Michał Kamiński
Justyna Strużewska-Smirnow
Mateusz Wieczerza

Charakterystyka modeli systemów bezpieczeństwa teleinformatycznego oraz ochrony sieci teleinformatycznych z punktu widzenia służb specjalnych

I. Wprowadzenie

Dynamiczny rozwój technologiczny stwarza nowe wyzwania dla organów odpowiedzialnych za bezpieczeństwo państwa. Pojawiające się cyberzagrożenia stale jednak ewoluują, dlatego też przeciwdziałanie niekorzystnym zjawiskom przez ich badanie i monitorowanie nie zapewni pełnej skuteczności zwalczania tych zagrożeń. Efektywne działania wymagają także przewidywania scenariuszy prawdopodobnych sytuacji kryzysowych oraz opracowywania nowych narzędzi, które skutecznie będą chronić dobra społeczne.

Istotną przeszkodą w stworzeniu odpowiedniego modus operandi w zakresie utworzenia na poziomie państwowym kompleksowej ochrony teleinformatycznej jest trudność w uchwyceniu negatywnych zjawisk, szczególnie na początkowym etapie ich rozwoju. Z tego względu zapewnienie przez agendy rządowe właściwego stopnia bezpieczeństwa teleinformatycznego wymaga ścisłej współpracy wielu podmiotów, które – w zakresie swoich kompetencji – potrafią dostrzec i odpowiednio zdefiniować zagrożenia o niejednolitym charakterze. Warto zaznaczyć, że zdarzenia, które powodują negatywne skutki dla społeczeństwa, wynikają zarówno ze szczegółowo zaplanowanych, nierzadko motywowanych ideologicznie działań w obszarze teleinformatyki, takich jak: cyberprzestępczość, cyberterroryzm czy cyberszpiegostwo, jak też z hackingu realizowanego przez niewielkie grupy lub jednostki działające pod wpływem indywidualnych motywów. Potencjalny atak może być ukierunkowany zarówno na pozyskanie wrażliwych informacji, uszkodzenie infrastruktury krytycznej bądź utrudnienie w innym zakresie funkcjonowania obywateli, np. powodując brak dostępu do określonych serwisów informacyjnych lub e-usług. Działalność ukierunkowana na zapewnienie bezpieczeństwa teleinformatycznego musi być zatem realizowana w formach partnerstwa publiczno-prywatnego i musi uwzględniać i usługodawców, i odbiorców usług teleinformatycznych.

Dodatkowym elementem, który utrudnia walkę z cyberzagrożeniami, jest ich globalny charakter. W dokumencie *Wizja Sił Zbrojnych RP – 2030* dostrzeżono, że w przyszłości ta walka obejmie niemal każdy obszar ludzkiej aktywności, odmienny od klasycznego pola walki charakteryzowanego przez szerokość, głębokość oraz wysokość. Oprócz tradycyjnych, fizycznych geoprzestrzeni, jak ląd, morze, przestrzeń powietrzna (i kosmiczna), do prowadzenia walki będą wykorzystywane sfery pozbawione parametrów geograficznych, niemierzalne i nieograniczone, takie jak wirtualna przestrzeń cybernetyczna i sfera informacyjna. Te obszary będą się na siebie nakładać i wzajemnie uzupełniać, tworząc jednolitą, nieznaną do tej pory przestrzeń walki sił zbrojnych[1].

[1] http://d.wiadomosci24.pl/g2/pdf/250_8a52ebb24514c5ec0a386c8867cef049.pdf [dostęp: 7 VIII 2017].

Przytoczoną uwagę, dotyczącą ponadnarodowego charakteru działań militarnych rozgrywających się w cyberprzestrzeni można przenieść na wszelką aktywność związaną z zapewnianiem bezpieczeństwa narodowego. Ścisła współpraca międzynarodowa będzie zatem jednym z zasadniczych elementów skutecznego modelu efektywnej cyberobrony.

Zaznaczone powyżej aspekty dotyczące zagrożeń cybernetycznych mają wpływ na kształtowanie modeli systemów bezpieczeństwa teleinformatycznego w różnych krajach, jednak wyzwania, jakim muszą sprostać właściwe organy w poszczególnych państwach, są uzależnione także od uwarunkowań geopolitycznych czy modelu ustrojowego. W ramach rozwiązań prawnych, których celem jest ochrona sieci teleinformatycznych, ważną rolę odgrywają służby specjalne, ustawowo zobowiązane do podejmowania kompleksowych lub jedynie cząstkowych działań związanych z cyberobroną.

II. REPUBLIKA CZESKA

1. Stan prawny do lipca 2017 r.

W Republice Czeskiej ustawodawca zdecydował się na uregulowanie zagadnienia cyberbezpieczeństwa w jednym, kompleksowym akcie prawnym, jakim jest ustawa Nr 181 z 23 lipca 2014 r. o cyberbezpieczeństwie i zmianie niektórych innych ustaw, która weszła w życie 1 stycznia 2015 r.[2] (zwana dalej „ustawą").

1.1. Systematyka i zakres ustawy o cyberbezpieczeństwie, najważniejsze definicje

Przedmiotowa ustawa dzieli się na sześć części:

- część pierwsza – *Cyberbezpieczeństwo*,
- część druga – *Zmiany w ustawie o ochronie informacji niejawnych i kompetencjach w dziedzinie bezpieczeństwa*,
- część trzecia – *Zmiany w ustawie o komunikacji elektronicznej*,
- część czwarta – *Zmiany w ustawie o wolności informacji*,
- część piąta – *Zmiany w ustawie o dostarczaniu transmisji radiowej i telewizyjnej*,
- część szósta – *Wejście w życie*.

Część pierwsza, obejmująca większość zawartych w ustawie przepisów, dzieli się na pięć rozdziałów:

I – *Przepisy ogólne*,
II – *System na rzecz zapewnienia cyberbezpieczeństwa*,
III – *Stan zagrożenia cybernetycznego*,
IV – *Wykonywanie administracji państwowej*,
V – *Kontrola, nadzór i wykroczenia administracyjne*,
VI – *Przepisy końcowe*.

W rozdziale I znalazły się unormowania odnośnie do przedmiotu regulacji ustawy oraz definicje podstawowych wykorzystywanych w niej pojęć.

Zakres regulacji ustawy został określony w jej pierwszym paragrafie. Zgodnie z ustępem pierwszym tego przepisu reguluje ona prawa i obowiązki stron oraz zakres kompetencji organów władzy państwowej w dziedzinie bezpieczeństwa cybernetycz-

[2] https://www.govcert.cz/en/legislation/legislation/ [dostęp: 5 X 2017].

nego. Natomiast ustęp drugi omawianego paragrafu wyłącza z zakresu przedmiotowego ustawy systemy informacyjne i komunikacyjne służące do przetwarzania informacji niejawnych.

Następnie, w § 2, zawarto definicje najważniejszych, występujących w ustawie pojęć: cyberprzestrzeń, krytyczna infrastruktura teleinformatyczna, bezpieczeństwo informacji, kluczowy system informacyjny, administrator systemu informacyjnego, administrator systemu komunikacyjnego oraz kluczowa sieć.

Spośród wskazanych definicji należy przytoczyć definicję bezpieczeństwa informacji zawartą w § 2 lit. c, która oznacza: (…) *zapewnienie poufności, integralności i dostępności informacji*.

Z kolei kluczowy system informacyjny, zgodnie z lit. d § 2 oznacza (…) *system informacyjny zarządzany przez organ władzy publicznej, który nie stanowi krytycznej infrastruktury informacyjnej i w przypadku którego naruszenie bezpieczeństwa informacji może ograniczyć lub poważnie zagrozić skuteczności działań władzy publicznej*. Natomiast kluczowa sieć, zdefiniowana w § 2 lit. g, to (…) *sieć komunikacji elektronicznej, zapewniająca bezpośrednie połączenia zagraniczne do publicznej sieci łączności lub zapewniająca bezpośrednie podłączenie do krytycznej infrastruktury informacyjnej*.

Z zakresu powyższych definicji można wysnuć wniosek, że pojęcie bezpieczeństwo cybernetyczne jest odnoszone przez przepisy projektowanej ustawy głównie do domeny publicznej.

1.2. Zagadnienia funkcjonalne systemu cyberbezpieczeństwa

W § 3 zawarto listę podmiotów (władz publicznych oraz osób fizycznych i prawnych) mających obowiązki w sferze cyberbezpieczeństwa. Są to:

- dostawcy usług i sieci komunikacji elektronicznej,
- władze publiczne oraz osoby fizyczne i prawne administrujące sieciami kluczowymi,
- administratorzy krytycznej infrastruktury informatycznej,
- administratorzy krytycznej infrastruktury komunikacyjnej,
- administratorzy kluczowych systemów informacyjnych.

W rozdziale II części pierwszej omawianej ustawy pt. *System na rzecz zapewnienia cyberbezpieczeństwa* znajduje się większość zawartych w jej postanowieniach uregulowań merytorycznych. Przedmiotowy rozdział dzieli się na tytuły obejmujące od jednego do kilku paragrafów:

- *Środki bezpieczeństwa* (§ 4–6),
- *Zdarzenie i incydent w zakresie cyberbezpieczeństwa* (§ 7),
- *Raportowanie incydentów cyberbezpieczeństwa* (§ 8),
- *Przechowywanie dokumentacji* (§ 9–10),
- *Środki* (§ 11),
- *Ostrzeżenia* (§ 12),
- *Środki reagowania i środki ochronne* (§ 13–15),
- *Dane kontaktowe* (§ 16),
- *CERT krajowy* (§ 17),
- *Administrator CERT-u krajowego* (§ 18),

- *Umowa prawa publicznego* (§ 19),
- *CERT rządowy* (§ 20).

Pojęcie ś r o d k i b e z p i e c z e ń s t w a zostało zdefiniowane w ustępie 1 § 4. Oznacza ono: (…) *wszystkie czynności, mające na celu zapewnienie bezpieczeństwa informacji w systemach informacyjnych oraz zapewnienie dostępności i niezawodności usług i sieci elektronicznej komunikacji w cyberprzestrzeni*. Przepis ust. 2 przedmiotowego paragrafu nakłada obowiązki w zakresie ustanowienia i wdrożenia środków bezpieczeństwa dla informacyjnych systemów krytycznej infrastruktury informacyjnej, komunikacyjnego systemu informacyjnej infrastruktury krytycznej lub kluczowego systemu informacyjnego oraz prowadzenia dokumentacji bezpieczeństwa ich dotyczącej na następujące osoby:

- administratorów krytycznej infrastruktury informatycznej,
- administratorów krytycznej infrastruktury komunikacyjnej,
- administratorów kluczowych systemów informacyjnych.

W § 5 zawarto katalog środków bezpieczeństwa. Podstawowy ich podział (zgodnie z ust. 1) to środki organizacyjne i środki techniczne.

Stosownie do ustępu 2 § 5 środki organizacyjne obejmują:

a) system zarządzania bezpieczeństwem informacji,
b) zarządzanie ryzykiem,
c) politykę bezpieczeństwa,
d) bezpieczeństwo organizacyjne,
e) wymogi bezpieczeństwa dla dostawców,
f) zarządzanie kapitałem,
g) bezpieczeństwo zasobów ludzkich,
h) obsługę krytycznej infrastruktury informatycznej lub kluczowego systemu informacyjnego i zarządzanie komunikacją,
i) kontrolę dostępu osób do krytycznej infrastruktury informatycznej lub kluczowego systemu informatycznego,
j) nabywanie, rozwój i utrzymywanie krytycznej infrastruktury informatycznej lub kluczowego systemu informatycznego,
k) zarządzanie zdarzeniami w zakresie cyberbezpieczeństwa i incydentami cyberbezpieczeństwa,
l) zarządzanie ciągłością działania,
m) kontrolę i audyt krytycznej infrastruktury informacyjnej i kluczowych systemów informacyjnych.

Natomiast ustęp 3 zalicza do środków technicznych następujące zagadnienia:

a) bezpieczeństwo fizyczne,
b) narzędzia ochrony integralności sieci łączności,
c) narzędzia weryfikacji tożsamości użytkowników,
d) narzędzia zarządzania prawem dostępu,
e) narzędzia ochrony przed szkodliwym kodem,
f) narzędzia rejestrowania działalności krytycznej infrastruktury informacyjnej i kluczowych systemów informacyjnych, ich użytkowników i administratorów,
g) narzędzia wykrywania zdarzeń w zakresie bezpieczeństwa cybernetycznego,
h) narzędzia zbierania i oszacowania zdarzeń w zakresie bezpieczeństwa cybernetycznego,
i) bezpieczeństwo aplikacji,

j) urządzenia kryptograficzne,
k) narzędzia zabezpieczania poziomu dostępności informacji,
l) bezpieczeństwo systemów przemysłowych i służących do zarządzania.

Przepis § 7 ustawy definiuje pojęcia zdarzenie w zakresie cyberbezpieczeństwa oraz incydent cyberbezpieczeństwa, a także formułuje obowiązki niektórych podmiotów związane z zaistnieniem tego rodzaju zdarzeń.

Zdarzenie w zakresie cyberbezpieczeństwa to zdarzenie, które może powodować naruszenie bezpieczeństwa informacyjnego w systemach informatycznych lub naruszenie bezpieczeństwa lub integralności komunikacji elektronicznej. Incydent cyberbezpieczeństwa oznacza natomiast naruszenie bezpieczeństwa informacyjnego w systemie informatycznym lub naruszenie bezpieczeństwa usług lub integralności sieci komunikacji elektronicznej wynikające ze zdarzenia w zakresie cyberbezpieczeństwa.

Władze publiczne oraz administratorzy krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej i kluczowych systemów informatycznych są obowiązani wykrywać zdarzenia z zakresu cyberbezpieczeństwa (§ 7 ust. 3). Przepis § 8 ust. 1 nakłada na władze publiczne oraz osoby fizyczne i prawne administrujące kluczowymi sieciami, administratorów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej i kluczowych systemów informatycznych obowiązek raportowania o incydentach cyberbezpieczeństa natychmiast po ich wykryciu, przy czym raporty od władz publicznych oraz podmiotów administrujących sieciami kluczowymi powinny być kierowane do krajowego CERT-u (ust. 2), a od pozostałych podmiotów – do Krajowej Władzy Bezpieczeństwa (ust. 3).

Krajowy Urząd Bezpieczeństwa jest obowiązany przechowywać dokumentację dotyczącą incydentów cyberbezpieczeństwa, a także udostępniać ją innym władzom publicznym, jeśli jest im potrzebna do wykonywania ustawowych obowiązków. Może też udostępniać tę dokumentację krajowemu CERT-owi oraz innym krajowym i zagranicznym podmiotom wykonującym zadania w obszarze cyberbezpieczeństwa, w zakresie niezbędnym do ochrony cyberprzestrzeni (§ 9).

Przepis § 11 ust. 1 definiuje środki jako działania niezbędne w celu ochrony systemów informacyjnych lub usług i sieci komunikacji elektronicznej przed zagrożeniami na polu cyberbezpieczeństwa lub przed incydentami cyberbezpieczeństwa oraz działania mające na celu neutralizację już występującego incydentu cyberbezpieczeństwa.

Ustęp 2 dzieli środki na ostrzeżenia, środki reakcji i środki ochronne. Stosownie do ust. 3 środki reakcji są obligatoryjnie stosowane przez administratorów systemów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej oraz kluczowej infrastruktury informatycznej. Natomiast dostawcy usług i sieci komunikacji elektronicznej, a także władze publiczne oraz osoby fizyczne i prawne administrujące sieciami kluczowymi, wdrażają je w stanie cyberzagrożenia.

Środki ochronne są obligatoryjnie stosowane przez administratorów systemów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej oraz kluczowej infrastruktury informatycznej.

Ostrzeżenia są wydawane przez Krajową Władzę Bezpieczeństwa w sytuacji zaistnienia zagrożenia cyberbezpieczeństwa. Wiedza o zaistnieniu zagrożenia może pochodzić z ustaleń własnych albo zostać przekazana przez krajowy CERT lub odpowiednie organy innych państw. Ostrzeżenia są publikowane na stronie internetowej i doręczane podmiotom obowiązanym, wskazanym w § 3 ustawy.

Środki reakcji natomiast są wdrażane przez podmioty obowiązane na podstawie decyzji administracyjnej, wydawanej przez Krajową Władzę Bezpieczeństwa, w celu przeciwdziałania skutkom incydentu cyberbezpieczeństwa lub zabezpieczenia systemów informatycznych oraz sieci komunikacji elektronicznej przed incydentem. Taka decyzja jest niezwłocznie doręczana podmiotom obowiązanym i natychmiast wykonalna – ewentualne odwołanie nie powoduje zawieszenia wykonalności. Krajowy Urząd Bezpieczeństwa może również zarządzać wdrożenie środków reakcji o charakterze generalnym – bez wskazywania konkretnych adresatów decyzji. W takim trybie wyżej wymieniony Urząd nakazuje również stosowanie środków ochronnych w celu zwiększenia ochrony systemów informatycznych lub sieci i usług komunikacji elektronicznej, na podstawie analizy zakończonego już incydentu cyberbezpieczeństwa. Środki o charakterze generalnym obowiązują od chwili publikacji przez Krajową Władzę Bezpieczeństwa stosownego ogłoszenia.

1.3. Instytucje systemu cyberbezpieczeństwa

Główną instytucją systemu cyberbezpieczeństwa Republiki Czeskiej, według pierwotnej wersji ustawy Nr 181/2014, był Krajowy Urząd Bezpieczeństwa (Národní bezpečnostní úřad – NBU). O roli tego urzędu w obszarze cyberbezpieczeństwa stanowił rozdział IV – *Wykonywanie administracji państwowej*, zawierający tylko jeden paragraf – 22. Ustęp 1 tego paragrafu tworzył domniemanie kompetencji na rzecz NBU, wskazując, że ten urząd wykonuje zadania administracji państwowej w obszarze cyberbezpieczeństwa, chyba że przepisy odrębne stanowią inaczej. Do zadań administracyjnych NBU w obszarze cyberbezpieczeństwa ustawa w § 22 ust. 2 zaliczała: określanie środków bezpieczeństwa, wydawanie środków zaradczych, zapewnianie działania Narodowego Centrum Cyberbezpieczeństwa, przechowywanie rekordów na temat zdarzeń cyberbezpieczeństwa, nakładanie kar administracyjnych, pełnienie funkcji koordynacyjnych podczas stanu cyberzagrożenia, współpracę z władzami publicznymi oraz osobami fizycznymi i prawnymi działającymi w obszarze cyberbezpieczeństwa, jednostkami badawczo-rozwojowymi, innymi jednostkami typu CERT, zapewnianie współpracy międzynarodowej, w tym negocjowanie i zawieranie porozumień międzynarodowych, zapewnianie prewencji, edukacji i metodycznego wsparcia w obszarze cyberbezpieczeństwa, prowadzenie badań i rozwoju w obszarze cyberbezpieczeństwa, zawieranie kontraktu prawa publicznego z administratorem krajowego CERT-u, przekazywanie ministrowi spraw wewnętrznych propozycji określenia elementów infrastruktury krytycznej w obszarze komunikacji i systemów informacyjnych w zakresie cyberbezpieczeństwa, jeśli ich administrator jest państwową jednostką organizacyjną, oraz uznawanie innych systemów informatycznych i komunikacyjnych za elementy infrastruktury krytycznej zgodnie z ustawą o zarządzaniu kryzysowym, a także wykonywanie innych, przewidzianych prawem zadań.

Rządowy CERT, zgodnie z § 20, stanowił część składową Krajowej Władzy Bezpieczeństwa. W zakresie zadań rządowego CERT-u znalazło się m.in. przyjmowanie raportów na temat incydentów cyberbezpieczeństwa od administratorów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej i kluczowych systemów informatycznych, dokonywanie oceny zdarzeń i incydentów cyberbezpieczeństwa, które wystąpiły w obszarze krytycznej infrastruktury informatycznej, kluczowych systemów informatycznych oraz innych systemów administracji publicznej,

zapewnianie metodycznego wsparcia dla administratorów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej i kluczowych systemów informatycznych, współpraca z tymi podmiotami podczas incydentów i zdarzeń cyberbezpieczeństwa, otrzymywanie danych od podmiotów istotnych w obszarze cyberbezpieczeństwa i analiza tych danych oraz prowadzenie analiz podatności w obszarze cyberbezpieczeństwa.

Zadania krajowego CERT-u zostały określone w § 17. Zgodnie z ust. 1 tego przepisu głównym zadaniem CERT-u jest zapewnianie wymiany informacyjnej w zakresie cyberbezpieczeństwa na szczeblu krajowym i zagranicznym.

Zadania przypisane administratorowi CERT-u, określone w ustępie 2 tego przepisu, to m.in.: przyjmowanie raportów na temat incydentów cyberbezpieczeństwa od administratorów sieci kluczowych oraz dokonywanie ich ewaluacji, dostarczanie podmiotom administrującym sieciami kluczowymi oraz dostawcom usług i sieci łączności elektronicznej metodycznego wsparcia, pomocy i współpracy, w sytuacji wystąpienia incydentu cyberbezpieczeństwa, działanie jako punkt kontaktowy dla tych podmiotów, prowadzenie analiz podatności w zakresie cyberbezpieczeństwa, przekazywanie do Krajowej Władzy Bezpieczeństwa danych dotyczących incydentów cyberbezpieczeństwa bez ujawniania osób zgłaszających, w czasie stanu cyberzagrożenia zaś – udostępnianie Krajowej Władzy Bezpieczeństwa danych kontaktowych dostawców usług i sieci łączności elektronicznej i administratorów sieci kluczowych.

Jak wynika z powyższego, CERT krajowy i CERT rządowy wykonują dość podobne zadania administracyjne wobec odmiennych grup podmiotów obowiązanych na podstawie ustawy. CERT krajowy przyjmuje raporty o incydentach od administratorów sieci kluczowych, natomiast CERT rządowy – od administratorów krytycznej infrastruktury informatycznej, krytycznej infrastruktury komunikacyjnej i kluczowych systemów informatycznych. Wykonując swoje zadania, administrator krajowego CERT -u był zobowiązany koordynować swoją działalność z Krajową Władzą Bezpieczeństwa i zachować bezstronność w działaniach. Dopuszczalne jest natomiast prowadzenie przez niego działalności gospodarczej w zakresie cyberbezpieczeństwa, jeśli daje się ona pogodzić z zadaniami statutowymi.

