją autora koncepcji. Dokładnie rzecz ujmując mowa jest o utrzymaniu właściwego poziomu cyberbezpieczeństwa podczas tworzenia każdej kolejnej strategii. Istotny jest również fakt, że nie wszystkie dokumenty poziomu strategii wymagają utrzymania wysokiego poziomu cyberbezpieczeństwa, przy czym jest to rozwiązanie dotyczące jedynie:

   - Długookresowa Strategia Rozwoju Kraju (DSRK);
   - Średniookresowa Strategia Rozwoju Kraju (ŚSRK);
   - Strategia Bezpieczeństwa Narodowego (SBN);
   - Strategia Rozwoju Systemu Bezpieczeństwa (SRSBN);
   - Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej (SCRP).

Wobec tak przedstawionej sytuacji można oddalić uwagę eksperta, ponieważ nie wnosi ona żadnych zmian do koncepcji.

5) *Rekomendacja* - Respondent zaproponował wdrożenie Operatora Strategicznej Sieci Bezpieczeństwa (OSSB) w oparciu o zdolności będące w posiadaniu Ministerstwa Obrony Narodowej.

   Komentarz - Analizując uwagę eksperta należy uznać, że takie rozwiązanie powinno być alternatywą w przypadku braku możliwości realizacji zadania OSSB przez NASK-PIB. Wobec czego uwaga eksperta jest zasadna i należy pozostawić ją do decyzji decydentów. W chwili obecnej uwaga nie zmienia koncepcji.

6) *Rekomendacja* - Ekspert pomimo pełnej aprobaty, obawiał się braku akceptacji przez środowisko decydentów rozwiązania mającego na celu utworzenie Krajowej Rady ds. Dezinformacji (KRD). Wątpliwości dotyczyły pytania: czy kazus francuski jest wystarczającym argumentem do przekonania klasy politycznej co do słuszności rozwiązania problemu?

   Komentarz - Należy uznać uwagę eksperta jako słuszną. Argumentem pomocniczym mogącym mieć wpływ na akceptację rozwiązania przez decydentów jest fakt, że na szczeblu całej Unii Europejskiej podejmowane są działania mające na celu walkę z dezinformacją i zjawiskami pokrewnymi. Wykorzystując powyższy przykład wraz z kazusem francuskim jako „namacalny" dowód na powodzenie przedmiotowego rozwiązania pozwala uznać argumentację jako wystarczającą. Obecnie uwaga wniesiona przez eksperta nic nie zmienia w koncepcji.

7) *Rekomendacja* - Ekspert miał wątpliwości co do przedmiotu z higieny cyfrowej w toku nauczania wczesnoszkolnego. Uważa on, że poziom klas wczesnoszkolnych jest to za wcześnie, aby tego typu przedmiot wprowadzić.

   Komentarz - Należy mieć świadomość, że współcześnie dzieci już w wieku od 4, 5 lat obcują z technologią cyfrową i jest to czas, kiedy należy ich działania w sieci ukierunkowywać. Jako argumentu wsparcia można użyć tu nauki jazdy na rowerze wraz z tłumaczeniem dziecku zasad bezpieczeństwa poruszania się na drogach podczas jazdy na tym rowerze. Tak samo powinno być z używaniem technologii cyfrowych, wobec czego należy oddalić uwagę i uznać ją jako nic nie zmieniającą w koncepcji.

8) *Rekomendacja* - Ekspert zaproponował, aby podczas podnoszenia rangi cyberbezpieczeństwa w dokumentach strategicznych przebadano i uwzględniono również podniesienie rangi innych obszarów bezpieczeństwa, ponieważ

dynamiczne zmiany w regionie Europy Środkowo-Wschodniej wymuszają holistyczne podejście do bezpieczeństwa.

Komentarz - Prowadzenie badań nad podnoszeniem rangi innych obszarów bezpieczeństwa jest poza obszarem badań prowadzonych w dysertacji, wobec czego uwaga nie jest uwzględniona w koncepcji a jedynie będzie widniała jako informacja dotycząca dalszych działań rozwojowych.

9) *Rekomendacje* - Ekspert przedstawił uwagi do rozwiązania problemu związanego z ustawodawczym szkoleniem w administracji państwowej. Sugeruje utworzenie specjalistycznego organu, którego zadaniem byłoby propagowanie i kontrolowanie szkoleń na szczeblu krajowym. Respondent zasugerował, że skoro szkolenia z cyberbezpieczeństwa mają być bliźniaczym szkoleniem do BHP to wskazane jest również utworzenie bliźniaczej instytucji do Państwowej Inspekcji Pracy celem monitorowania i kontroli przedmiotowych szkoleń (czyli np. Państwowej Inspekcji Cyberbezpieczeństwa przyp. autor).

   Komentarz - Tworzenie dodatkowych organów (instytucji, inspekcji) jest obciążone dodatkowymi kosztami w związku z czym nie jest wskazane. W badaniach zawartych w dysertacji nad rozwiązaniem przedmiotowego problemu uwzględniono koszty i wskazano organ kontrolny jakim jest Ministerstwo Cyfryzacji. Reasumując, przedmiotowa uwaga nie zostanie uwzględniona, ponieważ wykracza poza zakres ustalonych ram koncepcji.

10) *Rekomendacja* - Ekspert miał wątpliwości co do wysokości kwoty z zmodyfikowanego abonamentu RiTV, ponieważ kwota ta powinna być poddana analizie i głębszym badaniom społecznym. Dopasowanie odpowiedniej wysokości kwoty przełoży się na akceptację społeczną oraz wysoki poziom dobrowolnego regulowania opłaty (w przeciwieństwie do obecnego abonamentu RiTV).

    Komentarz - Uwaga jest zasadna i zostanie uwzględniona do dalszych badań rozwojowych na etapie wdrażania koncepcji.

Przedmiotowe uwagi i rekomendacje w większości zostały uwzględnione jedynie informacyjnie z przyczyn podanych w komentarzach natomiast należy podkreślić fakt, że eksperci poważnie podeszli do wywiadu angażując się na bardzo wysokim poziomie. Jak już wspomniano każde zaproponowane rozwiązanie do wdrożenia wymaga akceptacji zarówno środowiska decydentów jak i całego społeczeństwa. Dodatkowo jak sami eksperci podkreślają zawarte w koncepcji rozwiązania mają dość wysoki potencjał do akceptacji, ponieważ w głównej mierze oddziaływają na łączne potrzeby wszystkich

podmiotów w ujęciu całego państwa wraz z obywatelami na pierwszym miejscu. Sugestie ekspertów, które zostały wyeksponowane w zakończeniu dysertacji podczas wskazywania dalszych kierunków badań i szczegółowych prac nad wdrażaniem koncepcji, powinny również stanowić dodatkową informację dla decydentów. Na tym etapie nie są wymagane już żadne badania a wielkości sił i środków niezbędna do wdrożenia pożądanych rozwiązań eliminujących stwierdzone podatności została zaakceptowana przez ekspertów.

6.4. Ocena skutków implementacji koncepcji

Jak przedstawiono na wstępie rozdziału również zasadne jest dokonanie oceny skutków implementacji utworzonej koncepcji. Odbędzie się to poprzez zamieszczenie odpowiedzi na wskaźnikowe pytania do których należą:

Jaki problem jest rozwiązywany?

Podstawowym a zarazem najważniejszym problemem, który został rozwiązany jest poprawa stanu cyberbezpieczeństwa z poziomu systemów/podmiotów/obywateli. Należy w tym miejscu również uwzględnić główny problem badawczy rozprawy jakim jest odpowiedź na pytanie: Jakie luki, wady, słabości występują w obecnym Systemie Bezpieczeństwa Narodowego i w jaki sposób można ograniczać skutki ich wykorzystania do nieuprawnionych działań w celu podniesienia poziomu bezpieczeństwa państwa?

Jakie są rekomendowane rozwiązania, w tym planowane narzędzia interwencji oraz oczekiwany efekt?

Rekomendowane rozwiązania i niezbędne narzędzia potrzebne do realizacji celów zostały opisane w podrozdziale 6.2 wraz z oszacowaniem wielkości instytucji, ilością zmian regulacji prawnych oraz nakładami finansowymi.

Jak problem został rozwiązany w innych krajach, w szczególności krajach członkowskich UE?

Koncepcja zawiera szereg rozwiązań, które po części są zaczerpnięte z innych krajów Unii Europejskiej i Stanów Zjednoczonych Ameryki. Mowa tu o dwóch rozwiązaniach, które na wysokim poziomie funkcjonują za granicą a dotyczą Centrów Wymiany i Analizy Informacji (ISAC) z USA oraz utworzenia Krajowej Rady ds. Dezinformacji z Francji.

Na jakie podmioty oddziałuje koncepcja?

Utworzona koncepcja poprawy bezpieczeństwa państwa oddziałuje na podmioty opisane w rozdziale IV, a należą do nich:

- System Bezpieczeństwa Narodowego;
- Krajowy System Cyberbezpieczeństwa;
- System Zarządzania Kryzysowego;
- System Obrony Państwa;
- sektory bezpieczeństwa narodowego;
- podmioty ważne i kluczowe;
- zasoby informacyjne;
- podatności;
- obywatele.

Dodatkowo należy w to wliczyć wszystkie podsystemy i instytucje wchodzące w skład prezentowanych podmiotów oraz organy samorządu terytorialnego. Głównymi interesariuszami są organy Krajowego Systemu Cyberbezpieczeństwa, Zarządzania Kryzysowego oraz Systemu Bezpieczeństwa Narodowego.

Jakie są informacje na temat zakresu?

Zakres przedmiotowej koncepcji obejmuje spektrum bezpieczeństwa teleinformatycznego, bezpieczeństwa informacji oraz wybrane obszary bezpieczeństwa wewnętrznego i zewnętrznego, bezpieczeństwa fizycznego, bezpieczeństwa finansowego oraz bezpieczeństwa osobowego.

Jaki jest wpływ na sektor finansów publicznych?

Kwestie nakładów finansowych niezbędnych do wprowadzenia przedmiotowej koncepcji zostały wyliczone w rozdziale 6.2 wraz z ewentualnymi długofalowymi zyskami jakie przyniesie implementacja rozwiązań.

Jaki jest wpływ na konkurencyjność gospodarki i przedsiębiorczość oraz na rodzinę, obywateli i gospodarstwa domowe?

Przewiduje się następujący wpływ na powyższe sfery:

Konkurencyjność – w wyniku wprowadzenia nowelizacji rozporządzenia dotyczącego świadczeń teleinformatycznych na atrakcyjności zyska praca/służba w administracji państwowej wobec „cywilnego” rynku pracy.

Gospodarka i przedsiębiorczość – poprawa bezpieczeństwa w holistycznym ujęciu będzie działała korzystnie dla zagranicznych inwestorów i przyciągnięcie ich inwestycje do naszego kraju. Zostaną zainwestowane dość duże nakłady finansowe na badania w kraju na potrzeby utworzenia konsorcjum akademickiego.

Rodzina, obywatele i gospodarstwa domowe – przedmiotowe zmiany są oczekiwane przez społeczność. Przewiduje się poprawę poziomu społecznej świadomości, bezpieczeństwa oraz wspieranie rozwoju i wychowania w zdrowiu najmłodszych użytkowników technologii cyfrowych. Szkolenia pracowników w administracji państwowej przyczynią się do zwiększenia ochrony całych rodzin.

Jaki jest wpływ na rynek pracy?

Kształtowanie świadomości społecznej oraz podniesienie rangi i znaczenia cyberbezpieczeństwa wśród dokumentów strategicznych oraz prawnych będzie indukowało w społeczeństwie chęć rozwoju na kierunkach związanych z cyberbezpieczeństwem i technologiami cyfrowymi. Dodatkowo rozpoczęcie prac naukowo-badawczych nad nowymi technologiami oraz projektami mającymi na celu wykluczenie technologii od „dostawców wysokiego ryzyka" zapewni liczne miejsca pracy. Na atrakcyjności nabierze praca i służba w organach administracji państwowej poprzez nowelizację rozporządzenia o świadczeniach teleinformatycznych.

Jaki jest wpływ na pozostałe obszary?

Opracowana koncepcja w głównej mierze oprócz obszarów bezpieczeństwa będzie wpływała na takie dziedziny społeczne jak edukacja, programy naukowo-badawcze w tym rozwój uczelni, finanse publiczne (budżet), media oraz poziom „kultury" informacyjnej w państwie.

Jaki wpływ na regulacje prawne?

Propozycja zmian regulacji prawnych została przedstawiona w podrozdziale 6.2. Ostatecznie oprócz nowelizacji dokumentów poziomu strategii należy zmienić bądź zaktualizować łącznie w przedziale pomiędzy 16 a 34 dokumenty takie jak rozporządzenia, ustawy normy, porozumienia.

W jaki sposób i kiedy nastąpi ewaluacja efektów projektu oraz jakie mierniki zostaną zastosowane?

Jak już wspomniano wszystkie utworzone rozwiązania są inwestycjami, na które początkowo trzeba dużo włożyć i długo czekać na efekty. Biorąc pod uwagę zasięg

opracowanej koncepcji to pierwsze efekty widoczne będą już po 6 miesiącach (opracowanie dokumentacji) oraz pojawią się efekty długoterminowe (uświadamianie społeczne), których efekty będą widoczne dopiero za kilka lat.

6.5. Podsumowanie rozdziału

Implementacja opracowanej koncepcji pozwoliła wskazać jakie inwestycje należy poczynić, aby w pełni wdrożyć przedmiotowe rozwiązania. Analiza potrzeb w obszarach doskonalenia wykazała, że aby całościowo wyeliminować stwierdzone podatności należy utworzyć lub zainwestować w następujące elementy:

- Infrastrukturę tj. nowe instytucje lub rozbudowę istniejących wraz nowymi stanowiskami dla wykwalifikowanych specjalistów i personelem pomocniczym oszacowaną średnio na 500 miejsc pracy łącznie;
- Personel rozumiany jako dziedzinowi specjaliści wraz personelem pomocniczym, oszacowanym średnio na 500 osób łącznie;
- Zmianę regulacji prawnych, w tym rozporządzenia, ustawy, kodeksy pracy, normy i standardy w ilości średniej około 25 dokumentów;
- Koszty utworzenia, rozumiane jako budowa lub rozbudowa instytucji wraz z wdrożeniem planów naukowo badawczych wyniesie średnio 60 mln zł w fazie wstępnej;
- Koszty utrzymania, w miesięcznej skali utworzonych miejsc pracy oraz infrastruktury wyniesie średnio około 3 mln zł.

Ponadto, należy mieć świadomość, że przytoczone wartości są mocno przybliżone i obliczone na podstawie bliźniaczych istniejących już rozwiązań. Wobec czego rzeczywiste wartości mogą być wyższy w granicach tolerancji, nawet o 10-20% ostatecznej sumy. Analizując wydatki należy wziąć pod uwagę długofalowe zyski jakie będą generowane z tytułu walki z cyberprzestępczością oraz modyfikacji abonamentu RiTV. Z szacunkowych obliczeń wynika, że w optymistycznym wariancie może być to kwota rzędu 310 mln[177] zł miesięcznie. Co daje 3,72 mld rocznie (310 mln x 12 miesięcy) z tytułu abonamentu oraz 455 mln rocznie z tytułu walki z cyberprzestępczością przy założeniu rozbudowy CBZC. Łączne zyski z przedmiotowych działań osiągną 4,17 mld zł. Jest to niebagatelna kwota, ponieważ obecny Fundusz Cyberbezpieczeństwa wynosi

[177] Przy założeniu, że akceptowalność i windykacja abonamentu będą na poziomie około 90%.

jedynie 250 mln zł rocznie.

Należy podkreślić, że interesująco brzmią wskaźniki z oczekiwanych skutków wprowadzenia przedmiotowej koncepcji, ponieważ poprawie ulegnie nie tylko obecny stan cyberbezpieczeństwa, ale i również inne obszary bezpieczeństwa co pozostanie nie bez znaczenia. Z gospodarczego punktu widzenia zainwestowane pieniądze szybko się zwrócą, przybędzie miejsc pracy, zmniejszy się poziom cyberprzestępczości a obywatele będą świadomi zagrożeń wykorzystujących cyberprzestrzeń.

