System bezpieczeństwa cyberprzestrzeni RP

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, wrzesień 2015

Publikacja została opracowana przez zespół ekspertów, przedstawicieli

Naukowej Akademickiej Sieci Komputerowej instytutu badawczego (NASK), w tym

zespołu **CERT Polska** funkcjonującego w ramach **NASK**.

Skład zespołu ekspertów:

Iwona Jarosz
Przemysław Jaroszewski
Piotr Kijewski
Tomasz Jordan Kruk
Krzysztof Silicki
Tomasz Grudziecki

Praca wykonana na podstawie Umowy
Ministerstwa Administracji i Cyfryzacji (MAC)
z **Naukową i Akademicką Siecią Komputerową (NASK)**.

Warszawa, wrzesień 2015 r.

wersja 1.01

Streszczenie

Przedmiotem niniejszej ekspertyzy jest rekomendacja modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce. Dokument został opracowany na zlecenie Ministerstwa Administracji i Cyfryzacji przez ekspertów instytutu badawczego NASK i działającego w jego ramach zespołu CERT Polska.

Dynamiczny rozwój zagrożeń i incydentów naruszających bezpieczeństwo systemów i sieci komputerowych oraz użytkowników korzystających z usług oferowanych przez nowoczesne technologie informatyczne powoduje, że zachowanie bezpieczeństwa przestrzeni tworzonej przez te systemy, usługi, wraz z relacjami z użytkownikami – zwanej cyberprzestrzenią – jest obecnie jednym z istotniejszym problemów na poziomie krajowym i międzynarodowym w kontekście konieczności zapewnienia niezakłóconego funkcjonowania państw, gospodarki i społeczeństwa.

Według raportów krajowych, publikowanych przez zespoły reagujące CERT[1], agencje Unii Europejskiej[2] czy firmy komercyjne zajmujące się bezpieczeństwem cyberprzestrzeni, technologiczne zagrożenia bezpieczeństwa (np. techniki infekowania szkodliwym oprogramowaniem) są coraz bardziej zaawansowane, a skala incydentów rośnie z roku na rok. Narasta także problem nielegalnych i szkodliwych treści w Internecie. Wzrasta przestępczość opierająca się na nielegalnej działalności w cyberprzestrzeni (np. oszustwa z wykorzystaniem szkodliwego oprogramowania atakującego konta bankowości elektronicznej).

Taki obraz sytuacji w cyberprzestrzeni determinuje konieczność prowadzenia skoordynowanych działań na poziomie krajowym, które będą angażowały zarówno administrację państwową, jak też innych interesariuszy w postaci: podmiotów gospodarczych w różnych sektorach (w szczególności będących częścią infrastruktury krytycznej, ale także średnich i małych przedsiębiorstw), sektora badawczo-naukowego, organizacji pozarządowych, czy wreszcie samych użytkowników cyberprzestrzeni.

Przedmiotem niniejszej ekspertyzy jest opis istniejącej sytuacji w Polsce w dziedzinie ochrony cyberprzestrzeni na poziomie krajowym, traktowany jako punkt wyjścia do zaproponowania organizacji przyszłego systemu, który zapewni akceptowalny poziom bezpieczeństwa cyberprzestrzeni. W ramach proponowanych rozwiązań przeanalizowano trzy warianty systemu, zróżnicowane pod względem stopnia centralizacji.

[1] Takie jak CERT.GOV.PL, CERT Polska
[2] Takie jak ENISA, EC3/ Europol

Wariant zdecentralizowany, zwany rozproszonym, w maksymalnym stopniu wykorzystuje istniejące obecnie podmioty i kompetencje w dziedzinie ochrony cyberprzestrzeni. Drugi wariant, pośredni, zakłada pewien stopień centralizacji (instytucja koordynująca w postaci ministerstwa oraz organizacja reagująca w warstwie operacyjnej w postaci ABW), lecz nie zakłada wymogu powoływania nowych centralnych instytucji. W wariancie scentralizowanym założono z kolei powstanie nowej instytucji (agencji), która skupia większość funkcji koordynujących i wykonawczych zapewniających odpowiedni poziom bezpieczeństwa na poziomie krajowym.

Zdefiniowano role i obowiązki poszczególnych podmiotów w każdym z wariantów, a następnie dokonano analizy typu SWOT, która prowadzi do wniosku, iż najbardziej optymalne dla szybkiego stworzenia kompleksowego i efektywnego systemu będzie wybranie wariantu rozproszonego.

Kluczową rekomendacją, niezależnie od przyjętego wariantu, jest powołanie instytucji koordynującej, która zapewni odpowiednie funkcjonowanie systemu zarówno w warstwie strategiczno-legislacyjnej jak również w aspekcie koordynacji w warstwie operacyjnej. W wariancie rozproszonym oraz pośrednim proponuje się przypisanie tej roli, wraz z odpowiednimi uprawnieniami i zasobami budżetowymi, jednemu z istniejących ministerstw: Ministerstwu Administracji i Cyfryzacji bądź Ministerstwu Spraw Wewnętrznych. W wariancie scentralizowanym rola ta byłaby przypisana nowej instytucji (agencji), która musiałaby zostać powołana.

W warstwie operacyjnej budowanie systemu ochrony cyberprzestrzeni rekomenduje się oprzeć o podmioty, które dysponują odpowiednim przygotowaniem, doświadczeniem i rozpoznawalnością na arenie krajowej i międzynarodowej. W tej warstwie, kluczowej dla efektywnego działania całego systemu, rozumianej jako zdolność do skutecznego rozwiązywania problemów w określonym czasie, proponuje się wykorzystanie i zaangażowanie funkcjonujących zespołów CERT, takich jak: CERT.GOV.PL, CERT Polska – i w sferze militarnej zespołu CERT w resorcie obrony narodowej (MIL-CERT).

W niniejszej ekspertyzie opisano role i zadania wielu podmiotów czy ciał stanowiących istotne elementy krajowego systemu bezpieczeństwa cyberprzestrzeni, takich jak wspomniany Koordynator, CSIRT krajowy, a także Krajowe Centrum Analityczne, Rada Koordynacyjna przy Premierze RP, Zespół Łącznikowy, CSIRTy sektorowe, centra ISAC czy Zespoły Zadaniowe do rozwiązywania zdefiniowanych problemów (np. technicznych, systemowych) w obszarze cyberprzestrzeni.

Także istniejące instytucje, takie jak Rządowe Centrum Bezpieczeństwa, organa ścigania i służby (m.in. Policja, ABW) czy poszczególne ministerstwa i inne instytucje państwowe zostały scharakteryzowane pod kątem ról, jakie odgrywają w dziedzinie cyberbezpieczeństwa.

W ramach ekspertyzy zostały również przeanalizowane kluczowe oficjalne dokumenty o charakterze strategicznym lub kierunkowe, odnoszące się do omawianego obszaru – zarówno krajowe, jak też obowiązujące na poziomie Unii Europejskiej.

Sformułowano szereg rekomendacji, które odnoszą się zarówno do poziomu strategicznego jak i operacyjnego. Rekomendacje zostały podsumowane w osobnym rozdziale wieńczącym ekspertyzę. Wśród kluczowych rekomendacji znalazły się między innymi:

- konieczność określenia ram systemu ochrony cyberprzestrzeni RP, który zapewni ochronę interesu narodowego, przy uwzględnieniu ponadgranicznego charakteru zagrożeń w cyberprzestrzeni oraz planowanej legislacji na poziomie Unii Europejskiej;
- zapewnienie, aby utworzony system uwzględniał i maksymalnie wykorzystywał istniejące dokonania i potencjał w dziedzinie cyberbezpieczeństwa, a w odpowiednich przypadkach, również doświadczenia innych krajów;
- niezależnie od przyjętego modelu ochrony cyberprzestrzeni RP, powołanie instytucji koordynującej działania administracji publicznej w zakresie ochrony cyberprzestrzeni RP. Preferowana formuła – przypisanie tej funkcji ministrowi lub wiceministrowi, co najmniej w randze podsekretarza stanu oraz szczegółowe określenie zakresu działania właściwego ministra;
- doprowadzenie do uspójnienia wszelkich dokumentów o charakterze strategicznym, obejmujących zagadnienia bezpieczeństwa cyberprzestrzeni, a docelowo – opracowanie jednego dokumentu o charakterze strategicznym: strategii ochrony cyberprzestrzeni RP;
- zapewnienie przeznaczenia odpowiednich zasobów (finansowych, technicznych, osobowych) w celu efektywnej realizacji zadań wynikających z opracowanych dokumentów o charakterze strategicznym, jak również z transpozycji dyrektywy NIS;
- niezależnie od przyjętego modelu ochrony cyberprzestrzeni RP, pilne powołanie oficjalnego zespołu reagującego na zagrożenia i incydenty bezpieczeństwa w cyberprzestrzeni na poziomie krajowym – CSIRT-u krajowego. Preferowana formuła – powierzenie roli CSIRTu krajowego jednemu z już działających zespołów reagowania, tj. CERT Polska, działającemu w ramach NASK, lub CERT.GOV.PL, działającemu w ramach ABW, przy jednoczesnym rozszerzeniu kompetencji CERT.GOV.PL o obowiązki w zakresie ochrony instytucji administracji samorządowej i, ewentualnie, infrastruktury krytycznej;
- niezależnie od przyjętego modelu ochrony cyberprzestrzeni RP, powołanie organu opiniodawczego i doradczego dla Rady Ministrów w sprawach dotyczących cyberbezpieczeństwa, w szczególności w celu formułowania ocen i wyrażania opinii w sprawach projektów aktów normatywnych dotyczących cyberbezpieczeństwa, kierunków i planów działania organów zaangażowanych w ochronę cyberprzestrzeni czy koordynowania ich współdziałania;

- wypracowanie metod okresowej oceny skuteczności/ efektywności przyjętego rozwiązania w zakresie krajowego systemu ochrony cyberprzestrzeni (m.in. poprzez określenie mierników, które mogą zostać w tym procesie wykorzystane);
- ustanawianie minimalnych lub optymalnych wymogów bezpieczeństwa, na podstawie procesów analiz ryzyka i wiedzy na temat zagrożeń oraz technologii zabezpieczających oraz wdrażanie schematów raportowania o istotnych incydentach w danym sektorze w celu zapewnienia skoordynowanego podejścia do cyberbezpieczeństwa, przy jednoczesnym zachowaniu zasad dialogu pomiędzy organami regulacyjnymi czy tworzącymi prawo a przedstawicielami danego sektora. Przygotowywanie poradników i instrukcji dla podmiotów, które będą zobowiązane wdrażać ustanowione wymogi bezpieczeństwa.

Precyzyjne oszacowanie kosztu wdrożenia proponowanego systemu jest na tym etapie zadaniem niewykonalnym ze względu na wariantowość propozycji oraz konieczność podjęcia decyzji co do szczegółowego zakresu funkcjonowania struktur w wybranym wariancie. Dlatego też, wykonując pierwszy krok w celu dokonania szacunków, opracowano katalog kategorii kosztów, jakie wiązałyby się z wdrożeniem krajowego systemu bezpieczeństwa cyberprzestrzeni, jak również przedstawiono oszacowanie liczby etatów merytorycznych jaka, według wiedzy autorów, zapewnia odpowiedni poziom bezpieczeństwa na poziomie kraju.

Autorzy ekspertyzy wyrażają pogląd, że konieczny do realizacji proces budowy i rozbudowy krajowego systemu bezpieczeństwa cyberprzestrzeni RP powinien się odbywać w ramach dialogu pomiędzy wszystkimi interesariuszami przestrzeni komunikacji elektronicznej, w którym to procesie administracja państwa powinna odegrać rolę koordynatora i katalizatora współpracy pomiędzy zainteresowanymi stronami.

Spis treści

Streszczenie I

1 Wprowadzenie 1

2 Kluczowe podmioty związane z funkcjonowaniem obszaru cyberbezpieczeństwa kraju – stan obecny 4

2.1 Wstęp 4
2.2 Charakterystyka kluczowych podmiotów 4
2.3 Role instytucjonalne w podziale na obszary i działy 18

3 Rozwiązania regulacyjne i strategiczno-programowe w Polsce i UE dotyczące ochrony cyberprzestrzeni 24

3.1 Rozwiązania krajowe 24
3.1.1 Polityka Ochrony Cyberprzestrzeni RP 24
3.1.2 Doktryna Cyberbezpieczeństwa RP 25
3.1.3 Prawo telekomunikacyjne a obowiązki w dziedzinie cyberbezpieczeństwa 26
3.1.4 Inne dokumenty 39
3.2 Rozwiązania UE 40
3.2.1 Projekt dyrektywy NIS 40
3.2.2 Inne dokumenty 48
3.3 Aspekt skoordynowanego procesu raportowania o naruszeniach bezpieczeństwa w różnych sektorach i obszarach 51
3.3.1 Schematy zgłaszania naruszeń – konkluzje 54

4 Kluczowe obowiązki w zakresie zarządzania bezpieczeństwem sieci i informacji systemów teleinformatycznych 57

4.1 Sposób organizacji systemu zarządzania ryzykiem teleinformatycznym i zakres podmiotów zobowiązanych do jego prowadzenia 57
4.1.1 Analiza stosowanych dokumentów pod względem zarządzania ryzykiem 58
4.1.2 Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej 58
4.1.3 Metodyka szacowania ryzyka na potrzeby systemów jawnych 59
4.1.4 Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego 60
4.1.5 Sprawozdanie z szacowania ryzyka cyberprzestrzeni w administracji rządowej w 2013 r. 61
4.1.6 Koncepcja i założenia do metodyki oceny ryzyka i przygotowania sprawozdania dotyczącego cyberbezpieczeństwa 62
4.1.7 Rekomendacja systemu zarządzania ryzykiem teleinformatycznym 63
4.2 Mechanizmy tworzenia krajowego rejestru ryzyka 65

5 Analiza i zdefiniowanie roli zespołów CSIRT 67

5.1 CERT vs. CSIRT ... 67
5.2 CSIRT rządowy a CSIRT krajowy ... 67

6 System ochrony cyberprzestrzeni – warstwa operacyjna ... 69
6.1 Wstęp ... 69
6.2 Mapa podmiotów ... 70
6.2.1 Opis podmiotów i interesariuszy w warstwie operacyjnej ... 72
6.3 Zadania interesariuszy systemu ochrony cyberprzestrzeni ... 73
6.3.1 Koordynator ochrony cyberprzestrzeni ... 74
6.3.2 Punkt Kontaktowy ... 74
6.3.3 CSIRT Krajowy ... 75
6.3.4 Krajowe Centrum Analityczne ... 76
6.3.5 Zespół Łącznikowy ... 77
6.3.6 Zespoły Zadaniowe ds. bezpieczeństwa cyberprzestrzeni ... 80
6.3.7 Sektorowe zespoły CSIRT ... 81
6.3.8 Platforma wymiany informacji ... 83
6.3.9 Centra ISAC ... 84
6.3.10 Zespoły CSIRT powoływane przez poszczególne podmioty ... 85
6.3.11 Pełnomocnicy Ochrony Cyberprzestrzeni (POC) ... 86
6.3.12 Nieformalne fora współpracy ... 87
6.3.13 SOC (Security Operations Center) ... 88
6.3.14 Punkt przyjmowania zgłoszeń o nielegalnych lub niepożądanych treściach (m.in. CSAM) - Hotline ... 91
6.3.15 Zespół Łącznikowy ... 91
6.3.16 Organa ścigania cyberprzestępstw ... 93
6.3.17 System wczesnego ostrzegania o zagrożeniach ... 95
6.3.18 Łowcy ... 96
6.4 Usługi CSIRT, które muszą być realizowane niezależnie od przyjętego wariantu ... 97
6.5 Rekomendacja ogólna w podejściu do budowania systemu ... 107
6.6 Wariant zdecentralizowany ... 107
6.6.1 Koordynator (MAC lub MSW) ... 109
6.6.2 CSIRT krajowy (CERT Polska/NASK) ... 111
6.6.3 Krajowe Centrum Analityczne (CERT Polska/NASK) ... 111
6.6.4 CSIRT rządowy (ABW) ... 112
6.6.5 Opcjonalnie CSIRT-IK ... 112
6.6.6 Pozostałe podmioty ... 113
6.6.7 Opis zalet i wad modelu ... 113
6.6.8 Wymiar prawny ... 115
6.7 Wariant pośredni ... 118
6.7.1 Koordynator (MAC lub MSW) ... 119
6.7.2 CSIRT krajowy (ABW) ... 119
6.7.3 Krajowe Centrum Analityczne (CERT Polska/NASK) ... 120
6.7.4 Opcjonalnie CSIRT-IK (RCB) ... 120
6.7.5 Pozostałe podmioty ... 120
6.7.6 Opis zalet i wad modelu ... 121

6.7.7 Wymiar prawny 122
6.8 Wariant scentralizowany 124
6.8.1 Narodowe Centrum Cyberbezpieczeństwa 125
6.8.2 Opcjonalnie – Krajowe Centrum Analityczne (NASK) 127
6.8.3 Opis zalet i wad modelu 127
6.8.4 Wymiar prawny 128
6.9 Wariant - pozostawienie sytuacji bez zmian 132

7 Warstwa strategiczna funkcjonowania krajowego systemu ochrony cyberbezpieczeństwa 134
7.1 Wstęp 134
7.2 Opis ogólny w warstwie strategicznej 134
7.2.1 Koordynator 135
7.2.2 Rada Koordynacyjna przy Premierze 136
7.2.3 Zespół Łącznikowy 137
7.2.4 Informatyczna Infrastruktura Krytyczna 139
7.2.5 Sektor energetyczny 139
7.2.6 Sektor telekomunikacyjny 139
7.2.7 Sektor finansowy 140
7.2.8 Administracja publiczna 140
7.2.9 Inne sektory i obszary 141
7.2.10 Zespoły Zadaniowe 142
7.3 Warianty organizacji systemu ochrony cyberprzestrzeni w warstwie strategicznej 142
7.3.1 Wariant rozproszony 142
7.3.2 Wariant pośredni 145
7.3.3 Wariant scentralizowany 145

8 Analiza SWOT trzech wariantów 147
8.1 Wariant rozproszony 148
8.2 Wariant pośredni 149
8.3 Wariant scentralizowany 150
8.4 Mocne (S) i słabe (W) strony – zestawienie 152
8.5 Szanse (O) i zagrożenia (T) - zestawienie 153
8.6 Podsumowanie wariantów 153

9 Budowa relacji w dziedzinie cyberbezpieczeństwa z interesariuszami spoza administracji publicznej 157
9.1 Przedsiębiorcy 158
9.1.1 Operatorzy telekomunikacyjni 158
9.1.2 Dostawcy treści, media społecznościowe 159
9.1.3 Dostawcy rozwiązań bezpieczeństwa 160
9.1.4 Przedsiębiorcy będący częścią infrastruktury krytycznej 160
9.1.5 Przedsiębiorcy nie będący częścią infrastruktury krytycznej 161
9.2 Sektor naukowy, akademicki oraz edukacja 161
9.3 Współpraca z organizacjami pozarządowymi oraz izbami branżowymi 163

9.4 Partnerstwo publiczno prywatne a system zachęt do współpracy 163
9.5 System zachęt 164
9.5.1 Przekazywanie informacji na temat zagrożeń i incydentów 165
9.5.2 Dzielenie się informacją przez administrację publiczną 165
9.6 Ćwiczenia 166

10 Szacowanie kosztów 169
10.1 Kategorie kosztów 169
10.2 Szacowanie etatów merytorycznych 171
10.3 Pozostałe kategorie kosztów 173

11 Kluczowe rekomendacje 175

Bibliografia 180

Załącznik: Opracowanie ENISA na temat modeli zarządzania bezpieczeństwem cyberprzestrzeni 187

1 Wprowadzenie

Niniejszy dokument zawiera ekspertyzę dotyczącą rekomendowanego, optymalnego strategicznego modelu organizacji systemu bezpieczeństwa cyberprzestrzeni w Polsce, opracowaną przez NASK na zlecenie Ministerstwa Administracji i Cyfryzacji

Ekspertyza dotyczy zagadnień związanych z kwestiami bezpieczeństwa sieci i systemów komputerowych, przesyłanych, przetwarzanych czy składowanych w nich informacji, bezpieczeństwa usług elektronicznych z wykorzystaniem systemów i sieci komputerowych - wraz z bezpieczeństwem użytkowników korzystających z tych usług. Całą przestrzeń, którą tworzą owe systemy, sieci oraz usługi wraz z relacjami z użytkownikami często określa się mianem cyberprzestrzeni. Precyzyjne zdefiniowanie czym jest cyberprzestrzeń nie jest zadaniem łatwym. Oprócz aspektów technologicznych, prawnych czy organizacyjnych czasem włączane są do pojęcia cyberprzestrzeni także na przykład zagadnienia społeczne – co jednak znajduje się poza zakresem niniejszego opracowania. Przyjęto, iż należy się oprzeć na definicjach cyberprzestrzeni znajdujących się w oficjalnych dokumentach, takich jak: Ustawa o stanie wojennym[3] , Polityka Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej czy Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Mimo nieznacznych różnic w sformułowaniach, we wspomnianych dokumentach pojęcie to jest definiowane praktycznie w ten sam sposób, jako przestrzeń, którą tworzą urządzenia i programy informatyczne komunikując się pomiędzy sobą i z użytkownikami. Chociaż w trakcie rozmaitych konferencji podnoszony jest czasem postulat opracowania bardziej zwartej i precyzyjnej definicji cyberprzestrzeni, autorzy niniejszej ekspertyzy wyrażają pogląd, że o ile samo dążenie do tworzenia coraz lepszych definicji jest godne pochwały, to z drugiej strony nie ma to kluczowego znaczenia dla budowania sprawnego systemu ochrony cyberprzestrzeni. Co do samego obszaru, który powinien podlegać skoordynowanemu systemowi ochrony przyjęto, że powinien on objąć nie tylko sieci i systemy komputerowe, które mają połączenie z sieciami publicznymi, ale wszystkie systemy teleinformatyczne (w stopniu zależnym od funkcji, które pełnią) ze względu na to, że zagrożenia bezpieczeństwa teleinformatycznego mogą propagować się bez konieczności istnienia fizycznego połączenia pomiędzy sieciami czy systemami.

Ekspertyza koncentruje się zatem na zagadnieniach bezpieczeństwa cyberprzestrzeni w wymiarze krajowym, analizując role istniejących obecnie podmiotów a następnie

[3] Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej – Art. 2.1b

proponując wariantowo kształt przyszłego systemu ochrony cyberprzestrzeni Rzeczpospolitej Polskiej. Zakłada się, że sprawność systemu ochrony cyberprzestrzeni jest ściśle uzależniona od prawidłowego zaplanowania, wdrożenia i funkcjonowania warstwy operacyjnej, odpowiedzialnej głównie za zdolność do rozwiązywania wszelkich pojawiających się problemów z bezpieczeństwem w cyberprzestrzeni (zagrożenia, incydenty). W szczególności nowo powstały system powinien umożliwiać skoordynowaną reakcję na sytuacje kryzysowe i na incydenty dużej skali. Powinien też w sposób proaktywny działać w celu podwyższenia poziomu odporności na ataki, wspierać działania uświadamiające i edukacyjne, a także naukowo-badawcze. Aby system mógł właściwie funkcjonować w warstwie operacyjnej potrzebne jest ustanowienie odpowiednich ram prawnych, organizacyjnych i proceduralnych – co zostało określone na potrzeby niniejszej ekspertyzy mianem warstwy strategicznej.

Precyzując dalej zakres niniejszego opracowania, należy zwrócić uwagę, że koncentruje się ono na systemach jawnych – w sferze cywilnej. Systemy niejawne są bowiem objęte oddzielnymi przepisami, i co oczywiste nie mogą i nie powinny być omawiane w tej ekspertyzie. Z kolei systemy teleinformatyczne w sferze militarnej realizują między innymi zadania właściwe dla obronności kraju i ich relacje z kwestiami bezpieczeństwa cyberprzestrzeni mogą zawierać kwestie potencjalnie wrażliwe, które powinny być analizowane w ramach odrębnych działań w ramach administracji rządowej. Nie znaczy to, że zagadnienia cyberbezpieczeństwa w sektorze obronnym czy też cyberobrony powinny być traktowane zupełnie oddzielnie od bezpieczeństwa cyberprzestrzeni w sferze cywilnej. Przeciwnie, są obszary, które powinny być taktowane w sposób spójny. Mówi o tym między innymi unijna strategia bezpieczeństwa cyberprzestrzeni[4] określając jako jeden ze strategicznych priorytetów działania opracowanie polityki obronnej i rozbudowę zdolności w dziedzinie cyberbezpieczeństwa w powiązaniu ze wspólną polityką bezpieczeństwa i obrony UE. Dlatego też, chociaż w ekspertyzie nie używamy terminu "cyberobrona" to nakreślone w niej działania - w sferze cywilnej - zmierzają do zwiększenia postawy obronnej kraju w przypadku działań militarnych w cyberprzestrzeni i relacje z podmiotami sfery militarnej uwzględniane są w powstałych schematach.

Innym z priorytetów wyznaczonych przez dokument strategii europejskiej jest radykalne ograniczenie cyberprzestępczości. Aspekt ten, często pomijany lub niedoceniany w dyskusjach czy opracowaniach dotyczących bezpieczeństwa cyberprzestrzeni jest przez autorów niniejszej ekspertyzy wyraźnie podkreślony poprzez uwzględnienie roli organów ścigania w proponowanym systemie ochrony cyberprzestrzeni.

[4] Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-społecznego i Komitetu Regionów - Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń (Bruksela, 7.2.2013)

Jednak na pierwszym miejscu strategii cyberbezpieczeństwa UE znajduje się kwestia osiągnięcia odporności na zagrożenia cybernetyczne (ang. achieving cyber resillience).

I to przede wszystkim temu celowi podporządkowane są analizy i propozycje zawarte w niniejszym dokumencie ekspertyzy.

Oczywiście można się zastanawiać nad znaczeniem wielu określeń i terminów jakie pojawiają się w literaturze w kontekście bezpieczeństwa cyberprzestrzeni. Na przykład wspomniana wyżej „odporność na zagrożenia cybernetyczne" nie wydaje się najszczęśliwszym tłumaczeniem terminu „cyber resillience". Pominąwszy kwestię, czy stosowanie określeń typu „cybernetyczne" w stosunku do zagrożeń pojawiających się w cyberprzestrzeni jest najbardziej właściwe, można by dyskutować na temat pojemności samego terminu „resillience", który może odnosić się w pewnych sytuacjach do szeroko pojętego bezpieczeństwa, które zawierałoby także np. odporność na awarie sprzętu czy oprogramowania.

Dlatego też, gwoli uściślenia, cyberbezpieczeństwo, w ramach niniejszej ekspertyzy, odnosi się do zabezpieczeń i działań jakie mogą być wykorzystywane do ochrony systemów komputerowych, sieci, aplikacji i użytkowników przed zagrożeniami bezpieczeństwa teleinformatycznego. Jest to także zgodne z przypisami wyjaśniającymi to pojęcie w ramach wspomnianej strategii cyberbezpieczeństwa UE.

2 Kluczowe podmioty związane z funkcjonowaniem obszaru cyberbezpieczeństwa kraju – stan obecny

2.1 Wstęp

Obszar cyberbezpieczeństwa jest obszarem horyzontalnym, przenikającym wszystkie sektory gospodarki kraju, mającym wpływ na funkcjonowanie państwa i społeczeństwa w niemal wszystkich jego wymiarach. W niniejszym rozdziale podjęto próbę naszkicowania mapy podmiotów, głównie państwowych, które pełnią określone role w obszarze bezpieczeństwa cyberprzestrzeni lub są istotne z punktu widzenia zapewnienia odpowiedniego poziomu bezpieczeństwa na poziomie krajowym. Opisywany stan odnosi się do sytuacji aktualnej na przełom sierpnia i września 2015 roku.

Poniżej przedstawiono krótkie charakterystyki podmiotów, o których mowa, jedynie z punktu widzenia problematyki szeroko pojętego bezpieczeństwa informacji, systemów teleinformatycznych oraz ich użytkowników.

2.2 Charakterystyka kluczowych podmiotów

Ministerstwo Administracji i Cyfryzacji (MAC)

Rolę Ministerstwa Administracji i Cyfryzacji bardziej szczegółowo opisano w rozdziale 2.3. Generalnie, zgodnie z obowiązującymi przepisami, ministerstwo odgrywa kluczową rolę w procesach związanych z ochroną cyberprzestrzeni poprzez:

- koordynowanie wdrażania Polityki Ochrony Cyberprzestrzeni RP,
- pełnienie roli organu właściwego ds. łączności, w tym odpowiedzialność za kształt przepisów ustawy z dnia 16 lipca 2004 roku - Prawo telekomunikacyjne oraz nadzorowanie Urzędu Komunikacji Elektronicznej, który to organ odpowiada między innymi za funkcjonowanie regulacji dotyczących bezpieczeństwa sieci i informacji w obrębie Prawa telekomunikacyjnego,
- pełnienie roli organu właściwego ds. informatyzacji, w tym odpowiedzialność za wykonywanie obowiązków wynikających z ustawy z dnia 17 lutego 2005 roku o informatyzacji podmiotów realizujących zadania publiczne[5], związanych z informatyzacją administracji publicznej (w ustawie znajdują się zapisy dotyczące

[5] Dz. U. Nr.64, poz. 565, z późn. zm.

bezpieczeństwa informatycznego. Na podstawie ustawy zostało wydane rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych – w tym sposoby zapewnienia bezpieczeństwa przy wymianie informacji),

- pełnienie kluczowej roli w czasie negocjacji projektu dyrektywy NIS,
- pełnienie wiodącej roli w kwestii rozwoju społeczeństwa informacyjnego.

Agencja Bezpieczeństwa Wewnętrznego (ABW)

Do zadań ABW należy między innymi rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa, a także obronność oraz rozpoznawanie, zapobieganie i wykrywanie przestępstw, m.in. przestępstw godzących w bezpieczeństwo państwa. ABW realizuje zadania służby ochrony państwa oraz krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych. W ramach tej instytucji funkcjonują w szczególności:

- Departament Bezpieczeństwa Teleinformatycznego, w ramach którego funkcjonują m.in.:
  - zespół CERT.GOV.PL – Rządowy Zespół Reagowania na Incydenty Komputerowe,
  - jednostka certyfikacyjna w zakresie ochrony informacji niejawnych oraz laboratoria badawcze
- Centrum antyterrorystyczne (CAT),
- Departament Ochrony Informacji Niejawnych.

ABW prowadzi postępowania sprawdzające w odniesieniu do bezpieczeństwa osobowego oraz postępowania w ramach bezpieczeństwa przemysłowego. Dokonuje także certyfikacji urządzeń i akredytacji systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych o klauzuli „poufne” lub wyższej.

ABW jest również partnerem programu bezpieczeństwa GSP (Government Security Program) jednego z najważniejszych dostawców oprogramowania komputerowego – firmy Microsoft.

Ministerstwo Spraw Wewnętrznych (MSW)

Minister Spraw Wewnętrznych jest ministrem właściwym w dziale sprawy wewnętrzne, który z punktu widzenia niniejszego opracowania dotyczącego bezpieczeństwa cyberprzestrzeni pełni, zgodnie z ustawą z dnia 4 września 1997 roku o działach administracji rządowej, kluczową rolę. Powyższy dział zawiera m.in. obszary:

- ochrony bezpieczeństwa i porządku publicznego,
- zarządzania kryzysowego,
- obrony cywilnej,
- ochrony granicy państwa.

Minister ten sprawuje nadzór nad Policją, Strażą Graniczną, Obroną Cywilną Kraju, Biurem Ochrony Rządu, Krajowym Centrum Informacji Kryminalnej.

Obszar ochrony bezpieczeństwa i porządku publicznego jest obecnie rozumiany głównie jako działania związane ze ściganiem przestępczości. W kontekście zagadnień związanych z cyberprzestrzenią, omawiając rolę MSW, mówić można przede wszystkim o działaniach Policji (nadzorowanej przez MSW) w dziedzinie zwalczania przestępczości w cyberprzestrzeni. [6]

Obszar zarządzania kryzysowego reguluje ustawa z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym. Odpowiedzialna za zarządzanie kryzysowe jest Rada Ministrów, zaś minister spraw wewnętrznych sprawuje zarządzanie kryzysowe w przypadkach niecierpiących zwłoki, a także pełni rolę zastępcy przewodniczącego (wspólnie z ministrem obrony narodowej) Rządowego Zespołu Zarządzania Kryzysowego. W Krajowym Planie zarządzania Kryzysowego MSW pełni wiodącą rolę w fazach przygotowania, reagowania i odbudowy dla zagrożeń o charakterze terrorystycznym. W ramach zaś zagrożeń terrorystycznych, istotna sferą działań jest cyberterroryzm – ten fakt podkreślono w Narodowym Programie Antyterrorystycznym na lata 2015-2019.

MSW prowadzi istotne z punktu widzenia państwa systemy informatyczne i rejestry takie jak: CEP, CEK, PESEL, ewidencja dowodów osobistych, paszportów, Krajowy System Informatyczny (KSI), nadzoruje systemy teleinformatyczne takie jak: Sieć Łączności Rządowej, TESTA, sTESTA, SIS, VIS i inne. Bezpieczeństwo teleinformatyczne tych systemów ma kluczowe znaczenie dla funkcjonowania administracji publicznej.

Policja

Policja, jako umundurowana i uzbrojona formacja przeznaczona do ochrony bezpieczeństwa ludzi oraz do utrzymywania bezpieczeństwa i porządku publicznego, jest służbą podległą MSW.

Jednym z obszarów ścigania przestępstw jest obszar przestępczości w cyberprzestrzeni. Od roku 2014 w Policji zaczęto powoływać specjalne wydziały do walki z cyberprzestępczością. Powstały one zarówno w Komendzie Głównej Policji, Komendzie Stołecznej Policji, jak i w komendach wojewódzkich w całej Polsce.

[6] Patrz „Raport o stanie bezpieczeństwa w Polsce - 2013" Ministerstwa Spraw Wewnętrznych (http://bip.msw.gov.pl/bip/raport-o-stanie-bezpie/18405,Raport-o-stanie-bezpieczenstwa.html)

Na stronie internetowej Biura Służby Kryminalnej Komendy Głównej Policji[7] znaleźć można listę zadań takiej jednostki organizacyjnej. Do zadań Wydziału do Walki z Cyberprzestępczością należy w szczególności:

- inicjowanie i koordynowanie działań Policji w zakresie identyfikowania głównych zagrożeń przestępstwami w sieci Internet, metod i form ich zwalczania oraz współdziałania jednostek Policji z organami i podmiotami pozapolicyjnymi w celu ich skutecznego zwalczania;
- współpraca na szczeblu krajowym i międzynarodowym z instytucjami państwowymi oraz sektorem prywatno – publicznym w zakresie pozyskiwania informacji o metodach i formach przestępstw popełnianych w cyberprzestrzeni, w tym pozyskiwanie i współpraca z Osobowymi Źródłami Informacji;
- opracowywanie rodzaju współpracy z podmiotami sektorów publicznych, prywatnych i akademickich oraz ustalanie kanałów i sposobu gromadzenia i wymiany informacji o przestępstwach oraz zabezpieczenia dowodów cyberprzestępstw;
- opracowanie koncepcji wykorzystania kwalifikowanych środków pracy operacyjnej do ofensywnego rozpoznawania i zwalczania przestępstw związanych z siecią Internet oraz prowadzenie form pracy operacyjnej;
- prowadzenie wieloźródłowych konsultacji technicznych i współpracy z podmiotami krajowymi i zagranicznymi zmierzających do rozpoznawania i implementowania nowoczesnych rozwiązań w walce z przestępczością popełnianą w świecie wirtualnym;
- wdrażanie i utrzymywanie dedykowanych systemów teleinformatycznych realizujących zadania takie jak: monitorowanie sieci Internet pod kątem wykrywania przestępstw, nielegalnych treści, wykrywanie użytkowników korzystających z sieci anonimowych, zapewnienie zdalnego dostępu do dedykowanych systemów komórkom powołanych w ramach komend wojewódzkich (stołecznej) Policji;
- opiniowanie i opracowywanie propozycji zmian legislacyjnych w zakresie bezpieczeństwa teleinformatycznego;
- organizowanie oraz udział w doskonaleniu zawodowym policjantów w zakresie właściwości wydziału;
- prowadzenie czynności operacyjno-rozpoznawczych, w tym form pracy operacyjnej w zakresie właściwości wydziału.

W obszarze Policji funkcjonuje Wyższa Szkoła Policji w Szczytnie (WSPol), która zajmuje się między innymi problematyką przestępczości komputerowej (cyberprzestępczości)

[7] Źródło: http://www.policja.pl/pol/kgp/bsk/struktura/wydzialy/wydzial-do-walki-z-cybe/87086,Wydzial-do-Walki-z-Cyberprzestepczoscia.html

w ramach prowadzonej działalności oświatowej i badawczej. W WSPol planowane jest powołanie Centrum Analityczno-Wywiadowczego i Doskonalenia Zwalczania Cyberprzestępczości.[8]

Policja jest także tymczasowym operatorem infrastruktury informatycznej sieci OST 112, wykorzystywanej m.in. w Systemie Informatycznym Powiadamiania Ratunkowego, a w przyszłości mającej stanowić platformę komunikacyjną na potrzeby podmiotów administracji publicznej.[9]

Ministerstwo Obrony Narodowej (MON)

Kluczowym dokumentem opisującym podejście MON do problematyki bezpieczeństwa w cyberprzestrzeni jest „**Strategia Bezpieczeństwa Narodowego RP**", opublikowana w roku 2014, która jako jeden z celów strategicznych w dziedzinie bezpieczeństwa wymienia „zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni".[10] Na tę strategię powołuje się opublikowana w roku 2015 Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej[11], w której zawarto między innymi definicję pojęcia *cyberbezpieczeństwo RP,* a także odniesienie do obszaru *cyberobrony (ang. cyberdefence).* Doktryna zakłada prowadzenie aktywnej cyberobrony i, w jej ramach, działań ofensywnych w cyberprzestrzeni oraz utrzymanie gotowości do cyberwojny.

MON powołało także w 2008 roku zespół typu CERT, działający na potrzeby resortu obrony.

Decyzją nr 275/MON Ministra Obrony Narodowej z dnia 13 lipca 2015 roku w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej, ustalono m.in., że:

1. **SRnIK - System Reagowania na Incydenty Komputerowe** resortu obrony narodowej (w kontaktach międzynarodowych określany jako MIL-CERT PL), zorganizowany jest w trzypoziomową strukturę, w skład której wchodzą:
    a. Centrum Koordynacyjne SRnIK, którego funkcję pełni właściwa komórka wewnętrzna Służby Kontrwywiadu Wojskowego,
    b. Centrum Wsparcia SRnIK, którego funkcję pełni właściwa komórka wewnętrzna Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych,

[8] http://www.wspol.edu.pl/d/start/1896-w-wspol-powstaje-centrum-analityczno-wywiadowcze-i-doskonalenia-zwalczania-cyberprzestpczoci-
[9] Źródło: OST 112. Ogólnopolska sieć teleinformatyczna na potrzeby obsługi numeru alarmowego 112: http://www.cpi.gov.pl/materialy_do_pobrania,163.html
[10] Źródło: Strategia Bezpieczeństwa Narodowego rzeczypospolitej Polskiej: http://mon.gov.pl/dokumenty/
[11] https://www.bbn.gov.pl/ftp/dok/01/DCB.pdf

c. administratorzy systemów teleinformatycznych w jednostkach i komórkach organizacyjnych.

2. SRnIK organizuje się w celu zapewnienia koordynacji i realizacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach teleinformatycznych oraz autonomicznych stanowiskach komputerowych organizowanych przez jednostki organizacyjne, z wyłączeniem systemów Żandarmerii Wojskowej wykorzystywanych bezpośrednio do prowadzenia działalności dochodzeniowo-śledczej oraz operacyjno-rozpoznawczej.
3. Nadzór nad funkcjonowaniem SRnIK w odniesieniu do systemów teleinformatycznych przeznaczonych do przetwarzania informacji jawnych sprawuje Pełnomocnik Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni.
4. Nadzór nad funkcjonowaniem SRnIK w odniesieniu do systemów teleinformatycznych przeznaczonych do przetwarzania informacji niejawnych sprawuje Szef Służby Kontrwywiadu Wojskowego.

Minister Obrony Narodowej powołał również decyzją nr 38/MON z dnia 16 lutego 2012 roku **Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni**. Obsługę merytoryczną Pełnomocnika zapewnia Centrum Koordynacyjne Systemu Reagowania na Incydenty Komputerowe. Pełnomocnik jest upoważniony do:

1. koordynowania przedsięwzięć przewidzianych dla Ministra Obrony Narodowej w sprawach bezpieczeństwa cyberprzestrzeni, w odniesieniu do wszystkich komórek organizacyjnych Ministerstwa Obrony Narodowej i jednostek organizacyjnych resortu obrony narodowej, z wyłączeniem zadań zastrzeżonych dla pełnomocników do spraw ochrony informacji niejawnych określonych odrębnymi przepisami;
2. inicjowania oraz wspierania działań komórek organizacyjnych Ministerstwa Obrony Narodowej i jednostek organizacyjnych resortu obrony narodowej w obszarze osiągania zdolności do zapewnienia bezpieczeństwa cyberprzestrzeni resortu obrony narodowej;
3. sprawowania nadzoru nad realizacją zadań wynikających z aktów prawnych, polityk i programów rządowych dotyczących zapewnienia bezpieczeństwa cyberprzestrzeni;
4. współpracy ze Służbą Kontrwywiadu Wojskowego w zakresie kreowania spójnego, jednolitego i efektywnego systemu zarządzania bezpieczeństwem cyberprzestrzeni resortu obrony narodowej;
5. ustanowienia, z zachowaniem warunków bezpieczeństwa informacji oraz kompetencji komórek organizacyjnych Ministerstwa Obrony Narodowej i jednostek organizacyjnych resortu obrony narodowej, spójnego, współdzielonego systemu informacyjnego o bieżącym stanie oraz zagrożeniach cyberprzestrzeni;

6. reprezentowania resortu obrony narodowej w pracach kierowniczych gremiów Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej w zakresie bezpieczeństwa cyberprzestrzeni.

MON powołało[12] także jednostkę podległą, zwaną **Narodowym Centrum Kryptologii** (NCK), zajmującą się w szczególności badaniami i wdrażaniem rozwiązań kryptograficznych na potrzeby administracji publicznej i wojska.

Ministerstwo Gospodarki (MG)

W ramach omawiania ról pełnionych przez poszczególne organy państwowe i instytucje, nie można pominąć istotnej roli Ministerstwa Gospodarki, które pełni rolę instytucji nadzorującej wdrażanie **rozporządzenia eIDAS**[13]. Główne cele rozporządzenia to:

- zapewnienie wzajemnego uznawania i transgranicznej akceptacji elektronicznej identyfikacji (eID) przez kraje członkowskie UE,
- ujednolicenie ram prawnych świadczenia usług zaufania (związanych z wykorzystaniem podpisu elektronicznego) oraz nadzoru nad dostawcami usług w UE,
- zapewnienie uznawania usług zaufania związanych z transakcjami elektronicznymi oraz uwierzytelnianiem witryn internetowych.

Rozporządzenie przewiduje m.in. obowiązek wdrożenia przez dostawców usług zaufania odpowiednich środków technicznych i organizacyjnych dla zapewnienia bezpieczeństwa oraz obowiązek raportowania incydentów związanych z naruszeniami bezpieczeństwa.

Rządowe Centrum Bezpieczeństwa (RCB)

Rządowe Centrum Bezpieczeństwa pełni ważną rolę w obszarze zarządzania kryzysowego i ochrony infrastruktury krytycznej. Podstawą prawną dla tych działań jest ustawa o zarządzaniu kryzysowym[14]. Infrastruktura sieci teleinformatycznych i łączności jest na liście sektorów, które są zdefiniowane jako krytyczne dla funkcjonowania państwa. RCB jest odpowiedzialne za przygotowanie Narodowego Programu Ochrony Infrastruktury Krytycznej, we współpracy z ministerstwami i innymi organami odpowiedzialnymi za sprawy bezpieczeństwa narodowego oraz organami odpowiedzialnymi za poszczególne sektory uznawane za krytyczne.

Generalny Inspektor Ochrony Danych Osobowych (GIODO)

[12] ZARZĄDZENIE Nr 10/MON MINISTRA OBRONY NARODOWEJ z dnia 29 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej – Narodowe Centrum Kryptologii.
[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym
[14] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym

GIODO, pełniąc rolę organu dbającego o ochronę danych osobowych w kraju oraz harmonizację przepisów krajowych w tym obszarze z dyrektywami i regulacjami Unii Europejskiej, w szczególny sposób odgrywa także rolę w kwestii danych osobowych przetwarzanych przez przedsiębiorców telekomunikacyjnych. W ustawie Prawo telekomunikacyjne, oprócz przepisów związanych z bezpieczeństwem lub integralnością sieci lub usług, zostały wprowadzone przepisy dotyczące bezpieczeństwa danych osobowych. Mówią o tym art. 174 a-d ustawy. W szczególności w przepisach jest mowa o obowiązku zgłaszania do GIODO naruszeń danych osobowych przetwarzanych przez przedsiębiorcę telekomunikacyjnego w związku ze świadczeniem publicznie dostępnych usług telekomunikacyjnych.

Urząd Komunikacji Elektronicznej (UKE)

UKE, pełniąc rolę regulatora rynku telekomunikacyjnego i pocztowego, w kontekście bezpieczeństwa w cyberprzestrzeni zapewnia implementację Prawa telekomunikacyjnego, w szczególności w odniesieniu do zapisów sformułowanych w Dziale VIIa Bezpieczeństwo i integralność sieci i usług telekomunikacyjnych. Szczegółowe kwestie z tym związane zostały omówione w rozdziale 3.1.3

Ministerstwo Sprawiedliwości (MS)

Ministerstwo Sprawiedliwości odpowiada za dział administracji rządowej – sprawiedliwość. Minister właściwy do spraw sprawiedliwości zapewnia m.in. przygotowywanie projektów kodyfikacji prawa cywilnego i karnego. W obszarze nowoczesnych technologii, w tym w szczególności dotyczących bezpieczeństwa w cyberprzestrzeni oraz ścigania cyberprzestępstw, nadążanie prawa za rzeczywistością jest istotnym problemem cywilizacyjnym. Tak więc rola organu kreującego prawo w tym zakresie i nadzorującego jego prawidłowe wykonywanie jest zasadnicza dla zapewnienia właściwego porządku w przestrzeni wirtualnej.

Ministerstwo Spraw Zagranicznych (MSZ)

Ministerstwo Spraw Zagranicznych, z racji pełnionych zadań i rozproszonej infrastruktury placówek na całym świecie (co wiąże się z utrzymywaniem rozległej infrastruktury teleinformatycznej), jest ważnym elementem na mapie podmiotów, którym zależy na jak największym bezpieczeństwie w cyberprzestrzeni. Na świecie podmioty tego typu są częstym celem kampanii cyberszpiegowskich. Polska nie jest w tym aspekcie

wyjątkiem[15], stąd konieczność traktowania MSZ jako istotnego elementu w systemie krajowego cyberbezpieczeństwa. Ministerstwo posiada zaawansowane rozwiązania techniczno-organizacyjne w dziedzinie zapewnienia odpowiedniego poziomu bezpieczeństwa teleinformatycznego.

Ministerstwo Finansów (MF)

Ministerstwo Finansów, odpowiadając za dział administracji – finanse publiczne, w decydującej mierze wpływa na ostateczny kształt możliwości budżetowych w odniesieniu do bezpieczeństwa cyberprzestrzeni.

Wśród służb podległych MF znajdują się m.in.: Generalny Inspektor Informacji Finansowej, urzędy i izby skarbowe, urzędy kontroli skarbowej, w tym Wywiad Skarbowy oraz Służba Celna.

MF i podległe służby posługują się systemami teleinformatycznymi, które są kluczowe z punktu widzenia systemu finansowego państwa (np. system e-Deklaracje). Ataki na te systemy mogą powodować największe konsekwencje dla funkcjonowania państwa oraz wielkie straty finansowe, również dla obywateli.

Komisja Nadzoru Finansowego (KNF)

Komisja Nadzoru Finansowego sprawuje nadzór nad sektorem bankowym, rynkiem kapitałowym, ubezpieczeniowym, emerytalnym, nadzór nad instytucjami płatniczymi i biurami usług płatniczych, instytucjami pieniądza elektronicznego oraz nad sektorem kas spółdzielczych. Są to sektory, które są ściśle uzależnione od systemów teleinformatycznych w kraju, a wszelkie incydenty naruszające bezpieczeństwo mogą mieć duży, negatywny wpływ na funkcjonowanie gospodarki i powodować straty finansowe w dużej skali. Nadzór nad działalnością KNF sprawuje Prezes RM.

Na podstawie ustawy z dnia 29 sierpnia 1997 roku Prawo bankowe, KNF wydała w styczniu 2013 roku Rekomendację D, dotyczącą zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (Rekomendacja D).

Rekomendacja D wskazuje bankom oczekiwania ze strony nadzorcy co do właściwego (ostrożnego i stabilnego) zarządzania obszarami technologii informacyjnej i bezpieczeństwa teleinformatycznego.

Rekomendacja D dla sektora bankowego oraz "Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatyczego w zakładach ubezpieczeń i zakładach reasekuracji", wydane przez KNF w grudniu 2014 roku,

[15] Por: https://niebezpiecznik.pl/post/kancelaria-premiera-msz-mon-i-kancelaria-prezydenta-zhackowane-wiemy-kto-stoi-za-tymi-wlamaniami/

są dobrymi przykładami tworzenia sektorowych ram regulacyjnych w obszarze bezpieczeństwa teleinformatycznego.

Ministerstwo Infrastruktury i Rozwoju (MIR)

Ministerstwo Infrastruktury i Rozwoju zarządza systemem wdrażania funduszy europejskich oraz infrastrukturą transportową (drogi, kolej, ruch lotniczy i żegluga).

W pierwszej grupie zadań, dotyczącej funduszy europejskich MIR zarządza m.in. programem Polska Cyfrowa, na który przeznaczono w latach 2014-2020 2,2 mld euro. Ma on na celu zwiększenie dostępności do Internetu, stworzenie przyjaznej dla obywatela e-administracji oraz upowszechnienie w społeczeństwie wiedzy i umiejętności korzystania z komputerów. Jest niezwykle istotne, aby projekty realizowane w ramach tego programu opierały się na spójnej, skoordynowanej koncepcji zapewnienia bezpieczeństwa teleinformatycznego.

Druga grupa zadań, czyli zarządzanie infrastrukturą transportową, z punktu widzenia ochrony infrastruktury krytycznej, w kontekście coraz powszechniejszego wykorzystania technologii cyfrowych, między innymi do zarządzania i sterowania – dotyczy grupy kluczowych sektorów w rozumieniu procesu kształtowania krajowego systemu ochrony cyberprzestrzeni.

Prezydent RP

W dziedzinie bezpieczeństwa w cyberprzestrzeni Prezydent RP ma do dyspozycji mocne narzędzia w sytuacjach nadzwyczajnych. Może on, na podstawie ustawy z dnia 29 sierpnia 2002 roku o stanie wojennym, wprowadzić, na wniosek Rady Ministrów, stan wojenny z powodu wystąpienia zewnętrznego zagrożenia państwa – w tym zagrożenia w cyberprzestrzeni. Ponadto, w sytuacji szczególnego zagrożenia konstytucyjnego ustroju państwa, bezpieczeństwa obywateli lub porządku publicznego, w tym spowodowanego działaniami o charakterze terrorystycznym lub działaniami w cyberprzestrzeni, które nie może być usunięte poprzez użycie zwykłych środków konstytucyjnych, Rada Ministrów może podjąć uchwałę o skierowaniu do Prezydenta Rzeczypospolitej Polskiej wniosku o wprowadzenie stanu wyjątkowego (ustawa z dnia 21 czerwca 2002 roku o stanie wyjątkowym).

Prezydent RP ma do dyspozycji w kwestiach dotyczących bezpieczeństwa narodowego organ doradczy w postaci Biura Bezpieczeństwa Narodowego.

Biuro Bezpieczeństwa Narodowego (BBN)

BBN jest organem doradczym Prezydenta RP. W ramach tematyki bezpieczeństwa narodowego instytucja ta zajmuje się też kwestiami bezpieczeństwa w cyberprzestrzeni.

W tym kontekście warto wspomnieć, że BBN przygotowało *Doktrynę Cyberbezpieczeństwa Rzeczypospolitej Polskiej,* która została przyjęta przez Prezydenta RP w roku 2015. Dokument ten jest elementem strategii bezpieczeństwa narodowego RP w odniesieniu do bezpieczeństwa cyberprzestrzeni. Niestety, w zbyt małym stopniu zadbano o skoordynowanie dokumentu doktryny oraz dokumentu Polityki Ochrony Cyberprzestrzeni RP, opracowanego przez administrację rządową, a jest to konieczne, gdyż oba dokumenty odnoszą się do bezpieczeństwa w istocie tej samej cyberprzestrzeni.

Istotnym aspektem doktryny jest zdefiniowanie podejścia do aspektu cyberobrony (cyberdefence), w szczególności możliwość wykonywania aktywnej obrony i działań ofensywnych w cyberprzestrzeni.

Narodowe Centrum Kryptologii (NCK)

Ministerstwo Obrony Narodowej powołało[16] jednostkę budżetową podległą bezpośrednio MON, zwaną **Narodowym Centrum Kryptologii** (NCK).

Do zadań centrum, zgodnie ze statutem Narodowego Centrum Kryptologii nadanym przywołanym wyżej zarządzeniem w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej – Narodowe Centrum Kryptologii, należy konsolidacja kompetencji i zasobów resortu obrony narodowej w obszarze kryptologii. W ramach swoich kompetencji realizuje zadania związane m.in. z prowadzeniem badań, projektowaniem, budową, wdrażaniem, użytkowaniem, dystrybucją oraz ochroną narodowych technologii kryptologicznych, wytwarzaniem nowych produktów dla państwa przez zespolenie potencjału naukowego i przemysłowego w obszarze zaawansowanych technologii informatycznych i kryptograficznych, jak również identyfikowaniem potrzeb w tym względzie resortu obrony narodowej i innych organów administracji publicznej. NCK realizuje także zadania związane z pełnieniem funkcji gestora sprzętu wojskowego stanowiącego urządzenia i narzędzia kryptograficzne oraz przygotowuje i przeprowadza postępowania o zamówienie publiczne w projektach naukowo badawczych w obszarze związanym z kryptologią i cyberobroną, we współpracy z jednostkami inicjującymi, oraz zawiera umowy w tym zakresie.

Naukowa i Akademicka Sieć Komputerowa (NASK)

Naukowa i Akademicka Sieć Komputerowa jest instytutem badawczym, którego organem nadzorującym jest Ministerstwo Nauki i Szkolnictwa Wyższego. NASK prowadzi szereg działań związanych z problematyką bezpieczeństwa w cyberprzestrzeni. Wśród najważniejszych można wymienić:

[16] ZARZĄDZENIE Nr 10/MON MINISTRA OBRONY NARODOWEJ z dnia 29 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej – Narodowe Centrum Kryptologii.

- powołanie w roku 1997 pierwszego w kraju zespołu typu CERT, funkcjonującego do chwili obecnej (CERT Polska), który pełni *de facto* rolę CSIRTu krajowego (i jako taki figuruje w dokumentach ENISA), a wśród realizowanych zadań ma:
  - reagowanie na zagrożenia i incydenty w polskiej przestrzeni internetowej (.pl),
  - publikowanie informacji o zagrożeniach oraz raportów rocznych[17],
  - tworzenie narzędzi i systemów informatycznych zwiększających potencjał cyberbezpieczeństwa w kraju: systemu wczesnego ostrzegania ARAKIS, platformy zbierania, zarządzania i wymiany informacji n6, systemu wymiany informacji NISHA i wielu innych,
  - udział w międzynarodowych forach współpracy zespołów CERT/CSIRT (FIRST, TF CSIRT),
  - stymulowanie i uczestnictwo w krajowych forach wymiany informacji (ABUSE Forum),
  - prowadzenie szkoleń specjalistycznych i organizacja konferencji (cykl SECURE),
  - od 2006 r. reprezentowanie Polski na spotkaniach CSIRTów z krajową odpowiedzialnością organizowanych corocznie przez CERT/CC[18],
  - przygotowywanie wkładów do międzynarodowych raportów podsumowujących incydenty komputerowe, m.in. jako jedyny polski CSIRT do raportu Verizon Data Breach Investigation Report[19],
- powołanie w roku 2005 zespołu zwalczającego niebezpieczne i nielegalne treści w Internecie (w tym CSAM)[20] – Dyżurnet.pl, działającego w sieci INHOPE,
- działalność badawczą w dziedzinie ochrony cyberprzestrzeni, prowadzona wspólnie przez zespół CERT Polska oraz Pracownię Metod Bezpieczeństwa Sieci i Informacji Pionu Naukowego NASK, a także przez Pracownię Biometrii,
- ścisłą współpracę z Agencją Unii Europejskiej ds. Bezpieczeństwa i Informacji - ENISA (zaangażowanie w ciałach zarządczych agencji, praca w grupach roboczych, opracowywanie ekspertyz i poradników na zlecenie ENISA).

Narodowe Centrum Badań i Rozwoju (NCBiR)

NCBiR jest agencją wykonawczą Ministra Nauki i Szkolnictwa Wyższego. Powołane zostało w 2007 roku jako jednostka realizująca zadania z zakresu polityki naukowej, naukowo-technicznej i innowacyjnej państwa. Wśród wielu programów i projektów, jakie są

[17] http://www.cert.pl/raporty
[18] https://www.cert.org/incident-management/national-csirts/meeting/
[19] http://www.verizonenterprise.com/DBIR/2015/
[20] ang. *Child Sexual Abuse Material*

realizowane przy dofinansowaniu NCBiR, znajduje się także obszar poświęcony obronności i bezpieczeństwu państwa.

Badania na rzecz bezpieczeństwa i obronności Narodowe Centrum Badań i Rozwoju prowadzi w porozumieniu z ministrem obrony narodowej i ministrem spraw wewnętrznych.

Na stronach NCBiR[21] czytamy , iż: „W konkursach na konkretnie sprecyzowane tematy badawcze finansowane są przedsięwzięcia, które w największym stopniu rokują rzeczywiste zwiększenie bezpieczeństwa narodowego. Celem realizowanych programów i projektów jest nie tylko zwiększenie potencjału polskich podmiotów naukowych i przemysłowych, ale także dążenie do niezależności technologicznej poprzez tworzenie polskiego „know- how" w zakresie krytycznych technologii w zakresie bezpieczeństwa i obronności państwa."

Wśród technologii będących przedmiotem dofinansowywanych projektów znajdują się również technologie informatyczne.

Agencja Wywiadu (AW)

Agencja Wywiadu jest urzędem administracji rządowej, jednak jej działalność nie jest objęta zakresem działów administracji rządowej. Agencją kieruje szef Agencji Wywiadu, a bezpośredni nadzór sprawuje Prezes Rady Ministrów. Do zadań Agencji Wywiadu należy m.in.:

- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego;
- rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczypospolitej Polskiej;
- zapewnienie ochrony kryptograficznej łączności z polskimi placówkami dyplomatycznymi i konsularnymi oraz poczty kurierskiej;
- rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej;
- prowadzenie wywiadu elektronicznego.

Nie można tracić z pola widzenia okoliczności, że we współczesnym świecie działalność służb wywiadowczych państw obcych jest również nakierowana na technologie informatyczne i działania w cyberprzestrzeni.

Służba Kontrwywiadu Wojskowego (SKW)

[21] http://www.ncbir.pl/programy-i-projekty---obronnosc-bezpieczenstwo

SKW realizuje zadania wynikające z ustawy z dnia 05 sierpnia 2010 roku o ochronie informacji niejawnych w odniesieniu do MON i jednostek podległych oraz ataszatów obrony w placówkach zagranicznych – w zakresie bezpieczeństwa osobowego oraz bezpieczeństwa przemysłowego. SKW dokonuje także certyfikacji środków ochrony elektromagnetycznej (w trybie art. 50 ust. 1 ustawy), certyfikacji urządzeń i narzędzi kryptograficznych (w trybie art. 50 ust. 2 ustawy), certyfikacji urządzeń i narzędzi służących do realizacji zabezpieczenia teleinformatycznego (w trybie art. 50 ust. 3 ustawy), szkoleń specjalistycznych dla administratorów systemów teleinformatycznych i inspektorów bezpieczeństwa teleinformatycznego (w trybie art. 52 ust. 4 ustawy).

Służba Wywiadu Wojskowego (SWW)

SWW jest służbą specjalną, właściwą w sprawach ochrony przed zagrożeniami zewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej. Służba ta uczestniczy w wymianie informacji i doświadczeń pomiędzy służbami wywiadowczymi państw NATO i UE.

Nie można tracić z pola widzenia okoliczności, że we współczesnym świecie działalność służb wywiadowczych państw obcych jest również nakierowana na technologie informatyczne i działania w cyberprzestrzeni.

Centralne Biuro Antykorupcyjne (CBA)

Centralne Biuro Antykorupcyjne utworzono jako służbę specjalną do spraw zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także do zwalczania działalności godzącej w interesy ekonomiczne państwa.

Mając na uwadze, że podstawowym zadaniem CBA jest rozpoznawanie, zapobieganie i wykrywanie przestępstw oraz ściganie ich sprawców, i przy uwzględnieniu, że sprawcy przestępstw, również popełnianych w celu uzyskania korzyści majątkowej kosztem Skarbu Państwa lub państwowych czy samorządowych osób prawnych, coraz częściej korzystają z nowoczesnych technologii, należy rozważyć zaangażowane CBA w system ochrony cyberprzestrzeni RP.

Narodowy Bank Polski (NBP)

Narodowy Bank Polski jest odpowiedzialny za stabilność i bezpieczeństwo całego systemu bankowego. Nadzoruje także systemy płatności w Polsce. NBP prowadzi także Narodowe Centrum Certyfikacji, pełniące funkcję głównego urzędu certyfikacji w ramach infrastruktury bezpiecznego podpisu elektronicznego w Polsce. Bank prowadzi szereg

kluczowych systemów dla funkcjonowania obszaru bankowości (np. system TARGET2-NBP), których bezpieczeństwo jest wprost zależne od bezpieczeństwa teleinformatycznego NBP oraz bezpieczeństwa całej cyberprzestrzeni RP.