Przepis § 18 określa wymogi wobec administratora krajowego CERT-u. Zgodnie z ust. 1 wskazanego przepisu administratorem CERT-u może zostać wyłącznie osoba prawna, spełniająca warunki określone w ust. 2, która zawarła kontrakt prawa publicznego z Krajową Władzą Bezpieczeństwa. Przepis ust. 2 stanowi, że administratorem krajowego CERT-u może być jedynie osoba prawna, która spełnia wymogi określone w ustawie o ochronie informacji niejawnych odnośnie do nieprowadzenia działalności skierowanej przeciwko Republice Czeskiej, legitymująca się co najmniej pięcioletnim doświadczeniem w zakresie operowania i administrowania systemami lub usługami i sieciami komunikacji elektronicznej, posiadająca bazę techniczną do wykonywania zadań CERT-u, będąca członkiem organizacji międzynarodowej zajmującej się cyberbezpieczeństwem, niemająca zaległości podatkowych oraz spełniająca wymóg niekaralności – w rozumieniu ustawy o odpowiedzialności karnej osób prawnych. Administrator CERT-u nie może być również osobą prawną prawa obcego ani też stworzoną jedynie w celu zdobycia zysku.

Wybór administratora krajowego CERT-u odbywa się w trybie określonym przepisami kodeksu postępowania administracyjnego. Ze zwycięzcą postępowania selekcyjnego Krajowy Urząd Bezpieczeństwa podpisuje kontrakt prawa publicznego (§ 19).

1.4. Stan cyberzagrożenia

Niewątpliwie ciekawą instytucją zawartą w omawianej ustawie jest stan cyberzagrożenia, któremu poświęcono rozdział III części pierwszej, obejmujący tylko jeden paragraf – 21. Zgodnie z zawartą w ust. 1 tego przepisu definicją, jest to stan, w którym bezpieczeństwo informacyjne w systemach informacyjnych lub bezpieczeństwo i integralność usług i sieci komunikacji elektronicznej są poważnie zagrożone oraz występuje ryzyko naruszenia lub zagrożenia interesów Republiki Czeskiej, stosownie do przepisów ustawy o ochronie informacji niejawnych.

Zgodnie z ust. 2 stan cyberzagrożenia wprowadza dyrektor Krajowej Władzy Bezpieczeństwa, ogłaszając publicznie swoją decyzję, również w środkach masowego przekazu. Decyzja o ogłoszeniu stanu cyberzagrożenia wchodzi w życie w momencie wskazanym w jej treści, i obowiązuje przez czas w niej określony, nieprzekraczający siedmiu dni. Istnieje możliwość przedłużania stanu cyberzagrożenia na kolejne okresy, jednak całkowity czas jego trwania nie może przekroczyć 30 dni.

Podczas trwania stanu cyberzagrożenia dyrektor Krajowej Władzy Bezpieczeństwa jest obowiązany informować rząd o wdrożonych procedurach mających na celu neutralizację cyberzagrożeń oraz o aktualnym poziomie zagrożeń, które doprowadziły do ogłoszenia stanu cyberzagrożenia. Krajowy Urząd Bezpieczeństwa mógł wydawać decyzje i stosować środki o charakterze generalnym również w stosunku do dostawców sieci i usług komunikacji elektronicznej oraz administratorów kluczowych sieci (ust. 4). Stan cyberzagrożenia nie powinien być ogłaszany, jeśli NBU byłaby zdolna do neutralizacji zagrożenia bezpieczeństwa informacji w systemach informatycznych oraz bezpieczeństwa usług lub bezpieczeństwa i integralności sieci komunikacji elektronicznej za pomocą swoich zwykłych ustawowych kompetencji (ust. 5).

Jeśli natomiast odwrócenie skutków zagrożenia bezpieczeństwa informacji w systemach informatycznych oraz bezpieczeństwa usług lub bezpieczeństwa i integralności sieci komunikacji elektronicznej przy użyciu oprzyrządowania prawnego, dotyczącego stanu cyberzagrożenia, okazałoby się niemożliwe, to dyrektor NBU jest zobowiązany do niezwłocznego wystąpienia do rządu o ogłoszenie stanu wyjątkowego. W przypadku ogłoszenia stanu wyjątkowego decyzje i środki podjęte uprzednio przez dyrektora NBU pozostają w mocy do momentu zastąpienia ich przez środki zastosowane przez rząd na podstawie przepisów o stanie wyjątkowym (ust. 6).

Zakończenie stanu cyberzagrożenia ma miejsce w terminie określonym w decyzji o jego ogłoszeniu, chyba że dyrektor NBU zadecydował o jego wcześniejszym zakończeniu albo jeśli ogłoszono stan wyjątkowy (ust. 7).

1.5. Systemy teleinformatyczne policji i służb specjalnych

Przytoczenia wymaga jeszcze przepis § 33 omawianej ustawy, zawarty w rozdziale VI jej części pierwszej, w podtytule: *Przepisy wspólne*. Określa on zastosowanie ustawy do systemów informacyjnych i komunikacyjnych służb wywiadowczych i policji. Do systemów służb wywiadowczych spełniających kryteria ustanowienia krytycznej infrastruktury komunikacyjnej stosuje się odpowiednio § 4 ustawy dotyczący środków bezpieczeństwa, jednak te systemy nie są ujmowane w spisie infrastruktury krytycznej. Podobne rozwiązanie ma miejsce w odniesieniu do Systemu Informacji Policji Republiki

Czeskiej, wykorzystywanego do działań analitycznych w ramach postępowania karnego, chyba że ten system stanowi krytyczną infrastrukturę informacyjną[3].

2. Reforma systemu cyberbezpieczeństwa – stan prawny po 1 sierpnia 2017 r.

W ostatnim czasie miała miejsce poważna reforma instytucjonalna systemu cyberbezpieczeństwa Republiki Czeskiej, związana z uchwaleniem ustawy nr 205/2017 z 7 czerwca 2017 r. o zmianie ustawy nr 181/2014 o cyberbezpieczeństwie i o zmianie niektórych innych ustaw (ustawa o cyberbezpieczeństwie), o zmianie ustawy nr 104/2017 i niektórych innych ustaw[4]. Wskazana nowelizacja ustawy o bezpieczeństwie cybernetycznym została wprowadzona przede wszystkim ze względu na konieczność implementacji *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dz. Urz. UE L z 2016 r. nr 194, s. 1)[5].

Zgodnie z postanowieniami wskazanej ustawy z dniem 1 sierpnia 2017 r. zaczął funkcjonować nowy urząd – Krajowy Urząd ds. Cyberbezpieczeństwa i Bezpieczeństwa Informacji (ang. National Cyber and Information Security, czes.: Národní úřad pro kybernetickou a informační bezpečnost – NUKIB),

Do głównych zadań nowego urzędu zalicza się:

- zapewnienie działania CERT- rządowego (GocCERT.cz),
- współpracę z krajowymi zespołami CERT i zespołami CSIRT,
- współpracę z zagranicznymi zespołami CERT i zespołami CSIRT,
- wypracowywanie standardów dla systemów informatycznych infrastruktury krytycznej i infrastruktury kluczowej,
- wspieranie edukacji w zakresie cyberbezpieczeństwa,
- badania i rozwój w obszarze cyberbezpieczeństwa,
- ochronę informacji niejawnych w obszarze systemów informacyjnych i komunikacyjnych,
- ochronę kryptograficzną[6].

Nowo powołany urząd przejął zatem uprawnienia administracyjne Narodowego Urzędu Bezpieczeństwa (NBU) w odniesieniu do sfery cyberbezpieczeństwa. Ma sprawować nadzór nad ochroną systemów infrastruktury krytycznej, odbierać raporty o incydentach i być koordynatorem działań w przypadku zagrożeń cybernetycznych. Siedzibą nowego urzędu ma być Brno[7].

Najważniejsze pozostałe zmiany wprowadzone do ustawy o cyberbezpieczeństwie ustawą nr 205/2017 to:

- wprowadzenie w § 2 nowych definicji: m.in. usługi podstawowej i usługi cyfrowej,
- wprowadzenie w § 3 nowych podmiotów odpowiedzialnych: administratora i operatora systemu informatycznego usług podstawowych oraz dostawcy usług cyfrowych,

[3] https://www.govcert.cz/download/legislation/container-nodeid-1122/actoncybersecuritypopsp.pdf [dostęp: 5 IX 2017].

[4] https://www.govcert.cz/en/ [dostęp: 10 IX 2017].

[5] https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2541-zacatkem-srpna-dojde-u-nckb-k-zasadni-zmene/ [dostęp: 19 IX2017].

[6] https://www.govcert.cz/en/ [dostęp: 10 IX 2017].

[7] https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2541-zacatkem-srpna-dojde-u-nckb-k-zasadni-zmene/ [dostęp: 19 IX 2017].

- wprowadzenie w § 4 nowej regulacji odpowiedzialności stron w ramach zawierania umów między organami władz publicznych a dostawcami tzw. *cloud computing* (przetwarzania danych w chmurze),
- wprowadzenie nowych obowiązków informacyjnych organów i osób odpowiedzialnych (§ 4a),
- rozszerzenie zadań podmiotów obowiązanych przy zdarzeniach i incydentach z zakresu cyberbezpieczeństwa (§ 7 i 8),
- wprowadzenia regulacji udzielania informacji w zakresie bezpieczeństwa publicznego (§ 10a),
- rozszerzenie uprawnień krajowego CERT (§ 17),
- rozszerzenie uprawnień rządowego CERT (§ 20),
- powołanie nowego centralnego organu administracji państwowej – Narodowego Urzędu ds. Cyberbezpieczeństwa i Bezpieczeństwa Informacyjnego oraz określenie jego praw i obowiązków (§ 21a – § 24b),
- nowa regulacja wykroczeń administracyjnych i kar za nie (§ 25 – § 27).

Spośród nowych definicji wprowadzonych ustawą nowelizującą omówienia wymaga pojecie usługa podstawowa (§ 2 lit. i). Zostało ono zdefiniowane jako posiadające trzy cechy konstytutywne:

1) zabezpiecza działalność społeczną lub gospodarczą w jednej z dziedzin wskazanych w ustawie (energetyka, transport, bankowość, infrastruktura rynków finansowych, służba zdrowia, gospodarka wodna, infrastruktura cyfrowa i przemysł chemiczny),
2) jest udostępniana w sieciach komunikacji elektronicznej lub systemach informatycznych,
3) naruszenie sieci komunikacji elektronicznej lub systemów informatycznych, w których ta usługa jest udostępniana, mogłoby mieć znaczny wpływ na bezpieczeństwo społeczne lub ekonomiczne.

Z tym pojęciem łączą się pojęcia: system informatyczny usług podstawowych (§ 2 lit. j) oraz operator usług podstawowych (§ 2 lit. k)[8].

3. Podsumowanie

Republika Czeska jest przykładem kraju mającego uporządkowany i scentralizowany system cyberbezpieczeństwa. Wyrazem tego jest uregulowanie przedmiotowego zagadnienia jedną, kompleksową ustawą oraz powierzenie kompetencji administracyjnych w tym obszarze jednemu wyspecjalizowanemu organowi państwowemu. W tym systemie nie przewidziano żadnej istotnej roli dla służb specjalnych, natomiast rolę organu odpowiedzialnego za cyberbezpieczeństwo powierzono Krajowej Władzy Bezpieczeństwa (Narodowemu Urzędowi Bezpieczeństwa – NBU), która w Republice Czeskiej jest odrębnym urzędem administracji. Taki rozdział kompetencji miał miejsce do 1 sierpnia 2017 r., kiedy to zaczęła działać wyspecjalizowana agencja – Narodowy Urząd ds. Cyberbezpieczeństwa i Bezpieczeństwa Informacji NUKIB, odpowiedzialna jedynie za bezpieczeństwo informatyczne i telekomunikacyjne.

[8] https://www.psp.cz/sqw/sbirka.sqw?cz=205&r=2017 [dostęp: 15 IV 2017].

III. GRECJA

Republika Grecka najważniejszą rolę w swoim systemie cyberbezpieczeństwa przyznała cywilnej służbie specjalnej – Narodowej Służbie Wywiadu (ang. National Intelligence Service – NIS, gr. EYP), do której zadań, oprócz zadań informacyjnych, prowadzenia wywiadu i kontrwywiadu, zaliczają się sprawy techniczne: pełnienie funkcji Władzy Technicznej w zakresie Bezpieczeństwa Informacyjnego – INFOSEC oraz Krajowej Władzy ds. Przeciwdziałania Atakom Elektronicznym[9].

Przypisanie tych funkcji NIS zostało dokonane w art. 4 ustawy nr 3649 – *Narodowa Służba Wywiadu i inne przepisy* (Dz. Urz. Republiki Greckiej Nr 39 z 3 marca 2008 r.), regulującym kompetencje służby. Przepis art. 4 ust. 7 stanowi, że EYP pełni w kraju funkcję *Władzy Technicznej w zakresie Bezpieczeństwa Informacyjnego – INFOSEC*. W tym zakresie EYP zapewnia bezpieczeństwo krajowych systemów informacyjnych i komunikacyjnych. Prowadzi również certyfikację urządzeń służących do ochrony informacji niejawnych. Za dokonanie certyfikacji pobiera opłatę, której wysokość jest określona we wspólnej uchwale ministrów: spraw wewnętrznych oraz gospodarki i finansów.

Na mocy art. 4 ust. 8 ustawy nr 3649 EYP pełni także funkcję Krajowej Władzy ds. Przeciwdziałania Atakom Elektronicznym (ang.: National Authority Against Electronic Attacks – NAAEA), czyli krajowego CERT-u. Zadaniem EYP w tym zakresie jest zapobieganie, a także pasywne i aktywne przeciwdziałanie atakom elektronicznym, skierowanym przeciwko sieciom komunikacyjnym, infrastrukturze służącej do przechowywania danych i systemom komputerowym[10].

Według dostępnych informacji na temat misji NAAEA obejmuje ona przede wszystkim ochronę przed atakami jednostek sektora publicznego oraz krajowej infrastruktury krytycznej. NAAEA wykorzystuje odpowiedni sprzęt oraz zatrudnia wykwalifikowany personel niezbędny do prowadzenia działań, w tym do implementacji strategicznych rodzajów polityki cyberbezpieczeństwa odnoszących się do przeciwdziałania zagrożeniom i atakom oraz zbierania, przetwarzania i dystrybuowania informacji ich dotyczących. W celu zwiększenia efektywności realizacji swojej misji Krajowa Władza Przeciwdziałania Atakom Elektronicznym współpracuje z zagranicznymi zespołami CERT oraz innymi właściwymi organami i służbami[11].

IV. FRANCJA

Wstęp[12]

Zadania w sferze cyberbezpieczeństwa realizowane są we Francji przez cztery organy: Narodową Agencję Bezpieczeństwa Systemów Informatycznych (Agence nationale de la sècurité des systèmes d'information – ANSSI) podlegającą premierowi, Sztab Generalny

[9] http://www.nis.gr/portal/page/portal/NIS/Competences [dostęp: 4 IX 2017].

[10] http://www.nis.gr/npimages/docs/LAW_NUMBER%203649_en.pdf [dostęp: 4 IX 2017].

[11] http://www.nis.gr/portal/page/portal/NIS/NCERT [dostęp: 19 IX 2017].

[12] Ogólna charakterystyka instytucjonalna została opracowana na podstawie dokumentu *Pour une véritable politique publique du renseignement*, Sebastian-Yves Laurent, Institut Montaigne, juillet 2014, www.institutmontaigne.org/res/files/publications/Etude renseignement juillet 2014.pdf, s. 41–45 [dostęp: 10 VIII 2017].

Sił Zbrojnych (l'État major des armées – EMA), Generalną Dyrekcję Uzbrojenia (Direction Générale de l'armement – DGA) oraz w zakresie wywiadu elektronicznego – Generalną Dyrekcję Bezpieczeństwa Zewnętrznego (Direction Générale de la Sécurité Extérieure – DGSE). System ten ma zatem charakter mieszany, składający się zarówno z instytucji cywilnych, jak i wojskowych. Zadania realizowane przez najistotniejszy z punktu widzenia niniejszego opracowania organ – ANSSI, należy ocenić jako wyłącznie defensywne.

Punktem wspólnym opisanych dalej strategicznych dokumentów dotyczących cyberbezpieczeństwa oraz dokumentów analitycznych, tworzonych przez niezależnych ekspertów, jest podkreślenie znaczenia gospodarczego wymiaru cyberbezpieczeństwa i potencjalnych skutków, jakie mógłby wywołać ewentualny atak informatyczny na systemy wykorzystywane przez najważniejsze przedsiębiorstwa. W raporcie Instytutu Montaigne podkreślono, że francuskie podmioty gospodarcze odgrywają istotną rolę w produkcji i eksportcie technologii związanych ze sferą cyberbezpieczeństwa – m.in. Airbus Defence and Space, Thales, Atos czy Sogeti. W dokumencie podkreślono rosnącą rolę partnerstwa publiczno-prywatnego oraz wskazano na sprzyjające uwarunkowania strukturalne, które mogą przyczynić się do zwiększenia ogólnej skuteczności systemu cyberbezpieczeństwa – wzrost świadomości organów państwa, wysoki poziom szkolnictwa wyższego w matematyce i informatyce, a także szybki rozwój sektora prywatnego w sferze nowych technologii. Należy także zauważyć, że potrzeby Francji dotyczące stworzenia skutecznych instrumentów przeciwdziałania i reagowania na zagrożenia cybernetyczne są większe niż w przypadku pozostałych państw europejskich (z wyjątkiem Wielkiej Brytanii) z uwagi na posiadanie technologii pozwalających na wykorzystywanie energii nuklearnej, zarówno w wymiarze cywilnym, jak i wojskowym.

1. Charakterystyka ewolucji systemu cyberbezpieczeństwa na podstawie najważniejszych aktów normatywnych i dokumentów programowych na przestrzeni lat 2008–2017[13]

Biała Księga Obrony i Bezpieczeństwa Narodowego z 2008 r.[14]

Biała księga z 2008 r. określiła zagrożenia związane z atakami informatycznymi wymierzonymi w najważniejsze elementy infrastruktury państwa jako jedno z najbardziej prawdopodobnych zagrożeń na przestrzeni kolejnych 15 lat. Wskazała równocześnie na wiążące się z tego rodzaju zdarzeniem poważne skutki dla funkcjonowania społeczeństwa i wszystkich aspektów życia publicznego. Dokument określa instrumenty informatyczne i komunikacyjne jako system nerwowy społeczeństwa, bez którego jego prawidłowe funkcjonowanie byłoby niemożliwe. Ponadto, w sposób wykładniczy wzrasta uzależnienie wszystkich elementów składowych społeczeństwa od nowych technologii oraz usług społeczeństwa informacyjnego. Warto podkreślić, że biała księga z 2008 r. była pierwszym oficjalnym dokumentem, w której zagrożenia w cyberprzestrzeni określono mianem „poważnych" i jako ich potencjalne formy wymieniono m.in. działalność polegającą na atakach hakerskich czy zorganizowaną przestępczość.

[13] Opracowano na podstawie informacji zawartych na stronie www.ssi.gouv.fr/agence/cybersecurite/ssi-en-france/ [dostęp: 10 VIII 2017].

[14] *Défense et Sècurité nationale. Le Livre Blanc*, 2008, http://archives.livreblancdefenseetsecurite.gouv.fr/2008/IMG/pdf/livre_blanc_tome1_partie1.pdf [dostęp: 16 VIII 2017].

Autorzy dokumentu zwracają uwagę na różnorodność zagrożeń bezpieczeństwa w cyberprzestrzeni. Należą do nich m.in. blokowanie prawidłowego działania najważniejszych elementów infrastruktury informatycznej, możliwość ich fizycznego zniszczenia (np. satelitów czy newralgicznych elementów sieci informatycznych), kradzież danych, a także wrogie przejęcie kontroli nad określonym urządzeniem. Skalę zagrożeń potęguje sukcesywne tworzenie przez inne państwa ofensywnych strategii walki w cyberprzestrzeni i nabywanie coraz bardziej zaawansowanych instrumentów technologicznych w tym zakresie. Ataki prowadzone z wykorzystaniem tych metod mogą mieć zarówno charakter otwarty, jak i zamaskowany.

Biorąc pod uwagę ewolucję technologiczną i coraz większy stopień powiązań między poszczególnymi sieciami i urządzeniami, strategia cyberbezpieczeństwa – oparta wyłącznie na pasywnych instrumentach ochronnych, mimo że w dalszym ciągu są one ważne – nie może w pełni odpowiadać na nowe rodzaje zagrożeń. Te uwarunkowania sprawiają, że konieczne jest stopniowe przekształcenie strategii defensywnej w strategię aktywnej obrony, łączącej w sobie ochronę systemów i nadzór nad ich funkcjonowaniem z możliwościami szybkiej reakcji i działań ofensywnych, jeżeli zajdzie ku temu potrzeba. Ta ewolucja nie będzie jednak możliwa bez odpowiednich działań w wymiarze politycznym i zmiany w sposobie myślenia o problemach związanych z cyberbezpieczeństwem. Właściwe organy państwa powinny pełnić funkcję katalizatora tych modyfikacji przez wspieranie rozwoju wiedzy eksperckiej i udzielanie niezbędnego wsparcia zarówno podmiotom gospodarczym, jak i operatorom sieci informatycznych.

Charakter zagrożeń związanych z cyberprzestrzenią, ich nieprzewidywalność i szybkość wydarzeń wymagają stworzenia zdolności reagowania kryzysowego, zarówno na etapie faktycznego wystąpienia danego zagrożenia, jak i w fazie usuwania jego skutków, co zagwarantuje ciągłość działań sieci dotkniętych atakiem oraz pomoże wykryć osoby odpowiedzialne za tego typu działania. Te czynniki sprawiają, że cyberprzestrzeń należy uznać za nowe pole działań, w którym mogą być prowadzone czynności o charakterze wojskowym. W konsekwencji, niezbędne jest wypracowanie odpowiednich metod postępowania, które można porównać do funkcjonującego w sferze wojskowej angielskiego terminu „*rules of engagement*" (zasada podejmowania działań przy użyciu siły), obejmującego zbiór zasad określających w sposób szczegółowy okoliczności i sposób prowadzenia działań związanych z użyciem instrumentów wojskowych[15].

Główne tezy białej księgi z 2008 r. sprowadzają się do stwierdzenia, że państwo powinno wypracować instrumenty pozwalające na skuteczne zwalczanie zagrożeń w cyberprzestrzeni – cel ten powinien stać się jednym z priorytetów Francji w sferze bezpieczeństwa narodowego. W dokumencie podkreślono konieczność wypracowania zdolności wczesnego wykrywania ataków informatycznych i reagowania na incydenty mające charakter zarówno ściśle ukierunkowany na określone sieci czy urządzenia, jak i na działania o charakterze masowym. Natomiast w sferze zapobiegania zagrożeniom zaproponowano w białej księdze wykorzystywanie urządzeń i sieci mających wysoki stopień zabezpieczeń i stworzenie katalogu kompetencji oraz instrumentów, którymi w razie zagrożenia mogłyby się posługiwać zarówno organy administracji publicznej, jak i tzw. operatorzy infrastruktury krytycznej (fr. *opérateurs d'infrastructures vitales*).