ZAKOŃCZENIE

Głównym celem badań w dysertacji była identyfikacja luk, wad, słabości w Systemie Bezpieczeństwa Narodowego i opracowanie na podstawie ich wyników koncepcji zwiększenia poziomu bezpieczeństwa państwa. Problem badawczy przedstawiono w formie pytania: Jakie luki, wady, słabości występują w obecnym Systemie Bezpieczeństwa Narodowego i w jaki sposób można ograniczać skutki ich wykorzystania do nieuprawnionych działań w celu podniesienia poziomu bezpieczeństwa państwa? W związku z tym powstała hipoteza zakładająca, że w cyberprzestrzeni występuje szereg zagrożeń dla bezpieczeństwa narodowego, które wymagają stosownych odpowiedzi ze strony instytucji państwa w szczególności eliminacji podatności obniżających odporność państwa na cyberzagrożenia.

W rozprawie doktorskiej wykorzystano szereg metod, technik i narzędzi badawczych. W ramach przygotowania do wprowadzenia w dziedzinę problemu dokonano krytycznej analizy istniejących definicji podstawowych pojęć oraz uzupełniono je autorskimi definicjami. W celu dokonania wglądu w rodzaje zagrożeń przeprowadzono studium przypadków zdarzeń mających poważne konsekwencje i w znacznym stopniu przyczyniających się do utraty informacyjnej ciągłości działania organizacji. Metoda ta była przydatna, ponieważ pomogła przedstawić przypadki zdarzeń mających duży rozgłos oraz wpływ na zmiany w systemach wielu krajów. Przegląd kluczowej dla obszaru badań dokumentacji normatywnej pozwolił na wstępną analizę podatności z poziomu strategii, polityk, ustaw, rozporządzeń. Działania te z połączeniu z analizą statystyk wraz z odpowiedziami na wywiad ekspercki pozwoliły na utworzenie zbioru zagrożeń, który został skonfrontowany z zdolnościami Systemu Bezpieczeństwa Narodowego celem wyłonienia tych zagrożeń, na które obecny system jest nieprzygotowany. To właśnie te metody badawcze okazały się najbardziej przydatne przy tworzeniu koncepcji.

Główny cel oraz szczegółowe zrealizowano poprzez sześć merytorycznych rozdziałów wraz z wstępem oraz zakończeniem. W rozdziale pierwszym dokonano przeglądu kluczowych dla obszaru badań pojęć wraz z ustaleniem ich definicji. Zaistniała tu potrzeba redefinicji takich pojęć jak cyberbezpieczeństwo, informacyjna ciągłość działania i Systemu Bezpieczeństwa Narodowego. Ponadto w rozdziale tym dokonano przedstawienia głównych systemów bezpieczeństwa państwa wraz utworzeniem na nowo schematu operacyjnego tych systemów. Dodatkowo dokonano analizy porównawczej

rozwiązań oraz samego podejścia do cyberbezpieczeństwa wybranych państw europejskich i Stanów Zjednoczonych Ameryki. Wnikliwa analiza dokumentacji szczebla strategicznego, pozwoliła na zdiagnozowanie na tym etapie pewnych podatności prawno-proceduralnych, które były przedmiotem dalszych badań.

Rozdział drugi był metodycznym opisem wykonywanych badań wraz z uzasadnieniem podjęcia przedmiotowej problematyki. Zostały tu opisane cele: poznawczy i utylitarny. Ponadto przedstawiono problemy badawcze oraz hipotezy z jednoczesnym wyeksponowaniem logicznego ciągu podejmowanych działań wraz z wymienionymi metodami, narzędziami badawczymi, które posłużyły do osiągnięcia zakładanego celu głównego i szczegółowych. W części tej zdefiniowano kierunek badań oraz przedstawiono jakie zagadnienia będą rozpatrywane w procesie badawczym z jednoczesnym uargumentowanym odcięciem się od problematyki, która nie była przedmiotem badań. Ustalono ograniczenia czasowe i przestrzenne. Dodatkowo dokonano analizy literatury kluczowej dla danej dziedziny badań celem przedstawienia obecnego stanu wiedzy.

W trzeciej części dysertacji dokonano przeglądu studium przypadku celem odzwierciedlenia istoty i skali zagrożeń jakie dotychczas się zmaterializowały. Metodą „desk research" zestawiono dane statystyczne czołowych instytucji krajowych zajmujących się cyberbezpieczeństwem w celu wyeksponowania sposobów realizacji zagrożeń, narzędzi, metod i technik wykorzystywanych do realizacji zagrożeń oraz dalszej identyfikacji podatności. Uwieńczeniem rozdziału było przeprowadzenie wywiadów i wywiadów eksperckich mających na celu zdiagnozowanie wad, luk i słabości systemowych instytucji kluczowych z punktu widzenia bezpieczeństwa. Końcową częścią tego etapu badań było skonfrontowanie wyłonionych „zagrożeń" z zdolnościami obronnymi i ochronnymi Systemu Bezpieczeństwa Narodowego wraz z podsystemami celem utworzenia katalogu „zagrożeń szczątkowych" na które obecny system nie jest przygotowany.

Rozdział czwarty dotyczył wykorzystania elementów zarządzania ryzykiem w celu zbadania jakie będą oczekiwane straty przy założeniu, że nie zostaną podjęte żadne działania naprawcze wobec obecnego stanu. Poprzez zestawienie podatności z elementami składowymi wykorzystywanymi do materializacji zagrożeń oraz zdefiniowanymi podmiotami/systemami uzyskano kluczowe wskaźniki ryzyka, które posłużyły jako punkt wyjściowy do tworzenia koncepcji poprawy bezpieczeństwa. Jako

metodę zarządzania ryzykiem przyjęto minimalizację ryzyka poprzez eliminację zdiagnozowanych podatności.

Przedmiotowa koncepcja poprawy bezpieczeństwa została opisana w rozdziale piątym. Dla każdej stwierdzonej podatności zostało przedstawione rozwiązanie problemu w ujęciu obszarów takich jak finansowo-ekonomiczny, prawno-proceduralny, techniczno-logistyczny i mentalny. W celu zweryfikowania zalet i wad dla każdego rozwiązania przeprowadzono analizę SWOT co pozwoliło nie tylko na wyeksponowanie mocnych stron i szans, ale też ujawniło ukryte (nieznane) zagrożenia i słabe strony.

Ostatni rozdział zawiera propozycję sposobu implementacji opracowanej koncepcji poprawy bezpieczeństwa. Każda eliminowana podatność (każde rozwiązanie z rozdziału V) zostało opisane na podstawie niezbędnych do osiągnięcia zakładanego celu wskaźników takich jak: rozbudowa niezbędnej infrastruktury, pozyskanie wyspecjalizowanych kadr, zmiana niezbędnych regulacji prawnych, wstępne koszty utworzenia i cykliczne koszty utrzymania. Dokonane w taki sposób zestawienie pozwoliło na analizę wymaganych nakładów sił i środków do implementacji przedmiotowej koncepcji. W końcowym etapie utworzona koncepcja została poddana opinii eksperckiej oceny proponowanych rozwiązań.

W wyniku przeprowadzonych badań stwierdzono, że obecnie najważniejszy system bezpieczeństwa państwa, jakim jest niewątpliwie System Bezpieczeństwa Narodowego wymaga aktualizacji. Biorąc pod uwagę, że obecnie żyjemy w czasach pomiędzy IV i V rewolucją przemysłową, której imperatywami są Internet, Sztuczna Inteligencja i komputery kwantowe, to współczesny System Bezpieczeństwa Narodowego wraz z podsystemami (SZK, KSC, SOP, itp.) powinien opierać się przede wszystkim na solidnej, spójnej, aktualnej dokumentacji strategicznej z jednoczesną wizją rozwoju dla tych systemów. Ponieważ cyberbezpieczeństwo zaczyna się od strategii, polityk, wizji i regulacji prawnych, to punktem wyjściowym do dalszych działań jest podniesienie rangi cyberbezpieczeństwa do poziomu ponaddziedzinowego. Jak wskazują badania zawarte w dysertacji jest to warunek konieczny do tego, aby wszystkie systemy bezpieczeństwa państwa mogły mieć zdolność do wypełniania zadań na wysokim poziomie skuteczności i efektywności. Kolejnym czynnikiem podnoszącym bezpieczeństwo jest techniczna rozbudowa obecnych instytucji (CBZC) oraz utworzenie nowych organizacji (KRD) w administracji państwowej. Jak wykazały analizy instytucje te zminimalizują poziom cyberprzestępczości oraz dezinformacji w przestrzeni

publicznej. Nie bez znaczenia pozostają tu rozwiązania, które zniwelują dwa najpoważniejsze problemy w cyberbezpieczeństwie tzn. niski poziom finansowania cyberbezpieczeństwa i brak specjalistycznych kadr. Proponowane w tym zakresie rozwiązania jak wskazują analizy przewidują na wprowadzenie do budżetu państwa corocznie około 4,17 mld zł. Prezentowana kwota pozwoli na zatrudnienie wielu wysokiej klasy specjalistów o pożądanych kwalifikacjach zajmujących się cyberbezpieczeństwem oraz poprawę warunków finansowych obecnych pracowników. Jednocześnie kwoty te pokryją nieliczne, ale konieczne koszty wdrożenia w życie opracowanej koncepcji poprawy bezpieczeństwa państwa. Uzupełnieniem koncepcji są rozwiązania mające na celu podnoszenie świadomości obywateli. Realizacja tego zamiaru planowana jest dwutorowo. Po pierwsze szkolenie ustawowe dzieci na poziomie wczesnoszkolnym z przedmiotu higiena cyfrowa. Po drugie obowiązkowe szkolenia pracowników administracji państwowej z cyberbezpieczeństwa. Połączenie obu szkoleń spowoduje, że wzrośnie nie tylko świadomość obywateli na zagrożenia w cyberprzestrzeni, ale również przyczyni się do akceptacji społeczeństwa na wprowadzane zmiany i konieczność poniesienia odpowiednich nakładów na zwiększenie sił i środków niezbędnych do utrzymania krajowego cyberbezpieczeństwa na wysokim poziomie.

W procesie badawczym na poziomie instytucjonalnym (Załączniki 3-6) wg załączonego kwestionariusza (Załącznik 2) napotkano na bariery formalne i związany z tym niski poziom skuteczności badawczej. Stąd też odwołano się do indywidualnych ekspertów dziedzinowych, przy czym szczegółowy spersonalizowany zbiór odpowiedzi (znany autorowi) został zanonimizowany (z uwagi na RODO) i umieszczony w odrębnej broszurze (Załącznik nr 8). Syntetyczne wyniki zamieszczone są w treści rozprawy wg kwestionariusza wywiadu końcowego (Załącznik 7). Wyniki te pozwalają na potwierdzenie, że przedmiotowa koncepcja poprawy bezpieczeństwa jest zasadna i pożądana. Zgodnie z rekomendacjami ekspertów należy co prawda podjąć dodatkowe działania mające na celu realizację sondażu diagnostycznego ustalając wysokość stawki na podatek, ale jest to możliwe tylko w momencie realnego wdrażania koncepcji. Na uznanie zasługuje również rekomendacja utworzenia Operatora Strategicznej Sieci Bezpieczeństwa OSSB w zasobach Ministerstwa Obrony Narodowej, ale tylko w przypadku niepowodzenia realizacji tego zadania w NASK-PIB zgodnie z przedmiotową koncepcją.

Jak już wspomniano współcześnie żyjemy na przełomie IV i V rewolucji przemysłowej, gdzie cyfryzacja i digitalizacja „wszystkiego" stała się codziennością a wiele klasycznych systemów bezpieczeństwa funkcjonuje w oparciu o technologie cyfrowe. Doinwestowanie cyberbezpieczeństwa, aktualizacja procedur, wdrażanie nowych technik i kształtowanie przestrzeni informacyjnej tej w dziedzinie przełoży się na poprawę bezpieczeństwa niemal w każdym obszarze Rzeczpospolitej Polskiej. Podchodząc do wizji prowadzenia dalszych badań należałoby usystematyzować i cyklicznie przeprowadzać podobne analizy do tych zawartych w przedmiotowej dysertacji po to, aby w maksymalny sposób wykorzystać społeczne, prawne i technologiczne zmiany, na korzyść naszego państwa. Nie dotyczy to tylko cyberbezpieczeństwa wręcz przeciwnie w każdym obszarze bezpieczeństwa taka analiza jest pożądana. Przedmiotowe badania wskazują na to, że dynamika obecnych zmian w środowisku cyberprzestrzeni wymaga wręcz cyklicznej aktualizacji oraz zorientowania na nowe często nieznane kierunki zagrożeń wszystkich systemów bezpieczeństwa państwa. Z tego też powodu należy uznać słuszność stwierdzenia, że cyberprzestrzeń i cyberbezpieczeństwo są realnymi determinantami bezpieczeństwa współczesnego państwa.

WYKAZ LITERATURY

Pozycje książkowe

1. Apanowicz J., 2005, Metodologiczne uwarunkowania pracy naukowej. Prace doktorskie. Prace habilitacyjne, Difin, Warszawa.
2. Babbie E., 2013, Podstawy badań społecznych, Wyd. PWN, Warszawa.
3. Bielski M., 2002, Podstawy teorii organizacji i zarządzania, C.H. Beck, Warszawa.
4. Brzeski R., 2014, Wojna informacyjna – wojna nowej generacji, wyd. Antyk, Komorów.
5. Cieślarczyk M. (red. nauk.), 2003, Metody, techniki i narzędzia badawcze oraz elementy statystyki stosowane w pracach magisterskich i doktorskich, AON, Warszawa.
6. Dąbrowski M., 2022, Wyzwania i zagrożenia dla bezpieczeństwa Europy środkowo-wschodniej. Dezinformacja w działaniach hybrydowych, [w] Bezpieczeństwo Europy Środkowo-Wschodniej Perspektywa narodowa i międzynarodowa, Kominek, Ł., Balogh O., Śmiałek W., (red. nauk.), Wyd. Fundacja na rzecz Czystej Energii, Boża Wola.
7. Ficoń K., 2007, Inżynieria zarządzania kryzysowego. Podejście systemowe, BEL Studio, Warszawa.
8. Flakiewicz W., 2002, Systemy informacyjne w zarządzaniu (uwarunkowania, technologie, rodzaje), C.H. Beck, Warszawa.
9. Goodman M., 2016, Zbrodnie przyszłości. Jak cyberprzestępcy, korporacje i państwa mogą używać technologii przeciwko tobie., Wyd. Helion, Gliwice.
10. Gryz J., Kitler W. (red. nauk.), 2012, System reagowania kryzysowego, wyd. Adam Marszałek, Toruń.
11. Jagusiak B., 2019, Zagrożenia procesów informacyjnych w systemie bezpieczeństwa państwa: zagadnienia wybrane, WAT, Warszawa.
12. Jakubczak R., Flis J., 2006, Bezpieczeństwo Narodowe Polski w XXI wieku, Dom Wydawniczy Bellona, Warszawa.
13. Jaźwiński J., 1993, Ważyńska-Fiok K., Bezpieczeństwo systemów, PWN, Warszawa.
14. Kaczmarek T., Ćwiek G., 2009, Ryzyko kryzysu a ciągłość działania. Business Continuity Management, Difin, Warszawa.
15. Kamola M., Arabas P., 2018, Sieci społeczne i technologiczne. Jak zrozumieć, jak wykorzystać, Wyd. PWN, Warszawa.