Krajowa Izba Rozliczeniowa (KIR)

KIR jest instytucją pośredniczącą w rozliczeniach między bankami. Instytucja ta odpowiada za prawidłowość rozliczeń niemal wszystkich przelewów międzybankowych wykonywanych w Polsce. Prowadzi kluczowy z punktu widzenia funkcjonowania operacji międzybankowych system elektronicznych rozliczeń międzybankowych ELIXIR.

2.3 Role instytucjonalne w podziale na obszary i działy

Dla pogłębienia charakterystyki obecnego podziału instytucjonalnego w kontekście jego wykorzystania dla określenia przyszłego kształtu bezpieczeństwa cyberprzestrzeni RP, w niniejszym rozdziale przedstawiono bardziej szczegółowe analizy na ten temat.

Obszary dedykowane MAC

W ramach Ministerstwa Administracji i Cyfryzacji skupia się zarządzanie kilkoma działami, które są istotne w kontekście zagadnień ochrony cyberprzestrzeni. Minister właściwy ds. administracji i cyfryzacji odpowiada, wraz z odpowiednimi podsekretarzami stanu, za takie obszary jak: telekomunikacja, informatyzacja czy społeczeństwo informacyjne. Także odpowiedzialność za dział administracja jest istotna, w kontekście omawianego obszaru cyberbezpieczeństwa.

Taka sytuacja stanowi z jednej strony duże wyzwanie dla ministerstwa, ale jest jednocześnie szansą na skoordynowane działanie w odniesieniu do problematyki bezpieczeństwa cyberprzestrzeni i pozwala na kompleksowe podejście do zagadnienia, co jest niezwykle ważne w przypadku obszaru, który staje się obszarem horyzontalnym poprzez powszechne zastosowanie nowoczesnych technologii informacyjnych w państwie i społeczeństwie.

Poniżej przedstawiono krótką charakterystykę tematyki bezpieczeństwa sieci i informacji w kontekście wymienionych wyżej działów.

Telekomunikacja

Dział łączności jest w Polsce uregulowany poprzez Prawo Telekomunikacyjne, która, szczególnie w wyniku nowelizacji z roku 2013 (uchwalona pod koniec 2012 r.), spowodowała, w wyniku harmonizacji z dyrektywami europejskimi z roku 2009 (tzw. pakiet telekomunikacyjny), wprowadzenie nowego działu: DZIAŁ VIIa Bezpieczeństwo i integralność

sieci i usług telekomunikacyjnych. Szersze omówienie tego aspektu zostało przedstawione w rozdziale 3.1.3.

W najogólniejszym podsumowaniu zmiany te dotyczyły, z jednej strony, przyjęcia i egzekwowania pewnych minimalnych środków bezpieczeństwa, które powinny być zaimplementowane u podmiotów działających na rynku telekomunikacyjnym oraz narzucenia obowiązku informowania (zgłaszania) istotnych przypadków naruszenia bezpieczeństwa lub integralności sieci i usług. Dodatkowo, istotnym elementem jest informowanie użytkowników sieci i usług o zagrożeniach bezpieczeństwa teleinformatycznego, międzynarodowa wymiana w ramach UE informacji o istotnych przypadkach zagrożeń i incydentów naruszających bezpieczeństwo lub integralność oraz tworzenie przez organ regulacyjny raportów zbiorczych o zagrożeniach i incydentach w celu między innymi przekazywania ich do Komisji Europejskiej oraz Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA).

Takie podejście, związane z ustanawianiem minimalnych środków bezpieczeństwa i zgłaszaniem incydentów, jest, można powiedzieć, ogólnym trendem – pewnym minimum, jeśli chodzi o dyrektywy i regulacje w UE w różnych sektorach gospodarki. Sektor telekomunikacji jest w istocie pierwszym sektorem, w którym wprowadzono tego typu mechanizmy i ten kierunek należy uznać za istotny krok w procesie ustanawiania reguł bezpieczeństwa teleinformatycznego na poziomie krajów członkowskich i całej UE. Równolegle, obowiązek zgłaszania incydentów wprowadzono także (w tej samej ustawie) w odniesieniu do obszaru ochrony danych osobowych (w tym przypadku - zgłoszenie do GIODO). Mechanizmy minimalnych wymagań bezpieczeństwa i zgłaszania incydentów zostały następnie wprowadzone w uregulowaniach UE, w tzw. rozporządzeniu e-IDAS[22]; jednocześnie, co godne podkreślenia, planowana Dyrektywa NIS także zawiera zapisy na temat wprowadzania w innych sektorach podobnych mechanizmów.

Wobec powyższego można uznać, że sektor telekomunikacji stanowi swoistą forpocztę w dziedzinie podnoszenia poziomu cyberbezpieczeństwa i tworzyć może dobre pole do rozwoju i monitorowania praktycznych efektów wprowadzanych regulacji i zaleceń w obszarze bezpieczeństwa ICT (*information and communication technologies*) na poziomie krajowym, a także w relacjach międzynarodowych.

Informatyzacja

W dziale informatyzacja MAC zajmuje się bardzo wieloma obszarami, których sprawne funkcjonowanie ściśle zależy od odpowiedniego ukierunkowania i skoordynowania działań

[22] e-IDAS: ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE

na rzecz procesu podnoszenia bezpieczeństwa teleinformatycznego. Można tu wspomnieć m.in. takie ważne obszary, jak:

- prowadzenie działań wynikających z ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne związanych z informatyzacją administracji publicznej,
- rekomendowanie strategicznych zadań państwa, standardów i wytycznych w zakresie informatyzacji administracji publicznej,
- współpraca międzynarodowa w zakresie informatyzacji administracji publicznej,
- Program Zintegrowanej Informatyzacji Państwa,
- realizacja zadań związanych z wdrażaniem rozwiązań informatycznych w zakresie chmury obliczeniowej w administracji publicznej,
- rozwój elektronicznej administracji,
- przygotowywanie rekomendacji dotyczących minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej z podmiotami publicznymi.

Rozpatrując kwestie bezpieczeństwa teleinformatycznego w kontekście ustanowionych przepisów, należy zwrócić uwagę, iż na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne zostało wydane rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.

Między innymi rozporządzenie to określa minimalne wymagania systemów teleinformatycznych, w tym sposoby zapewnienia bezpieczeństwa przy wymianie informacji. W szczególności rozporządzenie przewiduje, że podmioty realizujące zadania publiczne są zobowiązane do opracowania i wdrożenia (a także utrzymania, monitorowania i rozwijania) systemu zarządzania bezpieczeństwem informacji. Aspekt zarządzania bezpieczeństwem informacji jest rozwinięty szczegółowo i między innymi przewidziane są takie działania jak przeprowadzanie okresowych analiz ryzyka i podejmowanie działań minimalizujących to ryzyko, stosownie do wyników tychże analiz. Zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych jest w rozporządzeniu opisane z wymienieniem podstawowych koniecznych działań takich jak min.: aktualizacja oprogramowania, stosowanie mechanizmów kryptograficznych, zarządzanie podatnościami, dbanie o zgodność ze standardami i polityką bezpieczeństwa, reagowanie na incydenty czy przeprowadzanie okresowych (nie rzadziej niż raz na rok) audytów. Co istotne rozporządzenie wskazuje na zestaw norm, które należy stosować dla spełnienia wymagań określonych w przepisach, w postaci PN-ISO/IEC 27001 w odniesieniu do systemu zarządzania bezpieczeństwem informacji, PN-ISO/IEC 17799 w odniesieniu do ustanawiania zabezpieczeń, PN-ISO/IEC 27005 w odniesieniu do zarządzania ryzykiem, czy PN-ISO/IEC

24762 w zakresie zarządzania ciągłością działania. Te zalecenia są traktowane jako minimalne, także w uzasadnionych sytuacjach podmioty realizujące zadania publiczne są zobowiązane stosować dodatkowe zabezpieczenia.

Ustanowione przepisy tworzą właściwe ramy dla działań w kierunku zapewnienia właściwego poziomu bezpieczeństwa w systemach teleinformatycznych w sektorze administracji publicznej.

Społeczeństwo informacyjne

Obszarem ściśle związanym z informatyzacją jest rozwój społeczeństwa informacyjnego, który jest kolejnym obszarem działalności MAC, w którym kwestie bezpieczeństwa cyberprzestrzeni odegrają w najbliższej przyszłości kluczową rolę ze względu na rosnące tempo zagrożeń cyberbezpieczeństwa oraz trwające działania legislacyjne chociażby trwające w UE, jak planowana dyrektywa NIS.

W ramach tychże zadań MAC aktywnie zajmuje się m.in. wdrażaniem Polityki Ochrony Cyberprzestrzeni RP, przyjętej w roku 2013. Chociaż polityka jest dokumentem obowiązującym jedynie podmioty administracji rządowej, jest też rekomendowana i zalecana dla innych interesariuszy komunikacji elektronicznej w cyberprzestrzeni. Polityka stanowi ważny krok na drodze budowania strategicznego podejścia do ochrony cyberprzestrzeni kraju. Obecnie w Unii Europejskiej praktycznie wszystkie kraje przyjęły tzw. narodowe strategie bezpieczeństwa cyberprzestrzeni (NCSS – National Cyber Security Strategy)[23], które opisują skoordynowane podejście do tego obszaru nie tylko w obrębie systemów administracji państwa, ale wszystkich interesariuszy, w szczególności podmiotów odpowiedzialnych za infrastrukturę krytyczną, przedsiębiorców czy użytkowników sieci. Działania krajowe w UE powinny być jednocześnie skoordynowane z europejską strategią cyberbezpieczeństwa (European Cyber Security Strategy[24]), przyjętą w roku 2013.

Administracja

W kontekście np. implementacji Polityki ochrony cyberprzestrzeni RP, fakt, że minister właściwy ds. administracji i cyfryzacji jest odpowiedzialny za administrację publiczną, w tym organizację urzędów administracji publicznej oraz procedur administracyjnych, wprowadzanie reform i nadzorowanie organizacji struktur administracji publicznej, a także zespolonej administracji rządowej w województwach, również stwarza możliwości skoordynowanego działania na polu bezpieczeństwa cyberprzestrzeni w odniesieniu do całej administracji.

[23] patrz zestawienie w postaci mapy na stronie ENISA: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world
[24] http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

Inne podmioty państwowe na mapie cyberbezpieczeństwa

Nie ulega wątpliwości, iż oprócz wymienionych wyżej podmiotów odgrywających zasadniczą rolę w ochronie bezpieczeństwa cyfrowego RP, niezbędne jest uwzględnienie innych instytucji i obszarów aktywności państwa.

Jednym z ważniejszych elementów profilaktyki i reagowania na zagrożenia i incydenty jest posiadanie w kraju sprawnej struktury zespołów reagowania na zagrożenia i incydenty, zwane zespołami CSIRT (Computer Security Incident Response Team) lub CERT (Computer Emergency Response Team)[25]. Obecnie w naszym kraju funkcjonuje rządowy zespół reagowania na incydenty komputerowe CERT.GOV.PL, powołany w roku 2007 w ramach Agencji Bezpieczeństwa Wewnętrznego (Departament Bezpieczeństwa Teleinformatycznego). ABW także uczestniczyła w kreowaniu, wspólnie z MAC, Polityki Ochrony Cyberprzestrzeni RP. Sieć CERTów w naszym kraju jest dość rozbudowana, ponieważ oprócz CERT.GOV.PL, od roku 1996 w ramach Instytutu Badawczego NASK działa zespół CERT Polska, zaś resort obrony powołał do działania w 2008 roku zespół MIL-CERT. W środowisku akademickim działa PIONIER-CERT. Również wiele podmiotów komercyjnych – szczególnie operatorzy telekomunikacyjni oraz banki – powołało zespoły reagujące (nazwane formalnie CERT lub CSIRT) bądź zespoły bezpieczeństwa, w których realizowana jest profesjonalnie rola reagowania na incydenty.

Innym kluczowym elementem na mapie cyberbezpieczeństwa jest ochrona infrastruktury krytycznej, gdzie aspekt bezpieczeństwa teleinformatycznego jest niezwykle istotny. Obecnie za zagadnienia związane z infrastrukturą krytyczną odpowiada Rządowe Centrum Bezpieczeństwa, które opracowało w roku 2013 Narodowy Program Ochrony Infrastruktury Krytycznej, w którym to programie sieci teleinformatyczne traktowane są dziedzinowo jako element infrastruktury krytycznej.

Kolejnym dużym obszarem powiązanym z cyberbezpieczeństwem jest kwestia wykrywania oraz ścigania cyberprzestępstw. Tu z kolei organem właściwym jest Ministerstwo Spraw Wewnętrznych wraz Policją.

Nie mniej ważnym obszarem jest także obszar zadań tzw. *cyberdefence*, czyli obrony w cyberprzestrzeni. Może być on różnie definiowany w różnych krajach, ale domyślnie przynależy organom odpowiedzialnym za obronność państwa, w przypadku naszego kraju jest to Ministerstwo Obrony Narodowej oraz Prezydent RP. Właśnie Biuro Bezpieczeństwa Narodowego przy Prezydencie opublikowało w roku 2015 Doktrynę Cyberbezpieczeństwa RP, w której zawarto - między innymi – aspekty związane z obroną w cyberprzestrzeni.

[25] Formalnie nazwa CERT jest zastrzeżoną marką przez Carnegie Mellon University, choć za zgodą właściciela - szeroko używanym skrótem przez zespoły reagujące na całym świecie.

Oprócz powyższych elementów związanych z bezpieczeństwem w cyberprzestrzeni należy wskazać na zakresy działania również innych organów czy urzędów, które są przedmiotowo związane z omawianą tematyką.

Przykładowo, Ministerstwo Gospodarki jest odpowiedzialne za wdrożenie postanowień rozporządzenia Parlamentu Europejskiego i Rady Unii Europejskiej nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.[26] W rozporządzeniu tym znajdują się między innymi podobne postanowienia, jak obowiązek zgłaszania przypadków naruszenia bezpieczeństwa, w odniesieniu do podmiotów rynku telekomunikacyjnego wprowadzony przez Prawo Telekomunikacyjne. Naturalna więc wydaje się harmonizacja w tym obszarze, ponieważ co do zasady reguły, procedury i wymagania mogą być bardzo podobne – z uwzględnieniem różnic wynikających ze specyfiki danego sektora.[27]

Także sektor bankowy nadzorowany przez Komisję Nadzoru Finansowego ma swoje rozbudowane zasady bezpieczeństwa teleinformatycznego (Rekomendacja D).

W przyszłości należy planować rozszerzanie się roli regulatora danego sektora rynku na obszary związane z bezpieczeństwem teleinformatycznym. Jednym z przykładów może być regulator rynku energetycznego (w przypadku naszego kraju – Urząd Regulacji Energetyki), który jest traktowany jako jeden z bardziej krytycznych, jeśli chodzi o bezpieczeństwo. Rozwój technologiczny w kierunku sieci inteligentnych czy rozproszonych źródeł energii jest w dużej mierze oparty na wprowadzaniu technologii teleinformatycznych w energetyce.

Zarysowany wyżej obraz powinien stanowić przesłankę do tworzenia takich rozwiązań na poziomie kraju, które z jednej strony uwzględniałyby jak najszerzej dziedziny, w których bezpieczeństwo cyberprzestrzeni jest czy powinno być istotnym elementem, z drugiej zapewniałyby harmonizację, współpracę i koordynację.

[26] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

[27] o takiej synergii mówią opracowania Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji, min. dokument: https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/implementation-of-article-15

3 Rozwiązania regulacyjne i strategiczno-programowe w Polsce i UE dotyczące ochrony cyberprzestrzeni

3.1 Rozwiązania krajowe

3.1.1 Polityka Ochrony Cyberprzestrzeni RP

Polityka Ochrony Cyberprzestrzeni RP (POC RP)[28], przedłożona do uchwalenia Radzie Ministrów przez Ministerstwo Administracji i Cyfryzacji oraz Agencję Bezpieczeństwa Wewnętrznego, jest obecnie jednym z kluczowych dokumentów, w których administracja rządowa wyraziła swe podejście do wdrażania skoordynowanego procesu bezpieczeństwa sieci i informacji w kraju. Chcąc omawiać efekty wdrażania Polityki należy wziąć pod uwagę, że dokument ten został przyjęty w połowie roku 2013. Jednak już obecnie można zwrócić uwagę na takie realizowane elementy Polityki jak: rosnąca grupa powoływanych **pełnomocników ochrony cyberprzestrzen**i w instytucjach administracji publicznej, przeprowadzanie **procesu szacowania ryzyka** (wraz z inwentaryzacją kluczowych systemów), powołanie przez Komitet Rady Ministrów do spraw cyfryzacji **Zespołu zadaniowego do spraw bezpieczeństwa cyberprzestrzeni**, przyjęcie przez ten zespół w marcu 2015 r. **Planu działań w zakresie zapewnienia bezpieczeństwa cyberprzestrzeni RP.** Wymienione wyżej działania należy uznać za dobry przyczynek do rozpoczęcia prac nad całościowym podejściem do stworzenia skoordynowanego, krajowego systemu ochrony cyberprzestrzeni.

Strategiczne dokumenty przyjmowane w wielu krajach, określające planowane działania w dziedzinie bezpieczeństwa cyberprzestrzeni, zawierają z definicji komponent ewaluacji strategii co dwa, trzy lata, ze względu na konieczność oceny efektów oraz szybko zmieniającego się środowiska zagrożeń w cyberprzestrzeni.

[28] https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf

Rekomenduje się, aby dokument POC RP został poddany ewaluacji przed zakończeniem trzech lat jego funkcjonowania (czyli przed czerwcem 2016 roku), pod kątem spełniania założonej roli, zawartości (czy zawiera wszystkie komponenty typowe dla strategii cyberbezpieczeństwa), umocowania w prawodawstwie, zakresu podmiotowego i przedmiotowego. Zaleca się, aby wziąć pod uwagę dokonania innych, rozwiniętych krajów w tym zakresie, przykładowo zebranych i opracowanych przez ENISA[29]

Nie należy wykluczać, że wnioskiem z takiej ewaluacji byłoby napisanie drugiej wersji dokumentu ochrony cyberprzestrzeni (tak jak dzieje się to w wielu krajach, takich jak Holandia, Wielka Brytania czy Estonia).

Zaznaczyć należy, że uwagi do obecnej wersji dokumentu zostały wyrażone między innymi w raporcie NIK[30]: *Realizacja przed podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP.*

3.1.2 Doktryna Cyberbezpieczeństwa RP

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej opracowana przez Biuro Bezpieczeństwa Narodowego, została opublikowana w styczniu 2015 r. W przesłaniu Prezydenta RP zawartym na początku dokumentu można przeczytać, iż:

> Doktryna cyberbezpieczeństwa wskazuje strategiczne kierunki działań dla zapewnienia pożądanego poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni. Jednocześnie powinna być traktowana jako jednolita podstawa koncepcyjna, zapewniająca spójne i kompleksowe podejście do zagadnień cyberochrony i cyberobrony – jako wspólny mianownik dla działań realizowanych przez podmioty administracji publicznej, służby bezpieczeństwa i porządku publicznego, siły zbrojne, sektor prywatny oraz obywateli. Dzięki temu doktryna cyberbezpieczeństwa może stanowić punkt wyjścia do dalszych prac na rzecz wzmocnienia bezpieczeństwa Polski i Polaków w cyberprzestrzeni.

Przy takim sformułowaniu celów dokumentu zachodzi pytanie, jaka jest jego relacja do dokumentu POC RP (który powstał wcześniej). Znajdujemy w doktrynie następujące wyjaśnienia:

[29] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss
[30] https://www.nik.gov.pl/kontrole/P/14/043/

> Na potrzeby polskiej administracji wprowadzono nowe rozwiązania w toku prac nad Polityką Ochrony Cyberprzestrzeni RP, przyjętą przez Radę Ministrów w 2013 r. Dokument ten dotyczy przede wszystkim ochrony cyberprzestrzeni w wymiarze pozamilitarnym.

A także:

> Punktem wyjścia niniejszej Doktryny są kierunkowe postanowienia Strategii Bezpieczeństwa Narodowego RP dotyczące cyberbezpieczeństwa, a także zapisy Polityki Ochrony Cyberprzestrzeni RP oraz Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń.

Wydaje się jednak, że związek tych dwóch dokumentów jest dość luźny, a relacja pomiędzy nimi nie jest do końca jasna. Jest to sytuacja, która może świadczyć o braku wystarczającej koordynacji w ramach organów państwa w dziedzinie bezpieczeństwa cyberprzestrzeni.

Rekomenduje się, aby administracja państwowa jak najszybciej doprowadziła do uspójnienia wszelkich dokumentów o charakterze strategicznym dotyczących bezpieczeństwa cyberprzestrzeni. Docelowym modelem byłoby opracowanie jednego dokumentu: strategii ochrony cyberprzestrzeni RP, który mógłby pełnić rolę podobną do analogicznych dokumentów strategii innych krajów.

To, co jednak zdecydowanie odróżnia oba dokumenty w sensie obszaru, którym się zajmują, to fakt uwzględnienia w dokumencie doktryny aspektów cyberobrony (*cyberdefence*) wraz z wyartykułowaniem podejścia do działań ofensywnych, wyrażonych w intencjach budowy podsystemów zdefiniowanych jako:

> podsystemy operacyjne i wsparcia – zdolne do samodzielnego prowadzenia defensywnych (ochronnych i obronnych) oraz ofensywnych cyberoperacji, a także udzielania i przyjmowania wsparcia w ramach działań sojuszniczych.

3.1.3 Prawo telekomunikacyjne a obowiązki w dziedzinie cyberbezpieczeństwa

Prawo telekomunikacyjne w obecnej formie zawiera postanowienia związane z kwestiami bezpieczeństwa lub integralności sieci i usług telekomunikacyjnych, a także bezpieczeństwem danych osobowych.

W związku z przyjęciem tzw. europejskiego pakietu telekomunikacyjnego[31] w roku 2009, rynek łączności elektronicznej zyskał nowe ramy, także w odniesieniu do kwestii bezpieczeństwa telekomunikacyjnego czy bezpieczeństwa danych.

I tak, na szczególną uwagę zasługują art.13 a i b Dyrektywy 2009/140/WE:

„ROZDZIAŁ III a :BEZPIECZEŃSTWO I INTEGRALNOŚĆ[32] SIECI I USŁUG

Artykuł 13a Bezpieczeństwo i integralność

W odniesieniu do Artykułu 13a Bezpieczeństwo i integralność główne postanowienia przewidują, iż:

1. *Państwa członkowskie zapewnią, aby operatorzy sieci publicznych lub świadczące usługi publicznie dostępne podjęły odpowiednie środki bezpieczeństwa – proporcjonalnie do ryzyka,*
2. *Państwa członkowskie zapewnią, aby przedsiębiorstwa udostępniające publiczne sieci łączności stosowały właściwe środki w celu zapewnienia integralności swoich sieci, a tym samym zapewniały ciągłość świadczenia usług za pośrednictwem tych sieci.*
3. *Przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej powiadamiają właściwy krajowy organ regulacyjny o każdym naruszeniu bezpieczeństwa lub utracie integralności, które miały znaczący wpływ na funkcjonowanie sieci lub usług.*
4. *Krajowy organ regulacyjny informuje o naruszeniach organy regulacyjne innych państw członkowskich oraz Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz może podać tę informację do wiadomości publicznej lub nałożyć taki obowiązek na przedsiębiorstwa,*
5. *Raz w roku krajowy organ regulacyjny przekazuje Komisji i ENISA sprawozdanie podsumowujące otrzymane zgłoszenia oraz podjęte działania.*
6. *Komisja Europejska, uwzględniając opinię ENISA, może przyjąć właściwe techniczne środki wykonawcze mające na celu harmonizację środków, o których mowa w ust. 1, 2 i 3, w tym środki określające okoliczności, format i procedury stosowane w odniesieniu do wymogów dotyczących zgłoszenia.*

W odniesieniu do Artykułu 13b *Wdrożenie i egzekwowanie* główne postanowienia przewidują, iż:

1. *Państwa członkowskie zapewniają, aby w celu wdrożenia art. 13a krajowe organy regulacyjne były uprawnione do wydawania wiążących instrukcji, w tym instrukcji na temat ograniczeń czasowych dotyczących wdrożenia, przedsiębiorstwom*

[31] Dyrektywa Parlamentu Europejskiego i Rady 2009/140/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę ramową (2002/21/WE) 2009/140/WE

[32] Trzeba zwrócić uwagę, że słowo integralność (ang. *Integrity*) zostało zastosowane w dyrektywie w sposób mogący powodować konsternację wśród środowisk zajmujących się tematyką bezpieczeństwa. W tym wypadku intencja prawodawcy dotyczyła raczej kwestii niezawodności i dostępności sieci i usług.

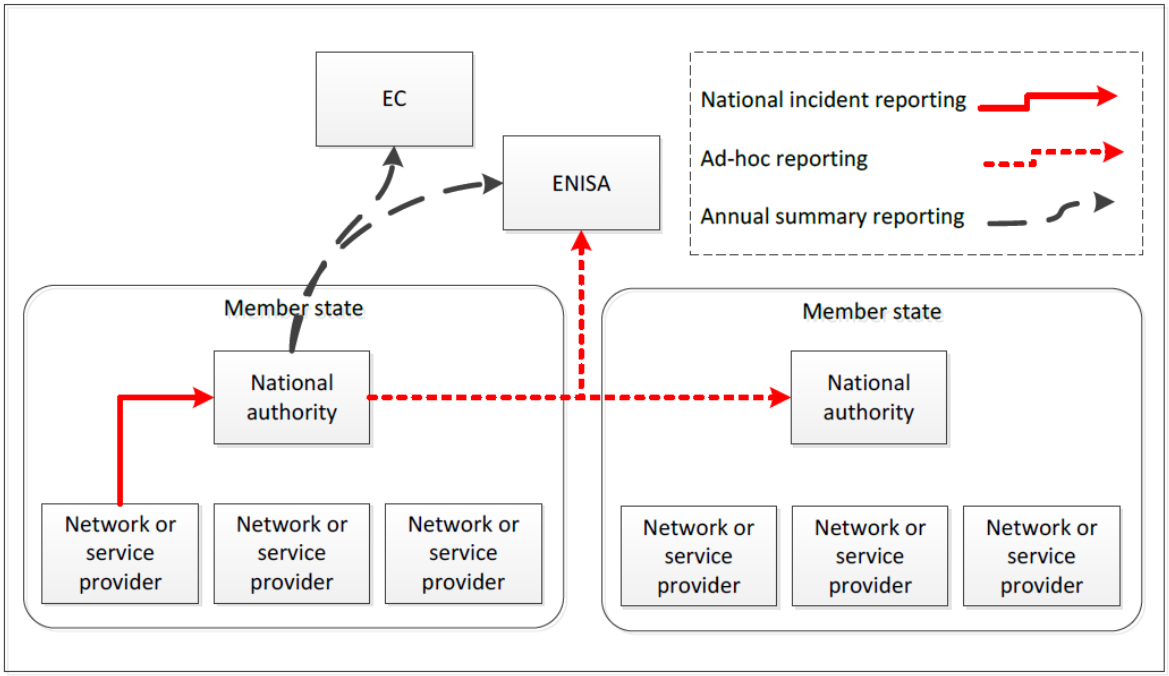
udostępniającym publiczne sieci łączności lub świadczącym publicznie dostępne usługi łączności elektronicznej,

2. *Państwa członkowskie zapewniają, aby krajowe organy regulacyjne były uprawnione do wymagania od przedsiębiorstw udostępniających publiczne sieci łączności lub świadczących publicznie dostępne usługi łączności elektronicznej:*
    a. *dostarczania informacji potrzebnych do oceny bezpieczeństwa i integralności ich usług i sieci, w tym dokumentów dotyczących polityki bezpieczeństwa,*
    b. *poddania się audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany niezależny podmiot lub właściwy organ krajowy i udostępnienia krajowemu organowi regulacyjnemu wyników takiego audytu. Koszty audytu ponosi przedsiębiorstwo.*
3. *Państwa członkowskie zapewniają, aby krajowe organy regulacyjne posiadały wszelkie uprawnienia niezbędne do badania przypadków nieprzestrzegania wymogów oraz jego wpływu na bezpieczeństwo i integralność sieci.*

Podsumowując, art.13a mówi generalnie o konieczności:

- stosowania przez operatorów właściwych środków bezpieczeństwa,
- adekwatnego do zagrożeń reagowania,
- konieczności powiadamiania o naruszenia bezpieczeństwa lub integralności właściwy organ regulacyjny.

Ilustrację procesów związanych z raportowaniem, przewidzianych w art.13a można przedstawić w sposób następujący, zgodnie ze schematem publikowanym w kilku opracowaniach Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) poświęconych implementacji tych przepisów w krajach członkowskich:



Rysunek 1. Typy raportowania przewidziane w art.13a. Źródło: ENISA

Rysunek pokazuje trzy typy informacji przekazywanej.

Typ pierwszy oznaczony czerwoną linią dotyczy zgłaszania przypadków naruszeń bezpieczeństwa lub integralności sieci przez operatorów do krajowego organu regulacyjnego w sektorze łączności

Typ drugi oznaczony czerwoną linią przerywaną dotyczący ostrzegania przez krajowe organy (regulatorów) o istotnych przypadkach (w szczególności o transgranicznym charakterze) – organy właściwe w innych krajach UE a także agencję ENISA

Typ trzeci oznaczony czarną linią przerywaną dotyczy przekazywania przez regulatorów rocznych raportów do Komisji Europejskiej (EC) oraz agencji ENISA

Artykuł 13b europejskiego pakietu telekomunikacyjnego idzie dalej. Mówi on o tym, że, żeby krajowi regulatorzy mogli skutecznie wdrażać postanowienia art. 13a, powinni oni być wyposażeni w odpowiednie uprawnienia do wydawania wiążących instrukcji operatorom (w tym do zakreślania ram czasowych dostosowania się do przepisów), a także uprawnienia do wymagania od przedsiębiorców dostarczania odpowiednich informacji np. o stosowaniu zdefiniowanych polityk bezpieczeństwa, poddawania się audytom bezpieczeństwa oraz uprawnienia kontrolne (analiza konkretnych przypadków naruszeń).

W polskiej ustawie Prawo telekomunikacyjne, po nowelizacji przyjętej w roku 2012, transpozycja art.13a nastąpiła do odpowiednich artykułów w Dziale VII a *Bezpieczeństwo i*

integralność sieci i usług telekomunikacyjnych. Poniższy rysunek przedstawia istotę zapisów w tym dziale w podziale na poszczególne paragrafy:

Rysunek 2. Artykuły Działu VII a PT.

Artykuły 175, 175a,b,c,d,e stanowią istotny krok w kierunku podnoszenia poziomu bezpieczeństwa cyberprzestrzeni. Sektor telekomunikacyjny jest pierwszym sektorem, który na mocy ustawy podlega określonym rygorom bezpieczeństwa telekomunikacyjnego. Dlatego istotne jest obserwowanie, jak w praktyce sprawdzają się regulacje zobowiązujące podmioty gospodarcze do stosowania odpowiednich wymagań w kwestii bezpieczeństwa.

I tak, art. 175 nakłada obowiązek zapewnienia przez operatorów bezpieczeństwa integralności sieci i transmisji w tych sieciach, a także obowiązek informowania użytkowników o wystąpieniu ryzyk, sposobach zabezpieczania i koszcie takich zabezpieczeń.

Z art. 175a wynika obowiązek informowania regulatora o wystąpieniu istotnych naruszeń bezpieczeństwa sieci lub usług, a także o podjętych działaniach zapobiegawczych i naprawczych.

Art. 175b mówi o konieczności przekazywania przez organ regulacyjny informacji o istotnych naruszeniach do podmiotów zagranicznych, publikowaniu informacji o naruszeniach na stronach internetowych oraz przekazywaniu raportów rocznych do odpowiednich podmiotów.

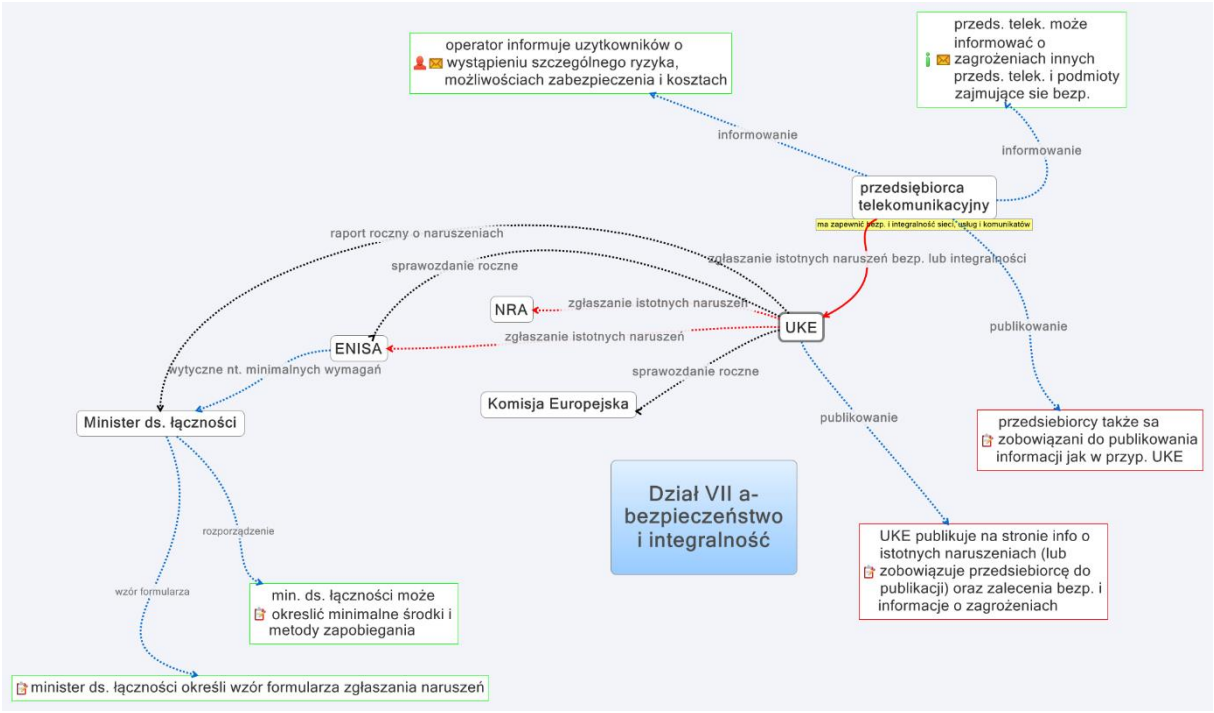
Rolą art. 175c jest określenie zasad reagowania na naruszenia bezpieczeństwa lub integralności przez operatorów.

Bardzo istotną rolę pełni art. 175d, który przewiduje możliwość określenia przez ministra ds. łączności w drodze rozporządzenia minimalnych środków technicznych i

organizacyjnych oraz metod zabezpieczania w celu zapewnienia bezpieczeństwa i integralności sieci oraz usług- biorąc pod uwagę rekomendacje ENISA i Komisji Europejskiej. Wytyczne takie stanowiłyby bowiem dużą pomoc dla podmiotów, które są zobowiązane do zapewnienia bezpieczeństwa sformułowane w art. 175.

Ostatni artykuł, 175e mówi z kolei o podnoszeniu świadomości użytkowników o zagrożeniach i możliwych środkach zapobiegawczych (zabezpieczeniach) poprzez publikowanie informacji na stronach organu regulacyjnego, stronach operatorów lub poprzez odnośniki do stron podmiotów zajmujących się bezpieczeństwem sieci.

Kolejny rysunek ilustruje przepływy zadań pomiędzy głównymi interesariuszami: krajowymi regulatorami, operatorami telekomunikacyjnymi, abonentami/użytkownikami, ministrem właściwym ds. łączności, Komisją Europejską oraz agencją ENISA.



Rysunek 3. Procesy zachodzące w ramach realizacji zapisów Działu VII a ustawy PT.

W kontekście powyższych obserwacji, poniżej prezentujemy **szereg obserwacji i wniosków** związku z wdrażaniem mechanizmów przewidzianych w Dyrektywie 2009/140/WE.

Przepisy przewidziane w dyrektywie europejskiej zostały przeniesione do polskiego prawa w zakresie Art. 13a. Wdrożenie postanowień Art. 13b wydaje się zadaniem wciąż stojącym przed administracją państwa.

Jak wspomniano wyżej, w art.13a europejskiego pakietu telekomunikacyjnego jest mowa o tym, aby przedsiębiorstwa udostępniające publiczne sieci łączności lub świadczące publicznie dostępne usługi łączności elektronicznej powiadamiały właściwy krajowy organ regulacyjny o każdym naruszeniu bezpieczeństwa lub utracie integralności, które miały

znaczący wpływ na funkcjonowanie sieci lub usług. W celu harmonizacji mechanizmów implementowanych w krajach członkowskich w UE, Komisja Europejska przy pomocy Agencji ENISA dostarcza rozmaite zalecenia, jak w praktyce stosować rozmaite zapisy. I tak kwestia podstawowa, jak definiować naruszenia o znaczącym wpływie, po wypracowaniu w grupach roboczych[33], przedstawiona poradniku agencji ENISA: *Article_13a_ENISA_Technical_Guideline_On_Incident_Reporting_v2_1.pdf*[34] (obecna wersja 2.1 dokumentu została opublikowana w roku 2014). W kontekście raportów rocznych o naruszeniach (incydentach), które krajowi regulatorzy są zobowiązani do przesyłania Komisji Europejskie oraz agencji ENISA przyjęto następujące zalecenia:

	1h-2h	2h-4h	4h-6h	6h-8h	>8h
1% - 2%					
2% - 5%					
5% - 10%					
10% - 15%					
> 15%					

Figure 2. Absolute threshold based on the duration and the percentage of the national user base.

Rysunek 4. Rekomendacje co do definiowania incydentów o znaczącym wpływie na bezpieczeństwo lub integralność sieci i usług. Źródło: ENISA

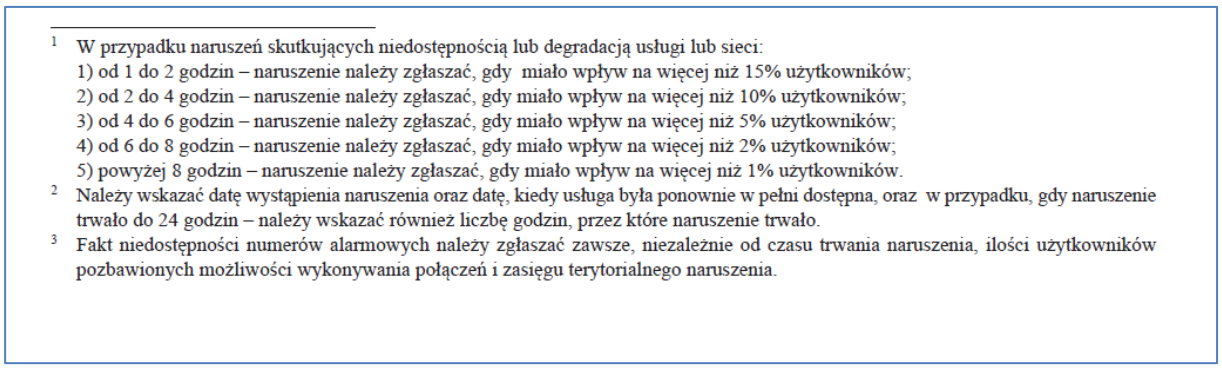
Kraje członkowskie mogą dowolnie definiować incydenty o znaczącym wpływie. Jednakże chociażby z powodu harmonizacji procesu raportowania, krajowe definicje powinny umożliwiać możliwie łatwe agregowanie danych i tworzenie wspólnych statystyk.

W Polsce ukazało się rozporządzenie Ministra Administracji i Cyfryzacji z marca 2013 roku, w którym widzimy analogiczne, jak w opracowaniu ENISY progi, powyżej których należy zgłaszać dane naruszenie (np. w przypadku incydentu trwającego 1-2 h, który objął powyżej 15% użytkowników); jednak jest podstawowa różnica w rozumieniu procentu użytkowników. W zaleceniach agencji ENISA chodzi o procent użytkowników w kraju (*national user base*), co do rozporządzenia ministra, należy domniemywać, że jest tam mowa o użytkownikach danego operatora. W ten sposób, w zależności od wielkości operatora, zdarzenie mające wpływ na niewielką liczbę użytkowników (np. 10), które trwa powyżej 4h, powinno być przez

[33] W roku 2010 ENISA powołała grupę roboczą składającą się z ekspertów krajowych organów regulacyjnych

[34] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting

małego operatora, który ma przykładowo 200 użytkowników, zgłaszane do UKE jako istotne. UKE zaś, otrzymując od wielu operatorów dane procentowe odnośnie użytkowników, którzy ucierpieli z powodu danego zdarzenia, nie jest prawdopodobnie w stanie określić procentu użytkowników w skali całego kraju, na których dane zdarzenie miało wpływ.



[1] W przypadku naruszeń skutkujących niedostępnością lub degradacją usługi lub sieci:
1) od 1 do 2 godzin – naruszenie należy zgłaszać, gdy miało wpływ na więcej niż 15% użytkowników;
2) od 2 do 4 godzin – naruszenie należy zgłaszać, gdy miało wpływ na więcej niż 10% użytkowników;
3) od 4 do 6 godzin – naruszenie należy zgłaszać, gdy miało wpływ na więcej niż 5% użytkowników;
4) od 6 do 8 godzin – naruszenie należy zgłaszać, gdy miało wpływ na więcej niż 2% użytkowników;
5) powyżej 8 godzin – naruszenie należy zgłaszać, gdy miało wpływ na więcej niż 1% użytkowników.

[2] Należy wskazać datę wystąpienia naruszenia oraz datę, kiedy usługa była ponownie w pełni dostępna, oraz w przypadku, gdy naruszenie trwało do 24 godzin – należy wskazać również liczbę godzin, przez które naruszenie trwało.

[3] Fakt niedostępności numerów alarmowych należy zgłaszać zawsze, niezależnie od czasu trwania naruszenia, ilości użytkowników pozbawionych możliwości wykonywania połączeń i zasięgu terytorialnego naruszenia.

Rysunek 5. Progi definiowane w rozporządzeniu MAC.

Dodatkowo operatorzy, którzy świadczą usługi przedsiębiorcom, zwykle nie mają wiedzy o liczbie końcowych użytkowników, więc trudno im obliczyć wymagany procent. Mogliby zgłaszać liczbę swych klientów instytucjonalnych lub indywidualnych, którzy, np. ucierpieli w danym zdarzeniu, ale tu pojawia się problem, jak z takich danych wywnioskować o prawdziwej skali problemu.

Uwagę zwraca także fakt, że w rozporządzeniu jest mowa o naruszeniach skutkujących niedostępnością lub degradacją usługi lub sieci, co oznacza, że te incydenty bezpieczeństwa, które nie powodują niedostępności (np. włamanie w celu wykradzenia danych), w ogóle nie będzie zgłaszane.

Powyższe uwagi skłaniają do wniosku, że istniejące rozporządzenie z 19 marca 2013 r. w sprawie wzoru formularza do przekazywania informacji o naruszeniu bezpieczeństwa lub integralności (…) powinno zostać poddane ponownej rewizji w celu wprowadzenia ewentualnych modyfikacji ułatwiających jego stosowanie.

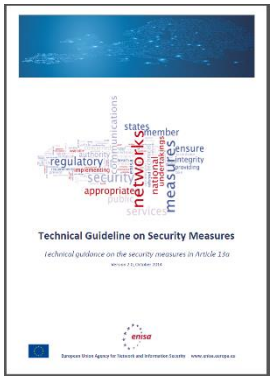
Wykorzystanie środków fakultatywnych

Art. 175d Prawa telekomunikacyjnego przewiduje, jak wspomniano wyżej, możliwość wydania rozporządzenia określającego minimalne środki techniczne i organizacyjne oraz metody zabezpieczania w celu zapewnienia bezpieczeństwa i integralności sieci oraz usług świadczonych przez operatorów. W naszym kraju jak do tej pory nie wydano takiego rozporządzenia. Choć, z punku widzenia prawa, wydanie takiego rozporządzenia jest fakultatywne, a więc jego braku nie można zaliczyć do uchybień legislacyjnych, to jednak,

z praktycznego punktu widzenia, brak wytycznych co do definiowania poziomu, który uznaje się za spełnienie minimalnych standardów zabezpieczeń nie jest pomocny w praktycznym, zharmonizowanym wdrażaniu polityk bezpieczeństwa w całym sektorze. Rekomenduje się zatem, aby rozważyć wprowadzenie rozporządzenia określającego minimalne środki techniczne i organizacyjne oraz metody zabezpieczania w celu zapewnienia bezpieczeństwa i integralności sieci oraz usług świadczonych przez operatorów.

Można powiedzieć, że istnieją dwa główne filary, na których opierają się istniejące i projektowane dyrektywy oraz rozporządzenia Unii Europejskiej: jest to określanie minimalnych standardów bezpieczeństwa oraz przepływ informacji (raportowanie) odnośnie incydentów o istotnym znaczeniu. Takie schematy można znaleźć nie tylko w pakiecie telekomunikacyjnym, ale także w dyrektywach dot. ochrony danych osobowych, rozporządzeniu eIDAS czy planowanej dyrektywie NIS.

Wobec powyższego Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji



przygotowała szereg rekomendacji dla krajów członkowskich odnośnie określania minimalnych wymagań bezpieczeństwa, które powinni zastosować operatorzy. Konkretnie mowa tu o opracowaniu: *Article_13a_ENISA_Technical_Guideline_On_Security_Measures_v2_0.pdf* [35], którego aktualna wersja powstała w październiku 2014r.

Opracowanie to było w ciągu ostatnich trzech lat aktualizowane, w wyniku prac grupy ekspertów pochodzących m.in. ze środowiska krajowych regulatorów telekomunikacyjnych i stanowi praktyczny podręcznik dla regulatorów i ministerstw odpowiedzialnych za rynek komunikacji elektronicznej w poszczególnych krajach, w szczególności w zakresie odpowiedzi na pytanie, jak wdrażać punkt 1 i 2 artykułu 13a, czyli: zagwarantować, że będą stosowane środki zapewniające bezpieczeństwo i integralność sieci i usług (właściwie: niezawodności sieci i dostępności usług) odpowiednie do ryzyk. Wymaga to oczywiście zmierzenia się z kwestią oszacowania ryzyk i dobrania odpowiednich, minimalnych środków bezpieczeństwa. Rekomendacje odnośnie tych zagadnień znajdują się we wspomnianym wyżej poradniku ENISA.

[35] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures

Rekomenduje się zatem, aby wytyczne odnośnie minimalnych środków bezpieczeństwa i zapewnienia niezawodności oraz dostępności usług telekomunikacyjnych zostały w Polsce opracowane na bazie wyżej wymienionego podręcznika oraz ogólnie przyjętych standardów w Europie, a następnie zostały wydane w formie rozporządzenia.

Efekt praktyczny wprowadzenia regulacji

Praktyczny efekt wprowadzenia omawianych regulacji jest między innymi widoczny w corocznych raportach Urzędu Komunikacji Elektronicznej przekazywanych ministrowi właściwemu ds. łączności (*Raport Prezesa Urzędu Komunikacji Elektronicznej o zgłoszonych w danym roku zagrożeniach i podjętych przez przedsiębiorców telekomunikacyjnych działaniach zapobiegawczych i środkach naprawczych w zakresie bezpieczeństwa lub integralności sieci lub informacji)*. Opracowanie takiego raportu wynika z zapisów art. 175b ust. 4 Prawa telekomunikacyjnego.

Ze względu na fakt, że zgłaszanie incydentów mających wpływ na funkcjonowanie numerów alarmowych następuje bez względu na progi czasowe czy ilości dotkniętych użytkowników, w raporcie UKE zdecydowana większość zgłaszanych przypadków dotyczy właśnie numerów alarmowych – w telefonii stacjonarnej (97% w roku 2013). Tylko 1,3% przypadków (w roku 2013) przekraczało progi zdefiniowane przez ENISA. Przyczyną większości raportowanych zdarzeń były awarie sprzętu bądź oprogramowania (81% w roku 2013), choć średnio nie trwały długo. Z kolei awarie zasilania miały stosunkowo największy skutek na użytkowników (duża liczba dotkniętych awarią, a także długi czas ich usuwania).

Zwraca jednak uwagę fakt, że w praktycznie wszystkie zgłaszane przypadki to zdarzenia mające wpływ na dostępność usług i sieci (awarie). Tak więc z punktu widzenia kwestii bezpieczeństwa telekomunikacyjnego czy też bezpieczeństwa cyberprzestrzeni, przyjęte w Prawie telekomunikacyjnym obowiązki raportowania nie dają w praktyce wiedzy na ten temat.

Nie jest to jednak wyłącznie specyfika rynku polskiego. Wystarczy spojrzeć na raporty ENISA, powstające na bazie raportów przesyłanych corocznie przez wszystkich regulatorów europejskich (NRA).

W raporcie opublikowanym przez agencję ENISA za rok 2013, wśród głównych spostrzeżeń, na uwagę zasługują:

- jedna piąta incydentów zaraportowanych przez krajowych regulatorów dotyczyła niedostępności numerów alarmowych,
- 61% incydentów było spowodowane awariami systemów, 19% błędami ludzkimi, 14% to skutki zjawisk atmosferycznych a 6% zostało skategoryzowane jako umyślne działania szkodliwe (ang. malicious actions),
- umyślne działania szkodliwe (np. cyberataki ale także kradzieże kabli) powodowały dużą niedostępność usług , porównywalną do tych spowodowanych skutkami działań atmosferycznych (np. klęski żywiołowe)

Analizując dwa typy raportów: krajowy i europejski można wyróżnić szereg podobieństw, ale także różnic. Główne podobieństwo jest takie, że w efekcie wdrożenia regulacji odnośnie bezpieczeństwa i integralności sieci i usług , ta druga kategoria, związana głównie z awariami, wzięła górę nad kwestiami bezpieczeństwa. Jest to poniekąd zrozumiałe, gdyż w środowisku regulatorów sektora telekomunikacyjnego, parametry niezawodnościowe infrastruktury oraz usług (takich jak klasyczna telefonia, telefonia mobilna oraz mobilny internet) tradycyjnie są przedmiotem zainteresowania tych organów. Obszar bezpieczeństwa telekomunikacyjnego jest mniej znany i przykłada się do niego mniejszą wagę. Fakt, iż ustalono, że jedynie incydenty, które powodują niedostępność usług dla użytkowników są zgłaszane do regulatorów, powoduje, że wiele typów ataków naruszających bezpieczeństwo w ogóle nie będzie zgłaszanych. Tak więc, przykładowo atak DDoS, powodujący niedostępność usług powinien być zgłaszany, ale już np. fraudy telefonii VoIP, będące skutkiem ataków hackerskich, powodujące straty materialne u użytkowników, ale nie powodujące niedostępności usługi, nie zostaną odnotowane.

Oczywiście każdy kraj może według własnego uznania zdefiniować, jakie naruszenia mają być zgłaszane jako istotne. Z raportu UKE wynika, że w Polsce zdecydowana większość zgłoszeń dotyczy numerów alarmowych i wynika to z przyjętych przepisów, które mówią, że takie przypadki mają być zgłaszane niezależnie od parametrów tejże niedostępności (czas trwania, ilość użytkowników). Jednak w roku 2014 tylko 0,7% wszystkich zgłoszonych naruszeń przekroczyło progi zdefiniowane przez ENISA, a więc zostało przekazane do wiadomości ciałom europejskim.

UKE podnosi także w raporcie kwestię pewnej dowolności przy określaniu, czy dany incydent przekracza próg, który powoduje, że powinien być on zgłoszony do regulatora, co powoduje, że, w praktyce, otrzymywane z rynku dane nie mogą być uznane za wiarygodny obraz zdarzających się naruszeń. W zasadzie incydenty stricte naruszające bezpieczeństwo są zgłaszane w nieznacznym zakresie. W roku 2014 Prezes UKE otrzymał jedynie 5 zgłoszeń związanych z cyberatakiem (w roku 2013 – 1 atak).

W związku z powyższym można rekomendować, jak wyżej, aby rozporządzenie definiujące, jakie naruszenia muszą być raportowane przez operatorów, poddać rewizji, między innymi pod kątem precyzyjnego określenia metody szacowania jego istotności (w tym liczby użytkowników, na których zdarzenie miało wpływ). W celu uzyskania rzeczywistej informacji o naruszeniach bezpieczeństwa warto rozważyć wprowadzenie kategorii naruszenia związanej z cyberatakami; jednocześnie, poziom istotności nie powinien koniecznie wiązać się z okresem niedostępności czy częściowej niedostępności usługi.

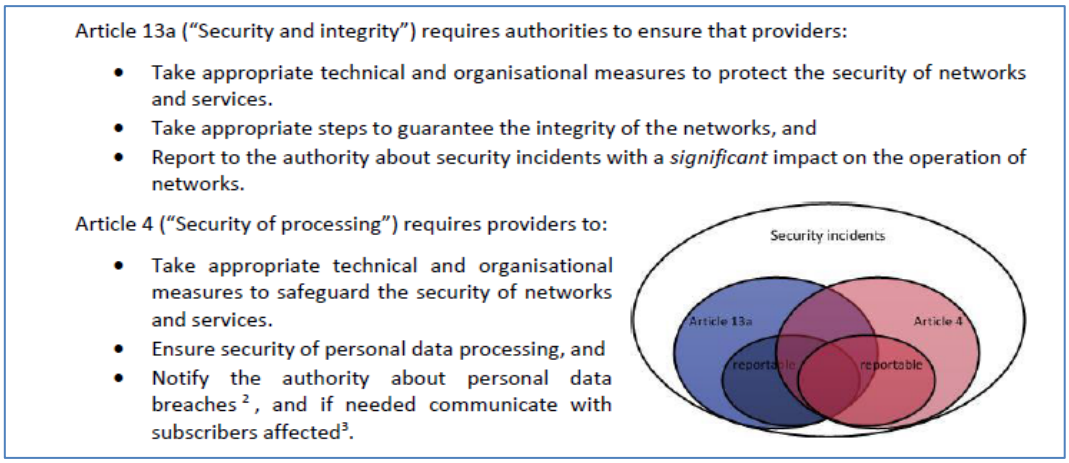
Naruszenia związane z ochroną danych osobowych

Oprócz naruszeń związanych z bezpieczeństwem lub integralnością sieci lub usług, w Prawie telekomunikacyjnym zostały wprowadzone przepisy związane z bezpieczeństwem danych osobowych. Mówią o tym art.174 a-d ustawy. Główne postanowienia dotyczą:

- obowiązku zgłaszana do GIODO naruszeń danych osobowych przetwarzanych przez przedsiębiorcę telekomunikacyjnego w związku ze świadczeniem publicznie dostępnych usług telekomunikacyjnych,
- obowiązku informowania abonentów/użytkowników końcowych będących osobami fizycznymi o naruszeniach mających niekorzystny wpływ (np. naruszenie dóbr osobistych, ujawnienie tajemnicy bankowej itp.),
- obowiązku prowadzenia przez operatora rejestru naruszeń danych osobowych (w tym faktów, skutków, podjętych działań).

Harmonizacja obowiązków zapewniania bezpieczeństwa i raportowania o naruszeniach przez przedsiębiorców telekomunikacyjnych

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji w swoich opracowaniach podkreśla potrzebę harmonizacji w obszarze obowiązków nakładanych na podmioty odnośnie bezpieczeństwa teleinformatycznego (zapewnianie minimalnych środków bezpieczeństwa, raportowanie o naruszeniach, prowadzenie akcji uświadamiających. W kontekście opisanych w tym rozdziale obowiązków, ENISA mówi o harmonizacji postanowień wynikających z art. 13a telekomunikacyjnej dyrektywy ramowej (Dyrektywa 2009/140/WE) oraz art. 4 Dyrektywy o ochronie prywatności (e-privacy directive 2002/58/EC). Oba artykuły traktują o bezpieczeństwie sieci komunikacji elektronicznej i usług. Przedstawia to poniższa ilustracja:



Rysunek 5 Porównanie obowiązków dostawców usług odnośnie bezpieczeństwa wynikających z dwóch dyrektyw. Źródło: ENISA[36]

Art. 13a dyrektywy telekomunikacyjnej oraz art. 4 dyrektywy o prywatności dotyczą oczywiście innych typów naruszeń. Z jednej strony chodzi o bezpieczeństwo i integralność sieci lub usług, z drugiej rzecz dotyczy danych osobowych. W wielu krajach europejskich, tak jak w Polsce oba typy naruszeń są raportowane do innych instytucji.

Jednak, jak wskazuje ENISA, natura naruszeń bezpieczeństwa czy ochrony prywatności często jest bardzo podobna (częstokroć jeden incydent zawiera w sobie oba komponenty). Odpowiednie środki zaradcze także wielokrotnie są te same lub bardzo podobne. Przykładowo, mechanizmy kontroli dostępu są konieczne dla zapewnienia bezpieczeństwa infrastruktury, ale także chronią przed nieuprawnionym dostępem do danych. Także samo raportowanie o naruszeniach dla obu typów wygląda lub może wyglądać bardzo podobnie.

W opracowaniu *Technical Guideline on Security Measures for Article 4 and Article 13a* z października 2014 roku ENISA przedstawia jednolitą koncepcję zapewniania odpowiednich środków bezpieczeństwa w obu obszarach. Stanowi on doskonałą pomoc dla instytucji krajowych, które wdrażają postanowienia dotyczące bezpieczeństwa teleinformatycznego wynikające z obu dyrektyw (w naszym kraju jest to UKE i GIODO).

[36] *Technical Guideline on Security Measures for Article 4 and Article 13a : http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/guideline-on-security-measures-for-article-4-and-article-13a*

Harmonizacja w zakresie obowiązków raportowania naruszeń oraz zapewniania odpowiednich mechanizmów bezpieczeństwa jest wysoce rekomendowana, w szczególności, jeśli dotyczy tych samych podmiotów (w tym wypadku operatorów i dostawców usług komunikacji elektronicznej). Także z punktu widzenia posiadania pełniejszego obrazu sytuacji związanej ze stanem cyberbezpieczeństwa w kraju oraz występującymi naruszeniami, harmonizacja pomiędzy podobnymi obszarami byłaby działaniem we właściwym kierunku.

3.1.4 Inne dokumenty

Strategia Bezpieczeństwa Narodowego

Jak wspomniano wcześniej, Doktryna Bezpieczeństwa Cyberprzestrzeni RP została opracowana w następstwie powstania dokumentu strategicznego w postaci Strategii Bezpieczeństwa Narodowego. W tym dokumencie czytamy miedzy innymi:

„Do najważniejszych zadań przygotowawczych w obszarze cyberbezpieczeństwa należy wdrożenie i rozwijanie systemowego podejścia do sfery cyberbezpieczeństwa w wymiarze prawnym, organizacyjnym i technicznym. Konieczne jest określenie zasad prowadzenia aktywnej obrony oraz budowa narodowego systemu obrony cybernetycznej, w tym rozwijanie Krajowego Systemu Reagowania na Incydenty Komputerowe w Cyberprzestrzeni Rzeczypospolitej Polskiej, kompatybilnego z systemami państw sojuszniczych. Istotne jest stworzenie narodowego ośrodka koordynacji, wspierającego organizację współpracy pomiędzy poszczególnymi podmiotami realizującymi zadania w zakresie cyberbezpieczeństwa i wymianę informacji oraz promującego dobre praktyki w dziedzinie cyberbezpieczeństwa. Ważne jest nabycie pełnych kompetencji do rozpoznawania, zapobiegania i zwalczania cyberzagrożeń oraz zdolności do wytwarzania polskich rozwiązań technologicznych przeznaczonych do zapewnienia odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni. Zapewnione zostaną odpowiednie warunki tworzenia i działania partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa. Istotne jest też zwiększanie świadomości użytkowników o zagrożeniach w cyberprzestrzeni poprzez intensyfikację działań edukacyjnych na wszystkich poziomach nauczania, a także w formie szkoleń i kampanii społecznych. Wskazane jest uruchomienie specjalnych kierunków studiów związanych z bezpieczeństwem funkcjonowania w cyberprzestrzeni oraz rozwijanie programów badawczych w tym obszarze."

3.2 Rozwiązania UE

3.2.1 Projekt dyrektywy NIS

Jednym z najważniejszych dokumentów programowych UE w dziedzinie bezpieczeństwa cyberprzestrzeni jest projekt tak zwanej dyrektywy NIS.

Projekt Dyrektywy NIS Parlamentu Europejskiego i Rady, czyli: *Directive of the European Parliament and of the Council concerning measures with a view to achieving a high common level of network and information security across the Union*[37] został przedstawiony przez Komisję Europejską w lutym 2013 roku. Od tego czasu, przez pięć kolejnych prezydencji w Unii Europejskiej, był on dyskutowany i uzgadniany. Mimo że większość, jeśli nie wszystkie kraje, popierają powstanie takiej dyrektywy, to w szczegółach jest pomiędzy nimi wiele różnic w podejściu do tematu ochrony cyberprzestrzeni, w tym w szczególności w kontekście jej zakresu przedmiotowego, poziomu harmonizacji w Unii Europejskiej czy mechanizmów współpracy międzynarodowej. Niemniej jednak należy się liczyć z tym, że Dyrektywa NIS zostanie w końcu przyjęta.

Celem Dyrektywy NIS, który został zapowiedziany w dokumencie Strategii bezpieczeństwa w cyberprzestrzeni Unii Europejskiej *(Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*)[38], jest ustanowienie w Unii Europejskiej jednolitego, wysokiego poziomu bezpieczeństwa sieci teleinformatycznych i informacji (ang. *NIS – Network and Information Security*).

Dyskutowana propozycja dyrektywy zawiera szereg zasadniczych elementów, które powinny być wprowadzone przez kraje członkowskie, takich jak:

- ustanowienie odpowiedniej organizacji koordynowania kwestii cyberbezpieczeństwa na poziomie krajowym, w tym ustanowienie punktu kontaktowego do współpracy międzynarodowej,
- powołanie struktury zespołów reagujących typu CSIRT (Computer Security Response Team) na poziomie krajowym,
- przyjęcie narodowych strategii bezpieczeństwa cyberprzestrzeni oraz planów współpracy w tym obszarze,
- określenie operatorów krytycznej infrastruktury, uzależnionych od technologii teleinformatycznych, którzy będą zobowiązani do analizy ryzyka, wprowadzania odpowiednich mechanizmów bezpieczeństwa oraz do raportowania poważnych incydentów do odpowiednich władz.

