NASK Cyber POLICY

Cyberbezpieczeństwo A.D. 2018

Strategia. Policy. Rekomendacje
– cyberbezpieczeństwo w perspektywie policy

www.cyberpolicy.nask.pl

NASK Cyber POLICY

SPIS TREŚCI

Wprowadzenie

Szanowni Państwo,

Państwowy Instytut Badawczy NASK (NASK PIB) od wielu lat działa na rzecz podnoszenia poziomu bezpieczeństwa teleinformatycznego w Polsce. Od 1996 roku w strukturze Instytutu funkcjonuje zespół CERT Polska, pierwszy w Polsce zespół reagowania na incydenty komputerowe. Kompetencje technologiczne i badawcze instytutu w dziedzinie cyberbezpieczeństwa postanowiliśmy rozszerzyć o działania na rzecz propagowania wiedzy z obszaru organizacyjnego, regulacyjnego i strategicznego. Po przyjęciu w 2016 roku tzw. Dyrektywy NIS, rozpoczęliśmy w NASK działania wokół kompetencji w zakresie tzw. *policy level*. W efekcie już rok później uruchomiliśmy portal CyberPolicy (https://cyberpolicy.nask.pl/), który stanowi kompendium wiedzy na temat cyberbezpieczeństwa w aspekcie strategicznym, regulacyjnym i organizacyjnym.

Ustawa o krajowym systemie cyberbezpieczeństwa nałożyła na NASK PIB, rolę CSIRT NASK – jednego z trzech CSIRT poziomu krajowego. Poza działaniami operacyjnymi, legitymizuje ona także działania na poziomie *policy* – prowadzenie analiz strategicznych i opracowywanie rekomendacji, proponowanie rozwiązań systemowych w postaci standardów i dobrych praktyk, czy też wspieranie uczestników krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa.

Publikacja *Cyberbezpieczeństwo A.D.* 2018 to podsumowanie ubiegłego roku w zakresie *policy*. Znajdziecie tu Państwo informacje na temat najważniejszych aktów legislacyjnych i strategicznych w Polsce, Unii Europejskiej, Organizacji Narodów Zjednoczonych, Sojuszu Północnoatlantyckim (NATO) i Organizacji Bezpieczeństwa i Współpracy w Europie. To przegląd najważniejszych inicjatyw i wydarzeń z 2018 roku oraz próba przybliżenia tego, jak kształtuje się dyskusja w zakresie cyberbezpieczeństwa i nowoczesnych technologii na świecie, przed jakimi nowymi wyzwaniami stajemy i jak są one adresowane na różnych forach.

Zapraszam do lektury!

Krzysztof Silicki, Zastępca Dyrektora ds. Cyberbezpieczeństwa i Innowacji, NASK PIB

Polska – przełomowy rok dla cyberbezpieczeństwa

W perspektywie polskiego cyberbezpieczeństwa, rok 2018 z pewnością był przełomowy.

10 maja przyjęta została nowa Ustawa o ochronie danych osobowych, uwzględniająca przepisy zawarte w Rozporządzeniu ogólnym o ochronie danych osobowych (RODO/GDPR). Jest to swoista rewolucja, zapewniająca o wiele silniejszą, niż do tej pory, ochronę prywatności. Przyjęcie ustawy poprzedził proces długotrwałych konsultacji społecznych i międzyresortowych.

5 lipca przyjęto Ustawę o krajowym systemie cyberbezpieczeństwa, implementującą do polskiego porządku prawnego zapisy tzw. Dyrektywy NIS[1] z lipca 2016 roku. Ustawa ta, wraz z aktami delegowanymi, nakreśla kształt ekosystemu cyberbezpieczeństwa RP. Zgodnie z Dyrektywą NIS, czas na implementację zapisów minął 9 maja 2018 roku. Polska nieznacznie spóźniła się więc z wdrożeniem prawa europejskiego. Nad zapisami ustawy pracowała międzyresortowa grupa ekspertów, prowadzono też intensywne konsultacje z sektorami rynku.

Oba akty prawne są niezwykle istotne i stanowią wyzwanie zarówno dla sektora publicznego, jak i prywatnego.

W związku z wejściem w życie Dyrektywy PSD2 wprowadzono także zmiany w Ustawie o usługach płatniczych. Sektor finansowy zyskał tym samym jeszcze silniejsze regulacje w zakresie cyberbezpieczeństwa.