Jednym z działań wdrażającym założenia przedstawione w białej księdze było powołanie, na podstawie dekretu nr 2008-934 z 7 lipca 2009 r.[16], Narodowej Agencji

[15] Tamże, s. 53.

[16] *Décret n° 2009-834 du 7 juillet 2009 portant creation d'un service à competence nationale dénommé*

Bezpieczeństwa Systemów Informatycznych – wyspecjalizowanego organu administracji publicznej pełniącego funkcję narodowej władzy bezpieczeństwa systemów informatycznych. Zapisy dekretu o utworzeniu ANSSI były również podstawą do powołania Komitetu Strategicznego ds. Bezpieczeństwa Systemów Informacji (fr. *comité stratégique de la SSI*), którego celem było opracowanie narodowej strategii bezpieczeństwa systemów informacji.

Strategia Francji w zakresie ochrony i bezpieczeństwa systemów informacji (strategia SSI) z 2011 r.[17]

Główne założenia strategii SSI są kontynuacją najważniejszych tez zawartych w białej księdze z 2008 r. W dokumencie wymieniono cztery cele strategiczne, do których osiągnięcia mają zmierzać działania podejmowane w sferze cyberbezpieczeństwa. Są nimi:

1. Uzyskanie statusu mocarstwa w sferze cyberobrony.

Francja powinna dążyć do przynależności do ograniczonej grupy państw mających najbardziej rozwinięte zdolności w sferze cyberobrony, zachowując jednocześnie wysoki stopień autonomii w wymiarze strategicznym. W dokumencie zwraca się uwagę na ścisły związek między tymi kompetencjami a pozycją państwa na arenie międzynarodowej – rozwój społeczeństwa informacyjnego i sieci komunikacji elektronicznej jest elementem istotnie przyczyniającym się do wzrostu gospodarczego i poprawy konkurencyjności francuskich podmiotów gospodarczych. Skuteczna ochrona sieci informatycznych jest niezbędna z uwagi na intensyfikację działań wywiadowczych prowadzonych przez inne państwa, których celem jest uzyskanie dostępu do informacji istotnych dla zachowania suwerenności państwa (m.in. informacji niejawnych dotyczących obronności, badań naukowych, technologii, informacji finansowych czy handlowych).

W przeciwieństwie do tradycyjnych konfliktów zbrojnych działania w cyberprzestrzeni nie są ograniczone granicami uczestniczących w nich państw. W konsekwencji, skuteczny system cyberobrony nie może mieć wymiaru wyłącznie narodowego i musi opierać się na ścisłej współpracy z właściwymi organami innych państw, pozwalającej na prowadzenie w czasie rzeczywistym wymiany informacji o potencjalnych zagrożeniach, atakach i możliwych do zastosowania środkach przeciwdziałania skutkom tych zdarzeń.

2. Zagwarantowanie autonomii decyzyjnej przez ochronę informacji istotnych z punktu widzenia suwerenności Francji.

Ten cel jest ściśle powiązany z dwoma aspektami niezwykle istotnymi dla systemu cyberbezpieczeństwa: ogólnymi celami polityki kontrwywiadowczej państwa oraz rozwojem zdolności technologicznych w zakresie bezpieczeństwa informacji. Informacje mające największe znaczenie strategiczne zostały w dokumencie określone jako informacje istotne dla zachowania suwerenności (fr. *l'information de souveraineté*), których prawidłowa ochrona jest warunkiem zachowania suwerenności i autonomii zarówno w polityce wewnętrznej, jak i zagranicznej. Najbardziej efektywnym środkiem zapobiegania nieuprawnionemu uzyskaniu dostępu do tego rodzaju informacji jest stosowanie

"Agence nationale de la sécurité des systèmes d'information", www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212 [dostęp: 10 VIII 2017].

[17] *Défense et sécurité des systèmes d'information – Stratégie de la France*, www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf [dostęp: 11 VIII 2017].

technik kryptograficznych uniemożliwiających lub opóźniających uzyskanie do nich faktycznego dostępu lub zrozumienie ich treści. Obserwowany na przestrzeni ostatnich lat proces stałego zwiększania mocy obliczeniowej komputerów pociąga za sobą znaczny postęp w dziedzinie kryptoanalizy, co wymaga z kolei wykorzystywania coraz bardziej zaawansowanych i wyrafinowanych narzędzi służących do ochrony informacji. Jednym z warunków utrzymania samodzielności decyzyjnej najważniejszych organów jest posiadanie autonomicznych, niezależnych od jakichkolwiek podmiotów zewnętrznych, zdolności oraz technologii w dziedzinach kryptografii i kryptoanalizy.

3. Poprawa cyberbezpieczeństwa najważniejszych elementów infrastruktury krytycznej.

W ustawie – Kodeks obrony[18] określono sektory wchodzące w skład infrastruktury krytycznej, w ramach których działają operatorzy zapewniający: zaspokojenie najważniejszych dla społeczeństwa potrzeb, możliwość sprawowania władzy publicznej, prawidłowe funkcjonowanie systemu gospodarczego, obronnego czy bezpieczeństwa państwa. Rosnące współzależności między sferami gospodarki i informatyki sprawiają, że bezpieczeństwo sieci informatycznych jest jednym z podstawowych warunków utrzymania rozwoju gospodarczego na odpowiednim poziomie. W razie poważnego zakłócenia funkcjonowania sieci telekomunikacyjnych czy Internetu wypracowanie alternatywnych metod wymiany informacji okazałoby się bardzo utrudnione lub niemożliwe, biorąc pod uwagę stale zwiększający się stopień informatyzacji we wszystkich obszarach gospodarki i przemysłu. Z tego względu rozwój nowoczesnych metod reagowania na zagrożenia w cyberprzestrzeni jest jednym z narodowych priorytetów Francji.

4. Zapewnienie bezpieczeństwa w cyberprzestrzeni.

W tym punkcie autorzy strategii zwracają uwagę na społeczny wymiar cyberbezpieczeństwa. Pomimo że zaawansowane ataki informatyczne mające na celu pozyskanie informacji najistotniejszych dla bezpieczeństwa lub gospodarki są jednym z najpoważniejszych zagrożeń strategicznych interesów państwa, należy zwrócić uwagę również na aspekt społeczny i powszechne korzystanie z sieci komunikacji elektronicznej przez większość obywateli. Do potencjalnych zagrożeń należy zatem zaliczyć również takie elementy, jak kradzież tożsamości, haseł do kont bankowych oraz handel bazami zawierającymi dane osobowe. Ponadto, coraz częstszym zjawiskiem jest zdalne przejmowanie kontroli nad urządzeniami informatycznymi przez tzw. botnety. Zadaniem właściwych organów państwa jest zatem zapewnienie odpowiedniego poziomu zaufania do usług świadczonych drogą elektroniczną oraz innych powszechnie wykorzystywanych instrumentów informatycznych. Jednym z przykładów działań pomocnych przy realizacji tego celu było stworzenie w 2010 r. tzw. ogólnego repozytorium bezpieczeństwa (fr. *référentiel général de securité*) – instrumentu służącego zwiększeniu bezpieczeństwa procesu wymiany danych pomiędzy organami publicznymi a obywatelami za pośrednictwem środków komunikacji elektronicznej[19].

Francja zamierza także wspierać wszelkie działania i inicjatywy mające na celu wypracowanie skutecznych instrumentów prawnych regulujących sposób funkcjonowania Internetu i przyczyniające się do zwiększenia efektywności międzynarodowej współpracy dotyczącej ścigania przestępstw cybernetycznych.

---

[18] *Code de la défense*, www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006071307 [dostęp: 16 VIII 2017].

[19] www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/ [dostęp: 16 VIII 2017].

Biała księga obrony i bezpieczeństwa narodowego Francji z 2013 r.[20]

Opublikowanie nowej wersji białej księgi w 2013 r. miało na celu charakterystykę możliwych do podjęcia działań służących przeciwdziałaniu zaobserwowanej na przestrzeni lat 2008–2013 intensyfikacji cyberataków wymierzonych w systemy informatyczne, które były używane przez podmioty gospodarcze, wykorzystujących coraz bardziej zaawansowane metody technologiczne. Ten dokument to punkt zwrotny w procesie wypracowania mechanizmów chroniących infrastrukturę informatyczną przed potencjalnymi zagrożeniami. Twórcy dokumentu uznali, że skala rozwoju cyberzagrożeń oraz ich negatywne implikacje sprawiają, że organy administracji publicznej nie mogą w dalszym ciągu koncentrować się wyłącznie na cyberbezpieczeństwie sfery publicznej. Konieczne jest również uwzględnienie potrzeb podmiotów prywatnych zarządzających najważniejszymi dla interesów państwa sieciami informatycznymi. Ponadto, rozwój ofensywnych zdolności cybernetycznych został uznany za integralną część strategii cyberobrony[21].

W tym dokumencie zwraca się uwagę na kontynuację trendów opisywanych w analogicznym dokumencie z 2008 r. Wzrost zagrożeń połączony z rozwojem technologii wykorzystywanych w cyberatakach i rosnącą rolą społeczną systemów informatycznych sprawia, że posiadanie mechanizmów efektywnie neutralizujących tego rodzaju wyzwania jest jednym z warunków zachowania pełnej suwerenności państwa. W tym kontekście istotne znaczenie ma pełna i autonomiczna zdolność wytwarzania instrumentów służących zapewnieniu bezpieczeństwa sieci – zwłaszcza w sferze kryptologii oraz wykrywania ataków. Rozwój autonomicznych kompetencji w tym zakresie jest jednak warunkowany stworzeniem niezbędnej infrastruktury naukowej, technologicznej i finansowej.

W tym dokumencie zapowiedziano podjęcie działań mających na celu stworzenie ambitnej i komplementarnej polityki w odniesieniu do systemów informatycznych, opartej głównie na dalszym wykorzystywaniu sieci, które cechują się wysokim poziomem zabezpieczeń przez organy publiczne, dostosowaniem polityki zamówień publicznych do potrzeb związanych z cyberbezpieczeństwem oraz prawidłowym zarządzaniem urządzeniami ruchomej łączności. Dopełnieniem tej polityki ma być prowadzenie działań informacyjnych mających na celu zwiększenie świadomości kierowniczych organów administracji terenowej, jednostek samorządu terytorialnego oraz użytkowników sieci. Poprawie musi ulec również bezpieczeństwo dostawców produktów i usług informatycznych.

W odniesieniu do operatorów infrastruktury krytycznej w dokumencie zapowiedziano przyjęcie aktów normatywnych służących określeniu odpowiednich standardów bezpieczeństwa w kontekście ewentualnych zagrożeń cybernetycznych, które pozwolą na weryfikację stosowania przez operatorów niezbędnych środków bezpieczeństwa. Ten akt stworzy również precyzyjny katalog obowiązków podmiotów publicznych i prywatnych dotyczących zasad prowadzenia audytów, powiadamiania ANSSI o strukturze zarządzanych przez nie systemów oraz o wystąpieniu incydentów zagrażających ich bezpieczeństwu.

---

[20] *Défense et Sécurité nationale. Le Livre Blanc*, 2013, www.livreblancdedefenseetsecurite.gouv.fr/pdf/le_livre_blanc_de_la_defense_2013.pdf, s. 105–107 [dostęp: 10 VIII 2017].

[21] P. Brangetto, *National Cyber Security Organisation*: *France, NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn, Estonia, www.ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_FRANCE_032015_0.pdf, s. 8 [dostęp: 14 VIII 2017].

Narodowa doktryna przeciwdziałania atakom cybernetycznym jest oparta na komplementarnych i całościowych działaniach, których podstawą są dwie wzajemnie uzupełniające się części składowe:

1) wypracowanie wydajnych i odpornych na ataki cybernetyczne mechanizmów ochrony systemów informatycznych organów państwowych, operatorów infrastruktury krytycznej oraz strategicznie istotnych przedsiębiorstw, które jest połączone z operacyjną organizacją działań obronnych; te elementy mają być koordynowane przez premiera, wszelkie zaś działania mają być oparte na ścisłej współpracy poszczególnych organów w celu jak najszybszego wykrywania zagrożeń;
2) stworzenie całościowych i dostosowanych do okoliczności zróżnicowanych mechanizmów reagowania działających na zasadzie subsydiarności, które polegają na wykorzystaniu w pierwszej kolejności środków prawnych, dyplomatycznych oraz policyjnych, dopuszczających jednakże możliwość stopniowego stosowania mechanizmów znajdujących się w kompetencji Ministerstwa Obrony, jeżeli będą zagrożone strategiczne interesy państwa.

Biała księga z 2013 r. zwraca również uwagę na konieczność rozwoju zdolności ofensywnych, połączonych z działaniami w sferze wywiadowczej, które wywierają istotny wpływ na możliwości skutecznego reagowania na zagrożenia w cyberprzestrzeni. Te zdolności pozwalają na dokonanie kompleksowej charakterystyki zagrożeń, identyfikację ich źródeł, a także stwarzają możliwości przewidywania wystąpienia zagrożeń cybernetycznych i odpowiedniej konfiguracji metod reagowania. Zdolności o charakterze ofensywnym przyczyniają się do znacznego wzbogacenia katalogu środków pozostających w dyspozycji właściwych organów.

W dokumencie zwraca się również uwagę na istotną rolę współpracy z partnerami zagranicznymi w zakresie cyberbezpieczeństwa (do najważniejszych partnerów zaliczono: Niemcy i Wielką Brytanię). Położono również nacisk na wspieranie procesu wypracowywania wspólnych rozwiązań, mających na celu wzmocnienie ochrony przed zagrożeniami infrastruktury krytycznej i sieci komunikacji elektronicznej na poziomie Unii Europejskiej.

Pakt cyberobrony[22]

W nawiązaniu do ogólnych założeń polityki cyberbezpieczeństwa zawartych w białej księdze z 2013 r. Ministerstwo Obrony przedstawiło zarys analogicznych działań w sektorze wojskowym. Dokument zwraca uwagę na konieczność wypracowania skutecznych mechanizmów ochrony przed atakami cybernetycznymi z uwagi na postępującą informatyzację poszczególnych komponentów sił zbrojnych. Podmioty te wykorzystują zaawansowane i najistotniejsze – pod kątem strategicznym – systemy informatyczne związane m.in. z zarządzaniem instrumentami odstraszania nuklearnego czy zaawansowanymi systemami obronnymi wykorzystywanymi przez wojska lądowe, powietrzne i marynarkę wojenną.

W konsekwencji, bezpieczeństwo cybernetyczne jest jednym z priorytetowych obszarów działań zarówno Ministerstwa Obrony, jak i poszczególnych podmiotów wchodzących w skład francuskich sił zbrojnych. Mimo że ogólna odpowiedzialność

[22] *Pacte Défense Cyber – 50 mesures pour changer d'échelle,* www.defense.gouv.fr/content/download/237708/2704474/file/Pacte%20D%C3%A9fense%Cyber-1.pdf [dostęp: 14 VIII 2017].

za zagwarantowanie bezpieczeństwa systemów informatycznych spoczywa na ANSSI, w razie ewentualnego konfliktu zbrojnego i zaburzenia ciągłości funkcjonowania instytucji państwa te zadania będą realizowane przez podmioty wojskowe. Z tego powodu Ministerstwo Obrony powinno odgrywać pomocniczą rolę zarówno wobec ANSSI, jak i wobec innych podmiotów, do których kompetencji należy przeciwdziałanie zagrożeniom w systemach i sieciach informatycznych (np. jednostek podlegających Ministerstwu Spraw Wewnętrznych odpowiedzialnych za zwalczanie cyberprzestępczości).

Pakt Cyberobrony stanowił dokument określający wszystkie działania, które miały zostać zrealizowane w latach 2014, 2015 i 2016 zgodnie z ustawą o programowaniu wojskowym na lata 2014–2019[23]. Zawiera on środki, które miały zostać podjęte w Ministerstwie Obrony i podległych mu jednostkach, oraz instrumenty mające oddziaływać na sferę zewnętrzną, m.in. w zakresie wspierania jednostek samorządu terytorialnego. Opisane w dokumencie z działania zostały podzielone na sześć głównych tematów:

1) podniesienie poziomu bezpieczeństwa systemów informatycznych oraz wzmocnienie instrumentów ochrony i reagowania wykorzystywanych przez Ministerstwo Obrony i jego najważniejszych partnerów,
2) intensyfikacja działań w sferze badań i rozwoju,
3) właściwe wykorzystanie potencjału ludzkiego i stworzenie spójnego systemu kształcenia i zatrudnienia wyspecjalizowanych kadr,
4) rozwój centrum eksperckiego cyberobrony w Bretanii,
5) rozwój współpracy z partnerami zagranicznymi,
6) wspieranie procesu tworzenia narodowej wspólnoty cyberobrony.

2. Podstawy prawne i struktura organizacyjna systemu cyberbezpieczeństwa

Zgodnie z art. 21 przywołanej powyżej ustawy o programowaniu wojskowym na lata 2014–2019 premier, zgodnie z założeniami strategii bezpieczeństwa narodowego i polityki obrony, określa główne kierunki polityczne i koordynuje działania rządu w zakresie bezpieczeństwa i obrony systemów informatycznych. W tym celu korzysta ze wsparcia narodowej władzy bezpieczeństwa systemów informacji. Jak wskazano we wstępie, tę funkcję pełni powołana na mocy dekretu nr 2009-834 z 7 lipca 2009[24] Narodowa Agencja Bezpieczeństwa Systemów Informatycznych. Organ ten działa przy Sekretarzu Generalnym Obrony i Bezpieczeństwa Narodowego[25]. Do zadań ANSSI, zgodnie z art. 3 dekretu, należy:

- pełnienie funkcji narodowej władzy bezpieczeństwa systemów informatycznych. W tym celu przedkłada ona premierowi propozycje działań zmierzających do reagowania na sytuacje kryzysowe i zagrożenia bezpieczeństwa systemów wykorzystywanych przez organy publiczne, operatorów infrastruktury krytycznej, a także koordynuje, w ramach określonych przez premiera wytycznych, działania rządu w powyższym zakresie;

[23] *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portent diverses dispositions concernant la défense et la sécurité nationale*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&categorieLien=id [dostęp: 14 VIII 2017].

[24] *Décret n° 2009-834 du 7 juillet 2009 portant creation d'un service a competence nationale dénommé "Agence nationale de la sécurité des systèmes d'information"*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020828212 [dostęp: 14 VIII 2017].

[25] Sekretarz Generalny ds. Obrony i Bezpieczeństwa Narodowego wspiera działania premiera w zakresie obrony i bezpieczeństwa narodowego, www.sgdsn.gouv.fr [dostęp: 14 VIII 2017].

- opracowywanie, i wdrażanie międzyresortowych bezpiecznych środków komunikacji elektronicznej wykorzystywanych przez prezydenta i rząd;
- inicjowanie i koordynowanie międzyresortowych działań dotyczących bezpieczeństwa systemów informatycznych;
- opracowywanie środków ochrony systemów informatycznych, które następnie są przedstawiane premierowi, oraz nadzorowanie procesu ich stosowania przyjętych środków;
- prowadzenie inspekcji systemów informatycznych wykorzystywanych przez organy administracji publicznej i operatorów infrastruktury krytycznej;
- opracowywanie systemów wykrywania zdarzeń mogących naruszać bezpieczeństwo państwowych systemów informatycznych oraz koordynacja działań, które mają na celu przeciwdziałanie tym zdarzeniom; zbieranie informacji technicznych o incydentach dotyczących państwowych systemów informatycznych i operatorów infrastruktury krytycznej;
- wydawanie certyfikatów dopuszczających do użytku urządzenia i mechanizmy techniczne chroniące informacje objęte tzw. tajemnicą obrony (fr. *de la défense nationale*);
- udział w negocjacjach międzynarodowych oraz prowadzenie współpracy z zagranicznymi organami pełniącymi analogiczne funkcje;
- prowadzenie działalności szkoleniowej dla osób zajmujących się problematyką bezpieczeństwa systemów informatycznych.

Narodowa Agencja Bezpieczeństwa Systemów Informatycznych dokonuje ponadto oceny poziomu bezpieczeństwa urządzeń i usług niezbędnych do ochrony systemów informatycznych (art. 4). Agencja jest odpowiedzialna przede wszystkim za:

- kwalifikację urządzeń bezpieczeństwa i dostawców usług zaufania; wydawanie upoważnień podmiotom, o których mowa w dekrecie nr 2010-112 z 2 lutego 2010 r.[26] (podmioty dokonujące kwalifikacji dostawców usług zaufania), po dokonaniu oceny kompetencji technicznych tych podmiotów do oszacowania bezpieczeństwa instrumentów stosowanych przez dostawców usług zaufania;
- kwalifikację urządzeń bezpieczeństwa i dostawców usług zaufania, a także zatwierdzanie punktów ewaluacji przewidzianych w dekrecie nr 2015-350 z 27 marca 2015 r. o kwalifikacji urządzeń bezpieczeństwa i dostawców usług zaufania na potrzeby bezpieczeństwa narodowego[27];
- certyfikację urządzeń służących do generowania i weryfikacji podpisów elektronicznych przewidzianych w dekrecie z 30 marca 2001 r. wydanym w celu stosowania art. 1316-4 kodeksu cywilnego i dotyczącym podpisu elektronicznego[28];
- zatwierdzanie punktów ewaluacji i certyfikacji poziomu bezpieczeństwa urządzeń i systemów informatycznych, o których mowa w dekrecie z 18 kwietnia

[26] *Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9,10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relatif aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&categorieLien=cid [dostęp: 14 VIII 2017].

[27] *Décret n° 2015-350 du 27 mars 2015 relatif à la qualification des produits de sécurité et des prestataires de service de confiance pour les besoins de la sécurité nationale*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030405903&categorieLien=cid [dostęp: 14 VIII 2017].

[28] *Décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-14 du code civil et relatif à la signature électronique*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000404810&categorieLien=cid [dostęp: 14 VIII 2017].

2002 r. o ewaluacji i certyfikacji poziomu bezpieczeństwa urządzeń i systemów informatycznych[29];

- wydawanie autoryzacji i zarządzanie deklaracjami dotyczącymi środków i dostawców instrumentów kryptologicznych, o których mowa w dekrecie z 2 maja 2007 r. wydanym w celu stosowania art. 30, 31 i 36 ustawy nr 2004-575 z 21 czerwca 2004 r. o zaufaniu do gospodarki cyfrowej oraz dotyczącym instrumentów kryptologicznych i ich dostarczania[30];
- wydawanie i cofanie zezwoleń, o których mowa w art. 226-3 kodeksu karnego (zezwolenia na produkcję i sprzedaż urządzeń służących do utrwalania treści rozmów i pozyskiwania danych informatycznych).