W trakcie negocjacji i uzgodnień projekt dyrektywy przechodził wiele modyfikacji

[37] ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
[38] j.w.

(m.in. w dalszym ciągu nie ma porozumienia co do zakresu podmiotowego obowiązywania dyrektywy w stosunku do określonych sektorów czy rodzajów podmiotów). Niemniej jednak, rdzeń projektu, wymieniony w punktach powyżej, pozostaje niezmieniony i należy założyć, że dyrektywa zostanie w końcu przyjęta, co może w znacznym stopniu wspomóc przeprowadzenie skoordynowanych działań na rzecz podnoszenia bezpieczeństwa w cyberprzestrzeni, zarówno na poziomie krajowym jak i w całej Unii Europejskiej.

Obecna wersja projektu (lipiec 2015) charakteryzuje się następującymi głównymi postanowieniami:

1. Kraje członkowskie są zobligowane do przyjęcia **narodowych strategii bezpieczeństwa sieci i informacji** (*national NIS strategy)*, zwanymi także NCSS (*National Cyber Security Strategy)*
2. De facto, większość krajów przyjęła już takie strategie. Kraje najbardziej zaawansowane, takie jak Holandia, Niemcy, Wielka Brytania opracowały już drugie wersje swych strategii na podstawie zebranych doświadczeń z wdrażania ich pierwszych wersji.
3. Tworzy się **strategiczny mechanizm wspierający rozwój współpracy pomiędzy krajami** członkowskimi *(tzw. cooperation group)*, pozwalający na wymianę informacji i doświadczeń, budujący zaufanie, które jest niezbędne przy współpracy w dziedzinie bezpieczeństwa.
4. Na poziomie współpracy operacyjnej, w ramach realizacji zapisów dyrektywy, ma powstać **międzynarodowa sieć krajowych zespołów typu CSIRT**, współdziałających ze sobą w sposób efektywny w celu reagowania na zagrożenia i incydenty (w szczególności o charakterze transgranicznym)[39]. Przewiduje się, że ENISA będzie prowadziła sekretariat dla tej sieci współpracy.
5. Konieczne jest ustanowienie wymagań odnośnie stosowania odpowiednich środków bezpieczeństwa a także powiadamiania o incydentach przez operatorów infrastruktury - mieszczących się w zakresie podmiotowym dyrektywy[40].
6. Kraje członkowskie mają ustanawiać **odpowiednie organy** (tzw. *competent authorities*) **zajmujące się koordynacją, krajowe punkty kontaktowe** (tzw. *single points of contacts)* do współpracy oraz **zespoły CSIRT na poziomie krajowym**.

[39] Międzynarodowe sieci współpracy zespołów CSIRT (w tym CERT) istnieją od dziesięcioleci. W tym wypadku chodzi o ustanowienie oficjalnych mechanizmów współpracy operacyjnej na poziomie CERTów krajowych krajów członkowskich

[40] W tym zakresie w dalszym ciągu trwają uzgodnienia pomiędzy krajami członkowskimi, Parlamentem Europejskim i Komisją.

W projekcie podkreśla się, iż celem dyrektywy jest uzyskanie minimum harmonizacji w dziedzinie NIS na poziomie Unii Europejskiej. Kraje członkowskie mogą natomiast przyjąć wyższe standardy bezpieczeństwa. Przykładowo, jeśli administracja publiczna zostanie wyłączona z zapisów dyrektywy NIS, mimo wszystko należy podjąć w naszym kraju wysiłki w celu ustanowienia minimalnych wymagań bezpieczeństwa oraz mechanizmów raportowania o naruszeniach dla tego niezwykle ważnego sektora, gdyż na mapie zagrożeń, ataki dedykowane na sieci rządowe (np. APT – *advanced persistent* threat) są coraz większym zagrożeniem mogącym naruszyć zdolność do sprawnego funkcjonowania państwa.

Istotne pojęcia zawarte w projekcie dyrektywy

Wśród wielu pojęć, jakie są wprowadzane w projekcie, oprócz pojęć znanych z literatury (choć niekiedy rozmaicie definiowanych), takich jak: systemy i sieci informacyjne, ryzyko, incydent, bezpieczeństwo sieci i informacji warto zwrócić uwagę na nowe pojęcia w tekście dokumentu, mające kluczowe znaczenie dla konceptu NIS prezentowanego w dyrektywie. Po pierwsze, jest to pojęcie tzw**. *essential services***, które oznacza usługi, które są niezbędne do zapewnienia kluczowych funkcji społecznych i ekonomicznych kraju. Na tym pojęciu w dużej mierze koncentruje się projekt dyrektywy, jeśli mowa o zapewnieniu bezpieczeństwa w cyberprzestrzeni.

Innym ważnym pojęciem jest pojęcie **operatora**, czyli podmiotu prywatnego lub publicznego (należącego do pewnej grupy podmiotów określonych typów – wymienionych w kluczowym dla zdefiniowania podmiotowego zakresu dyrektywy Załączniku II projektu dyrektywy NIS), który to operator dostarcza właśnie kluczowe usługi (wspomniane wyżej *essential services*) w danym sektorze. Chodzi o takie usługi, które są zależne od sieci teleinformatycznych, a potencjalne incydenty bezpieczeństwa u tego operatora mogą mieć istotny wpływ na możliwość dostarczania tych kluczowych usług lub wpływ na bezpieczeństwo publiczne.

W gestii poszczególnych krajów członkowskich jest zidentyfikowanie kluczowych operatorów. W tekście projektu dyrektywy podane są kryteria, które mogą posłużyć do wyznaczania listy operatorów, takie jak: wpływ operatora na całość usług w danym sektorze (przykładowo: energetycznym), liczba użytkowników, oszacowanie skutków przerwy w działaniu usługi danego operatora na sytuację ekonomiczną i społeczną (włączając np. oszacowanie czasu niedostępności).

Krajowa strategia bezpieczeństwa sieci i informacji

Projekt zobowiązuje kraje członkowskie do opracowania i przyjęcia strategii cyberbezpieczeństwa, w której znajdują się strategiczne cele danego kraju w dziedzinie cyberbezpieczeństwa, jak również zdefiniowane są konkretne środki (polityczne, regulacyjne), które będą wspierać osiąganie wysokiego poziomu bezpieczeństwa.

Co istotne, dyrektywa wymaga, aby strategia dotyczyła przynajmniej tych obszarów, które są w niej zaproponowane w postaci listy typów operatorów/sektorów (obecnie art. 3 projektu dyrektywy oraz Załączniki II i III).

W szczególności strategia powinna zawierać odniesienie do kwestii:

- określenia celów do osiągnięcia oraz priorytetów działania,
- nakreślenia ram krajowych zarządzania cyberbezpieczeństwem, aby zrealizować zdefiniowane cele oraz priorytety, w szczególności określenia ról i odpowiedzialności rządu oraz innych istotnych aktorów (interesariuszy),
- zdefiniowania sposobów i środków uzyskiwania odpowiednich poziomów gotowości, reakcji i przywracania do stanu gotowości po zdarzeniu w odniesieniu do cyberzagrożeń, włączając w to współpracę pomiędzy sektorem publicznym a prywatnym,
- edukacji, programów podnoszących świadomość oraz programów szkoleniowych w dziedzinie bezpieczeństwa sieci i informacji,
- programów badawczo rozwojowych skojarzonych z realizacją strategii,
- szacowania ryzyka związanego z zagrożeniami cyberprzestrzeni,
- listy aktorów i interesariuszy, którzy będą zaangażowani w realizację strategii bezpieczeństwa.

W Polsce obecnie rolę dokumentu o charakterze strategicznym w obszarze cyberprzestrzeni pełni *Polityka Ochrony Cyberprzestrzeni RP*[41], która jednak nie ma rangi strategii w polskim porządku prawno-administracyjnym. Dodatkowo dokument ten dotyczy tylko administracji rządowej, więc w rozumieniu planowanej dyrektywy NIS, nie wyczerpuje wymaganego zakresu (sektorów i operatorów zaproponowanych w projekcie). Istnieje także drugi dokument odnoszący się do bezpieczeństwa cyberprzestrzeni na poziomie kraju – *Doktryna bezpieczeństwa cyberprzestrzeni RP*[42], opracowana przez BBN. Związek tych dwóch dokumentów pomiędzy sobą jest jedynie symboliczny, Autorzy opracowania rekomendują ich harmonizację.

Kompetentne organy i pojedynczy punkt kontaktowy

Jednym z najważniejszych elementów przewidzianych w projekcie dyrektywy jest powołanie w krajach członkowskich odpowiednich organów odpowiedzialnych za realizację jej postanowień, a tym samym za ustanowienie struktur dla skoordynowanego działania w obszarze NIS, zarówno w poszczególnych krajach, jak i na płaszczyźnie współpracy międzynarodowej.

Każdy kraj ustanawia jeden lub więcej organów (*competent authorities*), odpowiadających za bezpieczeństwo sieci i informacji. Mają one monitorować (koordynować) wdrażanie postanowień dyrektywy na poziomie krajowym. Oprócz tego ma zostać ustanowiony organ służący za pojedynczy punkt kontaktowy (*single point of contact)* w dziedzinie NIS (rolę tę można oczywiście przypisać już istniejącej instytucji). Jeśli w danym kraju jest jeden organ typu *competent authority,* staje się on jednocześnie krajowym punktem kontaktowym. Punkt kontaktowy odgrywa rolę łącznika pomiędzy rządem danego kraju a powoływanymi w ramach dyrektywy sieciami współpracy (*cooperation group, sieć zespołów CSIRT*).

[41] Por. rozdział 3.1.1
[42] Por. rozdział 3.1.2

W tekście projektu dyrektywy podkreśla się, że dla prawidłowego funkcjonowania właściwych organów krajowych i punktu kontaktowego, rządy krajów członkowskich są zobowiązane do przeznaczenia odpowiednich zasobów (technicznych, finansowych, osobowych), aby można było efektywnie realizować zadania wynikające z transpozycji dyrektywy NIS. Dotyczy to także środków potrzebnych na utrzymywanie bezpiecznej łączności w ramach wspomnianych grup współpracy międzynarodowej (*cooperation group, sieć zespołów CSIRT*).

Wśród ważnych zadań organów krajowych w dziedzinie cyberbezpieczeństwa jest także:

- przyjmowanie zgłoszeń o naruszeniach bezpieczeństwa (organ właściwy lub CSIRT),
- informowanie o poważnych incydentach o charakterze ponadgranicznym (punkt kontaktowy),
- współpraca z organami ścigania oraz inspektorem ochrony danych osobowych.

Ustanawianie wymogów bezpieczeństwa i raportowanie o incydentach

Ważnymi warunkami przewidzianymi w projekcie dyrektywy jest kompetencja organów krajowych do ustanawiania odpowiednich do występującego ryzyka wymagań bezpieczeństwa, jakie mają stosować operatorzy danego sektora, a także narzucenie obowiązku zgłaszania istotnych naruszeń bezpieczeństwa do właściwych (sektorowych bądź krajowych) organów. W tym momencie warto wspomnieć, że projekt dyrektywy nie dotyczy sektora łączności (telekomunikacja) oraz operatorów tzw. usług zaufania (*ang. trust providers)*, ponieważ te sektory **zostały już objęte** podobnymi wymogami[43].

Sieci współpracy

Jak zostało wspomniane, projekt dyrektywy zakłada powstanie stałych mechanizmów współpracy w dziedzinie NIS pomiędzy krajami członkowskimi, w postaci:

- grupy współpracy (cooperation group),
- sieci zespołów CSIRT.

W pierwszym przypadku chodzi o grupę składającą się z przedstawicieli państw członkowskich, Komisji Europejskiej oraz agencji ENISA, w ramach której ma być wypracowany plan działań (tzw. *roadmapa*), służący osiąganiu celów i podejmowaniu zadań przewidzianych w dyrektywie. Grupa ta wypracowuje także strategiczne zalecenia funkcjonowania sieci zespołów CSIRT. Oprócz tego, w ramach grupy następowałaby wymiana najlepszych praktyk w zakresie wymiany informacji o incydentach i innych obszarach NIS.

[43] Art. 13a oraz 13b Dyrektywy 2002/21/EC oraz art. 19 Rozporządzenia 910/2014

Z kolei sieć współpracy zespołów CSIRT ma zadanie organizacji operacyjnego współdziałania CSIRTów krajowych. W zakresie obecnie przewidzianym w projekcie dyrektywy jest mowa o dobrowolnej wymianie informacji związanych z poszczególnymi incydentami, dyskutowanie o konkretnych incydentach na wniosek poszkodowanego kraju oraz znajdowanie sposobów skoordynowanej reakcji, dobrowolne wspieranie innych CSIRTów w reakcji na incydenty o charakterze transgranicznym, a także przygotowywanie warunków do rozszerzania współpracy operacyjnej poprzez np. przekazywanie ostrzeżeń o zagrożeniach. Informacje o zagrożeniach i incydentach powinny być także dostępne publicznie, pod warunkiem, że nie są to informacje wrażliwe, mogące powodować dodatkowe zagrożenie. Widać, że sieć CSIRT może się w praktyce okazać silnym mechanizmem wpływającym na skoordynowane działania na poziomie Unii Europejskiej w dziedzinie bezpieczeństwa cyberprzestrzeni. Poprzez obowiązek przekazywania cyklicznych raportów oraz informacji o wynikach swych prac na temat rozszerzania form współpracy może być siłą napędową pogłębiania współpracy w Europie.

Zakres podmiotowy dyrektywy

Wspomniany Załącznik II oraz III projektu dyrektywy NIS określają jej zakres podmiotowy, w kontekście typów podmiotów, które byłyby objęte zharmonizowanymi wymaganiami w zakresie bezpieczeństwa cyberprzestrzeni.

Lista typów podmiotów ewoluowała w trakcie prac nad projektem dyrektywy, a i obecnie trudno uznać, że jej kształt jest już powszechnie zaakceptowany przez kraje członkowskie. Należy przyjąć, że w dalszym ciągu prac lista będzie modyfikowana, aż do uzyskania końcowej postaci, która wyznaczy minimalny katalog sektorów, typów podmiotów, który będzie podlegał harmonizacji w kontekście bezpieczeństwa cyberprzestrzeni w Europie. Godne podkreślenia jest to, że Polska może przyjąć szerszy katalog sektorów objętych zasadami bezpieczeństwa proponowanymi w dyrektywie, chociażby włączyć obszar administracji publicznej, który paradoksalnie jest wykreślany z projektu dyrektywy. [44]

Przykładowo, zgodnie ze stanem propozycji kompromisowej projektu w lipcu 2015, lista sektorów podmiotów przedstawiała się następująco:

- sektor energetyczny,
- sektor transportu,
- sektor bankowy,
- infrastruktura rynku finansowego,

[44] W pierwotnym projekcie przedstawionym przez Komisję Europejską sektor ten znajdował się w zakresie dyrektywy

- sektor zdrowia,
- obszar związany z produkcją i dystrybucją wody pitnej,
- infrastruktura cyfrowa (digital infrastructure),
- cyfrowe platformy usługowe (digital service platforms).

W ramach poszczególnych sektorów są w projekcie wymienione typy podmiotów, na przykład **w przypadku cyfrowych platform usługowych** są to platformy e-commerce, systemy płatności internetowych, sieci społecznościowe, usługi chmurowe, sklepy z aplikacjami a nawet wyszukiwarki.

Można by się zastanawiać, czy wszystkie tego typu podmioty powinny rzeczywiście znajdować się na liście. Jednak jądrem problemu jest to, czy dany podmiot dostarcza kluczową usługę w rozumieniu dyrektywy. Nie chodzi więc o to, żeby wszystkie tego typu podmioty niezależnie od ich wielkości i wpływu na gospodarkę obarczać twardymi wymogami bezpieczeństwa, lecz by skoncentrować się na tych podmiotach (operatorach), którzy oferują usługi kluczowe czy krytyczne dla funkcjonowania państwa.

Mając na uwadze, że kilka kwestii z projektu dyrektywy będzie w dalszym ciągu przedmiotem uzgodnień i uszczegółowienia, przykładowo lista obszarów, sektorów czy typów podmiotów, kwestia zakresu terytorialnego (czy objąć dyrektywą podmioty, które nie mają siedziby na terenie UE ale świadczą tu usługi), próby doprecyzowania kryteriów pozwalających identyfikować operatorów kluczowych usług, zachodzi pytanie, **czy i ewentualnie na ile należy wstrzymywać się z pracami związanymi z opracowaniem kształtu systemu zarządzania i koordynacji działań w celu ochrony cyberprzestrzeni RP do czasu uchwalenia dyrektywy NIS.**

Odpowiedź na tak postawione pytanie nasuwa się sama. Etap wyznaczania kluczowych operatorów czy usług uzależnionych od cyberbezpieczeństwa jest etapem późniejszym w stosunku do ustanawiania prawno-organizacyjnych mechanizmów zarządzania cyberbezpieczeństwem na poziomie krajowym. Nic nie stoi na przeszkodzie, a wręcz **istnieje pilna konieczność wykonywania prac służących zaplanowaniu, a następnie ustanowieniu ram systemu ochrony cyberprzestrzeni, który musi chronić interes narodowy (bezpieczeństwo cyberprzestrzeni RP), a także uwzględnić ponadgraniczny charakter zagadnienia i tym samym uwzględnić kluczowe filary dyrektywy**, takie jak wyznaczenie krajowych organów koordynujących, punktów kontaktowych czy krajowego systemu CERTów/CSIRTów. Tak przygotowane struktury będą w stanie dokonać prawidłowej identyfikacji kluczowych sektorów, usług i operatorów czy podmiotów, posiłkując się wiedzą krajową oraz powstającymi kryteriami w ramach projektowanej dyrektywy NIS.

3.2.2 Inne dokumenty

Poniżej przedstawiono zestawienie istotnych dokumentów Unii Europejskiej dotyczących bezpieczeństwa sieci i informacji (NIS - Network Information Security):[45]

The Cybersecurity Strategy of the EU

Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, available at: http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_en.pdf

The proposal for NIS directive

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48, http://eeas.europa.eu/policies/eu-cyber-security/cybsec_directive_en.pdf

Council Conclusions on the Cybersecurity Strategy

Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, agreed by the General Affairs Council on 25 June 2013, http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf

Digital Agenda

A Digital Agenda for Europe, COM(2010)245, May, 2010

Directive on ECIs

Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

The CIIP Action Plan

The Commission Communication “Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience” COM(2009)149, available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

Commission Communication on Critical Information Infrastructure Protection

The Commission Communication on Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" adopted on 31 March

[45] na podstawie informacji ENISA

2011 and the Council Conclusion on CIIP of May 2011, http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf

Electronic Communications Regulatory Framework

Telecommunications Regulatory Package (article 13a. amended Directive 2002/21/EC Framework Directive)

Review of the Data Protection Framework

Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM 2012/11 final of 25.1.2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

Regulation on electronic identification and trusted services for electronic transactions in the internal market

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG

Commission Regulation on the measures applicable to the notification of personal data breaches

Commission Regulation (EU) No 611/2013, of 24 June 2013, on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC of the European Parliament and of the Council on privacy and electronic communications, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

Framework to build trust in the Digital single market for e-commerce and online services

European Commission, "A coherent framework for building trust in the Digital Single Market for e-commerce and online services" COM (2011)942, 11.1.2012, http://ec.europa.eu/internal_market/e-commerce/communication_2012_en.htm

Directive on attacks against information systems

Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013 replacing Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems

Communication on EC3

Commission Communication 'Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre', European Commission, COM(2012) 140 final, 28.3.2012, available

at: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/pdf/communication_european_cybercrime_centre_en.pdf

Council Resolution of December 2009 on a collaborative approach to Network and Information Security

Council resolution of 18 December, 2009 on a collaborative approach to network and information security (2009/C 321 01), available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:C:2009:321:TOC

Council conclusion on CIIP of May 2011

Council Conclusion on CIIP of May 2011, available at: http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pd

Action Plan for an innovative and competitive Security Industry

Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee regarding an Action Plan for an innovative and competitive Security Industry, COM(2012) 417 final

Single Market Act

Single Market Act – Twelve levers to boost growth and strengthen confidence "Working Together To Create New Growth", COM(2011)206 Final

Internet of Things – An Action Plan for Europe

Communication of the Commission to the Parliament, the Council, the EU Economic and Social Committee and the Committee of Regions on the Internet of Things, COM(2009)278 final of 18. June 2009.

European cloud computing strategy

The Communication COM(2012)529 'Unleashing the potential of cloud computing in Europe', adopted on 27 September 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

Internal Security Strategy for the European Union

An internal security strategy for the European Union (6870/10), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/113055.pdf

Telecom Ministerial Conference on CIIP

Telecom Ministerial Conference on CIIP organised by the Presidency in Balatonfüred, Hungary, 14-15 April 2011

Data Protection Directive

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

Digital Single Market Strategy

A Digital Single Market Strategy for Europe, COM(2015) 192 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee of the regions, May 2015, available at: http://ec.europa.eu/priorities/digital-single-market/docs/dsm-communication_en.pdf

The new ENISA Regulation (EU) No 526/2013

REGULATION (EU) No 526/2013 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, available at: http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=OJ:L:2013:165:TOC

3.3 Aspekt skoordynowanego procesu raportowania o naruszeniach bezpieczeństwa w różnych sektorach i obszarach

Zgłaszanie istotnych naruszeń bezpieczeństwa jest jednym z istotnych elementów ogólnie pojmowanego systemu bezpieczeństwa w cyberprzestrzeni Unii Europejskiej. W wielu dokumentach Unii Europejskiej znajdują się odniesienia do kwestii wprowadzania takiego obowiązku dla uczestników komunikacji elektronicznej w różnych sektorach czy obszarach. Przykładem jest dyrektywa ramowa w telekomunikacji (2009/140/WE), dyrektywa *e-Privacy* (2002/58/EC), rozporządzenie e-IDAS, czy planowane: dyrektywa NIS oraz rozporządzenie o ochronie danych osobowych.

Kwestii kompleksowego podejścia do tematu zgłaszania incydentów w różnych sektorach i obszarach zależnych od technologii teleinformatycznych poświęcone jest opracowanie ENISA *Cyber Incident Reporting in the EU* [46] z roku 2012.

W opracowaniu podkreśla się, że w wielu krajach europejskich (ale oczywiście także poza Europą) w ostatnich latach wdrażane są obowiązkowe lub dobrowolnie stosowane schematy raportowania o incydentach. Jest to element monitorowania sytuacji cyberbezpieczeństwa kraju, reagowania na incydenty, tworzenia statystyk i podejmowania odpowiednich działań na

[46] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu

przyszłość (np. w ramach określania celów w krajowych strategiach ochrony cyberprzestrzeni).

Oczywiście istnieją duże różnice w podejściu poszczególnych krajów, jednak podkreśla się, że przyjęcie w Europie wspólnych pryncypiów w dziedzinie bezpieczeństwa cyberprzestrzeni (w tym także reagowania na incydenty) jest sprawą kluczową, chociażby z powodu istnienia wspólnego rynku oraz transgranicznego charakteru, z jednej strony usług a z drugiej zagrożeń i incydentów bezpieczeństwa.

Komisja Europejska dąży do zaproponowania w powstających dyrektywach i rozporządzeniach dotyczących rynku cyfrowego postanowień pewnego wspólnego schematu opierającego się na dwóch podstawowych filarach:

- wymogu zapewniania odpowiednich środków bezpieczeństwa,
- wymogu zgłaszania naruszeń (incydentów bezpieczeństwa).

Najwcześniej zmiany te zaczęto wprowadzać w telekomunikacji. I tak w roku 2009 wprowadzono odpowiednie zapisy do pakietu dyrektyw w ramach reformy rynku telekomunikacyjnego (w szczególności w dyrektywie 2009/140/WE)[47]. To posunięcie wymusiło także zmianę w dyrektywie *e-Privacy*, która dotyczy zagadnień ochrony danych osobowych i prywatności odnośnie sieci komunikacji elektronicznej. Także rozporządzenie eIDAS przyjęte w roku 2014, a dotyczące zagadnień identyfikacji elektronicznej oraz usług zaufania w odniesieniu do transakcji elektronicznych zawiera w artykule 19 *"Security requirements applicable to trust service providers"* postanowienia odnośnie zapewniania środków bezpieczeństwa przez operatorów usług zaufania oraz zgłaszania naruszeń bezpieczeństwa do odpowiednich organów.

Obecnie w Unii Europejskiej jest przygotowywana reforma dotycząca ochrony danych, która ma zastąpić dyrektywę z roku 1995 (95/46/EC). Przygotowywane rozporządzenie będzie dotyczyło podmiotów, które przetwarzają dane osobowe, niezależnie od tego, w jakim sektorze się znajdują. Postanowienia odnośnie stosowanych środków bezpieczeństwa oraz kwestii zgłaszania naruszeń także i w tym dokumencie zajmują swoje poczesne miejsce i przypominają znane schematy, stosowane wcześniej:

- podmioty przetwarzające dane osobowe muszą wdrożyć odpowiednie środki bezpieczeństwa (techniczne i organizacyjne) adekwatnie do ryzyka,
- obowiązkowe jest zgłaszanie naruszeń bezpieczeństwa danych osobowych we wszystkich sektorach,
- zgłaszanie incydentów do odpowiednich organów ma być realizowane bez zbędnej zwłoki (w ciągu 24 godzin),

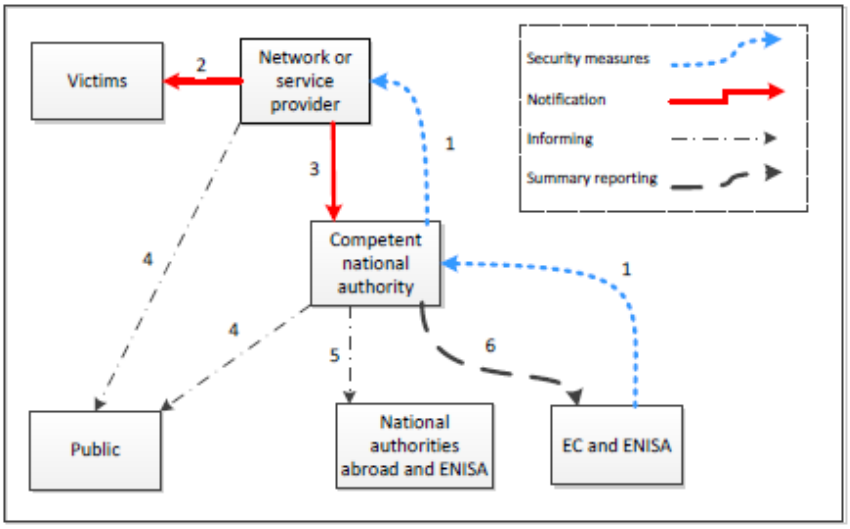
[47] Patrz także rozdział:3.1.3

– o naruszeniach bezpieczeństwa danych osobowych muszą być informowani użytkownicy, jeśli jest podejrzenie, że mogło to spowodować naruszenie ich prywatności[48].

W przygotowanej w roku 2013 Europejskiej Strategii Cyberbezpieczeństwa Komisja Europejska zawarła propozycję rozszerzania mechanizmów zapewniania bezpieczeństwa i integralności sieci i usług znanych i wdrożonych w sektorze telekomunikacyjnym (opisanych w art. 13a pakietu telekomunikacyjnego) na inne sektory, w szczególności te krytyczne, takie jak: energetyka, sektor finansowy, transportu, gospodarki wodnej. Dalszym krokiem, przewidzianym w tejże strategii jest przygotowanie tzw. dyrektywy NIS, w której koncepcje powyższe zostają rozwinięte.

Różne środowiska – podobny model

Biorąc pod uwagę potrzeby związane z zapewnieniem odpowiednich mechanizmów i procesów dla różnych obszarów i sektorów, w szczególności w aspekcie raportowania o naruszeniach, ENISA ilustruje to za pomocą poniższego, uproszczonego diagramu.



Rysunek 6. Uproszczony schemat procesów związanych z raportowaniem o naruszeniach i określaniem środków bezpieczeństwa. Źródło: ENISA.

Niebieskie linie ilustrują procesy rekomendowania czy narzucania standardów dotyczących wymagań bezpieczeństwa. Komisja Europejska przy pomocy ENISA opracowuje rekomendacje dotyczące środków bezpieczeństwa (minimalnych), jakie powinny być stosowane, aby można było mówić o zharmonizowanym podejściu. Te rekomendacje

[48] Nie jest to konieczne, jeśli dane były w odpowiedni sposób zaszyfrowane

powinny służyć krajowym organom, które w danym sektorze czy obszarze definiują wymagania dla usługodawców.

Czerwone linie ilustrują obowiązek informowania właściwych organów oraz użytkowników (ofiar incydentów) o istotnych naruszeniach, które miały miejsce.

Gruba, czarna przerywana linia ilustruje coroczne przekazywanie do KE i ENISA raportów przez organy krajowe.

Cienka czarna, przerywana linia ilustruje procesy informowania przez właściwe organy krajowe o incydentach – odpowiednie organy w innych krajach członkowskich oraz ENISA a także informowanie publiczne.

Można uznać, że powyższy schemat jest rekomendowany, jeśli mówimy o podstawowych filarach bezpieczeństwa ICT (ang. *information and communication technologies*) w kontekście zapisów regulacyjnych. Jest istotne, aby mieć świadomość, że w istocie jest to cykl działań, czyli na podstawie informacji i doświadczeń zbieranych w ramach powyższego schematu, rekomendacje co do standardowych wymagań bezpieczeństwa powinny być okresowo aktualizowane.

Schemat jest oczywiście uproszczony, bo między innymi nie uwzględnia, że może być kilka organów przyjmujących zgłoszenia i określających minimalne wymagania bezpieczeństwa, w zależności od sektora. Na przykład obecnie w Polsce MAC wraz z UKE odpowiada za telekomunikację, GIODO za dane osobowe, Ministerstwo Gospodarki za wdrażanie rozporządzenia eIDAS. Jednak w innych krajach spotyka się rozwiązania, że regulator telekomunikacji jest pojedynczym punktem kontaktowym dla sektora (także w zakresie przyjmowania zgłoszeń dotyczących naruszeń danych osobowych w telekomunikacji).

Także nie we wszystkich przypadkach (schematach) przewidzianych przez poszczególne dyrektywy albo rozporządzenia występują wszystkie procesy. Niemniej jednak model ten stanowić może bazę dla wdrażania całościowego systemu cyberbezpieczeństwa w kraju, tym bardziej, że regulacje europejskie mówią o pewnym minimalnym poziomie do zaimplementowania, a więc każdy kraj może (i często powinien) wdrażać pełniejszy model bezpieczeństwa.

3.3.1 Schematy zgłaszania naruszeń – konkluzje

Wdrażanie odpowiednich środków bezpieczeństwa i zgłaszanie przypadków naruszeń to istotny element w podnoszeniu cyberbezpieczeństwa. Unia Europejska proponuje bądź wymusza stosowanie pewnego standardowego podejścia, opisanego w niniejszym rozdziale,

w celu harmonizacji obszaru w Europie. Z pewnością, harmoniazcja ta jest jeszcze daleka od doskonałości i wymaga wielu zabiegów w celu uszczegóławiania zapisów poszczególnych regulacji w kontekście rozwoju technologii oraz coraz bardziej złożonych incydentów naruszających bezpieczeństwo ICT.

- Istnieje wiele podobieństw w poszczególnych regulacjach odnośnie raportowania o naruszeniach oraz określania wymagań bezpieczeństwa dla uczestników rynku komunikacji elektronicznej. Powoduje to możliwość, a nawet konieczność, przyjęcia zharmonizowanego podejścia na poziomie kraju.
- Ważną kwestią do rozstrzygnięcia jest podjęcie decyzji, czy zgłaszanie incydentów do właściwych organów (CERTów, regulatorów itp.) powinno być dobrowolne czy obowiązkowe. Ogólna tendencja, oparta na doświadczeniach z ostatnich kilku lat (sektor telekomunikacji) dąży do narzucania obowiązku zgłaszania, bowiem w przeciwnym przypadku nie ma mowy o zdobyciu wiarygodnego obrazu stanu bezpieczeństwa w kraju oraz o właściwych działaniach prewencyjnych.
- Samo zgłaszanie naruszeń nie jest jednak wystarczającym środkiem zaradczym. Równie ważne jest ustanawianie minimalnych czy optymalnych wymogów bezpieczeństwa (na podstawie procesów analiz ryzyka i wiedzy na temat zagrożeń oraz technologii zabezpieczających). Różne sektory mają niewątpliwie swoją specyfikę, którą należy uwzględniać przy określaniu wymogów bezpieczeństwa na poziomie krajowym.
- Ustanawianie wymogów bezpieczeństwa dla danego sektora czy obszaru powinno uwzględniać dialog organów regulacyjnych czy tworzących prawo krajowe z przedstawicielami danego sektora. Jest z drugiej strony istotnym, aby zapisy nie były zbyt ogólne i nie pozostawiały wątpliwości interpretacyjnych. Należy zadbać, by przedsiębiorcy mieli odpowiednie przepisy i wskazówki (poradniki), co i jak wdrażać, aby funkcjonować zgodnie z przepisami, nie tylko w zapisach dokumentacji ale i w praktyce.
- Na poziomie krajowym powinny istnieć zdefiniowane (obowiązkowe) mechanizmy współpracy pomiędzy organami (szczebla krajowego, sektorowymi), aby reguły bezpieczeństwa były spójne, obowiązki nie nakładały się lub, co gorsza, były ze sobą sprzeczne.

Należy podkreślić różnicę pojęciową pomiędzy reakcją na incydenty (ang. *incident response*) a obowiązkowym zgłaszaniem naruszeń do właściwych organów nadzorujących dany obszar czy sektor (ang. *mandatory incident reporting*). Reagowanie na incydenty jest procesem czasu rzeczywistego, który wymaga natychmiastowej współpracy na poziomie technicznym z odpowiednimi zespołami reagującymi (CSIRT, CERT), po to, aby dany incydent obsłużyć (zniwelować jego rozprzestrzenianie się i skutki, jakie powoduje). Natomiast zgłaszanie naruszeń do kompetentnych krajowych organów (np. regulatora danego sektora rynku) jest procesem koniecznym dla oceny kondycji danego sektora czy obszaru pod kątem bezpieczeństwa i spełniania wymagań.

4 Kluczowe obowiązki w zakresie zarządzania bezpieczeństwem sieci i informacji systemów teleinformatycznych

Zarządzanie ryzykiem to proces, którego zadaniem jest przyczynianie się do podejmowania racjonalnych decyzji strategicznych w celu utrzymania ryzyka na przyjętym jako akceptowalny poziomie. W tym kontekście racjonalność rozumiana jest jako metoda takiego podejmowania decyzji, by zaangażować minimalne, co do idei ograniczone bądź rzadkie, nakłady i działania w celu osiągnięcia założonego efektu. Racjonalnym jest wyjątkowo dobrze chronić rzeczy wyjątkowo ważne. Racjonalnym jest nie wydawać na ochronę systemu więcej niż wynieść może maksymalna szkoda powstała w wyniku niewdrożenia planowanego zabezpieczenia. Nie jest też racjonalnym budowanie bardzo drogich systemów informatycznych bez poczynienia istotnych nakładów na ich adekwatne zabezpieczenie. Wreszcie nie jest racjonalnym niedbanie o bezpieczeństwo systemów ważnych, czy też zakładanie, że taka troska może zachodzić bezkosztowo.

Aby móc ustalać, czy poziom ryzyka mieści się poniżej przyjętego progu należy co najmniej ustalić ten próg oraz znaleźć metodę szacowania ryzyka. Na potrzeby szacowania ryzyka niezbędne jest ustalenie dziedziny szacowania, czyli inwentaryzacja zasobów oraz inwentaryzacja możliwych typów zagrożeń. Jakość szacowania ryzyka polepszy uwzględnienie miary istotności poszczególnych zasobów oraz przyjęcie realistycznych prawdopodobieństw zmaterializowania się poszczególnych typów ryzyk, choćby na podstawie danych historycznych, danych z innych krajów czy analizy trendów.

4.1 Sposób organizacji systemu zarządzania ryzykiem teleinformatycznym i zakres podmiotów zobowiązanych do jego prowadzenia

Szacowanie ryzyka jest zagadnieniem, w którym pojęcia podstawowe nie mają jednoznacznej definicji, czy raczej ich definicji jest wiele. Na potrzeby niniejszego dokumentu przyjmuje się następującą opisową interpretację dwóch zasadniczych dla zagadnienia pojęć, ryzyko i zarządzanie ryzykiem:

Ryzyko, miara zagrożenia, rozumiana jako miara wystąpienia zdarzenia, które może doprowadzić do strat. Ryzyko jako miara jest zasadniczo wprost proporcjonalne do

prawdopodobieństwa wystąpienia związanego z nim zagrożenia oraz wprost proporcjonalne do wielkości straty, którą wystąpienie danego zdarzenia implikuje.

Zarządzanie ryzykiem, skoordynowane działania dotyczące kierowania i nadzorowania organizacją w odniesieniu do ryzyka (definicja z ISO 31000:2009). Proces zarządzania ryzykiem powinien obejmować co najmniej następujące aktywności: szacowanie ryzyka, monitorowanie ryzyka oraz postępowanie z ryzykiem. Zarządzanie ryzykiem jest z natury procesem ciągłym a nie działaniem jednorazowym.

4.1.1 Analiza stosowanych dokumentów pod względem zarządzania ryzykiem

Poniżej odniesiono się do treści istniejących dokumentów, które w pewnym aspekcie dotyczą zarządzania ryzykiem i są w dzisiejszej praktyce wykorzystywane przez różne podmioty bądź z mocy prawa, bądź przyjętej pragmatyki. Analiza obejmuje następujące dokumenty:

1. Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej, opracowana w Ministerstwie Administracji i Cyfryzacji we współpracy z Agencją Bezpieczeństwa Wewnętrznego;
2. Metodyka szacowania ryzyka na potrzeby systemów jawnych, opracowana przez Zespół CERT.GOV.PL;
3. Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego, opracowany przez Rządowe Centrum Bezpieczeństwa;
4. Sprawozdanie z szacowania ryzyka cyberprzestrzeni w administracji rządowej w 2013 r., przygotowane w Ministerstwie Administracji i Cyfryzacji;
5. Koncepcja i założenia do metodyki oceny ryzyka i przygotowania sprawozdania dotyczącego cyberbezpieczeństwa, opracowane w Ministerstwie Administracji i Cyfryzacji.

W kolejnych sekcjach opisano syntetycznie zawartość z punktu widzenia szacowania ryzyka oraz ewentualne wnioski na potrzeby niniejszej analizy w powyższych dokumentach.

4.1.2 Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej

Zgodnie z zapisami Polityki, celem strategicznym jest osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni Państwa, a działania podejmowane na rzecz realizacji celu strategicznego są wynikiem oszacowań ryzyka prowadzonych przez uprawnione podmioty w odniesieniu do zagrożeń występujących w cyberprzestrzeni.

W zakresie zarządzania ryzykiem polityka koncentruje się na zbieraniu informacji, w niewielkim stopniu sugerując, jakie działania na poziomie strategicznym, w szczególności związane z wydatkowaniem środków budżetowych, mają być podjęte na podstawie obrazu,

który minister właściwy ds. informatyzacji ma uzyskiwać regularnie do końca stycznia każdego roku kalendarzowego. Sprawozdania powinny zawierać ogólne dane dotyczące rodzajów ryzyka, zagrożeń i słabych punktów zdiagnozowanych w każdym z sektorów, w których poszczególna instytucja działa i za które odpowiada. W sprawozdaniu powinny być przedstawione informacje o sposobach postępowania z ryzykiem.

Dokument zapowiada określenie przez ministra właściwego ds. informatyzacji jednolitej metodyki przeprowadzania analizy ryzyka oraz zaleca zespołowi CERT.GOV.PL przedstawienie katalogów zawierających specyfikację zagrożeń oraz możliwych podatności godzących w bezpieczeństwo cyberprzestrzeni.

W praktyce dokument zaznacza jako element polityki aspekt zarządzania ryzykiem definiując jednak w tym zakresie jedynie zobowiązana opracowania kolejnych dokumentów, które mają bezpośrednio dotyczyć zarządzania ryzykiem, w tym dokumentów obejmujących metodykę zarządzania ryzykiem oraz słownikowych zestawień katalogów zagrożeń.

4.1.3 Metodyka szacowania ryzyka na potrzeby systemów jawnych

Zespół CERT.GOV.PL w ABW przygotował propozycję szacowania ryzyka na potrzeby systemów jawnych, które zgodnie z dokumentem Polityki ochrony cyberprzestrzeni RP powinno być przeprowadzone w administracji rządowej. Metodyka zaproponowana przez ABW wykorzystuje elementy hiszpańskiej metodyki Magerit i tu obejmuje:

- rozpisany na etapy proces szacowania ryzyka,
- katalog zagrożeń teleinformatycznych,
- uwzględnienie mechanizmów przeciwdziałających,
- metodę oceny zastosowanych zabezpieczeń,

Szacowanie ryzyka wedle proponowanej metody obejmuje kolejno:

1. identyfikację zasobów i ustalenie ich istotności pod kątem cech stanowiących bezpieczeństwo, czyli dostępności, integralności i poufności. Istotność zasobu jest definiowana w pięciu klasach operujących na 11 wartościach, od małej do najwyższej wartości zasobu i od 0 do 10 punktów.
2. wyznaczenie przez kierownika jednostki wartości zagrożenia dla każdego zasobu w trójstopniowej skali zagrożenia (od niskie do wysokie, a zarazem od 1 do 10 punktów),
3. uwzględnienie mechanizmów przeciwdziałania skutkujące wyznaczeniem aktualnego poziomu zagrożenia określanego również ryzykiem szczątkowym,
4. na podstawie ryzyk szczątkowych wyznaczenie wartości poszczególnych ryzyk, cały czas z podziałem na dostępność, integralność i poufność.

Końcowy etap ryzyka ma stanowić analiza uzyskanych wyników pod kątem możliwych do zaimplementowania potrzebnych środków zaradczych mających na celu zmniejszenie ryzyka do poziomu akceptowalnego. Jest to rekomendowane szczególnie w stosunku do systemów, których wyznaczone ryzyko znajduje się w przedziale *wysokie*. Takie sformułowanie implikuje domyślnie prawdopodobieństwo podjęcia dodatkowych działań, ale i również wydatkowania dodatkowych środków na podstawie analizy ryzyka.

Zaproponowana metodyka wydaje się być przydatna i wysoce praktyczna dla pewnej klasy zagrożeń. Mianowicie, gdy ryzyko ocenia się poprzez ryzyka każdego ze zinwentaryzowanych systemów analizując potencjalne podatności. Należy jednak podkreślić, że unifikacja podejścia i uproszczenie modelu ma również swoje wady. Przykładowo, nie zawsze rozróżnianie dostępności, integralności i poufności jest racjonalne. Nie zawsze też zasadnym jest wyznaczanie wartości ryzyka poprzez uśrednianie ryzyk szczątkowych. Czasem obowiązywać powinna analogia do najsłabszego ogniwa w łańcuchu – jakość, odporność czy wytrzymałość złożonego systemu jest tak duża jak stosowna cecha jego najsłabszego elementu składowego – szczególnie, jeżeli rozpatrywalibyśmy krótką listę istotnie krytycznych systemów teleinformatycznych państwa.

4.1.4 Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego

Jest do dokument Rządowego Centrum Bezpieczeństwa, którego ma uzasadniać ocenę ryzyka zagrożeń, ustalać aktorów i organizację procesu, przedstawiać metodę oceny oraz opisać zagrożenia. Głównym materiałem źródłowym jest niejawny dokument Raport o zagrożeniach bezpieczeństwa narodowego przyjęty uchwałą Rady Ministrów. Działania RCB w przedmiotowym zakresie reguluje przede wszystkim Ustawa o zarządzani u kryzysowym z dnia 26 kwietnia 2007 r. oraz Rozporządzenie w sprawie Raportu o zagrożeniach bezpieczeństwa narodowego z dnia 30 kwietnia 2010 roku.

Na potrzeby Raportu o zagrożeniach bezpieczeństwa narodowego przygotowywane są raporty cząstkowe. Metodyka opracowywania raportu głównego i raportów cząstkowych obejmuje wypełnianie przez zaangażowane w wytwarzanie raportu podmioty następujących zakładek w postaci arkusza kalkulacyjnego: zagrożenia, zapobieganie, przygotowanie, reagowanie, dane historyczne. Wśród rozpatrywanych skutków występują również skutki dla infrastruktury krytycznej, w tym objętych tą definicją sieci teleinformatycznych – jako jedynego elementu cyberprzestrzeni objętego zgodnie z ustawą definicją infrastruktury krytycznej.

Dla każdego z zagrożeń rozpatruje się prawdopodobieństwo wystąpienia ryzyka w skali pięciostopniowej (bardzo rzadkie – bardzo prawdopodobne) oraz pięciostopniową skalę

oceny skutków (nieistotne – katastrofalne) z rozróżnieniem charakteru skutku: dla życia i zdrowia, dla mienia bądź dla środowiska. Wyznaczona wartość ryzyka następnie etykietuje się poziomem jego akceptowalności, skala czterostopniowa (od akceptowalne przez tolerowalne i warunkowo tolerowalne do nieakceptowalne). Poziom akceptacji ryzyka powinien następnie być pisemnie uzasadniony. W raporcie głównym wyróżniono około 50 typów zagrożeń, przy czym 18 z nich zawarto w Krajowym Planie Zarządzania Kryzysowego, wśród nich zagrożenie *cyberterroryzm*. Następnie w dokumencie - wyliczając i omawiając 18 zagrożeń, gdy dochodzi do omówienia ataków cybernetycznych - konkretnie pisze się jedynie o możliwych skutkach ataków cybernetycznych, dla ludzi i w mieniu.

Jako potencjalne skutki dla ludności wymienia się:

- zagrożenie dla życia i zdrowia ludzi spowodowane zakłóceniami systemów energetycznych, sterowania ruchem, itp.,
- utratę zaufania do instytucji publicznych,
- brak możliwości realizacji zadań merytorycznych,
- brak możliwości komunikacji.

Jako potencjalne skutki dla mienia wymienia się tak zasadnicze punkty:

- znaczące straty finansowe i gospodarcze oraz skutki społeczne,
- zakłócenia zaopatrzenia w energię, paliwa, żywność, wodę pitną,
- zakłócenia pracy infrastruktury przesyłowej.

W rzeczywistości z założenia dostępny jako dokument publiczny na stronie RCB Plan Zarządzania Kryzysowego w części drugiej „Zespół przedsięwzięć na wypadek sytuacji kryzysowych" w ogóle pomija działkę odnoszącą się wcześniej do ogólnie opisanej pozycji z podanymi powyżej skutkami „Zagrożenia cyberprzestrzeni".

Zarządzanie kryzysowe obejmuje wprawdzie swoim zakresem sieci teleinformatyczne, ale bardziej jako jeden z typów sieci przesyłowych i zarazem w ogóle nie uwzględnia warstwy udostępniania, przetwarzania i przechowywania informacji, która przenika wszelkie aspekty funkcjonowania państwa.

4.1.5 Sprawozdanie z szacowania ryzyka cyberprzestrzeni w administracji rządowej w 2013 r.

W dokumencie przyjęto następujące główne kategorie i podkategorie zagrożeń:

1. zagrożenia ukierunkowane na informacje,
    a. kradzież informacji celem publikacji bądź sprzedaży,
    b. fałszowanie informacji,
2. zagrożenia ukierunkowane na infrastrukturę teleinformatyczną,

a. usunięcie danych,
b. zakłócenie funkcjonowania,
c. przejęcie systemu teleinformatycznego,

3. awarie IT,
4. niedostateczne kompetencje.

Ponadto wprowadzono rozróżnienie w rejestrze zagrożeń na zagrożenia wewnętrzne i zewnętrzne – z punktu widzenia wypełniających zestawienia instytucji. Zawarte w dokumencie rekomendacje objęły między innymi:

- jako najpilniejsze zadanie ustanowienie i doskonalenie zasad zarządzania usługami, incydentami i problemami, aby zapobiec naruszeniom bezpieczeństwa zewnętrznej infrastruktury teleinformatycznej,
- celem przeprowadzenia szacowania ryzyka bezpieczeństwa cyberprzestrzeni zbudowanie wiedzy na temat krytycznych systemów teleinformatycznych użytkowanych w administracji państwowej,
- skuteczność egzekwowania obowiązków sprawozdawczych,
- konieczność uwzględnienia w planowaniu budżetu ministerstw, a więc budżetu państwa, potrzeb związanych z koniecznością zapewniania właściwego poziomu bezpieczeństwa,
- konieczność organizowania szkoleń dotyczących cyberbezpieczeństwa oraz kontrolę kompetencji pracowników w tym względzie.

Ostatnią rekomendacją było wskazanie, że metodyka szacowania ryzyka powinna obejmować szacunki kosztów, zarówno dotyczących mechanizmów ochronnych, technicznych i proceduralnych, jak i kosztów podnoszenia kwalifikacji zawodowych pracowników w zakresie bezpieczeństwa teleinformatycznego.

Dokument zasadnie wskazywał, że w procesie szacowania ryzyka, poza zbieraniem informacji o ryzyku, jego prawdopodobieństwie i krytyczności, należy również dążyć do szacowania kosztów niezbędnych do poniesienia w celu utrzymania właściwego poziomu zabezpieczeń.

4.1.6 Koncepcja i założenia do metodyki oceny ryzyka i przygotowania sprawozdania dotyczącego cyberbezpieczeństwa

Dokument MAC dotyczący 2014 roku wskazywał jako cel przeprowadzenia analizy ryzyka i sprawozdawczości realizację systemowych, horyzontalnych i systematycznych działań zapewniających i podnoszących bezpieczeństwo w cyberprzestrzeni.

4.1.7 Rekomendacja systemu zarządzania ryzykiem teleinformatycznym

Jakość funkcjonowania systemu zarządzania ryzykiem teleinformatycznym będzie zależeć między innymi od następujących czynników:

- racjonalności przyjętej metody zarządzania ryzykiem. Gdy zbiera się zbyt mało informacji niewiele można z niej wywnioskować. Gdy usiłuje się zebrać zbyt dużo informacji, ta obarczana jest w coraz większym stopniu błędem nietrafionych niemerytorycznych wycen,
- zebranych doświadczeń i wieloletniego doskonalenia wdrożonej metodyki. Największym wyzwaniem jest uzyskanie wartościowych jakościowo danych do raportów cząstkowych – by uzyskać dobre odpowiedzi, należy zadawać dobre pytania – ale jedynie kompetentnym osobom a nie wszystkim i wszędzie. Sam fakt masowości zadawania zbyt specjalistycznych pytań wręcz niekorzystnie wpłynie na jakość i wiarygodność udzielonych odpowiedzi,
- realnego przełożenia bieżącej identyfikacji zagrożeń o poziomie zagrożenia większym niż ryzyko akceptowalne na podjęcie konkretnych działań przez różne podmioty, niekoniecznie bezpośrednio zaangażowane w proces oceny ryzyka,
- gotowości finansowej państwa do dokonywania inwestycji zmniejszających ryzyko szczątkowe do poziomów akceptowalnych.

Pozostałe rekomendacje dotyczące szacowania ryzyka:

- trudno będzie przekonać się, czy ostatecznie wybrana metodyka będzie lepsza od wszystkich propozycji konkurencyjnych, nie ma czasu na wdrożeniowe eksperymenty porównawcze - jednak pewnym jest, że nawet wysoce niedoskonała ale za to wdrożona metoda zarządzania ryzykiem, czyni poziom bezpieczeństwa cyberprzestrzeni państwa wyższym niż nieposiadanie żadnej metody zarządzania ryzykiem,
- zasadniczą rolę, jeżeli chodzi o realne pozytywne oddziaływanie całego procesu zarządzania ryzykiem na uzyskiwany poziom bezpieczeństwa cyberprzestrzeni będzie mieć znajdująca swoje odzwierciedlenie w ustawie budżetowej gotowość państwa do ponoszenia kosztów na inwestycje niezbędne z punktu widzenia minimalizacji ryzyk o nieakceptowalnym poziomie. Należy podkreślić, że bez realnego finansowania i budżetu jako mechanizmu minimalizacji ryzyka, nie da się zapewnić akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni, a wszelkie działania będą co do zamierzonego skutku nieefektywne,
- metody zarządzania ryzykiem na rzecz infrastruktury krytycznej nie nadają się do bezpośredniego przeniesienia na rzecz zarządzania ryzykiem w ochronie cyberprzestrzeni. Rozwiązania zapisane w regulacjach dotyczących zarządzania ryzykiem infrastruktury krytycznej państwa silnie uwzględniają terytorialność,

lokalizacje i sięganie do danych historycznych na poszczególnych obszarach. Rozwiązania te w silnym stopniu angażują hierarchicznie lokalne władze samorządowe – ten aspekt wydaje się w kontekście zagrożeń dla/z cyberprzestrzeni mało istotny,

- poza inwentaryzacją systemów teleinformatycznych niezbędna jest strategiczna priorytetyzacja istotności poszczególnych zinwentaryzowanych systemów. Proponowaną miarą istotności może być szacunek możliwych strat ponoszonych przez państwo na skutek wystąpienia każdego z analizowanych typów zagrożeń,
- analizowane metody szacowania ryzyka zasadniczo opierają się w swoich wyliczeniach na wzorach angażujących jedynie różne formy średnich ważonych. Tymczasem na poziomie strategicznym z punktu widzenia funkcjonowania państwa, niefunkcjonowanie któregokolwiek z systemów rzeczywiście krytycznych w wymiarze zarządzania informacją w państwie (a liczba takich systemów musi być na potrzeby szacowania ryzyka silnie ograniczona, tylko do kilku kluczowych systemów) to rzeczywista katastrofa a nie stan jakkolwiek akceptowalny.
- Stąd propozycja, by ryzyko na najwyższym poziomie było wyliczane jako kondycja najsłabszego ze zidentyfikowanych jako krytyczne dla państwa systemów teleinformatycznych, z ograniczonym uwzględnieniem spełniania pewnych ogólnych wymagań dotyczących bezpieczeństwa przez wszystkie pozostałe, niekrytyczne aczkolwiek ważne systemy państwa,
- przy zbieraniu informacji na rzecz wyceny ryzyka unifikacja na pewnym poziomie ogólności jest wskazana, jednak nie należy próbować tworzyć doskonale szczegółowo zunifikowanych wyłącznych katalogów zagrożeń i przewidywanych środków zaradczych. Zagadnienie obejmuje zbyt różnorodną materię, by przesadne sformalizowanie nie miało doprowadzić do trudności i pomyłek w zbieraniu danych, wycenie ryzyka, a ponadto do statystycznego rozmywania i zaburzania wartościowych fachowych odpowiedzi poprzez masowość zebranych odpowiedzi na to samo pytanie, czy wycen tych samych zagrożeń, przez osoby z danym problemem na co dzień nie mające żadnych doświadczeń,
- nie należy stosować zbyt rozbudowanych skal miary ryzyka, bo są zwyczajnie niepraktyczne. Wydaje się, że nigdzie nie należy przekraczać poziomu co najwyżej skali pięciowartościowej. Ocena ryzyka z natury jest i tak obarczona bardzo dużym marginesem błędu, nie ma też jednoznacznie skutecznych metod weryfikacji jakości procesu oceny ryzyka,
- szacowanie ryzyka ma na celu nie tyle wytworzenie kolejnych dokumentów sprawozdawczych, ale ma wspomagać dysponenta budżetu (na zapewnianie odpowiedniego poziomu bezpieczeństwa cyberprzestrzeni) we właściwym

przeznaczaniu środków finansowych na bezpieczeństwo teleinformatyczne w kolejnym roku budżetowym,

- w sytuacjach nagłych i krytycznych musi istnieć szybka ścieżka raportowania i podejmowania decyzji na absolutnie najwyższych szczeblach państwowych.

4.2 Mechanizmy tworzenia krajowego rejestru ryzyka

W państwie powinna być jednoznacznie wyznaczona rola dedykowanego stanowiska odpowiedzialnego za zarządzanie i koordynację bezpieczeństwa teleinformatycznego. By działać skutecznie, powinna to być funkcja nie niższa niż podsekretarza stanu, a zarazem ze względu na rzeczywisty charakter operacyjny, niekoniecznie funkcja ministra konstytucyjnego. Stąd rekomendacja, by stanowiskiem odpowiedzialnym w rządzie za bezpieczeństwo teleinformatyczne, w tym zarządzanie ryzykiem i prowadzenie krajowego rejestru ryzyka dla zagrożeń cyberprzestrzeni oraz operacyjne zarządzanie powiązaną z nim częścią budżetu państwa, było stanowisko dedykowanego wiceministra w stosownym ministerstwie.

Na dzień dzisiejszy, wbrew powszechnemu przekonaniu odpowiedzialność za bezpieczeństwo teleinformatyczne nie jest precyzyjnie przypisana w ustawie o działach. Stanowisko to utożsamia się ze stanowiskiem osoby odpowiedzialnej za dział informatyzacja państwa, w Ministerstwie Administracji i Cyfryzacji, natomiast zarówno sama materia informatyzacji i bezpieczeństwa cyberprzestrzeni nie są tożsame formalnie, jak i znane są opinie ze strony MAC kwestionujące w bieżącym stanie prawnym odpowiedzialność ministra właściwego ds. informatyzacji za bezpieczeństwo teleinformatyczne. Ta kwestia wymaga precyzyjnego uściślenia przy okazji ustalenia dysponenta środków budżetu państwa na bezpieczeństwo teleinformatyczne.

W docelowym modelu minister właściwy ds. bezpieczeństwa teleinformatycznego odpowiada za zarządzanie krajowym rejestrem ryzyk teleinformatycznych oraz dysponuje budżetem na prowadzenie rejestru oraz na co najmniej współfinansowanie długofalowych ale i doraźnych działań w różnych aspektach funkcjonowania państwa, niezbędnych do praktycznego obniżania ryzyk teleinformatycznych zidentyfikowanych jako ryzyka z nieakceptowalnie wysokim poziomem zagrożeń.

Zadaniem ministra jest zatem nie tylko prowadzenie rejestru ryzyk, ale przede wszystkim doprowadzanie do zmniejszania poziomu występujących ryzyk do założonego poziomu akceptowalnego, również poprzez doraźne wydatkowanie środków publicznych.

Minister właściwy ds. bezpieczeństwa teleinformatycznego powinien gromadzić zapotrzebowania na działania i środki zgłaszane w ramach procesu zbierania danych z różnych instytucji na rzecz szacowania ryzyka i aktualizacji rejestru ryzyka. Zebrane

zapotrzebowania powinny być priorytetyzowane i następnie stanowić uzasadnienie dla wkładu zapotrzebowania finansowego zgłaszanego przez dysponenta krajowego rejestru ryzyka do projektu ustawy budżetowej na rok następny.

5 Analiza i zdefiniowanie roli zespołów CSIRT

5.1 CERT vs. CSIRT

Dla zespołów reagowania na incydenty komputerowe używa się powszechnie określeń: CERT lub CSIRT.

Określenie CERT pochodzi od amerykańskiego zespołu, który powstał w 1988 roku w Software Engineering Institute (SEI) przy Uniwersytecie Carnegie Mellon (CMU) w Pittsburghu i jest znakiem handlowym zarejestrowanym przez ten uniwersytet. Choć powstało ono jako akronim angielskiego *Computer Emergency Response Team*, CMU nakazuje traktowanie go jak nazwy własnej, a nie jak rzeczownik powszechny oznaczający zespół reagujący na incydenty. Wykorzystanie słowa „CERT" w nazwie innego zespołu także możliwe jest formalnie wyłącznie na podstawie zgody wyrażonej przez CMU[49]. Należy zwrócić uwagę również na inne rozwinięcia terminu CERT - np. *Computer Emergency Readiness Team*, jak w przypadku US-CERT, które zawężają zakres działalności zespołu.

Z powyższych względów, na potrzeby niniejszej ekspertyzy korzystamy z określenia CSIRT (ang. *Computer Security Incident Response Team*) w odniesieniu do konkretnych zespołów reagujących.

Należy pamiętać, że w praktyce obydwa terminy bywają używane naprzemiennie. W szczególności, Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji konsekwentnie posługuje się pojęciem CERT i określenia tego używamy cytując jej publikacje.

5.2 CSIRT rządowy a CSIRT krajowy

Nie istnieje powszechnie akceptowana, formalna definicja CSIRTu rządowego czy krajowego. W dokumencie tym będziemy posługiwać się nieformalnymi definicjami określonymi przez ENISA w opracowaniu "*Deployment of Baseline Capabilities of National/Governmental CERTs*"[50], które same w sobie wskazują, że różne kraje przyjmują różne definicje tych pojęć.

[49] https://www.cert.org/incident-management/csirt-development/cert-authorized.cfm?
[50] http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012

W myśl tych definicji, rządowy CSIRT jest odpowiedzialny za ochronę sieci rządowej/administracji państwowej, a jego "*consitutency*"[51] stanowi rząd oraz inne instytucje publiczne.

W przypadku CSIRTu krajowego ENISA mówi o zespole pełniącym rolę punktu kontaktowego na potrzeby dzielenia się informacjami z innymi CSIRTami krajowymi. Krajowy CSIRT może być uznawany jako "*CERT of the last resort*", czyli CSIRT "ostatniej" instancji. Oznacza to, że w przypadku kiedy podmiot zagraniczny nie jest w stanie uzyskać bezpośredniego kontaktu lub oczekiwanej pomocy zgłaszający incydent z zagranicy nie jest w stanie załatwić jego obsługi u podmiotu, który jest zaangażowany w incydent bezpośrednio, zgłaszający przekazuje zapytanie do CSIRTu krajowego.

Role obu zespołów – rządowego i krajowego – mogą, ale nie muszą, być łączone.

Warto tutaj podnieść kwestię tłumaczenia (i rozumienia) określenia "*national*". Można je bowiem tłumaczyć na trzy sposoby: *krajowy*, *narodowy* lub *państwowy*. W kontekście powyższych definicji ENISA, a także w kontekście wspierania modelu wielu CSIRTów w kraju, uważamy określenie: *krajowy* jako najbardziej odpowiedni. Zarówno ENISA, jak i wspierający aktywnie CSIRTy krajowe CERT w CMU[52] dopuszczają bowiem istnienie wielu tego rodzajów zespołów w jednym kraju, nie sugerując jednocześnie nadrzędności jednego względem innych.