16. Kaszubski R., Romańczuk D. (red.), 2012, Księga dobrych praktyk w zakresie zarządzania ciągłością działania. Business Continuity Management, Związek Banków Polskich, Warszawa.
17. Kowalewski M., 2015, Aspekty bezpieczeństwa narodowego rzeczypospolitej polskiej, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.
18. Kowalewski M., 2021, Cyberprzemoc szczególnym zagrożeniem społeczeństwa informacyjnego, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.
19. Krawiec J., 2019, Cyberbezpieczeństwo podejście systemowe, Oficyna Wydawnicza Politechniki Warszawskiej, Warszawa.
20. Kuc B., Ścibiorek Z., 2013, Podstawy metodologiczne nauk o bezpieczeństwie, wyd. Menedżerskie PTM, Warszawa.
21. Lakomy M., 2015, Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw, Wyd. Uniwersytet Śląski, Katowice.
22. Liderman K., 2017, Bezpieczeństwo informacyjne. Nowe wyzwania, Wydawnictwo Naukowe PWN, Warszawa.
23. Liderman K., 2008, Analiza ryzyka i ochrona informacji w systemach komputerowych, PWN, Warszawa.
24. Luttgens J., Pepe M., Mandia K., 2016, Incydenty bezpieczeństwa. Metody reagowania w informatyce śledczej, Helion, Gliwice.
25. Mayer-Schonenberger V., 2014, Cukier K.: Big Data. Rewolucja, Która Zmieni Świat, Pracę I Życie. MT Biznes. Warszawa.
26. Miller M., 2016, Internet Rzeczy. Jak Inteligentne Telewizory, Samochody, Domy I Miasta Zmieniają Świat, PWN. Warszawa.
27. Mazur M., 1999, Cybernetyka i charakter, Wyższa Szkoła Przedsiębiorczości i Zarządzania im. B. Jańskiego w Warszawie, Warszawa.
28. Nowak E., 2007, Zarządzanie kryzysowe w sytuacjach zagrożeń niemilitarnych, AON, Warszawa.
29. Pamuła W., 2011, Niezawodność i bezpieczeństwo. Wybór zagadnień, PŚ, Gliwice.
30. Sienkiewicz P., 1983, Inżynieria systemów, MON, Warszawa.
31. Sienkiewicz P., 1988, Poszukiwanie Golema. O cybernetyce i cybernetykach, Krajowa Agencja Wydawnicza, Warszawa.
32. Schwab K., 2018, Czwarta rewolucja przemysłowa, tłum. A.D. Kamińska,

wydawnictwo studio Emka, Warszawa.
33. Syta J., 2025, Zarządzanie cyberbezpieczeństwem. Pracownicy, Procesy, Technologie, Wydawnictwo Naukowe PWN, Warszawa.
34. Szymański J., 1991, Życie systemów, Wyd. Wiedza Powszechna, Warszawa.
35. Wiener N., 1971, Cybernetyka, czyli sterowanie i komunikacja w zwierzęciu i maszynie, PWN, Warszawa.
36. Włoch R., Śledziewska K., 2020, Gospodarka cyfrowa. Jak nowe technologie zmieniają świat, Wydawnictwa Uniwersytetu Warszawskiego, Warszawa.
37. Wołowski J., Zawiła-Niedźwiecki J., 2012, Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, edu-Libri, Kraków.
38. Woźniak J., Zaskórski P., 2018, Projektowanie Organizacji Procesowej. Perspektywa Systemów Analitycznodecyzyjnych, WAT, Warszawa.
39. Zaskórski P. (red. nauk.), 2011, Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania, WAT, Warszawa.
40. Zaskórski P., 2012, Asymetria informacyjna w zarządzaniu procesami, WAT, Warszawa.
41. Zaskórski P., Woźniak J., Szwarc K., Tomaszewski Ł., 2015, Zarządzanie projektami w ujęciu systemowym, WAT, Warszawa.
42. Zaskórski P., Zaskórski W., Woźniak J., 2021. Świadomość sytuacyjna a bezpieczeństwo i informacyjna ciągłość działania w organizacjach rozproszonych, wyd. CeDeWu.
43. Zajko D., Zaskórski P., 2020, Wybrane problemy bezpieczeństwa osobowego. Systemy ochrony VIP. Organizacja i efektywność funkcjonowania, WAT, Warszawa.

Artykuły w czasopismach

1. Czaja S., Becla A., 2016, Wybrane informacyjne problemy definiowania zrównoważonego i trwałego rozwoju, ujęcie teoretyczne, Uniwersytet Ekonomiczny we Wrocławiu, Optimum. Studia Ekonomiczne nr. 1 (79), s 17.
2. Kołodziejczak M., Wymiar prawny systemu kierowania bezpieczeństwem narodowym RP., Studenckie Zeszyty Naukowe 2019, Vol. XXII, nr 42., s. 93
3. Marczyk M., 2018, Cyberprzestrzeń jako nowy wymiar aktywności człowieka – analiza pojęciowa obszaru, Przegląd teleinformatyczny, Warszawa, NR 1-2, 59, s. 59.
4. Sienkiewicz P., 2015, Ontologia cyberprzestrzeni, Zeszyty Naukowe WWSI,

Warszawa, No 13, Vol. 9, s.15.
5. Spustek H., Paluch A., 2017, Struktura systemu bezpieczeństwa narodowego polski. Uniwersytet Opolski, Zeszyty naukowe politechniki śląskiej, seria: organizacja i zarządzanie z. 100 Nr kol. 1972, s. 109.
6. Szwarc K., Zaskórski P., 2012, Identyfikacja zagrożeń dla ciągłości działania organizacji, Studia Bezpieczeństwa Narodowego, Warszawa, Tom R. 2, Nr 3, s. 215.
7. Wieczorek P., 2018, Czwarta rewolucja przemysłowa, Wizja przemysłu nowej generacji - perspektywa dla Polski, Państwo i społeczeństwo, Kontrola Państwowa, Warszawa, R. 63, nr 3, s. 89-115
8. Zaskórski P., 2012, Ewaluacja projektów, Zeszyty Naukowe Wyższej Szkoły Informatyki w Warszawie, nr 8, s. 36.

Międzynarodowe akty prawne

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27.04.2015 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE ogólne rozporządzenie o ochronie danych.
2. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2000/31/WE z dnia 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, 2w szczególności handlu elektronicznego w ramach rynku wewnętrznego.
3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2001/29/WE z dnia 22.05.2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym.
4. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2002/58/WE z dnia 12.07.2002 r. o prywatności i komunikacji elektronicznej – dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej.
5. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2005/222//WSiSW z dnia 30.09.2010 r. dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady.
6. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2006/24/WE z dnia 15.03.2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca Dyrektywę 2002/58/WE.

7. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2009/136/WE z dnia 25.11.2009 r. zmieniająca Dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, Dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie WE nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, zmieniona Dyrektywą 2009/136/WE.
8. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2011/83/UE z dnia 25.10.2011 r. w sprawie praw konsumentów, zmieniająca Dyrektywę Rady 93/13/EWG i Dyrektywę 1999/44/WE Parlamentu Europejskiego i Rady oraz uchylająca Dyrektywę Rady 85/577/EWG i Dyrektywę 97/7/WE Parlamentu Europejskiego i Rady.
9. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2013/40/UE z dnia 12.08.2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiS, Dz. U. UE, L 218 z dnia 14.08.2013 r.
10. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz. U. UE, L 194/1, PL 19.07.2016.
11. Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 17.12.2011 r. w sprawie zwalczania niegodziwego traktowania i wykorzystywania seksualnego dzieci, w tym pornografii dziecięcej na stronach internetowych, Dz. U. L 335 z 17.12.2011.
12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2016/679 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE ogólne rozporządzenie o ochronie danych, Dz. U. UE L 119, 4.05.2016, Bruksela 2016.
13. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21.05.2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji ENISA oraz uchylające rozporządzenie WE nr 460/2004, Dz. U. UE, PL 18.06.2013 r., L 165/41, Bruksela 2013.
14. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23.07.2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu

do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE, Dz. U. UE L 257 z 28.08.2014, Bruksela 2014.
15. Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 12.09.2018 ustanawiające Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji, COM 2018 630 final 2018/0328 COD, Bruksela 2018.
16. Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 7.06.2018 r. ustanawiają-ce program ramowy w zakresie badań naukowych i innowacji „Horyzont Europa" oraz zasady uczestnictwa i upowszechniania obowiązujące w tym programie, Komisja Europejska, COM 2018 435 final, 2018/0224 COD, Bruksela 2018.
17. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 460/2004 z dnia 10.03.2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, Dz.U. L 77 z dnia 13.03.2004, Bruksela 2004.
18. Rozporządzenie Parlamentu Europejskiego i Rady (UE) z dnia 12.09.2018 r., ustanawiające Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji, COM 2018 630 final, 2018/0328 COD, Komisja Europejska, Bruksela 2018.
19. Rozporządzenie Parlamentu Europejskiego i Rady (UE) ustanawiające program „Cyfrowa Europa na lata 2021-2027" z dnia 6.06.2018, SWD 2018 306 final, COM 2018 434 final, 2018/0227 COD, Bruksela 2018.
20. Rozporządzenie w zakresie swojej regulacji wdraża dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Dz. U. E L 194 z dnia 19.07.2016 r., Bruksela 2016.
21. Traktat między Rzeczpospolitą Polską a Federacją Rosyjską o przyjaznej i dobrosąsiedzkiej współpracy, Dz. U. 1993 Nr 61 poz. 291.
22. Traktat o funkcjonowaniu Unii Europejskiej, Dz. U. UE nr C 115 z dnia 9.05.2008 r.
23. Traktat ustanawiający Konstytucję dla Europy, Dz. U. UE, nr C 310 z dnia 16.12.2004 r.
24. Traktat Waszyngtoński, Dz. U. 2000, nr 87, poz. 970.
25. Konwencja Rady Europy o zwalczaniu cyberprzestępczości z dnia 23.11.2001 r., Dz. U. 2015 r. poz. 728.

26. Konwencja Rady Europy o zwalczaniu terroryzmu z dnia 27.01.1977 r., Dz. U. 1996 r. nr 117, poz. 557.
27. Konwencja Rady Europy o zapobieganiu terroryzmowi z dnia 16.05.2005 r., Dz. U. 2008 r. nr 161, poz. 998.
28. Konkluzje Rady Europy z dnia 9.06.2016 r. w sprawie poprawy rzetelności w sprawach karnych w cyberprzestrzeni, a także Konkluzje Rady w sprawie dalszych prac nad usprawnieniem wymiany informacji i zapewnieniem interoperacyjności unijnych systemów informacyjnych z dnia 14.06.2017 r.

Polskie akty prawne

1. Decyzja Ministra Obrony Narodowej nr 357/MON z dnia 29.07.2008 r. w sprawie organizacji systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz. U. MON 2008 r. nr 16, poz. 205).
2. Konstytucja Rzeczypospolitej Polskiej uchwalona dnia 2.04.1997 r., Dz. U. 1997 r. nr 78, poz. 483.
3. Rozporządzenie Rady Ministrów z dnia 30.04.2010 r. w sprawie planów ochrony infrastruktury krytycznej, Dz. U. 2010 r. nr 83, poz. 542.
4. Rozporządzenie Rady Ministrów z dnia 23.12.2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych, Dz.U. 2002 nr 239 poz. 2039 i 2004 r poz. 597.
5. Rozporządzenie Ministra Sprawiedliwości z dnia 24.06.2003 r. w sprawie sposobu technicznego przygotowania sieci służących do przekazywania informacji, do kontroli przekazów informacji oraz sposobów dokonywania, rejestracji, przechowywania, odtwarzania i niszczenia zapisów z kontrolowanych przekazów, Dz. U. 2003 r. nr 110, poz. 1052.
6. Rozporządzenie Rady Ministrów z dnia 28.03.2005 r. w sprawie Planu Informatyzacji Państwa na lata 2007-2010, Dz. U. 2007 r. nr 61, poz. 415.
7. Rozporządzenie Prezesa Rady Ministrów z dnia 25.08.2005 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego, Dz. U. 2005 r. nr 171, poz. 1433.
8. Rozporządzenie Rady Ministrów z dnia 11.10.2005 r. w sprawie minimalnych wymagań dla systemów informatycznych, Dz. U. 2005 r. nr 212, poz. 1766.

9. Rozporządzenie Prezesa Rady Ministrów z dnia 10.07.2008 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa, Dz. U. 2008 r. nr 128, poz. 821.
10. Rozporządzenie Rady Ministrów z dnia 30.04.2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, Dz. U. 2010 r. nr 83, poz. 541.
11. Rozporządzenie Prezesa Rady Ministrów, z dnia 11.04.2011 r. w sprawie organizacji i trybu działania Rządowego Centrum Bezpieczeństwa, Dz. U. 2015 r. poz. 508.
12. Rozporządzenie Rady Ministrów z dnia 20.01.2012 r. w sprawie wymagań technicznych i eksploatacyjnych dla interfejsów umożliwiających wykonanie zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego, Dz. U. 2012 r. poz. 200.
13. Rozporządzenie Rady Ministrów z dnia 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, Dz. U. 2012 r. poz. 526.
14. Rozporządzenie Prezesa Rady Ministrów z dnia 22.09.2014 r. w sprawie szczegółowego zakresu działania Ministra Spraw Wewnętrznych, Dz. U 2014 r. poz. 1265.
15. Rozporządzenie Prezesa Rady Ministrów z dnia 17.11.2015 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji, Dz. U. 2015 poz.1910.
16. Rozporządzenie Wykonawcze Komisji (UE) 2018/151 z dnia 30.01.2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia czy incydent ma istotny wpływ (Dz. U. L 26/48 PL UE 31.01.2018 r.).
17. Rozporządzenie Rady Ministrów z dnia 16.03.2018 r. w sprawie ustanowienia Pełnomocnika Rządu do spraw Cyberbezpieczeństwa, Dz. U. 2018 r. poz. 587.
18. Rozporządzenie Ministra Cyfryzacji z dnia 10.09.2018 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo, Dz. U. 2018 r. poz. 1780.

19. Rozporządzenie Rady Ministrów z dnia 11.09.2018 r. w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych, Dz. U. 2018 r. poz. 1806.
20. Rozporządzenie Ministra Cyfryzacji z dnia 20.09.2018 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych, które miało istotny wpływ na funkcjonowanie sieci lub usług, Dz. U. 2018 r. poz. 1831.
21. Rozporządzenie Ministra Cyfryzacji z dnia 20.09.2018 r. w sprawie kryteriów uznania naruszenia bezpieczeństwa lub integralności sieci lub usług telekomunikacyjnych za naruszenie o istotnym wpływie na funkcjonowanie sieci lub usług, Dz. U. 2018 r. poz. 1830.
22. Rozporządzenie Rady Ministrów z dnia 2.10.2018 r. w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa, Dz. U. 2018 r. poz. 1952.
23. Rozporządzenie Ministra Cyfryzacji z dnia 12.10.2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu, Dz. U. 2018 r. poz. 1999.
24. Rozporządzenie Rady Ministrów z dnia 16.10.2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, Dz. U. 2018 r. poz. 2080.
25. Rozporządzenie Rady Ministrów z dnia 31.10.2018 r. w sprawie progów uznania incydentu za poważny, Dz. U. 2018 r. poz. 2180.
26. Rozporządzenie Ministra Obrony Narodowej z dnia 08.02.2019 r. w sprawie limitów miejsc na kierunki studiów dla kandydatów na żołnierzy zawodowych w poszczególnych uczelniach wojskowych, Dz. U. 2019 r., poz. 287.
27. Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 8.08.2011 r. w sprawie obszarów wiedzy, dziedzin nauki i sztuki oraz dyscyplin naukowych i artystycznych, Dz. U. 2011 r. nr 179, poz. 1065, załącznik do rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 8.08.2011 r.
28. Ustawa o administracji rządowej z dnia 4.09.1997 r. Dz. U. 1997 nr 141 poz. 943.
29. Ustawa o działalności pożytku publicznego i wolontariacie z dnia 24.04.2003 r., Dz. U. 2003 r. nr 96, poz. 873 ze zm.
30. Ustawa o e-podpisie, bezpieczny podpis elektroniczny weryfikowany przy pomocy ważnego kwalifikowanego certyfikatu z dnia 18.09.2001 r., Dz. U. 2001 r. nr 130, poz. 1450 ze zm.
31. Ustawa o łączności z dnia 23.11.1990 r., Dz. U. 1995 r. nr 117, poz. 564 ze zm.