Dekret nakłada na ANSSI również ogólny obowiązek podejmowania działań mających na celu promocję problematyki związanej z bezpieczeństwem systemów informatycznych w kontekście rozwoju i opracowywania nowych technologii w tej sferze. Agencja bierze ponadto udział w badaniach naukowych mających na celu rozwój potencjału technologii informatycznych (art. 6).

Utworzenie ANSSI oraz opracowanie opisanych powyżej dokumentów strategicznych przyczyniło się do poprawy zdolności skutecznego reagowania na zagrożenia cybernetyczne i uporządkowania kompetencji organów administracji publicznej. Niemniej jednak raport[31] opracowany w 2012 r. pod kierownictwem senatora Jean -Marie'a Bockela wskazuje na występowanie licznych ograniczeń natury systemowej, które są związane zarówno ze sposobem ukształtowania kompetencji i środkami, jakimi dysponuje ANSSI, jak i z innymi aspektami funkcjonowania systemu. Pomimo upływu około pięciu lat od czasu wydania powyższego dokumentu i niewątpliwej poprawy stanu systemu cyberbezpieczeństwa we Francji, zamieszczone w nim zagadnienia oraz problemy natury strukturalnej niewątpliwie zachowują znaczenie do chwili obecnej.

Główna teza raportu Bockela sprowadza się do stwierdzenia, że pomimo niewątpliwych postępów dokonanych od chwili wydania białej księgi w 2008 r., możliwości francuskiego systemu zapobiegania i przeciwdziałania cyberzagrożeniom należy uznać za niesatysfakcjonujące[32]. Z praktycznego punktu widzenia zarówno kompetencje ANSSI, jak i instrumenty pozostające w dyspozycji Agencji są znacznie bardziej ograniczone, niż w przypadku analogicznych instytucji funkcjonujących w innych państwach europejskich, np. w Wielkiej Brytanii czy Niemczech. Zdaniem twórców raportu pomimo że Agencja ma status narodowej władzy bezpieczeństwa w odniesieniu do systemów informatycznych, zakres i sposób uregulowania jej uprawnień nie pozwalają na realne i efektywne zapewnienie jednolitego przestrzegania najważniejszych – z punktu widzenia bezpieczeństwa informatycznego – zasad.

---

[29] *Décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000412673&categorieLien=cid [dostęp: 14 VIII 2017].

[30] *Décret n° 2007-663 du 2 mai 2007 pris pour l'application des articles 30, 31 et 36 de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique et relatif aux moyens et aux prestations de cryptologie*, www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000646995&categorieLien=cid [dostęp: 14 VIII 2017].

[31] *Rapport d'information fait au nom de la commission des affaires étrangères, de la défense et des forces armées sur la cyberdéfense, par M. Jean-Marie BOCKEL, Sénateur*, 18 juillet 2012, https://www.senat.fr/rap/r11-681/r11-6811.pdf [dostęp: 19 IX 2017].

[32] Tamże, s. 82.

Do najistotniejszych wad systemu skutkujących strukturalnymi ograniczeniami możliwości efektywnego realizowania zadań przez ANSSI raport Bockela zalicza niedostateczne środki, jakimi dysponuje Agencja (niedostateczna liczba pracowników i niewystarczający budżet), niski poziom wrażliwości i świadomości w sferze ochrony systemów informatycznych, zarówno w organach administracji publicznej, jak i wśród najważniejszych przedsiębiorców i operatorów infrastruktury krytycznej.

Zagadnienie ochrony systemów informatycznych wykorzystywanych przez operatorów infrastruktury krytycznej zostało określone jako najważniejszy aspekt systemu cyberbezpieczeństwa[33]. To pojęcie, zgodnie z art. R-1332-1 ustawy – Kodeks obrony, obejmuje operatorów publicznych lub prywatnych wskazanych w art. L 1332-1[34] tej ustawy oraz podmioty zarządzające przedsiębiorstwami, o których mowa w art. L 1332-2[35].

Operatorzy infrastruktury krytycznej wykonują zadania zapisane w art. R 1333-2 oraz zarządzają lub wykorzystują w tym celu przedsiębiorstwa, instalacje lub obiekty, których niedostępność lub zniszczenie w wyniku sabotażu, terroryzmu lub innych form szkodliwego działania mogłoby spowodować, bezpośrednio lub pośrednio, obniżenie potencjału gospodarczego lub wojskowego, bezpieczeństwa lub zdolności zachowania podstawowych funkcji społeczeństwa lub stworzyć poważne zagrożenie zdrowia lub życia ludności (art. R 1332-1 II pkt 2 a i b ustawy – Kodeks obrony).

Zgodnie z art. R 1332-2 tej ustawy sektor infrastruktury krytycznej, o którym mowa w art. R 1332-1, obejmuje działania dotyczące produkcji i dystrybucji dóbr lub usług niezbędnych do zaspokojenia podstawowych potrzeb ludności, wykonywania władzy państwowej, funkcjonowania gospodarki, zachowania potencjału obronnego lub bezpieczeństwa państwa, jeżeli ich zastąpienie byłoby niemożliwe lub poważnie utrudnione lub które same w sobie mogą stwarzać poważne zagrożenie. Listę sektorów infrastruktury krytycznej określa, na mocy zarządzenia, pre-

[33] Tamże, s. 86.

[34] *Code de la defense*…, art. L 1332-1:

„Operatorzy publiczni lub prywatni zarządzający przedsiębiorstwami lub wykorzystujący instalacje lub obiekty, których niedostępność spowodowałaby istotne obniżenie potencjału wojskowego lub gospodarczego, bezpieczeństwa lub zdolności zachowania podstawowych funkcji społeczeństwa, zobowiązani są do współpracy, na własny koszt, na warunkach przewidzianych w niniejszym rozdziale, w celu ochrony tych przedsiębiorstw, instalacji i obiektów przed wszelkimi rodzajami zagrożeń, zwłaszcza przed zagrożeniami o charakterze terrorystycznym. Przedsiębiorstwa, instalacje i obiekty, o których mowa w niniejszym artykule, wyznaczane są przez organ administracji publicznej" (tłum. aut.).

[35] Tamże, art. L 1332-2:

„Obowiązki przewidziane w niniejszym artykule mogą zostać rozciągnięte na przedsiębiorstwa wskazane w art. L 511-1 ustawy – Kodeks środowiska (*Code de l'environnement*) lub na przedsiębiorstwa obejmujące podstawową instalację nuklearną, o której mowa w art. L 593-1 ustawy – Kodeks środowiska, jeżeli ich zniszczenie lub awaria ich niektórych instalacji może stwarzać poważne zagrożenie dla ludności. Przedsiębiorstwa te wyznaczane są przez organ administracji publicznej" (tłum. aut.).

Art. L 511-1 ustawy – Kodeks środowiska:

„Obowiązkom wymienionym w niniejszym tytule podlegają fabryki, zakłady, składy, miejsca budowy lub, w ujęciu ogólnym, instalacje wykorzystywane przez osoby fizyczne lub prawne, publiczne lub prywatne, mogące stwarzać zagrożenie dla zdrowia publicznego, bezpieczeństwa, rolnictwa, ochrony środowiska naturalnego, racjonalnego wykorzystania energii czy dziedzictwa kulturowego" (tłum. aut.), https://www.legifrance.gouv.fr/affichCode.do;jsessionid=73175D5154B5C5F9BB10A189852B30AA.tpdila09v_2?idSectionTA=LEGISCTA000006159272&cidTexte=LEGITEXT000006074220&dateTexte=20170919 [dostęp: 19 IX 2017].

mier, po zasięgnięciu opinii Międzyresortowej Komisji Bezpieczeństwa i Obrony. To zarządzenie wskazuje również ministra koordynatora dla każdego z wyżej wymienionych sektorów, do którego zadań należy nadzór nad stosowaniem wytycznych rządu w danym sektorze.

Raport wskazuje, że systemy informatyczne wykorzystywane przez operatorów infrastruktury krytycznej są szczególnie wrażliwe i podatne na wszelkie formy zagrożeń cybernetycznych. Tej tezy dowodzą przytoczone w dokumencie przykłady ataków na instytucje lub przedsiębiorstwa najważniejsze dla funkcjonowania państwa, np. ataki na systemy informatyczne ministerstw gospodarki i finansów w grudniu 2010 r. czy ingerencja w sieci informatyczne wykorzystywane przez strategiczne przedsiębiorstwo AREVA w 2011 r.[36]

Wnioski

Ewolucja systemu bezpieczeństwa cybernetycznego we Francji, zapoczątkowana opracowaniem w 2008 r. białej księgi określającej podstawowe cele i założenia polityczne w obszarze cyberbezpieczeństwa, doprowadziła do uporządkowania organizacyjnego i legislacyjnego. Za najważniejszy element procesu tworzenia spójnego systemu zapobiegania i przeciwdziałania zagrożeniom w cyberprzestrzeni należy uznać utworzenie w 2009 r. Narodowej Agencji Bezpieczeństwa Systemów Informatycznych – centralnego organu odpowiedzialnego za bezpieczeństwo systemów informatycznych. Zarówno sposób uregulowania kompetencji tego organu, jak i środki, jakimi realnie dysponuje, zostały ocenione w raporcie Bockela jako niewystarczające do efektywnego przeciwdziałania atakom na najważniejsze dla państwa systemy informatyczne. Jedna z rekomendacji zawartych w dokumencie[37] zalecała zmianę zakresu kompetencji ANSSI przez przyznanie jej uprawnień do prowadzenia tzw. inżynierii odwrotnej (tr. *rétroconception*) stosowanej w celach związanych z bezpieczeństwem i do analizy zachowania złośliwych elementów oprogramowania. Agencja powinna także móc wykorzystywać urządzenia umożliwiające śledzenie działań podmiotów odpowiedzialnych za ataki informatyczne oraz identyfikować słabe punkty wykorzystywanych przez te podmioty urządzeń lub oprogramowania w celu podjęcia ewentualnych działań odwetowych. Dokument rekomenduje także nadanie ANSSI kompetencji umożliwiających faktyczne oddziaływanie na politykę organów administracji publicznej i operatorów infrastruktury krytycznej w zakresie bezpieczeństwa wykorzystywanych przez nich systemów informatycznych.

Biorąc pod uwagę kształt ustawowych kompetencji ANSSI, należy uznać, że mają one charakter wyłącznie defensywny. Do najważniejszych z nich zalicza się opracowywanie środków ochrony systemów informatycznych i tworzenie mechanizmów wykrywania zagrożeń w systemach i sieciach. Agencja nie dysponuje jednak instrumentami ofensywnymi pozwalającymi na aktywne zwalczanie incydentów mogących negatywnie wpływać na bezpieczeństwo systemów najistotniejszych – z punktu widzenia funkcjonowania organów państwowych czy operatorów – dla infrastruktury krytycznej.

[36] *Rapport d'information*…, s. 20–25.
[37] Tamże, s. 123.

V. MODEL SYSTEMU BEZPIECZEŃSTWA TELEINFORMATYCZNEGO ORAZ OCHRONY SIECI TELEINFORMATYCZNYCH W REPUBLICE FEDERALNEJ NIEMIEC[38]

Zgodnie z § 1 ustawy z 14 sierpnia 2009 r. o Federalnym Urzędzie Bezpieczeństwa Teleinformatycznego (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) jest on odpowiedzialny za bezpieczeństwo informacji na poziomie krajowym. Federalny Urząd Bezpieczeństwa Teleinformatycznego (Bundesamt für Sicherheit in der Informationstechnik – BSI) powstał na mocy ustawy z 1 stycznia 1991 r., ma siedzibę w Bonn i podlega nadzorowi Federalnego Ministerstwa Spraw Wewnętrznych (Bunderministerium des Innern). Aktualnie w Urzędzie jest zatrudnionych ok. 600 pracowników.

Celem działalności BSI jest umożliwienie bezpiecznego korzystania z technologii informacyjnych i komunikacyjnych. Pod nadzorem i przy wsparciu ze strony BSI bezpieczeństwo teleinformatyczne jest realizowane jako priorytetowe działanie w administracji, gospodarce i społeczeństwie. W tym zakresie BSI opracowuje minimalne normy i zalecenia odnoszące się do bezpieczeństwa w sieciach teleinformatycznych oraz w Internecie, które mają pomóc użytkownikom w unikaniu zagrożeń. Urząd jest również odpowiedzialny za ochronę federalnych systemów IT przed różnego typu zagrożeniami (np. wirusy lub oprogramowanie trojańskie). Co roku BSI składa sprawozdanie ze swej działalności Komisji Spraw Wewnętrznych Bundestagu.

W myśl § 3 ustawy o BSI do najważniejszych zadań tego Urzędu należy:

- ochrona sieci federalnych, wykrywanie i zapobieganie atakom na sieci rządowe;
- udostępnianie organom federalnym produktów związanych z bezpieczeństwem IT;
- testowanie, certyfikacja i akredytacja produktów i usług IT;
- ostrzeganie przed złośliwym oprogramowaniem oraz lukami bezpieczeństwa w oprogramowaniu, produktach i usługach IT;
- doradztwo w zakresie bezpieczeństwa teleinformatycznego dla administracji federalnej oraz innych grup docelowych;
- wspieranie organów federalnych odpowiedzialnych za bezpieczeństwo technologii informacyjnych, zwłaszcza gdy te organy wykonują zadania doradcze lub nadzorcze (w szczególności wspieranie Federalnego Komisarza ds. Ochrony Danych i Wolności Informacji, zgodnie z zakresem jego uprawnień);
- wspieranie:
  - policji i organów ścigania w wykonywaniu ich ustawowych obowiązków,
  - organów odpowiedzialnych za ochronę konstytucji w zakresie analizy i oceny informacji pochodzących z rozpoznawania działalności terrorystycznej lub z działań wywiadowczych zgodnych z prawem federalnym i państwowym,
  - Federalnej Służby Wywiadu w realizacji jej ustawowych zadań.

[38] Zagadnienia związane z działalnością Federalnego Urzędu Bezpieczeństwa Teleinformatycznego oraz architekturą bezpieczeństwa teleinformatycznego uregulowaną w związku z założeniami Strategii Bezpieczeństwa Cybernetycznego dla Niemiec opracowano na podstawie ustawy z 14 sierpnia 2009 r. o Federalnym Urzędzie Bezpieczeństwa Teleinformatycznego http://www.gesetze-im-internet.de/bsig_2009/index.html#BJNR282110009BJNE000101116 [dostęp: 1 VIII 2017] oraz materiałów opublikowanych na stronie internetowej Federalnego Ministerstwa Spraw Wewnętrznych www.bmi.bund.de [dostęp: 1 VIII 2017].

To wsparcie może być udzielane tylko w przypadkach, gdy konieczne jest zapobieganie działaniom skierowanym przeciw bezpieczeństwu technologii informacyjnych lub przeprowadzenie w ich sprawie śledztwa lub jeśli działania muszą być zrealizowane przy wykorzystaniu technologii informacyjnych. Urząd prowadzi rejestr takich wniosków;

- zapewnianie wsparcia i doradztwa w sprawach związanych ze środkami technicznymi i organizacyjnymi oraz przeprowadzanie testów technicznych w celu ochrony informacji niejawnych przed nieuprawnionym dostępem w myśl § 4 ustawy z 20 kwietnia 1994 r. o wymogach i zasadach postępowań sprawdzających oraz ochronie informacji niejawnych;
- informowanie i podnoszenie świadomości społecznej w zakresie bezpieczeństwa teleinformatycznego i bezpieczeństwa w Internecie;
- opracowywanie jednolitych i obowiązujących standardów bezpieczeństwa teleinformatycznego;
- tworzenie i rozwijanie systemów kryptograficznych dla teleinformatyki federalnej.

Grupami docelowymi, do których BSI kieruje swoje działania, są:

- publiczna administracja na szczeblu centralnym i lokalnym,
- przedsiębiorstwa handlowe,
- instytucje naukowe i badawcze,
- użytkownicy prywatni.

Podczas wykonywania swoich obowiązków BSI współpracuje z innymi służbami, organami i instytucjami, które dostarczają ekspertyzy oraz służą doradztwem. Współpraca jest prowadzona również na płaszczyźnie międzynarodowej.

Strategia Bezpieczeństwa Cybernetycznego dla Niemiec[39], zatwierdzona 23 lutego 2011 r. przez rząd federalny, uznaje ochronę cyberprzestrzeni za podstawowe wyzwanie XXI w., które jest ściśle związane ze współpracą w Europie oraz na świecie. W *Strategii* stworzono ramy dla międzynarodowego zaangażowania BSI, natomiast konkretne działania międzynarodowe Urzędu są związane z kierunkami jego działania. Przykładowo, w ramach Unii Europejskiej i NATO przedsięwzięcia te są realizowane w postaci standaryzacji oraz normalizacji, zarówno na szczeblu dwustronnym, jak i wielostronnym.

Federalny Urząd Bezpieczeństwa Teleinformatycznego utrzymuje kontakty z najważniejszymi międzynarodowymi firmami telekomunikacyjnymi i producentami technologii informatycznych, jest również reprezentowany w niektórych istotnych konsorcjach przemysłowych. Ponadto Urząd, w ramach realizowanych działań profilaktycznych, wymienia regularnie z innymi organami – zarówno w UE, jak też poza nią – wiedzę na temat zagadnień technicznych dotyczących bezpieczeństwa teleinformatycznego oraz bezpieczeństwa w Internecie. W ramach partnerstwa w NATO, BSI współpracuje z organami odpowiedzialnymi za techniczne zagadnienia dotyczące ochrony systemów komputerowych, m.in. z amerykańską Agencją Bezpieczeństwa Narodowego (National Security Agency – NSA). Ta współpraca dotyczy tylko profilaktycznych aspektów cyberbezpieczeństwa, zgodnie z ustawowymi obowiązkami i uprawnieniami BSI.

Konieczność współpracy międzynarodowej w zakresie bezpieczeństwa teleinformatycznego jest jednym z postulatów wspomnianej *Strategii*. Ten dokument dotyczy też innych aspektów bezpieczeństwa cybernetycznego. Jako cel nadrzędny wskazano

[39] http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf?__blob=publicationFile [dostęp: 1 VIII 2017].

tu zapewnienie na odpowiednim poziomie ochrony połączonym siecią strukturom informatycznym, bez naruszania możliwości, jakie daje korzystanie z cyberprzestrzeni. Realizacji tej wytycznej służą następujące elementy:

- ochrona systemów informatycznych w Niemczech, szczególnie w dziedzinie infrastruktury krytycznej,
- promowanie podstawowych funkcji zabezpieczających, certyfikowanych przez państwo (np. nowy dowód osobisty, De-Mail[40]),
- podnoszenie świadomości obywateli na temat bezpieczeństwa teleinformatycznego, utworzenie Narodowego Centrum Przeciwdziałania Zagrożeniom Cyberprzestrzeni (Nationalen Cyber-Abwehrzentrum – NCAZ),
- powołanie Narodowej Rady Cyberbezpieczeństwa (Nationalen Cyber-Sicherheitsrat – NCS).

Za realizację założeń *Strategii* są odpowiedzialne: Narodowe Centrum Przeciwdziałania Zagrożeniom Cyberprzestrzeni oraz Narodowa Rada Cyberbezpieczeństwa. Z uwagi na rolę tych podmiotów, istotną dla całego niemieckiego systemu bezpieczeństwa teleinformatycznego, należy przybliżyć ich zadania oraz strukturę.

Narodowego Centrum Przeciwdziałania Zagrożeniom Cyberprzestrzeni to płaszczyzna współpracy wybranych organów, które – zgodnie ze swoją właściwością rzeczową – opracowują i przekazują informacje związane z cyberbezpieczeństwem kraju. Pod przewodnictwem BSI tę platformę współtworzą przedstawiciele:

- Federalnego Urzędu Ochrony Konstytucji (Bundesamt für Verfassungsschutz – BfV),
- Federalnego Urzędu Ochrony Ludności i Reagowania Kryzysowego (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe – BBK),
- Federalnego Urzędu Kryminalnego (Bundeskriminalamt – BKA),
- Policji Federalnej (Bundespolizei – BPol),
- Celnego Urzędu Kryminalnego (Zollkriminalamt – ZKA),
- Federalnej Służby Wywiadu (Bundesnachrichtendienst – BND),
- Bundeswehry.

Podstawą działania służb skupionych w NCAZ jest szybka wymiana informacji, tak aby wiedza pochodząca z obszaru działania poszczególnych służb procentowała w postaci wspólnych oszacowań, które dadzą możliwość dokonania analizy i podjęcia decyzji odnośnie do dalszych działań oraz zaleceń. Przedstawiciele wszystkich skupionych w NCAZ organów pracują wspólnie przy jednoczesnym, ścisłym zachowaniu swoich ustawowych uprawnień i obowiązków. Ocena incydentów cyberbezpieczeństwa jest przeprowadzana zgodnie z obowiązkami poszczególnych służb, np.:

- BSI ocenia atak z technicznego punktu widzenia,
- BfV dokonuje oceny z punktu widzenia zagrożeń wywiadowczych,
- BKA ocenia z punktu widzenia zadań policyjnych,
- BBK ocenia wpływ ataku na infrastrukturę krytyczną.

Wszystkie organy reprezentowane w NCAZ, które stanowi centrum wymiany informacji, wnoszą wkład w rozwój świadomości sytuacyjnej. W celu osiągnięcia satysfakcjonującego poziomu współpracy stworzono skuteczne kanały komunikacyjne. Podstawą pracy są codzienne briefingi oraz praca w grupach, zorganizowana tematycznie. Przedstawiciele wszystkich organów, które są niezbędne do przeciwdziałania incydentom bezpieczeństwa cybernetycznego, wymieniają i uzgadniają swoją wiedzę, a jeśli to

[40] Jest to określenie systemu opartego na technologii poczty elektronicznej.

konieczne – spotykają się także z poszkodowanym podmiotem. Istotnym elementem współpracy jest koordynacja działań.

Należy podkreślić, że powszechnie odnotowywany jest stały wzrost liczby zarówno przypadków cyberprzestępczości, jak i cyberszpiegostwa oraz cybersabotażu. Dlatego też duży wpływ na architekturę bezpieczeństwa IT ma monitorowanie incydentów bezpieczeństwa i wnioskowanie na tej podstawie o możliwych scenariuszach zagrożenia. Obowiązkowa jest również ścisła współpraca między organami bezpieczeństwa. Od początku utworzenia NCAZ przedmiotem codziennych briefingów było ok. 3700 przypadków, z czego wiedza na temat 820 meldunków została pogłębiona[41].