[51] *constituency* - grupa użytkowników instytucjonalnych bądź fizycznych, którą zajmuje się dany CERT.
[52] https://www.cert.org/incident-management/national-csirts/index.cfm

6 System ochrony cyberprzestrzeni – warstwa operacyjna

W niniejszym rozdziale przedstawiono modelową koncepcję organizacji systemu ochrony cyberprzestrzeni w warstwie operacyjnej z uwzględnieniem proponowanych typów głównych podmiotów uczestniczących w systemie oraz podstawowych rodzajów systemów narzędziowych zapewniających współpracę na tym poziomie.

6.1 Wstęp

Pierwszym krokiem do stworzenia koncepcji jest przedstawienie mapy podmiotów (interesariuszy), które powinny łącznie stanowić całościowy model ochrony cyberprzestrzeni, wraz z opisem ról tych podmiotów na poziomie ogólnym. Następnie koncepcja organizacji systemu ochrony cyberprzestrzeni zostanie uszczegółowiona poprzez rozważenie możliwych wariantów, w tym wskazanie ról konkretnych istniejących już organizacji oraz zdefiniowanie nowych.

W koncepcji wyróżniono trzy podstawowe warianty ze względu na stopień centralizacji systemu. W wariancie zdecentralizowanym (rozproszonym) zakłada się jak najpełniejsze wykorzystanie istniejących podmiotów pełniących obecnie określone role w dziedzinie bezpieczeństwa cyberprzestrzeni w Polsce oraz powołanie nowych podmiotów, dla wypełnienia ról, które obecnie nie są pełnione (lub pełnione w stopniu niesatysfakcjonującym albo wynikają z planowanych zmian w regulacjach Unii Europejskiej).

W wariancie scentralizowanym zakłada się powołanie jednej, głównej instytucji, skupiającej większość ról i odpowiedzialności w dziedzinie cyberbezpieczeństwa.

Wariant pośredni jest propozycją wykorzystującą istniejące podmioty administracji państwowej w celu większego skupienia pewnych grup zadań i odpowiedzialności w jednej instytucji – nie przewiduje jednak koncentracji do pojedynczego podmiotu.

W prezentowanych wariantach starano się opierać na specyfice związanej z istniejącym systemem administracji kraju, jego wielkością, obowiązującym systemem prawnym i istniejącymi rozwiązaniami w obszarach mających związek z cyberprzestrzenią. Starano się także wykorzystać pewne doświadczenia zagraniczne, jednak przy takim zastrzeżeniu, że istniejące modele w innych krajach nie będą mogły być w prosty sposób skopiowane na grunt krajowy (ze względu na różnice wielkości krajów, różnice w ustroju administracyjnym,

tradycji itp.), lecz mogą dostarczać inspiracji, szczególnie w odniesieniu do przykładów rozwiązań organizacyjnych, technicznych czy prawnych, które okazały się skuteczne w praktyce[53].

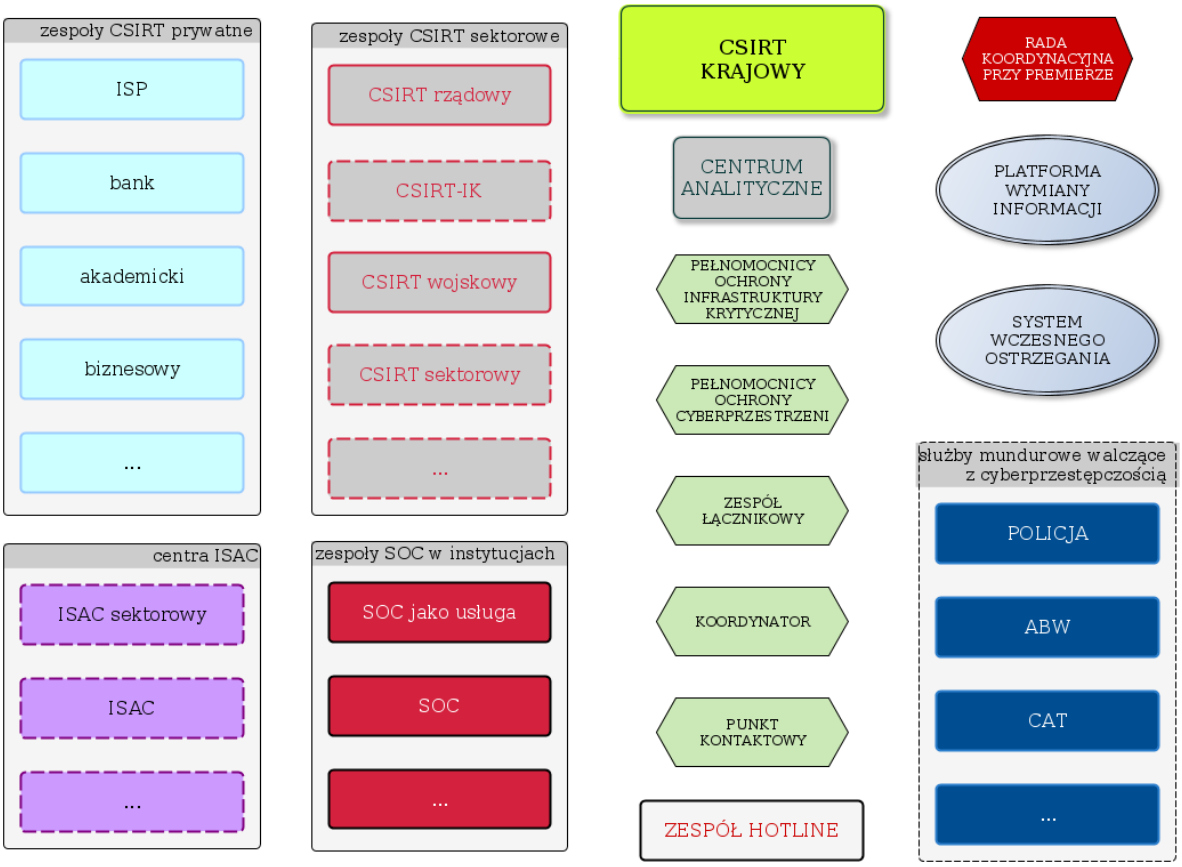
Ze względu na dynamikę zmian w cyberprzestrzeni jest istotne, aby w konstruowanym systemie ochrony cyberprzestrzeni zapewnić jak największą elastyczność (możliwość dostosowywania się do zmieniającej się sytuacji i zdarzeń) przy położeniu nacisku na efektywność i skuteczność (zdolność rozwiązywania problemów w określonym czasie).

O konsultację w zakresie modeli zarządzania systemem ochrony cyberprzestrzeni została poproszona na potrzeby niniejszej ekspertyzy ENISA. Wynik tej konsultacji jest przedstawiony w załączniku. Jest to także koncepcja wariantowa.

6.2 Mapa podmiotów

W ramach konstruowania krajowego systemu współpracy w dziedzinie cyberbezpieczeństwa na poziomie operacyjnym, został opracowany diagram podmiotów oraz aktywnych interesariuszy. W kolejnym kroku zostały zdefiniowane propozycje ról i odpowiedzialności jakie poszczególne elementy systemu powinny pełnić. Na mapie elementów znajdują się także główne mechanizmy techniczno-organizacyjne wspierające system.

[53] Częstokroć rozwiązania, o których czytamy w oficjalnych dokumentach pochodzących z innych krajów wydają się pozbawione wad, a w rzeczywistości mają swoje mankamenty, które nie są szeroko dokumentowane.



Rysunek 7. Mapa podmiotów systemu ochrony cyberprzestrzeni oraz kluczowych narzędzi.

Założeniem głównym przyświecającym tej koncepcji, jest to aby system był efektywny w praktyce, a także uwzględniał i właściwie wykorzystywał istniejące dokonania i potencjał w dziedzinie cyberbezpieczeństwa.

System powinien również uwzględniać zarówno realia krajowe jak też istniejącą i planowaną legislację na poziomie Unii Europejskiej.

Tam, gdzie jest to możliwe system powinien także uwzględniać doświadczenia innych krajów w tym obszarze.

Mówiąc o tym, że system powinien być efektywny w praktyce autorzy koncepcji proponują, aby charakteryzował się on określoną „zwinnością" bądź „elastycznością" (*ang. agile)* tzn. mógł się dynamicznie dostosowywać do zmieniających się wyzwań, potrzeb, zagrożeń i uwarunkowań zewnętrznych.

Zakłada się także, że w oparciu o przedstawioną mapę interesariuszy i zależności pomiędzy nimi można kształtować mniej lub bardziej scentralizowane bądź rozproszone

architektury krajowego systemu cyberbezpieczeństwa – wykorzystując zdefiniowane na mapie elementy, poprzez łączenie niektórych z nich w większe podmioty.

Na tym etapie staramy się nie przypisywać konkretnej istniejącej instytucji do omawianych podmiotów i ról, chyba że pewne role można uznać za oczywiste i jednoznaczne. Więcej szczegółów w kwestii odpowiedzialności jest przedstawionych w częściach dokumentu opisujących poszczególne warianty.

6.2.1 Opis podmiotów i interesariuszy w warstwie operacyjnej

W ramach proponowanej mapy poziomu operacyjnego można wyróżnić następujące elementy, które zostały zobrazowane na rysunku i zostaną szerzej omówione poniżej.

Koordynator – podmiot pełniący określone funkcje koordynacyjne w czasie rozwiązywania problemów związanych z bezpieczeństwem w cyberprzestrzeni ale także, w warstwie strategicznej, nadzorujący wdrażanie strategii cyberbezpieczeństwa i innych dokumentów programowych lub regulacyjnych[54],

Punkt Kontaktowy – podmiot przewidziany w projekcie dyrektywy NIS uczestniczący w europejskich mechanizmach współpracy międzynarodowej (ang. *cooperation group)* przewidzianych w dyrektywie,

CSIRT krajowy – zespół reagujący na zagrożenia i incydenty bezpieczeństwa w cyberprzestrzeni na poziomie krajowym,

Krajowe Centrum Analityczne (CA) – podmiot dysponujący wiedzą sytuacyjną oraz odpowiednimi kompetencjami technicznymi pozwalającymi na głęboką analizę zagrożeń cyberprzestrzeni i oferujący zaawansowane wsparcie techniczne przy rozwiązywaniu trudnych, bądź dużej skali, incydentów naruszających bezpieczeństwo cyberprzestrzeni. CA analizuje także trendy i rekomenduje działania profilaktyczne,

Zespoły Zadaniowe (task force) – powoływane przez Koordynatora w celu rozwiązywania problemów w warstwie operacyjnej, wypracowywania sposobów koordynacji w sytuacjach kryzysowych, stanach nadzwyczajnych, podejmujące działania proaktywne (np. opracowanie planu usunięcia określonego problemu technologicznego czy strukturalnego),

CSIRTy sektorowe – zespoły CSIRT powoływane w poszczególnych sektorach gospodarki (np. infrastruktura krytyczna, administracja publiczna, sektory przewidziane w projekcie dyrektywy NIS),

[54] Rola tego podmiotu na poziomie strategicznym czy regulacyjnym jest omówiona w rozdziale dotyczącym poziomu strategicznego(117)

Zespół łącznikowy (liason) – działający na stałe w siedzibie Koordynatora lub CSIRTu krajowego, zespół przedstawicieli kluczowych instytucji, które zajmują się obszarem cyberbezpieczeństwa (przedstawiciele ministerstw, kluczowych firm telekomunikacyjnych, sektora infrastruktury krytycznej),

Sektorowe centra ISAC (Information Sharing and Analysis Center) – szczególnie w sektorach, w których nie ustanowiono sektorowych CSIRTów (ale także jeśli takie zespoły istnieją) należy wspierać powstawanie centrów wymiany informacji i dokonywania analiz sytuacji bezpieczeństwa IT danego sektora,

Zespoły CSIRT powoływane przez poszczególne podmioty – np. w sektorze telekomunikacyjnym, bankowym, akademickim, przez firmy komercyjne,

SOC (ang. *Security Operation Center*) – centra zajmujące się monitorowaniem i obsługą zdarzeń bezpieczeństwa IT w zdefiniowanych środowiskach infrastrukturalnych, np. w danej instytucji lub grupie. Budowane na terenie danej instytucji bądź realizowane jako usługa pozyskiwana od dostawców specjalizujących się w oferowaniu usług typu MSS *(*ang. *managed security services)*,

Pełnomocnicy Ochrony Cyberprzestrzeni – osoby przewidziane w Polityce Ochrony Cyberprzestrzeni zajmujące się bezpieczeństwem w danej instytucji i współpracujące z Koordynatorem oraz zespołami typu CSIRT,

Nieformalne fora współpracy – takie jak ABUSE Forum, w ramach którego współpracują ze sobą zespoły zajmujące się bezpieczeństwem teleinformatycznym w różnych (z reguły dużych) instytucjach,

Platforma wymiany informacji – oficjalny mechanizm wymiany informacji krajowego systemu cyberbezpieczeństwa, którego opiekunem jest Koordynator,

System wczesnego ostrzegania o zagrożeniach – wykorzystywany od wielu lat przez administrację rządową system ostrzegający przed zagrożeniami – w wersji drugiej generacji - *ARAKIS2*,

Łowcy - nowy typ zespołu bezpieczeństwa: zespoły, których głównym zadaniem jest okresowe sprawdzania sieci kluczowych podmiotów (np. administracji państwa) w celu zaawansowanego poszukiwania, czy dana instytucja nie została spenetrowana.

6.3 Zadania interesariuszy systemu ochrony cyberprzestrzeni

W tej części dokumentu opisujemy bardziej szczegółowo zadania i role interesariuszy systemu ochrony cyberprzestrzeni.

6.3.1 Koordynator ochrony cyberprzestrzeni

Jest to kluczowy podmiot pełniący określone funkcje koordynacyjne w dziedzinie ochrony cyberprzestrzeni. Powinien być ustanowiony w randze co najmniej podsekretarza stanu. Osobą formalnie odpowiedzialną powinien być minister, a w praktyce realizacja zadań powinna spoczywać na jednym urzędniku w randze podsekretarza stanu. Na poziomie strategicznym podmiot koordynujący powinien nadzorować wdrażanie dokumentów programowych (strategii cyberbezpieczeństwa), aktów prawnych (ustaw dotyczących ochrony cyberprzestrzeni), a także harmonizacji z prawodawstwem Unii Europejskiej w tym obszarze. W niniejszym rozdziale skupiono się jednak bardziej na funkcjach operacyjnych, które powinny być przypisane do podmiotu Koordynatora.

I tak, podmiot koordynujący powinien w warstwie operacyjnej:

- współpracować z CSIRTem krajowym w oparciu o zasady szczegółowo opisane w prawie,
- powoływać, na wniosek CSIRTu krajowego, Zespołu Łącznikowego lub z własnej inicjatywy Zespoły Zadaniowe dla rozwiązywania problemów bieżących (incydentów, sytuacji kryzysowych) oraz wypracowywania rozwiązań dla problemów strukturalnych, systemowych, prawnych,
- eskalować na poziom Rady Ministrów problemy dużej skali związane z bezpieczeństwem cyberprzestrzeni bądź problemy ze współpracą w ramach administracji publicznej,
- wspierać rozwój współpracy, a także reagować na problemy w tejże współpracy pomiędzy CSIRTem krajowym, CSIRTami sektorowymi oraz centrami ISAC,
- współpracować z Punktem Kontaktowym (przekazywanie informacji o incydentach o charakterze transgranicznym),
- współpracować z organami ścigania oraz organem właściwym w zakresie ochrony danych osobowych.

6.3.2 Punkt Kontaktowy

To podmiot przewidziany w projekcie dyrektywy NIS, uczestniczący w europejskich mechanizmach współpracy międzynarodowej przewidzianych w dyrektywie. Punkt kontaktowy odgrywa rolę łącznika pomiędzy rządem danego kraju a powoływanymi w ramach dyrektywy sieciami współpracy (*cooperation group, sieć zespołów CSIRT*). Punkt Kontaktowy otrzymuje informacje o poważnych naruszeniach bezpieczeństwa mających charakter transgraniczny i informuje o tym punkty kontaktowe w innych krajach za pomocą ustanowionych sieci współpracy. Punkt Kontaktowy może istnieć w ramach Koordynatora ochrony cyberprzestrzeni.

6.3.3 CSIRT Krajowy

Zespół reagowania na incydenty bezpieczeństwa w cyberprzestrzeni na poziomie krajowym – CSIRT (Computer Security Incident Response Team), powinien zajmować się koordynacją obsługi incydentów na poziomie bezpieczeństwa kraju, funkcjonując w trybie ciągłym (24h/dobę).[55]

Trzeba zaznaczyć, że obsługa incydentów dotyczących całej cyberprzestrzeni przez jeden zespół nie jest w praktyce możliwa. Należy więc zadbać, by rozwinęła się sieć współpracujących zespołów typu CSIRT/CERT w różnych sektorach gospodarki. Ponadto powinno się wykorzystać potencjał innych elementów proponowanego systemu, takich jak: centra ISAC, Grupy Zadaniowe, Pełnomocnicy Ochrony Cyberprzestrzeni czy centra SOC powstające w różnych instytucjach.

Tak więc incydent bezpieczeństwa powinien być rozwiązywany poprzez zespół, który jest w stanie zareagować najbliżej źródła problemu (czy też zgłaszającego problem). Nie jest bowiem możliwe, by CSIRT krajowy mógł interweniować fizycznie w każdym przypadku – i nie należy zakładać takiego scenariusza.

CSIRT krajowy powinien koordynować reakcję na zagrożenia i incydenty, które dotyczą wielu sektorów, przekazywać rozwiązywanie przypadków do właściwych podmiotów (np. CSIRTów sektorowych) lub rozwiązywać fizycznie problemy wtedy, gdy takie CSIRTy nie istnieją i nie ma innych zespołów czy centrów bezpieczeństwa, które działają w danym sektorze (ISAC, SOC itp.). CSIRT krajowy powinien także – przy obsłudze incydentów – pełnić rolę instancji „ostatniej instancji" (last resort). Jeśli bowiem nie wiadomo w danym przypadku, kto może czy powinien obsłużyć dany przypadek, CSIRT krajowy byłby zobowiązany do podjęcia stosownych działań

CSIRT krajowy powinien mieć pełny obraz występujących zagrożeń w kraju, także współpracujące z nim zespoły (CSIRTy) powinny mieć obowiązek raportowania o zgłoszonych incydentach.

CSIRT krajowy powinien udostępniać zbiorcze statystyki Koordynatorowi ochrony cyberprzestrzeni.

CSIRT krajowy powinien na bieżąco wykorzystywać informację z Centrum Analitycznego i korzystać ze wsparcia eksperckiego Centrum przy rozwiązywaniu problemów.

CSIRT krajowy może także wnioskować do Koordynatora o powołanie konkretnego Zespołu Zadaniowego do rozwiązywania danego przypadku.

[55] Założenie funkcjonowania w trybie 24/7 nie musi oznaczać fizycznej obecności pracowników przez cała dobę. Możliwe jest wprowadzenie systemu dyżurów zdalnych.

W związku z zapisami projektu dyrektywy NIS, krajowy CSIRT uczestniczy w pracach międzynarodowej sieci współpracy zespołów CSIRT powołanych w krajach Unii Europejskiej.

Jest to ważny element funkcjonowania CSIRTu, gdyż jest tu mowa o współpracy o charakterze operacyjnym, wymianie informacji o incydentach transgranicznych, możliwości poproszona o asystę przy rozwiązywaniu problemów w kraju, a także o wypracowywaniu standardów wymiany informacji i nowych propozycji w dziedzinie poszerzania i pogłębiania współpracy operacyjnej w obszarze NIS.

6.3.4 Krajowe Centrum Analityczne

Tworzenie zaleceń i ocena sytuacji wyłącznie na podstawie zgłoszeń i raportów zewnętrznych jest niewystarczające i może być potencjalnie niebezpieczne. W szczególności autorami raportów dotyczących zagrożeń są często podmioty komercyjne z krajów trzecich, które oprócz oczywistych i zrozumiałych celów komercyjnych mogą także mieć nałożone ograniczenia czy wręcz embargo na dystrybucję niektórych informacji, wynikające choćby z charakteru współpracy z lokalnymi rządami.

Niezbędnym elementem systemu dbania o cyberbezpieczeństwo państwa jest więc utrzymywanie i rozwijanie własnych zdolności analitycznych w zakresie oceny ogólnej sytuacji oraz weryfikacji i dogłębnej analizy konkretnych zagrożeń.

Zdolności takie jak – Analityka, Świadomość Sytuacyjna, Badania i Rozwój – wymieniane są także wprost w zaktualizowanym katalogu usług zespołów CSIRT przedstawionym w rozdziale 6.4, ponieważ uznano je za kluczowe elementy misji współczesnych zespołów reagujących. Naszym zdaniem zasadne jest uwzględnienie tych usług w krajowym systemie reagowania na incydenty, przy jednoczesnym wyraźnym odróżnieniu ich od usług świadczonych z definicji przez CSIRT krajowy oraz CSIRT rządowy.

Postulujemy w związku z tym, aby wyróżnić jako oddzielny podmiot Centrum Analityczne. W zależności od modelu, kompetencje Centrum Analitycznego mogą być włączone w obszar jednego z innych podmiotów (na przykład CSIRTu Krajowego). W szczególnych przypadkach może być zasadne korzystanie z więcej niż jednego Centrum Analitycznego. Niepożądany jest jednak stan, gdy każde zadanie analityczne jest osobno zlecane podmiotom zewnętrznym, nieumocowanym w planach zarządzania cyberbezpieczeństwem w sposób strukturalny.

Do zadań Centrum Analitycznego należeć powinny w szczególności:

- wsparcie techniczne przy analizie szczególnie trudnych incydentów,

- przeprowadzanie zaawansowanych analiz złośliwego oprogramowania zagrażającego użytkownikom cyberprzestrzeni RP,
- analiza podatności,
- bieżące monitorowanie wskaźników zagrożeń takich jak: rozmiary botnetów, reputacje sieci – przede wszystkim na podstawie informacji zbieranych w Platformie Wymiany Informacji oraz w systemie monitorowania i ostrzegania o zagrożeniach,
- rozwój narzędzi i metod do wykrywania i zwalczania zagrożeń,
- identyfikowanie problemów do rozwiązania i na tej podstawie przekazywanie Koordynatorowi rekomendacji w zakresie tworzenia, zadaniowania, modyfikowania i odwoływania Zespołów Zadaniowych,
- proponowanie Koordynatorowi rozwiązań systemowych w postaci standardów i rekomendacji, do dyskusji w ramach Zespołów Zadaniowych i do publikacji przez Koordynatora.

Ze względu na zakres specjalistycznych kompetencji technicznych, którymi powinno dysponować Centrum Analityczne nie rekomendujemy umieszczenia go w którejkolwiek instytucji administracji publicznej. Ze względu na dużą konkurencyjność sektora prywatnego w zakresie wysokości płac, wiązałoby się to bowiem z potencjalnymi problemami z zatrudnieniem oraz utrzymaniem odpowiednio wyszkolonego personelu merytorycznego.

6.3.5 Zespół Łącznikowy

Celem powołania stałego zespołu składającego się z przedstawicieli różnych instytucji pracujących wspólnie, zgromadzonych w jednym miejscu, jest zapewnienie stałej współpracy kluczowych podmiotów z punktu widzenia ochrony cyberprzestrzeni RP.

W skład zespołu powinni wchodzić przedstawiciele następujących ministerstw (wg podziału administracyjnego obowiązującego w trakcie przygotowywania niniejszego dokumentu):

- Ministerstwo Administracji i Cyfryzacji,
- Ministerstwo Spraw Wewnętrznych,
- Ministerstwo Obrony Narodowej,
- Ministerstwo Spraw Zagranicznych.

Oprócz tego członkami zespołu powinni być przedstawiciele ważnych instytucji zajmujących się bezpieczeństwem czy też ściganiem przestępstw, takich jak:

- Agencja Bezpieczeństwa Wewnętrznego,

- Policja,
- Rządowe Centrum Bezpieczeństwa,
- Narodowe Centrum Kryptologii,
- Biuro Bezpieczeństwa Narodowego.

W skład zespołu powinni także wchodzić przedstawiciele instytucji, w których funkcjonują:

- CSIRT krajowy,
- CSIRTy sektorowe ,
- Krajowe Centrum Analityczne.

Zaleca się także, aby kluczowe instytucje państwowe, nie będące administracją rządową, takie jak: Kancelaria Sejmu także desygnowały swojego łącznika do Zespołu Łącznikowego. Również instytucje istotne z punktu widzenia np. bezpieczeństwa funkcjonowania obiegu finansowego, takie jak Narodowy Bank Polski, także powinny mieć stałego lub zapraszanego w razie potrzeby przedstawiciela w Zespole.

Siedzibą działania zespołu powinna być siedziba instytucji sprawującej rolę Koordynatora w krajowym systemie ochrony cyberprzestrzeni lub krajowego CSIRT. Koordynator powinien prowadzić sekretariat i na bieżąco korzystać z efektów pracy zespołu.

Zespół łącznikowy ma mieć możliwość rozszerzania na rzecz konsultacji merytorycznych o kolejne zaproszone do współpracy, wyznaczone wcześniej, osoby łącznikowe z innych instytucji i firm, które zadeklarują wolę wspierania pracy zespołu.

Rolą zespołu jest bieżące zbieranie informacji o zagrożeniach i incydentach bezpieczeństwa w cyberprzestrzeni RP – od CSIRTu krajowego, CSIRTów sektorowych, instytucji macierzystych łączników i Koordynatora, śledzenie przebiegu zdarzeń, wnioskowanie o podjęcie działań niestandardowych (np. włączenie do działań dodatkowych ekspertów, wnioskowanie o powołanie określonego Zespołu Zadaniowego itp.). Najważniejszym jednak zadaniem zespołu, jest wyciągnięcie wniosków z każdego zdarzenia oraz wnioskowanie (do Koordynatora lub macierzystych instytucji) o podjęcie działań usprawniających (np. wprowadzenie nowych lub zmiana istniejących procedur, stworzenie nowych ram prawnych lub organizacyjnych itp.)

Zespół nie koordynuje rozwiązywania incydentów. Tym zadaniem od strony technicznej zajmuje się CSIRT krajowy (lub CSIRTy sektorowe, jeśli incydent dotyczy jednego sektora), a od strony strategicznej – instytucja Koordynatora, która także poprzez Punkt Kontaktowy wymienia informacje z grupą współpracy międzynarodowej w ramach UE. Zespół wspiera rozwiązywanie problemów poprzez szybką ścieżkę kontaktów w danych, kluczowych

instytucjach, które wyznaczyły osoby łącznikowe, a także powinien wyciągać wnioski (doraźne i systemowe) po każdym poważnym incydencie.

Zespół tworzy także cykliczne raporty dla Koordynatora i macierzystych instytucji z zawartymi w nich rekomendacjami. Rekomendacje te są analizowane przez Koordynatora, który jest zobowiązany do nadania sprawie dalszego biegu (np. poprzez powołanie Zespołu Zadaniowego do rozwiązania problemu, czy rekomendowanie zmian systemowych na Radzie Koordynacyjnej przy Radzie Ministrów.

Rekomenduje się także, aby Zespół Łącznikowy rozwijał się w ramach zdobywania praktycznych doświadczeń we współpracy stron, w kierunku angażowania (na stałe lub w zależności od potrzeb) przedstawicieli spoza administracji publicznej.

Przedstawiciele poszczególnych instytucji uczestniczący w pracach Zespołu ściśle współpracują z CSIRTem krajowym, również na poziomie operacyjnym. Koncepcja Zespołu zakłada, że jego członkowie osobiście spotykają się regularnie z przedstawicielami CSIRTu krajowego. Na bieżąco uzyskują informacje o poważnych zagrożeniach i uczestniczą (wspierają działania CSIRTu) w rozwiązywaniu problemów dużej rangi (również konkretnych incydentów), jak też zauważonych problemów systemowych. Zespół Łącznikowy powinien zatem mieć siedzibę przy zespole CSIRTu krajowego. Spotkania zespołu i CSIRTu powinny odbywać się regularnie (np. dwa razy w tygodniu), oprócz tego każdy z łączników powinien mieć możliwość indywidualnych spotkań z pracownikami CSIRTu krajowego.

Zespół Łącznikowy tworzy raporty dotyczące bieżących incydentów oraz zauważonych problemów systemowych (np. luki w systemie bezpieczeństwa cyberprzestrzeni), może tworzyć rekomendacje i przedstawić je macierzystym instytucjom oraz instytucji Koordynatora. Wyznaczeni łącznicy, będąc oddelegowanymi (np. na część etatu) pracownikami macierzystych instytucji mają możliwość bezpośredniego przekazywania informacji do swoich instytucji, jak również powinni mieć możliwość występowania o konkretne wsparcie do kierownictwa danej instytucji, jeśli bieżąca sytuacja będzie tego wymagała.

Oficjalnie Zespół jest powoływany przez Koordynatora, na podstawie wyznaczenia danej osoby przez macierzystą instytucję. Instytucje rządowe, przynajmniej w pierwszym etapie, mogą delegować swych pełnomocników ochrony cyberprzestrzeni do pracy w Zespole.

Ze względu na charakter pracy, łącznicy powinni dysponować odpowiednią wiedzą techniczną w zakresie technologii informatycznych i bezpieczeństwa, rozeznaniem co do funkcjonowania systemu cyberbezpieczeństwa, a także powinni móc realnie poświęcić odpowiednią ilość swojego czasu na pracę w Zespole Łącznikowym.

Współpraca z CSIRTem krajowym jest głównym elementem pracy zespołu. Dodatkowo, należy rozważyć włączanie do zespołu, czasowo lub na stałe, przedstawicieli CSIRTów sektorowych, w miarę ich powstawania.

Tak jak zaznaczono wyżej, zespół powinien się rozwijać, wypracowując swój optymalny *modus operandi* oraz skład instytucjonalny (permanentny oraz czasowo rozbudowywany w zależności od bieżących potrzeb).

6.3.6 Zespoły Zadaniowe ds. bezpieczeństwa cyberprzestrzeni

Ważnym elementem koncepcji systemu ochrony cyberprzestrzeni, który powinien cechować się elastycznością i „zwinnością" (ang. *agility*) wobec dynamicznie zmieniającej się i rozwijającej gamie zagrożeń byłyby tzw. Zespoły Zadaniowe – powoływane przez instytucję Koordynatora do rozwiązywania problemów, zarówno na poziomie operacyjnym, jak też dla wypracowywania propozycji rozwiązań technologicznych, organizacyjnych czy prawnych – w dłuższej skali czasowej.

Zespoły takie zajmowałyby się także wypracowywaniem sposobów koordynacji w sytuacjach kryzysowych, stanach nadzwyczajnych, podejmowałyby działania proaktywne (np. opracowanie planu usunięcia określonego problemu technologicznego czy strukturalnego).

Skład Zespołu Zadaniowego powinien być jak najbardziej dopasowany do przedmiotu zadania postawionego przed zespołem. Zakłada się, że przedstawiciele zespołu mogliby się wywodzić z dowolnego podmiotu, zarówno krajowego, jak i zagranicznego, państwowego, jak i komercyjnego, środowiska akademickiego, dostawców rozwiązań, prawników, izb, organizacji zajmujących się bezpieczeństwem a także udział w pracach mogliby brać uznani indywidulani eksperci.

Zespoły wolontariuszy

Proponuje się, żeby członkami niektórych Zespołów Zadaniowych mogli zostać wyselekcjonowani ochotnicy, zapraszani do zespołu w oparciu o bazę wolontariuszy prowadzoną przez Koordynatora lub instytucję, której zostałoby powierzone takie zadanie. Chodziłoby o wykorzystanie potencjału wielu setek młodych osób, które pasjonują się teleinformatyką i bezpieczeństwem, które chciałby się zaangażować w konkretnych zadaniach związanych z bezpieczeństwem cyberprzestrzeni RP (np. w sytuacjach kryzysowych, w których potrzebny jest skokowy wzrost zasobów ludzkich do przeprowadzenia określonych działań na dużym obszarze lub na dużą skalę, np. natychmiastowa pomoc informatyczna). Osoby te musiałyby przestrzegać określonego kodeksu postępowania w cyberprzestrzeni, ich umiejętności powinny być weryfikowane np.

za pomocą organizowanych przez CSIRT krajowy wyzwań *(hacking challenge, capture the flag*) czy programów typu *bug bounty* .

6.3.7 Sektorowe zespoły CSIRT

Tak jak wspomniano, nie jest w praktyce wykonalne, aby jeden zespół CSIRT na poziomie krajowym (niezależnie od wielkości) mógł obsłużyć (tzn. zajmować się rozwiązywaniem) wszystkich incydentów bezpieczeństwa cyberprzestrzeni. Konieczne jest ustanawianie CSIRTów w poszczególnych, kluczowych sektorach, a także w poszczególnych instytucjach i przedsiębiorstwach (szczególnie tych o kluczowym znaczeniu).

Taka idea przyświecała twórcom pierwszego w kraju zespołu CSIRT (powstałego w roku 1997 CERT NASK a od roku 2000 funkcjonującego jako CERT Polska). Zespół ten przez lata swojej działalności, oprócz zajmowania się klasycznymi zadaniami związanymi z reagowaniem na incydenty, publikowaniem ostrzeżeń, statystyk, raportów, a także kreowaniem zaawansowanych narzędzi wspomagających system bezpieczeństwa w kraju (system ARAKIS, baza N6), wspierał powstawanie kolejnych zespołów CSIRT w naszym kraju, poprzez wyspecjalizowane szkolenia, przekazywanie doświadczeń, pomoc we włączeniu się w struktury międzynarodowe.

Także obecnie, w ramach konstruowania systemu ochrony cyberbezpieczeństwa należy ustanowić program wspierający powstawanie coraz większej ilości zespołów CSIRT, wykorzystując wiedzę i doświadczenie najbardziej zaawansowanych zespołów reagujących w kraju.

Takie podejście spowoduje osiąganie coraz większego potencjału cyberbezpieczeństwa w kraju, bowiem z jednej strony będzie łatwiej obsłużyć dużą liczbę zdarzeń, z drugiej zaś będzie możliwe uwzględnienie specyfiki poszczególnych sektorów.

Przykładowo, gdyby istniał CSIRT dedykowany dla sektora energetycznego, wyspecjalizowałby się w technologiach energetycznych i znałby specyfikę systemów IT tego sektora. Synergia wiedzy o technologii danego sektora (ICS,SCADA) oraz zagrożeń typowych dla cyberprzestrzeni (systemów opartych na protokole IP) jest bowiem koniecznym elementem właściwego podejścia do problematyki ochrony sieci przemysłowych. [56]

Podejście do kreowania CSIRTów sektorowych jest także wspierane przez zapisy projektu dyrektywy NIS.

W niektórych krajach (np. USA) powołuje się CSIRTy dla całej infrastruktury krytycznej – niezależnie od sektora.

[56] Częstokroć inżynierowie danego sektora przemysłu (np. paliwowego) doskonale znają się na swoich systemach a nie maja wiedzy i przygotowania w zakresie technologii IP, która coraz śmielej wkracza do przemysłu – a z drugiej strony klasyczne CSIRTy mogą nie mieć wystarczającego rozeznania co do systemów ICS/SCADA

Należy zwrócić uwagę, że powoływanie zespołów CSIRT to proces niełatwy i czasochłonny. Rekomenduje się zatem założenie, że jest to właśnie proces rozłożony na lata, który tak jak rośnięcie drzewa, powoli rozłoży obowiązki reagowania na zagrożenia i incydenty na coraz większą liczbę gałęzi.
Warto więc przyjąć pewien plan rozwojowy (roadmapa) wspierania powstawania kolejnych CSIRTów, które mogłyby przejmować poszczególne obszary cyberprzestrzeni (*constituency*) pod swoją pieczę, w ramach działania na danym polu czy sektorze.

Obecnie istnieje CSIRT, który zakresem swojego działania pokrywa obszar administracji (CERT.GOV.PL), a także angażuje się z pomocą się w sytuacjach cyberzagrożeń dotyczących państwowych przedsiębiorstw infrastruktury krytycznej[57]. Analizując załącznik II projektu dyrektywy NIS, należy się zastanowić, w których jeszcze sektorach należałoby w pierwszej kolejności powołać zespoły sektorowe. Sektor telekomunikacyjny, w którym już istnieje obowiązek zgłaszania poważnych incydentów do regulatora, nie ma swego CSIRTu (Prawo telekomunikacyjne tego nie wymaga). Jednak u poszczególnych operatorów telekomunikacyjnych zespoły reagujące (nie zawsze określane mianem CSIRT lub CERT) w wielu przypadkach już istnieją. W sektorze energetycznym regulator (URE) nie ma obecnie przewidzianych obowiązków związanych z ochroną cyberprzestrzeni. Inne ważne sektory, jak np. bankowy mają swoje regulacje bezpieczeństwa IT (np. Rekomendacja D), w poszczególnych dużych bankach istnieją nawet CSIRTy, ale nie istnieje jeden punkt reagowania dla całego sektora. W pozostałych kluczowych sektorach (transport, zdrowie, paliwa) obraz sytuacji w tej dziedzinie jest dużo skromniejszy .

Widać więc, że budowanie CSIRTów i sieci ich współpracy w naszym kraju to będzie zadanie trudne, czasochłonne i kosztowne. Tym bardziej należy postawić na zwinne formy współdziałania: proponowane w tym rozdziale Zespoły Zadaniowe), wykorzystanie istniejących centrów typu ISAC (i wspieranie powstawania nowych), a także postawienie na fora współpracy (np. Pełnomocników Ochrony Cyberprzestrzeni, nieformalne ciała typu ABUSE Forum). Równolegle zaś należy opracować plan kreowania zespołów CSIRT dla poszczególnych obszarów – na bazie analizy ryzyka związanej z kluczowością danego obszaru dla prawidłowego funkcjonowania państwa i społeczeństwa.

[57] W przyszłym kształcie systemu cyberbezpieczeństwa umocowanie takiego zespołu powinno być silne, a zakres działania powinien być formalnie i precyzyjnie zdefiniowany.

6.3.8 Platforma wymiany informacji

W świecie zespołów zajmujących się cyberbezpieczeństwem nie ma wypracowanych jednoznacznych mechanizmów wymiany informacji o cyberbezpieczeństwie czy nawet jego wybranych podzbiorów (np. wymiany informacji o zagrożeniach). W ramach studium dla ENISA (opracowanie "*Actionable Information for Security Incident Response*"[58]), zespół CERT Polska zidentyfikował aż 53 standardy wymiany informacji cyberbezpieczeństwa oraz 16 przykładowych darmowych narzędzi (na licencji *opensource*) do zarządzania nimi. W niniejszym opracowaniu nie będziemy omawiali konkretnych standardów, wskażemy jednak na rodzaje informacji, które powinny być wymieniane.

W każdym w rozpatrywanych potencjalnych wariantów organizacji ochrony cyberprzestrzeni w Polsce rekomendujemy ustanowienie platformy wymiany informacji cyberbezpieczeństwa, w szczególności pomiędzy podmiotami administracji państwowej, ale również w niektórych aspektach, z CSIRTami sektorowymi, centrami ISAC czy podmiotami prywatnymi. Nie musi ona koniecznie stanowić jednego narzędzia czy systemu, ale może się składać z wielu ich instancji, charakteryzujących się obsługą różnych typów informacji. Z naszego doświadczenia budowy podobnych systemów (projekty FISHA/NISHA[59] czy platforma n6[60]) wynika bowiem, że charakter wymienianych informacji (w tym ich ilość oraz możliwe zastosowanie) jest tak różnorodny, że jest mało prawdopodobne, aby mogło powstać jedno efektywne rozwiązanie do ich wymiany.

Wśród wymienianych informacji powinny znajdować się m.in.:[61]

- ostrzeżenia (alerty) o nowych zagrożeniach czy podatnościach [NISHA],
- zalecenia dotyczące zagrożeń i podatności [NISHA],
- opracowania "najlepszych praktyk" w zakresie zagadnień cyberbezpieczeństwa [NISHA],
- materiały typu "*awareness*" [NISHA],
- informacje o wykrytej złośliwej aktywności (np. komputery zainfekowane botami, biorące udział w ataku DDoS czy przechowujące złośliwe strony WWW itp.) [n6],
- informacje o źle skonfigurowanej, otwartej lub podatnej infrastrukturze (np. otwarte systemy DNS, NTP itp) [n6],
- informacje o wskaźnikach "IoC" (Indicators of Compromise) [n6],
- istotne próbki złośliwego oprogramowania (do ewentualnej wspólnej analizy),

[58] http://www.enisa.europa.eu/activities/cert/support/actionable-information
[59] http://nisha-network.eu/
[60] http://n6.cert.pl
[61] W nawiasach kwadratowych zaznaczono nazwy istniejących narzędzi, które wspierają wymianę danego typu informacji

- informacje o TTP (ang. *Tactics, Techniques and Procedures*) i ew. aktorach stojących za atakami (w szczególności Advanced Persistent Threats - APT),
- logi systemowe, sieciowe, kopie dysków i inne materiały mogące być przedmiotem analizy forensics,
- informacje o nielegalnych treściach w sieci.

Dostęp do platformy wymiany wiedzy powinien odbywać się na różne sposoby, w tym poprzez portal WWW, ale też API, umożliwiające automatyzację. Dyskusje mogą być również prowadzone w formie list mailingowych. Rozwiązanie powinno pozwalać na pełną automatyzację (komunikacje system - system), ale również system - człowiek i człowiek - człowiek. Jako minimum, informacje w platformie powinny być klasyfikowane, jeśli chodzi o stopnie poufności i zakresu dystrybucji protokołem TLP[62]. Opisywana platforma ma na celu obsługę informacji nie objętych klauzulą niejawności (w rozumieniu ustawy o ochronie informacji niejawnych). W związku z tym informacji niejawne (w rozumieniu ww. ustawy) powinny być wymieniane innymi mechanizmami poprzez odpowiednie dostosowaną wersję platformy.

Oczywiście, istnienie takiej platformy nie eliminuje innych kanałów wymiany informacji, w szczególności tych istniejących, w tym także nieformalnych.

6.3.9 Centra ISAC

Dzielenie się informacjami o zagrożeniach bezpieczeństwa między podmiotami prywatnymi jest podstawą budowy systemu przeciwdziałania zagrożeniom, nie tylko dla instytucji prywatnych, ale także dla państwa. Fakt ten został już dawno dostrzeżony w środowisku ekspertów zajmujących się cyberbezpieczeństwem. Nacisk na wymianę informacji o zagrożeniach pomiędzy podmiotami na wielu poziomach (nie tylko pomiędzy zespołami CSIRT) kładziony jest również w opracowaniach agencji ENISA (*Incentives and Challenges for Information Sharing in the Context of Network and Information Security*[63]).

Jednym z mechanizmów zaproponowanych w Stanach Zjednoczonych, mających na celu wspomożenia środowiska prywatnego było powołanie tzw. centrów ISAC (*Information Sharing and Analysis Centres*). ISAC to centra wymiany wiedzy budowane wokół określonych sektorów gospodarki (np. instytucji finansowych[64], energetyki, lotnictwa) i zrzeszające instytucje zainteresowane wymianą doświadczeń o zagrożeniach skierowanych na ich

[62] http://www.cert.pl/tlp

[63] https://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/incentives-and-barriers-to-information-sharing/at_download/fullReport

[64] Najbardziej znanymi ISACami funkcjonującymi w USA i Europie są te skupione wokół sektora finansowego: FS-ISAC (USA) i FI-ISAC (W Europie, wspieranego przez agencję ENISA).

działalność. Czasem wymiana wiedzy realizowana jest nie tyle przez instytucje typu ISAC a przez tzw. ISAO (*Information Sharing and Analysis Organizations*).

Centra ISAC działają jako instytucje non-profit i służą również jako mechanizm dwukierunkowej komunikacji z administracją państwową i innymi ISACami. Mogą przyjmować mniej lub bardziej formalny charakter, np. dysponować wspólnym rozwiązaniem informatycznym do wymiany wiedzy lub tylko będąc platformą do częstych spotkań ekspertów z danego środowiska. W kontekście niniejszego opracowania centra ISAC mogą być rozumiane jako najbardziej podstawowy budulec krajowego systemu cyberbezpieczeństwa, obejmującego podmioty prywatne. Ich udane ustanowienie może być podstawą do budowy CSIRTów sektorowych, jeżeli zostanie zidentyfikowana taka potrzeba. Inicjatywa budowy ISACów w danych sektorach gospodarki powinna wychodzić ze środowiska prywatnego, jednakże państwo może w naszej opinii wspomóc ich powstawanie, współfinansując ich stworzenie i utrzymanie, np. poprzez mechanizm konkursowy.

6.3.10 Zespoły CSIRT powoływane przez poszczególne podmioty

Przy obecnym zaawansowaniu technologii informacyjnych i związanych z tym zagrożeń bezpieczeństwa, istnienie dedykowanych osób lub zespołów (w zależności od wielkości organizacji) zajmujących się bezpieczeństwem IT, w szczególności reagowaniem na pojawiające się zagrożenia i incydenty jest wymogiem niekwestionowanym.

Czy będą się one nazywać CSIRT, CERT czy inaczej – nie ma to specjalnego znaczenia. Ważne, aby obszar dbania o bezpieczeństwo teleinformatyczne w danej instytucji czy firmie był elementem stałych procesów funkcjonujących w organizacji.

Można wyróżnić kilka podstawowych funkcji czy ról, które zwykle są pełnione rozdzielnie w procesie zapewniania bezpieczeństwa, takich jak:

- opracowywanie polityk bezpieczeństwa, planów ciągłości działania i regulaminów,
- wdrażanie zabezpieczeń,
- administrowanie systemami,
- monitorowanie i zarządzanie bezpieczeństwem,
- reagowanie na incydenty,
- analiza bieżących zagrożeń,
- wykonywanie audytów bezpieczeństwa.

Niektóre z tych ról są łączone, inne powinny być rozłączne (np. administrowanie systemami a zarządzanie bezpieczeństwem czy przeprowadzanie audytów), jednak wiele zależy w praktyce od wielkości i zasobów danej organizacji. Nie w każdej instytucji jest

możliwe wdrożenie idealnego modelu opartego o separację wielu ról potrzebnych do pełnienia w procesie zapewniania bezpieczeństwa IT.

Dość specjalną rolę pełnią na tej mapie zespoły CSIRT. Nominalnie powstałe dla pełnienia roli reagującej, na przestrzeni lat sprawdziły się jako ważny element w walce o bezpieczeństwo IT, dzięki praktycznemu podejściu do bezpieczeństwa sieci i informacji. CSIRTy, mając bezpośredni kontakt z zagrożeniami oraz technikami i narzędziami wykorzystywanymi przez cyberprzestępców, współpracując z rozbudowaną siecią podobnych zespołów na całym świecie, są w stanie nie tylko reagować na incydenty, ale także prowadzić działalność prewencyjną, edukacyjną czy badawczą.

Katalog usług, jakie oferują zespoły CSIRT stale się rozszerza (patrz rozdział 6.4). Nie każdy zespół musi jednak oferować pełen zestaw usług.

Powstawanie zespołów CSIRT w ramach poszczególnych podmiotów gospodarczych należy zatem pozostawić normalnym procesom biznesowym, jako że bezpieczeństwo IT, będąc coraz bardziej wymiernym elementem prowadzenia działalności w dużych przedsiębiorstwach czy organizacjach, w sposób naturalny prowadzi do powstawania wyspecjalizowanych zespołów cyberbezpieczeństwa.

Państwo powinno pełnić rolę katalizatora takich procesów poprzez uświadamianie kadrze kierowniczej przedsiębiorstw i instytucji konieczności prowadzenia analizy ryzyka oraz powoływania zespołów CSIRT, a także opracować odpowiedni system zachęt dla podmiotów, aby stymulować podejmowanie takich działań.

W kwestii współpracy z sektorowymi CSIRTami – w przypadku jeśli istnieją – wydaje się, że państwo powinno narzucać obowiązek współpracy zespołów bezpieczeństwa powoływanych w instytucjach danego sektora z takim CSIRTem, jednak również dbając o to, by nie było to wyłącznie obciążenie dla instytucji, ale aby istniały dwustronne korzyści z takiej współpracy.

6.3.11 Pełnomocnicy Ochrony Cyberprzestrzeni (POC)

Jednym z ciekawych pomysłów Polityki Ochrony Cyberprzestrzeni RP jest powołanie w instytucjach administracji pełnomocników Ochrony Cyberprzestrzeni. Ponieważ POCRP jest obowiązkowa jedynie dla obszaru administracji rządowej, grupę POC można określić jako grupę sektorową, niemniej jednak sama idea jest godna rozwijania i naśladowania w innych

kluczowych sektorach[65]. Z drugiej zaś strony, także w kwestii pełnomocników związanych z bezpieczeństwem należy dążyć do możliwie kompleksowego podejścia, ponieważ można sobie wyobrazić, iż w jednej instytucji będzie funkcjonowało niezależnie czterech pełnomocników zajmujących się kwestiami bezpieczeństwa (ochrona cyberprzestrzeni, ochrona infrastruktury krytycznej, ochrona informacji niejawnych, ochrona danych osobowych – ABI), każdy w oparciu o odrębnie ustanawiane przepisy. Ze względu zaś na horyzontalny charakter kwestii związanych z ochroną systemów IT i informacji oraz wiele podobieństw, zarówno w obszarze zagrożeń, jak i metod przeciwdziałania, wartością dodaną byłaby synergia pomiędzy tymi obszarami i funkcjami pełnomocników.

Pełnomocnicy Ochrony Cyberprzestrzeni, którzy aktywnie uczestniczą w wymianie informacji oraz szkoleniach, perspektywicznie będą stanowili dobre oparcie dla praktycznie funkcjonujących modeli współdziałania, gdzie jest budowane wzajemne zaufanie poprzez wspólną pracę oraz wspólne podejście do tematyki, a także usystematyzowana wiedza merytoryczna.

Rekomenduje się, w kolejnych edycjach Polityki lub nowej strategii cyberbezpieczeństwa, stworzenie faktycznych warunków do powoływania tego rodzaju pełnomocników w kluczowych podmiotach gospodarki – w tym uwspólnianie rozwiązań wynikających z RPOC i NPOIK – w kwestii pełnomocników ochrony.

Ustanowieni pełnomocnicy powinni stanowić ogniwo współpracy danych instytucji z zespołami CSIRT oraz Koordynatorem.

6.3.12 Nieformalne fora współpracy

W obszarze bezpieczeństwa teleinformatycznego kwestia istnienia praktycznych mechanizmów współpracy pomiędzy zespołami reagującymi na incydenty jest kluczowa dla skoordynowanego przeciwdziałania zagrożeniom oraz istotnie wspiera szybką wymianę informacji, co zasadniczo skraca czasy rozwiązywania problemów.

Chociaż, z jednej strony, w systemie ochrony cyberprzestrzeni na poziomie krajowym jest niezbędne ustanowienie formalnych, osadzonych w prawodawstwie elementów, takich jak podmioty odpowiedzialne za wdrażanie polityk czy reagowanie na zdarzenia naruszające bezpieczeństwo, a także przewidzenie formalnych mechanizmów oraz ścieżek współpracy, to nie należy zapominać o popieraniu istnienia nieformalnych ciał, forów lub mechanizmów zapewniających współpracę, funkcjonujących na zasadach dobrowolności.

Przykładem takiej inicjatywy jest polskie ABUSE Forum zrzeszające zespoły CSIRT i inne zespoły zajmujące się bezpieczeństwem w wielu typach instytucji (operatorzy

[65] W obszarze infrastruktury krytycznej wcześniej powstała funkcja pełnomocnika ds. Ochrony infrastruktury krytycznej

telekomunikacyjni, banki, portale społecznościowe, środowisko akademickie). W ramach ABUSE Forum, działającego od roku 2005, przedstawiciele około trzydziestu znaczących firm i instytucji (w tym wszystkie znaczące CSIRTy w kraju) dzielą się informacjami na temat zagrożeń, współpracują w ramach rozwiązywania problemów, cyklicznie spotykają się w celu omawiania tematów technicznych i organizacyjnych nurtujących całą społeczność.

Nieformalny charakter ABUSE Forum jest, być może paradoksalnie, siłą tej inicjatywy. Nierzadko podmioty zrzeszone w forum konkurują ze sobą na płaszczyźnie biznesowej. Dość trudno byłoby więc zawrzeć formalne umowy współpracy pomiędzy wszystkimi uczestnikami. Jednakże na poziomie technicznym istnieje powszechne zrozumienie, że współpraca jest koniecznością, niezależnie od tego, czy istnieją formalne ścieżki oraz ściśle zdefiniowany zakres.

Oprócz tego, praktyka współpracy CSIRTów na całym świecie pokazuje, że bez zbudowania zaufania pomiędzy zespołami/członkami poszczególnych zespołów reagujących efektywna współpraca nie może mieć miejsca i zawieranie formalnych porozumień nie jest czynnikiem decydującym. Częstokroć ważniejsze od formalnych porozumień o współpracy jest faktyczna współpraca, oparta na wzajemnym zaufaniu i wiedzy co do kompetencji partnera.

Nieformalne inicjatywy, takie jak ABUSE Forum przyczyniają się właśnie do budowania relacji pomiędzy zespołami i ich członkami, co potem procentuje w przypadku sytuacji kryzysowej w cyberprzestrzeni, która często dotyka operatorów w kilku sektorach (np. rozprzestrzenianie się nowego trojana bankowego na urządzeniach mobilnych w sieciach operatorów komórkowych).

6.3.13 SOC (Security Operations Center)

Centra monitorujące stan bezpieczeństwa infrastruktury informatycznej i reagujące na pojawiające się incydenty oraz zagrożenia stają obecnie jednym z obowiązkowych elementów zarządzania IT, szczególnie w dużych przedsiębiorstwach posiadających rozbudowane systemy komputerowe i sieciowe.

Centra SOC (Security Operations Center), aby móc dobrze spełniać swą rolę, powinny działać w trybie ciągłym (24h/dobę), czyli mieć zapewnioną prace zmianową. Infrastruktura techniczna centrum powinna składać się z systemów informatycznych pozwalających na monitorowanie stanu bezpieczeństwa, alarmowanie w sytuacjach podejrzenia wystąpienia zagrożenia lub naruszenia bezpieczeństwa (systemy wczesnego ostrzegania, system SIEM korelujący logi, dzienniki flows i inne informacje napływające ze wszystkich systemów podwyższających bezpieczeństwo, jak również z systemów i aplikacji będących pod ochroną).

Personel SOC musi się charakteryzować najwyższymi kompetencjami w dziedzinie bezpieczeństwa teleinformatycznego.

Powyższe cechy (podstawowe) SOC jednoznacznie determinują, że powołanie efektywnego centrum nie jest sprawą łatwą.

Utrzymywanie grupy osób, która w sposób zmianowy jest w stanie całą dobę przez cały rok monitorować stan bezpieczeństwa stanowi duży koszt dla organizacji. Dodatkowo, z reguły w SOC występuje kilka linii operacyjnych: pierwsza linia, która monitoruje alerty pojawiające się na konsolach i uruchamiające dalsze działania oraz jedna lub więcej linii personelu analitycznego, który jest w stanie rozwiązywać zaawansowane problemy spowodowane danym incydentem naruszającym bezpieczeństwo (wyśledzenie źródła problemu, opracowanie technicznych sposobów zabezpieczenia, zabezpieczenie dowodów itd.). Aby wdrożenie SOC mogło przynieść spodziewane korzyści, personel centrum musi współpracować z administratorami poszczególnych systemów, którzy rozumieją kwestie bezpieczeństwa teleinformatycznego.

Infrastruktura dedykowana SOC to także spore obciążenie inwestycyjne, utrzymaniowe i rozwojowe. Dodatkowo, systemy wspierające monitorowanie bezpieczeństwa całej infrastruktury, takie jak SIEM wymagają sporych zasobów (wiedzy eksperckiej i czasu), aby stale je dostosowywać do specyfiki danej organizacji i zmiennego otoczenia. Wiele wdrożeń SOC zakończyło się niepowodzeniem z powodu tego, że masa dodatkowej informacji w postaci dużej ilości pojawiających się alertów nie mogła być obsłużona w praktyce przez personel z powodu np. zbyt szeroko skonfigurowanych scenariuszy alertowania, braku kwalifikacji personelu czy szczupłości zasobów ludzkich.

Dlatego też centra SOC powstają w dużych organizacjach (operatorzy telekomunikacyjni, duże banki, przedsiębiorstwa infrastruktury krytycznej), gdzie istnieje uzasadnienie biznesowe i zgoda zarządu na dedykowanie odpowiedniego budżetu na zatrudnienie i utrzymanie specjalistów, systematyczne szkolenia, wdrożenie i utrzymanie infrastruktury technicznej (systemy informatyczne, pomieszczenia itp.), a także determinacja organizacyjna, aby powstały i były przestrzegane procedury związane z funkcjonowaniem SOC na odpowiednim poziomie.

Mniejsze organizacje mogą za to korzystać z coraz bardziej rozwijanych usług typu MSP (ang. *managed security services)* w zakresie SOC. W takim modelu jeden usługodawca obsługuje wielu klientów, dedykując im odrębne instancje w swoich systemach, co pozwala na monitorowanie bezpieczeństwa ich systemów. Klient nie musi wtedy posiadać służb działających 24h/dobę (może funkcjonować dyżur pod telefonem), otrzymuje informacje o alertach, zalecenia odnośnie środków zaradczych, a także raporty okresowe. Ważne, aby

umowa klienta z dostawcą gwarantowała określone SLA i zawierała postanowienia odnośnie ochrony danych klienta.

Możliwy jest również model, kiedy takie centrum jest budowane dla całego sektora, np. administracji rządowej.[66] Wtedy, wykorzystując efekt skali i rozłożenia kosztów na wielu interesariuszy, można zapewnić standard bezpieczeństwa uwzględniający specyfikę danego sektora.

Można postawić pytanie, jakie są podobieństwa oraz różnice pomiędzy koncepcją centrum SOC a trybem i zakresem funkcjonowanie zespołu CSIRT.

Centrum SOC jest bezpośrednio związane z daną infrastruktura teleinformatyczną podlegającą ochronie. Oznacza to, że na bieżąco otrzymuje logi, dzienniki flows i traps oraz inne informacje z serwerów, aplikacji, systemów firewall, antywirusowych, IDS, antymalware, a także z routerów, switchy, czy baz danych. Również, jeśli mamy do czynienia z modelem MSP, informacje z systemów klientów na bieżąco spływają do systemów SIEM w SOC.

Z kolei zespoły CSIRT nie muszą być bezpośrednio (technicznie) związane z daną infrastrukturą. Mogą dysponować systemami wczesnego ostrzegania z sondami rozmieszczonymi w wielu miejscach sieci (działanie proaktywne), ale ich zasadniczym *modus operandi* jest reagowanie na zgłoszenia, a także wymiana informacji z jak największą ilością CSIRTów i innych organizacji zajmujących się bezpieczeństwem w celu pozyskania jak najlepszego obrazu sytuacyjnego (*situational awareness*), dotyczącego własnego obszaru działania (zdefiniowanego jako *constituency*).

Ogólnie można stwierdzić, że powstawanie centrów SOC to kierunek godny polecenia. Takie centra, jeśli pokonają bariery wymienione wyżej, stają się między innymi naturalnymi partnerami do współpracy z CSIRTami.

Przykładowo, działający SOC w przedsiębiorstwie infrastruktury krytycznej, współpracując z CSIRTem sektorowym, otrzymuje na bieżąco obraz sytuacyjny dotyczący mapy zagrożeń w sektorze (w tym np. alerty o zagrożeniach w innych krajach w podobnych sektorach), a z kolei CSIRT sektorowy korzysta z informacji o incydentach zauważonych w poszczególnych przedsiębiorstwach, by móc na to reagować w postaci ostrzegania innych przedsiębiorstw czy poprzez asystę w rozwiązywaniu incydentów przez współpracujący SOC.

[66] NASK przedstawił taką koncepcję na seminarium ”Bezpieczeństwo teleinformatyczne jako element integrujący systemy informatyczne administracji?” w MAC w marcu 2014 r, opartą na realizacji bezpiecznego węzła internetowego dla administracji wraz z ustanowieniem SOC dla partycypujących urzędów i instytucji.

6.3.14 Punkt przyjmowania zgłoszeń o nielegalnych lub niepożądanych treściach (m.in. CSAM[67]) - Hotline

W ramach tematyki ochrony w Internecie czy w cyberprzestrzeni istotnym aspektem bezpieczeństwa jest nie tylko aspekt technologiczny i związane z nim zagrożenia oraz incydenty, ale także kwestia ochrony użytkowników – szczególnie młodych - przed zagrożeniami od strony szkodliwych czy nielegalnych treści[68].

Od 2004 roku działa w strukturach NASK zespół Dyżurnet.pl, który w ramach programu Safer Internet (a obecnie CEF-*Connecting Europe Facility*) zajmuje się przyjmowaniem zgłoszeń od Internautów na temat nielegalnych lub szkodliwych treści (w szczególności CSAM). Ten punkt kontaktowy, działający w NASK, jest częścią Polskiego Centrum Safer Internet powołanego przez NASK i Fundację Dzieci Niczyje. Dużurnet.pl jest członkiem stowarzyszenia INHOPE, które zrzesza podobne zespoły z całej Europy, a także spoza naszego kontynentu.

Zespół w swej działalności współpracuje z dostawcami treści, Policją i podobnymi zespołami na całym świecie, a rodzaj współpracy przy przeciwdziałaniu rozpowszechnianiu szkodliwych lub nielegalnych treści w dużej mierze przypomina działania zespołów CSIRT. Zresztą w Polsce istnieje ścisła współpraca pomiędzy Dyżurnet.pl oraz CERT Polska w zakresie konsultacji co do technologicznej strony zjawiska.

Wskazane byłoby ustanowienie jak najbardziej efektywnej formuły funkcjonowania zespołu hotline (Dyżurnet.pl) w polskiej rzeczywistości w kontekście ram prawnych, potrzebnej współpracy z organami ścigania, operatorami i dostawcami treści, czy zespołami CSIRT.

6.3.15 Zespół Łącznikowy

Zespół Łącznikowy to zespół składający się z przedstawicieli kluczowych instytucji administracji państwa odgrywających istotną rolę w zapewnianiu bezpieczeństwa cyberprzestrzeni.

Rekomenduje się także, aby Zespół Łącznikowy rozwijał się w ramach zdobywania praktycznych doświadczeń we współpracy stron, w kierunku angażowania (na stałe lub w zależności od potrzeb) przedstawicieli spoza administracji publicznej.