32. Ustawa o Policji z dnia 6.06.1990 r. Dz. U. 1990 nr 30 poz. 179.
33. Ustawa o stanie klęski żywiołowej z dnia 18.04.2002 r. Dz. U. 2002 nr 62 poz. 558.
34. Ustawa o stanie wojennym i kompetencje Naczelnego Wodza i jego podporządkowanie władzom konstytucyjnym RP z dnia 29.08.2002 r., Dz. U. 2018 r. poz. 1932 ze zm.
35. Ustawa o stanie wyjątkowym z dnia 21.06.2002 r. (Dz. U. 2017 r. poz. 1928 ze zm.).
36. Ustawa o zasadach prowadzenia polityki rozwoju z dnia 6.12.2006 r., Dz. U. 2017 r. poz. 1475 ze zm.
37. Ustawa o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw z dnia 22.12.2015 r., Dz. U. 2015 poz. 2281 ze zm.
38. Ustawa o zasadach finansowania nauki, Załącznik do uchwały nr 164/2011 Rady Ministrów z dnia 16.08.2011 r.
39. Ustawa Prawo telekomunikacyjne z dnia 16.07.2004 r., Dz. U. 2004 r. nr 171, poz. 1800 ze zm.
40. Ustawa Prawo telekomunikacyjne z dnia 21.07.2000 r., Dz. U. 2000 r. nr 73, poz. 852 ze zm.
41. Ustawa z dnia 10.01.2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw Dz. U. 2013 r. poz. 235, Dz. U. 2014 r. poz. 183, z 2015 r. poz. 1311, z 2016 r. poz. 1579, z 2018 r. poz. 696, 1544 ze zm.
42. Ustawa z dnia 10.06.2016 r. o działaniach antyterrorystycznych, Dz. U. 2016 r., poz. 904 ze zm.
43. Ustawa z dnia 12.09.2014 r. o ratyfikacji Konwencji Rady Europy o cyberprzestępczości, sporządzonej w Budapeszcie w dniu 23.11.2001 r., Dz. U. 2014 r., poz. 1514 ze zm.
44. Ustawa z dnia 13.04.2016 r. o systemach oceny zgodności i nadzoru rynku, Dz. U. 2017 r. poz. 1398 oraz z 2018 r. poz. 650 i 1338 ze zm.
45. Ustawa z dnia 14.07.1983 r. o narodowym zasobie archiwalnym i archiwach, Dz. U. 2018 r. poz. 217, 357, 398, 650 ze zm.
46. Ustawa z dnia 15.01.2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, Dz. U. 2016 poz. 147 ze zm.
47. Ustawa z dnia 16.02.2007 r. o ochronie konkurencji i konsumentów, Dz. U. 2007 nr 3 poz. 369 ze zm.

48. Ustawa z dnia 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2017 r. poz. 570 ze zm. Ustawa z dnia 18.04.2002 r. o stanie klęski żywiołowej, Dz. U. 2017 poz. 1897 ze zm.
49. Ustawa z dnia 18.07.2002 r. o świadczeniach usług drogą elektroniczną, Dz. U. 2017 r. poz. 1219 ze zm.
50. Ustawa z dnia 18.09.2001 r. o podpisie elektronicznym, Dz. U. 2013 r. poz. 262 ze zm.
51. Ustawa z dnia 20.12.1996 r. o gospodarce komunalnej, Dz. U. 2017 r. poz. 827 oraz z 2018 r. poz. 1496 ze zm.
52. Ustawa z dnia 21.06.2002 r. o stanie wyjątkowym, Dz. U. 2017 r. poz. 1928 ze zm.
53. Ustawa z dnia 21.11.1967 r. o powszechnym obowiązku obrony Rzeczypospolitej Polskie Dz. U. z 2017 r. poz. 1430 ze zm.
54. Ustawa z dnia 22.01.1999 r. o ochronie informacji niejawnych, Dz. U. 2005 r. nr 196, poz. 1631 ze zm.
55. Ustawa z dnia 22.12.2015 r. o zmianie ustawy o działach administracji rządowej oraz niektórych innych ustaw (Dz. U. 2015 r. poz. 2281 ze zm.).
56. Ustawa z dnia 23.04.1964 r. Kodeks postępowania cywilnego Dz. U. 1964 r. nr 43, poz. 296 ze zm.
57. Ustawa z dnia 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, Dz. U. 2002 r. nr 74, poz. 676 ze zm.
58. Ustawa z dnia 26.04.2007 r. o zarządzaniu kryzysowym, Dz. U. 2017 r. poz. 209 ze zm.
59. Ustawa z dnia 27.07.2001 r. o ochronie baz danych, Dz. U. 2001 r. nr 128, poz. 1402 ze zm.
60. Ustawa z dnia 27.08.2009 r. o finansach publicznych, Dz. U. 2017 r. poz. 2077 oraz z 2018 r. poz. 62, 1000 i 1366 ze zm. Ustawa z dnia 27.09.2009 o finansach publicznych, Dz. U. 2016 r. poz. 1870 ze zm.
61. Ustawa z dnia 28.07.2005 r. o partnerstwie publiczno-prywatnym, Dz. U. 2005 r. nr 169 poz. 1420 ze zm.
62. Ustawa z dnia 29.08.1997 r. o ochronie danych osobowych, Dz. U. 2016 r. poz. 922, z 2018 r. poz. 138, 723 ze zm.
63. Ustawa z dnia 29.08.1997 r. Ordynacja podatkowa, Dz. U. 2017 r. poz. 201, 648, 768, 935, 1428, 1537, 2169, 2491, z 2018 r. poz. 106, 138, 398, 650, 723 ze zm.

64. Ustawa z dnia 29.08.2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczy-pospolitej Polskiej, Dz. U. 2018 r. poz. 1932 ze zm.
65. Ustawa z dnia 4.02.1994 r. o prawie autorskim i prawach pokrewnych, Dz. U. 1994 r. nr 24, poz. 83 ze zm.
66. Ustawa z dnia 4.09.1997 r. o działach administracji rządowej, Dz. U. 2016 r. poz. 543 ze zm.
67. Ustawa z dnia 5.07.2002 r. o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym, Dz. U. 2002 r. nr 126, poz. 1068 ze zm.
68. Ustawa z dnia 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. 2018 r. poz. 1560 ze zm.
69. Ustawa z dnia 5.07.2018 r. o zmianie ustawy o partnerstwie publiczno-prywatnym oraz niektórych innych ustaw, Dz. U. 2018 r. poz. 1693 ze zm.
70. Ustawa z dnia 5.08.2010 r. o ochronie informacji niejawnych realizujących zadania publiczne (Dz. U. 2010 r. nr 182, poz. 1228 ze zm.).
71. Ustawa z dnia 5.09.2016 r. o usługach zaufania oraz identyfikacji elektronicznej, Dz. U. 2016 r. poz. 1579 oraz z 2018 r. poz. 650 ze zm.
72. Ustawa z dnia 6.06.1997 r. Kodeks Karny, Dz. U. 2016 r. poz. 1137 ze zm.
73. Ustawa z dnia 6.12.2006 r. o zasadach prowadzenia polityki rozwoju, Dz. U. 2006 r. nr 227, poz. 1658, ze zm.
74. Ustawa z dnia 6.12.2006 r. o zasadach prowadzenia polityki rozwój, Dz. U. 2009 r. nr 84 poz. 712 ze zm.
75. Ustawa z dnia 9.06.2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego, Dz. U. 2006 r. nr 104, poz. 709 ze zm.
76. Ustawa z dnia 16.07.2004 r. Prawo telekomunikacyjne, Dz. U. 2004 r. nr 171, poz. 1800 ze zm.
77. Ustawa z dnia 16.11.2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw, Dz. U. 2012 r. poz. 1445 ze zm.
78. Ustawa z dnia 5.08.2010 r. o ochronie informacji niejawnych, Dz. U. 2010 r. nr 182, poz. 1228 ze zm.
79. Ustawa z dnia 14.06.1960 r. Kodeks postępowania administracyjnego Dz. U. 1960 r. nr 30, poz. 168 Dz. U. 2018 r. poz. 209 ze zm.

Strategie, programy, ekspertyzy

1. Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, Warszawa 2013.
2. Długookresowa Strategia Rozwoju Kraju. Polska 2030. Trzecia fala nowoczesności, Ministerstwo Administracji i Cyfryzacji, Warszawa, 11.01.2013 r.
3. Doktryna Cyberbezpieczeństwa Rzeczypospolita Polskiej, BBN, Warszawa 2015.
4. Ekspertyza dotycząca rekomendowanego modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce, wykonana na zlecenie Ministerstwa Administracji i Cyfryzacji. Naukowa i Akademicka Sieć Komputerowa (NASK / CERT POLSKA), Warszawa 2015.
5. Koncepcja Obronna Rzeczpospolitej Polskiej, MON, Warszawa, 23.05.2017 r.
6. Koncepcja Przestrzennego Zagospodarowania Kraju, Projekt Dokumentu Rządowego przeznaczony do konsultacji, Warszawa, 25.01.2011 r.
7. Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, Ministerstwo Cyfryzacji, Warszawa 2017.
8. Plan Szerokopasmowy, MAiC, Warszawa, 24.09.2013 r.
9. Program Ochrony Infrastruktury Krytycznej, Rządowe Centrum Bezpieczeństwa, Warszawa 2013.
10. Plan działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP. Dokument przyjęty przez Zespół Zadaniowy ds. bezpieczeństwo cyberprzestrzeni Rzeczypospolitej Polskiej zatwierdzony przez Komitet Rady Ministrów ds. Cyfryzacji, Warszawa, 20.03.2015 r.
11. Plan działania UE na rzecz administracji elektronicznej na lata 2016-2020, Przyśpieszenie transformacji cyfrowej w administracji (COM2016-179) przedstawioną przez Komisję Europejską w dniu 19.04.2016 r.
12. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego, Warszawa, 25.06.2013.
13. Polityka w zakresie widma radiowego przyjęta przez Parlament Europejski i Radę na mocy art. 8a ust. 3 dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7.03.2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej

14. Program Nauczania do Informatyki, dla szkół ponadgimnazjalnych z 2019 r. z wydawnictw: WSIP, Operon, Migra.
15. Program operacyjny Polska Cyfrowa na lata 2014 – 2020, Ministerstwo Rozwoju, Departament Rozwoju Cyfrowego, Warszawa 2014.
16. Program przeciwdziałania i zwalczania przestępczości gospodarczej na lata 2015-2020, Prokuratura Generalna, Ministerstwo Finansów, Ministerstwo Spraw Wewnętrznych, Warszawa 22.06.2015 r.
17. Program Zintegrowanej Informatyzacji Państwa, MC, Warszawa, czerwiec 2016.
18. Ramy Polityki UE w zakresie cyberobrony, Rada Unii Europejskiej, nr 14413/18 Bruksela, 19.11.2018 r.
19. Program ochrony cyberprzestrzeni RP na lata 2009-2011. Założenia, Warszawa, marzec 2009.
20. Program Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011-2016, MSWiA, Warszawa 2010.
21. Strategia „Sprawne Państwo 2020" przyjęta uchwałą nr 17 Rady Ministrów z dnia 12.02.2013 r. M. P. 2013 r. poz. 136.
22. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, Warszawa, 2000.
23. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, Warszawa, 2003.
24. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, Warszawa, 2007.
25. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, Warszawa, 2009.
26. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, BBN, Warszawa, 2014.
27. Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy, COM (2010)
28. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2016-2020, MC, Warszawa 2016.
29. Strategia cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, MC, Warszawa 2017.
30. Strategia Informatyzacji Państwa - Plan Działań Ministra Cyfryzacji, MC, Warszawa 2016.

31. Strategia Jednolitego Rynku Cyfrowego, COM (2015) 192 final, Bruksela 2015.
32. Strategia na rzecz Odpowiedzialnego Rozwoju, Warszawa 2017.
33. Strategia obronności Rzeczypospolitej Polskiej. Strategia sektorowa do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2009.
34. Strategia Rozwoju Kraju 2020, Ministerstwo Rozwoju Regionalnego, dokument przyjęty uchwałą Rady Ministrów w dniu 25.09.2012 r.
35. Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022 stanowi załącznik do uchwały Nr 67 Rady Ministrów z 9.04.2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022", M.P. 2013 r. poz. 377.
36. Strategies for Incident Response and Cyber Crisis Cooperation, ENISA, UE 2017.
37. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020 r.
38. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2017-2022.
39. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej 2019-2024.
40. Założenia Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej, Zespół zadaniowy Ministerstwa Cyfryzacji, luty 2016 r. Warszawa

Normy

1. PN-I-13335-1:1999, Wytyczne do zarządzania bezpieczeństwem systemów informatycznych.
2. PKN-ISO Guide 73:2012, Zarządzanie ryzykiem, Terminologia.
3. PN-EN IEC 31010:2020-01, Zarządzanie ryzykiem, Techniki oceny ryzyka.
4. PN-EN ISO 9000:2006, System zarządzania jakością. Podstawy i terminologia.
5. PN-EN ISO 22301:2020-04, Bezpieczeństwo i odporność, Systemy zarządzania ciągłością działania.
6. PN-ISO/IEC 27001:2017-06, Technika informatyczna, Techniki bezpieczeństwa, Systemy zarządzania bezpieczeństwem informacji.
7. PN-N-18002:2011, Systemy zarządzania bezpieczeństwem i higieną pracy, Ogólne wytyczne do oceny ryzyka zawodowego.
8. PN-IEC 62198:2005 Zarządzanie ryzykiem przedsięwzięcia.

Strony internetowe

1. Bezpieczeństwo informacji, www.nflo.pl/slownik/bezpieczenstwo-informacji/ [dostęp: 31.07.2023].

2. Budowa definicji, www.pl.wikipedia.org/wiki/Definicja#Budowa_definicji. [dostęp: 21.11.2021].
3. Ciągłość działania, www.2business.pl/index.php?page=ciaglosc-dzialania---slowniczek-pojec [dostęp: 08.08.2023].
4. Cyberbezpieczeństwo dla początkujących, www.hackeru.pl/Cyberbezpiecze
5. nstwo-dla-poczatkujacych [dostęp 21.11.2021].
6. Cyberbezpieczeństwo główne i nowe zagrożenia,www.europarl.europa.eu
7. /news/pl/headlines/society/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia [dostęp: 07.11.2023].
8. Cybersecurity glossary, www.niccs.cisa.gov/about-niccs/cybersecurity-glossary, Adapted from: CNSSI 4009, NIST SP 800-53 Rev 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review. [dostęp: 19.11.2021].
9. Duńska strategia, www.wojsko-polskie.pl/aszwoj/u/8a/10/8a10c049-b55b-4559-b59a-dca6c4db61f8/dania.pdf [dostęp: 22.03.2021].
10. Encyklopedia zarządzania - cyberbezpieczeństwo, www.mfiles.pl/pl/index.php
11. /Cyberbezpiecze%C5%84stwo [dostęp: 19.11.2021].
12. ENISA Threat Landscape 2022/23, www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport [dostęp: 02.08.2024].
13. Francja przeciwdziałanie manipulacjom informacjami, LOI n° 2018-1202 du 22 décembre 2018 relative à la lutte contre la manipulation de l'information [dostęp: 23.01.2024].
14. Fundusze dla cyberbezpieczeństwahttps://www.gov.pl/web/baza-wiedzy/
15. wiecej-pieniedzy-na-fundusz-cyberbezpieczenstwa [dostęp: 20.06.2024].
16. Furmanek W., Piąta rewolucja przemysłowa. Eksplikacja pojęcia, „Edukacja-Technika-Informatyka” 2018, nr 2/24, s. 276, https://doi.org/10.15584/eti. [dostęp: 03.05.2023].
17. Gruzja konflikt, www.cybsecurity.org/pl/gruzja-rosja-konflikt-w-cyberprzestrzeni [dostęp: 28.04.2023].
18. ISAC, www.cyberpolicy.nask.pl/isac-centra-wymiany-analizy-informacji/ [dostęp: 03.11.2023].
19. Krajowy System Cyberbezpieczeństwa, www.parp.gov.pl/component/content/
20. article/85058:krajowy-system-cyberbezpieczenstwa-zmiany-funkcjonowaniu-i-ich-wplyw-na-rynek-ict [dostęp: 04.02.2024].