Zgodnie z fikcyjnym scenariuszem przedstawionym dziennikarzom w przededniu otwarcia Centrum, jego zwykły cykl pracy może wyglądać następująco:

- BSI uzyskuje informacje o luce bezpieczeństwa, której producent oprogramowania lub sprzętu nie potrafi skutecznie zabezpieczyć,
- BSI przekazuje otrzymane informacje do NCAZ,
- równocześnie BfV dowiaduje się o podjętej „próbie sabotażu", polegającej na usiłowaniu zainstalowania szkodliwego oprogramowania w placówce zaliczanej do infrastruktury krytycznej przez jej pracownika,
- BSI poddaje przedmiotowe oprogramowanie analizie technicznej,
- BSI stwierdza, że wykorzystuje ono rozpoznaną lukę bezpieczeństwa,
- pracownicy NCAZ wspólnie formułują wniosek o zaistnieniu realnego zagrożenia dla infrastruktury krytycznej,
- NCAZ ostrzega zagrożone jednostki organizacyjne, prosząc jednocześnie o informacje zwrotne.

Powyższa procedura ma zapewnić kontrolę NCAZ nad bezpieczeństwem niemieckiej cyberprzestrzeni[42]. Ten scenariusz uświadamia, że kluczowe znaczenie dla spójnego i skutecznego działania w przypadku zagrożenia ma wczesna wymiana informacji między służbami. W ocenie podmiotów nadzorujących NCAZ praca zespołu jest oceniana jako celowa i efektywna.

Jednym z założeń ujętym w Strategii było zapewnienie współpracy pomiędzy państwem a przedsiębiorcami. W celu realizacji tego postulatu została powołana Narodowa Rada Cyberbezpieczeństwa. Powołanie NCS ma służyć zauważalnej poprawie współpracy w obszarze cyberbezpieczeństwa zarówno w ramach administracji rządowej, jak i z innymi istotnymi podmiotami gospodarczymi.

W skład NCS wchodzą:

- Urząd Policji Kryminalnej,
- Ministerstwo Spraw Zagranicznych,
- Ministerstwo Obrony,
- Ministerstwo Gospodarki i Energii,
- Ministerstwo Sprawiedliwości,
- Ministerstwo Oświaty i Badań,
- Ministerstwo Finansów,
- przedstawiciele krajów związkowych Badenii-Wirtembergii oraz Hesji.

Sektor przedsiębiorczości jest natomiast reprezentowany przez:

- Federalny Związek Przemysłu Niemieckiego,

[41] Dane opublikowane w 2017 r.

[42] K. Sacewicz, *Niemiecka strategia ochrony cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7, s. 129.

- Stowarzyszenie Cyfrowe,
- Izbę Przemysłowo-Handlową,
- operatora przemysłu przesyłowego Amprion,
- UP-KRITIS – partnerstwo publiczno-prywatne pomiędzy operatorami infrastruktury krytycznej – ich związkiem a odpowiednimi agencjami rządowymi.

Spotkania Rady odbywają się do trzech razy w roku, a przewodzi im Pełnomocnik Rządu ds. Technologii Informacyjnych. Działania NCS przyczyniły się do tej pory do:

- wdrożenia istotnych zmian w zakresie ochrony infrastruktury krytycznej,
- skupienia na wspólnych celach działań i interesów związkowych, krajów i przemysłu,
- utworzenia spójnej cyberpolityki zagranicznej,
- podniesienia świadomości zagadnień oraz wyzwań technologicznych na wyższy szczebel polityczny.

Z uwagi na potrzebę uwzględnienia nowych wyzwań, jakie są konsekwencją stałego postępu technologii cyfrowych, 11 września 2016 r. rząd federalny wprowadził nową *Strategię Bezpieczeństwa Cybernetycznego* dla Niemiec[43]. Jest ona kontynuacją strategii zatwierdzonej w 2011 r. W nowej *Strategii Bezpieczeństwa Cybernetycznego* zostały uwypuklone cztery obszary działań:

- bezpieczne i autonomiczne działanie w przestrzeni cyfrowej (m.in. znak jakości – IT dla obywateli, prace nad nowym dowodem osobistym),
- współpraca na styku państwa i przedsiębiorczości (objęcie kolejnych branż ustawą o bezpieczeństwie IT),
- tworzenie wydajnej i trwałej państwowej architektury bezpieczeństwa cybernetycznego (utworzenie cyfrowych sił reagowania),
- aktywny udział Niemiec w europejskiej i międzynarodowej polityce bezpieczeństwa cybernetycznego.

Wraz z wdrożeniem nowej *Strategii*, Federalne Ministerstwo Gospodarki i Technologii powołało grupę roboczą ds. bezpieczeństwa teleinformatycznego w gospodarce (przedsiębiorczości), która we współpracy ze środowiskiem biznesowym podejmuje działania w ramach istniejących inicjatyw. Grupami docelowymi są przede wszystkim małe i średnie przedsiębiorstwa, które nie mają doświadczenia w zakresie bezpieczeństwa teleinformatycznego.

Udział w realizacji zadań określonych w *Strategii*, sprzyja niewątpliwie ścisłej współpracy także w innych obszarach narodowego cyberbezpieczeństwa, które należą do właściwości BSI. Do głównych zadań Federalnego Urzędu Bezpieczeństwa Teleinformatycznego należy m.in. podejmowanie prewencyjnych działań ochronnych, które mają na celu wzmocnienie bezpieczeństwa teleinformatycznego w administracji publicznej. Zgodnie z § 3 pkt 1 ustawy o BSI podstawowym zadaniem Urzędu jest zapobieganie zagrożeniom teleinformatycznych sieci federalnych. W tym kontekście należy wyróżnić pojęcie s i e c i r z ą d o w e, które oznacza infrastrukturę komunikacyjną dla niezawodnych i bezpiecznych transmisji głosu i danych między najwyższymi organami federalnymi i konstytucyjnymi w Niemczech.

Najważniejszymi stosowanymi środkami bezpieczeństwa sieci rządowych jest stałe szyfrowanie komunikacji oraz efektywna polityka bezpieczeństwa, która zapewnia ciągłe i wiarygodne funkcjonowanie komunikacji. W ramach infrastruktury technicznej wprowadzane są także modyfikacje i ulepszenia, jak również bezpieczne połączenia

[43] https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf [dostęp: 2 VIII 2017].

na szczeblu administracji lokalnej. Podejmowane przez BSI działania związane z ochroną sieci rządowych są przedmiotem ciągłego rozwoju i adaptacji do pojawiających się wciąż nowych zagrożeń.

Na co dzień zadaniem BSI jest identyfikacja cyberataków na sieci rządowe oraz reakcja polegająca na: ostrzeżeniu, natychmiastowym działaniu, zapewnieniu konkretnej pomocy oraz przekazywaniu zaleceń dla podmiotów. Głównymi jednostkami odpowiedzialnymi za inicjowanie opisanych powyżej środków są: Centrum Sytuacyjne Bezpieczeństwa Teleinformatycznego (IT-Lagezentrum) oraz umieszczony w wydziale BSI Zespół Reagowania na Incydenty Komputerowe (CERT). Zadaniem Centrum Sytuacyjnego jest bieżące monitorowanie bezpieczeństwa teleinformatycznego, ukierunkowane na zapewnienie właściwej oceny potrzeby reagowania oraz podjęcia działań w odpowiedzi na incydenty związane z bezpieczeństwem teleinformatycznym. Natomiast zadaniem CERT jest ocena informacji dotyczących bezpieczeństwa systemów i sieci teleleinformatycznych, rozpoznawanie incydentów w celu zapobiegania ich rozprzestrzenianiu się oraz minimalizowanie ewentualnych skutków, a także pomoc w przywracaniu normalnego funkcjonowania.

Wykonując zadania określone w § 3 pkt 1 ustawy o BSI, Urząd ten realizuje także projekt „sieci federacji", którego zadaniem jest utworzenie jednolitej i bezpiecznej infrastruktury teleinformatycznej dla podmiotów administracji publicznej. Korzystając ze wspólnej infrastruktury, urzędy będą mogły – w zależności od potrzeb – w bezpieczny sposób połączyć wspólną siecią swoje siedziby, komunikować się drogą ponadurzędową, a także oferować np. usługi IT lub same z nich korzystać.

W zakresie telefonii komórkowej w administracji federalnej BSI jest odpowiedzialny za wskazanie odpowiednich urządzeń oraz odpowiednich wymogów ochrony dla przekazywanych informacji. Jeśli informacje nie są objęte szczególną ochroną, pracownicy administracji federalnej mogą korzystać z urządzeń zgodnie z własnym wyborem. Jednak w zakresie komunikacji mobilnej, która wymaga wyższych środków bezpieczeństwa, zaleca się stosowanie specjalnych rozwiązań zatwierdzonych przez BSI.

Urząd wykonuje ustawowe obowiązki także dzięki wiarygodnym, potwierdzonym doświadczeniem informacjom uzyskiwanym w ramach grup roboczych, komitetów i zespołów. Pośród form współpracy BSI należy wymienić: współpracę publiczno-prywatną między operatorami infrastruktury krytycznej, ich stowarzyszeniami oraz odpowiednimi agencjami rządowymi, wymianę informacji pomiędzy administracją i przedsiębiorcami za pośrednictwem krajowego Centrum Sytuacyjnego (mieszczącego się w strukturach BSI), prewencyjną oraz stanowiącą odpowiedź na ataki współpracę federalnych CERT z innymi krajowymi oraz międzynarodowymi sieciami CERT, a także współpracę z partnerami w ramach Sojuszu dla Cyberbezpieczeństwa[44]. Te informacje są uzupełniane dzięki stałemu monitorowaniu i ocenie powszechnie dostępnych źródeł informacji, takich jak serwisy informacyjne i blogi w internecie.

[44] Sojusz dla Cyberbezpieczeństwa powstał z inicjatywy BSI i został zawiązany w 2012 r. we współpracy z Federalnym Stowarzyszeniem Zarządzania Informacją, Telekomunikacją i Nowymi Mediami. Jest to związek wszystkich kluczowych podmiotów działających w obszarze cyberbezpieczeństwa w Niemczech, którego celem jest dostarczanie aktualnych, istotnych informacji na temat zagrożeń cyberbezpieczeństwa. Ta inicjatywa wspiera również wymianę informacji i doświadczeń między uczestnikami. Sojusz dla Cyberbezpieczeństwa obejmuje obecnie ponad 2000 instytucji, z czego prawie 100 to przedsiębiorstwa partnerskie. Uczestnictwo w Sojuszu jest bezpłatne i można się o nie ubiegać w każdej niemieckiej instytucji. Działania Sojuszu koncentrują się głównie na poprawie cyberbepieczeństwa w małych i średnich przedsiębiorstwach.

W związku z obowiązkiem ochrony sieci rządowych Federalny Urząd Bezpieczeństwa Teleinformatycznego, w myśl § 5 ust. 1 pkt 1 i 2 ustawy o BSI, otrzymał uprawnienie do wykorzystania zautomatyzowanych procesów do gromadzenia i oceny protokołu przesyłania danych generowanych przez operowanie federalnymi technologiami komunikacyjnymi w celu rozpoznawania, zawierania lub usuwania zakłóceń lub problemów albo w związku z atakami na federalne technologie komunikacyjne. W ramach tych uprawnień BSI może także wykorzystywać zautomatyzowane procesy do oceny danych generowanych na federalnych interfejsach w celu rozpoznania i ochrony przed szkodliwym oprogramowaniem. Urząd posiada także uprawnienie do usuwania złośliwych programów lub zapobiegania ich funkcjonowaniu, w związku z czym może uruchomić system przeciwdziałania złośliwym oprogramowaniom, aby zapobiec nieautoryzowanemu dostępowi do sieci rządowych przez zainfekowane strony internetowe, bądź może uruchomić system wykrywania szkodliwego oprogramowania.

Istotne znaczenie dla krajowego bezpieczeństwa teleinformatycznego ma obowiązek informacyjny realizowany przez BSI zgodnie z § 7 ust. 1 ustawy. Do uprawnień tej służby należy bowiem ogłaszanie ostrzeżeń o lukach w zabezpieczeniach informatycznych produktów i usług oraz ostrzeżeń przed szkodliwymi programami lub też rekomendowanie środków bezpieczeństwa albo zaleceń odnośnie do korzystania z niektórych produktów. Ostrzeżenia te mogą być wysyłane do podmiotu, którego dotyczą, lub mogą być upowszechniane, np. za pośrednictwem mediów. Producenci są informowani przed publikacją ostrzeżenia. Uprawnienie to jest realizowane przez BSI bardzo ostrożnie, gdyż publiczne ostrzeżenie BSI dla konkretnych produktów może mieć poważne konsekwencje ekonomiczne dla danego przedsiębiorstwa. Z tego względu, w ramach ustawowych uprawnień, Urząd może podjąć decyzję o nieupublicznieniu ostrzeżenia i ograniczeniu kręgu jego adresatów.

Przy omawianiu ochrony sieci teleinformatycznych, która jest wdrażana i nadzorowana przez powołaną specjalnie w tym celu służbę, nie można pominąć istotnego aspektu działalności BSI, jakim jest zadanie realizowane na podstawie art. 9 ust. 1 ustawy, tj. wykonywanie zadań krajowego organu ds. certyfikacji w zakresie bezpieczeństwa teleinformatycznego. Wraz z szansą, jaką stwarza rozwój technologiczny, wzrasta także ryzyko, stale bowiem powiększa się ilość poufnych danych przetwarzanych za pośrednictwem najnowszych technik informacyjnych. Dlatego też sprawne funkcjonowanie obszarów istotnych dla społeczeństwa zależy od niezawodności i bezpieczeństwa nowoczesnych urządzeń i systemów.

Bezpieczeństwo teleinformatyczne odgrywa zatem główną rolę w zminimalizowaniu pojawiającego się ryzyka. Z technicznego punktu widzenia funkcjonalność produktów oraz systemów teleinformatycznych nie jest jednak zrozumiała dla szerszego kręgu użytkowników. Natomiast zaufanie do technologii informacyjnych może powstać tylko wtedy, gdy użytkownicy mogą polegać na ich stosowaniu. Odnosi się to zwłaszcza do zapewnienia bezpieczeństwa danych. Jednym ze sposobów na stworzenie przejrzystości w odniesieniu do właściwości bezpieczeństwa produktów i systemów IT są badania, ocena i certyfikacja produktów oraz systemów opartych na standardowych kryteriach przez niezależne ośrodki uznane przez BSI. To właśnie ten urząd zapewnia obiektywizm i spójność oraz bezstronność badań.

Realizując to uprawnienie, BSI odgrywa także istotną rolę w rozwoju kryteriów bezpieczeństwa. Ocena techniczna produktu jest przeprowadzana po złożeniu wniosku o certyfikację w BSI, na ogół w laboratoriach akredytowanych i licencjonowanych przez

BSI. Wnioskodawca ma prawo wyboru laboratorium, któremu zostaje powierzona realizacja procedur badawczych. Laboratoria służą również doradztwem w zakresie stosowanej procedury na każdym etapie badań. Dzięki certyfikacji poziomu bezpieczeństwa dostawca produktów i usług IT może prezentować swoją ofertę w przystępny sposób. Użytkownicy certyfikowanych produktów i rozwiązań teleinformatycznych są w stanie ocenić, w jakim zakresie produkty i usługi są odpowiednie i jaki wkład będzie musiał ponieść użytkownik w związku z korzystaniem z urządzenia oraz rozwiązań, aby osiągnąć odpowiedni poziom w zakresie bezpieczeństwa IT.

Przedstawione powyżej najważniejsze zadania realizowane przez Federalny Urząd Bezpieczeństwa Teleinformatycznego zarówno w związku z ustawowymi obowiązkami, jak i w ramach wykonywania założeń *Strategii Bezpieczeństwa Teleinformatycznego*, podlegają kontroli. Stały nadzór techniczny nad Urzędem sprawuje Ministerstwo Spraw Wewnętrznych. Ponadto, zgodnie z § 5 ust. 9 ustawy o BSI, służba ta raz w roku przedkłada sprawozdanie Pełnomocnikowi Rządu Federalnego ds. Ochrony Danych i Wolności Informacji. Analogicznie – co roku Komisja Spraw Wewnętrznych Bundestagu jest informowana o stosowaniu uprawnień określonych w § 5 ustawy o BSI.

VI. REPUBLIKA WŁOSKA

1. Ogólna charakterystyka *Dyrektywy wyznaczającej wskazówki w zakresie narodowej cyberobrony i bezpieczeństwa informatycznego*

Najważniejszym obecnie aktem prawnym regulującym systemowe kwestie dotyczące obszaru cyberobrony bezpieczeństwa teleinformatycznego w Republice Włoskiej jest *Dekret Prezesa Rady Ministrów z dnia 17 lutego 2017 r. „Dyrektywa wyznaczająca wskazówki w zakresie narodowej cyberobrony i bezpieczeństwa informatycznego"* (Dz. Urz. Nr 87 z 13 kwietnia 2017 r.)[45], zwany dalej „dekretem". Zastąpił on poprzedni dekret Prezesa Rady Ministrów z 24 stycznia 2013 r., który do tej pory regulował architekturę cyberbezpieczeństwa Republiki Włoskiej[46] Niniejszy dekret został wydany w celu implementacji do krajowego porządku prawnego we Włoszech artykułu 7 ust. 1 *Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii* (Dz. Urz. UE z 2016 r. L nr 194, s. 1), który nakazuje państwom członkowskim Unii Europejskiej przyjęcie krajowej strategii w zakresie bezpieczeństwa systemów i sieci teleinformatycznych.

Dekret składa się z 13 artykułów. Artykuł 1 określa przedmiot jego regulacji, artykuł 2 – definicje występujących w nim pojęć, artykuły od 3 do 12 regulują obowiązki poszczególnych podmiotów państwowych i prywatnych, artykuł 13 natomiast zawiera przepisy przejściowe i końcowe.

Zgodnie z art. 1 ust. 1 dekret definiuje w jednolity i zintegrowany sposób architekturę instytucjonalną dedykowaną ochronie bezpieczeństwa narodowego w odniesieniu do materialnych i niematerialnych aspektów infrastruktury krytycznej, ze szczególnym

[45] http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html [dostęp: 2 VIII 2017].

[46] http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cyber-security-approvato-nuovo-decreto.html [dostęp: 2 VIII 2017].

uwzględnieniem narodowej cyberobrony i bezpieczeństwa informatycznego. Wskazuje jednocześnie zadania przypisane wszystkim jej komponentom, a także mechanizmy i procedury wymagające stosowania w celu zmniejszenia podatności, zapobiegania różnego rodzaju ryzyku oraz adekwatnej odpowiedzi na ataki i niezwłocznego przywracania funkcjonalności systemów w sytuacji kryzysowej.

Co ważne – ustęp 2 art. 1 dekretu wskazuje, że podmioty uczestniczące w architekturze instytucjonalnej narodowej cyberobrony i bezpieczeństwa informatycznego działają w ramach kompetencji już przyznanych im w aktach rangi ustawowej. Dekret nie przyznaje samoistnie żadnych nowych kompetencji żadnym podmiotom, stanowi więc w istocie instrument tzw. miękkiego prawa. W preambule wskazano wiele przepisów i aktów prawnych przyznających podmiotom objętym zakresem dekretu kompetencje w zakresie bezpieczeństwa informatycznego i cyberobrony. Wśród przytoczonych aktów prawnych na pierwszym miejscu wymieniono ustawę nr 124 z 3 sierpnia 2007 r. ustanawiającą system informacyjny na rzecz bezpieczeństwa Republiki i nowy reżim ochrony tajemnicy państwowej, zmienioną ustawą nr 133 z 7 sierpnia 2012 r., a zatem kluczowy akt prawny regulujący funkcjonowanie służb specjalnych we Włoszech. Art. 1 ust. 3-bis wymienionej ustawy upoważnia Prezesa Rady Ministrów, po zasięgnięciu opinii Międzyresortowego Komitetu Bezpieczeństwa Republiki, do wydawania Departamentowi Informacji Bezpieczeństwa oraz służbom informacyjnym dyrektyw na rzecz wzmocnienia aktywności informacyjnej w zakresie ochrony materialnej i niematerialnej infrastruktury krytycznej, ze szczególnym uwzględnieniem narodowej obrony cybernetycznej oraz bezpieczeństwa informacyjnego.

Przepis art. 1 ust. 3 dekretu przewiduje, że jego celem jest stworzenie systemu organizacyjno-funkcjonalnego dążącego do pełnej integracji działań podejmowanych w ramach kompetencji różnych podmiotów, takich jak: Ministerstwo Rozwoju Ekonomicznego, Agencja na Rzecz Cyfrowych Włoch oraz Ministerstwo Obrony – w zakresie ochrony systemów i sieci oraz prowadzenia operacji wojskowych w cyberprzestrzeni, Ministerstwo Spraw Wewnętrznych – w zakresie działań nakierowanych na przeciwdziałanie i zwalczanie przestępczości informatycznej, obronę cywilną i ochronę ludności. Innymi słowy – celem dekretu jest stworzenie systemu krajowej cyberobrony, z jasnym podziałem zadań i kompetencji między poszczególnymi organami administracji rządowej a innymi podmiotami. Należy zwrócić uwagę na brak wskazania jednego organu odpowiedzialnego za cyberbezpieczeństwo kraju; zamiast tego wskazano główną rolę kilku instytucji odpowiedzialnych za różne sfery administracji. Można zatem stwierdzić, że Włochy przyjęły model rozproszonej odpowiedzialności za bezpieczeństwo informatyczne kraju.

2. Definicje

Z definicji zawartych w art. 2 dekretu można przytoczyć następujące:

- przestrzeń cybernetyczna – zespół wzajemnie połączonych infrastruktur informatycznych, złożony zarówno z urządzeń, oprogramowania, danych i użytkowników, jak i powiązań logicznych między nimi, niezależnie od ich trwałości (art. 2 ust. 1 lit. h),
- bezpieczeństwo cybernetyczne – stan, w którym przestrzeń cybernetyczna jest chroniona dzięki przyjęciu odpowiednich środków bezpieczeństwa fizycznego, logicznego i proceduralnego, w odniesieniu do zdarzeń natury umyśl-

nej lub przypadkowej, polegających na nieuprawnionym przejęciu lub transferze danych, ich bezprawnej modyfikacji lub zniszczeniu, nieuprawnionym przejęciu kontroli, uszkodzeniu, zniszczeniu lub zablokowaniu normalnego funkcjonowania systemów i sieci informatycznych oraz ich kluczowych elementów (art. 2 ust. 1 lit. f),

- zagrożenie cybernetyczne – zbiór zachowań, które mogą być realizowane w przestrzeni cybernetycznej lub za jej pośrednictwem, lub na jej szkodę, lub konstytuujących ją elementów, czego przejawem są przede wszystkim działania jednostek lub organizacji – państwowych i niepaństwowych, publicznych i prywatnych, nakierowane na nieuprawniony dostęp i transfer danych, ich bezprawną modyfikację lub zniszczenie, lub na nieuprawnione przejęcie kontroli, uszkodzenie, zniszczenie lub wstrzymanie regularnego funkcjonowania systemów i sieci informatycznych oraz ich elementów konstytutywnych (art. 2 ust. 1 lit. l),
- zdarzenie cybernetyczne – istotne wydarzenie natury umyślnej lub przypadkowej, polegające na nieuprawnionym dostępie lub przekazaniu danych, ich nieuprawnionej modyfikacji lub zniszczeniu lub zablokowaniu regularnego funkcjonowania sieci i systemów teleinformatycznych oraz ich elementów konstytutywnych (art. 2 ust. 1 lit. m),
- sytuacja kryzysu cybernetycznego – sytuacja, w której zdarzenie cybernetyczne przyjmuje takie rozmiary, intensywność lub charakter, że oddziałuje na bezpieczeństwo narodowe albo nie może być opanowane po zastosowaniu zwykłych kompetencji działających pojedynczo właściwych organów, lecz wymaga podjęcia decyzji koordynacyjnych na szczeblu międzyministerialnym (art. 2 ust. 1 lit. o).