[67] CSAM: Child Sexual Abuse Material – treści z seksualnym wykorzystaniem małoletnich, zwane także pornografia dziecięcą

[68] W programie Safer Internet Komisji Europejskiej jest mowa o treściach nielegalnych, takich jak : CSAM, rasizm, ksenofobia a także innych, szkodliwych, z którymi, w szczególności młodzi użytkownicy Internetu nie powinni mieć kontaktu.

Przedstawiciele poszczególnych instytucji uczestniczący w pracach Zespołu ściśle współpracują z CSIRTem krajowym, również na poziomie operacyjnym. Koncepcja Zespołu zakłada, że jego członkowie osobiście spotykają się regularnie z przedstawicielami CSIRTu krajowego. Na bieżąco uzyskują informacje o poważnych zagrożeniach i uczestniczą (wspierają działania CSIRTu) w rozwiązywaniu problemów dużej rangi (również konkretnych incydentów), jak też zauważonych problemów systemowych. Zespół Łącznikowy powinien zatem mieć siedzibę przy zespole CSIRTu krajowego. Spotkania zespołu i CSIRTu powinny odbywać się regularnie (np. dwa razy w tygodniu), oprócz tego każdy z łączników powinien mieć możliwość indywidualnych spotkań z pracownikami CSIRTu krajowego.

Zespół Łącznikowy tworzy raporty dotyczące bieżących incydentów oraz zauważonych problemów systemowych (np. luki w systemie bezpieczeństwa cyberprzestrzeni), może tworzyć rekomendacje i przedstawia je macierzystym instytucjom oraz instytucji Koordynatora. Wyznaczeni łącznicy, będąc oddelegowanymi (np. na część etatu) pracownikami macierzystych instytucji mają możliwość bezpośredniego przekazywania informacji do swoich instytucji, jak również powinni mieć możliwość występowania o konkretne wsparcie do kierownictwa danej instytucji, jeśli bieżąca sytuacja będzie tego wymagała.

Oficjalnie Zespół jest powoływany przez Koordynatora, na podstawie wyznaczenia danej osoby przez macierzystą instytucję. Instytucje rządowe, przynajmniej w pierwszym etapie, mogą delegować swych pełnomocników ochrony cyberprzestrzeni do pracy w Zespole. **Trzeba jednak zwrócić uwagę, że ze względu na charakter pracy, łącznicy powinni dysponować odpowiednią wiedzą techniczną w zakresie technologii informatycznych i bezpieczeństwa, rozeznaniem co do funkcjonowania systemu cyberbezpieczeństwa, a także powinni móc realnie poświęcić odpowiednią ilość swojego czasu na pracę w Zespole Łącznikowym.**

Proponuje się aby w pierwszym etapie zespół składał się minimalnie z przedstawicieli następujących instytucji:

- Ministerstwo Administracji i Cyfryzacji,
- Ministerstwo Spraw Wewnętrznych,
- Ministerstwo Obrony Narodowej,
- Agencja Bezpieczeństwa Wewnętrznego,
- Policja,
- Rządowe Centrum Bezpieczeństwa,
- Ministerstwo Spraw Zagranicznych,
- Ministerstwo Finansów,

- Biuro Bezpieczeństwa Narodowego,
- Narodowe Centrum Kryptologii
- Narodowy Bank Polski.

Współpraca z CSIRTem krajowym jest głównym elementem pracy zespołu. Dodatkowo, należy rozważyć włączanie do zespołu, czasowo lub na stałe, przedstawicieli CSIRTów sektorowych, w miarę ich powstawania.

Tak jak zaznaczono wyżej, zespół powinien się rozwijać, wypracowując swój optymalny *modus operandi* oraz skład instytucjonalny (permanentny oraz czasowo rozbudowywany w zależności od bieżących potrzeb).

6.3.16 Organa ścigania cyberprzestępstw

Organa ścigania cyberprzestępstw są ważnym elementem krajowego systemu ochrony cyberprzestrzeni.

Rekomenduje się opracowanie w Polsce kilkuletniego Narodowego Programu do Walki z Cyberprzestępczością, na wzór chociażby programu przyjętego w obszarze walki z terroryzmem[69].

Obecnie kwestie walki z cyberprzestępczością są niedocenianym a koniecznym elementem każdego skoordynowanego działania, zarówno na poziomie strategiczno-politycznym, jak również na poziomie operacyjnym.

Od roku 2014 w Policji zaczęto powoływać specjalne wydziały do walki z cyberprzestępczością. Powstały one zarówno w Komendzie Głównej Policji, Komendzie Stołecznej Policji, jak i w komendach wojewódzkich w całej Polsce. Jest to krok w dobrym kierunku.

Bezpieczeństwo cyberprzestrzeni RP jest silnie uzależnione od skuteczności zwalczania cyberprzestępczości przez organa ścigania. Największe ryzyka dla osób prywatnych oraz przedsiębiorców związane są bowiem z najpowszechniejszymi rodzajami złośliwego oprogramowania, takimi jak trojany bankowe czy ransomware oraz z atakami DDoS.[70] Każde z tych zjawisk daje się obecnie zakwalifikować jako przestępstwo. Ich ściganie nastręcza jednak polskim organom ścigania poważne problemy na każdym etapie – od przyjęcia zgłoszenia po wydanie wyroku skazującego. Z drugiej strony, w Polsce od wielu lat obserwujemy rozwój rynku złośliwego oprogramowania oraz tworzenie się grup

[69] Por. Narodowy Program Antyterrorystyczny na lata 2015-2019.
[70] Por. raporty roczne CERT Polska: http://www.cert.pl/raporty/langswitch_lang/pl

przestępczych zajmujących się realizacją zysków z cyberprzestępczości, nie tylko z terenu Polski.

Postulujemy, aby Policja była stałym uczestnikiem Zespołu Łącznikowego, co najmniej za pośrednictwem przedstawiciela Wydziału do Walki z Cyberprzestępczością BSK KGP. Postulat taki wpisuje się w zadania przypisane temu wydziałowi, do których należy[71]:

- inicjowanie i koordynowanie działań Policji w zakresie identyfikowania głównych zagrożeń przestępstwami w sieci Internet, metod i form ich zwalczania oraz współdziałania jednostek Policji z organami i podmiotami pozapolicyjnymi w celu ich skutecznego zwalczania;
- współpraca na szczeblu krajowym i międzynarodowym z instytucjami państwowymi oraz sektorem prywatno – publicznym w zakresie pozyskiwania informacji o metodach i formach przestępstw popełnianych w cyberprzestrzeni, w tym pozyskiwanie i współpraca z Osobowymi Źródłami Informacji;
- opracowywanie rodzaju współpracy z podmiotami sektorów publicznych, prywatnych i akademickich oraz ustalanie kanałów i sposobu gromadzenia i wymiany informacji o przestępstwach oraz zabezpieczenia dowodów cyberprzestępstw;
- prowadzenie wieloźródłowych konsultacji technicznych i współpracy z podmiotami krajowymi i zagranicznymi zmierzających do rozpoznawania i wdrażania nowoczesnych rozwiązań w walce z przestępczością popełnianą w świecie wirtualnym.

Przedstawiciel tego wydziału powinien prowadzić z CSIRTem Krajowym ścisłą współpracę także poza Zespołem Łącznikowym. Podczas regularnych spotkań (nie rzadziej niż co dwa tygodnie) powinna następować stała wymiana informacji o bieżących zagrożeniach. Rolą policji powinno być ustalanie priorytetów w zwalczaniu konkretnych przypadków cyberprzestępstw i korzystanie z zasobów wiedzy CSIRTu krajowego (a za jego pośrednictwem także Centrum Analitycznego) do efektywnego zbierania materiałów operacyjnych oraz procesowych. Kompetencje CSIRTu krajowego powinny być także wykorzystywane przez Policję podczas skoordynowanych akcji międzynarodowych, prowadzonych między innymi przez Interpol czy Europol. Należy zwrócić uwagę, że realizacja wsparcia dla policji ze strony CSIRTu krajowego wymaga zapewnienia odpowiednich zasobów po stronie tego podmiotu.

Innym podmiotem ze strony Policji, który mógłby być zaangażowany w system łączników jest Wydział Zwalczania Cyberprzestępczości CBŚP, przy czym należy pamiętać, że głównym obszarem zainteresowania CBŚP jest przestępczość zorganizowana.

[71] Źródło: http://www.policja.pl/pol/kgp/bsk/struktura/wydzialy/wydzial-do-walki-z-cybe/87086,Wydzial-do-Walki-z-Cyberprzestepczoscia.html

Należy także spowodować, aby CSIRT Krajowy miał możliwość zgłaszania Policji obserwowanych przez siebie przypadków cyberprzestępstw. W chwili obecnej, mimo pełnej świadomości tego, że prawo jest łamane, sama obserwacja botnetu i jego ofiar jest niewystarczająca do zgłoszenia przestępstwa, jeśli nie zgłoszą się osoby poszkodowane, bowiem przestępstwa z art. 267 Kodeksu karnego ścigane są na wniosek pokrzywdzonego, który często nie ma wiedzy, że stał się ofiarą przestępstwa.

Wreszcie, CSIRT Krajowy powinien być wykorzystywany do budowania kompetencji w organach ścigania, nie tylko w Policji, ale także w prokuraturach i innych organach wymiaru sprawiedliwości. Należy w tym celu zapewnić zasoby po stronie CSIRTu Krajowego na organizację regularnych szkoleń, uwzględniających bieżący stan wiedzy i najnowsze zagrożenia.

Rozwój kompetencji w organach ścigania nie będzie możliwy bez zapewnienia odpowiedniego poziomu finansowania także w samej Policji i prokuraturach. Obecnie częste są przypadki rezygnowania przez Policję z udziału w szkoleniach czy warsztatach (także bezpłatnych, np. organizowanych przez Europol), ze względu na brak funduszy na pokrycie choćby kosztów dojazdu czy zakwaterowania. Jest to zjawisko tym bardziej niebezpieczne, że skuteczne ściganie sprawców cyberprzestępstw jest w praktyce niemożliwe bez stałego zapoznawania się z najnowszymi technologiami i metodami pracy przestępców. Dodatkowe fundusze na walkę z cyberprzestępczością powinny być w szczególności przeznaczone na zwiększenie liczby etatów w Policji (dedykowanych do przypadków cyberprzestępczości), szkolenia, udziału w grupach roboczych i konferencjach międzynarodowych, a także zapewniania zaplecza technicznego do analizy zagrożeń (również w formie zakupu usług).

Istotnym kanałem komunikacji jest również współpraca operacyjna z zespołem hotline do walki z nielegalnymi i szkodliwymi treściami w Internecie (zespół Dyżurnet.pl).

Policja powinna także być aktywnym uczestnikiem Platformy wymiany informacji o zagrożeniach.

6.3.17 System wczesnego ostrzegania o zagrożeniach

Jednym z dotychczasowych sukcesów w zakresie ochrony cyberprzestrzeni w Polsce było wdrożenie w administracji państwowej systemu monitorowania i wczesnego ostrzegania o zagrożeniach w sieci - ARAKIS-GOV, wspólnego przedsięwzięcia ABW i NASK.[72] System jest wdrożony w kilkudziesięciu podmiotach administracji. System został zaktualizowany w ostatnich latach tak, aby sprostać ewolucji zagrożeń i rozszerzać jego funkcjonalność. System ARAKIS 2.0 GOV obecnie jest wdrażany produkcyjnie. System posiada modułową budowę, umożliwiającą dostosowanie różnych funkcjonalności

[72] http://www.cert.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html

w zależności od zapotrzebowania. Działa w oparciu o rozproszoną sieć sensorów. Jest zasilany wiedzą z platformy n6[73], w tym wskaźnikami infekcji (*indicators of compromise*) dostarczającymi przez zewnętrznych analityków. Dzięki temu system posiada możliwie najbardziej aktualne informacje np. o serwerach C&C, złośliwych adresach IP, źródłach phishingu, itp., które wykorzystuje do wykrywania infekcji wewnątrz chronionych sieci. Poza danymi z sieci produkcyjnej system zasilany jest wiedzą o zdarzeniach wykrytych przez chmurę honeypotów. System posiada rozbudowane możliwości analityczne, w tym własny język zapytań.

Informacje o zagrożeniach wykrytych w sieciach administracji państwowej stanowią podstawę reakcji na incydenty bezpieczeństwa. Zalecane jest, żeby system ten stanowił integralną część organizacji ochrony cyberprzestrzeni w Polsce, a swoim zasięgiem obejmował wszystkie podmioty administracji państwowej. Jego funkcjonowanie powinno okresowo być poddawane ocenie (np. poprzez powołany przez Koordynatora Zespoł Zadaniowy). Konieczne jest też przyznawanie środków na dalszy rozwój funkcjonalności tak, aby system był w stanie sprostać nowo pojawiającym się typom zagrożeń.

6.3.18 Łowcy

Nowością, którą proponujemy, jeżeli chodzi o działania proaktywne w zakresie ochrony cyberprzestrzeni RP, są usługi łowieckie (ang. *hunting*). Propozycja wiąże się z założeniem, bardzo często spotykanym, w szczególności w środowisku amerykańskim, że w każdej instytucji prędzej czy później dojdzie do włamania. Istotą systemu przeciwdziałaniu zagrożeniom w sieci jest więc nie tylko zapobiegnięcie włamaniu (oczywiście nie znaczy to, że nie należy inwestować w tego typu ochronę), ale również maksymalne skrócenie okna czasowego jego wykrycia, tak aby nie zostały wyrządzone rzeczywiste szkody (np. nie nastąpiła eksfiltracja istotnych danych). W tym kontekście pojawia się zapotrzebowanie na nowy rodzaj usługi: zespołów bezpieczeństwa, których głównym zadaniem będzie okresowe sprawdzanie sieci podmiotów (np. państwowych) w celu wykrycia, czy instytucja nie została spenetrowana. W proponowanych modelach organizacji ochrony cyberprzestrzeni w Polsce zespoły takie mogłyby być organizowane przez Koordynatora (w tym poprzez zakontraktowanie podmiotów komercyjnych) lub przez CSIRT rządowy czy krajowy. Podobnie - dla podmiotów infrastruktury krytycznej - mógłby postępować CSIRT-IK. Dodatkowo, należy rozważyć możliwość wsparcia przez Państwo w tym zakresie innych podmiotów.

[73] n6.cert.pl

6.4 Usługi CSIRT, które muszą być realizowane niezależnie od przyjętego wariantu

Zakres usług świadczonych przez zespoły CSIRT został zdefiniowany przez CERT/CC w dokumencie "*Handbook for Computer Security Incident Response Teams (CSIRTs)*" w 1998 roku (dokument został zaktualizowany w 2003 roku[74]). Uznawany jest za wzorcowy, również przez agencję ENISA, która na jego bazie stworzyła wiele dokumentów, w tym istotny w kontekście rozpatrywanych w tej ekspertyzie zagadnień i wspomniany już "*Deployment of Baseline Capabilities of n/g CERTs - Status Report 2012*".

Jednakże model ten, który zasadniczo od jego utworzenia w ubiegłym wieku nie przeszedł znaczących zmian odzwierciedlających ewolucję zagrożeń informatycznych, obecnie uważany jest już za przestarzały. Fakt ten skłonił szereg krajowych CSIRTów do podjęcia działań w ramach światowej organizacji FIRST[75] w celu zredefiniowania katalogu usług tak, aby lepiej odpowiadały wymaganiom stawianym przed współczesnymi zespołami CSIRT. Tworzony katalog ma służyć jako nowa baza materiałowa do przeprowadzania szkoleń.

Nowy dokument opisujący zakres usług znajduje się obecnie w fazie późnego draftu (określanego mianem "*first final draft*", w którym jeszcze możliwe będą drobne zmiany). Ponieważ autorzy ekspertyzy w pełni zgadzają się z tym, że możliwości starego katalogu usług CSIRT - tak jak został on zdefiniowany pod koniec lat 90-tych - zostały wyczerpane, niniejsza ekspertyza będzie wykorzystywać pojęcia wypracowane w nowym katalogu, wg dokumentu "*CSIRT Services Framework - first final draft*" omawianego na spotkaniu w czasie konferencji FIRST 2015 w Berlinie, 14 czerwca 2015 roku. Warto nadmienić, że CERT Polska miał wymierny udział merytoryczny w procesie powstawania tego dokumentu.

Nowy katalog definiuje 7 podstawowych usług zespołów CSIRT. Usługi te dzielą się na funkcje (niezbędne do realizacji usługi) oraz podfunkcje. Przykładowo, usługa 1 nazwana jest Zarządzanie Incydentem (ang. *Incident Management*). W jej skład wchodzą dwie funkcje - Obsługa Incydentu (ang. *Incident Handling*) oraz Zarządzanie Podatnościami, Konfiguracją oraz Zasobami (ang. *Vulnerability, Configuration and Asset Management*). W tej ekspertyzie celowo pomijamy omawianie podfunkcji jako zadanie zbyt szczegółowe jak na potrzeby niniejszego opracowania - tym bardziej, że jest możliwe, że nastąpią w nich jeszcze zmiany. Jednakże w przyszłości system cyberbezpieczeństwa powstały w Polsce powinien wzmiankowane podfunkcje uwzględniać.

[74] http://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf. Prezentowany jest również na stronie http://www.cert.org/incident-management/services.cfm?
[75] https://www.first.org/

Dodatkowo, nowy model wprowadza trzy pojęcia, które obejmują ogólną zdolność do świadczenia usług jak i funkcji: poziom zdolności (*capability*), możliwość przepustową (*capacity*) oraz poziom dojrzałości (*maturity*). Na dzień dzisiejszy na spotkaniach roboczych, dla oceny danego poziomu proponowane były skale 5-stopniowe, jednakże nie ma jeszcze ich oficjalnego potwierdzenia. **W niniejszym opracowaniu zakładamy, że maksymalne poziomy dla każdej z wymienionych usług czy funkcji nie muszą być reprezentowane w pojedynczym podmiocie: rekomendujemy jednak, żeby system ochrony jako całość dążył do maksimum w każdej kategorii.** Rolą Koordynatora byłoby zinwentaryzowanie możliwości wszystkich podmiotów uczestniczących w ochronie cyberprzestrzeni RP, tak aby zapewnić maksima w obszarze każdej usługi. W szczególności w razie wystąpienia większego incydentu lub sytuacji kryzysowej, Koordynator powinien odpowiednio rozdysponować zadania względem możliwości deklarowanych przez różne podmioty.

Warto w kontekście nowego modelu zwrócić uwagę na wyróżnienie usług, takich jak działania badawcze i rozwój narzędzi (znacznie słabiej akcentowane w starym modelu), a także na rozwój świadomości sytuacyjnej i analityki, co naszym zdaniem wzmacnia argumentacje za powstaniem Centrów Analitycznych.

Wyróżnione zostały następujące usługi (dla większej czytelności nazwy usług pozostawiamy w wersji angielskiej):

Usługa 1: Incident Management

Szeroko pojęte zarządzanie incydentem, na które składają się:

1.1 Incident Handling

Usługi związane z zarządzaniem incydentami w cyberprzestrzeni, łącznie z ostrzeganiem o zdarzeniach bezpieczeństwa, koordynowaniem działań reagujących, podejmowanie działań ograniczających rozprzestrzenienieie się zagrożenia oraz jego usunięcie. Usługa ta jest blisko powiązana z Usługą 2, czyli analizą.

Jest to podstawa systemu reakcji na zdarzenia bezpieczeństwa i podstawowy element usług CSIRT - świadczona powinna być przez wszystkie wyróżnione zespoły CSIRT, niezależenie od przyjętego modelu wariantowego. Koordynator uczestniczy w najpoważniejszych incydentach i sytuacjach nadzwyczajnych, w pozostałych odbiera jedynie raporty z CSIRTu krajowego/rządowego. Koordynator rozstrzyga spory kompetencyjne i ew. powołuje Zespoły Zadaniowe.

Podmioty świadczące usługę na 5: CSIRT krajowy, CSIRT rządowy.

1.2 Vulnerability, Configuration and Asset Management

Usługi związane z zarządzaniem wiedzą o podatnościach, sposobach im przeciwdziałania, konfiguracjami oprogramowania i inwentarzem zasobów.

Usługa w szczególności dotyczy CSIRTu rządowego i innych CSIRTów sektorowych, pełnomocników i administratorów sieci, ale też centrów ISAC, ponieważ wymaga szczegółowej znajomości używanych rozwiązań. Na poziomie ogólnych zaleceń dotyczy też CSIRTu Krajowego. Istnieje też tutaj rola dla Centrum Analitycznego, które byłoby w stanie zgłębiać i analizować dane podatności i oprogramowanie je wykorzystujące - odkrycia byłyby wkładem do zaleceń na poziomie krajowym i sektorowym.

Podmioty ze zdolnościami na 5: CSIRT krajowy, CSIRT rządowy.

Usługa 2: Analysis

Szeroko pojęte usługi związane z analityką.

2.1 Incident Analysis

Usługa identyfikacji i określenia charakterystyk zdarzeń lub incydentu, takich jak: zasięg, dotknięte podmioty, systemy, zakres czasowy (kiedy wykryty, zaraportowany lub rozwiązany), itp. Bardziej szczegółowe analizy znajdują się w dalszych punktach.

Każdy CSIRT, SOC powinien zapewniać podstawowe możliwości w zakresie analizy incydentu, stosownie do swojego sektora czy obszaru infrastruktury Wymiana informacji na ten temat powinna się odbywać poprzez platformę wymiany informacji. Incydenty rozpoznane jako bardziej złożone przez któryś z zespołów CSIRT powinny być przekazane Centrum Analitycznemu i CSIRTowi krajowemu, a te o największym stopniu zagrożenia, również Koordynatorowi (poprzez CSIRT krajowy lub rządowy).

Podmioty świadczące usługę na 5: CSIRT krajowy, CSIRT rządowy.

2.2 Artifact Analysis

Usługi związane z analizą i zrozumieniem możliwości oraz intencji działania artefaktów (np. plików złośliwego oprogramowania - *malware*, exploitów, spamu) i sposobach ich dystrybucji, ich wykrywania oraz neutralizacji.

Podmiotem wiodącym w tym zakresie powinno być Centrum Analityczne. Jednakże również CSIRT krajowy i rządowy powinny posiadać duże możliwości w takim zakresie. Pozostałe jednostki mogą mieć w tym aspekcie tylko podstawowe zdolności.

Podmioty świadczące usługę na 5: Centrum Analityczne.

2.3 Media Analysis

Usługi obejmujące analizę danych z systemów, sieci, nośników przechowywania i nośników wymiennych tak, aby lepiej zrozumieć, jak zapobiegać, wykrywać i / lub łagodzić

podobne lub powiązane incydenty. Usługi te mogą być również świadczone na potrzeby postępowań organów ściągania i sądów.

Podmiotem wiodącym w tym zakresie powinno być Centrum Analityczne. CSIRT krajowy i rządowy może dysponować ograniczonymi możliwościami w tym zakresie. Analizy takie mogą być świadczone również przez organy ścigania albo zlecane podmiotom prywatnym. W szczególności zaleca się, aby w miarę możliwości wykorzystywać w tym procesie podmioty komercyjne.

Podmioty świadczące usługę na 5: Centrum Analityczne razem z podmiotami komercyjnymi.

2.4 Vulnerability/Exploitation Analysis

Usługi polegające na szczegółowej i głębokiej analizie podatności i sposobach jej wykorzystania.

Podmiotem wiodącym w tym zakresie powinno być Centrum Analityczne. CSIRT krajowy i rządowy może dysponować ograniczonymi możliwościami w tym zakresie. W szczególności zaleca się, aby w miarę możliwości wykorzystywać w tym procesie podmioty komercyjne.

Podmiot świadczący usługę na 5: Centrum Analityczne.

Usługa 3: Information Assurance

Usługi związane z szeroko pojętym *information assurance*.

3.1 Risk/Compliance Assessment

Usługi związane z działalnością w zakresie oceny ryzyka, oceny zgodności (*compliance*), w tym ich przeprowadzenia. Zazwyczaj odbywają się w kontekście wymogu zgodności ze standardami (np ISO 27XXX, COBIT). Usługi obejmują również testy penetracyjne i wszelkie audyty.

Proponujemy, aby podmiotem odpowiedzialnym w tym zakresie był Koordynator we współpracy z podmiotami komercyjnymi (wyłonionymi w drodze konkursu). Koordynator może powołać Zespół Zadaniowy, który ma na celu nadzór tego rodzaju prac. W poszczególnych podmiotach państwowych zagadnienie nadzorują Pełnomocnicy ds. ochrony informacji. Jednostki mogą też zlecać tego typu oceny podmiotom komercyjnym niezależenie, po konsultacjach z Koordynatorem. W działaniach mogą brać również udział łowcy, opisani w rozdziale 6.3.18, którymi mogą dysponować zarówno CSIRT krajowy i rządowy jak i podmioty prywatne.

Podmiot świadczący usługę na 5: Koordynator przy wsparciu z podmiotów zewnętrznych.

3.2 Patch Management

Usługi mające na celu wspomaganie *constituency* w zakresie inwentaryzacji systemów IT, stopnia ich aktualności/załatania, wdrażania i weryfikacji instalacji poprawki.

Wiodące role w tym zakresie mają CSIRTy sektorowe (w tym rządowy), powstałe zespoły SOC oraz pełnomocnicy ds. ochrony cyberprzestrzeni. Nie oznacza to, że sam CSIRT sektorowy powinien bezpośrednio zajmować się całym procesem, jednakże powinien blisko współpracować ze swoim sektorem, a same instytucje powinny wykonywać te działania we własnym zakresie, zgodnie z wytycznymi.

Podmiot świadczący usługę na 5: CSIRTy sektorowe + zespoły SOC + pełnomocnicy + członkowie sektora (razem).

3.3 Operation Policies Management

Usługa polegająca na zarządzaniu politykami i scenariuszami działań operacyjnych - rozwój, utrzymanie i wdrażanie procedur oraz procesów w instytucjach.

Opracowywaniem procedur w skali krajowej zajmuje się Koordynator poprzez powołanie Zespołu Zadaniowego. Nad wdrażaniem procedur w administracji rządowej czuwają pełnomocnicy ds. ochrony informacji, którzy raportują do Koordynatora poprzez CSIRT rządowy. W innych sektorach zalecenia są przekazywane jako best practice.

Podmioty świadczące usługę na 5: Koordynator + CSIRT rządowy + pełnomocnicy.

3.4 Risk Analysis/Business Continuity Disaster Recovery Advisement

Usługi świadczone na rzecz *constituency* w celu zwiększenia odporności organizacyjnej na podstawie zidentyfikowanego ryzyka. Może to obejmować szereg działań w odniesieniu do zarządzania ryzykiem, od przeprowadzenia rzeczywistej oceny do udzielania wsparcia analitycznego w zakresie oceny, a następnie wydania zaleceń ograniczających ryzyko.

Analizą ryzyka na bieżąco zajmują się CSIRTy rządowy i krajowy, które przekazują wstępne obserwacje do Koordynatora i Centrum Analitycznego odpowiadającego za analizy długoterminowe. Nad procesem czuwa Zespół Zadaniowy, który wydaje kóncowe zalecenia.

Podmioty świadczące usługę na 5: Zespół Zadaniowy przy Koordynatorze + Centrum Analityczne.

3.5 Security Advisement

Doradztwo w zakresie przeprowadzania czy wdrażania funkcji bezpieczeństwa.

Usługami tego typu zajmują się przede wszystkim CSIRTy sektorowe (w tym rządowy) i CSIRT krajowy (na poziomie ogólnym) oraz centra ISAC, a także we własnym zakresie podmioty komercyjne.

Podmioty świadczące usługi na 5: CSIRTy sektorowe, centra ISAC.

Usługa 4: Situational Awareness

Usługi składające się na pozyskanie bieżącego obrazu sytuacyjnego poziomu bezpieczeństwa w cyberprzestrzeni.

4.1 Sensor/Metrics operations

Usługi, które skupiają się na rozwoju, wdrażaniu i eksploatacji systemów i metod analizy w celu zidentyfikowania działań wymagających dokładnego przeprowadzenia dochodzenia.

Usługa świadczona przez system wczesnego ostrzegania. System ten jest prowadzony wspólnie przez CSIRT rządowy i krajowy, a dostęp do niego uzyskuje również Centrum Analityczne. W poszczególnych sektorach działania takie mogą również być prowadzone przez inne CERTy, centra SOC i ISAC.

Podmioty świadczące usługi na 5: CSIRT rządowy i krajowy.

4.2 Fusion/Correlation

Łączenie i korelacja informacji z wielu źródeł w celu uzyskania obrazu sytuacyjnego.

Korelacja informacji z systemu wczesnego otrzegania, platformy wymiany informacji i poszczególnych CERTów. Odbywa sie w największym zakresie w CSIRTcie krajowym/rządowym i Centrum Analitycznym.

Podmiot świadczący usługę na 5: CSIRT Krajowy/rządowy i Centrum Analityczne przy wsparciu systemów i innych CSIRTów.

4.3 Development and Curation of Security Intelligence

Rozwój i utrzymanie *security intelligence*, w tym katalogowanie i rozpoznawania nowych źródeł informacji, ich ocena, tworzenie i dystrybucja indykatorów (IoC) dotyczących zagrożeń, w tym reguły anty-malware, informacje TTP stosowanych przez adwersarzy.

Wiodącą rolę w tym obszarze odgrywa CSIRT krajowy/rządowy i Centrum Analityczne, ale działania te odbywają się przy wsparciu innych CSIRTów sektorowych i ISACów.

Podmiot świadczący usługę na 5: CSIRT Krajowy/rządowy i Centrum Analityczne przy wsparciu systemów i innych CSIRTów.

4.4 Data and Knowledge Management

Usługi wspierające przechwytywanie, opracowanie, udostępnianie i efektywne wykorzystanie wiedzy poprzez wzbogacenie o znaczniki danych (np. STIX, TAXII, IODEF, TLP), bazy danych wskaźników oraz złośliwego oprogramowania / katalogi podatności.

Wiodącą rolę w tym obszarze wiedzie Centrum Analityczne przy wsparciu CSIRTu krajowego i rządowego.

Podmiot świadczący usługę na 5: Centrum Analityczne przy wsparciu CSIRTu krajowego i rządowego.

4.5 Organizational Metrics

Usługi, które koncentrują się na identyfikacji metryk, ich parametrów oraz analizy tychże by ocenić, czy dane cele organizacyjne zostały osiągnięte.

Wiodącą rolę w tym obszarze odgrywa Koordynator powołując Zespoł Zadaniowy, który ma na celu opracowanie podstawowych metryk, które mogą być stosowane zarówno w skali Państwa czy administracji Państwowej jak i w poszczególnych podmiotach. Duża rolę pełni tu również Centrum Analityczne, przy wsparciu CSIRTu krajowego i rządowego. Pełnomocnicy ochrony zbierają dane i przekazują do Koordynatora za pomocą CSIRTu rządowego.

Podmiot świadczący usługa na 5: Zespoł Zadaniowy przy Koordynatorze.

Usługa 5: Outreach/Communications

Szeroko pojęte usługi związane z komunikacją zewnętrzną oraz nawiązywaniem i utrzymywaniem kontaktów.

5.1 Cybersecurity Policy Advisory

Kształtowanie rozwoju polityki cyberbezpieczeństwa Państwa oraz jej okresowa aktualizacja. Współpraca z decydentami.

Wiodąca rolę w tym zakresie odgrywa Koordynator. Ważnymi podmiotami w tym zespole są CSIRTy krajowe i rządowe, które okresowo raportują, czy istnieje konieczność zmian w stosowanym podejściu do bezpieczeństwa. Sektorowe CSIRTy i centra SAC również powinny zajmować się rozwojem polityk w swoich zakresie, jak i uczestniczyć w niektórych pracach Zespołów Zadaniowych.

Podmiot realizujący usługę na 5: Koordynator.

5.2 Relationship Management

Usługi związane z nawiązywaniem i utrzymywaniem zewnętrznych relacji i kontaktów, zarówno krajowych jak i międzynarodowych.

Za kontakty międzynarodowe odpowiadają przede wszystkim Koordynator, CSIRT Krajowy i CSIRT rządowy. Podmioty te również powinny nawiązywać bliskie relacje z innymi CSIRTami, ISACami itp. Oczywiście pożądane jest, aby takie relacje nawiązywały również inne podmioty. Dla najpoważniejszych incydentów (sytuacji kryzysowych) punktem kontatkowym jest Koordynator.

Podmiot realizujący usługę na 5: Koordynator, CSIRT krajowy, CSIRT rządowy (pozostałe podmioty również we własnym zakresie).

5.3 Security Awareness Raising

Usługi, które mają na celu zwiększanie świadomości o zagrożeniach i sposobom im przeciwdziałania.

Każdy CERT czy ISAC powinien świadczyć usługi w tym zakresie. Oczywiście w skali krajowej byłyby to przede wszystkim inicjatywy Koordynatora przez wsparciu CSIRTu krajowego czy rządowego: w szczególności dotyczy to profesjonalnych kampanii przygotowanych we współpracy z mediami. Zdecydowanie widzimy tu duży udział organizacji typu NGO, instytutów badawczych i podmiotów komercyjnych. Uwaga: zalecenia techniczne znajdują się głównie w punkcie 5.5.

Podmioty realizujący usługę na 5: Koordynator, CSIRT krajowy.

5.4 Branding/Marketing

Usługi odpowiedniego pozycjonowania zespołów CSIRT względem swojego constituency. Zadbanie o to, by znane wszystkim były usługi, jakie dany CSIRT świadczy oraz jak się z nim skontaktować/skomunikować.

Każdy CSIRT czy ISAC powinien prowadzić tego typu działalność, w szczególności niezbędne jest to w kontekście CSIRTu krajowego czy rządowego. Nadzór nad prawidłowością tych procesów spoczywa na Koordynatorze.

Podmiot realizujący usługę na 5: Koordynator - przy udziale CSIRTu krajowego i rządowego.

5.5 Information Sharing and Publications

Szeroko pojęte usługi dzielenia się informacją i publikacjami.

Do dzielenia się informacją na wielu płaszczyznach wykorzystywana jest platforma wymiany informacji. W zakresie wydawania zaleceń technicznych, odpowiedzialność spoczywa przede wszystkim na CSIRTcie krajowym i w bardziej ograniczonym zakresie CSIRTcie rządowym. Jednakże wszystkie CERTy i ISAC powinny publikować informacje o zagrożeniach, dobrych praktykach, jak i informować o swojej działalności, nadchodzących wydarzeniach itp.

Podmiot realizujący usługę na 5: CSIRT krajowy, CSIRT rządowy (w mniejszym stopniu również Koordynator).

Usługa 6: Capability Building

Usługi skupiające się na rozwoju potencjału jednostek bezpieczeństwa.

6.1 Training and Education

Usługi szkoleń i edukacji, m.in. poprzez warsztaty i konferencję.

Wiodącą rolę w tym zakresie ponosi CSIRT krajowy, który powinien być wspierany przez inne instytucje, w tym Koordynatora i CSIRT rządowy, a także Centrum Analityczne. Może być również wspierany przez jednostki komercyjne.

Podmiot realizujący usługę na 5: CSIRT krajowy, CSIRT rządowy, Koordynator, Centrum Analityczne.

6.2 Organizing Exercises

Organizowanie ćwiczeń w zakresie ochrony cyberprzestrzeni, w celu przetestowania istniejących procedur reakcji oraz oceny poziomu gotowości operacyjnej.

Wiodącą rolę w tym zakresie ponosi Koordynator i CSIRT Krajowy, przy szczególnym uwzględnieniu CSIRTu rządowego i wojskowego. Koordynator powinien powołać Zespół Zadaniowy, który odpowiada za nadzór procesu powstawania i wykonywania ćwiczeń. Możliwe jest również organizowanie ćwiczeń sektorowych.

Podmiot realizujący usługę na 5: Koordynator, CSIRT krajowy i odpowiedni Zespół Zadaniowy.

6.3 Systems and Tools for Constituency Support

Usługi, które polegają na zbieraniu wymagań, ocenie, specyfikacji, rozwoju lub pozyskiwaniu narzędzi będących częścią warsztatu pracy zespołów CERT - uwaga: narzędzia te bezpośrednio dotyczą bezpieczeństwa IT, nie są to ogólne rozwiązania IT.

Na poziomie krajowym rozwojem narzędzi zajmuje się CSIRT krajowy we współpracy z Centrum Analitycznym, zgodnie z sugestiami i zapotrzebowaniem innych CSIRTów, w tym przede wszystkim CSIRTu rządowego. W procesie uczestniczyć też powinien Koordynator, który równiez poprzez powołanie Zespołów Zadaniowych może przekazywać sugestie i specyfikacje narzędzi do wykonania innym podmiotom, jak np. NCBiR.

Podmiot realizujący usługę na 5: CSIRT krajowy, Koordynator, Centrum Analityczne, CSIRT rządowy, NCBiR.

6.4 Stakeholder Services Support

Bezpośrednie usługi wsparcia udzielane *constituency* w celu rozbudowy ich potencjału obsługi zdarzeń bezpieczeństwa.

Usługi powinny być świadczone przez wiodący CSIRT w swoim sektorze - np. w obszarze administracji publicznej byłby to CSIRT rządowy. Również CSIRT Krajowy i Centrum

Analityczne powinny brać udział w tym procesie. Inwentaryzację najpilniejszych potrzeb powinien przeprowadzać Koordynator.

Podmiot realizujący usługę na 5: Koordynator, CSIRT krajowy, CSIRT rządowy, CSIRTy sektorowe, poszczególne ISACi

Usługa 7: Research/Development

Usługi R&D wspierające ochronę cyberprzestrzeni Państwa, w tym pracę CSIRTów.

7.1 Development of Vulnerability Discovery/Analysis/Remediation/Root Cause Analysis Methodologies

Rozwój metodyk wspierających wykrywanie podatności, ich analizy, sposoby przeciwdziałania i wykrycia przyczyn powstania podatności.

Zapotrzebowanie na tego rodzaju badania powinny wychodzić od zespołów CSIRT do Koordynatora, który może zdecydować o przyznanie środków, czy to Centrum Analitycznemu czy też podmiotom komercyjnym, a w przypadku większych projektów zgłosić temat do NCBiR.

Podmiot realizujący usługę na 5: Koordynator, Centrum Analityczne, przy wsparciu zespołów CSIRT.

7.2 Development of processes for Gathering/Fusing/Correlating Security Intelligence

Tworzenie procesów do zbierania, łączenia i korelacji danych bezpieczeństwa (*security intelligence*).

Zapotrzebowanie na rozwój metodyk/narzędzi powinny wychodzić od zespołów CSIRT do Koordynatora, który może zdecydować o przyznanie środków, czy to Centrum Analitycznemu czy też podmiotom komercyjnym, a w przypadku większych projektów zgłosić temat do NCBiR.

Podmiot realizujący usługę na 5: Koordynator, Centrum Analityczne, przy wsparciu zespołów CSIRT.

7.3 Development of Tools

Usługi, które identyfikują zapotrzebowanie na nowe narzędzia i opracowują te narzędzia, m. in. do automatyzacji realizacji procesów związanych z CSIRT.

Zapotrzebowanie na rozwój metodyk/narzędzi powinny wychodzić od zespołów CSIRT do Koordynatora, który może zdecydować o przyznaniu środków, czy to Centrum Analitycznemu czy też podmiotom komercyjnym, a w przypadku większych projektów zgłosić temat do NCBiR.

Podmiot realizujący usługę na 5: Koordynator, Centrum Analityczne, przy wsparciu zespołów CSIRT.

6.5 Rekomendacja ogólna w podejściu do budowania systemu

Jedną z wad obecnego podejścia do ochrony cyberprzestrzeni RP jest brak precyzyjniejszych określeń, przed jakimi zagrożeniami chcemy się chronić. Świadomość tych zagrożeń i charakterystyk podmiotów stojących za nimi jest podstawowym elementem przystąpienia do budowy ochrony cyberprzestrzeni Państwa. Zarys podstawowych zagrożeń wraz z definicjami został wymieniony w raporcie NIK[76]: cyberchuligaństwo, cyberaktywizm, cyberprzestępczość, cyberterroryzm, cyberszpiegostwo i cyberwojna. Każda z tych działalności ma inne cele, motywacje i charakter. Cechuje się też innym potencjałem podmiotu, które działania te prowadzi. Obrona przed wymienionymi działaniami wymaga w każdym przypadku nieco innej reakcji państwa, w tym także zaangażowania różnych instytucji i określenia ich ról oraz odpowiedzialności. Oczywiście, nie zawsze jest łatwo na początku określić, z jakimi działaniami mamy do czynienia, szczególnie, jeśli obserwujemy je w płaszczyźnie technicznej.

W związku z powyższym, rekomendujemy, aby przy tworzeniu nowego systemu ochrony cyberprzestrzeni (niezależnie od wybranego wariantu) stworzony został katalog zagrożeń wraz ze scenariuszami reakcji na te zagrożenia przez podmioty państwowe, uwzględniający również podmioty prywatne.

W skład tych scenariuszy powinny wchodzić jasno określone odpowiedzialności i role poszczególnych podmiotów. Katalog ten powinien być stale aktualizowany przez Zespół Zadaniowy powołany przez Koordynatora. Powinna zostać jasno określona ścieżka eskalacji dla każdego scenariusza, (w przypadku stwierdzenia rosnącego zagrożenia lub nieadekwatnej reakcji odpowiednich jednostek). Scenariusze powinny też uwzględniać zasady komunikacji i współpracy z mediami. Scenariusze powinny być regularne testowane lub też być elementem szerszych ćwiczeń.

6.6 Wariant zdecentralizowany

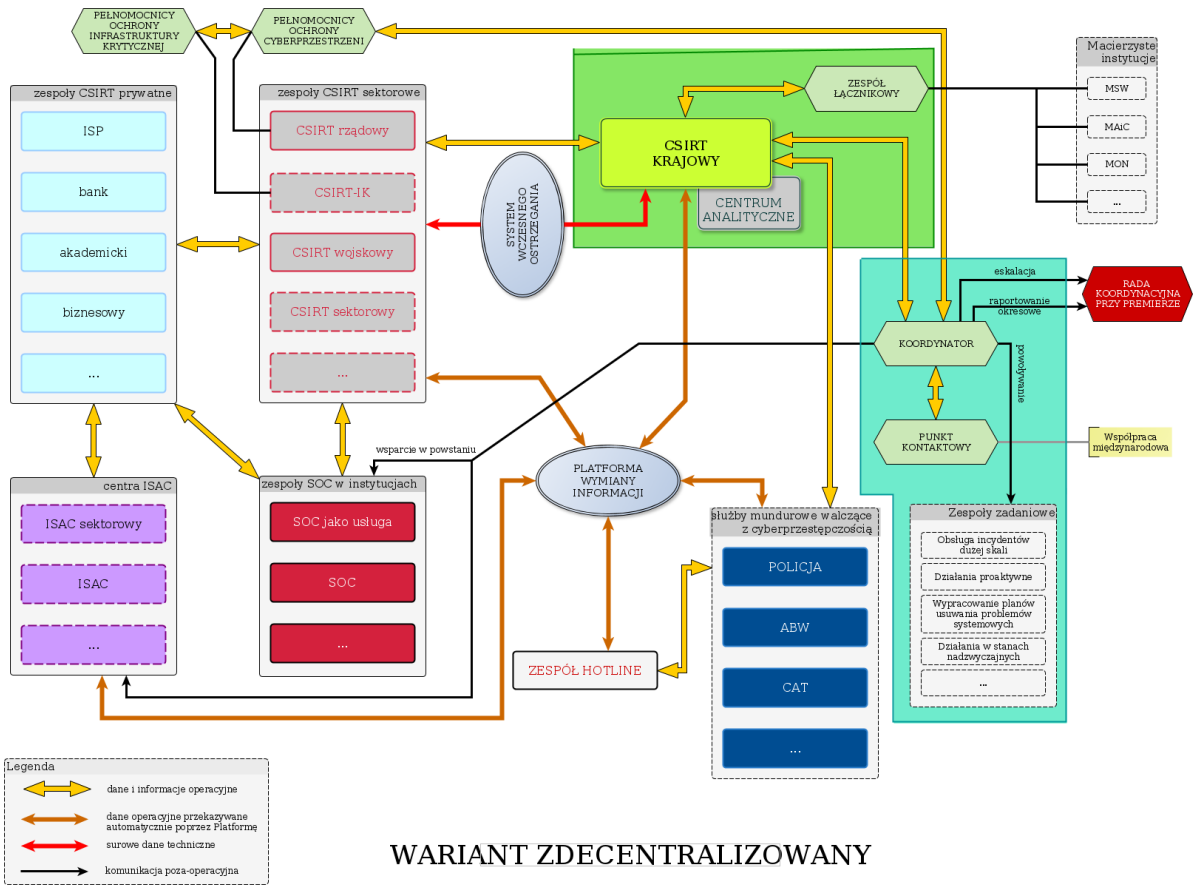
Jak zaznaczono na wstępie, wariant ten zakłada maksymalne wykorzystanie istniejących rozwiązań i instytucji pełniących obecnie określone role na rzecz bezpieczeństwa cyberprzestrzeni RP. Role te, pełnione obecnie często mniej lub bardziej formalnie, powinny

[76] https://www.nik.gov.pl/plik/id,8764,v,artykul_11824.pdf

być zainkorporowane do systemu wraz z takim osadzeniem w systemie prawnym, aby w procesie budowy systemu ochrony cyberprzestrzeni mogły być odpowiednio zdefiniowane i przypisane konkretnym podmiotom. Oczywiście pewne kluczowe role, takie jak koordynacja całości zagadnień ochrony cyberprzestrzeni, które nie są obecnie pełnione (są pełnione wycinkowo) muszą zostać od nowa zdefiniowane i przypisane do konkretnych podmiotów w sposób nie budzący wątpliwości co do umocowania i zakresu odpowiedzialności czy pełnionej roli.

Role i główne zadania poszczególnych podmiotów oraz elementów krajowego systemu bezpieczeństwa cyberprzestrzeni opisano w rozdziale 6.2.1. W tej części dokumentu uzupełniamy powyższe opisy odnośnie do wariantu zdecentralizowanego.

Poglądowy schemat ilustrujący wariant zdecentralizowany przedstawia poniższy rysunek.



Rysunek 8. Mapa relacji w wariancie zdecentralizowanym.

Wariant zakłada rozłączność podmiotów przypisanych do roli Koordynatora (MAC lub MSW), CSIRTu rządowego (ABW) i CSIRTu krajowego (CERT Polska/NASK). Ponieważ w wariancie tym zakładamy przypisaną rolę Centrum Analitycznego do NASK, rola ta występuje w połączeniu z CSIRTem krajowym.

Odpowiedzialność za działanie systemu i koordynację w przypadku sytuacji kryzysowych/incydentów większej skali ponosi (jak zresztą w wszystkich wariantach) instytucja z przypisaną rolą Koordynatora. Ważną rolą Koordynatora jest powoływanie Zespołów Zadaniowych, które przy nim funkcjonują wcelu rozwiązywania zdefiniowanych problemów. Koordynator jest również w stałym bezpośrednim kontakcie z CSIRTem krajowym (który do niego raportuje) jak i CSIRTem rządowym.

Przy CSIRTcie Krajowym działa Zespół Łącznikowy, składający się z przedstawicieli m.in. administracji państwowej oraz służb mundurowych.

CSIRT IK (zespół dedykowany obszarowi infrastruktury krytycznej) może w tym wariancie istnieć jako rola przypisana innemu podmiotowi – (RCB). Istnienie CSIRT IK jako roli odrębnej od CSIRTu rządowego uważamy za opcjonalne.

Poza rolami CSIRTowymi, w schemacie występują służby mundurowe - ich rolę należy rozumieć jako rolę ustawową, wykraczającą poza obszar zagadnień CSIRTowych. Niezależnie od tego oczywiście w niektórych przypadkach możliwe jest powierzenie ról CSIRTowych również tym instytucjom (np. w szczególności w tym wypadku ABW jako CSIRTu rządowego).

Schemat zawiera dwa rozwiązania warstwy technicznej bezpośrednio powiązane z administracją państwową: system wczesnego ostrzegania (podstawowy system informujący o wykrytych zagrożeniach w administracji państwowej) oraz platformę wymianę wiedzy służącą jako podstawowy mechanizm komunikacji o zagrożeniach pomiędzy interesariuszami.

Inne podmioty warstwy technicznej to zespoły SOC, które mogą być tworzone na poziomie instytucji - mogą funkcjonować jako element CSIRTów sektorowych lub też niezależnie.

Schemat nie wyczerpuje wszystkich relacji pomiędzy podmiotami, np. możliwości dostępu przez CSIRTy czy prywatne zespoły SOC do niektórych elementów platformy wymiany wiedzy.

Szczegółowe omówienie najważniejszych podmiotów systemu znajduję się poniżej.

6.6.1 Koordynator (MAC lub MSW)

Bez krajowego Koordynatora systemu ochrony cyberprzestrzeni nie może być mowy o dokonaniu pewnego przełomu w tej dziedzinie i przeprowadzenia skutecznego procesu budowy, utrzymania oraz rozwoju systemu w celu osiągania coraz wyższej zdolności ochrony i obrony przed zagrożeniami incydentami naruszającymi bezpieczeństwo. W niniejszym modelu przewidziano, iż koordynatorem jest (jako pewne minimum odnośnie stanowiska w administracji rządowej) wiceminister dedykowany do spraw cyberbezpieczeństwa, który jest pełnomocnikiem rządu i ma do dyspozycji odpowiedni budżet oraz personel w postaci

dedykowanych departamentów w określonym ministerstwie. W obecnych realiach podziału na działy administracji rządowej, ministerstwem właściwym do zlokalizowania takiej kompetencji byłyby przykładowo MAC lub MSW.

Role instytucji koordynującej, szczególnie w związku z planowaną dyrektywą NIS, zostały opisane w rozdziale „Mapa relacji systemu bezpieczeństwa cyberprzestrzeni – poziom operacyjny". Jednak podkreślić należy, że rola koordynatora jest niezwykle istotna zarówno w warstwie operacyjnej, jak i strategicznej czy politycznej.

Wśród zadań i ról, które powinny być przypisane instytucji pełniącej rolę Koordynatora w warstwie strategicznej i operacyjnej można wymienić:

- proponowanie i przygotowywanie projektów odpowiednich ram prawnych systemu bezpieczeństwa cyberprzestrzeni,
- nadzorowanie procesu wdrażania prawa i wynikających z niego polityk czy programów – w omawianym obszarze,
- współpracę z CSIRTem krajowym na bazie zasad szczegółowo opisanych w prawie,
- powoływanie Zespołu Łącznikowego oraz Zespołów Zadaniowych (które mogą dysponować budżetem od Koordynatora) dla rozwiązywania problemów bieżących (incydentów, sytuacji kryzysowych) oraz wypracowywania rozwiązań dla problemów strukturalnych, systemowych, prawnych.
- eskalacja na poziom Rady Koordynacyjnej przy Radzie Ministrów problemów dużej skali związanych z bezpieczeństwem cyberprzestrzeni bądź problemów ze współpracą w ramach administracji publicznej,
- wspieranie rozwoju współpracy w dziedzinie bezpieczeństwa cyberprzestrzeni,
- wspieranie powstawania CSIRTów sektorowych oraz centrów sektorowych ISAC,
- reagowanie na problemy we współpracy pomiędzy CSIRTem krajowym, CSIRTami sektorowymi a także centrami ISAC
- pełnienie roli Punktu Kontaktowego dla współpracy międzynarodowej (szczególnie w ramach Unii Europejskiej),
- współpraca z organami ścigania oraz organem właściwym w zakresie ochrony danych osobowych,
- raportowanie cykliczne na poziom Rady Koordynacyjnej przy Prezesie RM o stanie bezpieczeństwa cyberprzestrzeni i wysuwanie inicjatyw w zakresie poprawy tego stanu.

Koordynator jest podmiotem, który rozdysponowuje zadania w sytuacji kryzysowej.

6.6.2 CSIRT krajowy (CERT Polska/NASK)

Rola krajowego zespołu CSIRT została opisana w rozdziale 6.3. W tym wariancie w ramach CSIRTu krajowego działa Centrum Analityczne[77] zajmujące się dogłębną analizą zjawisk oraz artefaktów – na potrzeby działań wykonywanych operacyjnie przez CSIRT krajowy i powiązane CSIRTy siecią współpracy z wykorzystaniem Platformy wymiany informacji. CSIRT krajowy pozostaje w ścisłej współpracy z Koordynatorem, informuje o poważnych incydentach bezpieczeństwa, przekazuje Koordynatorowi cykliczne raporty, a także uczestniczy w międzynarodowych sieciach współpracy CSIRTów (krajowych, narodowych i wszelkich innych inicjatywach , takich jak FIRST, TF CSIRT). CSIRT krajowy nie zajmuje się obsługą wszystkich incydentów, pełni zaś rolę instancji „last resort" – jeśli np. nie można przypisać obsługi danego zdarzenia odpowiedniemu CSIRTowi sektorowemu.

Ze względu na unikalne kompetencje, pełnienie roli *de facto* CSIRTu krajowego od roku 1997, umiejscowienie w instytucie państwowym, nadzorowanym przez administrację rządową, który jednocześnie pełni funkcję krajowego rejestru domeny .pl oraz gov.pl – proponuje się, aby rolę CSIRTu krajowego oficjalnie przypisać do zespołu CERT Polska działającego w NASK. CERT Polska wypełnia także role przypisane Centrum Analitycznemu. Stworzył krajową platformę n6, będącą największym dynamicznym repozytorium wiedzy na temat zagrożeń i incydentów dotyczących polskiej przestrzeni adresowej Internetu (informacje pochodzą z całego świata) i jednocześnie platformą oferującą nieodpłatnie informacje na ten temat wszystkim zainteresowanym podmiotom (w odniesieniu do sieci tych podmiotów). Jest autorem rozwiązania ARAKIS, będącego systemem wykrywania i ostrzegania o zagrożeniach (kolejny kluczowy element krajowego systemu bezpieczeństwa cyberprzestrzeni), który we współpracy z ABW doprowadził do powstania systemu ARAKIS.GOV, chroniącego administrację publiczną. CERT Polska jest rozpoznawalny na całym świecie i należy do kluczowych inicjatyw związanych z cyberbezpieczeństwem w Polsce.

Powierzenie zespołowi CERT Polska roli krajowego CSIRTu mogłoby się odbyć w oparciu o przepis art. 37 ustawy o instytutach badawczych.

6.6.3 Krajowe Centrum Analityczne (CERT Polska/NASK)

Krajowe Centrum Analityczne, pełniące istotną funkcję w zakresie pozyskiwania informacji i bieżącego analizowania sytuacji w obrębie zagrożeń cyberprzestrzeni w kraju, a także prowadzące zaawansowane analizy dotyczące scenariuszy ataków, szkodliwego oprogramowania i sposobu działania cyberprzestępców jest w niniejszym modelu zlokalizowane w zespole CSIRTu krajowego – w tym wypadku w CERT Polska działającym w instytucie badawczym NASK.

[77] Por. rozdział 6.3.4

6.6.4 CSIRT rządowy (ABW)

Bezpieczeństwo sieci staje się w coraz większym stopniu obszarem zainteresowania Państw i zorganizowanej przestępczości (która bywa również wynajmowana przez państwa, jak wskazuje przypadek autora trojana bankowego ZeuS P2P[78]). Na cyberbezpieczeństwo Państwa nie można więc patrzeć tylko poprzez pryzmat zagrożeń technicznych, ale poprzez szerszą analizę ryzyka i działania operacyjne, w tym poprzez obserwacje i identyfikowanie aktorów stojących za atakami oraz technikami ich działania (szeroko pojęte "TTPs" - *Tactics, Techniques and Procedures*). Zrozumienie motywacji i celów ich działania jest kluczowe, jeżeli państwo ma mieć możliwości obrony. Oznacza to prowadzenie działań równoległych zupełnie poza obszarem cyberprzestrzeni, a nawet prowadzenia działań ofensywnych w jej obszarze.

Powyższa argumentacja, połączona z myślą przewodnią tego wariantu, czyli maksymalnym wykorzystaniem istniejących zasobów, sugeruje umiejscowienie CSIRTu rządowego w Agencji Bezpieczeństwa Wewnętrznego, czyli tak jak ma to miejsce obecnie (konieczne oczywiście jest uzupełnienie to aktem prawnym omawianym opisie wymiaru prawnego niniejszego wariantu). Założenie to jest poparte raportem NIK, który wskazuje wysoką kompetencję obecnej jednostki CERT.GOV.PL.

Odpowiedzialność CSIRTu rządowego powinna zostać rozszerzona o administrację samorządową.

Zespół ten również mógłby być odpowiedzialny za całość lub część infrastruktury krytycznej - patrz punkt 3.1.5.

Zwiększenie roli i zakresu odpowiedzialności CSIRTu rządowego musi iść w parze ze znacznie rozszerzonym budżetem tej jednostki.

CSIRT rządowy powinien odpowiadać za zarządzaniem systemem wczesnego ostrzegania ARAKIS.GOV 2 we współpracy z CSIRTem krajowym.

6.6.5 Opcjonalnie CSIRT-IK

W wariancie tym zakładamy możliwość powstania CSIRTu odpowiedzialnego za infrastrukturę krytyczną, który potencjalnie mógłby powstać w Rządowym Centrum Bezpieczeństwa. Co oczywiste, byłby to CSIRT trans-sektorowy, obejmujący przedstawicieli wielu sektorów uznanych za infrastrukturę krytyczną. Potencjalnym wyzwaniem byłby tutaj podział kompetencji z ABW, która również jest odpowiedzialna za ochronę infrastruktury krytycznej. Innym problemem jest fakt braku doświadczenia RCB w zakresie technicznej i operacyjnej obsługi incydentów bezpieczeństwa teleinformatycznego (dotychczasowy brak zespołu CSIRT) – kompetencje takie należałoby stworzyć od zera. Możliwy jest również

[78] https://www.fox-it.com/en/files/2015/08/FoxIT-Whitepaper_Blackhat-web.pdf

prostszy i tańszy model, np. ustanowienie w RCB punktu kontaktowego, który miałby za zadanie wstępną ocenę incydentu i przekazanie go następnie do CSIRTu rządowego lub krajowego.

6.6.6 Pozostałe podmioty

Zadania i role pozostałych interesariuszy nie różnią się w tym modelu zasadniczo od tego co zostało przedstawione w rozdziale 6.3.

6.6.7 Opis zalet i wad modelu

Głównym atutem rozwiązania rozproszonego jest jego praktyczna efektywność i jakość działania. Dzieje się tak, gdyż w tym wariancie, przy poprawnej implementacji, maksymalizujemy kompetencje i zasoby wielu ośrodków w celu osiągnięcia odpowiedniego poziomu reakcji na zagrożenia i nie skupiamy wszystkich działań operacyjnych w jednym podmiocie. Rozwiązanie to jest najbardziej elastyczne, co umożliwia szybkie dostosowanie się do ewolucji zagrożeń. CSIRT Krajowy, w tym wypadku znajdujący się w NASK zespół CERT Polska, funkcjonuje jako "CERT of the last resort" i nie musi być zaangażowany w reakcje na każde zagrożenie. Co istotne jednak, inne jednostki raportują CSIRTowi krajowemu o poważniejszych incydentach, a ten z kolei raportuje Koordynatorowi. Zalety tego modelu – rozproszona struktura oraz CSIRT krajowy w instytucie badawczym – zwiększa odporność systemu cyberbezpieczeństwa RP na doraźne decyzje polityczne.

Mocną stroną tego wariantu jest - potwierdzona przez kontrolę NIK[79][80] - wysoka jakość merytoryczna istniejących kluczowych zespołów CSIRT: CERT Polska i jego kadr, a także zespołów CSIRT w ABW i MON. Warto również podkreślić dobrą współpracę tych zespołów na co dzień i świetne wyniki wspólnych drużyn (wraz z innymi podmiotami państwowymi z Polski) w jednym z najbardziej wymagających ćwiczeń cyberobrony - ćwiczeń NATO Locked Shields. W ćwiczeniach tych reprezentacja Polski (złożona m.in. z reprezentantów z wyżej wymienionych zespołów CSIRT) w latach 2014 i 2015 zajęła 1 i 3 miejsce, skutecznie rywalizując z innymi państwami członkowskimi Sojuszu oraz zespołem NATO NCIRC. Dużym atutem jest też międzynarodowa rozpoznawalność zespołu CERT Polska, wypracowywana przez wiele lat, gwarantująca ciągłość współpracy międzynarodowej. Wysoka jakość kadr i reputacja zespołu pozwala na łatwiejsze przyciągnięcie kolejnych pracowników o wysokich atutach i wiedzy eksperckiej, a także na efektywne wyszkolenie kolejnych pracowników. Skutkuje to też dobrą reputacją całego systemu cyberbezpieczeństwa Polski na starcie i większego zaufania podmiotów zagranicznych.

[79] https://www.nik.gov.pl/kontrole/P/14/043/

[80] A także przez innych, w tym w oficjalnych raportach dla Brytyjskiej Izby Lordów: http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68we10.htm

Kolejnym ważnym atutem wariantu jest jego czas wdrożenia. Jest on stosunkowo krótki w porównaniu do alternatywnych wariantów, gdyż bazuje w wielu przypadkach na istniejących zasobach, czyli CERT.GOV.PL w ABW, CERT Polska i CERT w MON. Dodatkowo, uproszczona, w stosunku do innych modeli, jest ścieżka legislacyjna (mniejsza ilość koniecznych zmian) niezbędna do wprowadzenia w życie tego wariantu.

Warto też zwrócić uwagę na właściwy dla obszaru cyberbezpieczeństwa kontekst badawczo-rozwojowy. CERT Polska, jako część instytutu badawczego ma możliwość skuteczniejszego prowadzenia i wdrażania wyników prac badawczo-rozwojowych[81]. Od wielu lat w tym zakresie rozwija się współpraca ABW z NASK, która zaowocowała m.in. systemem ARAKIS-GOV. Oznacza to, że system na starcie daje dużą sprawność w reakcji na nowo pojawiające się zagrożenia sieciowe. Narzędzia niezbędne do ich zwalczania mogą być rozwijane bardzo szybko, bez konieczności czekania na rozwiązania zewnętrzne, w tym komercyjne, które ukazują się z większym opóźnieniem w stosunku do pojawiających się zagrożeń. Można w tym wypadku liczyć na większe szanse skutecznego ubiegania się o środki zewnętrzne na badania (Unii Europejskiej, NATO i innych).