21. Logika, www.doktorat.xn--pook-11a.pl/SEP/15Z/Logika/logika_2.pdf [dostęp 21.11.2021].
22. Minisłownik BBN, www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/Minislo
23. wnik-bbn-propozy/6035,minislownik-bbn-propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html [dostęp 21.11.2021].
24. National Council of ISACs, www.nationalisacs.org/ [dostęp: 03.02.2024].
25. Nowa siedziba dla speców od cyberprzestępczości, www.kielce.wyborcza.
26. pl/kielce/7,47262,29464437,wybuduja-nowa-siedzibe-dla-specow-od-cyberprzestepczosci-kosz.html [dostęp 02.02.2024].
27. Operator Strategiczny, www.bank.pl/watpliwosci-zwiazane-z-powolaniem-operatora-strategicznej-sieci-bezpieczenstwa/ [dostęp: 23.05.2024].
28. Piramida ludności, www.stat.gov.pl/obszary-tematyczne/ludnosc/ludnosc
29. /ludnosc-piramida/ [dostęp: 02.05.2025]
30. Polityka bezpieczeństwo cyberprzestrzeni, www.biznesalert.pl/hakerzy-colonial-pipeline-cyberatak-polityka-bezpieczenstwo-cyberprzestrzen/ [dostęp: 21.02.2023].
31. Poradnik NASK, www.cyberpolicy.nask.pl/wp-content/uploads/2019/04
32. /Poradnik-NASK-na-temat-tworzenia-ISAC.pdf [dostęp: 28.05.2024].
33. Projekt ustawy o KSB, www.gov.pl/web/premier/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa [dostęp: 04.02.2024].
34. Projekty aktów prawnych, www.mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpie
35. czenstwa-oraz-ustawy-prawo-zamowien-publicznych.html [dostęp: 05.04.2024].
36. Raporty Cyber, www.portal.pti.org.pl/wp-content/uploads/2024/03/8_cyber-raporty.pdf [dostęp: 09.05.2024].
37. Raporty o stanie bezpieczeństwa, www.csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [dostęp: 01.02.2024].
38. Russia cyber war, www.theguardian.com/world/2007/may/17/topstories3.
39. russia [22.02.2023]. Ryzyko w ochronie danych osobowych, www.uksw.edu.pl/images/artykuly/ uniwersytet/RODO/Ryzyko-w-ochronie-danych-osobowych-AK-29.01.2018.pdf [dostęp: 01.08.2024].
40. Securitologia, www.civitas.edu.pl/wp-content/uploads/2015/03/Securitologia-1-21-2015_007-017.pdf s-7. [dostęp: 21.11.2021].
41. Strategia Bezpieczeństwa Narodowego,www.bbn.gov.pl/ftp/dokumenty/Stra
42. tegia_Bezpieczenstwa_Narodowego_RP_2020.pdf. [dostęp: 28.04.2023].

43. Strategia Rozwoju Systemu Bezpieczeństwa Narodowego, www.bbn.gov.pl/ftp/dok/01/strategia_rozwoju_systemu_bezpieczenstwa_narodowego_rp_2022.pdf. [dostęp: 28.04.2023].
44. System Bezpieczeństwa Narodowwego, ww.zpe.gov.pl/a/system-bezpieczenstwa-narodowego---ogolna-charakterystyka/D10Rhn2ZnC [dostęp: 06.08.2024].
45. Vademecum bezpieczeństwa, www.depot.ceon.pl/Vademecum_bezpiecze
46. nstwa.pdf [dostęp 21.11.2021].
47. Współpraca krajowa, www.gov.pl/web/klimat/wspolpraca-krajowa [dostęp 21.11.2021].
48. Wyciek danych, www.wiadomosci.onet.pl/kraj/gigantyczny-wyciek-danych-z-wojska-ponad-17-mln-pozycji-w-internecie/1mknjtf [dostęp: 28.04.2023].
49. Zapewnienie ciągłości działania, www.gov.pl/web/baza-wiedzy/zapewnienie-ciaglosci-dzialania [dostęp: 01.02.2021].

ZAŁĄCZNIK NR 1 - PISMO PRZEWODNIE DO WYWIADÓW

Wojskowa Akademia Techniczna

Szkoła Doktorska

Warszawa, dn. 28.08.2023 r.

INFORMACJA

Pan mgr inż. Marcin Dąbrowski jest doktorantem 3 roku kształcenia w Szkole Doktorskiej Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w dyscyplinie naukowej Nauki o Bezpieczeństwie. W ramach przygotowywania rozprawy doktorskiej prowadzi badania na temat *„Cyberprzestrzeń i cyberbezpieczeństwo jako determinanty bezpieczeństwa narodowego”*. Koncepcja jego rozprawy obejmuje zarówno aspekty teoretyczne jak i praktyczne wynikające z przyjętego celu i metodologii prowadzenia projektu badawczego. Podstawą do analizy i weryfikacji założonych hipotez badawczych są dane źródłowe pozyskane w trakcie prowadzonych badań.

W związku z powyższym uprzejmie proszę o wsparcie i umożliwienie przeprowadzenia badań przez Pana mgr. Marcina Dąbrowskiego polegających na wywiadzie eksperckim.

Mam nadzieję, że wyniki przeprowadzonych badań i ich szczegółowa analiza skonkretyzowana w przygotowywanej rozprawie doktorskiej będą cenną lekturą dla decydentów z różnych sektorów bezpieczeństwa państwa.

Wykonała: - Elżbieta Rąpała ☎ tel. 261 83 93 32, e-mail: elzbieta.rapala@wat.edu.pl

ZAŁĄCZNIK NR 2 - WZÓR KWESTIONARIUSZA WYWIADU

Warszawa, dnia 16.08.2023 r.

Marcin Dąbrowski
Wojskowa Akademia Techniczna
Szkoła Doktorska

Pan ……..
……..
……..
……..

Dotyczy: *kwestionariusz wywiadu eksperckiego.*

Szanowni Państwo

Przedstawiony zestaw pytań jest jednym z narzędzi badań prowadzonych w ramach przygotowywania w Szkole Doktorskiej, Wojskowej Akademii Technicznej w dyscyplinie nauk o bezpieczeństwie pracy doktorskiej pod tytułem *„Cyberprzestrzeń i cyberbezpieczeństwo jako determinanty bezpieczeństwa narodowego RP”*.

Prowadzone przeze moją osobę wywiady mają charakter dobrowolny, a uzyskane informacje posłużą mi wyłącznie do celów badawczych. Wywiady są prowadzone w gronie wybranych specjalistów w dziedzinowych sektorach bezpieczeństwa. Jeśli Pan/Pani życzy sobie pozostać anonimowym w niniejszym badaniu, to wywiad zostanie przeprowadzony
w taki sposób, aby Państwa dane nie zostały ujawnione.

Celem wywiadów jest zgromadzenie opinii ekspertów dotyczących aktualnego stanu bezpieczeństwa, zagrożeń i wyzwań przed jakim stoi Rzecz Pospolita Polska oraz rozwiązań stosowanych w zakresie cyberbezpieczeństwa. Zebrane opinie będą stanowiły istotną część realizacji celu pracy doktorskiej, którym jest opracowanie koncepcji poprawy bezpieczeństwa państwa poprzez identyfikację luk, wad, słabości w obecnym

Systemie Bezpieczeństwa Narodowego z uwzględnieniem informacyjnej ciągłości działania.

Zwracam się z uprzejmą prośbą do Państwa o udzielenie szczerych i wyczerpujących odpowiedzi na zawarte w kwestionariuszu pytania, które pozwolą mi w sposób rzetelny przygotować rozprawę doktorską. Kwestionariusz można wypełnić w dwóch formach:

- w formacie MS word.doc, wzór kwestionariusza znajduje się na załączonej płycie CD oraz przesłanie go na adres mailowy marcin.dabrowski@wat.edu.pl,
- pisemnie jako załącznik do pisma, wypełniony kwestionariusz proszę wysłać pocztą zwrotną na adres uczelni Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego, gen. Sylwestra Kaliskiego 2. 00 -908 Warszawa 46, z dopiskiem: „Kwestionariusz wywiadu, Szkoła Doktorska - Marcin Dąbrowski"

W przypadku jakichkolwiek pytań zapraszam do kontaktu pod numerem telefonu 601-645-102 Marcin Dąbrowski.

Z góry dziękuję za poświęcony czas.

Serdecznie dziękuję za współpracę,

z wyrazami szacunku

Marcin DĄBROWSKI

Załączniki 1 szt.

Załącznik nr. 1 – kwestionariusz wywiadu

EKSPERT - …….

1. Jakie Pana/Pani zdaniem są główne kierunki rozwoju zagrożeń w cyberprzestrzeni mających istotny wpływ na informacyjną ciągłość działania w sektorze infrastruktury krytycznej?
2. Jakie według Pana/Pani występują luki, wady, słabości w dziedzinie cyberbezpieczeństwa w sektorze infrastruktury krytycznej?
3. Jakie działania Pana/Pani zdaniem należy podjąć, aby wzmocnić System Bezpieczeństwa Narodowego oraz zasoby informacyjne w sektorze infrastruktury krytycznej?
4. Czy uważa Pan/Pani, że w obecnych czasach cyberprzestrzeń i cyberbezpieczeństwo są głównymi determinantami systemu bezpieczeństwa państwa?
5. Jaką w Pana/Pani ocenie zajmuje pozycję Polska na tle europejskich krajów pod kątem rozwinięcia systemu cyberbezpieczeństwa? (w skali od 1 do 5)
6. Czy są jakieś rozwiązania w systemie cyberbezpieczeństwa z innych państw, o których Pan/Pani wie i które według Pana/Pani znalazłyby zastosowanie w sektorze infrastruktury krytycznej?
7. Jakich rozwiązań Pana/Pani zdaniem zabraknie w nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa?
8. Czy Pana/Pani zdaniem na przestrzeni ostatniej dekady poziom wiedzy społeczeństwa w Polsce o „cyberzagrożeniach" uległ poprawie i jakiego rodzaju, według Pana/Pani krytyczne zdarzenia przyczyniają się do kształtowania tej świadomości?

ZAŁĄCZNIK NR 3 - WYWIAD MINISTERSTWO ŚRODOWISKA

1. **Jakie Pana/Pani zdaniem są główne kierunki rozwoju zagrożeń w cyberprzestrzeni mających istotny wpływ na informacyjną ciągłość działania w sektorze środowiska naturalnego?**

Zagrożenia cyberprzestrzeni, których materializacja może mieć potencjalnie negatywny wpływ dla środowiska naturalnego, mogą dotyczyć przykładowo podatności w systemach zdalnego sterowania wykorzystywanych w przemyśle, a których kompromitacja może ewaluować w postaci zatrucia środowiska naturalnego (np. wyciek substancji toksycznych). Inne zagrożenia istniejące w cyberprzestrzeni to takie, które opierają się o fałszywe informacje i wprowadzają obywateli w błąd. Dotyczy to podszywania się pod instytucje zaufania publicznego, które dostarczają obywatelom informacji nt. chociażby jakości powietrza (np.: powietrze.gios.gov.pl/pjp/current). Popularyzacja fałszywych informacji niesie za sobą szereg zagrożeń oraz w sposób negatywny rzutuje na zaufanie publiczne oraz może prowadzić do chaosu informacyjnego lub nawet w skrajnych przypadkach paniki.

2. **Jakie według Pana/Pani występują luki, wady, słabości w dziedzinie cyberbezpieczeństwa w sektorze środowiska naturalnego?**

„Sektor środowiska naturalnego" jest niewątpliwie sektorem, który aktywnie przechodzi cyfrową rewolucję, dostępność informacji, którą organizacje państwowe starają się zapewnić wszystkim obywatelom za pośrednictwem systemów informacyjnych, rozwija się bardzo szybko i niewątpliwie zmierza w dobrym kierunku. Należy jednak zwrócić uwagę, że aktualnie wszystkie publiczne rozwiązania tego typu projektowane oraz wdrażane są zgodnie z zasadą *Security by Design,* a co za tym idzie kładziony jest specjalny nacisk na zapewnienie możliwie najwyższego poziomu cyberbezpieczeństwa.

3. **Jakie działania Pana/Pani zdaniem należy podjąć, aby wzmocnić System Bezpieczeństwa Narodowego oraz zasoby informacyjne w sektorze środowiska naturalnego?**

Podstawowymi działaniami, które w sposób jednoznaczny przełożą się na podniesienie bezpieczeństwa narodowego są wszelkie działania przekładające się na podnoszenie świadomości zagrożeń, zarówno wśród pracowników administracji (każdego szczebla) jak i obywateli. Podnoszenie świadomości powinno odbywać się z

wykorzystaniem takich narzędzi jak popularyzacja szkoleń z zakresu bezpieczeństwa informacji oraz kampanii społecznych wskazujących rzetelne źródła informacji.

4. **Czy uważa Pan/Pani, że w obecnych czasach cyberprzestrzeń i cyberbezpieczeństwo są głównymi determinantami systemu bezpieczeństwa państwa?**

Na przestrzeni ostatnich kilku lat obserwujemy dynamiczny rozwój technologii, zarówno służącej do zabezpieczania informacji przechowywanych w cyberprzestrzeni, jak i tych ukierunkowanych na ich pozyskanie. Niewątpliwie na bezpieczeństwo państwa składa się wiele różnych powiązanych czynników, w tym poziom cyberbezpieczeństwa.

5. **Jaką w Pana/Pani ocenie zajmuje pozycję Polska na tle europejskich krajów pod kątem rozwinięcia systemu cyberbezpieczeństwa? (w skali od 1 do 5)**

5

6. **Czy są jakieś rozwiązania w systemie cyberbezpieczeństwa z innych państw, o których Pan/Pani wie i które według Pana/Pani znalazłyby zastosowanie w sektorze środowiska naturalnego?**

Państwo Polskie aktywnie uczestniczy w projektach międzynarodowych, na forum unijnym oraz bierze aktywny udział w wydarzeniach z tego zakresu. Owocem tej współpracy jest wysoki poziom rozwinięcia cyberbezpieczeństwa, także w sektorze środowiska naturalnego. Polska jest jednym z krajów wyznaczającym trendy w tej materii.

7. **Jakich rozwiązań Pana/Pani zdaniem zabraknie w nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa?**

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, została wycofana i nie zostanie przyjęta w powszechnie znanej formie. Należy jednak pamiętać, że aby cały system był „silny" musi być on zaprojektowany w sposób spójny. Ustawa o Krajowym Systemie Cyberbezpieczeństwa jest implementacją Unijnej Dyrektywy NIS[1], tym samym zapewnia spójność zarówno na poziomie krajowym jak i unijnym.

[1] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Directive concerning measures for a high common level of security of network and information systems across the Union)

8. **Czy Pana/Pani zdaniem na przestrzeni ostatniej dekady poziom wiedzy społeczeństwa w Polsce o „cyberzagrożeniach" uległ poprawie i jakiego rodzaju, według Pana/Pani krytyczne zdarzenia przyczyniają się do kształtowania tej świadomości?**

Uważam, że na przestrzeni ostatniej dekady poziom wiedzy społeczeństwa w Polsce o „cyberzagrożeniach" uległ znacznej poprawie, nie tylko na skutek „krytycznych zdarzeń", ale w głównej mierze dzięki staraniom i wysiłkom podejmowanym przez instytucja publiczne. Należy na pewno zwrócić uwagę na kampanie społeczne realizowane chociażby przez CERT POLSKA. Niewątpliwie na podniesienie poziomu świadomości przełożyła się także popularyzacja tego tematu oraz zaangażowanie podmiotów prywatnych, które również dostrzegają potrzebę podnoszenia świadomości dotyczącej cyberbezpieczeństwa.

ZAŁĄCZNIK NR 4 - WYWIAD MINISTERSTWO SPRAW ZAGRANICZNYCH

EKSPERT - sektor dyplomatyczny

1. Jakie Pana/Pani zdaniem są główne kierunki rozwoju zagrożeń w cyberprzestrzeni mających istotny wpływ na informacyjną ciągłość działania w sektorze dyplomatycznym?

— PUCIA DYPLOMATÓW
I UJAWNIANIE INFORMACJI
W PRZESTRZENI INTERNETOWEJ

2. Jakie według Pana/Pani występują luki, wady, słabości w dziedzinie cyberbezpieczeństwa w sektorze dyplomatycznym?

— BRAK KOORDYNACJI
— BRAK WIEDZY DYPLOMATÓW.

3. Jakie działania Pana/Pani zdaniem należy podjąć, aby wzmocnić System Bezpieczeństwa Narodowego oraz zasoby informacyjne w sektorze dyplomatycznym?

— ZBUDOWANIE CIĄGU
SPRAWNYCH I INTERDYSCYPLINARNYCH
ZESPOŁÓW ANALITYCZNYCH WSPIERAJĄCYCH
CYCH INSTYTUCJI PAŃSTWOWE

4. Czy uważa Pan/Pani, że w obecnych czasach cyberprzestrzeń i cyberbezpieczeństwo są głównymi determinantami systemu bezpieczeństwa państwa?