3. Uprawnienia i obowiązki poszczególnych podmiotów

3.1. Prezes Rady Ministrów

Artykuł 3 dekretu mówiący o kompetencjach Prezesa Rady Ministrów odnosi je do jego roli jako osoby odpowiedzialnej za politykę rządu oraz zwierzchnika Systemu Informacyjnego na rzecz Bezpieczeństwa Republiki. Ten przepis przewiduje, że w celach ochrony bezpieczeństwa narodowego w cyberprzestrzeni premier:

- w sytuacjach kryzysowych dotyczących bezpieczeństwa narodowego zwołuje Komitet Międzyministerialny na rzecz Bezpieczeństwa Republiki (CISR),
- przyjmuje i aktualizuje, na wniosek CISR, Narodowe Ramy Strategiczne Bezpieczeństwa Cybernetycznego, zawierające: wskazanie profili i tendencji ewolucji zagrożeń oraz podatności systemów i sieci o znaczeniu narodowym, zdefiniowanie roli i zadań różnych podmiotów, publicznych i prywatnych, działających zarówno w kraju, jak i za granicą, identyfikację instrumentów i procedur, których stosowanie ma zwiększyć zdolności kraju w zakresie zapobiegania i odpowiedzi w odniesieniu do zdarzeń w cyberprzestrzeni, również pod kątem upowszechniania kultury bezpieczeństwa,
- przyjmuje, na wniosek CISR, Narodowy Plan Ochrony Cybernetycznej i Narodowego Bezpieczeństwa Informacyjnego zawierający cele i czynności wymagające podjęcia w celu realizacji narodowych ram strategicznych bezpieczeństwa informacyjnego,

- wydaje dyrektywy i inne akty niezbędne do wdrożenia Planu Ochrony Cybernetycznej i Narodowego Bezpieczeństwa Informacyjnego,
- wydaje, po zasięgnięciu opinii CISR, dyrektywy dla Departamentu Informacyjnego Bezpieczeństwa i dla agencji informacyjnych.

3.2. Komitet Międzyministerialny na Rzecz Bezpieczeństwa Republiki

Jest to ciało o charakterze doradczo-konsultacyjnym obsługujące funkcje Prezesa Rady Ministrów. Do jego kompetencji zalicza się przedkładanie premierowi projektu Narodowych Ram Strategicznych Bezpieczeństwa Cybernetycznego, Narodowego Planu Ochrony Cybernetycznej i Narodowego Bezpieczeństwa Informacyjnego oraz opracowywanie dla organów wywiadowczych wytycznych w zakresie cyberobrony i bezpieczeństwa informatycznego.

Komitet Międzyministerialny na rzecz Bezpieczeństwa Republiki w wykonywaniu swoich zadań w obszarze cyberbezpieczeństwa jest wspierany przez tzw. Techniczny CISR – organ kolegialny niższego szczebla, któremu przewodniczy dyrektor DIS. Techniczny CISR przygotowuje posiedzenia właściwego CISR poświęcone problematyce bezpieczeństwa cybernetycznego, zapewnia wsparcie eksperckie, weryfikuje wprowadzanie w życie działań przewidzianych przez Narodowy Plan Ochrony Cybernetycznej i Narodowego Bezpieczeństwa Informacyjnego, a także skuteczność procedur mających zapewnić koordynację między działaniami podmiotów publicznych i prywatnych. Ponadto koordynuje – w zakresie zaaprobowanym przez CISR i we współpracy z urzędami administracji, agencjami wywiadowczymi, Centrum Cyberbezpieczeństwa i operatorami prywatnymi – tworzenie zarówno zaleceń mających na celu polepszenie rozpoznawania zagrożeń bezpieczeństwa w cyberprzestrzeni i wykrywania podatności, jak i przyjmowania dobrych praktyk w zakresie bezpieczeństwa.

3.3. Dyrektor generalny Departamentu Informacyjnego Bezpieczeństwa

Artykuł 6 dekretu zawiera dość ogólną regulację, zgodnie z którą dyrektor generalny DIS, w celu osiągnięcia celów tego dekretu w zakresie bezpieczeństwa narodowego, podejmuje inicjatywy konieczne do zdefiniowania kierunków niezbędnych działań w interesie ogólnym, dla osiągnięcia celu polegającego na podniesieniu i polepszeniu poziomów bezpieczeństwa systemów i sieci. Realizując to zadanie ma dążyć przede wszystkim do identyfikacji i udostępniania najbardziej adekwatnych i zaawansowanych technologicznie środków wsparcia dla funkcji przygotowania do działań w zakresie zapobiegania, przeciwdziałania i reakcji w sytuacji kryzysu cybernetycznego ze strony organów administracji, podmiotów publicznych i operatorów prywatnych, o których mowa w art. 11 dekretu.

3.4. Podmioty Systemu Informacyjnego Bezpieczeństwa

Artykuł 7 ust. 1 – *Organizacje informacyjne bezpieczeństwa* – wskazuje, że zarówno DIS, jak i służby specjalne (AISI i AISE) prowadzą działalność w obszarze bezpieczeństwa cybernetycznego, posługując się instrumentami przewidzianymi w ustawie nr 124 z 2007 r. oraz w trybie i zgodnie z procedurami określonymi w przepisach tej ustawy.

W tym zakresie dyrektor generalny DIS, na podstawie dyrektyw premiera wydanych zgodnie z art. 1 ust. 3-bis ustawy nr 124 z 2007 r. oraz w świetle ogólnych kierunków oraz podstawowych celów zidentyfikowanych przez CISR, prowadzi koordynację pozyskiwania informacji, nakierowanych na wzmocnienie narodowej obrony cybernetycznej i bezpieczeństwa informacyjnego. Odpowiednie komórki DIS wspierają dyrektora generalnego w wykonywaniu tych funkcji. DIS opracowuje analizy, ewaluacje i prognozy odnoszące się do zagrożeń cybernetycznych. Zapewnia też przekazywanie organom administracji publicznej oraz innym podmiotom, także prywatnym, informacji istotnych dla bezpieczeństwa cybernetycznego i współdzielenie się tego rodzaju informacjami w obszarze właściwości Centrum Cyberbezpieczeństwa.

Zgodnie z art. 7 ust. 4 dekretu do kompetencji Agencji Informacyjnych Bezpieczeństwa (AISI i AISE) zalicza się poszukiwanie i opracowywanie informacji odnoszących się do narodowej cyberobrony i bezpieczeństwa informatycznego, zgodnie z kierunkami zdefiniowanymi w dyrektywach premiera oraz wytycznych koordynacyjnych w zakresie pozyskiwania informacji, ustalonych przez dyrektora generalnego DIS.

W celu udoskonalania potencjału w zakresie działań na rzecz cyberbezpieczeństwa DIS i agencje wywiadowcze AISI i AISE wymieniają informacje z organami administracji publicznej, upoważnionymi podmiotami służb publicznych, uniwersytetami, ośrodkami badawczymi, zawierając w tym celu stosowne porozumienia (podstawą prawną do zawierania tego rodzaju porozumień jest art. 13 ust. 1 ustawy nr 124 z 2007 r.). W tym samym celu te służby mogą uzyskiwać dostęp do baz danych organów administracji publicznej i służb publicznych. Procedura uzyskiwania takiego dostępu jest określona w art. 13 ust 2 ustawy nr 124 z 2007 r.

Zgodnie z ustępem 6 art. 7 dekretu DIS wdraża wszelkie inicjatywy na rzecz promocji i upowszechniania wiedzy i świadomości co do istoty różnych rodzajów ryzyka pochodzących z zagrożeń cybernetycznych oraz środków ochrony przed nimi.

3.5. Centrum Cyberbezpieczeństwa

Centrum Cyberbezpieczeństwa (Nucleo per la sicurezza cibernetica) jest instytucją wspierającą premiera i CISR w sprawach dotyczących bezpieczeństwa cyberprzestrzeni, w zakresie spraw odnoszących się do zapobiegania i przygotowania do wystąpienia ewentualnych sytuacji kryzysowych i uruchamiania procedur alarmowych. Odnosząc się do umiejscowienia organizacyjnego Centrum Cyberbezpieczeństwa, art. 8 ust. 1 dekretu stanowi, że działa ono przy Departamencie Informacji Bezpieczeństwa. Centrum jest kierowane przez wyznaczonego przez dyrektora generalnego DIS zastępcę dyrektora DIS, a składa się z Doradcy Wojskowego oraz przedstawicieli: DIS, AISI, AISE, Ministerstwa Spraw Zagranicznych, Ministerstwa Spraw Wewnętrznych, Ministerstwa Obrony, Ministerstwa Sprawiedliwości, Ministerstwa Rozwoju Gospodarczego, Ministerstwa Gospodarki i Finansów, Departamentu Obrony Cywilnej i Agencji na Rzecz Cyfrowych Włoch (art. 8 ust. 2). W zakresie spraw odnoszących się do przetwarzania informacji niejawnych w pracach Centrum uczestniczy przedstawiciel Centralnego Urzędu Ochrony Informacji Niejawnych (Ufficio centrale per la segretezza).

Członkom Centrum mogą towarzyszyć w posiedzeniach inni pracownicy delegujących ich urzędów. Dopuszczalne jest również zapraszanie do udziału w posiedzeniach przedstawicieli innych organów administracji, uniwersytetów, ośrodków badawczych, a także prywatnych operatorów, jeśli uzasadnia to tematyka spotkania.

Centrum zbiera się przynajmniej raz w miesiącu na wniosek przewodniczącego, którym jest wicedyrektor DIS, lub co najmniej jednego z członków. Z przeprowadzonych czynności Centrum składa sprawozdanie dyrektorowi generalnemu DIS, a ten przekazuje stosowne informacje premierowi i CISR.

Szczegółowy zakres zadań Centrum został określony w art. 9 dekretu. Najważniejszym zadaniem jest zapewnienie łączności między różnymi komponentami architektury instytucjonalnej cyberbezpieczeństwa, które z różnych tytułów podejmują działania w obszarze cyberbezpieczeństwa. Jako zadania Centrum w zakresie przeciwdziałania i przygotowania do wystąpienia sytuacji kryzysu cybernetycznego w dekrecie wymienia się:

- wspieranie opracowywania planów i programów operacyjnych reagowania w sytuacjach kryzysu cybernetycznego przez urzędy administracji i zainteresowanych operatorów prywatnych oraz wypracowanie niezbędnych procedur koordynacji międzyresortowej,
- utrzymywanie służby dyżurnej działającej 24 godziny na dobę siedem dni w tygodniu, właściwej do alarmowania i reagowania w sytuacji wystąpienia kryzysu cybernetycznego,
- ewaluację i wsparcie, w uzgodnieniu z organami administracji odpowiedzialnymi za poszczególne zagadnienia z obszaru cyberbezpieczeństwa, bez uszczerbku dla procedur wymiany informacji między informacyjnymi organami bezpieczeństwa, procedur dzielenia się informacjami, a także z zainteresowanymi operatorami prywatnymi – w celu rozpowszechniania systemu alertów dotyczących zdarzeń cybernetycznych i zarządzania kryzysowego,
- przyjmowanie zawiadomień o przypadkach naruszenia lub próbach naruszenia bezpieczeństwa oraz o przypadkach utraty integralności systemów i sieci od Ministerstwa Rozwoju Gospodarczego, od organów informacyjnych w zakresie bezpieczeństwa, od służb policyjnych, szczególnie od CNAIPIC[47],
- wsparcie i koordynacja, w uzgodnieniu z Ministerstwem Rozwoju Gospodarczego i Agencją na rzecz Cyfrowych Włoch, w zakresie ich właściwości, prowadzenia ćwiczeń międzyresortowych, a także uczestnictwa Włoch w ćwiczeniach międzynarodowych, odnoszących się do symulacji zdarzeń cybernetycznych,
- utrzymywanie narodowego punktu kontaktowego do spraw wymiany raportów z ONZ, NATO i UE, innymi organizacjami międzynarodowymi i innymi państwami.

Jako kompetencje Centrum w zakresie odpowiedzi i usuwania skutków kryzysu cybernetycznego dekret wymienia:

- przyjmowanie, również z zagranicy, sygnałów na temat zdarzeń cybernetycznych i dystrybucję alertów do organów administracji i operatorów prywatnych, w celu wykonania planów działania,
- dokonywanie oceny, czy zagrożenie przyjmuje rozmiary, intensywność lub naturę, które uniemożliwiają zaradzenie mu przez jeden właściwy organ przy użyciu zwyczajnych środków, czy też wymaga podjęcia decyzji koordynacyjnych na szczeblu międzyministerialnym, zapewniając w takim wypadku wdrożenie przewidzianych prawem środków współdziałania i koordynacji,

[47] CNAIPIC – Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – Narodowe Centrum Zwalczania Przestępczości Informatycznej w Celu Ochrony Infrastruktury Krytycznej – organ posiadający wyłączną właściwość w zakresie zapobiegania i zwalczania przestępstw informatycznych przeciwko informatycznej infrastrukturze krytycznej, które mają znaczenie ogólnokrajowe, stanowiący część *Polizia Postale* – Policji Pocztowej, https://www.commissariatodips.it/profilo/cnaipic.html [dostęp: 10 VIII 2017].

- informowanie we właściwym czasie premiera, za pośrednictwem dyrektora generalnego DIS, o bieżącej sytuacji.

Centrum opracowuje również raporty na temat stosowania środków koordynacji w zakresie przeciwdziałania i zarządzania sytuacją kryzysową i przekazuje je technicznemu CISR.

3.6. Zarządzanie kryzysem cybernetycznym

Zgodnie z art. 10 w celu zarządzania kryzysem cybernetycznym Centrum zbiera się w składzie dostosowanym do aktualnych potrzeb – jego skład może zostać poszerzony o upoważnionych przedstawicieli: Ministerstwa Zdrowia, Ministerstwa Infrastruktury i Transportu, Departamentu Straży Pożarnej, pogotowia ratunkowego, obrony cywilnej, w tym Międzyministerialnego Komitetu Technicznego Obrony Cywilnej (CIDTC) oraz Biura Doradcy Wojskowego Prezesa Rady Ministrów. Upoważnionym przedstawicielom mogą towarzyszyć inni pracownicy zatrudniających ich organów. Do udziału w posiedzeniach można wzywać również upoważnionych przedstawicieli innych władz i instytucji, także lokalnych, i operatorów prywatnych, do których odnosi się art. 11 dekretu, oraz ewentualnie innych zainteresowanych podmiotów. Centrum może spotykać się także, jeśli istnieje taka potrzeba, w składzie zawężonym do podmiotów zainteresowanych tematyką spotkania.

Zadaniem Centrum działającego w składzie w sytuacji zarządzania kryzysowego, jest zapewnienie, aby zadania w zakresie reakcji i stabilizacji, które pozostają w kompetencjach różnych podmiotów, były wykonywane w sposób skoordynowany, zgodnie z planami i programami opracowanymi przez Centrum, a w zakresie technicznych aspektów reakcji – były oparte na planach informatycznych i telematycznych[48] narodowego CERT-u, działającego przy Ministerstwie Rozwoju Gospodarczego i innych CERT-ów działających na podstawie obowiązujących norm (w tym CERT przy Agencji na rzecz Cyfrowych Włoch).

Centrum przekazuje systematycznie premierowi, za pośrednictwem dyrektora generalnego DIS, bieżące informacje na temat rozwoju sytuacji kryzysowej, zapewnia koordynację wdrażania zarządzeń premiera, które mają na celu przezwyciężenie kryzysu na szczeblu międzyresortowym, zbiera wszelkie dane niezbędne do przezwyciężenia kryzysu, wytwarza raporty i dostarcza informacji na temat kryzysu oraz przekazuje je zainteresowanym podmiotom publicznym i prywatnym. Zapewnia również współdziałanie z odpowiednimi instytucjami innych krajów, NATO, UE i organizacji międzynarodowych, których członkiem są Włochy.

3.7. Obowiązki operatorów prywatnych

Artykuł 11 dekretu reguluje obowiązki operatorów prywatnych na rzecz cyberbezpieczeństwa. Jego zakresem są objęte następujące kategorie operatorów: dostawcy

[48] Telematyka – dyscyplina zajmująca się przekazem cyfrowej informacji multimedialnej (audio, video, grafika, dane) za pośrednictwem sieci teleinformatycznych oraz przygotowaniem, gromadzeniem i udostępnianiem tego rodzaju informacji w formie usług teleinformatycznych; termin w obecnym znaczeniu wylansowany przez Komisję Europejską w latach 1994–1998, gdy w ramach IV Programu Ramowego realizowano program zastosowań telematyki w różnych dziedzinach życia publicznego, gospodarki i nauki jako Telematics Applications Programme; znaczącym obszarem zastosowań telematyki jest sektor środowiska, https://pl.glosbe.com/it/pl/telematica [dostęp: 10 VIII 2017].

publicznych sieci, dostawcy publicznie dostępnych usług, operatorzy kluczowych usług i dostawcy usług cyfrowych wymienionych w załączniku III do dyrektywy 2016/1148 (internetowe platformy handlowe, wyszukiwarki internetowe i usługi przetwarzane w chmurze), gestorzy infrastruktury krytycznej o znaczeniu krajowym i europejskim, której działanie jest uzależnione od działania systemów informatycznych i telematycznych.

Do ich obowiązków zaliczono w dekrecie:

- przekazywanie do Centrum Cyberbezpieczeństwa, z wykorzystaniem chronionych kanałów łączności, informacji o każdym istotnym naruszeniu bezpieczeństwa lub integralności systemów informatycznych,
- przyjęcie najlepszych praktyk i środków nakierowanych na ochronę cyberbezpieczeństwa, opracowanych przez techniczny CISR,
- dostarczanie informacji służbom bezpieczeństwa informacyjnego, a także umożliwianie im dostępu do Centrów Operacji Bezpieczeństwa (Security Operations Center) oraz innych archiwów informatycznych – w celu ochrony cyberbezpieczeństwa,
- współpracę w zarządzaniu kryzysami cybernetycznymi, co przyczynia się do przywracania funkcjonalności systemów i sieci pozostających w ich gestii.

W art. 11 ustęp 2 zawarto zapis, że minister rozwoju gospodarczego powołuje narodowe centrum ewaluacji i certyfikacji, które bada warunki bezpieczeństwa oraz podatność produktów, urządzeń i systemów używanych do zapewnienia funkcjonowania sieci, systemów i infrastruktury krytycznej, z zastrzeżeniem przepisów o ochronie informacji niejawnych[49].

4. Podsumowanie

Włoski system cyberbezpieczeństwa opisany w *Dyrektywie wyznaczającej wskazówki w zakresie narodowej cyberobrony i bezpieczeństwa informatycznego* jest przykładem systemu rozproszonej odpowiedzialności. Włochy nie zdecydowały się na powołanie centralnego urzędu odpowiedzialnego za bezpieczeństwo cybernetyczne kraju, obarczając odpowiedzialnością za to zagadnienie różne urzędy administracji. Centralnym punktem systemu jest automatycznie Prezes Rady Ministrów, który jest odpowiedzialny za całość administracji rządowej. Premiera wspierają ciała kolegialne złożone z przedstawicieli różnych podmiotów, mające zapewnić koordynację działań administracji w tym obszarze.

W systemie cyberbezpieczeństwa Republiki Włoskiej przewidziano istotną rolę dla podmiotów Systemu Informacyjnego Bezpieczeństwa, który tworzą agencje wywiadowcze AISI i AISE oraz koordynujący ich działalność Departament Informacyjny Bezpieczeństwa. Dotyczy to zwłaszcza DIS, który zapewnia funkcjonowanie Centrum Cyberbezpieczństwa – ciała o charakterze po części koordynacyjnym, po części informacyjnym, a po części opniodawczo-doradczym, posiadającego szczególne kompetencje w zakresie zarządzania sytuacją kryzysu cybernetycznego.

Samym służbom wywiadowczym AISI i AISE poza uczestnictwem w pracach Centrum Cyberbezpieczeństwa przypisano głównie klasyczne funkcje analityczno-informacyjne, nakierowane na wspieranie organów decyzyjnych.

[49] http://www.sicurezzanazionale.gov.it/sisr.nsf/documentazione/normativa-di-riferimento/dpcm-17-febbraio-2017.html [dostęp: 2 VIII 2017].

VII. CHARAKTERYSTYKA NAJWAŻNIEJSZYCH PROBLEMÓW ZWIĄZANYCH Z WYMIANĄ INFORMACJI O ZAGROŻENIACH CYBERBEZPIECZEŃSTWA W USA NA PRZYKŁADZIE USTAWY *CYBERSECURITY ACT OF 2015*

Dnia 18 grudnia 2015 r. ówczesny Prezydent USA Barack Obama podpisał ustawę *Cybersecurity Act of 2015*[50] określaną jako najważniejszy przyjęty do tej pory w Stanach Zjednoczonych federalny akt normatywny dotyczący cyberberpieczeństwa. Głównym elementem ustawy jest stworzenie dobrowolnego mechanizmu wymiany informacji o zagrożeniach bezpieczeństwa systemów i sieci informatycznych między jednostkami federalnymi, a także podmiotami należącymi do sektora prywatnego a tymi jednostkami. Ustawa wprowadza również przepisy wyłączające odpowiedzialność podmiotów prywatnych za ewentualne szkody związane z przekazaniem informacji w trybie wynikającym z ustawy oraz autoryzuje podejmowanie przez jednostki – zarówno publiczne, jak i prywatne – działań związanych z monitorowaniem niektórych systemów informatycznych i stosowaniem instrumentów defensywnych do celów zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Ten akt wprowadza również przepisy mające na celu osiągnięcie wyższego poziomu skuteczności środków ochronnych wykorzystywanych przez agencje federalne oraz poprawę gotowości najważniejszych systemów i sieci informatycznych do skutecznego reagowania na ewentualne zagrożenia[51].