Wariant ten oczywiście nie jest bez wad. Prawdopodobne formalne zadaniowanie i raportowanie wśród podmiotów w tym modelu będzie słabsze niż w przypadku wariantów bardziej scentralizowanych. Rozproszenie modelu może skutkować brakiem jednoznacznie określonej odpowiedzialności, należy więc zadbać, aby odpowiedzialności te zostały jasno określone. Oczywistym wyzwaniem będzie również logistyka koordynacji współpracy - model rozproszony z definicji wymaga w tym aspekcie większych starań.

Dodatkowe ryzyka w wariancie rozproszonym wynikają z niejednolitości źródeł finansowania. Elementy modelu należące do administracji finansuje budżet państwa, pozostałe elementy mają inne źródła finansowania. Stąd nawet niezmienna dostępność środków budżetowych nie musi gwarantować trwałości modelu. Przykładowo, hipotetyczne istotne problemy finansowe instytutu badawczego NASK, nie będącego elementem finansów publicznych, choć zarazem stanowiącego własność Skarbu Państwa, mogłyby zakłócić prawidłowe funkcjonowanie przyjętego modelu. Dodatkowe wyzwania w modelu rozproszonym wnosi również słabsze przełożenie podmiotów zewnętrznych względem administracji publicznej na zadaniowanie/ zalecanie/ egzekwowanie działań od podmiotów administracji publicznej – aspekt ten musiałby zostać starannie zdefiniowany w towarzyszącej modelowi legislacji.

Podsumowując, uważamy, że wariant ten ma bardzo wiele zalet przy stosunkowo niewielkiej liczbie wad.

[81] http://www.cert.pl/projekty

6.6.8 Wymiar prawny

Biorąc pod uwagę, że opisywany wariant wykorzystuje w większości funkcjonujące już instytucje i faktycznie realizowane przez te instytucje zadania, należy stwierdzić, że wprowadzenie go w życie nie będzie również wymagać dużego nakładu prac o charakterze legislacyjnym.

Jak w każdym wariancie proponowanym w niniejszym opracowaniu, **w pierwszej kolejności niezbędne jest powołanie Koordynatora**. Przypisany Koordynatorowi zakres zadań i odpowiedzialności wymaga, aby funkcję tę pełnił minister lub wiceminister, co najmniej w randze podsekretarza stanu.

Umiejscowienie nowej kategorii spraw w dziedzinie administracji rządowej, tj. cyberbezpieczeństwa musi poprzedzić analiza przepisów obowiązującej ustawy z dnia 04 września 1997 r. o działach administracji rządowej. Na obecnym etapie wydaje się, że równouprawnione będzie dodanie nowej sprawy albo do działu „Sprawy wewnętrzne", albo do działu „Informatyzacja".

Po podjęciu decyzji co do umiejscowienia nowej kategorii, Prezes Rady Ministrów powinien wydać odpowiednie rozporządzenie w sprawie szczegółowego zakresu działania właściwego Ministra.

Zadania z zakresu cyberbezpieczeństwa winny być realizowane we właściwym ministerstwie przez dedykowane osoby, w ramach nowoutworzonego departamentu.

W uzupełnieniu roli administracji rządowej **należy powołać Radę Koordynacyjną ds. Cyberbezpieczeństwa przy Radzie Ministrów**. Rada Koordynacyjna działałaby jako organ opiniodawczy i doradczy w sprawach dotyczących cyberbezpieczeństwa.

W tym celu, na podstawie art. 12 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów, Prezes Rady Ministrów, w drodze zarządzenia, powinien utworzyć Radę Koordynacyjną jako organ pomocniczy Prezesa Rady Ministrów.

Do zadań Rady należałoby formułowanie ocen i wyrażanie opinii w szczególności w sprawach projektów aktów normatywnych dotyczących cyberbezpieczeństwa, kierunków i planów działania organów zaangażowanych w ochronę cyberbezpieczeństwa czy koordynowania ich współdziałania. Rada mogłaby ponadto pełnić funkcję organu, do którego eskalowanoby poważne problemy w zakresie bezpieczeństwa w cyberprzestrzeni bądź problemy ze współpracą w ramach administracji publicznej.

Proponuje się, aby w skład Rady Koordynacyjnej weszli co najmniej:

1. przewodniczący – Prezes Rady Ministrów;
2. sekretarz Rady;
3. członkowie:
    a. minister właściwy do spraw wewnętrznych,

b. minister właściwy do spraw zagranicznych,
c. minister właściwy do spraw informatyzacji państwa,
d. Minister Obrony Narodowej,
e. minister właściwy do spraw finansów publicznych,
f. Szef Biura Bezpieczeństwa Narodowego.

W posiedzeniach Rady Koordynacyjnej, odbywających się nie rzadziej niż raz na kwartał lub *ad hoc* – w zależności od aktualnych potrzeb, mogą brać udział również, z głosem doradczym, eksperci zewnętrzni, których udział Rada uzna za niezbędny ze względu na tematykę spotkania.

Na tej samej podstawie prawnej mogą powstawać **zespoły zadaniowe**. Inicjatywa, a tym samym formalny wniosek do Prezesa Rady Ministrów w zakresie powołania zespołu zadaniowego, powinna obciążać Koordynatora.

Stały **Zespół Łącznikowy**, którego kompetencje opisano powyżej, powinien zostać powołany przy ministrze właściwym ds. cyberbezpieczeństwa. Biorąc pod uwagę planowany skład osobowy, zakres kompetencji oraz proponowane ulokowanie Zespołu przy Koordynatorze, podstawę w obowiązującym stanie prawnym można znaleźć w art. 34 ust. 3 ustawy z dnia 08 sierpnia 1996 roku o Radzie Ministrów. Zgodnie z przywołanym przepisem, Rada Ministrów może powołać przy ministrze komitet doradczy i określić zakres jego zadań.

Zgodnie z koncepcją opisywanego wariantu, rolę **krajowego CSIRTu oraz Krajowego Centrum Analitycznego obejmie, działający w ramach NASK, CERT Polska**. Powierzenie CERT Polska/NASK roli krajowego CSIRTu oraz Krajowego Centrum Analitycznego powinno się odbyć z wykorzystaniem procedury opisanej w art. 37 ustawy z dnia 30 kwietnia 2010 roku o instytutach badawczych. Na podstawie powołanego przepisu Minister Nauki i Szkolnictwa Wyższego, na wniosek ministra właściwego ds. cyberbezpieczeństwa, może nałożyć na NASK jako instytut badawczy zadanie, zgodnie z zakresem działania określonym w statucie instytutu, jeżeli jest to niezbędne ze względu na potrzeby obronności lub bezpieczeństwa publicznego, w przypadku stanu klęski żywiołowej lub w celu wykonania zobowiązań międzynarodowych. Zakres działania NASK określony w § 8 Statutu z dnia 25 marca 2011 roku obejmuje m.in. prowadzenie badań naukowych i prac rozwojowych w zakresie bezpieczeństwa sieci i systemów teleinformatycznych.

Realizacja zadania w postaci obowiązku utworzenia i pełnienia funkcji krajowego CSIRTu oraz Krajowego Centrum Analitycznego powinna odbywać się odpłatnie, na podstawie umowy pomiędzy NASK a właściwym ministrem. Umowa powinna określać zarówno szczegółowe obowiązki CERT Polska, w tym obowiązek prowadzenia platformy wymiany informacji, zasady składania raportów i przekazywania bieżących informacji do

Koordynatora, jak również zasady współpracy z CSIRTem rządowym, CSIRTami sektorowymi i Policją.

Zgodnie z koncepcją maksymalnego wykorzystania istniejących i funkcjonujących zasobów, w omawianym wariancie sugeruje się **pozostawienie funkcji CSIRTu rządowego w Agencji Bezpieczeństwa Wewnętrznego,** jak ma to miejsce dotychczas. Autorom niniejszego opracowania znane są pojawiające się w środowisku wątpliwości co do formalnego umocowania Agencji Bezpieczeństwa Wewnętrznego, a konkretnie – zespołu CERT.GOV.PL, funkcjonującego w ramach Departamentu Bezpieczeństwa Teleinformatycznego – do pełnienia funkcji CSIRTu rządowego. Powyższy problem dostrzegła również administracja publiczna. Już w dokumencie „*Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia*", przyjętym przez Komitet Stały Rady Ministrów w dniu 09 marca 2009 roku, wskazywano jako niezbędne do podjęcia przez administrację publiczną działania organizacyjno-prawne: „*stworzenie podstaw prawnych umożliwiających skuteczne realizowanie zadań na rzecz ochrony cyberprzestrzeni przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL",* a ponadto:

> *„Obecnie Szef ABW właściwy w sprawach ochrony bezpieczeństwa teleinformatycznego państwa dysponuje zasobami w postaci pionu informatycznego ABW, a konkretnie powołanego w lutym 2008 r. w strukturze Departamentu Bezpieczeństwa Teleinformatycznego (DBTI) ABW, Rządowego Zespołu Reagowania na Incydenty Komputerowe – CERT.GOV.PL.*
>
> *Osiągnięcie wskazanych powyżej celów możliwe będzie poprzez prawne określenie kompetencji, oraz procedur dla funkcjonującego w ABW zespołu CERT.GOV.PL do działania w obszarze całego państwa."*

Do dnia dzisiejszego założenia te nie zostały zrealizowane.

Wobec powyższego wydaje się niezbędne wprowadzenie odpowiednich zmian w art. 5 ustawy z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, poprzez wskazanie, że jednym z zadań Agencji Bezpieczeństwa Wewnętrznego jest pełnienie funkcji rządowego zespołu reagowania na incydenty komputerowe.

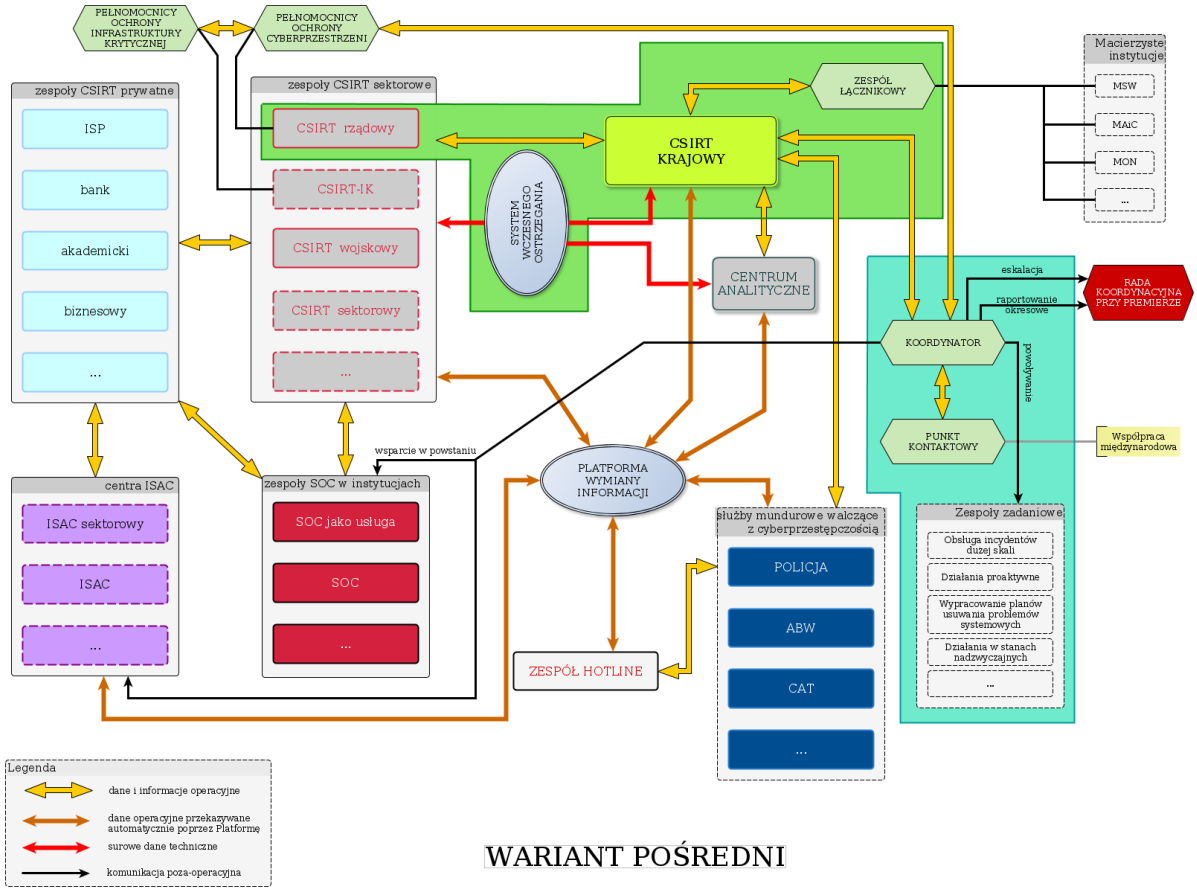
Należy uznać, że takie rozwiązanie znajduje oparcie w aktualnych uregulowaniach prawnych. Zgodnie z przyjętą Polityką Ochrony Cyberprzestrzeni RP, w zakresie realizacji zadań związanych z bezpieczeństwem cyberprzestrzeni RP, Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL pełni rolę głównego zespołu CSIRT w obszarze administracji rządowej. Podstawowym jego zadaniem jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami. Wskazanym byłoby również, rozszerzenie kompetencji

CERT.GOV.PL o administrację samorządową, a w przypadku, gdyby nie powołano odrębnego CSIRTu dla infrastruktury krytycznej, również o infrastrukturę krytyczną.

Powołanie CSIRTów sektorowych, np. dla energetyki czy sektora bankowego, powierzyć należy właściwym organom administracji rządowej, w ramach ich kompetencji. Dla przykładu, CSIRT dla sektora energetycznego mógłby działać przy Prezesie Urzędu Regulacji Energetyki (URE). Prezes URE zobowiązany jest m.in. do monitorowania funkcjonowania systemu gazowego i elektroenergetycznego w zakresie bezpieczeństwa dostarczania paliw gazowych i energii elektrycznej. Wydaje się zasadne, aby w opisanym pojęciu mieściło się również bezpieczeństwo teleinformatyczne przesyłu gazu i energii elektrycznej.

Rolą Koordynatora winno być ponadto dopilnowanie, aby zgodnie z obowiązującą Polityką Ochrony Cyberprzestrzeni RP, w ramach każdej jednostki organizacyjnej administracji rządowej **powołany został pełnomocnik ds. bezpieczeństwa cyberprzestrzeni**, z zadaniami określonymi tamże.

6.7 Wariant pośredni



Rysunek 9. Mapa relacji w wariancie pośrednim.

Wariant pośredni zakłada połączenie ról CSIRTu krajowego oraz CSIRTu rządowego. Rekomendujemy przy tym przypisanie obu ról zespołowi CERT.GOV.PL działającemu w Agencji Bezpieczeństwa Wewnętrznego. Zespół ten mógłby mieć także przypisaną część lub całość odpowiedzialności w zakresie infrastruktury krytycznej. Schemat wariantu przedstawiony jest na rysunku wyżej.

Rola Koordynatora warstwy operacyjnej - podobnie jak w wariancie zdecentralizowanym - jest przypisana innemu podmiotowi, MAC lub MSW. Centrum Analityczne znajdowałoby się poza CSIRTem rządowym/krajowym i mogłoby być przypisane do NASK (CERT Polska).

Pozostałe relacje są podobne jak w przypadku wariantu zdecentralizowanego.

Schemat nie wyczerpuje wszystkich relacji pomiędzy podmiotami, np. możliwości dostępu przez CSIRTy czy prywatne zespoły SOC do niektórych elementów platformy wymiany wiedzy.

Szczegółowe omówienie najważniejszych podmiotów systemu znajduje się poniżej.

6.7.1 Koordynator (MAC lub MSW)

Rola Koordynatora w wariancie pośrednim pozostaje niezmieniona w stosunku do rozważanego powyżej modelu rozproszonego. W szczególności Koordynator pełni także rolę Punktu Kontaktowego do współpracy międzynarodowej. Koordynator współpracuje także ściśle z CSIRTem krajowym odbierając od niego obraz sytuacyjny i rekomendacje dotyczące działań strategicznych. Koordynator jest podmiotem, który rozdysponowuje zadania w sytuacji kryzysowej.

6.7.2 CSIRT krajowy (ABW)

Rola CSIRTu krajowego w wariancie pośrednim jest rozszerzona względem modelu rozproszonego o odpowiedzialność za sferę administracji rządowej i samorządowej, a także część lub całość infrastruktury krytycznej. Przesłanką do umiejscowienia takiego zespołu w ABW są przede wszystkim zbudowane już kompetencje zespołu CERT.GOV.PL (potwierdzone w raporcie NIK). Przemawia za tym także posiadany przez ABW wymagany mandat do działań w instytucjach administracji rządowej, a także uprawnienia śledcze, które już w tej chwili wykorzystywane są przy poważnych naruszeniach bezpieczeństwa IT (w szczególności mogących mieć związek z cyberterroryzmem). W takiej postaci CSIRT Krajowy koncentrowałby wiedzę na temat bezpieczeństwa cyberprzestrzeni RP i mógłby podejmować działania operacyjne.

Należy podkreślić, że funkcjonowanie CSIRTu krajowego w opisanym tu zakresie w ramach ABW wymagałoby znacznego zwiększenia finansowania w porównaniu z obecnie działającym zespołem CERT.GOV.PL.

6.7.3 Krajowe Centrum Analityczne (CERT Polska/NASK)

Kompetencje CSIRTu krajowego uzupełniane powinny być przez Krajowe Centrum Analityczne, którego rolą ma być pozyskiwanie informacji i bieżące analizowanie sytuacji w obrębie zagrożeń cyberprzestrzeni. W wariancie pośrednim rekomendujemy przypisanie tej roli działającemu w NASK zespołowi CERT Polska. Przemawia za tym obecny status de facto CSIRTu krajowego, wieloletnie doświadczenie i wysokie kompetencje merytoryczne zespołu CERT Polska, potwierdzone także w kontroli NIK. NASK utrzymuje także i rozwija platformę wymiany informacji, publikuje raporty dotyczące analiz złośliwego oprogramowania oraz sposobów działania przestępców. Ponadto, NASK jest instytutem badawczym, działającym na podstawie ustawy o instytutach badawczych, nad którym nadzór sprawuje Minister Nauki i Szkolnictwa Wyższego, co oznacza, że pozostaje pod kontrolą administracji państwowej.

Powierzenie zespołowi CERT Polska roli Centrum Analitycznego mogłoby się odbyć w oparciu o przepisy art. 37 ustawy o instytutach badawczych.

Propozycja powierzenia roli Krajowego Centrum Analitycznego instytutowi badawczemu NASK nie wyklucza udziału także innych podmiotów, w miarę oceny ich kompetencji i posiadanych środków oraz wyników analizy ryzyka.

6.7.4 Opcjonalnie CSIRT-IK (RCB)

Podobnie jak w wariancie zdecentralizowanym, zakładamy możliwość utworzenia zespołu CSIRT odpowiedzialnego za infrastrukturę krytyczną. Ryzyka związane z powołaniem takiego zespołu opisane zostały w punkcie 6.6.5, przy czym podział kompetencji w wariancie pośrednim musiałby być dokonany względem CSIRTu krajowego. Możliwy jest również prostszy i tańszy model - np. ustanowienie w RCB punktu kontaktowego, który miałby za zadanie wstępną ocenę incydentu i przekazywanie go następnie do CSIRTu krajowego.

6.7.5 Pozostałe podmioty

Zadania i role pozostałych interesariuszy nie różnią się w tym modelu zasadniczo od tego, co zostało przedstawione w rozdziale 6.3.

6.7.6 Opis zalet i wad modelu

W wariancie pośrednim zachowane jest w większości zaangażowanie dotychczasowych kadr merytorycznych z obszaru bezpieczeństwa IT, choć wymagane są istotne zmiany organizacyjne i przesunięcia ról poszczególnych podmiotów. Oznacza to w szczególności konieczność znacznego zwiększenia zasobów Agencji Bezpieczeństwa Wewnętrznego.

Model jest też stosunkowo prosty do wprowadzenia, ponieważ nie wymaga daleko idących zmian legislacyjnych oraz związanych z planowaniem budżetu, ani wysokich nakładów na uruchomienie.

Przy zachowaniu większości zalet modelu rozproszonego, w tym dużej skuteczności i elastyczności działania, model pośredni niesie jednak ze sobą pewne ryzyka. Przede wszystkim, połączenie CSIRTu krajowego z obszarem administracji wiązać się musi ze zwiększeniem nakładów wynikających z formalizmów, biurokracji i proceduralizacji. Wiąże się z tym także ryzyko zapewnienia odpowiedniego poziomu finansowania wyłącznie ze środków publicznych, a co za tym idzie mała odporność na ewentualny kryzys finansów publicznych. Nowy podmiot musiałby także od nowa budować wizerunek, renomę i sieć kontaktów w środowisku międzynarodowym.

Umiejscowienie CSIRTu krajowego w ABW miałoby też potencjalne konsekwencje płynące z niechęci podmiotów do współpracy ze służbami specjalnymi. Z drugiej jednak strony, jak już pisaliśmy przy wariancie rozproszonym, za poważnym atakami na poziomie państwa stoją organizacje, którym skuteczne przeciwdziałanie możliwe jest przede wszystkim na poziomie służb, i to nie tylko w sferze technicznej. Choć w modelu należy przyjąć, że CSIRT krajowy dysponowałby odpowiednimi narzędziami prawnymi do wprowadzenia przymusu podjęcia określonych działań, korzyści płynące z dobrowolnej współpracy z podmiotami postrzeganymi jako niezależne są nie do przecenienia, tak więc w tym wypadku CSIRT krajowy w ABW musiałby być bardziej przejrzysty i otwarty na kontakty zewnętrzne. Należy jednak również wspomnieć, że część podmiotów prywatnych np. z sektora finansowego może mieć mniejszą skłonność do współpracy z CSIRTem krajowym, gdy ten jest osadzony w służbie specjalnej. Fakt ten nie jest obojętny dla oczekiwanej skuteczności działania modelu.

W modelu pośrednim mniejsza rola zostaje przypisana aspektowi badawczo-rozwojowemu na poziomie CSIRTu krajowego, którego role wyrażają się przede wszystkim w sferze działalności operacyjnej. Obszar badań zostaje zatem zagospodarowany przez Centrum Analityczne.

6.7.7 Wymiar prawny

Opisywany wariant pośredni w części opiera się na istniejących rozwiązaniach instytucjonalnych, niemniej jednak wymaga uzupełnień natury formalnoprawnej.

Również w niniejszym wariancie w pierwszej kolejności niezbędne jest powołanie Koordynatora. Przypisany Koordynatorowi zakres zadań i odpowiedzialności wymaga, aby funkcję tę pełnił minister lub wiceminister, co najmniej w randze podsekretarza stanu.

Umiejscowienie nowej kategorii spraw w dziedzinie administracji rządowej, tj. cyberbezpieczeństwa musi poprzedzić analiza przepisów obowiązującej ustawy z dnia 04 września 1997 r. o działach administracji rządowej. Na obecnym etapie wydaje się, że równouprawnione będzie dodanie nowej sprawy albo do działu „Sprawy wewnętrzne", albo do działu „Informatyzacja".

Po podjęciu decyzji co do umiejscowienia nowej kategorii, Prezes Rady Ministrów powinien wydać odpowiednie rozporządzenie w sprawie szczegółowego zakresu działania właściwego Ministra.

Zadania z zakresu cyberbezpieczeństwa winny być realizowane we właściwym ministerstwie przez dedykowane osoby, w ramach nowoutworzonego departamentu.

W uzupełnieniu roli administracji rządowej **należy powołać Radę Koordynacyjną ds. Cyberbezpieczeństwa przy Radzie Ministrów**. Rada Koordynacyjna działałaby jako organ opiniodawczy i doradczy w sprawach dotyczących cyberbezpieczeństwa.

W tym celu, na podstawie art. 12 ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów, Prezes Rady Ministrów, w drodze zarządzenia, powinien utworzyć Radę Koordynacyjną jako organ pomocniczy Prezesa Rady Ministrów.

Do zadań Rady należałoby formułowanie ocen i wyrażanie opinii w szczególności w sprawach projektów aktów normatywnych dotyczących cyberbezpieczeństwa, kierunków i planów działania organów zaangażowanych w ochronę cyberbezpieczeństwa czy koordynowania ich współdziałania. Rada mogłaby ponadto pełnić funkcję organu, do którego byłyby eskalowane poważne problemy w zakresie bezpieczeństwa w cyberprzestrzeni bądź problemy ze współpracą w ramach administracji publicznej.

Proponuje się, aby w skład Rady Koordynacyjnej weszli co najmniej:

1. przewodniczący – Prezes Rady Ministrów;
2. sekretarz Rady;
3. członkowie:
    a. minister właściwy do spraw wewnętrznych,
    b. minister właściwy do spraw zagranicznych,
    c. minister właściwy do spraw informatyzacji państwa,

d. Minister Obrony Narodowej,

e. minister właściwy do spraw finansów publicznych,

f. Szef Biura Bezpieczeństwa Narodowego.

W posiedzeniach Rady Koordynacyjnej, odbywających się nie rzadziej niż raz na kwartał lub *ad hoc* – w zależności od aktualnych potrzeb, mogą brać udział również, z głosem doradczym, eksperci zewnętrzni, których udział Rada uzna za niezbędny ze względu na tematykę spotkania.

Na tej samej podstawie prawnej mogą powstawać **zespoły zadaniowe**. Inicjatywa, a tym samym formalny wniosek do Prezesa Rady Ministrów w zakresie powołania zespołu zadaniowego, powinna obciążać Koordynatora.

Stały **Zespół Łącznikowy**, którego kompetencje opisano powyżej, powinien zostać powołany przy ministrze właściwym ds. cyberbezpieczeństwa. Biorąc pod uwagę planowany skład osobowy, zakres kompetencji oraz proponowane ulokowanie Zespołu przy Koordynatorze, podstawę w obowiązującym stanie prawnym można znaleźć w art. 34 ust. 3 ustawy z dnia 08 sierpnia 1996 roku o Radzie Ministrów. Zgodnie z przywołanym przepisem, Rada Ministrów może powołać przy ministrze komitet doradczy i określić zakres jego zadań.

Zgodnie z koncepcją opisywanego wariantu, rolę **krajowego CSIRTu obejmie, działający w ramach ABW, CERT.GOV.PL**. W omawianym wariancie aktualność zachowują zastrzeżenia podniesione w opisie wymiaru prawnego wariantu zdecentralizowanego, dotyczące braku formalnego umocowania CERT.GOV.PL do pełnienia funkcji CSIRTu rządowego. Jak wskazano powyżej, brak jest jednoznacznych podstaw prawnych, uzasadniających pełnienie przez zespół CERT.GOV.PL, funkcjonujący w ramach Departamentu Bezpieczeństwa Teleinformatycznego ABW, funkcji CSIRTu rządowego, a tym samym – krajowego. **Bezwzględnie konieczne jest zatem jednoznaczne określenie kompetencji, oraz procedur dla funkcjonującego w ABW zespołu CERT.GOV.PL do działania w obszarze całego państwa jako CSIRTu krajowego.** Wobec powyższego niezbędne będzie wprowadzenie odpowiednich zmian w art. 5 ustawy z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, poprzez wskazanie, że jednym z zadań Agencji Bezpieczeństwa Wewnętrznego jest pełnienie funkcji krajowego zespołu reagowania na incydenty komputerowe. Omawiane rozszerzenie kompetencji CERT.GOV.PL winno obejmować również administrację samorządową, a w przypadku, gdyby nie powołano odrębnego CSIRTu dla infrastruktury krytycznej, także infrastrukturę krytyczną.

Powierzenie CERT Polska/NASK funkcji Krajowego Centrum Analitycznego powinno się odbyć z wykorzystaniem procedury opisanej w art. 37 ustawy z dnia 30 kwietnia 2010 roku o instytutach badawczych. Na podstawie powołanego przepisu Minister Nauki i Szkolnictwa Wyższego, na wniosek ministra właściwego ds. cyberbezpieczeństwa, może nałożyć na NASK

jako instytut badawczy zadanie, zgodnie z zakresem działania określonym w statucie instytutu, jeżeli jest to niezbędne ze względu na potrzeby obronności lub bezpieczeństwa publicznego, w przypadku stanu klęski żywiołowej lub w celu wykonania zobowiązań międzynarodowych. Zakres działania NASK określony w § 8 Statutu z dnia 25 marca 2011 roku obejmuje m.in. prowadzenie badań naukowych i prac rozwojowych w zakresie bezpieczeństwa sieci i systemów teleinformatycznych.

Realizacja zadania w postaci obowiązku pełnienia funkcji Krajowego Centrum Analitycznego powinna odbywać się odpłatnie, na podstawie umowy pomiędzy NASK a właściwym ministrem Koordynatorem. Umowa powinna określać szczegółowe obowiązki CERT Polska w zakresie pozyskiwania informacji i bieżące analizowanie sytuacji w obrębie zagrożeń cyberprzestrzeni.

Powołanie CSIRTów sektorowych, np. dla energetyki czy sektora bankowego, powierzyć należy właściwym organom administracji rządowej, w ramach ich kompetencji. Dla przykładu, CSIRT dla sektora energetycznego mógłby działać przy Prezesie Urzędu Regulacji Energetyki (URE). Prezes URE zobowiązany jest m.in. do monitorowania funkcjonowania systemu gazowego i elektroenergetycznego w zakresie bezpieczeństwa dostarczania paliw gazowych i energii elektrycznej. Wydaje się zasadne, aby w opisanym pojęciu mieściło się również bezpieczeństwo teleinformatyczne przesyłu gazu i energii elektrycznej.

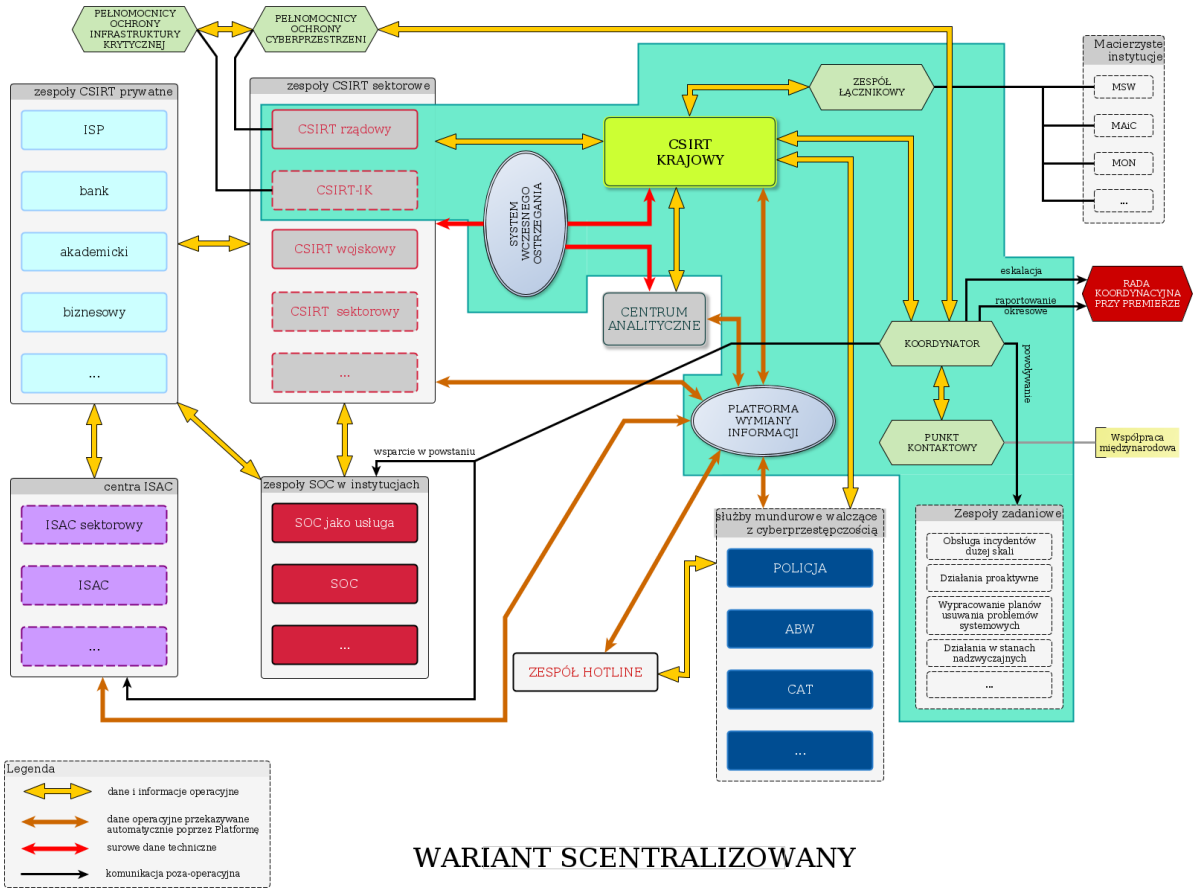
Rolą Koordynatora winno być ponadto dopilnowanie, aby zgodnie z obowiązującą Polityką Ochrony Cyberprzestrzeni RP, w ramach każdej jednostki organizacyjnej administracji rządowej **powołany został pełnomocnik ds. bezpieczeństwa cyberprzestrzeni**, z zadaniami określonymi tamże.

6.8 Wariant scentralizowany

Wariant scentralizowany zobrazowany schematyczne na rysunku poniżej, zakłada powołanie nowej instytucji – Narodowego Centrum Cyberbezpieczeństwa (ang. *National CyberSecurity Centre*), w której połączone zostałyby role Koordynatora, Punktu Kontaktowego, zespołów CSIRT – krajowego, rządowego oraz Infrastruktury Krytycznej, a opcjonalnie także Centrum Analitycznego. Należy zauważyć, że instytucja taka wypełniałaby rozliczne zadania nie tylko w warstwie operacyjnej, ale także w warstwie strategicznej. Oznacza to, że instytucja ta powinna być umocowana w strukturach administracji państwowej.

Schemat nie wyczerpuje wszystkich relacji pomiędzy podmiotami, np. możliwości dostępu przez CSIRTy prywatne zespoły SOC dostępu do niektórych elementów platformy wymiany wiedzy.

Szczegółowe omówienie najważniejszych podmiotów systemu znajduje się poniżej.



Rysunek 10. Mapa relacji w wariancie scentralizowanym.

6.8.1 Narodowe Centrum Cyberbezpieczeństwa

Narodowe Centrum Cyberbezpieczeństwa (NCC) jest w wariancie scentralizowanym głównym podmiotem odpowiedzialnym za koordynację i jednocześnie realizację zadań z obszaru cyberbezpieczeństwa. Wśród podstawowych zadań, wynikających z przypisania NCC ról Koordynatora i Punktu Kontaktowego znalazłyby się:

- proponowanie i przygotowywanie projektów odpowiednich ram prawnych systemu bezpieczeństwa cyberprzestrzeni,
- nadzorowanie procesu wdrażania prawa i wynikających z niego polityk czy programów – w omawianym obszarze,
- powoływanie Zespołu Łącznikowego oraz - Zespołów Zadaniowych (mogących dysponować budżetem od Koordynatora) dla rozwiązywania problemów bieżących (incydentów, sytuacji kryzysowych) oraz wypracowywania rozwiązań dla problemów strukturalnych, systemowych, prawnych,

- eskalacja na poziom Rady Ministrów problemów dużej skali związanych z bezpieczeństwem cyberprzestrzeni bądź problemów ze współpracą w ramach administracji publicznej,
- wspieranie rozwoju współpracy w dziedzinie bezpieczeństwa cyberprzestrzeni,
- wspieranie powstawania CSIRTów sektorowych oraz centrów sektorowych ISAC,
- bieżąca współpraca z CSIRTami sektorowymi a także centrami ISAC,
- pełnienie roli Punktu Kontaktowego dla współpracy międzynarodowej (szczególnie w ramach Unii Europejskiej),
- współpraca z organami ścigania oraz organem właściwym w zakresie ochrony danych osobowych,
- raportowanie cykliczne na poziom Rady Koordynacyjnej przy Prezesie RM o stanie bezpieczeństwa cyberprzestrzeni i wysuwanie inicjatyw w zakresie poprawy tego stanu.

NCC musiałoby jednocześnie dysponować bardzo szerokimi kompetencjami technicznymi, pozwalającymi na realizowanie zadań CSIRTu krajowego, rządowego oraz Infrastruktury Krytycznej, które w szczególności musiałyby obejmować:

- bezpośrednie reagowanie na incydenty w obszarach administracji rządowej, samorządów terytorialnych oraz w instytucjach stanowiących część IK,
- przyjmowanie raportów od CSIRTów sektorowych,
- prace w międzynarodowej sieci współpracy zespołów CSIRT powołanych w krajach Unii Europejskiej, w tym wymiana informacji o incydentach transgranicznych,
- koordynowanie reagowania na incydenty i zagrożenia dotyczące wielu sektorów,
- rozwiązywanie problemów w sytuacjach, gdy nie istnieją właściwe CSIRTy sektorowe, zespoły czy centra bezpieczeństwa,
- utrzymywanie stałej świadomości sytuacyjnej,
- prowadzenie Krajowego Centrum Analitycznego.

Narodowe Centrum Cyberbezpieczeństwa musiałoby współpracować ściśle z CSIRTami sektorowymi, ISACAmi oraz organami ścigania – przede wszystkim przez Zespół Łącznikowy. W wielu wypadkach byłoby także bezpośrednim partnerem do kontaktu dla Pełnomocników Ochrony Cyberprzestrzeni (przede wszystkim dla mniejszych instytucji administracji publicznej, oraz wszędzie tam, gdzie nie zostaną utworzone zespoły bezpieczeństwa czy CSIRT). W warstwie strategicznej NCC uczestniczyłoby w pracach Rady Koordynacyjnej przy Premierze RP.

W przypadku przypisania NCC również roli Centrum Analitycznego, w zakres działań tej instytucji zostałby włączony obszar naukowo-badawczy, co oczywiście oznacza zwiększenie

liczby pracowników NCC i rozszerza spektrum wymaganych kompetencji. Alternatywą jest korzystanie przez NCC z usług zewnętrznego Centrum Analitycznego, stale i/lub w formie zlecania i finansowania konkretnych badań i analiz przez podmioty zewnętrzne. Należy zauważyć, że nadmierne rozdzielenie badań w sposób niezależny po różnych podmiotach z dużym prawdopodobieństwem osłabiałoby zdolności analityczne NCC i nie wpływałoby pozytywnie na budowanie świadomości sytuacyjnej.

Z uwagi na szczególną rolę NCC w reagowaniu na incydenty z wielu istotnych obszarów, instytucja ta powinna zapewniać swoje usługi w trybie 24/7.

Z powyższych opisów wynika, że przy tworzeniu NCC konieczne byłoby zatrudnienie licznego personelu, zarówno o profilu administracyjno-prawnym, jak i technicznym (a w przypadku włączenia roli Centrum Analitycznego także naukowym). Ze względu na specyfikę zadań NCC, zasadne wydaje się, aby instytucja ta miała formę prawną agencji wykonawczej (patrz rozdział 6.8.4).

6.8.2 Opcjonalnie – Krajowe Centrum Analityczne (NASK)

W przypadku rezygnacji z przypisania NCC roli Krajowego Centrum Analitycznego, rekomendujemy wykorzystanie w tym zakresie kompetencji działającego w NASK zespołu CERT Polska. Uzasadnienie tej rekomendacji podajemy w 6.7.3.

6.8.3 Opis zalet i wad modelu

Stworzenie jednego podmiotu, w którym skupiona jest większość zadań i odpowiedzialności z dziedziny cyberbezpieczeństwa może się wydawać bardzo atrakcyjnym pomysłem, przede wszystkim ze względu na prostotę modelu. Znaczna część kluczowych interakcji i cały przepływ informacji na linii Koordynator – Punkt Kontaktowy – CSIRTy odbywa się w ramach jednej instytucji. Wiąże się to także z uproszczeniem tworzenia budżetu na cyberbezpieczeństwo, ponieważ środki mogą być dysponowane na jedną instytucję i wewnątrz niej alokowane. W ramach tego budżetu NCC mogłoby także korzystać z kompetencji zewnętrznych w ramach zapotrzebowania.

Podstawowym problemem związanym z modelem jest fakt, że w najmniejszym stopniu wykorzystuje on istniejące już kompetencje i zbudowane instytucje oraz relacje między nimi. Należy podkreślić, że w modelu scentralizowanym powinno się zadbać o zagospodarowanie potencjału osób i instytucji obecnie realnie operacyjnie zaangażowanych w proces ochrony cyberprzestrzeni. Niemniej jednak, stworzenie podmiotu o tak szerokich kompetencjach jak NCC wiązałoby się de facto z rewolucją wśród podmiotów zajmujących się obecnie cyberbezpieczeństwem – część z nich utraciłaby niektóre pełnione obecnie role. Prowadziłoby to także do potencjalnych konfliktów pomiędzy podmiotami, których kompetencje miałyby być integrowane. Wszystkie mechanizmy współpracy musiałyby zostać

zaprojektowane i przepracowane na nowo. Byłoby to zaprzepaszczenie dotychczasowych dokonań i włożonego już wysiłku, niekoniecznie prowadzące do lepszego efektu.

Kolejnym istotnym ryzykiem jest pozyskanie odpowiednio licznego personelu o odpowiednich wysokich kwalifikacjach. Biorąc pod uwagę ograniczoną dostępność specjalistów w dziedzinie cyberbezpieczeństwa na rynku pracy, nieuchronnie wiązałoby się to z problemami z jego zatrudnieniem i utrzymaniem. Jak pokazują doświadczenia z krajów takich jak np. Holandia, gdzie istniejące zespoły CSIRT zastąpione zostały przez NCC, istotna zmiana charakteru pracy (np. wprowadzenie pracy zmianowej, praca w charakterze urzędnika, obowiązek większej sprawozdawczości itd.) jest dla specjalistów zniechęcająca i powoduje ich odpływ do wyjątkowo chłonnego w dziedzinie bezpieczeństwa sektora prywatnego.

Stworzenie NCC wymaga także daleko idących zmian prawnych, zarówno związanych z powołaniem nowej instytucji, jak i z porządkowaniem relacji pomiędzy poszczególnymi podmiotami. Ponieważ szereg tych zmian musiałoby być wprowadzonych na poziomie ustaw, należy spodziewać się, że wprowadzenie tego modelu musiałoby być związane z długim czasem uruchomienia poprzedzonym odpowiednim procesem legislacyjnym.

Dużym ryzykiem jest także zapewnienie finansowania dla NCC na odpowiednim poziomie. Oprócz wysokiego kosztu uruchomienia, NCC będzie wymagało stałych wysokich środków na utrzymanie – na płace, szkolenia personelu, sprzęt czy podróże służbowe. Będzie to więc wysoka pozycja kosztowa skupiona w jednym centrum budżetowym, co może skłaniać do szukania oszczędności, które nie pozostałyby bez wpływu na działanie NCC. Konsekwencją jest bardzo silna zależność modelu od stanu finansów publicznych.

Podobnie jak w wariancie pośrednim, badania naukowe i działalność rozwojowa miałyby w modelu scentralizowanym stosunkowo niski priorytet.

Nie można również wykluczyć, że skupienie wielu kluczowych funkcji, zarówno operacyjnych, jak i strategicznych, w jednej instytucji, działającej w ramach administracji państwowej, może zwiększać jej podatność na doraźne zmiany polityczne.

6.8.4 Wymiar prawny

Powołanie NCC jako organu wyłącznie właściwego w sprawach cyberbezpieczeństwa RP może nastąpić wyłącznie w drodze ustawy, uzupełnionej szeregiem aktów wykonawczych.

W zakresie wyboru formy prawnej odpowiadającej założonemu zakresowi zadań NCC, autorzy opracowania dostrzegają dwie możliwości: ukształtowanie NCC jako agencji wykonawczej w rozumieniu ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, na wzór Narodowego Centrum Badań i Rozwoju albo urzędu centralnego, na wzór Agencji Bezpieczeństwa Wewnętrznego.

A. NCC jako agencja wykonawcza

NCC może zostać powołane w drodze ustawy jako nowa agencja wykonawcza w administracji publicznej.

Zgodnie z informacjami udostępnianymi przez Biuro Analiz Sejmowych: *„Agencje wykonawcze to instytucje nowego zarządzania publicznego, które od lat 90. wprowadza się w wielu krajach europejskich oraz w administracji Unii Europejskiej*". Z założenia, agencja wykonawcza, jako przykład nowoczesnego zarządzania w administracji publicznej, ma zajmować się określonym rodzajem usług, adaptując sposoby zarządzania wykorzystywane w sektorze prywatnym na grunt publicznoprawny.

Agencje wykonawcze są jednostkami sektora finansów publicznych, państwowymi osobami prawnymi, powoływanymi najczęściej w celu realizacji technicznych lub naukowych zadań państwa. **Agencje wykonawcze z reguły są podległe i nadzorowane przez konkretne organy centralnej administracji publicznej**, ale w odróżnieniu od departamentów ministerstw mają dużą autonomię.

W przypadku powołania NCC jako agencji wykonawczej w pierwszej kolejności należałoby ustalić, któremu z ministrów byłaby podległa nowa agencja wykonawcza. Analiza zadań przypisanych NCC prowadzi do wniosku, że w obecnym stanie prawnym równouprawnieni do sprawowania nadzoru nad NCC wydają się być minister spraw wewnętrznych i minister właściwy ds. informatyzacji państwa.

W dalszej kolejności należałoby określić zakres zadań NCC. W przypadku NCBiR, dyrektora Centrum powołuje na czteroletnią kadencję minister właściwy do spraw nauki, po przeprowadzeniu konkursu. Ministrowi właściwemu do spraw nauki dyrektor NCBiR składa również sprawozdania finansowe.

Ustawa powinna również określać zadania NCC. W tym kontekście należy wskazać, że zadania NCBiR, opisane w ustawie z dnia 30 kwietnia 2010 roku o Narodowym Centrum Badań i Rozwoju, w nieznacznym stopniu odpowiadają planowanym do przypisania zadaniom NCC. W zasadniczej części zadania NCBiR dotyczą **finansowania lub współfinansowania** strategicznych programów badań naukowych i prac rozwojowych, w tym na rzecz bezpieczeństwa i obronności państwa. NCBiR ma ponadto obowiązek zarządzania ww. programami, może także współpracować w toku realizacji swoich ustawowych zadań z innymi podmiotami lub zlecać ich realizację organizacjom pozarządowym.

Mając na uwadze powyższe można stwierdzić, iż **agencje wykonawcze w polskim systemie prawnym mają raczej charakter jednostek zarządzających określonymi dziedzinami administracji państwowej i finansowaniem w ich ramach programów i projektów, ich rola ogranicza się raczej do koordynowania działań innych podmiotów, a**

nie prowadzenia samodzielnej działalności operacyjnej, czego, jak się wydaje, należałoby wymagać od NCC.

Ponadto, agencje wykonawcze, a szczególnie zasady ich autonomii, spotykają się z krytyką. Najczęściej dotyczy ona **przepływu informacji oraz możliwości bezpośredniego oddziaływania ministerstwa na agencję, co może okazać się konieczne w razie zmian strategii rządowych lub konieczności interwencji politycznych**. Istnieje także pogląd, że **agencje niekiedy monopolizowane są przez ośrodki polityczne**, tworząc swoistego rodzaju „państwo w państwie". Istotną cechą funkcjonowania agencji wykonawczych jest również fakt, że z reguły **zadania agencji wykonawczych realizowane są w trybie zlecenia dawanego na zewnątrz agencji**.

Równie istotną kwestią, przemawiającą raczej przeciwko formułowaniu NCC jako agencji wykonawczej, jest okoliczność, że podstawą gospodarki finansowej agencji wykonawczej jest roczny plan finansowy, zatwierdzony przez sprawującego nad nią nadzór ministra. Agencja wykonawcza może zaciągać zobowiązania na okres realizacji danego zadania przekraczający rok budżetowy, jeżeli plan przewiduje także obsługę kosztów z tego tytułu w ramach pozycji wydatków. **Uzyskaną na koniec roku nadwyżkę finansową agencja zobowiązana jest odprowadzić do budżetu państwa. Odstąpienie od tej zasady możliwe jest tylko w szczególnie uzasadnionych wypadkach i za zgodą Rady Ministrów.** Z drugiej jednak strony, może się okazać, że w ramach budżetu NCC jako agencji wykonawczej będzie można swobodniej niż w urzędach administracji państwowej ustalać stawki wynagrodzeń dla pracowników NCC.

B. NCC jako urząd centralny

NCC może funkcjonować jako urząd administracji rządowej, którego szef byłby jednocześnie centralnym organem administracji rządowej, podległym bezpośrednio Prezesowi Rady Ministrów i podlegającym kontroli Sejmu RP.

Mając na uwadze opisane zadania NCC, kompetencje, obowiązki i sposób działania NCC, powinny być określone w ustawie. Jednocześnie, należy stwierdzić, że utworzenie NCC jako nowego urzędu centralnego będzie musiało się wiązać z jednoznacznym ograniczeniem kompetencji Agencji Bezpieczeństwa Wewnętrznego, a częściowo być może również innych instytucji, np. Rządowego Centrum Bezpieczeństwa. W przeciwnym wypadku bardzo prawdopodobne są spory kompetencyjne pomiędzy istniejącymi instytucjami a nową agencją wykonawczą. Dla przykładu, potencjalną dziedziną, w której ochrony zakresie może, w przypadku przyjęcia opisywanego wariantu scentralizowanego, dochodzić do wątpliwości co do tego, który z organów jest zobowiązany do podejmowania działań, jest ochrona infrastruktury krytycznej.

Dla zapewnienia skuteczności działania NCC niezbędne jest zagwarantowanie, aby podobnie, jak w art. 10 ustawy z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, wprowadzić zobowiązanie dla organów administracji publicznej i samorządowej oraz innych instytucji państwowych i, w pewnym zakresie, również prywatnych, do współpracy z NCC, w tym udzielania pomocy w realizacji zadań NCC.

Jeśli chodzi o sposób powołania szefa NCC, także powinien być zbliżony do określonego w ustawie z dnia 24 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu sposobu powoływania szefa ABW i AW, włączając w to wymogi podmiotowe dla ewentualnych kandydatów.

Mając na uwadze, że NCC miałoby być nowym centralnym organem administracji rządowej, absolutnie niezbędne jest również zapewnienie mu odpowiedniego budżetu. W tym kontekście należy rozważyć zmianę rozporządzenia Ministra Finansów z dnia 4 grudnia 2009 r. w sprawie klasyfikacji części budżetowych oraz określania ich dysponentów, poprzez dodanie nowej części - NCC.

C. Koncepcja NCC - podsumowanie

Niezależnie od uzgodnionej formy prawnej – tj. agencji wykonawczej albo urzędu centralnego – proces uchwalania ustawy powołującej NCC musi być poprzedzony szerokimi konsultacjami społecznymi ze środowiskiem i ekspertami, w tym z zakresu bezpieczeństwa teleinformatycznego. Z uwagi na stopień skomplikowania regulowanej materii, kompleksowy charakter regulacji, jak również fakt, że bezpieczeństwo teleinformatyczne odgrywa zasadniczą rolę w najróżniejszych dziedzinach życia społecznego (np. bankowość, komunikacja, handel, etc.), w procesie legislacyjnym będą musieli uczestniczyć nie tylko specjaliści z zakresu cyberbezpieczeństwa, ale również eksperci z innych sektorów.

Wariant scentralizowany przewiduje również, że NCC będzie odpowiedzialne za utrzymywanie systemu wczesnego ostrzegania. Aktualnie rolę tę spełnia system ARAKIS.GOV; prace nad jego drugą wersją dobiegają końca. Należy jednakże pamiętać, że autorskie prawa majątkowe do systemu ARAKIS.GOV 2.0 służą Agencji Bezpieczeństwa Wewnętrznego. W przypadku nieuzyskania przez NCC prawa do korzystania z systemu ARAKIS.GOV 2.0 od Agencji Bezpieczeństwa Wewnętrznego, konieczne będzie zlecenie stworzenia nowego systemu pełniącego rolę systemu wczesnego ostrzegania i nabycie praw do korzystania z niego przez NCC, co oczywiście wiąże się z dodatkowymi kosztami i długim terminem realizacji.

Zważywszy na fakt, że w NCC ma zostać w istocie skupiona całość kompetencji państwa w zakresie cyberbezpieczeństwa, bezwzględną koniecznością jest również uważny dobór kadr. Potencjalni pracownicy NCC, i to nie tylko techniczni, będą jednocześnie musieli prezentować relatywnie wysoki poziom wiedzy specjalistycznej z zakresu bezpieczeństwa

teleinformatycznego, a z tego względu, ich wynagrodzenia winny odpowiadać co najmniej przeciętnym wynagrodzeniom wypłacanym pracownikom w sektorze prywatnym.

Uwzględniając wszystko powyższe, można z prawdopodobieństwem graniczącym z pewnością stwierdzić, że utworzenie NCC będzie procesem długotrwałym legislacyjnie, w szczególności z uwagi na konieczność stworzenia nowego aktu prawnego o randze ustawy, poprzedzenia jego uchwalenia szerokimi konsultacjami społecznymi, zapewnienia odpowiedniego finansowania z budżetu państwa oraz uzgodnienia zakresu kompetencji nowego organu.

6.9 Wariant - pozostawienie sytuacji bez zmian

Brak wprowadzenia systemowego zarządzania ochroną cyberprzestrzeni RP niesie ze sobą poważne ryzyko braku odpowiedniej reakcji państwa (czy też w praktyce reakcji chaotycznej i przypadkowej) w obliczu zdarzenia kryzysowego w cyberprzestrzeni, które może nieść ze sobą poważne skutki dla obronności państwa oraz dla jego gospodarki i jej rozwoju.

Poza klasycznie już przytaczanym przykładem ataków DDoS na Estonię i możliwości ich powtórki względem Polski, można sobie wyobrazić w przyszłości również bardziej realistyczne scenariusze np. ataku DoS na system składania PITów, który niósłby konsekwencje dla Ministerstwa Finansów, a także zwykłych obywateli w zakresie potencjalnej odpowiedzialności karnoskarbowej. Hipotetycznie możliwe są też w przyszłości scenariusze terrorystycznych ataków na elektrownie, w konsekwencji doprowadzające do braków w dostarczaniu prądu ("blackout") na dużą skalę.

Innym przykładem sytuacji kryzysowej mogłoby być przeprowadzenie przez zorganizowaną grupę przestępczą czy terrorystyczną masowego włamania do kilku wiodących banków w Polsce, czym mogliby sparaliżować system finansowy, a także poważnie naruszyć zaufanie obywateli do bankowości internetowej.

Opracowanie scenariuszy, jak państwo reaguje w takich sytuacjach, wyznaczenie ról i odpowiedzialności oraz zapewnienie mechanizmów radzenia sobie z nieprzewidzianymi przypadkami jest kluczowe w celu minimalizacji negatywnych konsekwencji tych wydarzeń. Obecnie niestety takich rozwiązań systemowych brakuje.

Poza sytuacjami nadzwyczajnymi, nakreślonymi powyżej, wprowadzenie konsekwentnego systemu zarządzania ochroną cyberprzestrzeni RP pozwoli na skuteczniejsze działania przeciwko atakom, które już dziś są codziennością. Przykładem mogą być tu znane kampanie cyberszpiegowskie (stanowiące podzbiór ataków *Advanced Persistent Threats* - APT) przeprowadzane przez obce państwa (opisywane w ujęciu polskim m.in.

w raportach CERT.GOV.PL[82] i CERT Polska[83]. Podobnie z atakami przygotowawczymi innych państw mogących mieć na celu ułatwienie przejęcia kontroli nad polską infrastrukturą sieciową w przypadku ewentualnego konfliktu. W tej sytuacji konieczne jest wykonywanie działań proaktywnych w celu zwiększenia możliwości wczesnego wykrycia tego rodzaju zagrożeń i lepszego ich zrozumienia, a w konsekwencji minimalizacji strat.

Podobnie jest z cyberprzestępczością - skuteczniejsze mechanizmy jej zwalczania, przede wszystkim poprzez zwiększenie współpracy pomiędzy zespołami CERT, Policją, prokuraturą i Sądami, są niezbędne jeżeli cyberprzestępczość ma w przyszłości nie stać się poważnym problemem społecznym. Konieczne jest również wprowadzenie konsekwentnych i systemowych rozwiązań w zakresie zwiększenia świadomości obywateli co do zagrożeń w cyberprzestrzeni, w tym obszarze bowiem tzw. "przeciętny internauta" stanowi podstawowe ogniwo bezpieczeństwa państwa. Niestety, jak wykazują badania Komisji Europejskiej, w wielu sytuacjach świadomość obywateli RP dotycząca zagrożeń jest poniżej średniej Unijnej[84].

[82] http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html
[83] http://www.cert.pl/PDF/Raport_CP_2014.pdf
[84] Special Eurobarometer 404 Cyber Security Report
http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

7 Warstwa strategiczna funkcjonowania krajowego systemu ochrony cyberbezpieczeństwa

7.1 Wstęp

Obszar cyberbezpieczeństwa jest obszarem horyzontalnym, przenikającym wszystkie sektory gospodarki kraju, mający wpływ na funkcjonowanie państwa i społeczeństwa. W rozdziale 2.2 dokonano próby zidentyfikowania podmiotów, głównie państwowych, które pełnią obecnie określone role w obszarze cyberbezpieczeństwa, lub są istotne z punktu widzenia zapewnienia odpowiedniego poziomu bezpieczeństwa na poziomie krajowym.

Niniejszy rozdział prezentuje opis koncepcji funkcjonowania systemu cyberbezpieczeństwa krajowego w warstwie strategicznej. Odniesiono się nie tylko do ról opisanych we wspominanym rozdziale, ale także zawarto rekomendacje pełnienia określonych ról, które do tej pory nie były pełnione przez istniejące instytucje. Opis zawiera także propozycje powołania nowych instytucji.

Podobnie jak przy opisie warstwy operacyjnej funkcjonowania przyszłego systemu cyberbezpieczeństwa (por. rozdział 6) odniesiono się do podejścia wariantowego, w którym wyróżnia się trzy podstawowe warianty: scentralizowany, pośredni i rozproszony.

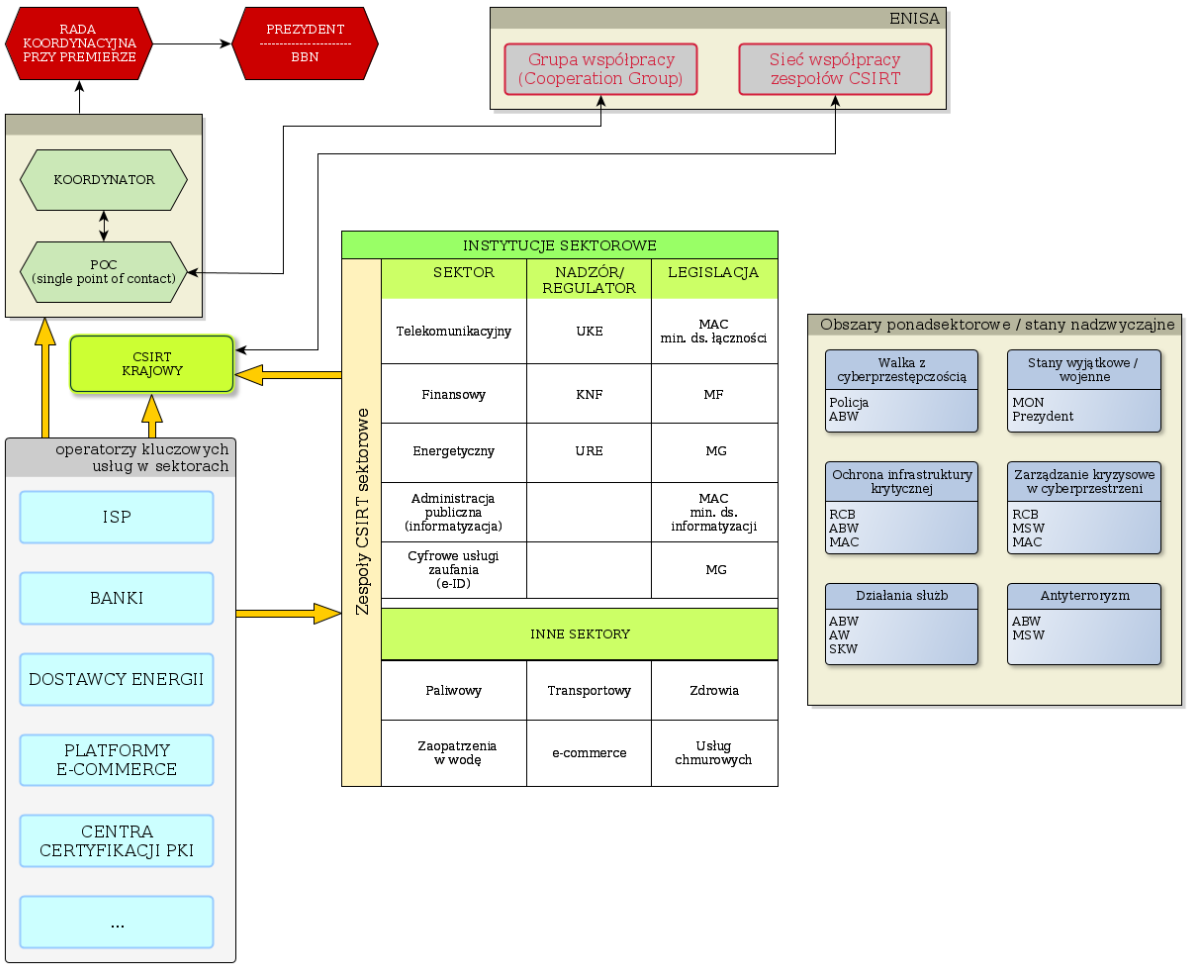
Warstwa strategiczna systemu jest na potrzeby niniejszego dokumentu definiowana jako podsystem, który zapewnia odpowiednie ramy legislacyjne, formalno prawne oraz polityczne funkcjonowania wszystkich istotnych podmiotów oraz współpracy pomiędzy nimi (także w obszarze międzynarodowym).