TAK

Marcin Dąbrowski
tel: 601-645-102

5. Jaką w Pana/Pani ocenie zajmuję pozycje Polska na tle europejskich krajów pod kątem rozwinięcia systemu cyberbezpieczeństwa? (w skali od 1 do 5)

4

6. Czy są jakieś rozwiązania w systemie cyberbezpieczeństwa z innych państw, o których Pan/Pani wie i które według Pana/Pani znalazłyby zastosowanie w sektorze dyplomatycznym?

brak

7. Jakich rozwiązań Pana/Pani zdaniem zabraknie w nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa?

– koordynacji na szczeblu politycznym.

8. Czy Pana/Pani zdaniem na przestrzeni ostatniej dekady poziom wiedzy społeczeństwa w Polsce o „cyberzagrożeniach" uległ poprawie i jakiego rodzaju, według Pana/Pani krytyczne zdarzenia przyczyniają się do kształtowania tej świadomości?

– WOJNA NA UKRAINIE, nie bardzo pomogła w poprawie tej wiedzy

Marcin Dąbrowski
tel: 601-645-102

ZAŁĄCZNIK NR 5 - WYWIAD SŁUŻBA KONTRWYWIADU WOJSKOWEGO

SKW

Egz. nr 1

SŁUŻBA KONTRWYWIADU WOJSKOWEGO
BIURO I

POWSTANIE STYCZNIOWE 1863×2023

Warszawa, dnia 08 września 2023 r.

RPW/6129/2023 N
Data:2023-09-18

Pan Marcin DĄBROWSKI
WOJSKOWA AKADEMIA TECHNICZNA
Szkoła Doktorska
ul. gen. Sylwestra Kaliskiego 2B
00-908 Warszawa

Dotyczy: odpowiedzi na pismo z dnia 28.08.2023 r. ws. przeprowadzenia badań naukowych polegających na wywiadzie eksperckim.

Informuję Pana, że zakres tematyczny pytań zawartych w dostarczonym kwestionariuszu wywiadu eksperckiego został poddany przez Biuro I SKW szczegółowej i wnikliwej analizie. Powyższe zostało dokonane mając na względzie zarówno bezpieczeństwo Służby jak i dobro polskiej nauki.

Wskazać jednak należy, iż treść pytań dotyka informacji wrażliwych mogących mieć bezpośrednio lub pośrednio negatywny skutek dla bezpieczeństwa ustawowo wykonywanych obowiązków SKW.

W związku z powyższym Biuro I SKW nie rekomenduje przeprowadzenia przedmiotowego badania w obecnej postaci.

DYREKTOR
Biura I
Służby Kontrwywiadu Wojskowego

Załączniki: 1

Zał. nr 1 – koperta z płytą DVD+R - tylko adresat.

Wykonano w 2 egz.

Egz. nr 1 - adresat
Egz. nr 2 - a/a
Wykonawca: 823

str.1/1

ZAŁĄCZNIK NR 6 - WYWIAD DOWÓDZTWO KOMPONENTU WOJSK OBRONY CYBERPRZESTRZENI

Egz. nr 1.

DOWÓDZTWO KOMPONENTU
WOJSK OBRONY CYBERPRZESTRZENI

25 LAT POLSKI W NATO

Warszawa, 23 stycznia 2024 r.

DOWÓDZTWO KOMPONENTU
WOJSK OBRONY CYBERPRZESTRZENI
KANCELARIA TAJNA NR 2
Nr 1134/24
2024 -01- 23
III 00-909 Warszawa III

pan Marcin Dąbrowski

Wojskowa Akademia Techniczna
Szkoła Doktorska
ul. gen. Sylwestra Kaliskiego 2
00-908 Warszawa 46

dotyczy: kwestionariusza wywiadu eksperckiego

Szanowny Panie,

odpowiadając na Pana pismo dotyczące udzielenia odpowiedzi na zawarte w kwestionariuszu pytania informuję, że zgodnie z decyzją nr 78/MON z dnia 15 lutego 2008 r. w sprawie prowadzenia badań społecznych w resorcie obrony narodowej warunkiem prowadzenia tych badań jest upoważnienie wydane przez Dyrektora CO MON. Wyjątek od przeprowadzenia badań na podstawie upoważnienia wynika z pkt 8 ppkt 2 decyzji nr 78/MON z dnia 15 lutego 2008 r. w sprawie prowadzenia badań społecznych w resorcie obrony narodowej (Dz. Urz. MON z 2008 r. poz. 26). Nie wymagają upoważnień jednorazowych badania wykonywane za zgodą kierownika komórki organizacyjnej Ministerstwa Obrony Narodowej oraz kierownika (dyrektora, szefa, dowódcy, komendanta) jednostki organizacyjnej podległej Ministrowi Obrony Narodowej lub przez niego nadzorowanej, w podporządkowanych mu komórkach i jednostkach organizacyjnych - na wniosek komendantów szkół wojskowych lub wojskowych jednostek badawczo-rozwojowych.
Podsumowując, nie zostały spełnione warunki formalne umożliwiające prowadzenie przez Pana badań w Dowództwie Komponentu Wojsk Obrony Cyberprzestrzeni polegających na wywiadzie eksperckim.

Z wyrazami szacunku

ppłk Przemysław LIPCZYŃSKI
RZECZNIK PRASOWY

Wykonano w 1 egz.
Egz. nr 1 – pan Marcin Dąbrowski
ppłk Przemysław LIPCZYŃSKI
tel.: 571-221-212
e-mail: rzecznik.woc@mon.gov.pl

tel.: 261-865-705, 262-762-501
sekretariat.dkwoc@mon.gov.pl
www.wojsko-polskie.pl/woc

ul. gen. T. Buka 1
05-119 Legionowo

ZAŁĄCZNIK NR 7 - KWESTIONARIUSZ WYWIADU KOŃCOWEGO

Szanowni Państwo informuję, że zgodnie z wszelkimi kanonami oraz ogólnie przyjętymi praktykami dane osobowe każdego z respondentów zostaną zanonimizowane a udzielone przez nich odpowiedzi będą autoryzowane przed umieszczeniem ich w dysertacji. Przedstawiony kwestionariusz wywiadu eksperckiego prezentuje rozwiązania, które mają na celu eliminację zdiagnozowanych podatności systemowych w ujęciu cyberbezpieczeństwa poziomu krajowego. Poniższe problemy zostały przedstawione w kwestionariuszu jedynie lapidarnie tak, aby wprowadzić respondenta w tematykę i uzyskać ocenę w związku z czym należy je traktować jako część szerszego kontekstu, który został przedstawiony w dysertacji.

Przyjęto następującą metodologię przeprowadzania wywiadów. Do każdego zdiagnozowanego problemu (łącznie 10) przedstawiono wprowadzenie mające na celu zapoznać respondenta z problematyką oraz przedstawiono działania naprawcze, które pozwolą na eliminację problemu. Dodatkowo w tabeli przedstawiono zbiorcze wskaźniki ilościowe, które pozwalają na oszacowanie sił i środków niezbędnych do realizacji celu. Autor dodatkowo przedstawi podczas wywiadu wszelkie aspekty związane z działaniami naprawczymi oraz w razie potrzeby szerzej opisze problematykę. Zadaniem respondentów jest ocena prezentowanych rozwiązań na podstawie 5 stopniowej skali zgodnie z następującymi wartościami:

1 - proponowane rozwiązanie oceniam w stopniu niedostatecznym (1)
2 - proponowane rozwiązanie oceniam w stopniu miernym (2)
3 - proponowane rozwiązanie oceniam w stopniu dostatecznym (3)
4 - proponowane rozwiązanie oceniam w stopniu dobrym (4)
5 - proponowane rozwiązanie oceniam w stopniu bardzo dobrym (5)

W przypadku oceny 3 lub poniżej dla wybranego problemu proszę o uzasadnienie własnej oceny. Zebranie przedmiotowych ocen cząstkowych pozwoli na całościową ocenę zastosowanych rozwiązań w dysertacji w sposób jakościowy co przełoży się na dalsze analizy i ewentualne działania korygujące.

Należy podkreślić, że pojedyncze rozwiązania nie będą tak efektywne jak w przypadku wdrożenia całej koncepcji poprawy bezpieczeństwa, ponieważ są one ściśle skorelowane i tylko holistyczne podejście pozwoli uzyskać efekt synergii.

Ekspertyza nr …

Problem 1 - Tworzenie krajowych zdolności technologicznych. Eksploatacja sprzętu teleinformatycznego od producentów uznanych za „dostawców wysokiego ryzyka (DWR)". Jest to potencjalny problem, ponieważ instytucja DWR zostanie dopiero wprowadzona. Niemniej jednak, gdyby okazało się, że potencjalny dostawca został w tej procedurze uznany, to problematyczne będzie zdiagnozowanie jakie systemy (technologie) były narażone na nieuprawniony dostęp do zasobów informacyjnych oraz od jak dawna.

Rozwiązanie problemu. Kluczowym działaniem wobec potencjalnego zagrożenia będzie zinwentaryzowanie wszystkich systemów eksploatowanych w infrastrukturze krytycznej oraz pozostałych gałęziach gospodarki i obrony. Jednocześnie należy dążyć do tworzenia własnej myśli technologicznej i sukcesywnego zastępowania technologii „obcej" własnymi „sprawdzonymi" rozwiązaniami. Wymaga to sporych nakładów natomiast biorąc pod uwagę krajowy potencjał akademicki oraz krajowe zdolności przemysłowe jest to realne do implementacji. Jako siły i środki niezbędne do realizacji rozwiązania, przyjęto:

Tab. Z - 1. Zestawienie sił i środków niezbędnych do rozwiązania problemu nr. 1

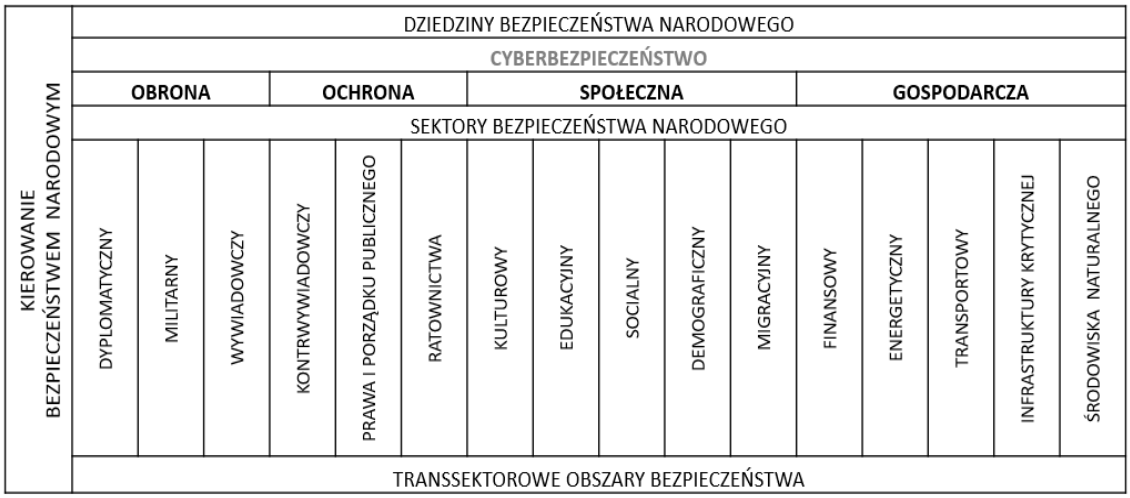
Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagany	2 - 5 dokumenty	nie są wymagane	100 tyś - 500 tyś / mc

<u>Ocena działań naprawczych przez respondenta – Załącznik nr 8</u>

Problem 2 - Wzmocnienie roli cyberbezpieczeństwa na poziomie strategii. Analiza strategii poziomu krajowego wyeksponowała problematykę braku powiązań między dokumentami w ujęciu cyberbezpieczeństwa oraz stwierdzono fakt, że dokumenty niższego szczebla niwelują starania wyższej rangi dokumentu. Na uwagę również zasługuję fakt, że obecnie cyberbezpieczeństwo traktowane jest jako transsektorowy obszar bezpieczeństwa a biorąc pod uwagę, że współcześnie żyjemy w dobie rewolucji przemysłowej 5.0, której determinantami są Sztuczna Inteligencja, cyfryzacja, technologie kwantowe oraz digitalizacja wszystkich gałęzi gospodarki należy ustanowić rangę cyberbezpieczeństwa na poziomie ponaddziedzinowym.

Rys. Z-1. Struktura dziedzin bezpieczeństwa sektorów bezpieczeństwa państwa.
Źródło: opracowanie własne na postawie strategii SR SNB 2013.

Rozwiązanie problemu. Ekspozycja roli cyberbezpieczeństwa we współczesnym świecie na odpowiednim poziomie przyniesie niewymierne pozytywne skutki. Przyczyni się do zwiększenia świadomości społecznej na zagrożenia, zwiększenia poziomu finansowania, poprawi prestiż niektórych grup zawodowych oraz ułatwi tworzenie solidniejszych regulacji prawnych. Należy dążyć do powiązywania dokumentów strategicznych z rolą cyberbezpieczeństwa na odpowiednim poziomie, ponieważ współcześnie jest to obszar, który oddziałuje na wszystkie dziedziny bezpieczeństwa narodowego. W związku z powyższą argumentacją schemat Systemu Bezpieczeństwa Narodowego powinien przybrać następującą formę:



Rys. Z-2. Zmodyfikowana struktura dziedzin bezpieczeństwa i sektorów bezpieczeństwa państwa.
Źródło: opracowanie własne na postawie strategii SR SNB 2013.

Należy zaznaczyć, że zarówno współcześnie jak i w przyszłych rewolucjach przemysłowych cyberbezpieczeństwo będzie determinantem wszystkich technologii, wobec czego zasadne jest zaktualizowanie kluczowych dokumentów strategicznych tak

aby utrzymać w nich jednolity wysoki poziom cyberbezpieczeństwa. Siły i środki wymagane do realizacji celu:

Tab. Z-2. Zestawienie sił i środków niezbędnych do rozwiązania problemu nr. 2.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
2	nie jest wymagana	nie jest wymagany	5 - 10 dokumentów	nie są wymagane	nie są wymagane

Ocena działań naprawczych przez respondenta - Załącznik nr 8

Problem 3 - Brak regulacji prawnych dotyczących finansowania działalności ISAC. Powstające w całym kraju Centra Wymiany i Analizy Danych nie są nowością. Są tworzone w większości państw europejskich oraz Stanach Zjednoczonych Ameryki i są dotowane poprzez wolontariat i darowizny. Znając potencjał oraz sposoby działania przeciwników (głównie kierunku wschodniego) zasadnym jest, aby w jakiś sposób kontrolować tak istotne podmioty w ujęciu finansowania.

Rozwiązanie problemu. Istnieje gotowe i sprawdzone rozwiązanie jakie zostało zaimplementowane w Stanach Zjednoczonych Ameryki. Otóż wyłoniono tam jeden z ISAC jako wiodący w pełni dotowany z publicznych pieniędzy, który pełni rolę koordynująco-nadzorczą nad pozostałymi centrami. Nakłady niezbędne do realizacji tego zadania są następujące:

Tab. Z-3. Zestawienie sił i środków niezbędnych do rozwiązania problemu nr. 3.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
3	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	100 tyś - 500 tyś / mc

Ocena działań naprawczych przez respondenta - Załącznik nr 8

Problem 4 - Brak ustawowego kształcenia użytkowników cyberprzestrzeni. Zidentyfikowane sposoby realizacji zagrożeń w głównej mierze wykorzystują błąd ludzki. Wszelkie sposoby, socjotechniki ukierunkowane są na ludzkie słabości oraz brak odpowiedniej wiedzy. Dlatego w celu minimalizacji zagrożeń kluczowym jest podniesienie świadomości całego społeczeństwa. Miejscem, w którym się uczy ludzi jest oczywiście szkoła natomiast trzeba mieć jednak świadomość, że część społeczeństwa dawno temu zakończyła edukację w związku z czym zachodzi konieczność sięgnięcia po inne metody. Miejscem, w którym ludzie również się uczą jest ich miejsce pracy. Każdy pracownik przed objęciem stanowiska pracy musi przejść 8 godzinne szkolenie BHP. Jest to warunek konieczny, przy czym raz na 4 lata zachodzi potrzeba ponownego podejścia

do jednodniowego kursu i zaliczenia egzaminu z tej tematyki. Podobnie powinno być z szkoleniem z zakresu cyberbezpieczeństwa.