Celem ustawodawcy było zatem stworzenie podstaw prawnych dobrowolnego przekazywania informacji mającego zachęcać podmioty publiczne i prywatne do wymiany informacji o zagrożeniach cyberbezpieczeństwa, bez nieuzasadnionych ograniczeń prawnych i perspektywy odpowiedzialności na gruncie cywilnym oraz karnym, za przekazanie tego rodzaju informacji. Jednocześnie ustawa dąży do zapewnienia wysokiego poziomu ochrony danych osobowych i innych informacji niezwiązanych z omawianymi zagrożeniami. Skuteczność przewidzianych w ustawie mechanizmów w dużej mierze będzie zależeć od woli i inicjatywy podmiotów posiadających informacje o zagrożeniach cyberbezpieczeństwa. Hipotetycznie można zakładać, że nadanie przewidzianym w ustawie instrumentom dobrowolnego charakteru miało zwiększyć szanse na realizację jednego z najważniejszych celów *Cybersecurity Act of 2015*, deklarowanego w uzasadnieniu ustawy – osiągnięcia większego poziomu współpracy w sferze cyberbezpieczeństwa pomiędzy organami państwa a podmiotami prywatnymi z uwagi na eskalację zagrożeń w tym zakresie[52].

1. Geneza ustawy

W ciągu ostatnich 20 lat informacje dotyczące potencjalnych zagrożeń i ataków cybernetycznych były wymieniane za pośrednictwem tzw. Centrów Wymiany i Analizy

[50] Tekst ustawy dostępny na stronie https://www.dni.gov/index.php/ic-legal-reference-book/cybersecurity-act-of-2015 [dostęp: 22 IX 2017].

[51] *Congress Passes and President Signs Long Anticipated Measure Setting Framework for Sharing Cyber Threat Information with Federal Government and Private Sector*, Sullivan&Cromwell LLP, https://www.sullcrom.com/siteFiles/Publications/SC_Publication_The_Cybersecurity_Act_of_2015.pdf [dostęp:16 IX 2017].

[52] *Joint Explanatory Statement to Accompany the Cybersecurity Act of 2015*, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/jes%20for%20cybersecurity%20act%20of%202015.pdf [dostęp: 19 IX 2017].

Informacji (Information Sharing and Analysis Center – ISAC)[53]. Te podmioty zostały utworzone w 1998 r. na podstawie prezydenckiej dyrektywy nr 63 z 22 maja 1998 r. o ochronie infrastruktury krytycznej[54]. W dokumencie podkreślano konieczność opracowania skutecznego systemu ochrony infrastruktury krytycznej, w tym najważniejszych systemów i sieci informatycznych przez stworzenie mechanizmów pozwalających na efektywną neutralizację zarówno fizycznych, jak i cybernetycznych ataków i innych form nielegalnego oddziaływania na te systemy. Centra miały odgrywać rolę mechanizmu umożliwiającego zbieranie, analizowanie i przekazywanie informacji mogących mieć istotne znaczenie dla podmiotów sektora prywatnego oraz dla Narodowego Centrum Ochrony Infrastruktury (National Infrastructure Protection Center – NIPC)[55] – z punktu widzenia cyberbezpieczeństwa. Do zadań ISAC miało również należeć przesyłanie podmiotom sektora prywatnego informacji uzyskanych od NIPC.

Pomimo rosnącego znaczenia centrów ISAC, podmioty zaangażowane w proces wymiany informacji za ich pośrednictwem oraz eksperci z zakresu cyberbezpieczeństwa argumentowali, że potencjalne czynniki ryzyka związane z wymianą informacji za pośrednictwem ISAC, dotyczące np. odpowiedzialności cywilnej za udostępnienie niezgodne z prawem danych czy ochrony własności intelektualnej, powodują, że efektywność wymiany informacji za pośrednictwem wymienionych organów była ograniczona. W celu neutralizacji tych problemów prezydent podpisał tzw. *Executive Order 13691*[56] w celu wzmocnienia i wspierania tej wymiany zarówno w sektorze prywatnym, jak i między podmiotami sektora prywatnego a organami administracji. Dokument przewidywał utworzenie, ISAO (Information Sharing and Analysis Organizations) – podmiotów odpowiedzialnych za tworzenie tzw. dobrych praktyk w omawianym zakresie oraz doprecyzował zakres kompetencji i sposób działania National Cybersecurity and Communications Integration Center – NCICC – agencji wchodzącej w skład Departamentu Bezpieczeństwa Wewnętrznego (Department of Homeland Security), odpowiedzialnej za koordynację i wymianę informacji zarówno między poszczególnymi jednostkami rządu federalnego, jak i między tymi jednostkami a podmiotami niewchodzącymi w skład administracji rządowej[57].

Przyjęcie ustawy *Cybersecurity Act of 2015* było poprzedzone licznymi inicjatywami legislacyjnymi, które miały stanowić odpowiedź organów federalnych na coraz liczniejsze przypadki ataków cybernetycznych czy szpiegostwa przemysłowego, skutkujących kradzieżą informacji handlowych, własności intelektualnej czy nieuprawnionym dostępem do wrażliwych informacji wytwarzanych i przetwarzanych przez poszczególne organy administracji publicznej. Rok 2014 był określany mianem „*cyber breach*" – spadek poziomu bezpieczeństwa informacji przetwarzanych w systemach i sieciach informatycznych postrzegano jako czynnik poważnie zagrażający bezpieczeństwu organów państwa oraz interesom podmiotów prywatnych, kluczowych z punktu widzenia bezpieczeństwa gospodarczego[58].

[53] Tamże.

[54] *Presidential Decision Directive/NSC-63*, May 22, 1998, https://fas.org/irp/offdocs/pdd/pdd-63.htm [dostęp: 16 IX 2017].

[55] Zgodnie z dyrektywą nr 63 w skład NIPC wchodzili funkcjonariusze FBI, Secret Service i innych organów mających istotne doświadczenie w zakresie zwalczania przestępstw informatycznych, a także przedstawiciele Departamentu Obrony i tzw. wspólnoty wywiadowczej (Intelligence Community). Zadaniem NIPC było przesyłanie innym podmiotom ostrzeżeń o zagrożeniach cyberbezpieczeństwa oraz dokonywanie analiz tego rodzaju zagrożeń.

[56] *Executive Order of February 13*, 2015, https://www.federalregister.gov/documents/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing [dostęp: 16 IX 2017].

[57] *Congress Passes and President Signs*…, s. 2.

[58] U.*S. House of Representatives Permanent Select Committee on Intelligence*, The Protecting Cyber

Inicjatywa legislacyjna obu izb Kongresu miała w tym wypadku charakter rozłączny: niemal równocześnie, w marcu 2015 r., Senat zainicjował prace nad projektem *Cybersecurity Information Sharing Act* – CISA[59], Izba Reprezentantów zaś – nad *Protecting Cyber Networks Act* – PCNA[60]. Oba wymienione akty tworzyły mechanizm umożliwiający podmiotom prywatnym wymianę informacji o zagrożeniach cybernetycznych, zachodziły między nimi jednak istotne różnice dotyczące sposobu i trybu, w którym ta wymiana ma być prowadzona, oraz nadzoru na tym procesem.

Mając na uwadze powyższe czynniki oraz dążenie ówczesnej administracji do stworzenia skutecznych podstaw prawnych wymiany informacji w zakresie cyberbezpieczeństwa, procedowane w obu izbach Kongresu projekty CISA i PCNA uległy połączeniu, tworząc *Cybersecurity Act of 2015*[61]. Ten akt należy zatem traktować jako projekt o charakterze kompromisowym mający na celu poprawę skuteczności funkcjonującego dotychczas w USA systemu, a także doprowadzenie do znalezienia odpowiedniej równowagi między wymienionymi powyżej pierwotnymi projektami i stworzenie jednego, spójnego aktu regulującego omawianą problematykę.

2. Charakterystyka najważniejszych elementów ustawy

C*ybersecurity Act of 2015* składa się z czterech tytułów:

1. *Cybersecurity Information Sharing* – przepisy tworzące scentralizowany mechanizm wymiany informacji z zakresu cyberbezpieczeństwa pomiędzy podmiotami sektora prywatnego;
2. *National Cybersecurity Advancement* – poprawa poziomu cyberbezpieczeństwa organów administracji;
3. *Federal Cybersecurity Workforce Assessment* – ocena zdolności i zasobów w zakresie cyberbezpieczeństwa;
4. *Other Cyber Matters* – pozostałe przepisy.

Celem niniejszego opracowania jest przedstawienie najważniejszych elementów tytułu I ustawy – *Cybersecurity Information Sharing*.

3. Wybrane definicje

- Cel związany z cyberbezpieczeństwem (*Cybersecurity Purpose* – sekcja 102 pkt 4) – cel związany z ochroną systemów informatycznych lub informacji przechowywanych, przetwarzanych lub przesyłanych za pośrednictwem tego systemu przed zagrożeniami dla cyberbezpieczeństwa lub podatnością systemów na ataki informatyczne.
- Zagrożenie cyberbezpieczeństwa (*Cybersecurity Threat* – sekcja 102 pkt 5) – działanie niepodlegające ochronie na podstawie Pierwszej Poprawki do Konstytucji Stanów Zjednoczonych, dokonane w systemie informatycznym lub

Networks Act (H.R.1560), s. 1, https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/new%20bill%20summary%20pdf.pdf [dostęp: 16 IX 2017].

[59] Projekt H.R. 1560 (114th): *Cybersecurity Information Sharing Act of 2015* został przegłosowany przez obie izby.

[60] Projekt H.R. 1560 (114th): *Protecting Cyber Networks Act* został przegłosowany przez Izbę Reprezentantów 22 IV 2015 r., nie został jednak przegłosowany przez Senat, proces legislacyjny zatem nie został zakończony, https://www.govtrack.us/congress/bills/114/hr1560 [dostęp: 22 IX 2017].

[61] J.L. Tran, *Navigating the Cybersecurity Act of 2015*, Chapman Law Review, http://digitalcommons.chapman.edu/cgi/viewcontent.cgi?article=1377&context=chapman-law-review [dostęp: 22 IX 2017].

za jego pośrednictwem, mogące skutkować naruszeniem bezpieczeństwa, dostępności, poufności lub integralności systemu informatycznego lub informacji przechowywanych, przetwarzanych lub przesyłanych przez ten system.

- Wskaźnik zagrożenia cybernetycznego (*Cybersecurity Threat Indicator* – sekcja 102 pkt 6) – informacja niezbędna do opisu lub identyfikacji –
  A. Wrogich działań rozpoznawczych, w tym wykazujących anomalie wzorców komunikacji, których celem może być pozyskiwanie informacji technicznych związanych z zagrożeniem dla cyberbezpieczeństwa lub z elementami systemu wykazującymi podatność na ataki,
  B. Metod obejścia systemu kontroli lub wykorzystywania podatności systemu na ataki,
  C. Podatności na ataki, w tym wykazującej anomalie aktywności, która może świadczyć o podatności określonych elementów systemu na atak,
  D. Metod powodujących, że użytkownik uprawniony do dostępu do systemu, do zgromadzonych w nim lub przesyłanych za jego pośrednictwem informacji w sposób nieświadomy umożliwia obejście systemu kontroli lub wykorzystanie podatności systemu na atak,
  E. Złośliwego kierowania i kontroli nad systemem,
  F. Faktycznej lub potencjalnej szkody spowodowanej incydentem, w tym opisu informacji uzyskanej z systemu wskutek wystąpienia określonego zdarzenia dla cyberbezpieczeństwa,
  G. Jakiekogolwiek innego parametru wskazującego na zagrożenie dla cyberbezpieczeństwa, jeżeli jego ujawnienie nie jest zabronione na mocy innych przepisów,
  H. Jakiejkolwiek kombinacji powyższych elementów.
- Środek defensywny (*Defensive Measure* – sekcja 102 pkt 7) –
  A. Z zastrzeżeniem punktu B, pojęcie środek defensywny oznacza działanie, urządzenie, procedurę, sygnaturę, technikę lub inny instrument stosowany w odniesieniu do systemu informatycznego lub do zgromadzonych w nim informacji, który wykrywa, zapobiega lub zmniejsza skutki znanego, lub którego zaistnienie można podejrzewać, zagrożenia dla cyberbezpieczeństwa lub podatności systemu na atak,
  B. Pojęcie środek defensywny nie obejmuje środków, które niszczą, czynią niezdatnymi do użytku, zapewniają nieautoryzowany dostęp lub wywołują poważną szkodę w systemie informatycznym lub w informacjach zgromadzonych, przetwarzanych lub przesyłanych za pośrednictwem tego systemu, który nie jest w posiadaniu –
     i) prywatnego podmiotu zarządzającego tym środkiem; lub
     ii) innej jednostki lub jednostki federalnej, która będąc do tego należycie umocowaną, wyraziła zgodę na wykorzystanie tego rodzaju środka.
- Jednostka federalna (*Federal Entity* – sekcja 102 pkt 8) – departament lub agencja Stanów Zjednoczonych lub jakakolwiek jednostka organizacyjna takiego departamentu lub agencji.
- System informatyczny (*Information System* – sekcja 102 pkt 9) –
  A. Oznacza system opisany w sekcji 3502 tytułu 44 Kodeksu Stanów Zjednoczonych[62],

[62] Zgodnie z sekcją 3502 tytułu 44 Kodeksu Stanów Zjednoczonych pojęcie system informatyczny oznacza indywidualny zbiór zasobów informacyjnych mający na celu zbieranie, przetwarzanie, przecho-

B. Pojęcie to obejmuje przemysłowe systemy kontroli, takie jak systemy nadzoru i systemy pozyskiwania danych, rozproszone systemy sterowania oraz programowalne kontrolery logiczne.

- Złośliwe kierowanie i kontrola systemu (*Malicious Cyber Command and Control* – sekcja 102 pkt 11) – metody służące do nieautoryzowanej zdalnej identyfikacji, uzyskania dostępu lub użycia systemu informatycznego lub informacji przechowywanych, przetwarzanych lub przesyłanych za pośrednictwem tego systemu.
- Złośliwe rozpoznanie (*Malicious Reconnaissance* – sekcja 102 pkt 12) – metody służące do aktywnego sondowania lub pasywnego monitorowania systemu informatycznego w celu wykrycia jego podatności na ataki, jeżeli są one powiązane ze znanym zagrożeniem cyberbezpieczeństwa lub zagrożeniem, którego wystąpienie można podejrzewać.
- Monitorowanie (*Monitor* – sekcja 102 pkt 13) – pozyskiwanie, identyfikacja, skanowanie lub posiadanie informacji przechowywanych, przetwarzanych lub przesyłanych za pośrednictwem systemu informatycznego.
- Jednostka niefederalna (*Non-Federal Entity* – sekcja 102 pkt 14) –
  A. Z zastrzeżeniem wyjątków przewidzianych w niniejszym paragrafie, pojęcie jednostka niefederalna oznacza jednostkę prywatną, niefederalną agencję rządową lub departament, lub rząd stanowy, lokalny lub plemienny (w tym pododdział polityczny, departament lub ich część składową),
  B. Pojęcie jednostka niefederalna oznacza agencję rządową lub departament Dystryktu Kolumbii, Wspólnoty Puerto Rico, Wysp Dziewiczych Stanów Zjednoczonych, Samoa Amerykańskiego, Marianów Północnych lub jakiegokolwiek innego terytorium znajdującego się w posiadaniu Stanów Zjednoczonych,
  C. Pojęcie jednostka niefederalna nie obejmuje obcego państwa w rozumieniu sekcji 101 ustawy *Foreign Intelligence Surveillance Act of 1978* (50 *United States Code* 1801)[63].
- Jednostka prywatna (*Private Entity* – sekcja 102 pkt 15) –
  A. Z zastrzeżeniem wyjątków przewidzianych w niniejszym paragrafie pojęcie jednostka prywatna oznacza prywatną osobę lub grupę, organizację, współwłasność, partnerstwo, trust, spółdzielnię, korporację lub inną jednostkę handlową lub non-profit, z uwzględnieniem osób pełniących funkcje kierownicze, pracowników lub agentów takiej jednostki,
  B. Pojęcie jednostka prywatna oznacza rząd stanowy, lokalny lub plemienny realizujący zadania użyteczności publicznej związane m.in. z usługami związanymi z elektrycznością, gazem naturalnym i wodą,
  C. Pojęcie jednostka prywatna nie obejmuje obcego państwa w rozumieniu sekcji 101 ustawy *Foreign Intelligence Surveillance Act of 1978*
     i) kontrola bezpieczeństwa (*Security Control* – sekcja 102 pkt 16) – zarządcze, operacyjne i techniczne środki kontrolne wykorzystywane w celu ochrony przed nieuprawnionym działaniem zmierzającym do naruszenia poufności, integralności lub dostępności systemu informatycznego lub zgromadzonych w nim informacji,

wywanie, wykorzystywanie, rozpowszechnianie i zarządzanie informacjami.

[63] *U.S Code* Title 50 Chapter 36 – *Foreign Intelligence Surveillance*, https://www.law.cornell.edu/uscode/text/50/chapter-36 [dostęp: 18 IX 2017].

ii) podatność na ataki (*Security Vulnerability* – sekcja 102 pkt 17) – jakakolwiek cecha sprzętu, oprogramowania, proces lub procedura mogące umożliwić lub ułatwić obejście kontroli bezpieczeństwa.

- Kontrola bezpieczeństwa (*Security Control* – sekcja 102 pkt 16) – zarządzanie, operacyjne i techniczne środki kontroli wykorzystywane w celu ochrony przed nieautoryzowanym działaniem mającym na celu naruszenie poufności, integralności i dostępności systemu informatycznego lub zgromadzonych w nim informacji.
- Podatność systemu na ataki (*Security Vulnerability* – sekcja 102 pkt 17) – jakakolwiek cecha sprzętu, oprogramowania, proces lub procedura mogąca umożliwić lub ułatwić obejście kontroli bezpieczeństwa.

4. Przekazywanie informacji o zagrożeniach cyberbezpieczeństwa przez organy rządu federalnego

Sekcja 103 pkt (a) ustawy zobowiązuje Narodowego Dyrektora ds. Wywiadu, Sekretarza ds. Bezpieczeństwa Wewnętrznego, Sekretarza Obrony i Prokuratora Generalnego do opracowania – po konsultacji z organami kierowniczymi właściwych jednostek federalnych i z poszanowaniem przepisów dotyczących ochrony informacji niejawnych – źródeł i metod wywiadowczych, prawa do prywatności oraz innych praw i wolności obywatelskich, procedur, mających na celu ułatwienie i wspieranie:

1. Szybkiej wymiany danych o wskaźnikach zagrożenia cybernetycznego i środkach defensywnych stanowiących informacje niejawne, będących w posiadaniu rządu federalnego, z przedstawicielami jednostek federalnych i niefederalnych, mających odpowiednie poświadczenie bezpieczeństwa – sekcja 103 (a) (1).

   Zgodnie z dokumentem *Executive Order 13636*[64] organy administracji dążą do szybkiego opracowywania jawnych raportów dotyczących zagrożeń cybernetycznych identyfikujących konkretny podmiot, który został dotknięty określonym atakiem informatycznym lub inną formą niezgodnego z prawem oddziaływania na systemy informatyczne. W przypadku gdy dane o takim zdarzeniu stanowią informacje niejawne, możliwość przekazania podmiotowi dotkniętemu atakiem informacji przez organy rządu federalnego jest uzależniona od posiadania przez ten podmiot poświadczenia bezpieczeństwa. Ponadto muszą być spełnione wymogi związane z ochroną źródeł i metod wywiadowczych. Wszystkie jednostki federalne uczestniczące w procesie wymiany informacji o zagrożeniach dla cyberbezpieczeństwa są zobowiązane do przestrzegania przepisów dotyczących sposobów oznaczania informacji niejawnych czy restrykcji związanych z ograniczeniem ich obiegu, jak np. klauzula ORCON (*Originator Controlled* – zasada przewidująca kontrolę wytwórcy nad sposobem wykorzystania danej informacji). W nagłych sytuacjach będzie możliwe zastosowanie w dalszym ciągu procedury szczególnej przewidzianej w tytule 32 sekcji 2001.52 Kodeksu Stanów Zjednoczonych[65]. Zgodnie z tą procedurą w sytuacjach kryzysowych, w których istnieje poważne zagrożenie życia,

[64] *Executive Order – Improving Critical Infrastructure Cybersecurity*, February 12, 2013, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [dostęp: 19 IX 2017].

[65] *Code of Federal Regulations*, Title 32, Subtitle B, Chapter XX, Part 2001, Subpart E, Section 2001.52, https://www.law.cornell.edu/cfr/text/32/2001.52 [dostęp: 18 IX 2017].

zdrowia lub obronności, szefowie agencji lub osoby przez nich wyznaczone mogą, pod pewnymi warunkami, zezwolić na ujawnienie informacji niejawnych osobie lub osobom nieposiadającym dostępu do informacji niejawnych[66].

2. Szybkiej wymiany z właściwymi jednostkami federalnymi i niefederalnymi informacji o wskaźnikach zagrożeń cyberbezpieczeństwa, środkach defensywnych oraz informacji dotyczących zagrożeń cyberbezpieczeństwa znajdujących się w posiadaniu rządu federalnego, które mogą być odtajnione i przekazane innym organom jako informacje jawne – sekcja 103 (a) (2).
   Efektywność procesu wymiany informacji dotyczących zagrożeń cyberbezpieczeństwa jest w naturalny sposób ograniczona, w przypadku gdy stanowią one informacje niejawne – znacznemu wydłużeniu ulega proces ich dystrybucji, krąg ich odbiorców zaś zostaje znacznie ograniczony. W związku z tym cytowany dokument S*haring of Cyber Threat Indicators and Defensive Measures under the Cybersecurity Information Act of 2015* zachęca jednostki federalne do ograniczenia korzystania z reżimu prawnego przewidzianego dla ochrony informacji niejawnych w odniesieniu do wymiany omawianych kategorii informacji. Te podmioty powinny, jeżeli nie jest to sprzeczne z charakterem określonych informacji, dążyć do odtajniania, obniżania klauzul tajności oraz usuwania najbardziej wrażliwych elementów. Jednostki federalne należące do tzw. wspólnoty wywiadowczej (Intelligence Community) powinny rozpowszechniać jawne informacje o zagrożeniach cyberbezpieczeństwa przez aplikacje typu „*tearline*"[67].
3. Szybkiej wymiany z właściwymi jednostkami federalnymi i niefederalnymi, a także przekazywanie – w razie potrzeby – do publicznej wiadomości informacji o wskaźnikach zagrożenia cyberbezpieczeństwa i środkach defensywnych niestanowiących informacji niejawnych, w tym informacji jawnych, których udostępnianie podlega kontroli (ang. *controlled unclassified*), będących w posiadaniu rządu federalnego – sekcja 103 (a) 3.
   Ustawa zakłada szeroką wymianę jawnych informacji dotyczących wskaźników zagrożeń cyberbezpieczeństwa i środków defensywnych zarówno pomiędzy jednostkami federalnymi, jak i tymi jednostkami a jednostkami niefederalnymi, z zastrzeżeniem szczególnych instrukcji w zakresie sposobu dystrybucji określonych informacji. Jeżeli jednostka federalna otrzyma od jednostki niefederalnej dane dotyczące wskaźnika zagrożeń lub środka defensywnego w sposób inny niż przewidziany w sekcji 105 (c) (mechanizm stworzony przez Departament Bezpieczeństwa Wewnętrznego, Departament of Homeland Security – DHS), powinna je przekazać

[66] *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Act of 2015*, February 16, 2016, s. 7, https://www.us-cert.gov/sites/default/files/ais_files/Federal_Government_Sharing_Guidance_%28103%29.pdf [dostęp: 18 IX 2017].