Autorzy dokumentu uznają, że kluczowe znaczenie ma przede wszystkim prawidłowe z praktycznego punktu widzenia funkcjonowanie warstwy operacyjnej całego systemu. Jednak bez odpowiednio zaprojektowanej i zorganizowanej warstwy strategicznej, która powinna pełnić rolę służebną w stosunku do warstwy operacyjnej – całość przyszłego systemu cyberbezpieczeństwa kraju nie będzie funkcjonowała w sposób optymalny.

W paragrafie 2. zamieszczono ogólny opis ról bez podziału na warianty, natomiast w paragrafie 3. zaprezentowano modele wariantowe funkcjonowania systemu w warstwie strategicznej.

7.2 Opis ogólny w warstwie strategicznej

Poglądowy schemat proponowanego systemu zarządzania bezpieczeństwem cyberprzestrzeni RP w warstwie strategicznej przedstawia poniższy rysunek.



Rysunek 11. Mapa podmiotów na poziomie strategicznym.

Wyróżniono kilka grup podmiotów, zarówno w relacjach krajowych jak też międzynarodowych (w ramach Unii Europejskiej). Kluczową rolą w tej warstwie jest rola instytucji koordynującej (Koordynator).

7.2.1 Koordynator

Rola instytucji koordynującej (Koordynator) została w innym rozdziale opisana także dla warstwy operacyjnej. W tym rozdziale skoncentrowano się zaś na zadaniach, które taka instytucja powinna pełnić w warstwie strategicznej.

Niezależnie od modelu (proponowanych wariantów) rola Koordynatora w tej warstwie powinna zakładać wypełnienie co najmniej zadań wymienionych poniżej:

- pełnienie roli głównego koordynatora całego systemu ochrony cyberbezpieczeństwa – głównie w warstwie cywilnej, lecz przy precyzyjnie ułożonych relacjach z obszarem wojskowym (cyberobrona),

- tworzenie, konsultowanie i przedstawianie odpowiednich rozwiązań legislacyjnych pozwalających na formalne funkcjonowanie całego systemu,
- nadzorowanie wdrażania ustaw i dokumentów programowych opisujących podejście do ochrony cyberprzestrzeni i sposób jej funkcjonowania w kraju, w tym określenie listy kluczowych sektorów i obszarów,
- opracowanie wieloletnich programów działania w dziedzinie bezpieczeństwa cyberprzestrzeni i przedstawianie ich do akceptacji Radzie Koordynacyjnej,
- pełnienie ról koordynacyjnych odnośnie współpracy międzynarodowej w dziedzinie ochrony cyberprzestrzeni wynikających z zobowiązań międzynarodowych, takich jak rola tzw. *competent authority* oraz *point of contact*, które przewiduje obecny projekt tzw. dyrektywy NIS,[85]
- przedstawianie raportów, propozycji zmian systemowych oraz w razie potrzeby eskalacji Radzie Koordynacyjnej przy Premierze,
- ścisła współpraca z CSIRTem krajowym,
- powoływanie i ścisła współpraca z Zespołem Łącznikowym,
- współpraca i koordynowanie działań z instytucjami administracji rządowej zajmującymi się pokrewnymi obszarami, takimi jak:
  - ochrona infrastruktury krytycznej państwa,
  - ściganie cyberprzestępstw,
  - ochrona antyterrorystyczna,
  - obrona narodowa,
  - obrona cywilna,
- powoływanie Zespołów Zadaniowych dla wypracowywania rozwiązań problemów w dowolnej warstwie systemu (operacyjnej lub strategicznej),
- wspieranie powstawania sektorowych zespołów CSIRT,
- wspieranie powstawania sektorowych centrów ISAC,
- współpraca z pozarządowymi ośrodkami administracji państwa zajmującycmi się problematyką ochrony cyberprzestrzeni (np. BBN).

7.2.2 Rada Koordynacyjna przy Premierze

Jest to organ polityczny, który składa się z przedstawicieli kluczowych organów administracji państwa. Ranga przedstawicieli w Radzie nie powinna być niższa niż:

[85] Autorzy dokumentu wyrażają pogląd, że w polskich realiach role *competent authority* oraz *point of contact* powinny zostać skupione w tej samej instytucji – niezależnie od wariantu

podsekretarz stanu w ministerstwie lub zastępca szefa danej instytucji – zajmującego się obszarem cyberprzestrzeni (idealnie: cyberbezpieczeństwa) jako główny priorytet.

Rekomenduje się, żeby stałymi członkami Rady byli nie tylko przedstawiciele administracji rządowej, ale także przedstawiciele Prezydenta RP, Sejmu, Senatu. Ważną rolę w posiedzeniach tego ciała powinien odgrywać Koordynator oraz krajowy CSIRT. Rada powinna także określić zasady, na jakich w jej spotkaniach (np. wybranych) mogliby brać udział interesariusze spoza administracji publicznej, reprezentujący określone sektory np. organizacje reprezentujące przedsiębiorców (Izby), którzy prowadzą działalnośc w obrębie cyberprzestrzeni i jej bezpieczeństwa. Proces poszerzania formuły Rady o przedstawicieli spoza administracji może być procesem ewolucyjnym w miarę kształtowania się praktyki funkcjonowania tego ciała.

Rada powinna zbierać się cyklicznie, nie rzadziej niż raz na kwartał, by otrzymywać aktualną informację od Koordynatora na temat bezpieczeństwa cyberprzestrzeni, stanu realizacji procesu wdrażania krajowego systemu ochrony wraz z propozycjami nowych rozwiązań pojawiających się problemów.

W obrębie zadań Rady jest akceptacja propozycji Koordynatora w zakresie działań strategicznych dotyczących ochrony cyberprzestrzeni, cykliczne omawianie sytuacji na podstawie raportów Koordynatora, a także przedstawianie Koordynatorowi uzgodnionych na forum Rady kierunkowych działań będacych w gestii Koordynatora.

Rada przyjmuje także wieloletnie programy działania w zakresie bezpieczeństwa cyberprzestrzeni, które przygotowuje Koordynator.

7.2.3 Zespół Łącznikowy

Zespół Łącznikowy zapewnienia stałą współpracę kluczowych podmiotów z punktu widzenia ochrony cyberprzestrzeni RP. Jest powoływany przez Koordynatora i składa się z przedstawicieli delegowanych przez macierzyste instytucje.

W skład zespołu powinni wchodzić przedstawiciele następujących ministerstw (wg podziału administracyjnego obowiązującego w trakcie przygotowywania niniejszego dokumentu):

- Ministerstwo Administracji i Cyfryzacji,
- Ministerstwo Spraw Wewnętrznych,
- Ministerstwo Obrony Narodowej,
- Ministerstwo Spraw Zagranicznych.

Oprócz tego członkami zespołu powinni być przedstawiciele ważnych instytucji zajmujących się bezpieczeństwem czy też ściganiem przestępstw, takich jak:

- Agencja Bezpieczeństwa Wewnętrznego,

- Policja,
- Rządowe Centrum Bezpieczeństwa,
- Narodowe Centrum Kryptologii,
- Biuro Bezpieczeństwa Narodowego,
- GIODO.

W skład zespołu powinni także wchodzić przedstawiciele instytucji, w których funkcjonują:

- CSIRT krajowy,
- CSIRTy sektorowe,
- Krajowe Centrum Analityczne.

Zaleca się także, aby kluczowe instytucje państwowe, nie będące administracją rządową, takie jak Kancelaria Sejmu także wyznaczyły swojego łącznika do Zespołu Łącznikowego.

Siedzibą działania zespołu powinna być siedziba instytucji sprawującej rolę Koordynatora w krajowym systemie ochrony cyberprzestrzeni lub krajowego CSIRT. Koordynator prowadzi sekretariat i na bieżąco korzysta z efektów pracy zespołu

Zespół łącznikowy ma mieć możliwość rozszerzania konsultacji merytorycznych o kolejne, zaproszone do współpracy, wyznaczonych wcześniej osoby łącznikowe z dowolnych instytucji i firm, które zadeklarują wolę wspierania pracy zespołu.

Role Zespołu Łącznikowego w warstwie operacyjnej zostały opisane w rozdziale 6.3.5. W warstwie wyższej zespół ten pełni istotną rolę poprzez wyciąganie wniosków z procesu rozwiązywania pojawiających się problemów cyberbezpieczeństwa oraz wnioskowanie do Koordynatora (a także macierzystych instytucji) o podjęcie działań usprawniających procesy (np. wprowadzenie nowych lub zmiana istniejących procedur, stworzenie nowych ram prawnych lub organizacyjnych itp.).

Zespół tworzy także cykliczne raporty dla Koordynatora i macierzystych instytucji – z zawartymi w nich rekomendacjami. Rekomendacje te są analizowane przez Koordynatora, który jest zobowiązany do nadania sprawie dalszego biegu (np. poprzez powołanie Grupy Zadaniowej do rozwiązania problemu, czy rekomendowania zmian systemowych na Zespole Zadaniowym przy Radzie Ministrów).

Instytucje sektorowe

W krajowym systemie ochrony cyberbezpieczeństwa, istotną rolę odgrywać powinny instytucje właściwe dla sektorów, które zostaną uznane za kluczowe w obszarze bezpieczeństwa. Pewną wskazówkę dla określenia listy sektorów lub obszarów istotnych

z punktu widzenia koordynacji krajowego systemu ochrony cyberprzestrzeni jest załącznik do projektowanej dyrektywy NIS. Rolą instytucji Koordynatora jest zaproponowanie, uzgodnienie i wpisanie do dokumentów legislacyjnych listy (wraz z definicjami) sektorów lub obszarów kluczowych. Wśród sektorów kluczowych standardowo wymienia się takie sektory jak: energetyka, telekomunikacja, transport, finanse, zdrowie czy administracja publiczna. Jednak w różnych krajach lista ta jest dostosowywana do lokalnych uwarunkowań.

Istotne dla całego procesu organizowania systemu bezpieczeństwa cyberprzestrzeni jest przyjęcie optymalnego podejścia do zagadnienia infrastruktury krytycznej we wszystkich kluczowych sektorach. Z jednej bowiem strony każdy z kluczowych sektorów opiera się na infrastrukturze teleinformatycznej, która powinna być odpowiednio chroniona. Z drugiej zaś strony istnieje pojęcie informatycznej infrastruktury krytycznej (ang. *Critical Information Infrastructure* - CII) jako często najważniejszej kategorii systemów (niezależnie jaką branżę reprezentują) podlegających skoordynowanej ochronie.

7.2.4 Informatyczna Infrastruktura Krytyczna

Informatyczna Infrastruktura Krytyczna występuje w sektorach gospodarki i obszarach społecznych uznanych za kluczowe czy krytyczne z punktu widzenia ochrony cyberprzestrzeni. Z tego względu jej bezpieczeństwo powinno być widziane całościowo (na wskroś poszczególnych sektorów) poprzez przypisanie odpowiedniej roli jednej instytucji, ale także w każdym sektorze z osobna, powinna istnieć instytucja odpowiedzialna za cyberbezpieczeństwo danego obszaru.

7.2.5 Sektor energetyczny

Sektor ten uznawany jest za kluczowy we wszystkich opracowaniach i strategiach wielu krajów dotyczących cyberbezpieczeństwa. W naszym kraju nie ma tymczasem instytucji, która na poziomie strategicznym lub operacyjnym zajmowałaby się całościowo, na poziomie calego kraju, cyberbezpieczeństwem tego sektora i byłaby za to odpowiedzialna. Dlatego też opisując stan obecny, pominięto np. instytucję regulatora w sektorze energetycznym w postaci Urzędu Regulacji Energetyki, która w przyszłym krajowym systemie ochrony niewątpliwie powinna odgrywać istotną rolę. Toteż w prezentowanych poniżej wariantach systemu w warstwie operacyjnej, URE został uwzględniony adekwatnie do wyzwań i koniecznych zadań do wypełnienia.

7.2.6 Sektor telekomunikacyjny

Telekomunikacja jest podstawą działania cyberprzestrzeni. Sektor ten jako pierwszy został uregulowany w obszarze cyberbezpieczeństwa – zarówno w Unii Europejskiej, jak też

wewnątrz kraju. Role ministra właściwego ds. łączności oraz Urzędu Komunikacji Elektronicznej zostały opisany w innym miejscu niniejszej ekspertyzy.

7.2.7 Sektor finansowy

Jest to także sektor wymieniany jako kluczowy w każdym opracowaniu strategicznym na temat bezpieczeństwa cyberprzestrzeni. Skala i możliwości operacji finansowych dokonywanych za pomocą systemów teleinformatycznych, zarówno w obrocie pomiędzy bankami, przedsiębiorcami, jak też z udziałem obywateli za pomocą Internetu jest coraz większa, a straty z powodu incydentów bezpieczeństwa wyrażają się w konkretnych kwotach. W Polsce zarówno system finansowy, jak też bankowy wraz z nadzorem w postaci KNF, który wyznacza odpowiednie standardy także w dziedzinie bezpieczeństwa teleinformatycznego, jest dobrze rozwinięty – patrząc nie tylko z punktu widzenia rozwoju infrastruktury informatycznej oraz jej bezpieczeństwa. Jednak rzeczywista skala incydentów nie jest znana, ze względu na niechęć (brak obowiązku) ujawniania przez instytucje finansowe jakichkolwiek danych na ten temat. Ten i inne problemy powinny być przedmiotem skoordynowanego działania w przyszłości w tym sektorze, poprzez np. powielenie wzorców współpracy sieci CSIRT, jak również poprzez rozwój roli instytucji regulatora w koordynacji sektorowego bezpieczeństwa teleinformatycznego.

7.2.8 Administracja publiczna

Obszar administracji publicznej jest niewątpliwie kluczowym obszarem, którego poziom cyberbezpieczeństwa wpływa na funkcjonowanie państwa, społeczeństwa i gospodarki. Wszelkie incydenty naruszające bezpieczeństwo systemów typu e-government powodują duże straty wizerunkowe, utratę zaufania a także konkretne szkody (np. wypływ wrażliwych danych). Jeszcze poważniejsze mogą być skutki ataków na systemy wewnętrzne administracji publicznej. Sieci ministerstw, parlamentu i innych ważnych instytucji państwowych są obiektem zaawansowanych ataków intruzów (często ze strony innych krajów).

Trudno jest więc sobie wyobrazić, aby administracja publiczna była obszarem wyłączonym z systemu obowiązków przestrzegania odpowiednich reguł i standardów bezpieczeństwa, a z drugiej strony koordynowała cały system bezpieczeństwa cyberprzestrzeni narzucając obowiązki w innych sektorach. Jednak obserwując negocjacje kształtu dyrektywy NIS można zaobserwować, że obszar ten, początkowo zawarty w propozycji Komisji Europejskiej, później zaczął zawężać się w kolejnych wersjach dyrektywy.

Niezależnie od końcowego kształtu dyrektywy NIS rekomenduje się, aby obszar systemów administracji publicznej w Polsce został włączony na podobieństwo innych sektorów do krajowego systemu cyberbezpieczeństwa jako obszar precyzyjnie zdefiniowanych obowiązków instytucji państwowych w dziedzinie osiągania właściwego poziomu ochrony. Istotne jest jednocześnie, aby nie ograniczać tego obszaru jedynie do instytucji administracji rządowej, pozostawiając poza systemem tak istotne organy państwa jak: Sejm, Senat czy Kancelarię Prezydenta.

7.2.9 Inne sektory i obszary

Na liście potencjalnych sektorów kluczowych czy krytycznych powinno się znaleźć jeszcze kilka innych, takich jak sektor paliwowy, transportowy czy też obszary związane z gospodarką elektroniczną, które nie podlegają pod regulacje sektora telekomunikacyjnego.

Szczególnie w tym ostatnim przypadku należy poważnie rozważyć włączenie sektora e-commerce pod skrzydła krajowego systemu ochrony cyberprzestrzeni. Chodziłoby głównie o duże przedsiębiorstwa zajmujące się handlem w internecie, duże portale czy sieci społecznościowe, które już obecne są obszarem zintensyfikowanego działania cyberprzestępców. Obecnie nie mają one obowiązków w zakresie zachowania minimalnych wymogów bezpieczeństwa teleinformatycznego, zgłaszania poważnych incydentów czy zasad sformalizowanej współpracy z organami ścigającymi cyberprzestępców. Taki stan rzeczy nie powinien się dalej utrzymywać. Argumenty słyszane z rożnych stron, że narzucanie jakichkolwiek standardów bezpieczeństwa w tym sektorze może doprowadzić do jego upadku, nie są trafne. Po pierwsze, skala nadużyć i incydentów stale rośnie i przekłada się na coraz większe straty obywateli, a po drugie, jeżeli obowiązki dotyczyłyby tylko przedsiębiorców prowadzących działalność na odpowiednio dużą skalę – wprowadzenie minimalnych wymogów bezpieczeństwa i np. obowiązku współpracy z zespołami CSIRT i organami ścigania doprowadzi raczej do zmniejszenia kosztów społecznych niż zagrożenia dla biznesu.

Wśród sektorów czy obszarów wymienianych we wspomnianym załączniku projektu dyrektywy NIS, który w dalszym ciągu ewoluuje, znajdują się także między innymi: systemy świadczące usługi chmurowe, internetowe punkty wymiany ruchu, sieci społecznościowe, elektroniczne systemy płatności, giełda papierów wartościowych i inne. Przy wyznaczaniu listy sektorów krytycznych i reguł jakim miałyby podlegać należy postępować ostrożnie i z rozwagą, przeprowadzając skrupulatną analizę ryzyk w danym sektorze. Takie zadanie powinno spoczywać na instytucji Koordynatora, który powinien wykorzystać wszelkie dostępne narzędzia dla przeprowadzenia właściwych analiz i konsultacji. Jednym

z podstawowych narzędzi może być wykorzystanie Zespołów Zadaniowych (powołanie przez Koordynatora zespołu ekspertów, który zajmie się sprawą wyznaczenia listy kluczowych obszarów i sektorów).

7.2.10 Zespoły Zadaniowe

Zespoły Zadaniowe byłyby powoływane przez instytucję Koordynatora do rozwiązywania zdefiniowanych problemów na poziomie operacyjnym jak i dla wypracowywania propozycji rozwiązań zagadnień w warstwie strategicznej czy organizacyjno-prawnej. Przykładowym zagadnieniem może być wyznaczanie kluczowych sektorów czy obszarów, które objęte zostałyby skoordynowanymi ramami systemu ochrony cyberprzestrzeni.

Skład Zespołu powinien być dostosowany do przedmiotu zadania postawionego przed zespołem. Zakłada się, że przedstawiciele danego Zespołu mogliby się wywodzić z dowolnego podmiotu, zarówno krajowego, jak i zagranicznego, państwowego jak i komercyjnego, środowiska akademickiego, dostawców rozwiązań, prawników, izb branżowych, organizacji zajmujących się bezpieczeństwem czy indywidualnych ekspertów.

Instytucja Koordynatora powoływałaby zespoły z własnej inicjatywy lub na wniosek np. CSIRTu krajowego bądź Rady Koordynacyjnej. Jest istotne, aby pracownicy Koordynatora posiadali zdolność zarządzania procesem pracy zespołów, a także potrafili ocenić efekty pracy zespołów, a nawet ich poszczególnych członków.

Zespół Zadaniowy może otrzymać budżet od Koordynatora na swoje działania.

7.3 Warianty organizacji systemu ochrony cyberprzestrzeni w warstwie strategicznej

Jak wspomniano w innych fragmentach ekspertyzy, w niniejszym opracowaniu przedstawiono trzy warianty organizacji krajowego systemu ochrony cyberprzestrzeni: wariant rozproszony, wykorzystujący maksymalnie istniejące instytucje i kompetencje w nich zgromadzone, wariant pośredni oraz wariant scentralizowany, wymagający powołania nowych instytucji,. Opis wariantów dla warstwy operacyjnej przedstawiono w rozdziale 6. Poniżej skoncentrowano się na opisach wariantów w kontekście warstwy strategicznej proponowanego systemu.

7.3.1 Wariant rozproszony

W wariancie rozproszonym instytucja Koordynatora powinna być zlokalizowana w jednym z istniejących ministerstw zajmujących się obszarami cyberprzestrzeni czy bezpieczeństwa. Wariant ten z założenia jest nastawiony na wykorzystanie istniejących

instytucji, także rekomendowane jest umiejscowienie Koordynatora w Ministerstwie Administracji i Cyfryzacji bądź w Ministerstwie Spraw Wewnętrznych. Wynika to z ról, które pełnią te ministerstwa, co zostało opisane w rozdziale 6. Ministerstwo to powinno także pełnić rolę Punktu Kontaktowego do współpracy międzynarodowej, gdyż nie widać przesłanek, by jeszcze bardziej system rozpraszać i rozdzielać funkcję Koordynatora i Punktu Kontaktowego.

Rada Koordynacyjna powinna być powoływana przez Prezesa Rady Ministrów niezależnie od wyboru wariantu. Przy powoływaniu tego ciała powinno się wykorzystać doświadczenia zebrane z pracy istniejącego obecnie Zespołu zadaniowego ds. bezpieczeństwa cyberprzestrzeni RP.

Zespół Łącznikowy także powinien zostać powołany (przez Koordynatora) niezależnie od przyjętego wariantu. Zespół ten powinien mieć zapewnione stałe warunki pracy i współpracy blisko CSIRTu krajowego przy stałym zaangażowaniu organizacyjnym a także merytorycznym ze strony Koordynatora.

CSIRT krajowy w wariancie rozproszonym został szerzej opisany w warstwie operacyjnej, gdyż w tej warstwie realizuje większość zadań. Jednakże tworzone przez krajowy CSIRT raporty oraz rekomendacje co do powoływania Zespołów zadaniowych przekazywane Koordynatorowi mają także znaczenie dla warstwy strategicznej. W wariancie rozproszonym CSIRT krajowy byłby zlokalizowany poza instytucją Koordynatora, w instytucji, w której funkcjonuje najstarszy i najbardziej doświadczony zespół CERT w Polsce (CERT Polska działający w NASK) – tak więc istotne jest właściwe ułożenie współpracy pomiędzy tymi dwoma podmiotami.

Wśród podmiotów zwanych na potrzeby opisu systemu ochrony cyberprzestrzeni- instytucjami sektorowymi, w wariancie rozproszonym zakładane jest maksymalne wykorzystanie ról i istniejących kompetencji.

W domenie ochrony infrastruktury krytycznej wiodącą rolę powinno pełnić Rządowe Centrum Bezpieczeństwa. W istniejących dokumentach programowych, takich jak NPOIK, teleinformatyczna infrastruktura krytyczna, wymieniona jest jako jeden z kluczowych sektorów wymagających ochrony. Jest to podejście prawidłowe, chodzi jednak o to, by przekładało się na praktycznie sprawne rozwiązania. W tym celu zaleca się, by RCB ściśle współpracowało z krajowym CSIRTem w zakresie transferu kompetencji w obszarze bezpieczeństwa cyberprzestrzeni, a także podejmowało działania skoordynowane z architekturą całego systemu nadzorowaną przez Koordynatora – w szczególności w aspekcie podziału ról i odpowiedzialności z innymi instytucjami, które zostaną wyznaczone do ochrony danego sektora krytycznego (np. w telekomunikacji, energetyce, sektora administracji publicznej itd.).

Przechodząc do poszczególnych sektorów można zaproponować podobne schematy działania w warstwie strategicznej. W każdym sektorze powinna być ustanowiona (często już taka istnieje) instytucja, która nadzoruje porządek prawny (modernizuje prawo, nadzoruje jego wdrażanie). W sektorze telekomunikacji jest to minister właściwy ds. łączności, w sektorze energetyki jest to ministerstwo gospodarki, administracja dysponuje działem informatyzacja, a sektor finansowy znajduje się w kompetencjach ministerstwa finansów. Oprócz tego Ministerstwo Spraw Wewnętrznych tworzy ramy systemu i nadzoruje bezpieczeństwo publiczne (przy wykorzystaniu np. Policji), czy zajmuje się kwestiami antyterrorystycznymi we współpracy z ABW. Instytucje te powinny dokonać odpowiednich aktywnych działań, aby w nowym systemie ochrony cyberprzestrzeni kraju rozwijać i nadzorować wdrażanie uregulowań w danych sektorach w odniesieniu do cyberbezpieczeństwa.

Oprócz podmiotów, które dbać będą o właściwy kształt i wdrażanie prawa w danych sektorach można wyróżnić instytucje regulatorów, które szczególny sposób tworzą rekomendacje i egzekwują w praktyce ustawy i rozporządzenia – tu w odniesieniu do bezpieczeństwa cyberprzestrzeni. Obecnie można wyróżnić przykłady takich rozwiązań dla sektorów: telekomunikacyjnego (UKE) i bankowości (KNF), które jednak działają w ramach nieco odmiennego podejścia do uzyskiwania właściwego efektu w postaci wysokiego poziomu bezpieczeństwa w danym sektorze.

Zaleca się, aby w każdym sektorze poważnie rozważyć zastosowanie modelu działania składającego się z trzech elementów: ustanawiania minimalnych wymogów bezpieczeństwa dla podmiotów działających w sektorze, obowiązku zgłaszania poważnych incydentów i zagrożeń cyberbezpieczeństwa oraz wprowadzenia wymogu przeprowadzania praktycznych audytów bezpieczeństwa, które byłyby przeprowadzane nie po to, by wyciągać konsekwencje, tylko by pomagać podmiotom w uzyskiwaniu coraz wyższego poziomu bezpieczeństwa teleinformatycznego. Należy zauważyć, że w wielu sektorach nie istnieją nawet takie ramy jak we wspomnianych wyżej sektorach bankowym i telekomunikacyjnym. W ramach powstawania systemu należy, jak wspomniano wyżej wypracować listę najważniejszych sektorów (może się ona rozszerzać w ramach realizacji wieloletnich planów czy strategii) oraz, jeśli to możliwe, ustanowić tandem instytucji: tworzącej prawo i regulatora (lub inaczej zdefiniowaną rolę, która zapewni jednak wdrażanie ustanowionych zasad cyber bezpieczeństwa). W szczególnych przypadkach w danym sektorze może być to jedna i ta sama instytucja.

Oczywiście bardzo ważnymi instytucjami są podmioty, w których funkcjonują CSIRTy sektorowe. Ponieważ zespoły CSIRT głównie działają w warstwie operacyjnej, zostało to szerzej opisane w innym rozdziale. W tym miejscu należy jednak zaznaczyć, że podmioty

takie jak Agencja Bezpieczeństwa Wewnętrznego, w której działa zespół CSIRTu administracji (CERT.GOV.PL) a także centrum antyterrorystyczne (CAT) odgrywają kluczową rolę jako ośrodki kompetencyjne, które wpływają (i jest to bardzo pożądane) na warstwę strategiczną, która bez wsparcia ze strony bieżącej, głębokiej wiedzy technologicznej i kompetencji operacyjnych – nie będzie mogła w praktyce właściwie funkcjonować i szybko oderwałaby się od rzeczywistości.

Pisząc o zespole CERT.GOV.PL można zarekomendować, by był on nie tylko CSIRTem administracji rządowej czy szerzej: publicznej ale także pełnił rolę CSIRTu infrastruktury krytycznej, względnie role wybranych CSIRTów sektorowych (np. energetyka, sektor paliwowy). Godne podkreślenia jest to, że niekoniecznie należy dążyć do powoływania odrębnych CSIRTów w każdym sektorze. Szczególnie w wariancie rozproszonym należy powierzać takie role istniejącym zespołom, a w dłuższej perspektywie dążyć do powoływania nowych zespołów CSIRT. Jest to jedna ze strategicznych ról dla Koordynatora.

7.3.2 Wariant pośredni

Wariant pośredni polega na tym, że w instytucja Koordynatora jest powoływana, podobnie jak w wariancie rozproszonym w jednym z istniejących ministerstw (MAC, MSW) i skupia w sobie także obowiązki Punktu Kontaktowego. Przez ten podmiot powoływane są i pracują na jego terenie Zespoły Zadaniowe.

Z kolei CSIRT krajowy, pracujący przy nim Zespół Łącznikowy, a także role CSIRTu administracji publicznej oraz CSIRTu dla infrastruktury krytycznej zostałyby w tym wariancie przypisane Agencji Bezpieczeństwa Wewnętrznego, w której funkcjonuje zespół CERT.GOV.PL. Inne instytucje sektorowe powinny funkcjonować podobnie jak w wariancie rozproszonym.

Analogicznie jak w wariancie rozproszonym zakłada się powstanie Rady Koordynacyjnej.

7.3.3 Wariant scentralizowany

W wariancie scentralizowanym zakłada się powstanie jednej, nowej instytucji centralnej w postaci agencji wykonawczej, która będzie w sobie skupiała wiele ról zarówno w warstwie strategicznej jak i operacyjnej. I tak agencja taka powinna pełnić rolę Koordynatora, Punktu Kontaktowego, a także CSIRTu krajowego i ośrodka, w którym jest powoływany i funkcjonuje Zespół Łącznikowy a także wszystkie Zespoły zadaniowe powoływane do rozwiązywania problemów i wyzwań. W ramach organizacji CSIRTu funkcjonującego w agencji, można lokować role CSIRTów sektorowych – odnośnie do potrzeb. Jednak docelowo, rozwiązania sektorowe powinny być obsługiwane przez dane sektory.

Centralna agencja wykonawcza ds. bezpieczeństwa cyberprzestrzeni powinna także przejąć obowiązki w zakresie ochrony krytycznej infrastruktury informatycznej w kraju (CIIP) obecnie znajdujące się w obszarze zadań RCB. Inne instytucje sektorowe powinny działać tak, jak opisano w wariancie rozproszonym.

Oprócz tego, jak w poprzednich wariantach powinna powstać Rada Koordynacyjna – niezależna od agencji wykonawczej ds. ochrony krajowej cyberprzestrzeni.

8 Analiza SWOT trzech wariantów

Poniżej przedstawiono analizę typu SWOT każdego z trzech opisanych wyżej wariantów dotyczących architektury przyszłego krajowego systemu ochrony cyberprzestrzeni. Następnie dokonano zestawienia pod kątem mocnych i słabych stron każdego z wariantów, a także zestawienia szans i zagrożeń towarzyszącym realizacji wariantów - według opinii autorów niniejszej ekspertyzy.

W szczególności, na potrzeby analizy SWOT przyjęto pewne kategorie, które podlegały ocenie porównawczej, takie jak:

- osiągnięty poziom bezpieczeństwa,
- wymiar czasowy, rozumiany jako czas realizacji danego wariantu,
- koszt wdrożenia wariantu (szacunkowo, porównawczy pomiędzy wariantami),
- wymiar kadrowy, rozumiany jako konieczność zaangażowania odpowiednich kadr merytorycznych,
- aspekt prawny, rozumiany jako skala koniecznych zmian legislacyjnych dla wdrożenia danego wariantu,
- wymiar reputacyjny, czyli między innymi kwestia poziomu zaufania do przyjętego modelu ze strony interesariuszy krajowych i aktorów międzynarodowych,
- aspekt operacyjny ,rozumiany jako praktyczna zdolność rozwiązywania problemów cyberprzestrzeni,
- aspekt badawczo rozwojowy, rozumiany jako możliwość prowadzenia koniecznych badań nad bezpieczeństwem cyberprzestrzeni.

Poszczególnym elementom podlegającym ocenie zostały przypisane pewne wagi odpowiadające priorytetom, jakie według oceny autorów należałoby przypisać oceniając skuteczność danego wariantu. I tak, najwyższy priorytet (1) został nadany kwestii poziomu bezpieczeństwa cyberprzestrzeni jaki jest osiągany w perspektywie 2-3 lat od rozpoczęcia wdrożenia danego wariantu.

Priorytet drugi (2) został przypisany takim kwestiom jak: czas wdrożenia (im krótszy, tym dany wariant wypada lepiej), jakość kadry merytorycznej (im skuteczniej w danym wariancie można wykorzystać istniejące kadry dysponujące wiedzą i praktyką, tym wariant wyżej oceniany), skuteczność procesu koordynacji, jednoznaczność odpowiedzialności czy zdolność do praktycznego wypełniania zobowiązań międzynarodowych.

Priorytet trzeci (3) przypisano takim cechom jak: koszty realizacji (funkcjonowania) wariantu, w tym narzut polityczny, ścieżka legislacyjna (w tym np. konieczność powoływania

nowych instytucji), kształcenie kadr i rozwój kompetencji, reputacja na starcie funkcjonowania systemu w danym wariancie i związane z tym zaufanie do modelu interesariuszy krajowych, zdolność do adaptowania się do nowych wyzwań i problemów, skuteczność formalnego zadaniowania i raportowania czy sprawność współpracy podmiotów zaangażowanych.

Najniższy priorytet - 4 - (choć są to elementy ważne, które także muszą być wzięte pod uwagę) przypisano takim zagadnieniom jak: koszt wdrożenia (jest to koszt rozumiany jako poniesiony jednorazowo, na starcie – w odróżnieniu od kosztów funkcjonowania ponoszonych rok po roku, która to cecha uzyskała priorytet 3), zaangażowanie prywatnych interesariuszy, rozpoznawalność na arenie międzynarodowej, zaufanie do modelu za granicą, utrzymanie zaangażowania dotychczasowych kadr merytorycznych i związana z tym kwestia skali koniecznych dopełnień tych kadr.

Poniżej zestawiono analizę SWOT trzech opisywanych w dokumencie wariantów: rozproszonego, pośredniego i scentralizowanego.

8.1 Wariant rozproszony

POZYTYWY	NEGATYWY
S mocne strony	**W słabe strony**
– wysoki poziom bezpieczeństwa cyberprzestrzeni (1), – krótki czas wdrożenia wariantu (2), – niższe koszty wdrożenia (4), – mniejsze koszty funkcjonowania, bez narzutu stanowisk politycznych (3), – utrzymanie zaangażowania wszystkich dotychczasowych merytorycznych kadr (4), – mniejszy wymóg dopełnienia ilościowego niezbędnych merytorycznych kadr (3), – większa zdolność do wykształcenia nowych kadr i dalszego rozwoju kompetencji (3), – wysoki poziom merytoryczności, wysoka jakość kadry (2), – mniejsza skala niezbędnych działań legislacyjnych (3), – większa zdolność do adaptowalnego angażowania nowych podmiotów do współpracy (4), – wyższa reputacja na starcie (3), – większe zaufanie do modelu ze strony podmiotów zagranicznych (4),	– mniejsza skuteczność formalnego zadaniowania i raportowania (3), – mniej jednoznacznie zdefiniowana odpowiedzialność (2), – brak mechanizmu ścieżki służbowej między wybranymi instytucjami (2), – mniejsza sprawność współpracy podmiotów (3),

– większe zaufanie do modelu ze strony zewnętrznych podmiotów krajowych (3), – większa rozpoznawalność międzynarodowa (4), – większa skuteczność działania, w tym zdolność reagowania , większa praktyczna efektywność i jakość działania (1), – lepsza adoptowalność do nowych problemów, nowych wyzwań (3), – lepsza praktyczna zdolność wypełniania zobowiązań międzynarodowych (2), – właściwy dla dziedziny kontekst badawczo-rozwojowy, skuteczniejsze prowadzenie i wdrażanie wyników badawczo-rozwojowych (3),	
O szanse	**T zagrożenia**
– większa szansa na skuteczne ubieganie się o środki zewnętrzne (unijne, natowskie, inne), – większa odporność na doraźne działania pozamerytoryczne (np. decyzje polityczne), – większa elastyczność w dostosowywaniu się do ewoluujących zagrożeń.	– gdy nienaruszona dostępność finansowania publicznego (budżetu państwa), to w dalszym ciągu ryzyko naruszenia trwałości rozwiązania – słabsze przełożenie na zewnętrzne ośrodki decyzyjne w państwie.

8.2 Wariant pośredni

POZYTYWY	NEGATYWY
S mocne strony	**W słabe strony**
– wysoki poziom bezpieczeństwa cyberprzestrzeni (1), – krótki czas wdrożenia wariantu(2), – niższe koszty wdrożenia (4), – mniejsze koszty funkcjonowania, mały narzut stanowisk politycznych (3), – częściowe utrzymanie zaangażowania wszystkich dotychczasowych merytorycznych kadr (4), – większa zdolność do wykształcenia nowych kadr i dalszego rozwoju kompetencji (3), – wysoki poziom merytoryczności, wysoka jakość kadry (2), – mniejsza skala niezbędnych działań legislacyjnych (3), – większe zaufanie do modelu ze strony podmiotów zagranicznych (4),	– wymóg poważnego ilościowo dopełnienia niezbędnych merytorycznych kadr (3), – mała zdolność do adaptowalnego angażowania nowych podmiotów do współpracy (4), – niższa reputacja na starcie (3), – ograniczone zaufanie do modelu ze strony zewnętrznych podmiotów krajowych (3), – mniejsza rozpoznawalność międzynarodowa (4), – ograniczone prowadzenie kierunkowych badań i wdrażanie wyników prac badawczo-rozwojowych (3).

– większa skuteczność działania, w tym zdolność reagowania , większa praktyczna efektywność i jakość działania (1), – lepsza adoptowalność do nowych problemów, nowych wyzwań (3), – precyzyjny przydział odpowiedzialności (2), – duża sprawność procesu formalnego zadaniowania i raportowania (3), – ścieżka służbowa jako mechanizm sprawnej koordynacji (2), – większa sprawność współpracy zaangażowanych podmiotów (3), – lepsza praktyka wypełniania zobowiązań międzynarodowych (2).	
O szanse	**T zagrożenia**
– rozszerzony wachlarz działań (ścieżka służbowa),	– zmniejszone możliwości i skuteczność ubiegania się o środki zewnętrzne (unijne, natowskie, inne), – mała odporność na doraźne decyzje polityczne, – zanikanie dotychczasowych kontaktów z CSIRTami i analitykami z całego świata, – biurokracja, formalizm działania, nadmierna proceduralizacja, – mała odporność na skokowe zmniejszenie finansowania (np. kryzys finansów publicznych), – niedostateczny priorytet dla badań naukowych i prac analitycznych, – niechęć do współpracy grupy podmiotów ze służbami specjalnymi.

8.3 Wariant scentralizowany

POZYTYWY	NEGATYWY
S mocne strony	**W słabe strony**
– duże zaufanie do modelu od strony podmiotów zagranicznych (4), – duże zaufanie do modelu podmiotów krajowych (3), – duża skuteczność formalnego zadaniowania i	– niedostateczna gwarancja wysokiego poziomu bezpieczeństwa cyberprzestrzeni (niewykorzystanie dotychczasowych kadr, zgubienie reputacji, urzędniczy charakter) (1),

raportowania (3), – jednoznaczność odpowiedzialnośći (2), – ścieżka służbowa jako silny mechanizm koordynacji (2), – duża formalna sprawność współpracy podmiotów (3).	– długi czas wdrożenia (2), – duże koszty wdrożenia (4), – większe koszty funkcjonowania wynikające z nadbudowy politycznej i biurokratycznej (3), – duże ryzyko niewykorzystania potencjału dotychczasowych kadr merytorycznych (4), – wymóg budowy kadry praktycznie od początku (4), – model niesprzyjający wykształcaniu kadry i budowaniu nowych kompetencji (3), – słabsza merytoryczna jakość kadry (2), – niezbędna długa ścieżka legislacyjna (3), – mniejsza zdolność do zaangażowaniu dotychczas nieuczestniczących podmiotów (4), – mała reputacja na starcie (3), – mała rozpoznawalność międzynarodowa (4), – mała praktyczna efektywność i jakość działania (1), – mała adaptowalność do nowych problemów, nowych wyzwań (3), – słaba praktyka wypełniania zobowiązań międzynarodowych (2), – ograniczone prowadzenie kierunkowych badań i wdrażanie wyników prac badawczo-rozwojowych (3).
O szanse	**T zagrożenia**
– prawdopodobna gwarancja dużego budżetu,	– zmniejszone możliwości i skuteczność ubiegania się o środki zewnętrzne (unijne, natowskie, inne), – mała odporność na doraźne decyzje polityczne, – zanikanie dotychczasowych kontaktów w obszarze cyberbezpieczeństwa z podmiotami z całego świata, – biurokracja, formalizm działania, nadmierna proceduralizacja, – mała odporność na kryzys finansów publicznych, – niedostateczny priorytet badań naukowych, – słabsze przełożenie na zewnętrzne ośrodki decyzyjne w państwie (bo to agencja wykonawcza a nie służba specjalna), – ze względu na długi czas wytworzenia, poważne ryzyko niedomknięcia się realizacji wariantu scentralizowanego - przeciągającego się w czasie stanu

	budowania, – ze względu na długi czas wytworzenia, długi czas okna nietrwałości i okresu przejściowego, – prawdopodobne konflikty ambicjonalne i konflikty odnośnie zakresu kompetencji nowej agencji.

8.4 Mocne (S) i słabe (W) strony – zestawienie

Wariant			priorytet i opis	
I	II	III		
Osiągnięty poziom bezpieczeństwa				
S	S	W	1	poziom bezpieczeństwa cyberprzestrzeni
Wymiar czasowy				
S	S	W	2	czas wdrożenia
Wymiar kosztowy				
S	S	W	4	koszty wdrożenia
S	S	W	3	koszty funkcjonowania, polityczny overhead
Wymiar kadrowy				
S	S	W	4	utrzymanie zaangażowania dotychczasowych merytorycznych kadr
S	W	W	4	skala niezbędności dopełnienia ilościowego merytorycznych kadr
S	S	W	3	wykształcenia kadry, rozwój kompetencji
S	S	W	2	merytoryczność, jakość kadry
Wymiar prawny				
S	S	W	3	konieczność powołania nowych instytucji: ścieżka legislacyjna (w szczególności ustawa o agencji wykonawczej)
Wymiar reputacyjny				
S	W	W	4	na ile dany model jest w stanie zaangażować aktorów (w tym prywatnych),
S	W	W	3	reputacja na starcie
S	S	S	4	zaufanie do modelu za granicą
S	W	S	3	zaufanie do modelu w kraju
S	W	W	4	rozpoznawalność międzynarodowa
Wymiar operacyjny				
W	W	S	3	skuteczność formalnego zadaniowania i raportowania,
S	S	W	1	skuteczność działania (praktyczna efektywność i jakość działania), zdolność reagowania
S	S	W	3	adaptowalność do nowych problemów, nowych wyzwań
W	S	S	2	jednoznaczność odpowiedzialności
W	S	S	2	skuteczność koordynacji/jakość
W	S	S	3	sprawność współpracy podmiotów
S	S	W	2	praktyka wypełnienia zobowiązań międzynarodowych
Wymiar badawczy				
S	W	W	3	aspekt badawczo rozwojowy (w tym ubieganie się o środki)

8.5 Szanse (O) i zagrożenia (T) - zestawienie

Wariant			opis
I	II	III	
O	T	T	skuteczność ubiegania się o środki (unijne, natowskie, inne)
O	T	T	odporność na doraźne decyzje polityczne (istotność, prawdopodobieństwo wystąpienia)
--	T	T	zanikanie kontaktów
T	--	--	naruszenie trwałości rozwiązania (z punktu widzenia np. budżetu)
--	T	T	biurokracja, formalizm działania, nadmierna proceduralizacja
--	T	T	brak odporności na kryzys finansów Państwa
	T	T	niedostateczny priorytet badań
T	--	T	niedostateczne przełożenia na ośrodki decyzyjne
--	--	T	ryzyko niedomykania przedłużających się przedsięwzięć
--	--	T	czas okna nietrwałości -> zmniejszenie istniejącej zdolności
O	--	--	elastyczność w dostosowywaniu się do ewoluujących zagrożeń
--	--	O	gwarancja dużego budżetu
--	O	--	rozszerzony wachlarz działań
--	T	--	niechęć do współpracy
--	--	T	konflikty ambicjonalne i zakresu kompetencji

8.6 Podsumowanie wariantów

Z przeprowadzonej analizy SWOT wynika, że **wariant rozproszony zawiera najwięcej (18) cech uznanych za mocne strony**, z trzech porównywanych modeli. Wśród nich znajdują się dwie kluczowe (z priorytetem 1): wysoki poziom bezpieczeństwa cyberprzestrzeni (możliwy do osiągnięcia w krótkiej perspektywie czasowej) oraz większa skuteczność działania, w tym zdolność reagowania, większa praktyczna efektywność (m.in. najmniej obciążona biurokracją) i jakość działania. Wśród głównych zalet tego modelu można też wymienić stosunkowo krótki czas wdrożenia systemu ochrony cyberprzestrzeni, zapewnienie wysokiego poziomu merytoryki i jakości kadr, mniejsze koszty funkcjonowania, bez narzutu stanowisk politycznych, większa zdolność do wykształcenia nowych kadr i dalszego rozwoju kompetencji, mniejsza skala niezbędnych działań legislacyjnych (nie jest konieczne powoływanie nowych instytucji), wyższa reputacja na starcie (wariant zakłada kontynuację działań podmiotów dotychczas zaangażowanych mniej lub bardziej formalnie w ochronę cyberprzestrzeni), a tym samym większe zaufanie do modelu ze strony zewnętrznych podmiotów krajowych. W wariancie tym z pewnością można oczekiwać najlepszej adoptowalności do nowych problemów, nowych wyzwań ze względu na pozycję CSIRTu krajowego umieszczonego poza jakimkolwiek urzędem, co pozwoli na pełne wykorzystywanie kanałów operacyjnej współpracy z aktorami krajowymi i zagranicznymi, zarówno tych formalnych jak i nieformalnych, szybki proces podejmowania decyzji , a także

szybką ścieżkę prowadzenia i wykorzystywania badań i analiz. Również kwestia możliwości wykształcenia kadr i stałego rozwoju kompetencji jest mocną stroną tego wariantu. Stwarza to określone szanse dla powodzenia funkcjonowania sprawnego systemu ochrony cyberprzestrzeni, takie jak: większa elastyczność w dostosowywaniu się do ewoluujących zagrożeń czy większa merytoryka i stabilność działania ze względu na większą odporność na doraźne działania pozamerytoryczne (np. decyzje polityczne).

Wśród słabszych stron wariantu zdecentralizowanego można byłoby wymienić brak mechanizmu ścieżki służbowej między wybranymi, współpracującymi instytucjami w porównaniu z modelem, w którym większość ról w systemie jest realizowana w jednej instytucji, gdzie obowiązują struktury zależności służbowej. To może potencjalnie prowadzić do mniejszej sprawności współpracy odrębnych instytucji, mniejszej skuteczności formalnego zadaniowania i raportowania. Wyzwaniem może być też jednoznaczne zdefiniowanie zakresów odpowiedzialności poszczególnych instytucji. Zagrożeniem w tym wariancie może być słabsze przełożenie na zewnętrzne ośrodki decyzyjne w państwie czy też ryzyko, że istotne podmioty systemu, nawet przy trwałości budżetu państwa dedykowanego na cyberbezpieczeństwo, mogą zmienić swoje priorytety funkcjonowania np. zmiany sytuacji finansowej danej instytucji.

W wariancie pośrednim (15 cech uznanych za mocne strony), wiele zalet wygląda podobnie jak w wariancie rozproszonym (np. szansa na osiągnięcie wysokiego poziomu bezpieczeństwa cyberprzestrzeni, krótki czas wdrożenia wariantu, niższe koszty wdrożenia, mniejsza skala niezbędnych działań legislacyjnych niż w wariancie całkowicie scentralizowanym, dobra skuteczność działania, w tym zdolność reagowania, praktyczna efektywność i jakość działania, dobra adoptowalność do nowych problemów, nowych wyzwań, wysoki poziom merytoryczności i wysoka jakość kadry. W tym wariancie będzie możliwe ustanowienie bardziej precyzyjnego przydziału odpowiedzialności niż w wariancie rozproszonym. Jednak utrzymanie zaangażowania wszystkich dotychczasowych merytorycznych kadr będzie jednak trudniejsze niż w wariancie pierwszym.

Wśród słabszych stron tego wariantu można wymienić problem ograniczonego zaufania do modelu ze strony podmiotów krajowych, przede wszystkim prywatnych, ze względu na umieszczenie CSIRTu krajowego w służbach specjalnych. Prawdopodobnie dużym wyzwaniem byłoby dopełnienie ilościowe niezbędnych kadr merytorycznych (bariera zatrudnienia w służbach) a także zaangażowanie do współpracy nowych podmiotów. Prowadzenie kierunkowych badań i wdrażanie ich wyników także wydaje się słaba stroną wariantu, który opiera się głównie na administracji państwowej i służbach. Zagrożeniem w tym modelu jest też mniejsza odporność na doraźne decyzje polityczne, ryzyko stopniowego zanikania dotychczas zbudowanych kontaktów z CSIRTami i analitykami

z całego świata. Także większy formalizm działania i ryzyko nadmiernej proceduralizacji może powodować mniejszą skuteczność działania. Model ten jest także nieodporny na skokowe zmniejszenie finansowania (np. kryzys finansów publicznych).

Wariant scentralizowany wykazuje, według naszej oceny więcej negatywnych cech niż pozytywnych (pozytywnych zaledwie 6). Wśród mocnych stron można wymienić jedynie prawdopodobne zaufanie do modelu ze strony podmiotów krajowych i zagranicznych, łatwą implementację formalnej ścieżki zadaniowania, raportowania i koordynacji, a także możliwą do uzyskania, przynajmniej teoretycznie, jednoznaczność zdefiniowanych odpowiedzialności.

Jednak w modelu tym nie ma dostatecznych gwarancji osiągnięcia wysokiego poziomu bezpieczeństwa cyberprzestrzeni. Słabością będzie bowiem brak szansy na wykorzystanie większości dotychczasowych kadr (powstaje nowa instytucja, która będzie się zmagała z koniecznością zatrudnienia nowych pracowników, nie posiadających takiej wiedzy i doświadczenia jak kadry istniejących podmiotów, które biorą udział w działaniach na rzecz ochrony cyberprzestrzeni; tylko niewielka część tych doświadczonych kadr będzie skłonna przejść do nowej instytucji państwowej). Także długi czas wdrożenia wariantu (spowodowany koniecznością przygotowania odpowiedniej legislacji i zbudowania od zera nowej instytucji) stanowi słabszą stronę wariantu i powoduje poważne zagrożenia dla osiągnięcie końcowego sukcesu. Przeciągający się proces budowania NCC i merytorycznego potencjału instytucji mógłby spowodować nawet fiasko całego przedsięwzięcia, gdyby w trakcie budowy zaszła jakaś kryzysowa sytuacja w cyberprzestrzeni, która nie zostałaby sprawnie rozwiązana albo przekroczono by czas dostosowania krajowego systemu ochrony cyberprzestrzeni do pojawiających się regulacji UE (np. dyrektywa NIS). Centralna instytucja generowałaby także prawdopodobnie wyższe koszty funkcjonowania wynikające z nadbudowy politycznej i biurokratycznej.

Problem z kadrami merytorycznymi wystąpiłby także w aspekcie kształcenia i rozwoju kadry, a także jej utrzymania po osiągnięciu wyższego poziomu merytorycznego (konkurencja płacowa ze strony rynku komercyjnego). Ze względu na konieczne sztywne ramy funkcjonowania (ustawa, rozporządzenia) instytucję taką cechowałaby mała adaptowalność do nowych problemów, nowych wyzwań pojawiających się w obszarze bezpieczeństwa cyberprzestrzeni. W praktyce więc efektywność i jakość działania pozostawałaby w wielu przypadkach na niewystarczającym poziomie. Także aspekt badawczo wdrożeniowy, podobnie jak w wariancie pośrednim zszedłby w tym wariancie najprawdopodobniej na dalszy plan. Jeśli dołożymy do tego niewielką odporność scentralizowanego systemu na decyzje o charakterze politycznym, zanikanie, wypracowanych przez lata kontaktów i relacji na forach międzynarodowych (konieczność budowania tej sfery od początku – co zajęłoby wiele lat), prawdopodobne konflikty

ambicjonalne i konflikty odnośnie zakresu kompetencji nowej agencji i inne zagrożenia wymienione w tabelce analizy SWOT – widać, że wariant scentralizowany obarczony jest poważnymi słabościami.

Biorąc powyższe pod uwagę, autorzy niniejszego opracowania rekomendują wybór wariantu rozproszonego jako optymalnego dla zagwarantowania osiągnięcia pozytywnego przełomu w dziedzinie ochrony cyberprzestrzeni w stosunkowo krótkim czasie i gwarantującego stały rozwój oraz zwinne dostosowywanie się do dynamiki zagrożeń i problemów. Proponujemy więc podejście ewolucyjne, budujące nowy system ochrony cyberprzestrzeni w kraju na podwalinach istniejących, powszechnie uznanych i dysponujących odpowiednim doświadczeniem podmiotów.

9 Budowa relacji w dziedzinie cyberbezpieczeństwa z interesariuszami spoza administracji publicznej

Niezależnie od wyboru wariantu organizacji krajowego systemu bezpieczeństwa cyberprzestrzeni, koniecznym elementem, który powinien być opracowany i rozwijany jest aspekt współpracy administracji publicznej ze wszystkimi interesariuszami, którzy odgrywają istotną rolę w tej dziedzinie. Po pierwsze są to prywatne podmioty gospodarcze w różnych sektorach, po drugie są to użytkownicy usług oferowanych w cyberprzestrzeni – w istocie coraz większa część społeczeństwa. Oprócz tego istnieją organizacje zrzeszające przedsiębiorców, grupy społeczne, organizacje NGO oraz takie sektory jak: naukowy, akademicki, edukacji. Przyjęcie właściwego modelu współpracy i uczestnictwa tych podmiotów w procesie budowania krajowego systemu bezpieczeństwa cyberprzestrzeni odegra w przyszłości istotną rolę. Argumentem przemawiającym bowiem za położeniem dużego nacisku na współpracę rozciągającą się na wszystkie sektory jest fakt, że zdecydowana większość infrastruktury funkcjonującej w cyberprzestrzeni jest w rękach podmiotów prywatnych.

W sektorze przedsiębiorstw, jest istotne aby zauważyć, iż w istocie mamy do czynienia z wieloma typami podmiotów, różniącymi się miedzy sobą wielkością, typem prowadzonej działalności, a tym samym pojawiają się różne grupy zainteresowania oraz interesów w odniesieniu do cyberprzestrzeni i jej bezpieczeństwa

Konieczne jest więc uwzględnienie specyfiki różnych grup interesów, które są reprezentowane przez takie typy podmiotów jak:

- operatorzy telekomunikacyjni,
- dostawcy treści, media społecznościowe,
- dostawcy rozwiązań bezpieczeństwa,
- przedsiębiorcy, w tym:
  - będący częścią infrastruktury krytycznej,
  - nie będący jej częścią.

Jak wspomniano wyżej, wśród wyróżników, które wpływają na podejście do bezpieczeństwa teleinformatycznego podmiotów biznesowych, jest także ich wielkość czy skala prowadzonej działalności. Inaczej bowiem rzecz się ma w przypadku dużych firm, które posiadają rozbudowaną infrastrukturę IT i potencjał środków oraz kadrowy do wdrażania

standardów bezpieczeństwa, a inaczej sprawa wygląda w grupie małych i średnich przedsiębiorstw, które koncentrują się na swej głównej działalności, nie mając koniecznie odpowiedniej wiedzy i zasobów, żeby podążać za rekomendacjami co do bezpieczeństwa IT.

W związku z tym trudno sobie wyobrazić jeden zunifikowany model partnerstwa administracji publicznej ze wszystkimi innymi interesariuszami ze sfery biznesowej.

Poniżej przedstawiono próbę scharakteryzowania uwarunkowań, które powinny być wzięte pod uwagę przy konstruowaniu optymalnego modelu relacji w ramach szeroko pojętej współpracy w dziedzinie cyberbezpieczeństwa – w podziale na typy podmiotów wymienione wyżej.

9.1 Przedsiębiorcy

9.1.1 Operatorzy telekomunikacyjni

W sektorze telekomunikacyjnym, jak to zostało przedstawione w rozdziale 3.1.3, obecnie istnieje prawo, które nakłada określone obowiązki w dziedzinie bezpieczeństwa teleinformatycznego, takie jak spełnienie wymogu wdrożenia minimalnych środków bezpieczeństwa przez operatorów czy też raportowania o istotnych naruszeniach. Aby w praktyce przynosiły one wyraźne korzyści, potrzebne jest przeanalizowanie skuteczności ich funkcjonowania i prawdopodobnie wprowadzenie odpowiednich zmian i usprawnień. Istnieją podmioty krajowe (operatorzy, CERTy) i europejskie (ENISA), które są w stanie wspomóc proces dochodzenia do optymalnego stanu implementacji prawa telekomunikacyjnego i praktyki w jego stosowaniu w odniesieniu do bezpieczeństwa teleinformatycznego. Nie powinno to więc stanowić większego problemu.

Nie wystarczy jednak ustanowić dobrej ramy regulacyjnej, aby doprowadzić do przełomu w procesie podnoszenia bezpieczeństwa cyberprzestrzeni. Oprócz precyzyjnych przepisów, które powinny uwzględniać dodatkowe aspekty, takie jak wielkość danego operatora i tym samym jego potencjał w dziedzinie bezpieczeństwa IT, system współpracy powinien zakładać istnienie określonych korzyści i zachęt dla przedsiębiorców, aby koncentrowali się na realizacji wymogów w praktyce, a nie – jak to często bywa – starali się wypełniać obowiązki jedynie formalnie bądź szukali korzystnych interpretacji prawnych w celu uniknięcia nadmiernych, w ich ocenie, obowiązków.

W przypadku operatorów, w pierwszym rzędzie należy skoncentrować się na kluczowych podmiotach świadczących usługi dla przedsiębiorstw infrastruktury krytycznej. Tacy operatorzy mają z reguły duże doświadczenie w dziedzinie cyberbezpieczeństwa. Zaproszenie takich podmiotów do współpracy przy wypracowywaniu optymalnych zasad stosowania prawa telekomunikacyjnego, aby uzyskać wartość dodaną z istnienia artykułów

definiujących kwestie bezpieczeństwa teleinformatycznego (np. zaproszenie do Zespołu Zadaniowego poświęconego tej tematyce) może w krótkim czasie dać pożądany efekt w postaci uwzględnienia praktycznej wiedzy co do funkcjonowania na rynku w tym obszarze. Oczywiście należy także uwzględnić interesy mniejszych przedsiębiorców, tak aby przyjęte zasady nie były dla nich za trudne do spełnienia. W tym przypadku można wykorzystać współpracę z izbami telekomunikacyjnymi, w których takie podmioty są zrzeszone (np. PIKE). Z drugiej strony warto oprzeć się też na rekomendacjach ciał międzynarodowych – np. BEREC czy ENISA.

Szczególnie w przypadku mniejszych przedsiębiorców telekomunikacyjnych, rolą administracji rządowej powinno być nie tyle narzucanie sztywnych obowiązków, co niesienie pomocy w postaci np. przeprowadzania szkoleń, proponowania udziału w przedsięwzięciach organizowanych przez centra typu ISAC lub CSIRTy sektorowe, próbnych audytów, które nie służyłyby nakładaniu kar a wskazywały sposoby radzenia sobie z problemami bezpieczeństwa.

9.1.2 Dostawcy treści, media społecznościowe

W przypadku sektora dostawców usług obejmującego: portale informacyjne, sieci społecznościowe, sklepy internetowe, platformy aukcyjne, platformy usług chmurowych i inne, obecnie nie ma wystarczających rozwiązań prawnych, które tak jak w sektorze telekomunikacyjnym regulowałyby kwestie obowiązków spełniania minimalnych standardów bezpieczeństwa IT, raportowania w związku z pojawiającymi się istotnymi incydentami czy współpracy z organami ścigania w ściganiu cyberprzestępców.

Stanowi to poważną lukę w systemie krajowego (ale także międzynarodowego) bezpieczeństwa cyberprzestrzeni, także rekomenduje się, aby poważnie rozważyć możliwość ustanowienia odpowiednich ram prawnych. Podobnie jak to postulowano w przypadku przedsiębiorców telekomunikacyjnych, nie należy przykładać równej miary do wszystkich podmiotów niezależnie do ich wielkości, rodzaju i skali prowadzonej działalności – należy raczej skoncentrować się w pierwszym rzędzie na obszarach, w których występuje najwięcej zagrożeń i mogą powodować najpoważniejsze skutki (np. duże platformy handlu elektronicznego).

Oczywiście nieco inna, lepsza sytuacja jest w odniesieniu do ochrony danych osobowych, poprzez funkcjonowanie odpowiedniej ustawy i organu kontrolnego (GIODO) – w praktyce niezależnie od tego w jakim sektorze przedsiębiorstwo prowadzi działalność.

Dyskusja na temat włączenia lub pominięcia sektora umownie zwanego dostawcami usług internetowych jest prowadzona także w ramach projektu dyrektywy NIS. Autorzy niniejszego dokumentu wyrażają jednak pogląd, że mówiąc o bezpieczeństwie

cyberprzestrzeni nie można pozostawić poza systemem jej ochrony, olbrzymiej grupy przedsiębiorców, których model biznesowy opiera się stricte na funkcjonowaniu Internetu.

9.1.3 Dostawcy rozwiązań bezpieczeństwa

Zupełnie inne interesy w kontekście udziału w ochronie cyberprzestrzeni mają dostawcy rozwiązań bezpieczeństwa. Z jednej strony są zainteresowani jak największym nasyceniem rynku swoimi produktami, wspierającym proces podnoszenia bezpieczeństwa cyberprzestrzeni. Wdrażanie rozwiązań zabezpieczających nie tylko dostarcza narzędzi technicznych, ale wspiera proces podnoszenia świadomości użytkowników cyberprzestrzeni na temat zagrożeń i metod przeciwdziałania (szkolenia, eksploatacja systemów bezpieczeństwa). Z drugiej strony, przynajmniej niektórzy z dostawców, szczególnie duże podmioty, mogą być zainteresowani ściślejszą współpracą z rządem – najchętniej w procesie wymiany informacji na temat zagrożeń faktycznie zauważonych i rozpoznanych przez użytkowników sieci oraz, CSIRTy sektorowe, CSIRT krajowy – w danym obszarze czy sektorze.

Rekomenduje się, aby zaprosić do współpracy najbardziej zaawansowanych i zainteresowanych dostawców w celu wypracowania modelu współpracy i wymiany informacji korzystnego dla obu stron. Formuła powinna się rozszerzać na kolejne podmioty w miarę upływu czasu i budowania zaufania we wzajemnej współpracy. Może się to odbywać w ramach Zespołów Zadaniowych powoływanych przez Koordynatora lub poprzez zaproszenia do współpracy z Zespołem Łącznikowym.