Rozwiązanie problemu - Pomysłem, który może wyjść naprzeciw zaistniałej sytuacji w cyberbezpieczeństwie jest obowiązkowe szkolenie z podstaw higieny cyfrowej w miejscu pracy. Proponowana jest realizacja programu, który wymuszałby na pracownikach zapoznanie z podstawami higieny cyfrowej wraz z ekspozycją zagrożeń. Szkolenie byłoby bliźniaczą formą szkolenia tak jak to ma miejsce w przypadku BHP. Przewiduje się następujące nakłady niezbędne do realizacji zakładanego celu:

Tab. Z-4. Zestawienie sił i środków niezbędnych do rozwiązania problemu nr 4.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
4	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	nie są wymagane

Ocena działań naprawczych przez respondenta - Załącznik nr 8

Problem 5 - Narodowy długoterminowy program szkolnictwa ustawowego. Obecnie, zachodzi konieczność ustanowienia obowiązkowego szkolenia z cyberbezpieczeństwa dla najmłodszych użytkowników cyberprzestrzeni. Szkolenie uczniów w wieku wczesnoszkolnym jest jak najbardziej wskazane, ponieważ należy mieć świadomość, że jest to wiek, w którym dzieci zaczynają eksplorację Internetu co w przypadku braku nadzoru stanowi zagrożenie. Problem jest o tyle poważny, że dzieci pozostawione samym sobie z technologią cyfrową czerpią wiedzę i inspiracje z sieci. Nie jest to złą praktyką natomiast treści umieszczane w Internecie pozostawiają wiele do życzenia. Obecnie problem nieumiejętnego korzystania z sieci jest bardzo mocno poruszany medialnie, gdzie zarówno nielegalne i obraźliwe treści oraz tzw. hejt w skrajnych przypadkach może doprowadzić dziecko do depresji a w konsekwencji nawet samobójstwa.

Rozwiązanie problemu. Zgodnie z przysłowiem „Czego Jaś się nie nauczy tego Jan nie będzie umiał", szkolenie najmłodszych użytkowników cyberprzestrzeni będzie miało pozytywne skutki zarówno w ujęciu zdrowotnym, bezpieczeństwa jak i perspektyw dalszego rozwoju w kierunku cyberbezpieczeństwa. W związku z czym szkoła jest podstawowym miejscem, gdzie należy młodzież uczyć z zakresu bezpiecznego posługiwania się technologią cyfrową. W odróżnieniu od zaproponowanego szkolenia dla dorosłych dzieci powinny być ukierunkowane w sposób ciągły a przedmiotem jaki powinien być wprowadzony jest przykładowo higiena cyfrowa. Przedmiot ten powinien być wprowadzeniem do zajęć informatycznych oraz ich uzupełnieniem. Nacisk kładziony powinien być na wyrobienie u dzieci prawidłowych nawyków (wzorców) zachowania

w sieci. Pomysł ten w połączeniu z propozycją szkolenia ludzi dorosłych z zakresu cyberbezpieczeństwa spowoduje, że niemal cały przekrój społeczeństwa będzie podlegał uświadamianiu wykluczając jedynie emerytów, rencistów oraz bezrobotnych.

Tab. Z-5. Zestawienie sił i środków niezbędnych do rozwiązania problemu nr. 5.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
5	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	nie są wymagane

Ocena działań naprawczych przez respondenta - Załącznik nr 8

Problem 6 - Wskazanie Operatora Strategicznej Sieci Bezpieczeństwa (OSSB) jako jedynego, w postaci jednoosobowej spółki skarbu państwa, realizowanego przez podmiot o znikomym znaczeniu na rynku telekomunikacyjnym. Zgodnie z wytycznymi dyrektyw unijnych rekomenduje się utworzenie OSSB. Należy mieć świadomość, że jak sama nawa wskazuje strategiczna sieć powinna mieć kluczowy priorytet ochrony, wobec czego zadanie to należy powierzyć podmiotom mającym do tego odpowiednie zaplecze i doświadczenie.

Rozwiązanie problemu. Biorąc pod uwagę znaczenie i destynację OSSB zaleca się, aby zadanie to powierzyć instytucji, która ma potencjał (infrastrukturę, kadry, doświadczenie) oraz bogate zaplecze naukowo-badawcze. Wszystkie powyższe przesłanki spełnia NASK-PIB, który ma nie tylko doświadczenie w utrzymywaniu sieci, ale ma również własny C-SIRT oraz jest jedną z najbardziej rozbudowanych instytucji w Krajowym Systemie Cyberbezpieczeństwa. Analizując niezbędne zasoby do implementacji prezentowanego rozwiązania szacuje się, że będą to następujące wielkości:

Tab. Z-6. Zestawienie sił i środków niezbędnych do rozwiązania problemu nr. 6.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
6	50 - 200 osób	50 - 200 osób	2 - 5 dokumentów	1 mln - 10 mln	500 tyś - 1 mln / mc

Ocena działań naprawczych przez respondenta - Załącznik nr 8

Problem 7 - Niewystarczająca ilość i jakość regulacji prawnych dotyczących dezinformacji. Zjawisko dezinformacji jest znane od zarania dziejów aj jej archetypem był „Koń Trojański". Współcześnie wspierane technologiami cyfrowymi może osiągać globalny zasięg oraz trafiać w ściśle sprecyzowaną grupę odbiorców. Istnieje uzasadniona potrzeba utworzenia zarówno regulacji prawnych oraz zinstytucjonalizowania grup doradczych w sprawach będących przedmiotem

dezinformacji. Doświadczenia z czasów pandemii COVID-19 pokazały jak bardzo ważne jest wdrożenie rozwiązań przedmiotowego problemu.

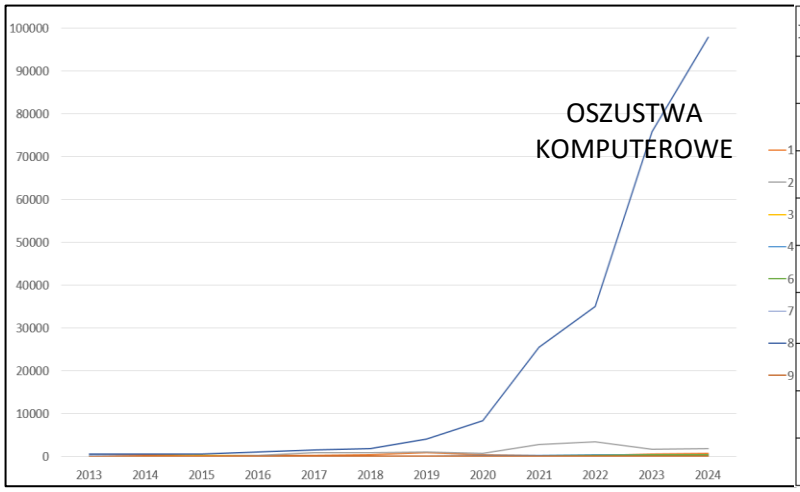
Rozwiązanie problemu. Godne uwagi jest podejście do dezinformacji przez państwo francuskie podczas wyborów prezydenckich z 2018 roku. Powstało wtedy specjalne rozporządzanie, które sankcjonowało masmedia i poprzez utworzenie 24 godzinnych sądów nakładano kary na twórców dezinformacji w postaci ograniczenia wolności lub niebagatelnej grzywny. W Polsce proponowane jest utworzenie Krajowej Rady ds. Dezinformacji składającej się z dziedzinowych członków Polskiej Akademii Nauk (uznanych autorytetów w każdej dziedzinie nauki) jako organ doradczy w sprawach dezinformacji. Rada miałaby charakter spotkań doraźnych i funkcjonowałaby przy PAN, gdzie wypracowane decyzje stanowiłyby podstawę do orzeczeń dla sądów (tak jak w modelu francuskim). Utworzenie przedmiotowej rady wraz z zmianą regulacji prawnych wymaga następujących nakładów:

Tab. Z-7. Zestawienie sił i środków niezbędnych do rozwiązania problemu nr. 7.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
7	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	20 tyś - 100 tyś / mc

Ocena działań naprawczych przez respondenta - Załącznik nr 8

Problem 8 - Zwiększenie liczby instytucji odpowiedzialnych za walkę z oszustwami komputerowymi i sprzężenie instytucji CBZC z KSC. Obecnie oszustwa komputerowe są „plagą" niemalże wszystkich państw rozwiniętych technologicznie (Rys 3).



LP	Incydent \ rok
1	Obraźliwe i nielegalne treści
2	Złośliwe oprogramowanie
3	Gromadzenie informacji
4	Włamania do systemów
5	Próby włamań do systemów
6	Dostępność zasobów ataki DDOS
7	Atak na bezpieczeństwo Informacji
8	Oszustwa komputerowe
9	Inne

Rys. Z - 3. Dane statystyczne kategorii incydentów za lata 2013-2024.
Źródło: Opracowanie na podstawie danych statystycznych raportu CSIRT GOV za lata 2013-2024.

Czasy pandemii COVID-19 ukierunkowały biznes (w tym handel) w kierunku zdalnym a co za tym idzie rozwinęły się mocno techniki, narzędzia i metody niezbędne do materializacji zagrożeń w Internecie. Skutkuje to tym, że zgodnie ze statystykami obecnie szeroko rozumiane oszustwa komputerowe są największym zagrożeniem z jakimi służby muszą walczyć.

Rozwiązanie problemu. Analiza operacyjnej działalności Centralnego Biura Zwalczania Cyberprzestępczości wykazała, że moce „przerobowe" biura są w stanie obsłużyć 1/49 obecnych przestępstw (incydentów) w związku z czym zachodzi konieczność rozbudowy lub utworzenia kolejnej placówki. Biorąc pod uwagę ilość odzyskanych środków z przestępczej działalności, będzie to inwestycja zwrotna z długofalową prognozą przynoszenia zysków dla budżetu państwa. Obecnie biuro za sam 2023 rok wykazało zyski w postaci 460 mln zł z tytułu odzyskanego mienia. Utworzenie kolejnego biura lub rozbudowa jednej z delegatur pozwoli na stopniowe zmniejszanie rosnącego trendu cyberprzestępczości. Zasadne jest również włączenie CBZC do Krajowego Systemu Cyberbezpieczeństwa tak aby nastąpił transfer wiedzy, doświadczenia oraz w odwód mocy „przerobowych" w sytuacjach kryzysowych. Nakłady niezbędne do realizacji potrzeb są następujące:

Tab. Z-8. Zestawienie sił i środków niezbędnych do rozwiązania problemu nr. 8.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
8	200 - 1000 osób	200 - 1000 osób	1 - 2 dokument	10 mln – 50 mln	500 tyś - 1 mln / mc

Ocena działań naprawczych przez respondenta - Załącznik nr 8

Problem 9 – Niski stan ukompletowania kadr w administracji państwowej. Problemem jest nie tylko mała liczba kadr, ale też i niski poziom kompetencji specjalistów. Aby utrzymać wysokie standardy i pozyskiwać wysokiej klasy specjalistów z branży „cyber" należy zrównać zarobki na rynku pracy administracji państwowej z rynkiem cywilnym.

Rozwiązanie problemu. Istnieje już rozwiązanie tego problemu natomiast jest ono realizowane w sposób niewłaściwy. Mowa tu o doprecyzowaniu i konsekwentnym stosowaniu zapisów z rozporządzenia w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa. Obecnie z powodu niedoprecyzowania wytycznych dodatki te nie są wypłacane a kierownicy jednostek organizacyjnych stosują praktyki nieujęte w dokumencie, aby zminimalizować wypłacanie tych dodatków (przy jednoczesnym pobieraniu go przez

własne osoby). Zmiana (doprecyzowanie rozporządzenia) w sprawie świadczeń teleinformatycznych może zmienić tendencję i uczynić, że państwowy sektor pracy w sektorze IT będzie bardzo atrakcyjnym dla specjalistów. W rozporządzeniu należy doprecyzować szczegółowy tryb przyznawania świadczeń oraz procedurę odwoławczą. Zasadne jest, aby uwzględniać nie tylko kwalifikacje pracownika, ale również i zadania wynikające karty opisu stanowiska służbowego (KOSS) bo to ona definiuje zakres wykonywanej pracy:

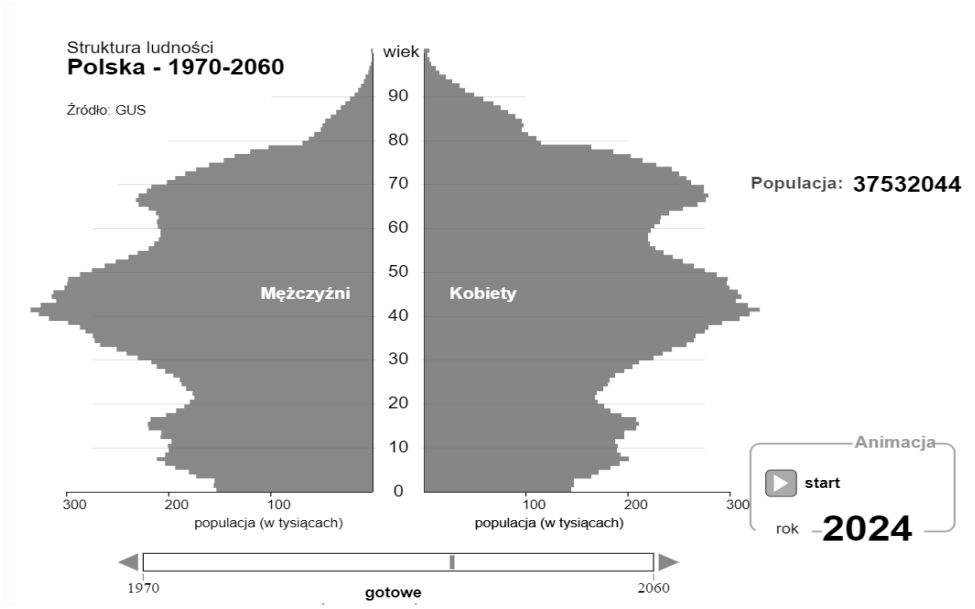
Tab. Z - 9. Zestawienie sił i środków niezbędnych do rozwiązania problemu nr. 9.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
9	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	nie są wymagane

<u>Ocena działań naprawczych przez respondenta - Załącznik nr 8</u>

Problem 10 - Niski poziom finansowania podmiotów odpowiedzialnych za Cyberbezpieczeństwo. W cyberbezpieczeństwie jest problemem nadrzędnym, ponieważ mając nieograniczony budżet można zatrudnić każdego specjalistę, kupić dowolną technologię czy prowadzić badania nad nowymi rozwiązaniami. Obecnie w wyniku niezbyt satysfakcjonującego poziomu finansowania cyberbezpieczeństwa w Polsce można zauważyć deficyt wyżej wymienionych składowych.

Rozwiązanie problemu - Należy zaznaczyć, że z punktu widzenia polityki wprowadzanie nowego podatku może okazać się nieakceptowalne przez społeczeństwo. Wobec czego rozwiązaniem problemu zdaje się być modyfikacja obecnego mało efektywnego podatku (o niskim poziomie windykacji), którym jest abonament radiowo telewizyjny. Abonament RiTV nie ma zbyt wielu zwolenników w Polsce a powody są różne. Ze statystyk wynika, że zaledwie 1/3 Polaków (dane za 2022 rok) uiszcza daninę. Zastąpienie abonamentu RiTV abonamentem cyberbezpieczeństwa pozwoli na uzyskanie finansowania „cyber" na wysokim poziomie. Zachowując zasady dotychczasowego abonamentu zwalniające najmniej zamożnych obywateli, zadłużonych, weteranów czy emerytów to nadal w państwie posiadamy potencjał demograficzny do utrzymania wysokiego poziomu finansowania cyberbezpieczeństwa. Przy założeniu, że tak jak z odbiorem nieczystości opłata jest pobierana od każdego domownika to statystycznie mamy około 31 milionów podatników.



Rys. Z - 4. Liczebność i struktura ludności w Polsce w 2024 roku.
Źródło: Opracowanie na podstawie danych z GUS 2025.