[67] Ang. *tearline* – rodzaj aplikacji służąca do wymiany jawnych informacji wywiadowczych stworzonych na podstawie dokumentów o wyższym poziomie tajności, z których zostały usunięte najbardziej wrażliwe elementy, np. informacje o źródłach czy sposobach pozyskania danej informacji. Z tego rodzaju aplikacji mogą korzystać wyłącznie upoważnione osoby – pracownicy tzw. wspólnoty wywiadowczej (Intelligence Community). Założeniem leżącym u podstaw stworzenia tego rodzaju aplikacji była możliwość szerokiego rozpowszechniania informacji o ewentualnych zagrożeniach w celu wspierania ogólnie pojmowanych interesów bezpieczeństwa narodowego; Intelligence Community Directive 209, 6 September 2012 – *Tearline Production and Dissemination*, https://fas.org/irp/dni/icd/icd-2IXpdf [dostęp: 19 IX 2017]. Ogólne informacje o aplikacji zawarto w artykule prasowym na stronie https://www.wired.com/2017/04/american-spies-now-smartphone-app/ [dostęp: 19 IX 2017]. Zob. *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government*, s. 9.

wszystkim pozostałym właściwym jednostkom federalnym, biorąc pod uwagę zakres ich zadań. W miarę możliwości powinna też zdjąć z nich klauzulę tajności i usunąć elementy wrażliwe, wykorzystując do tego aplikacje typu „*tearline*"[68].

4. Szybkiej wymiany z właściwymi jednostkami federalnymi i niefederalnymi informacji będących w posiadaniu rządu federalnego o zagrożeniach cyberbezpieczeństwa dotyczących tych jednostek, w celu zapobiegania lub neutralizacji negatywnych skutków tych zagrożeń – sekcja 103 (a) (4).
   Zgodnie z sekcją 4 (b) dokumentu *Executive Order 13636* sekretarz ds. Bezpieczeństwa Wewnętrznego i prokurator generalny, współdziałając z dyrektorem Wywiadu Narodowego, zostali zobowiązani do stworzenia systemu pozwalającego na szybkie przekazywanie raportów o zagrożeniach cyberbezpieczeństwa podmiotom, których dotyczy konkretne zagrożenie. Ten proces obejmuje również dystrybucję niejawnych raportów do upoważnionych jednostek infrastruktury krytycznej (ang. *critical infrastructure entities*)[69]. Na podstawie sekcji 103 (a) 4 ustawy organu rządu federalnego powinny one w sposób analogiczny przekazywać informacje również jednostkom niefederalnym, które zostały lub mogą zostać dotknięte wrogą działalnością w cyberprzestrzeni – również tym, które nie należą do tzw. *critical infrastructure entities*[70].
5. Okresowej wymiany tzw. dobrych praktyk w zakresie cyberbezpieczeństwa opracowanych na podstawie analiz wskaźników zagrożeń cyberbezpieczeństwa, środków defensywnych i innych informacji dotyczących tego rodzaju zagrożeń będących w posiadaniu rządu federalnego, z uwzględnieniem potrzeb małych przedsiębiorstw – sekcja 103 (a) (5).
   Do grupy podmiotów opracowujących tzw. dobre praktyki w zakresie bezpieczeństwa należą m.in. Narodowy Instytut Standaryzacji i Technologii (National Institute of Standards and Technology – NIST), Departament Bezpieczeństwa Wewnętrznego Departament Obrony oraz Agencja Bezpieczeństwa Narodowego[71].

W punkcie (b) sekcji 103 zawarto katalog przesłanek, którym powinny odpowiadać procedury wymiany informacji o zagrożeniach cyberbezpieczeństwa. Jako przykład należy wskazać ogólny wymóg, zgodnie z którym te procedury powinny zapewniać, że rząd federalny ma informacje o wskaźnikach zagrożeń i środkach defensywnych w czasie rzeczywistym, spełniające standardy wynikające z ochrony informacji niejawnych, i utrzymuje zdolności umożliwiające ich wymianę. Te procedury powinny przewidywać tryb, w jakim podmioty, których dane osobowe zostały przekazane niezgodnie z przepisami tytułu I ustawy, powinny zostać poinformowane o tym naruszeniu.

5. Monitorowanie systemów informatycznych i zarządzanie środkami defensywnymi przez jednostki prywatne

Sekcja 104 ustawy upoważnia jednostki prywatne do monitorowania systemów informatycznych i stosowania środków defensywnych zarówno w odniesieniu do wła-

[68] Tamże, s. 10.

[69] Pod pojęciem infrastruktura krytyczna (ang. *critical infrastructure*) zgodnie z sekcją 2 *Executive Order 13636* należy rozumieć systemy i środki, zarówno materialne, jak i wirtualne, na tyle istotne dla Stanów Zjednoczonych, że ich niezdolność do działania lub ich zniszczenie będzie negatywnie wpływało na bezpieczeństwo, narodowe bezpieczeństwo gospodarcze, narodową ochronę zdrowia publicznego lub na sprawy łącznie dotyczące tych elementów.

[70] *Sharing of Cyber Threat Indicators*…, s. 13.

[71] Tamże, s. 15–16.

snych systemów informatycznych, jak i systemów wykorzystywanych przez inne podmioty, po uzyskaniu ich pisemnej zgody (przepis ten obejmuje inne jednostki niefederalne oraz jednostki federalne – po uzyskaniu pisemnej zgody posiadającego odpowiednie kompetencje przedstawiciela tej jednostki federalnej). Jednostki, o których mowa, mogą również monitorować informacje przechowywane, przetwarzane lub przesyłane za pośrednictwem określonego systemu informatycznego [sekcja 104 (a) i (b)][72].

Sekcja 104 (c) upoważnia jednostki niefederalne do wymiany i otrzymywania od innych jednostek niefederalnych lub od organów rządu federalnego informacji dotyczących wskaźników zagrożeń cyberbezpieczeństwa i środków defensywnych, wyłącznie w celach związanych z ochroną cyberbezpieczeństwa i zgodnie z zasadami regulującymi ochronę informacji niejawnych. Informacje przekazane organom stanowym, lokalnym i plemiennym mogą zostać wykorzystane, oprócz celów związanych z ochroną cyberbezpieczeństwa, również do rozpoznawania, zapobiegania i ścigania przestępstw wymienionych w sekcji 105(d)(5)(A) – m.in. szpiegostwo i terroryzm.

Podmiot monitorujący system informatyczny, zarządzający środkami defensywnymi oraz dostarczający lub odbierający wskaźniki zagrożeń cyberbezpieczeństwa lub środki defensywne jest zobowiązany do wprowadzenia i wykorzystywania instrumentu kontroli bezpieczeństwa (ang. *security control*) w celu ochrony przed nieuprawnionym ujawnieniem lub pozyskaniem informacji dotyczących ww. wskaźników lub środków (sekcja 104 d). Ponadto sekcja nakłada na podmiot zamierzający dokonać wymiany informacji o wskaźnikach zagrożeń cyberbezpieczeństwa obowiązek weryfikacji, czy dany wskaźnik zawiera informacje niedotyczące bezpośrednio tego rodzaju zagrożeń, które – zgodnie z jego wiedzą – stanowią dane osobowe określonej osoby fizycznej lub informacje pozwalające na jej identyfikację, i usunięcia tego rodzaju danych lub zastosowania w tym celu odpowiednio skonfigurowanych urządzeń technicznych [sekcja 104 (d) (2) (A) i (B)][73].

Przepis sekcji 104 (e) jest jednym z przykładów tzw. *safe harbours* – przepisów wyłączających odpowiedzialność podmiotów prywatnych za wymianę informacji o zagrożeniach cyberbezpieczeństwa, jeżeli ta wymiana jest prowadzona zgodnie z przepisami ustawy. Wymiana informacji między dwiema (lub więcej) jednostkami prywatnymi na temat wskaźników zagrożeń, środków defensywnych lub udzielania wsparcia w zakresie zapobiegania, badania lub minimalizacji skutków wymienionych zagrożeń nie stanowi naruszenia jakichkolwiek przepisów prawa antymonopolowego (ang. *antitrust laws*).

6. Wymiana informacji o wskaźnikach zagrożeń cyberbezpieczeństwa i środków defensywnych z organami rządu federalnego

Prokurator Generalny i Sekretarz ds. Bezpieczeństwa Wewnętrznego zostali zobowiązani, nie później niż 180 dni od daty przyjęcia ustawy oraz w porozumieniu z organami kierowniczymi właściwych jednostek federalnych, do opracowania i opublikowania dokumentów opisujących procedury dotyczące sposobu postępowania organów rządu federalnego na wypadek otrzymania informacji o wskaźnikach zagrożeń i środkach defensywnych [sekcja 105 (a) 2].

[72] *Congress Passes and President Signs*…, s. 6–7.

[73] *Federal Guidance on the Cybersecurity Information Sparing Act of 2015*, Harvard Law School Forum on Corporate Governance and Financial Regulation, posted by Brad S. Karp, Paul, Weiss, Rifkind, Wharton & Garrison LLP, March 3, 2016, https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ [dostęp: 18 IX 2017].

Podczas gdy sekcja 104 (c) dotyczyła wymiany wskaźników zagrożeń i środków defensywnych zarówno z jednostkami federalnymi, jak i niefederalnymi, sekcja 105 dotyczy stricte wymiany tego rodzaju informacji z organami rządu federalnego. Wymiana jest prowadzona przez zarządzaną przez DHS platformę wymiany informacji, o której mowa w pkt c sekcji 105. Sekretarz ds. Bezpieczeństwa Wewnętrznego, nie później niż 90 dni od przyjęcia ustawy, w porozumieniu z organami kierowniczymi właściwych jednostek federalnych, opracowuje i implementuje w Departamencie Bezpieczeństwa Wewnętrznego procedury, które:

- umożliwiają przyjmowanie od jednostek niefederalnych w czasie rzeczywistym wskaźników zagrożeń i środków defensywnych,
- po uzyskaniu odpowiedniego certyfikatu potwierdzającego, że wymiana informacji działa w sposób kompletny i efektywny – będą służyły rządowi federalnemu do otrzymywania informacji dotyczących wskaźników zagrożeń oraz środków defensywnych udostępnianych mu przez jednostki niefederalne,
- gwarantują, że wszystkie właściwe jednostki federalne otrzymują w sposób zautomatyzowany informacje dotyczące wskaźników zagrożeń oraz środki defensywne za pośrednictwem wykorzystywanego przez DHS instrumentu działającego w czasie rzeczywistym,
- spełniają wymogi określone w procedurach i wytycznych tworzonych na podstawie niniejszej sekcji,
- nie ograniczają ani nie wyłączają zgodnego z prawem ujawnienia danych dotyczących komunikacji, nagrań lub innych informacji, w tym m.in. przekazywania przez jednostki niefederalne innym jednostkom niefederalnym lub jednostkom federalnym informacji dotyczących podejrzenia popełnienia przestępstwa, z uwzględnieniem wskaźników zagrożeń lub środków defensywnych, udostępnionych jednostce federalnej w ramach śledztwa federalnego.

Jednostki niefederalne mogą przekazywać tego rodzaju informacje DHS, podczas gdy ten organ będzie zobowiązany do przekazania w sposób zautomatyzowany otrzymanych w ten sposób informacji do Departamentu Handlu, Obrony, Energii, Sprawiedliwości, Skarbu oraz do Biura Narodowego Dyrektora Wywiadu zgodnie z sekcją 105 (a) (3) (A)[74].

Przekazane w trybie sekcji 105 organom rządu federalnego wskaźniki zagrożeń cyberbrzpieczeństwa oraz środki defensywne mogą być udostępnione, przechowywane lub wykorzystane przez agencję lub departament federalny, ich jednostkę organizacyjną, funkcjonariusza, pracownika lub przez agenta rządu federalnego wyłącznie:

- dla celów związanych z cyberbezpieczeństwem,
- w celu identyfikacji zagrożenia cyberbezpieczeństwa (w tym jego źródła) lub podatności systemu informatycznego na atak,
- w celu reagowania, zapobiegania lub neutralizacji konsekwencji bezpośredniego ryzyka utraty życia lub zdrowia, wystąpienia poważnej szkody gospodarczej, w tym aktu terrorystycznego lub użycia broni masowego rażenia,
- w celu reagowania, zapobiegania, neutralizacji konsekwencji lub ścigania poważnego zagrożenia dla małoletniego, w tym wykorzystywania seksualnego i zagrożeń jego fizycznego bezpieczeństwa;

[74] *Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015*, https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf, s. 12 [dostęp: 18 IX 2017].

- w celu zapobiegania, rozpoznawania, udaremnienia lub ścigania przestępstw: oszustwa, kradzieży tożsamości, szpiegostwa lub przestępstw związanych z naruszeniem tajemnicy handlowej.

7. Przepisy wyłączające odpowiedzialność podmiotów prywatnych za przekazywanie informacji zgodnie z ustawą

Sekcja 106 (a) stanowi, że przeciwko podmiotowi prywatnemu prowadzącemu działalność polegającą na monitorowaniu systemu informatycznego na podstawie sekcji 104 (a) nie może być wniesiona jakakolwiek skarga, jeżeli ta działalność była prowadzona zgodnie z przepisami ustawy.

Na zasadzie analogii – zgodnie z sekcją 106 (b) podmiot prywatny nie może zostać pociągnięty do odpowiedzialności za wymienianie informacji związanych ze wskaźnikami zagrożeń cyberbezpieczeństwa lub środków defensywnych zgodnie z sekcją 104 (c), jeżeli ta wymiana odbywała się w myśl przepisów ustawy oraz, w przypadku gdy informacje są przekazywane rządowi federalnemu oraz informacje, o których mowa, były przekazywane za pośrednictwem systemu stworzonego przez DHS[75].

Przekazanie rządowi federalnemu informacji o zagrożeniach cyberbezpieczeństwa nie powoduje uchylenia jakichkolwiek przywilejów ani środków ochronnych przewidzianych na podstawie innych ustaw, w tym tajemnicy handlowej [sekcja 105 (d) (1)].

Informacje przekazane rządowi federalnemu nie podlegają ujawnieniu na podstawie ustawy *Freedom of Information Act* ani na podstawie innych przepisów rangi stanowej czy aktów prawa miejscowego, przewidujących swobodny dostęp do informacji i rejestrów [sekcja 105 (d) (3)][76].

Biorąc pod uwagę to, że konstrukcja ustawy została oparta na założeniu dobrowolnego przekazywania informacji dotyczących zagrożeń cyberbezpieczeństwa, żaden z przepisów ustawy nie powinien być interpretowany jako nakładający obowiązek przekazania danych o wskaźniku zagrożeń lub środka defensywnego ani jako tworzący zobowiązanie do ostrzegania innych podmiotów lub do podejmowania innych działań w związku z otrzymaniem wymienionych informacji [sekcja 106 (c)]. Sekcja 108 (i) expressis verbis stanowi, że nieuczestniczenie danego podmiotu w dobrowolnych działaniach przewidzianych w ustawie, nie pociąga za sobą odpowiedzialności z tego tytułu.

Wnioski

Przyjęcie ustawy *Cybersecurity Act of 2015*, mającej na celu stworzenie mechanizmu wymiany informacji o zagrożeniach cyberbezpieczeństwa, było poprzedzone długotrwałymi rozmowami pomiędzy organami administracji a przedstawicielami przemysłu i sektora prywatnego. Motywem przewodnim prac legislacyjnych było wzmocnienie potencjału zarówno podmiotów publicznych, jak i prywatnych w zakresie identyfikacji omawianych zagrożeń i odpowiedzi na nie. Do najważniejszych kontrowersji wywołanych przez ustawę należy zaliczyć przewidziane w niej rozwiązania dotyczące ochrony prywatności oraz sposobu wykorzystywania przez władze publiczne informacji przekazywanych w trybie opisanym w tytule I ustawy (*Cybersecurity Information Sharing*).

[75] Tamże.

[76] *Federal Guidance on the Cybersecurity*…

Krytycy ustawy podnoszą, że w rzeczywistości jest ona zawoalowaną ustawą inwigilacyjną tworzącą kolejne – obok już istniejących – instrumenty przekazywania organom rządowym informacji o cyberzagrożeniach, zezwalając im jednocześnie na szerokie wykorzystywanie tych informacji również dla celów niezwiązanych z cyberbezpieczeństwem. Ustawa nie zawiera także rozważanego w toku prac legislacyjnych zakazu przekazywania informacji Agencji Bezpieczeństwa Narodowego i Pentagonowi[77]. Sekcja 105 (d) 5 A pozwala na przekazywanie przez organy rządu federalnego otrzymanych zgodnie z ustawą informacji wszystkim agencjom federalnym, departamentom, ich jednostkom organizacyjnym, funkcjonariuszom, pracownikom czy agentom rządu federalnego. Ten sposób sformułowania katalogu podmiotowego potencjalnych odbiorców nie świadczy o tym, że ustawodawca dążył do rzeczywistego ograniczenia przepływu tych danych. Przeciwnie – użycie w przywołanym w poprzednim zdaniu artykule słowa „*any*" (jakikolwiek, każdy) powoduje, że będzie on interpretowany rozszerzająco. Wątpliwości może również budzić szerokie ujęcie w art. 105 (d) 5 A katalogu przesłanek umożliwiających przekazanie informacji.

Kolejnym istotnym problemem jest konstrukcja sekcji 104 (d) 2 zobowiązująca jednostki niefederalne do usunięcia ze wskaźnika zagrożenia lub środka defensywnego informacji niezwiązanych bezpośrednio z cyberbezpieczeństwem, o których ta jednostka w momencie przekazania wie, że stanowią dane osobowe określonej osoby fizycznej lub identyfikują taką osobę. Krytycy ustawy podnoszą, że ten przepis pozwala w konsekwencji na przekazywanie danych osobowych praktycznie w każdym wypadku, czyniąc z tego opcję domyślną, usunięcie danych zaś – wyjątkiem. Obowiązek usunięcia informacji zawierających dane osobowe zachodzi zatem tylko wówczas, gdy jednostka niefederalna ma sprawdzoną wiedzę, że te osoby nie są bezpośrednio powiązane z zagrożeniem cyberbezpieczeństwa, Ten warunek będzie możliwy do spełnienia w nielicznych wypadkach[78].

Na uwagę zasługuje również zarzut przekazywania danych w trybie opisanym w ustawie. Tworzy ono – samo w sobie – potencjalne możliwości kradzieży danych, pomijając równocześnie realne problemy związane z cyberbezpieczeństwem, takie jak wykorzystywanie przez liczne podmioty przestarzałego oprogramowania, brak skutecznych środków ochronnych przed złośliwym oprogramowaniem czy sporadyczne korzystanie z szyfrowania plików. Dobrowolność systemu może powodować brak dostatecznego zainteresowania podmiotów sektora prywatnego udziałem w nim, co sprawi, że system nie będzie miał szans przynieść oczekiwanych rezultatów[79].

Za przyjęciem ustawy opowiadały się natomiast w głównej mierze prywatne podmioty działające w sektorze usług finansowych, argumentując, że przewidziane w ustawie kompleksowa i kolektywna wymiana informacji o zagrożeniach cyberbezpieczeń-

[77] *Last-Minute Budget Bill Allows New Privacy-Invading Surveillance In The Name of Cybersecurity*, https://theintercept.com/2015/12/18/last-minute-budget-bill-allows-new-privacy-invading-surveillance-in-the-name-of-cybersecurity/ [dostęp: 22 IX 2017].

[78] Te argumenty zostały zawarte w liście do prezydenta Baracka Obamy wystosowanym przez organizacje społeczeństwa obywatelskiego i ekspertów w dziedzinie bezpieczeństwa informatycznego; list dostępny na stronie https://static.newamerica.org/attachments/4459-pr-massive-coalition-of-security-experts-companies-and-civil-society-groups-urge-obama-to-veto-cisa/Final_Coalition%20Ltr%20Urging%20Pres.%20to%20Veto%20CISA.8b33e2d86dc14780b35c9cde44a41797.pdf [dostęp: 22 IX 2017].

[79] https://static.newamerica.org/attachments/4459-pr-massive-coalition-of-security-experts-companies-and-civil-society-groups-urge-obama-to-veto-cisa/Final_Coalition%20Ltr%20Urging%20Pres.%20to%20Veto%20CISA.8b33e2d86dc14780b35c9cde44a41797.pdf [dostęp: 22 IX 2017].

stwa przyczyni się do skutecznego zabezpieczenia interesów ich klientów w obliczu intensyfikacji tych zagrożeń[80].

Dokonanie całościowej oceny wszystkich aspektów funkcjonowania ustawy będzie możliwe dopiero po zbadaniu jej rzeczywistego sposobu działania, wpływu na poziom cyberbezpieczeństwa i ewentualnych naruszeń prawa do prywatności, sygnalizowanych w toku procesu legislacyjnego. Do pozytywnych aspektów tego aktu należy zaliczyć wprowadzenie pewnej spójności legislacyjnej i terminologicznej przez stworzenie definicji takich pojęć, jak: zagrożenie cyberbezpieczeństwa czy cel związany z cyberbezpieczeństwem. Trzeba też się zgodzić z krytyką jej rozwiązań dotyczących ograniczeń w zakresie przekazywania niezwiązanych z zagrożeniem informacji, zawierających dane osobowe lub pozwalających na identyfikację określonej osoby fizycznej, Konstrukcja zawartych w ustawie przepisów nie może być uznana za czynnik przesądzający o tym, że naruszenia prawa do prywatności będą występować w niemożliwej do zaakceptowania skali. Nie jest natomiast przekonujący pogląd, że jest to tak naprawdę kolejna ustawa inwigilacyjna. Biorąc pod uwagę charakter i ilość uprawnień przysługujących organom wchodzącym w skład tzw. Intelligence Community oraz skalę strat spowodowanych atakami cybernetycznymi, jest mało prawdopodobne, że ustawodawca zamierzał po raz kolejny skupić się na rozszerzaniu katalogu tych uprawnień.

[80] http://www.fsroundtable.org/fsr-launches-advertising-campaign-urging-congress-to-pass-cisa/ [dostęp: 22 IX 2017].