9.1.4 Przedsiębiorcy będący częścią infrastruktury krytycznej

Obecnie w ramach realizacji Narodowego Programu Ochrony Infrastruktury Krytycznej, który został opracowany przez Rządowe Centrum Bezpieczeństwa w związku z ustawą o zarządzaniu kryzysowym, przedsiębiorcy w sektorach uznanych za krytyczne są objęci określonymi działaniami wynikającymi z programu. Jak wynika z NPOIK znaczna część operatorów infrastruktury krytycznej pochodzi z sektora prywatnego.

Wśród sektorów wymienionych w programie jako krytyczne, dwa są bezpośrednio związane z technologiami IT. Jest to sektor sieci teleinformatycznych oraz sektor łączności. Pozostałe sektory, takie jak: energetyczny, paliwowy, finansowy, transportowy, zaopatrzenia w wodę i inne, w mniejszym lub większym stopniu zależą od infrastruktury IT i w tym sensie także muszą być traktowane jako element systemu chroniącego cyberprzestrzeń. Systemy IT, które teoretycznie nie mają styku z Internetem, także powinny być traktowane jako część cyberprzestrzeni, gdyż fakt, czy jakiś system IT ma z definicji połączenie z sieciami publicznie dostępnymi czy nie - nie powinien determinować, czy jest on częścią systemu ochrony cyberprzestrzeni. Można wskazać bowiem szereg przykładów incydentów, w których

szkodliwe programy przedostały się do sieci wydzielonych np. poprzez nośniki pamięci USB. Najbardziej spektakularnym przypadkiem tego typu był robak Stuxnet.[86]

Ze względu na fakt, iż w NPOIK kwestie ochrony infrastruktury teleinformatycznej czy cyberprzestrzeni nie są głównym tematem, istnieje przestrzeń do dalszego rozwinięcia tego zagadnienia, koordynacji działań oraz współpracy w tym obszarze pomiędzy Rządowym Centrum Bezpieczeństwa a jednostką koordynującą tematykę ochrony cyberprzestrzeni w kraju. Niektóre z wypracowanych przez RCB aspektów podejścia do ochrony infrastruktury krytycznej mogą zostać wykorzystane przy konstruowaniu systemu ochrony cyberprzestrzeni – jednak należy uwzględnić, że teleinformatyczna infrastruktura krytyczna może wymagać nieco innego podejścia, chociażby w kwestiach szacowania i zarządzania ryzykiem.

9.1.5 Przedsiębiorcy nie będący częścią infrastruktury krytycznej

Przedsiębiorcy nie będący częścią infrastruktury krytycznej, w zależności od wielkości, stopnia wykorzystania infrastruktury teleinformatycznej powinni być beneficjentami skoordynowanego podejścia do ochrony cyberprzestrzeni w kraju. System krajowy powinien zawierać skuteczne sposoby zwiększania świadomości przedsiębiorców o konieczności wdrażania organizacyjnych i technicznych środków bezpieczeństwa IT poprzez kampanie, konferencje, cykle szkoleń czy schematy certyfikacji popierane przez administrację. Koordynator systemu ochrony cyberprzestrzeni powinien także wspierać powstawanie branżowych czy sektorowych inicjatyw typu ISAC, w ramach których wypracowywane byłyby odpowiednie praktyki bezpiecznego korzystania z infrastruktury teleinformatycznej z uwzględnieniem specyfiki danej grupy, a także generowane byłyby sygnały zwrotne na temat rzeczywistych problemów przy wdrażaniu zaleceń bezpieczeństwa cyberprzestrzeni.

9.2 Sektor naukowy, akademicki oraz edukacja

Sektor naukowy i akademicki pełni w wielu krajach kluczową rolę w kształtowaniu potencjału danego państwa w dziedzinie nowoczesnych technologii informacyjnych, w tym bezpieczeństwa cyberprzestrzeni. Zadaniem państwa jest stworzenie takiego modelu funkcjonowania systemu badań naukowych, edukacji akademickiej, ale także edukacji szkolnej, aby maksymalnie wykorzystać potencjał intelektualny Polaków, którzy w wielu międzynarodowych konkursach informatycznych czy wyzwaniach typu *„capture the flag”* zajmują czołowe miejsca. Chodzi natomiast o to, by kształcić coraz więcej ekspertów w tej przyszłościowej dziedzinie, a następnie wykorzystywać ich potencjał w kraju zarówno w obszarze badań naukowych jak również wdrażania rozwiązań komercyjnych.

[86] https://en.wikipedia.org/wiki/Stuxnet

W obszarze bezpieczeństwa cyberprzestrzeni należy prowadzić ciągłe badania na rzecz aktualizacji wiedzy na temat zagrożeń oraz nowych metod im przeciwdziałania. Państwo powinno wspierać także badania prowadzące do powstawania narzędzi (**w tym narzędzi narodowych w obszarach, które zostaną uznane za kluczowe**) umożliwiających zaawansowane monitorowanie zagrożeń i skuteczna reakcję. Szczególne znaczenie ma to dla sektora infrastruktury krytycznej oraz sektora administracji publicznej.

Wspólnie z Ministerstwem Nauki i Szkolnictwa Wyższego, Narodowym Centrum Badań i Rozwoju oraz Ministerstwem Edukacji, Koordynator powinien móc wypracować odpowiednie warunki i ramy dla realizacji kilkuletnich programów krajowych w dziedzinie badań oraz edukacji na temat bezpieczeństwa cyberprzestrzeni. Działania te wymagają istotnego zaangażowania finansowego państwa.

Należy zwrócić uwagę, że **projekty badawcze, które kończą się sukcesem w postaci powstania konkretnych systemów czy narzędzi, których przydatność została zweryfikowana w praktyce, powinny uzyskać szczególne warunki dla dalszego rozwoju i wdrażania w środowisku rzeczywistym.**

Dziedzina teleinformatyki i w szczególności cyberzpieczeństwo powinno być jednym z kluczowych obszarów kierunkowych strategii badawczych w Polsce, ze względu na wspomniany potencjał intelektualny i zdolności w tej dziedzinie obywateli naszego kraju, a także ze względu na relatywnie niski „próg wejścia", rozumiany jako konieczny do poniesienia wkład inwestycyjny, aby móc rozpocząć zaawansowane badania. W obecnym świecie sama cyberprzestrzeń jest doskonałym laboratorium badawczym, wyposażonym w cały wachlarz narzędzi np. programistycznych czy wirtualnych przestrzeni obliczeniowych. Nie znaczy to oczywiście, że żadne inwestycje nie są potrzebne przed rozpoczęciem badań. Jednak skonstruowanie dedykowanego laboratorium badawczego dla rozpoczęcia badań w dziedzinie cyberbezpieczeństwa nie musi być procesem długotrwałym i nadmiernie kosztownym z punktu widzenia budżetu państwa, natomiast efekty jakie są do osiągnięcia mogą zbudować przewagę nawet nad krajami, które są dziś zaawansowane w tej dziedzinie.

Tymczasem w naszym kraju dziedzina teleinformatyki i bezpieczeństwa IT w ogóle nie jest traktowana priorytetowo. Wniosek taki wypływa z lektury dokumentu „*Krajowa inteligentna specjalizacja (KIS)"*[87], który został przyjęty w kwietniu 2014 r. przez Radę Ministrów w ramach Programu Rozwoju Przedsiębiorstw. Dokument KIS przedstawia proces wyłaniania obszarów B+R+I na poziomie krajowym, które stają się priorytetami polityki naukowej i innowacyjnej do roku 2020 oraz ma zasadniczy wpływ na dostępność finansowania środkami programów operacyjnych istotnych dla państwa przedsięwzięć.

[87]http://www.mg.gov.pl/Wspieranie+przedsiebiorczosci/Polityki+przedsiebiorczosci+i+innowacyjnosci/Krajowa+inteligentna+specjalizacja

Niestety w obecnej wersji KIS, technologie informacyjne występują w bardzo ograniczonym wymiarze, a kwestie bezpieczeństwa cyberprzestrzeni zostały właściwie całkowicie pominięte.

Rekomenduje się, aby zaktualizować wykaz krajowych inteligentnych specjalizacji (KIS), tak aby w większym stopniu uwzględniał on nowoczesne technologie informacyjne oraz dziedzinę badań na rzecz bezpieczeństwa cyberprzestrzeni, ponieważ specjalizacje te kształtują priorytety polskiej polityki naukowej i innowacyjnej.

9.3 Współpraca z organizacjami pozarządowymi oraz izbami branżowymi

Współpraca taka, wyrażająca się między innymi przeprowadzaniem konsultacji dokumentów programowych czy ustaw w obszarze cyberbezpieczeństwa czy też zapraszaniem ekspertów do pracy w zespołach zadaniowych - obecnie istnieje. Należy jednak wystrzegać się współpracy pozornej, która może powodować negatywne skutki w przyszłości. Jeśli przykładowo organ rządowy publikuje nowy dokument programowy do konsultacji i czas konsultacji jest stanowczo zbyt krótki lub zgłoszone uwagi i tak nie są uwzględniane w kolejnej wersji dokumentu, lub też praca zespołu zadaniowego nie kończy się konkretnym efektem, to może być to zniechęcać organizacje pozarządowe czy izby branżowe do jakiejkolwiek dalszej współpracy.

Administracja rządowa powinna postawić sobie zadanie konstruowania systemu, który będzie zachęcał do współpracy partnerów z izb branżowych czy organizacji pozarządowych.

9.4 Partnerstwo publiczno prywatne a system zachęt do współpracy

W wielu opracowaniach na temat współpracy interesariuszy systemu bezpieczeństwa cyberprzestrzeni pada określenie partnerstwa publiczno prywatnego, szczególnie w odniesieniu do współpracy w obszarze infrastruktury krytycznej.[88] Jest to aspekt rozważany zarówno na poziomie strategii cyberbezpieczeństwa większości krajów, a także ma wymiar praktyczny w codziennym funkcjonowaniu krajowego systemu bezpieczeństwa cyberprzestrzeni, gdzie większość infrastruktury podlegająca ochronie znajduje się w rekach podmiotów prywatnych. Stąd konieczność przyjęcia przez administrację rządową takiego

[88] Por. opracowania ENISA: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership

podejścia, które będzie pozwalało na skuteczne włączenie sektora prywatnego w cały system, który powinien opierać się na regulacjach, rozwiązaniach samoregulacyjnych oraz – co nie bez znaczenia – na systemie zachęt do współpracy dla rozmaitych podmiotów spoza administracji publicznej.

Rolą Koordynatora jest tworzenie i czuwanie nad właściwym funkcjonowaniem rozwiązań regulacyjnych w dziedzinie cyberbezpieczeństwa. Jednak warte podkreślenia jest to, że tworzenie przepisów dla tak skomplikowanego i dynamicznie rozwijającego się obszaru jak technologie informacyjne i sama gospodarka opierająca się na tych rozwiązaniach, jest relatywnie trudne i narażone na pozostawanie z tyłu za nowo pojawiającymi się zjawiskami.

Dlatego też pewna rola powinna być niejako pozostawiona dla rozwiązań samoregulacyjnych, szczególnie jeśli dotyczy to wypracowywania dobrych praktyk czy standardów bezpieczeństwa charakterystycznych dla danego sektora (np. energetycznego, ruchu powietrznego, finansowego). Tu istotną rolę mogą odgrywać centra typu ISAC opisywane wcześniej, które gromadziłyby podmioty i ich ekspertów w celu uzgadniania podejścia do bezpieczeństwa cyberprzestrzeni dla danego sektora (z tym, że nie byłaby to oczywiście jedyna rola ISAC). Rolą administracji rządowej (Koordynatora) byłoby zatem wspieranie powstawanie centrów ISAC i współpraca z nimi w celu skoordynowania działań na poziomie strategicznym.

9.5 System zachęt

Aby system współpracy mógł rzeczywiście funkcjonować, należy oprócz stworzenia ram formalno prawnych związanych z określeniem ról, odpowiedzialności (organizacyjnych czy finansowych) zastanowić się nad skonstruowaniem systemu zachęt do współpracy, które będą mogły wspierać wspomniane ramy.

Kwestia zachęt jest prawdopodobnie jednym z najtrudniejszych aspektów do opracowania i wdrożenia przy konstruowaniu systemu ochrony cyberprzestrzeni. Rodzaj zachęty, który jako pierwszy jest z tym kojarzony – czyli wsparcie finansowe lub zastosowanie ulg podatkowych itp. jest zarazem często najtrudniejszy do wdrożenia, ze względu na ograniczenia budżetui państwa. W opinii autorów niniejszego dokumentu, nie da się uniknąć stosowania tego typu zachęt - bezpieczeństwo cyberprzestrzeni po prostu kosztuje, a z drugiej strony zapobiega potencjalnym stratom, jeśli zmaterializuje się ryzyko cyberzagrożeń.

Niejako równolegle, rekomenduje się, aby opracować katalog zachęt pozafinansowych, które ułatwiałyby współpracę podmiotów z różnych sektorów. Poniżej przedstawiono kilka przemyśleń, które warto wziąć pod uwagę.

9.5.1 Przekazywanie informacji na temat zagrożeń i incydentów

Powszechnie występującym problemem jest niechęć podmiotów gospodarczych - ale można to rozciągnąć na wszystkie podmioty działające w cyberprzestrzeni - do dzielenia się informacją na temat zauważonych zagrożeń, incydentów, które miały miejsce oraz szacowanych strat. Brak tego typu informacji jest poważnym problemem zarówno ze względów operacyjnych, jak również statystycznych czy strategicznych. W wielu krajach coraz częściej rozważa się wprowadzenie obowiązku zgłaszania incydentów czy raportowania zbiorczego. Jednak warto jest równolegle przemyśleć stworzenie mechanizmów, które będą sprzyjały wymianie informacji na temat zagrożeń i incydentów. Przykładowo, można zastosować system, w którym dane przekazywane do podmiotów uprawnionych są odpowiednio anonimizowane, tak aby np. nazwa instytucji pozostawała nieznana lub zakodowana. Przykładowo, jeśli chcemy mieć obraz sytuacji w sektorze bankowym, nie musimy wymagać, aby wszystkie banki raportowały o swych incydentach do np. CSIRTu krajowego (co jest w praktyce mało realne). Można by skorzystać z sektorowego „pośrednika" w postaci np. Związku Banków Polskich lub innej instytucji, która ma zaufanie sektora, aby informacje o poważnych naruszeniach były przekazywane do instytucji krajowych w postaci odpowiednio zanonimizowanej (na wcześniej ustalonych zasadach).

Biorąc pod uwagę, że informacje o incydentach zawsze są informacjami wrażliwymi, zaletą dla przekazujących takie informacje byłby fakt poddania się pośredniczącej w wymianie instytucji procedurze gwarantującej bezpieczeństwo danych. Potrzebne by było stworzenie przejrzystych zasad, zaakceptowanych przez interesariuszy oraz zastosowanie wysokich standardów techniczno-organizacyjnych dla ochrony zbieranych informacji.

9.5.2 Dzielenie się informacją przez administrację publiczną

Jak to było wcześniej wspomniane, wiele podmiotów, które zajmują się wdrażaniem rozwiązań bezpieczeństwa czy też prowadzą zaawansowane badania w dziedzinie bezpieczeństwa w cyberprzestrzeni jest zainteresowanych otrzymywaniem faktycznych danych (ilościowych, merytorycznych) na temat pojawiających się zagrożeń czy typów zaistniałych incydentów w danym sektorze. Przy czym nie chodzi tu o dane ujawniające nazwy użytkowników czy podmiotów, a informacje, które pozwalałyby podmiotom współpracującym na pogłębienie własnych analiz informacjami o faktycznej skali danego incydentu. Oczywiście wiele informacji jest na tyle wrażliwych, że nie powinny być one publikowane w przestrzeni publicznej. Jednak można rozważyć stworzenie określonego systemu partnerstwa, w którym takie podmioty jak Koordynator czy krajowy CSIRT, mógłby przekazywać niektóre informacje podmiotom prywatnym lub społecznym, które uzyskałyby odpowiedni poziom zaufania. Dla tych podmiotów byłaby to korzyść praktyczna w postaci

otrzymywania ekskluzywnych informacji, a także korzyść wizerunkowa - znalezienia się w grupie partnerów administracji. Z kolei administracja państwowa mogłaby postawić określone warunki wejściowe (spełnienie wymogów, które pozwolą na obdarzenie danego podmiotu odpowiednim zaufaniem) oraz zastrzec obowiązek realnego wkładu do systemu ochrony cyberprzestrzeni, np. w postaci wymogu zaoferowania określonej liczby darmowych szkoleń czy audytów bezpieczeństwa dla samej administracji publicznej bądź np. przedsiębiorstw sektora MŚP.

9.6 Ćwiczenia

Ważnym elementem systemu bezpieczeństwa cyberprzestrzeni RP powinny być ćwiczenia pozwalające na sprawdzenie skuteczności jego działania, a także współpracy z systemami funkcjonującymi w innych krajach oraz międzynarodowymi.

Na poziomie ogólnokrajowym rekomendujemy organizację nie rzadziej niż raz na dwa lata kompleksowych ćwiczeń symulujących ogólnokrajowy incydent. Ćwiczenia te powinny być organizowane w trybie „full-scale exercise", to znaczy z wykorzystaniem rzeczywistego personelu i narzędzi oraz istniejących procedur. Powinny one uwzględniać zarówno aspekty techniczne, jak i operacyjne oraz strategiczne. W naturalny sposób powinny być w nie włączone podmioty realizujące role Koordynatora, CSIRTu rządowego, CSIRTu krajowego i Centrum Analitycznego, CSIRT-IK, Zespół Łącznikowy (ewentualnie: Zespoły Zadaniowe), a także Rada Koordynacyjna. W zależności od scenariusza, powinny być także uwzględniane inne podmioty, w szczególności CSIRTy sektorowe. Ćwiczenia mogą być prowadzone etapami, przy czym ich harmonogram powinien być planowany z około rocznym wyprzedzeniem, aby wszyscy uczestnicy mogli zaplanować udział. Podmiotem odpowiedzialnym za organizację ćwiczeń powinien być Koordynator (w tym poprzez powołanie stosownego Zespołu Zadaniowego), a ich wynikiem powinien być raport przedstawiany Radzie Koordynacyjnej zawierający wnioski na temat poziomu spełnienia oczekiwań, a także propozycje usprawnień systemu w warstwie organizacyjnej i prawnej. Możliwe jest również organizowanie serii mniejszych ćwiczeń z jasno sprecyzowanym celem.

Należy także stworzyć system zachęt dla poszczególnych sektorów do organizowania ćwiczeń w zakresie współpracy pomiędzy instytucjami z danego sektora. Ćwiczenia takie mogą mieć mniejszą skalę (także w formule Table Top Exercise), a ich podstawowym celem powinna być weryfikacja własnych kompetencji poszczególnych instytucji w zakresie bezpieczeństwa cyberprzestrzeni oraz możliwości bieżącej wymiany informacji i współpracy operacyjnej wewnątrz sektora na wypadek zagrożenia. Naturalnym podmiotem odpowiedzialnym za organizację takich ćwiczeń byłby CSIRT sektorowy, a w razie jego braku regulator lub inny organ sprawujący nadzór nad danym obszarem. Co istotne, wyniki ćwiczeń

powinny być przekazywane Koordynatorowi, który powinien wykorzystywać je w analizie, rekomendacjach oraz przy planowaniu ćwiczeń ogólnokrajowych. Należy jednocześnie wyraźnie podkreślić, że celem raportu nie może być wykazywanie słabych stron któregokolwiek z uczestników – powinien on służyć obserwacjom na poziomie systemowym (np. w jakim obszarze powinny być stosowane nowe zachęty, dodatkowe finansowanie, wsparcie strukturalne itp.). Ćwiczenia na poziomie sektorowym były do tej pory kilkukrotnie organizowane przez podmioty prywatne.

W zakresie współpracy międzynarodowej Polska powinna aktywnie włączać się w ćwiczenia prowadzone zarówno przez organizacje narodów jak i sieci CSIRTów. Wiele ćwiczeń i warsztatów organizuje ENISA, w szczególności:

- Cyber Europe[89] – ćwiczenia paneuropejskie w pełnej skali, oparte na scenariuszu sytuacji kryzysowej,
- warsztaty ENISA/EC3 organizowane wspólnie z Europolem dotyczące współpracy CSIRTów i organów ścigania,
- CERTs in Europe – techniczne warsztaty dla Krajowych i Rządowych zespołów CSIRT,
- National Cyber Security Strategies Workshop.

Inne warsztaty i ćwiczenia w zakresie cyberbezpieczeństwa są organizowane regularnie lub doraźnie przez takie organizacje jak TERENA TF-CSIRT, FIRST, CERT/CC (Workshop for CSIRTs with National Capability).

Podmiotem odpowiedzialnym za reprezentowanie Polski w ćwiczeniach międzynarodowych powinien być Koordynator w przypadku ćwiczeń o charakterze strategicznym, oraz CSIRT Krajowy dla ćwiczeń operacyjnych i technicznych.

W dziedzinie cyberobronności najważniejszymi ćwiczeniami międzynarodowymi są:

- Locked Shields - organizowane przez NATO Cooperative Cyber Defence Centre of Excelence ćwiczenia techniczne o zakresie przede wszystkim europejskim,
- Cyber Coalition – ćwiczenia na poziomie strategicznym i technicznym, dedykowane przede wszystkim wymianie informacji i koordynacji międzynarodowej.

Oba typy ćwiczeń organizowane są raz w roku, a Polska jest ich aktywnym uczestnikiem. Podmiotami odpowiedzialnymi za reprezentację kraju jest Ministerstwo Obrony Narodowej (MIL-CERT) dla Locked Shields oraz ABW (CERT.GOV.PL) dla Cyber Coalition.

Należy przy powyższym mieć też na uwadze liczne głosy w środowisku CSIRT, które twierdzą, że nawet obecnie ćwiczeń jest za wiele, i działania te stoją na przeszkodzie prowadzeniem codziennej pracy zespołów. W związku z tym zaangażowanie poszczególnych

[89] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe

podmiotów w konkretne ćwiczenia powinno być w zakresie i na poziomie odpowiednim do realizmu ćwiczenia i związku danego podmiotu z jego scenariuszem. Ćwiczenia ogólnokrajowe powinny być przy tym bezwzględnym priorytetem.

10 Szacowanie kosztów

Podanie na tym etapie kosztów związanych z wdrożeniem, utrzymaniem i rozwojem systemu ochrony cyberprzestrzeni RP nie jest możliwe. Niemniej jednak, w ramach niniejszego opracowania podjęto próbę wykonania pierwszego kroku w procesie szacowania budżetu poprzez wprowadzenie kategorii kosztów, które powinny zostać uwzględnione. Dodatkowo oszacowano łączną liczbę etatów merytorycznych, pozwalających na funkcjonowanie na optymalnym poziomie CSIRTu krajowego oraz rządowego, instytucji Koordynatora oraz Centrum Analitycznego, co łącznie stanowi trzon warstwy operacyjnej krajowego systemu cyberbezpieczeństwa, proponowanego w ramach ekspertyzy, Wszystkie szacunki powstały w oparciu o doświadczenia NASK, w szczególności CERT Polska.

10.1 Kategorie kosztów

W nawiązaniu do schematów obrazujących w różnych wariantach konieczne elementy krajowego systemu cyberbezpieczeństwa, aby zdefiniować kategorie kosztów, można je zgrubnie podzielić na te, które są wymagane dla wdrożenia i utrzymania kluczowych systemów proponowanych w niniejszym opracowaniu: platformy wymiany informacji oraz systemu wczesnego ostrzegania, oraz na grupę kosztów związanych z funkcjonowaniem kluczowych podmiotów, takich jak: Koordynator, CSIRT krajowy, CSIRT rządowy, Centrum Analityczne oraz Zespół Łącznikowy. Funkcjonowanie pozostałych podmiotów, takich jak CSIRTy sektorowe czy centra ISAC według autorów ekspertyzy powinno być finansowane przez zainteresowanych przedsiębiorców w danych sektorach, a rząd mógłby jedynie finansować działania wspierające powstawanie takich podmiotów. Z kolei Zespoły Zadaniowe teoretycznie mogłyby funkcjonować bez finansowania ze strony administracji państwowej, jednak w celu osiągnięcia praktycznych wyników pracy takich zespołów proponuje się, aby uwzględnić w budżecie Koordynatora - przynajmniej w stosunku do najważniejszych Zespołów - finansowanie przez rząd ich powstania oraz działania.

Przy powyższych założeniach, proponuje się wprowadzić w procesie szacowania kosztów następujące ich kategorie:

W grupie kluczowych systemów informatycznych wspomagających funkcjonowanie krajowego systemu cyberbezpieczeństwa:

Platforma wymiany informacji:

Platformę tę należy rozumieć jako określoną liczbę systemów informatycznych wraz z ich użytkownikami i administratorami. Celem głównym jest wymiana informacji. Każdy system będzie dysponował innym charakterem informacji. Z naszego doświadczenia wynika, że integracja tych systemów w jedno rozwiązanie będzie trudna do osiągnięcia i w gruncie rzeczy niepotrzebna, niemniej jednak łącznie systemy te będą mogły tworzyć platformę umożliwiającą jednostkom odpowiedzialnym za ochronę cyberprzestrzeni współpracę i wymianę informacji o różnym charakterze.

Nakłady jednorazowe:

- analiza wymagań i opracowanie specyfikacji rozwiązań (w ścisłej współpracy z interesariuszami),
- rozwój systemów (w tym prace programistyczne) w obszarach w których zidentyfikowano braki w istniejących rozwiązaniach (w ścisłej współpracy z interesariuszami),
- koszt wdrożenia systemów do wymiany informacji (zakup sprzętu, licencji oprogramowania, praca zespołu wdrażającego),
- koszt szkoleń administratorów i głównych użytkowników (może być częścią kosztu wdrożenia),
- ewentualny koszt integracji niektórych systemów (w zależności od tego, czy jest to możliwe i potrzebne - w tym prace programistyczne, testowanie, szkolenia),
- koszt wdrożenia kolejnych systemów mających stanowić elementy platformy (o których konieczności powstania decydować będzie Koordynator).

Koszty okresowe (utrzymania):

- koszt utrzymania infrastruktury systemu (energia elektryczna, powierzchnia w serwerowni, klimatyzacja, dostęp do sieci Internet, itp.),
- koszt wsparcia/serwisu w okresie amortyzacji systemu,
- koszt administrowania systemem (w danym okresie),
- koszt okresowego przeglądu potrzeb w zakresie funkcjonalności platformy,
- koszt rozwoju systemu (oprócz kosztu wdrażania kolejnych elementów platformy, konieczne jest rozwijanie funkcjonalności samej platformy wymiany informacji).

System wczesnego ostrzegania:

Proponowane jest wdrożenie drugiej generacji systemu ARAKIS.GOV z powodzeniem funkcjonującego w administracji rządowej od kilku lat.

Nakłady jednorazowe:

- koszt wdrożenia systemu informatycznego (zakup sprzętu, praca zespołu wdrożeniowego),
- koszt szkoleń administratorów i głównych użytkowników (może być częścią kosztu wdrożenia).

Koszty okresowe (utrzymania):

- koszt utrzymania infrastruktury systemu (energia elektryczna, powierzchnia, klimatyzacja, dostęp do sieci Internet itp.),
- koszt wsparcia/serwisu w okresie amortyzacji systemu, koszt administrowania systemem (w danym okresie).

Koszt rozwoju systemu – koszty dodawania nowych funkcjonalności, w tym wynikających z obserwacji zmian wektora ataków oraz wniosków uzyskiwanych z pracy wdrożonego systemu.

10.2 Szacowanie etatów merytorycznych

W niniejszym rozdziale znajdują się szacunki etatów merytorycznych w kluczowych podmiotach krajowego systemu ochrony cyberprzestrzeni.

Do oszacowania łącznej liczby etatów w warstwie operacyjno-technicznej wykorzystano nowy model CSIRT Services Framework opisany w rozdziale 6.4, w którym dla każdej usługi przypisujemy rozłączną liczbę etatów. Tak więc przykładowo, w celu poprawnej realizacji Usługi 1 *Incident Management* (Zarządzania Incydentami) na poziomie Państwa biorąc pod uwagę najbliższe kilka lat, szacujemy 70 etatów technicznych, z czego 50 dotyczyłoby etatów zajmujących się samym 1.1 *Incident Handling* (Obsługą Incydentów) a 20 *Vulnerability, Configuration and Asset Management* (Zarządzaniem Podatnościami, Konfiguracją i Zasobami). Uwaga: liczba etatów w wielu przykładach może być uzupełniona podmiotami komercyjnymi, zgodnie z opisem ogólnym usług w rozdziale 6.4. Przyjętę liczby nie obejmują CSIRTów sektorowych - w szczególności nie obejmują CSIRTu wojskowego. Liczby te należy traktować orientacyjne - mają na celu zilustrowania skali przedsięwzięcia.

Nazwa usługi	Szacunkowa liczba etatów	Uwagi
1: Incident Management		

1.1 Incident Handling	**50**	
1.2 Vulnerability, Configuration and Asset Management	**20**	
2: Analysis		
2.1 Incident Analysis	**20**	
2.2 Artifact Analysis	**50**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.
2.3 Media Analysis	**15**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.
2.4 Vulnerability/Exploitation Analysis	**20**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.
3: Information Assurance		
3.1 Risk/Compliance Assessment	**10**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.
3.2 Patch Management	**10**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.
3.3 Operation Policies Management	**5**	
3.4 Risk Analysis/Business Continuity Disaster Recovery Advisement	**5**	
3.5 Security Advisement	**5**	
4: Sensor Management		
4.1 Sensor/Metrics operations	**20**	
4.2 Fusion/Correlation	**10**	
4.3 Development and Curation of Security Intelligence	**10**	
4.4 Data and Knowledge Management	**10**	
4.5 Organizational Metrics	**5**	
5: Outreach/Communications		
5.1 Cybersecurity Policy Advisory	**5**	

5.2 Relationship Management	**10**	
5.3 Security Awareness Raising	**20**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.
5.4 Branding/Marketing	**5**	
5.5 Information Sharing and Publications	**20**	
6: Capability Building		
6.1 Training and Education	**10**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.
6.2 Organizing Exercises	**10**	
6.3 Systems and Tools for Constituency Support	**20**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.
6.4 Stakeholder Services Support	**20**	
7: Research/Development		
7.1 Development of Vulnerability Discovery/Analysis/Remediation/Root Cause Analysis Methodologies	**10**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.
7.2 Development of processes for Gathering/Fusing/Correlating Security Intelligence	**10**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.
7.3 Development of Tools	**20**	Istnieje możliwość uzupełnienia za pomocą zasobów zewnętrznych komercyjnych podmiotów.

Sumarycznie, szacunkowe wartości wychodza w tym wypadku na około 425 etatów, przy założeniu, że czynności świadczone przez osoby zatrudnione są zupełnie rozłączne.

10.3 Pozostałe kategorie kosztów

Kolejną kategorią kosztów byłyby etaty w zakresie obsługi administracyjnej, prawnej i finansowej koniecznej dla fukcjonowania podmiotów realizujących katalog usług wymieniony wyżej.

Jeśli chodzi o infrastrukturę w postaci siedzib, wyposażenia biurowego, infrastruktury komputerowej, to koszty, które należałoby uwzględnić silnie zależą od modelu całego

systemu, który zostałby wybrany. W wariancie scentralizowanym powstaje zupełnie nowa instytucja (NCC), co wymaga budżetu na stworzenie praktycznie od zera (nowej agencji) - co można by porównać z powstaniem np. NCBiR lub CBA (koszt powołania agencji wykonawczej albo służby specjalnej). Z kolei w wariancie rozproszonym zostałyby w dużej mierze wykorzystane istniejące zasoby oraz infrastruktura. Nie jest więc możliwe na obecnym etapie precyzyjne oszacowanie kosztów, niezależnie od wariantu.

Zespół Łącznikowy

Zakłada się, że członkowie zespołu byliby finansowani przez macierzyste instytucje (np. w wymiarze połowy etatu), a Koordynator zapewniałby obsługę administracyjną i biurową.

Zespoły Zadaniowe

Jak wspomniano wyżej proponuje się wyasygnowanie budżetu na dofinansowanie pracy najważniejszych Zespołów Zadaniowych. Przykładowo, jeśli założymy, że średnio w roku trzy umowne zespoły pracujące ciągle, o liczebności do 10 osób są dofinansowane, może to wymagać przeznaczenia kilkuset tysięcy złotych rocznie na ten cel.

Wspieranie powstawania centrów ISAC oraz CSIRTów sektorowych

W celu wspierania powstawania centrów ISAC, które mogłyby się z czasem przekształcać w CSIRTy sektorowe należałoby wyasygnować budżet na warsztaty i szkolenia a także opcjonalnie na opracowanie planu działania powstającego ISAC oraz kluczowych procedur funkcjonowania. Do rozważenia byłaby formuła konkursowa, w której Koordynator rozpisuje konkurs na jedno centrum ISAC rocznie, które uzyskiwałoby dofinansowanie na rozpoczęcie funkcjonowania.

11 Kluczowe rekomendacje

W rozdziale tym przedstawiamy kluczowe rekomendacje wynikłe z ekspertyzy:

1. Uznanie konieczności niezwłocznego określenia ram systemu ochrony cyberprzestrzeni RP, który zapewni ochronę interesu narodowego, przy uwzględnieniu ponadgranicznego charakteru zagadnienia zagrożeń w cyberprzestrzeni oraz planowanej legislacji na poziomie Unii Europejskiej.

2. Zapewnienie, aby utworzony system był efektywny w praktyce, tj. dynamicznie dostosowywał się do zmieniających się wyzwań, potrzeb, zagrożeń i uwarunkowań zewnętrznych w cyberprzestrzeni (własność *elastyczności/ zwinności*).

3. Precyzyjne zdefiniowanie obowiązkowych mechanizmów współpracy pomiędzy organami (szczebla krajowego, sektorowymi) zaangażowanymi w system ochrony cyberprzestrzeni RP w celu zapewnienia spójności reguł bezpieczeństwa i niesprzeczności w zakresach obowiązków poszczególnych organów.

4. Zapewnienie, aby utworzony system uwzględniał i maksymalnie wykorzystywał istniejące dokonania i potencjał w dziedzinie cyberbezpieczeństwa, a w odpowiednich przypadkach, również doświadczenia innych krajów.

5. Ewaluacja dokumentu Polityki Ochrony Cyberprzestrzeni RP (przed upływem trzech lat od dnia jego uchwalenia) pod kątem spełniania założonej roli, zupełności treści, umocowania w katalogu aktów prawnych, zakresu podmiotowego i przedmiotowego.

6. Pilne doprowadzenie do uspójnienia wszelkich dokumentów o charakterze strategicznym, obejmujących zagadnienia bezpieczeństwa cyberprzestrzeni, a docelowo – opracowanie jednego dokumentu o charakterze strategicznym: strategii ochrony cyberprzestrzeni RP.

7. Bezwzględne zapewnienie przeznaczenia odpowiednich zasobów (finansowych, technicznych, osobowych) w celu efektywnej realizacji zadań wynikających z opracowanych dokumentów o charakterze strategicznym, jak również z transpozycji dyrektywy NIS.

8. Niezależnie od przyjętego modelu ochrony cyberprzestrzeni RP, pilne powołanie instytucji koordynującej działania administracji publicznej w zakresie ochrony

cyberprzestrzeni RP. Preferowana formuła – przypisanie tej funkcji ministrowi lub wiceministrowi, co najmniej w randze podsekretarza stanu oraz szczegółowe określenie zakresu działania właściwego ministra.

9. Niezależnie od przyjętego modelu ochrony cyberprzestrzeni RP, pilne powołanie oficjalnego zespołu reagującego na zagrożenia i incydenty bezpieczeństwa w cyberprzestrzeni na poziomie krajowym – CSIRT-u krajowego. Preferowana formuła – powierzenie roli CSIRTu krajowego któremuś z już działających zespołów reagowania, tj. CERT Polska, działającemu w ramach NASK lub CERT.GOV.PL, działającemu w ramach ABW, przy jednoczesnym rozszerzeniu kompetencji CERT.GOV.PL o obowiązki w zakresie ochrony instytucji administracji samorządowej i, ewentualnie, infrastruktury krytycznej.

10. Niezależnie od przyjętego modelu ochrony cyberprzestrzeni RP, pilne powołanie organu opiniodawczego i doradczego dla Rady Ministrów w sprawach dotyczących cyberbezpieczeństwa, w szczególności w celu formułowania ocen i wyrażanie opinii w sprawach projektów aktów normatywnych dotyczących cyberbezpieczeństwa, kierunków i planów działania organów zaangażowanych w ochronę cyberprzestrzeni czy koordynowania ich współdziałania.

11. Niezależnie od przyjętego modelu ochrony cyberprzestrzeni RP, powołanie stałego zespołu przedstawicieli kluczowych instytucji, które zajmują się obszarem cyberbezpieczeństwa (przedstawiciele ministerstw, kluczowych firm telekomunikacyjnych, sektora infrastruktury krytycznej), dysponujących odpowiednią wiedzą techniczną w zakresie technologii informatycznych i bezpieczeństwa oraz rozeznaniem co do funkcjonowania systemu cyberbezpieczeństwa.

12. Niezależnie od przyjętego modelu ochrony cyberprzestrzeni RP, powołanie podmiotu dysponującego wiedzą sytuacyjną oraz odpowiednimi kompetencjami technicznymi pozwalającymi na głęboką analizę zagrożeń cyberprzestrzeni i oferującego zaawansowane wsparcie techniczne przy rozwiązywaniu trudnych bądź dużej skali incydentów naruszających bezpieczeństwo cyberprzestrzeni oraz rekomendującego działania profilaktyczne – Krajowego Centrum Analitycznego. Preferowana formuła – powierzenie funkcji Krajowego Centrum Analitycznego istniejącemu w NASK zespołowi CERT Polska.

13. Niezależnie od przyjętego modelu ochrony cyberprzestrzeni RP, opracowanie katalogu zagrożeń wraz ze scenariuszami reakcji na te zagrożenia przez podmioty państwowe, uwzględniającego również rolę podmiotów prywatnych.

14. Niezależnie od ostatecznego kształtu dyrektywy NIS, włączenie obszaru systemów administracji publicznej do krajowego systemu cyberbezpieczeństwa poprzez precyzyjne zdefiniowanie obowiązków wszystkich instytucji państwowych, w tym Sejmu, Senatu czy Kancelarii Prezydenta RP, w dziedzinie osiągania właściwego poziomu ochrony.

15. Opracowanie co najmniej kilkuletniego Narodowego Programu do Walki z Cyberprzestępczością, na wzór programu przyjętego w obszarze walki z terroryzmem.

16. Wypracowanie metod okresowej oceny skuteczności/efektywności przyjętego rozwiązania w zakresie krajowego systemu ochrony cyberprzestrzeni (m.in. poprzez określenie mierników, które mogą zostać w tym procesie wykorzystane).

17. Wspieranie badań prowadzących do wytworzenia narzędzi umożliwiających zaawansowane monitorowanie zagrożeń i skuteczną reakcję.

18. Podejmowanie działań w celu uświadamiania kadrze kierowniczej przedsiębiorstw i instytucji konieczności prowadzenia analizy ryzyka oraz powoływania zespołów CSIRT, a także opracowania odpowiedniego systemu zachęt dla podmiotów, aby stymulować podejmowanie takich działań.

19. Stworzenie realnych warunków do powoływania pełnomocników ds. bezpieczeństwa w kluczowych instytucjach publicznych.

20. Rozważenie zastosowania dla kluczowych sektorów, w tym obszaru infrastruktury krytycznej modelu działania składającego się z trzech elementów: ustanawiania minimalnych wymogów bezpieczeństwa dla podmiotów działających w sektorze, obowiązku zgłaszania poważnych incydentów i zagrożeń cyberbezpieczeństwa oraz wprowadzenia wymogu przeprowadzania audytów bezpieczeństwa, służących szczególnie osiąganiu coraz wyższego poziomu bezpieczeństwa teleinformatycznego.

21. Ustanawianie minimalnych lub optymalnych wymogów bezpieczeństwa, na podstawie procesów analiz ryzyka i wiedzy na temat zagrożeń oraz technologii zabezpieczających oraz wdrażanie schematów raportowania o istotnych incydentach w danym sektorze w celu zapewnienia skoordynowanego podejścia do cyberbezpieczeństwa, przy jednoczesnym zachowaniu zasad dialogu pomiędzy organami regulacyjnymi czy tworzącymi prawo a przedstawicielami danego sektora. Przygotowywanie poradników i instrukcji dla podmiotów, które będą zobowiązane wdrażać ustanowione wymogi bezpieczeństwa.

22. Opracowanie kryteriów wyboru oraz katalogu kluczowych sektorów i obszarów, w których wdrożone zostanie podejście do cyberbezpieczeństwa opisane dwa punkty

wyżej – z uwzględnieniem przepisów wynikających ze strategii bezpieczeństwa cyberprzestrzeni UE.

23. Przy wyznaczaniu listy kluczowych sektorów i reguł, jakim miałyby podlegać, przeprowadzenie skrupulatnej analizy ryzyk w danym sektorze przy wykorzystaniu odpowiedniej metodyki oraz procesu konsultacyjnego. Rekomendowane jest wykorzystanie proponowanego mechanizmu Zespołów Zadaniowych.

24. Aktywne wspieranie przez administrację państwową powstawanie branżowych czy sektorowych inicjatyw typu ISAC, w ramach których wypracowywane byłyby odpowiednie praktyki bezpiecznego korzystania z infrastruktury teleinformatycznej z uwzględnieniem specyfiki danej grupy, a także generowane byłyby sygnały zwrotne na temat rzeczywistych problemów przy wdrażaniu zaleceń bezpieczeństwa cyberprzestrzeni.

Zastrzeżenia

Niniejsze opracowanie zostało sporządzone w zakresie określonym w umowie pomiędzy Zleceniodawcą a Zleceniobiorcą, w oparciu o najbardziej aktualną wiedzą z zakresu bezpieczeństwa teleinformatycznego i przepisów prawa. W przypadku ewentualnego ujawnienia się bądź zaistnienia nowych, nieznanych wcześniej okoliczności, wszystkie lub niektóre wnioski z niniejszego opracowania mogą wymagać dodatkowej analizy z ewentualną korektą włącznie.

Bibliografia

Akty prawne

1. Strategia bezpieczeństwa wewnętrznego Unii Europejskiej. Rezolucja Parlamentu Europejskiego z dnia 22 maja 2012 r. w sprawie strategii bezpieczeństwa wewnętrznego Unii Europejskiej (2010/2308(INI)) (Dz. U. UE C 264E. 13.09.2013).
2. Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z dnia 5 listopada 2014 r.
3. Rozporządzenie Komisji (UE) nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej (Dz. U. UE L 173. 26.06.2013).
4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004. (Dz. U. UE L 165. 18.06.2013).
5. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE (Dz.U. UE L 257/73. 28.08.2014).
6. Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. (Dz. U. L 281. 23.11.1995).
7. Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. U. UE L 201, 31.07.2002).
8. Dyrektywa 2009/140/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. zmieniająca dyrektywy 2002/21/WE w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej, 2002/19/WE w sprawie dostępu do sieci i usług łączności elektronicznej oraz wzajemnych połączeń oraz 2002/20/WE w sprawie zezwoleń na udostępnienie sieci i usług łączności elektronicznej (Dz. U. UE L 337/37. 18.12.2009).

9. Dyrektywa Rady 2008/114/WE z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (Dz. U. UE L 345. 23.12.2008).
10. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz. U. UE L 218/8. 14.08.2013).
11. Ustawa z dnia 29 sierpnia 1997 r. - Prawo bankowe (tekst jednolity: Dz.U. 2015, poz. 128).
12. Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (tekst jednolity: Dz.U. 2015, poz. 812).
13. Ustawa z dnia 29 sierpnia 2002 r. o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej (tekst jednolity: Dz. U. 2014, poz. 1815).
14. Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (tekst jednolity: Dz. U. 2014, poz. 243).
15. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (tekst jednolity: Dz. U. 2014, poz. 1114).
16. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (tekst jednolity: Dz. U. 2014, poz. 1166).
17. Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. 2010, poz. 182 z późn. zm.)
18. Uchwała nr 252 Rady Ministrów z dnia 9 grudnia 2014 r. w sprawie „Narodowego Programu Antyterrorystycznego na lata 2015–2019” (M.P. 2014, poz. 1218).
19. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 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, poz. 526).
20. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 19 marca 2013 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. 2013, poz. 386).
21. Decyzja Nr 38/MON z dnia 16 lutego 2012 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw Bezpieczeństwa Cyberprzestrzeni (Dz. Urz. MON, poz. 52).

22. Zarządzenie Nr 10/MON z dnia 29 kwietnia 2013 r. w sprawie utworzenia i nadania statutu państwowej jednostce budżetowej - Narodowe Centrum Kryptologii (Dz. Urz. MON, poz. 121).
23. Decyzja Nr 275/MON z dnia 13 lipca 2015 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej (Dz. Urz. MON, poz. 208).

Pozostałe źródła

1. Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-społecznego i Komitetu Regionów - Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń. Komisja Europejska. [online] Ostatnia aktualizacja: 07.02.2013 [dostęp: 30 września 2015] http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667
2. Raport o stanie bezpieczeństwa w Polsce w 2013 roku. Ministerstwo Spraw Wewnętrznych RP. [online] Ostatnia aktualizacja: 19.09.2014 [dostęp: 30 września 2015] http://bip.msw.gov.pl/download/4/23032/00RAPORT2013.pdf
3. Biuro Służby Kryminalnej Komedy Głównej Policji – Wydział do Walki z Cyberprzestępczością [online] [dostęp: 30 września 2015] http://www.policja.pl/pol/kgp/bsk/struktura/wydzialy/wydzial-do-walki-z-cybe/87086,Wydzial-do-Walki-z-Cyberprzestepczoscia.html
4. Wyższa Szkoła Policji w Szczytnie - W WSPol powstaje Centrum Analityczno-Wywiadowcze i Doskonalenia Zwalczania Cyberprzestępczości [online] Ostatnia aktualizacja: 13 listopada 2014 [dostęp: 30 września 2015] http://www.wspol.edu.pl/d/start/1896-w-wspol-powstaje-centrum-analityczno-wywiadowcze-i-doskonalenia-zwalczania-cyberprzestpczoci-
5. OST 112. Ogólnopolska sieć teleinformatyczna na potrzeby obsługi numeru alarmowego 112. Centrum Projektów Informatycznych. Red. Karolina Jarosławska. Warszawa 2012. ISBN 978-83-935010-0-7.
6. Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej. Biuro Bezpieczeństwa Narodowego. Warszawa 2015. ISBN: 978-83-60846-25-4.
7. CERT Polska Raport 2014. Naukowa i Akademicka Sieć Komputerowa. Warszawa 2015. ISSN 2084-9079 (2014).
8. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 r. Agencja Bezpieczeństwa Wewnętrznego. Warszawa 2015. [online] [dostęp: 30 września 2015] http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html

9. Special Eurobarometer 404 Cyber Security Report. European Commission. Bruksela 2013. [online] [dostęp: 30 września 2015] http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf
10. Handbook for Computer Security Incident Response Teams. Carnegie Mellon Software Engineering Institute. Pittsburgh 2003 (wyd. 2). CMU-SEI-2003-HB-002
11. GameOver ZeuS. Backgrounds on the Badguys and the Backends. Fox-IT. [online] [dostęp: 30 września 2015] https://www.fox-it.com/en/files/2015/08/FoxIT-Whitepaper_Blackhat-web.pdf
12. CERT Polska. [online] [dostęp: 30 września 2015] http://www.cert.pl/
13. Naukowa i Akademicka Sieć Komputerowa. n6. [online] [dostęp: 30 września 2015] http://n6.cert.pl/
14. Agencja Bezpieczeństwa Wewnętrznego – System ARAKIS.GOV. [online] [dostęp: 30 września 2015] http://www.cert.gov.pl/cer/system-arakis-gov/310,System-ARAKIS-GOV.html
15. NISHA Network. [online] [dostęp: 30 września 2015] http://nisha-network.eu/
16. FIRST.org. [online] [dostęp: 30 września 2015] http://www.first.org/
17. Niebezpiecznik - Kancelaria Premiera, MSZ, MON i Kancelaria Prezydenta zhackowane. Wiemy kto stoi za tymi włamaniami. [online] Ostatnia aktualizacja 13.03.2013 [dostęp: 30 września 2015] https://niebezpiecznik.pl/post/kancelaria-premiera-msz-mon-i-kancelaria-prezydenta-zhackowane-wiemy-kto-stoi-za-tymi-wlamaniami/
18. Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach. Komisja Nadzoru Finansowego. 2013 [online] [dostęp: 30 września 2015] https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf
19. Wytyczne dotyczące zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatyczego w zakładach ubezpieczeń i zakładach reasekuracji. Komisja Nadzoru Finansowego. 2014 [online] [dostęp: 30 września 2015] https://www.knf.gov.pl/Images/PTE_Wytyczne_IT_16_12_2014_tcm75-40005.pdf
20. Narodowe Centrum Badań i Rozwoju – Programy i projekty – obronność, bezpieczeństwo. [online] [dostęp: 30 września 2015] http://www.ncbir.pl/programy-i-projekty---obronnosc-bezpieczenstwo
21. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej z dnia 25 czerwca 2013 r. Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego. [online] [dostęp: 30 września 2015] https://mac.gov.pl/files/polityka_ochrony_cyberprzestrzeni_rp_wersja_pl.pdf
22. European Union Agency for Network and Information Security – Security Strategies in the World. [online] [dostęp: 30 września 2015]

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

23. Incentives and Challenges for Information Sharing in the Context of Network and Information Secuirty. European Union Agency for Network and Information Security. 2010 [online] [dostęp: 30 września 2015] https://www.enisa.europa.eu/act/res/policies/good-practices-1/information-sharing-exchange/incentives-and-barriers-to-information-sharing/at_download/fullReport
24. Implementation of Article 15 of the draft regulation on electronic identification and trusted services for electronic transactions in the internet market. European Union Agency for Network and Information Security. 2012 [online] [dostęp: 30 września 2015] https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/implementation-of-article-15
25. Technical Guideline on Incident Reporting. European Union Agency for Network and Information Security. 2012 (wer. 2.1) [online] [dostęp: 30 września 2015] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/Technical%20Guidelines%20on%20Incident%20Reporting
26. Cyber Incidents Reporting in the EU. European Union Agency for Network and Information Security. 2012 [online] [dostęp: 30 września 2015] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/cyber-incident-reporting-in-the-eu
27. Deployment of Baseline Capabilities of n/g CERTs - Status Report 2012. European Union Agency for Network and Information Security. 2012 [online] [dostęp: 30 września 2015] https://www.enisa.europa.eu/activities/cert/support/files/status-report-2012
28. Actionable information for Security Incident Response. European Union Agency for Network and Information Security. 2014 [online] [dostęp: 30 września 2015] http://www.enisa.europa.eu/activities/cert/support/actionable-information
29. Annual Incident Reports 2013. European Union Agency for Network and Information Security. 2014 [online] [dostęp: 30 września 2015] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/annual-reports/annual-incident-reports-2013
30. Technical Guideline on Security Measures. European Union Agency for Network and Information Security. 2014 (wer. 2.0) [online] [dostęp: 30 września 2015] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting/technical-guideline-on-minimum-security-measures

31. Informacja o wynikach kontroli „Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP". Najwyższa Izba Kontroli. 2014 [online] [dostęp: 30 września 2015] https://www.nik.gov.pl/kontrole/P/14/043/
32. European Commission - EU Cybersecurity plan to protect open internet and online freedom and opportunity - Cyber Security strategy and Proposal for a Directive. [online] [dostęp: 30 września 2015] http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
33. Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48. 7 lutego 2013.
34. Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Council of the European Union. [online] Ostatnia aktualizacja: 22 lipca 2013 [dostęp: 30 września 2015] http://register.consilium.europa.eu/pdf/en/13/st12/st12109.en13.pdf
35. Critical Information Infrastructure Protection "Achievements and next steps: towards global cyber-security" (CIIP) -Adoption of Council conclusions. Council of the European Union. [online] Ostatnia aktualizacja: 19 maja 2011 [dostęp: 30 września 2015] http://register.consilium.europa.eu/pdf/en/11/st10/st10299.en11.pdf
36. Komunikat Komisji do Parlamentu europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury informatycznej - „Ochrona Europy przed zakrojonymi na szeroką skalę atakami i zakłóceniami cybernetycznymi : zwiększenie gotowości, bezpieczeństwa i odporności" (COM(2009) 149. 30.03.2009).
37. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Europejska agenda cyfrowa. (COM(2010) 245. 19.05.2010).
38. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów w sprawie ochrony krytycznej infrastruktury teleinformatycznej: Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni. (COM(2011) 163. 31.03.2011).
39. Wniosek Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) (COM(2012) 11. 21.01.2012).

40. Communication from the Commission to the Council and the European Parliament. Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre. (COM(2012) 140. 28.03.2012).

41. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Wykorzystanie potencjału chmury obliczeniowej w Europie. (COM(2012) 529. 27.09.2012).

42. Rezolucja Rady z dnia 18 grudnia 2009 r. w sprawie wspólnego europejskiego podejścia do bezpieczeństwa sieci i informacji (Dz. U. EU C 321. 29.12.2009).

43. Ocena ryzyka na potrzeby zarządzania kryzysowego. Raport o zagrożeniach bezpieczeństwa narodowego. Rządowe Centrum Bezpieczeństwa. 2013 [online] [dostęp: 30 września 2015] http://rcb.gov.pl/wp-content/uploads/ocenaryzyka.pdf

Załącznik: Opracowanie ENISA na temat modeli zarządzania bezpieczeństwem cyberprzestrzeni[90]

Cyber Security Strategies - Governance Models

Cyber Security Strategy overall

Model A: Centralised approach

One authority holds the mandate for cyber security in national level keeping responsibilities in-house and all other authorities need to report to it. In some cases this agency already exists, in others it is created based on the requirements of the strategy. Usually the central authority is the national security centre (in some other cases the national regulatory authority takes this role, or it even stays inside the Ministry) and is responsible for the full coordination of the implementation pf the strategy. The other agencies have supporting roles in the implementation of the strategy (monitoring, auditing etc.). Relevant stakeholders (public or private bodies) need to report risks and incidents to the coordinating authority. The coordinating authority issues recommendations and guidelines on the specific topics. The designated authority is authorised to issue binding instructions to companies and governmental authorities.

Advantages	– Fast response time, i.e. quick and easy decision-making and implementation of counter measures. Better control during crisis management. – Usually the national CERT exists within such authority i.e. better communication between technical specialists and policy-makers etc. – Existence of one point of contact for international partners in any cyber security issue – other communication can be afterwards diverted to other agencies. – Better for smaller countries, better use of limited resources.

[90] Opracowane przez Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji na potrzeby niniejszej ekspertyzy na podstawie wiedzy własnej oraz wywiadów z ekspertami z krajów członkowskich UE / sierpień 2015

	Less bureaucratic.
Disadvantages	– Difficult, if low trust-level between centralized agency and reporting bodies (especially if that agency is part of the same ministry as law enforcement). If the authority is not empowered with enough legal or political powers, the implementations of strategies can be cumbersome. Also from the opposite side, compliance is based on authority, not trust. – Challenge in separating political from operational functions. Cyber security issues are not homogenous: cyber-crime, collecting intelligence in cyberspace, education in cyber security (both technical and social) etc. are different issues. They are usually dealt in more effective way by authorities responsible for the specific area. – This approach is not promoting the multi stakeholder approach and the results might not me as effective as expected. – Decentralised structures need a strong project manager or coordination unit to keep things together and translate the big picture and make sure information is exchanged between the relevant players.

Model B: De-centralised approach

Roles and responsibilities in the field of cyber security are spread across a variety of different actors. Each agency and authority holds responsibility in its own sector and the operators/ stakeholders need to report incidents to these specific agencies. This example is usually followed when the country is divided in regions, where this model is followed for all governance topics. Or in other cases this approach is followed because more than one agencies related to cyber security exist already (for example in one agency the protection of citizens is the main target, and another agency is responsible for cybercrime issues). A network for communication exists between these (regional) coordinating authorities to share information and exchange on a voluntary basis.

Advantages	– Centralized decision-making (fast response time), yet decentralized responsibilities and sector-specific information

	gathering. – Better trust-level among decentralized sectors. – More stakeholders are involved and the work load is more distributed (multi-stakeholder approach). Actions can be promoted concurrently. Implementation becomes decentralised and more efficient. – Specialization of every actor can bring many different and often very interesting approaches how to tackle individual cyber-security problems. – Best option for bigger or decentralised countries or where more agencies already exist.
Disadvantages	– Differences of opinion can have a long way to reaching a solution to a problem, even more so when a topic is of a political nature. – Compliance is mostly voluntary (except where regulation exists). – Coordination among number of different subjects can be troublesome and ineffective. Difficult to monitor and enforce progress, set priorities, promote coordinated actions and impose national policies. – Cooperation becomes important but it is more difficult to achieve. Sometimes operational cooperation becomes very difficult and information sharing becomes a real challenge although not impossible. Possible “competition” among different subjects. – International cooperation can be more complicated.

Model C: Semi-centralised approach

In this hybrid approach there is a central ministry that is coordinating the implementation of the strategy; however per sector or per region a designated authority is being appointed as the main information hub. The operators, or the other stakeholders implementing the strategy, report only to the direct supervisory authority. This authority can impose measures, audit and take all measures necessary. Periodically these authorities report the status of cyber security to the central ministry.

Advantages	– In contrast to decentralised model, the cyber security strategy

	can be developed by one subject: no problem with the coherence of the strategy. – Slightly lower response time as tasks are delegated to the designated authorities. – Coordination is achieve at acceptable levels and the activities are distributed in a way that can be effective (multi-stakeholder approach). – One central point of contact for international partners.
Disadvantages	– Good communication mechanisms are necessary and effective coordination becomes more critical. Setting-up/drawing lines of responsibility may become more difficult. More difficult to monitor and enforce progress. Sometimes power struggles may arise. – Information from below (basic cyber-security actors), which can be very important for strategy making, does not have to find its way to the central ministry (or coordinating authority); the information can also be distorted as the collection and basic processing is up to sectoral or regional authorities. – Information sharing is less effective than in centralised approach. – Combines disadvantages from both models: too many players/authorities, which makes information exchange difficult. Who is in charge? Who leads in a crisis?

Critical Information Infrastructures protection

Model A: Centralised approach

One public authority has the mandate for cyber security, they need to conduct a national risk assessment, to identify the critical assets and issue guidelines on how to protect them. The critical infrastructures operators are obliged to report any incident, to comply with the specific legislation proposed (in some cases these are just guidelines) and make sure the security level is high. The authority needs to make sure that the operator has all the means needed to enhance cyber security (organise exercises, enhance cooperation between relevant stakeholders etc.). In some cases the authority in charge is the national CERT being part of a governmental body (ministry or national security agency).

Advantages	– Achieve good level of control on executing national risk assessments and identify critical assets in a homogenous way. Guidelines are drafted accordingly. – Coherent approach: better coordination in protecting critical infrastructures. – Effective information sharing (which is essential for cyber security and incident handling). – Easier and more clear international cooperation.
Disadvantages	– Collaboration with other stakeholders becomes essential, engagement of other stakeholders is more difficult. – Wider knowledge is necessary. Operators are in a better position to manage their systems. – Poorer knowledge on specifics of each sector. – Tougher coordination of implementation of cyber-security measures with physical-security measures. – CII operators know best what their critical processes are and what the corresponding risks are and should therefore be in charge of their risk assessment. Public authorities should only play a supporting subsidiary role

Model B: Sectorial approach

A designated authority is responsible for cyber security in each sector for example NRA for the Telecoms sector, MoH for the Health sector (or a National Health Authority), Regulator for Finance etc. These authorities run independently and has foul overview of their sector. They do not report to any other body, however is some cases there might be a communication channel with the central government to share information on the national cyber security status.

Advantages	– More effective in targeting the specific needs of each sector. – More specialised knowledge in each authority. – Better coordination and collaboration within the sector.
Disadvantages	– Sharing of information and operational cooperation becomes critical and usually becomes a problem. Approach might not be

	harmonised. – A cooperation mechanism/plan might be necessary, bilateral and at national level. Different levels of measures can be achieved in the different sectors. In the end an overseeing authority will be needed. – Approach to cyber security does not have to be coherent with other important subjects. – More difficult international cooperation – no single point of contact.

Stakeholders Engagement

Model A: Public Private Partnerships

Public private partnerships are officially setup and create a new body, in some cases this new body has cyber security mandate, and in other cases it operates are an advisory board. Public-Private Partnerships (PPPs) are essential for the Security and Resilience of Critical Information Infrastructures (CII), since a large part of them belongs to private sector stakeholders. Trusted information sharing, incident reporting are some of the functionalities of the PPP. Sometimes these PPPs are setup by a legal document i.e. cyber security strategy.

Advantages	– More structured cooperation between public and private sector that ensure a certain level of cooperation. Partnership embedded in a legal document and has some kind of a binding character.
	– For public sector: Access to private sector resources, e.g. information, manpower etc. Effectiveness: the private sector have the most effective means to handle both small and large-scale incidents.
	– For private sector: Active involvement in public sector decision-making
	– For both:
	  – Trust-building
	  – Institutionalized information exchange
	  – Closer touch with innovation and R&D, better implementation

Disadvantages	– Slower response time (various positions have to be considered) - can be compensated by well written statutory or contractual PPP basis – Rules of cooperation must be clear and transparent. Legal framework is necessary. May become more expensive to the public sector. Incentives might be necessary.

Model B: Voluntary working groups (per sector, steering committee from ministry)

A council can be established with the objective to foster public-private cooperation. The council brings together experts from both sides and acts as a platform to exchange information about problems and best practices for the improvement of the security of critical infrastructure. The strategic-level Cyber Security Council, a regular forum of decision makers from key governmental agencies involved in cyber security oversees the implementation of the National Cyber Security Strategy. A supervisory authority (ministry or any other agency with cyber security mandate) is responsible for the coordination of arrangements at national l level.

Advantages	– Involvement of private sector in public sector decision-making (if they accept to participate on voluntary basis, will need other type of motivation). – Easier to set-up. Lower costs for the public sector. More flexible collaboration between stakeholders. – Good approach if there is enough interest from stakeholders.
Disadvantages	– Engagement of stakeholders is not ensured (especially in small countries). Does not solve the necessity of proper and intense information sharing within private sector and between private and public sector. – Incentives to the private sector become more important. Sharing of information becomes difficult. – Building trust is not easy. Nobody will be willing to share information about such sensitive issues. Only established structures, with a certain level of confidentiality will prevail. – More difficult to effectively manage (and make it last).