Zakładając, że abonament od 1 osoby wyniesie 10 zł (obecnie abonament RiTV to 37 zł za telewizor i radio) to statystyczna 4 osobowa rodzina zapłaci 40 złotych miesięcznie. Aby zmotywować społeczeństwo do prezentowanej zmiany należy wprowadzić regulację stanowiące o braku możliwości zakupu technologii cyfrowej bez możliwości wylegitymowania się dokumentem potwierdzającym cykliczne opłaty abonamentu. Ta sama procedura dotyczy wywożenia odpadów do Punktu Selektywnej Zbiórki Odpadów Komunalnych więc tego typu regulację nie są obce. Dodatkowo obywatele w przypadku stania się ofiarą cyberprzestępców mogą rościć odszkodowanie, zadośćuczynienie czy ściganie z urzędu sprawców tylko w przypadku stałego opłacania abonamentu. Reasumując, zachowując windykację na poziomie tylko 90% to z prostego rachunku można wyliczyć:

31 mln. X 10 zł) x 0,9 = 279 mln/mc ≈ co daje rocznie 3,38 mld.

Prezentowana kwota w skali roku jest nieporównywalnie większa niż roczny Fundusz Cyberbezpieczeństwa, który zakłada **250 mln zł**. Niezbędne nakłady konieczne do uzyskania przedmiotowego rozwiązania przedstawia tabela:

Tab. Z-10. Zestawienie sił i środków niezbędnych do rozwiązania problemu nr. 10.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
10	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	nie są wymagane

<u>Ocena działań naprawczych przez respondenta - Załącznik nr 8</u>

Podsumowanie wywiadu.

Prezentowane problemy oraz proponowane rozwiązania są ze sobą ściśle powiązane co przykładowo oznacza, że aby pozyskać środki finansowe na cyberbezpieczeństwo należy wprowadzić program finansowania publicznego, natomiast aby to uczynić należy przekonać społeczeństwo do zagrożeń wynikających z działań w cyberprzestrzeni a to można dokonać jedynie poprzez ekspozycję odpowiednie roli i rangi cyberbezpieczeństwa w dokumentach strategicznych poziomu krajowego. Należy podkreślić, że zgodnie dobrą praktyką należy zaznaczyć pewien przedział niepewności wobec wprowadzania tak obszernych i radykalnych rozwiązań niemniej jednak są one konieczne do dalszego prawidłowego funkcjonowania państwa w obliczu nowych zagrożeń, które mogą wykorzystywać do materializacji cyberprzestrzeń. Poniższa tabela prezentuje zbiorcze nakłady niezbędne do kompleksowego wprowadzenia działań naprawczych.

Tab. Z-11. Zestawienie sił i środków niezbędnych do wdrożenia koncepcji.

Lp.	Wielkość infrastruktury (A)	Liczba personelu (B)	Zmiana regulacji prawnych (C)	Koszty utworzenia (D)	Utrzymanie miesięczne (E)
1	nie jest wymagana	nie jest wymagany	2 - 5 dokumenty	nie są wymagane	100 tyś - 500 tyś / mc
2	nie jest wymagana	nie jest wymagany	5 - 10 dokumentów	nie są wymagane	nie są wymagane
3	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	100 tyś - 500 tyś / mc
4	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	nie są wymagane
5	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	nie są wymagane
6	50 - 200 osób	50 - 200 osób	2 - 5 dokumentów	1 mln - 10 mln	500 tyś - 1 mln / mc
7	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	20 tyś - 100 tyś / mc
8	200 - 1000 osób	200 - 1000 osób	1 - 2 dokument	10 mln – 50 mln	500 tyś - 1 mln / mc
9	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	nie są wymagane
10	nie jest wymagana	nie jest wymagany	1 - 2 dokument	nie są wymagane	nie są wymagane
S	**250 - 1200 osób**	**250 - 1200 osób**	**16 - 34 dokumenty**	**11 mln - 60 mln**	**1,22 mln - 3,10 mln**

Źródło: Opracowanie własne.

Należy jednak mieć świadomość, że proponowane rozwiązania przyniosą również wkład do budżetu państwa np.: 3,38 mld/r. z tytułu abonamentu „cyber" oraz z działalności rozbudowanego biura CBZC w wysokości około 450 mln/r. co łącznie daje prawie 4 miliardy złotych na zaspokojenie potrzeb krajowego cyberbezpieczeństwa.

<u>Ocena całościowa (końcowa) działań naprawczych przez respondenta – załącznik nr 8</u>

<u>Opinia końcowa i uwagi do koncepcji - załącznik nr 8</u>

Serdecznie dziękuję za współpracę, wypełnienie kwestionariusza zgodnie z instrukcją, za poświęcony mi czas na wywiad oraz przekazanie jakże cennej wiedzy i uwag.

Z poważaniem

Marcin DĄBROWSKI

SPIS TABEL I RYSUNKÓW

OŚWIADCZENIE AUTORA ROZPRAWY DOKTORSKIEJ

Marcin DĄBROWSKI
imię i nazwisko

Warszawa 01.06.2025
miejscowość, data

Oświadczenie autora rozprawy doktorskiej o jej oryginalności, samodzielności jej przygotowania i o nienaruszeniu praw autorskich oraz zgodności z wersją cyfrową

Niniejszym oświadczam, że przedłożoną rozprawę doktorską pt.: **„Cyberprzestrzeń i cyberbezpieczeństwo jako determinanty bezpieczeństwa narodowego Rzeczpospolitej Polskiej”** napisałem samodzielnie, tj.

- ✓ Nie zleciłem opracowania pracy lub jej części innym osobom,
- ✓ Nie przepisałem pracy lub jej części z innych opracowań i prac związanych tematycznie z moją pracą,
- ✓ Korzystałem jedynie z niezbędnych konsultacji,
- ✓ Wszystkie elementy pracy, które zostały wykorzystane do jej realizacji (cytaty, ryciny, tabele, programy itp.), a niebędące mojego autorstwa, zostały odpowiednio zaznaczone oraz zostało podane źródło ich pochodzenia.

Oświadczam również, że niniejsza wersja rozprawy doktorskiej jest identyczna z załączoną wersją cyfrową umieszczoną na nośniku danych.

Mam świadomość, że złożenie nieprawdziwego oświadczenia skutkować będzie niedopuszczeniem do dalszych czynności nadania stopnia doktora lub cofnięciem decyzji o nadaniu mi stopnia doktora oraz wszczęciem postępowania dyscyplinarnego.

Marcin Dąbrowski

.....
czytelny podpis autora

PODZIĘKOWANIA

Niniejsza dysertacja mogła powstać dzięki dużej życzliwości wielu osób. Wszystkim tym, którzy przyczynili się do jej powstania, tj.: rodzinie, przyjaciołom, całej kadrze dydaktyczno-naukowej Wojskowej Akademii Technicznej im. Jarosława Dąbrowskiego w Warszawie, a w szczególności pracownikom Szkoły Doktorskiej, serdecznie dziękuję. Szczególne podziękowania kieruję pod adresem opiekunów naukowych, a zarazem promotorów pracy, Pana prof. dr hab. inż. Piotra ZASKÓRSKIEGO oraz promotora pomocniczego Pana dr inż. Krzysztofa LIDERMANA, od których czerpałem całą swoją wiedzę i którzy przyczynili się do zmiany mojego spojrzenia na świat…..za inspirację do podjęcia twórczego wysiłku, intelektualną motywację, merytoryczne oraz metodologiczne ukierunkowanie moich poczynań naukowych, a przede wszystkim za cierpliwość i zrozumienie oraz wiarę w moją wytrwałość. Za wszystko serdecznie dziękuję...

Jest jednak osoba, która w sposób wyjątkowy przyczyniła się do mojego myślenia twórczego. Jest to moja żona Anna, która zdecydowaną większość obowiązków rodzinnych wzięła na siebie, abym mógł tworzyć i się rozwijać...

Dziękuję Ci kochana Anno.

„Różnica pomiędzy niemożliwym a możliwym leży w determinacji człowieka”.

- Tommy Lasorda

„Nigdy nie rezygnuj z marzeń, tylko dlatego, że zrealizowanie ich wymaga czasu. Czas i tak upłynie”.

- Earl Nightingale

„Dedykuję wszystkim tym osobom, które myślą, że nie są wystarczająco zdeterminowane i nie mają czasu, aby spełniać marzenia”.

- Marcin Dąbrowski

STRESZCZENIE ROZPRAWY DOKTOSKIEJ

„Cyberprzestrzeń i cyberbezpieczeństwo jako determinanty bezpieczeństwa narodowego Rzeczpospolitej Polskiej”

autor: mgr inż. Marcin DĄBROWSKI

Słowa kluczowe: cyberprzestrzeń cyberbezpieczeństwo, bezpieczeństwo państwa, system bezpieczeństwa narodowego, krajowy system cyberbezpieczeństwa

Głównym celem badań w dysertacji była identyfikacja luk, wad, słabości w Systemie Bezpieczeństwa Narodowego i opracowanie na podstawie jej wyników koncepcji zwiększenia poziomu bezpieczeństwa państwa. Jako problem badawczy przedstawiono pytanie jakie luki, wady, słabości występują w obecnym Systemie Bezpieczeństwa Narodowego i w jaki sposób można ograniczać skutki ich wykorzystania do nieuprawnionych działań. W związku z czym sformułowano hipotezę, że cyberprzestrzeń jest wykorzystywana przez szereg zagrożeń dla bezpieczeństwa narodowego, które wymagają stosownych odpowiedzi ze strony instytucji państwa w szczególności eliminacji podatności obniżających odporność państwa na cyberzagrożenia. Główny cel oraz szczegółowe i sposób ich osiągania opisano w sześciu rozdziałach dysertacji opatrzonej wstępem oraz zakończeniem.

Głównym rezultatem przeprowadzonych badań, było opracowanie koncepcji poprawy bezpieczeństwa państwa w obszarze cyberbezpieczeństwa oraz (ze względu na wagę) zapewniania informacyjnej ciągłości działania.

Pierwszy rozdział stanowił wprowadzenie do dziedziny problemu z jednoczesnym wyeksponowaniem kluczowych definicji dla badanego obszaru i precyzyjnym wskazaniem pola badawczego.

Przy pomocy rozdziału drugiego uszczegółowiono jakie badania, przy pomocy jakich narzędzi i technik należy przeprowadzić, aby osiągnąć zakładane cele (wraz z szczegółowymi) oraz przedstawiono dostępny stan wiedzy w badanym obszarze.

Rozdział trzeci stanowił trzon rozprawy, gdzie zdiagnozowano występujące podatności systemowe oraz elementy materializacji zagrożenia poprzez przeprowadzenie wywiadów, analiz danych statystycznych oraz analizę krytyczną dokumentacji poziomu strategicznego i normatywnego.

Elementy zarządzania ryzykiem w rozdziale czwartym pozwoliły na usprawnienie systemu bezpieczeństwa państwa poprzez utworzenie mapy ryzyka oraz wskazanie oczekiwanych strat przy założeniu, że nie zostaną podjęte żadne działania naprawcze.

W rozdziale tym wykazano jakie relacje zachodzą pomiędzy podatnościami a potencjalnymi zagrożeniami uzyskanymi w poprzednim rozdziale i podjęto decyzję na podstawie szacowania i analiz jak postępować z stwierdzonym ryzykiem.

W rozdziale piątym, dla każdej stwierdzonej podatności zostało zaproponowane rozwiązanie problemu, w ujęciu obszarów takich jak finansowo-ekonomiczny, prawno-proceduralny, techniczno-logistyczny i mentalny. W celu zweryfikowania zalet i wad dla każdego rozwiązania przeprowadzono analizę SWOT co pozwoliło nie tylko na wyeksponowanie mocnych stron i szans, ale i na dostrzeżenie nowych sposobów realizacji zagrożeń.

W ostatnim rozdziale zaprezentowano propozycję sposobu implementacji opracowanej koncepcji poprawy bezpieczeństwa. Każda eliminowana podatność (każde rozwiązanie z rozdziału IV) została opisane na podstawie niezbędnych do osiągnięcia zakładanego celu wskaźników takich jak: rozbudowa niezbędnej infrastruktury, pozyskanie wyspecjalizowanych kadr, zmiana niezbędnych regulacji prawnych, wstępne koszty utworzenia i koszty cykliczne utrzymania. Dokonane w taki sposób zestawienie pozwoliło na analizę wymaganych nakładów sił i środków do implementacji przedmiotowej koncepcji w całości. Pracę zamykają wnioski podsumowujące wykonane badania oraz wskazania kierunków ewentualnych dalszych badań.

W wyniku przeprowadzonych badań stwierdzono, że obecnie najważniejszy system bezpieczeństwa państwa jaki jest System Bezpieczeństwa Narodowego wraz z podsystemami wymaga aktualizacji. Podstawą formalną zapewniania cyberbezpieczeństwa są ogólne (ponaddziedzinowe) strategie, polityki, wizje i regulacje prawne co wymaga podniesienia rangi cyberbezpieczeństwa do poziomu ponaddziedzinowego. Należy również rozbudować istniejącą infrastrukturę o pewne instytucje tak aby zachować zdolność radzenia sobie z współczesnymi zagrożeniami. W koncepcji zaproponowano również propozycję wyeliminowania dwóch najważniejszych w cyberbezpieczeństwie zagrożeń tj. niewystarczających środków finansowych i ukompletowania specjalistycznych kadr.

Jak wskazują badania zawarte w dysertacji wdrożenie w życie przedmiotowej koncepcji poprawy bezpieczeństwa jest to warunek konieczny do tego, aby wszystkie systemy i podsystemy bezpieczeństwa państwa mogły mieć zdolność do wypełniania zadań na wysokim poziomie skuteczności i efektywności.

SUMMARY OF DOCTORAL DISSERTATION

"Cyberspace and cybersecurity as determinants of national security of the Republic of Poland"

author: M.Sc. Eng. Marcin DĄBROWSKI

Keywords: cyberspace, cybersecurity, state security, national security system, national cybersecurity system

The main objective of the research in the dissertation was to identify gaps, defects, elimination in the National Security System and study on the results of the side effects of state security. As a research problem, what is the question, what is the risk, occurrence in the current National Security System and how can the effects of their use for unauthorized actions be limited. In connection with this, what results from the hypothesis, that cyberspace is a solution through a number of threats to national security, which require appropriate responses from state institutions in the event of eliminating vulnerabilities that reduce the state's exposure to cyber threats. The main objective and detailed and methods of achieving them in six chapters of the dissertation provided with an introduction and conclusions. The result of the research was the occurrence of the effects of state security in the case of cybersecurity and (due to the threat) provides information on the continuity of activities.

The first chapter presents the problem with exposing the extension for the studied area and using the indication of the research field.

The second chapter details what research, tools and techniques should be used to achieve the assumed goals (along with specific ones) and presents the available state of knowledge in the researched area.

The third chapter was the core of the dissertation, where the existing systemic vulnerabilities and elements of threat materialization were diagnosed by conducting interviews, statistical data analyses and critical analysis of strategic and normative level documentation.

The risk management elements in the fourth chapter allowed for the improvement of the state security system by creating a risk map and indicating the expected losses assuming that no corrective actions are taken.

This chapter shows what relationships occur between vulnerabilities and potential threats obtained in the previous chapter and a decision was made based on estimation and analysis on how to deal with the identified risk.

In the fifth chapter, a solution to the problem was proposed for each identified vulnerability, in terms of areas such as financial and economic, legal and procedural, technical and logistic and mental. In order to verify the advantages and disadvantages of each solution, a SWOT analysis was conducted, which allowed not only to highlight the strengths and opportunities but also to notice new ways of implementing threats. The last chapter presents a proposal for the implementation of the developed concept of improving security. Each eliminated vulnerability (each solution from chapter IV) was described on the basis of indicators necessary to achieve the assumed goal, such as: expansion of the necessary infrastructure, acquisition of specialized staff, change of necessary legal regulations, initial costs of creation and cyclical maintenance costs. The comparison made in this way allowed for an analysis of the required expenditures, forces and resources to implement the subject concept in its entirety. The work ends with conclusions summarizing the research carried out and indications of directions for possible further research.

As a result of the conducted research, it was found that currently the most important state security system, which is the National Security System together with its subsystems, requires updating. The formal basis for ensuring cybersecurity are general (transdisciplinary) strategies, policies, visions and legal regulations, which requires raising the rank of cybersecurity to a transdisciplinary level. It is also necessary to expand the existing infrastructure with certain institutions in order to maintain the ability to cope with contemporary threats.

The concept also proposes a proposal to eliminate the two most important threats in cybersecurity, i.e. insufficient financial resources and completing specialist cards. As indicated by the research included in the dissertation, the implementation of the subject concept of improving security is a necessary condition for all state security systems and subsystems to be able to fulfill tasks at a high level of effectiveness and efficiency.