Rok 2018 to także początek prac nad polską strategią sztucznej inteligencji. Kilkumiesięczne wysiłki ekspertów zaowocowały publikacją założeń strategii. Kolejnym etapem będzie wypracowanie właściwego dokumentu.

Ustawa o krajowym systemie cyberbezpieczeństwa

Ustawa o krajowym systemie cyberbezpieczeństwa to pierwszy akt prawny w tym zakresie w Polsce. Jest to implementacja do porządku krajowego tzw. Dyrektywy NIS. Ponieważ Dyrektywa NIS jest harmonizacją minimalną, polski ustawodawca skorzystał z możliwości bardziej szczegółowej regulacji. Dlatego do ustawy została włączona administracja publiczna oraz (pośrednio) sektor telekomunikacyjny. Dodatkowo celem ustawodawcy było wyraźne rozdzielenie obowiązków pomiędzy poszczególnymi CSIRT poziomu krajowego, ustanowienie nadzoru w zakresie cyberbezpieczeństwa (organy właściwe, wprowadzenie kar finansowych), a także stworzenie polityczno-strategicznych ram zarządzania cyberbezpieczeństwem w Polsce (Strategia Cyberbezpieczeństwa RP, powołanie Pełnomocnika i Kolegium ds. Cyberbezpieczeństwa).

Prace nad ustawą prowadzone były przez zespół międzyresortowy, a sam akt nie wyczerpuje złożonego tematu cyberbezpieczeństwa w Polsce. Wiele kwestii, jak na przykład wyznaczenie operatorów usług kluczowych, czy budowa kompetencji organów właściwych, wciąż wymaga wytężonej pracy po stronie administracji. Natomiast sektor prywatny, musi podjąć duży wysiłek, aby dostosować się do nowej regulacji, zwłaszcza w zakresie obowiązkowego raportowania incydentów do właściwego CSIRT poziomu krajowego (do tej pory raportowanie, z wyjątkiem sektora telekomunikacji i operatorów infrastruktury krytycznej, nie było obowiązkowe).

Ustawa obowiązuje od 28 sierpnia 2018 roku.

Zakres ustawy

Ustawa obejmuje trzy typy podmiotów: operatorów usług kluczowych, dostawców usług cyfrowych oraz podmioty publiczne.

Operatorzy usług kluczowych

Operatorzy usług kluczowych to firmy i instytucje świadczące usługi o istotnym znaczeniu dla utrzymania krytycznej działalności społecznej lub gospodarczej, zależne od systemów informatycznych[2]. Ustawa wskazuje sektory, w których mają zostać zidentyfikowani operatorzy usług kluczowych: **energetyczny, transportowy, bankowy i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją) i infrastruktury cyfrowej**[3]. Dokładna lista usług kluczowych jest zawarta w rozporządzeniu wykonawczym do ustawy[4]. **Wykaz operatorów usług kluczowych prowadzi minister właściwy do spraw informatyzacji,** a wpisanie i wykreślenie operatora z wykazu odbywa się na wniosek organu właściwego do spraw cyberbezpieczeństwa. Operatorów identyfikują organy właściwe[5], które wydają decyzję administracyjną[6] na podstawie trzech kryteriów:

1. świadczenie usługi kluczowej w jednym z trzech wskazanych sektorów,

[1] Dyrektywa Parlamentu Europejskiego i Rady wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii; https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148

[2] Operatorzy usług kluczowych (OUK) nie są tożsami z operatorami infrastruktury krytycznej (IK). Kwestie ochrony infrastruktury krytycznej regulowane są na mocy Ustawy z 27 kwietnia 2007 r. o zarządzaniu kryzysowym. Zawarta tam definicja określa IK jako „systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców". Obecnie Rządowe Centrum Bezpieczeństwa prowadzi prace mające na celu przejście od modelu obiektowego do usługowego w dziedzinie ochrony IK.

[3] W ramach infrastruktury cyfrowej wskazano punkty wymiany ruchu internetowego, rejestrację nazw domen najwyższego poziomu i usługi DNS.

[4] Rozporządzenie Rady Ministrów z 11 września 2018 roku w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.

[5] Art. 5 Ustawy o krajowym systemie cyberbezpieczeństwa

[6] Jeśli operator został już wcześniej zidentyfikowany jako operator infrastruktury krytycznej, realizowane przez niego obowiązki wynikające z Ustawy o zarządzaniu kryzysowym, takie jak przygotowanie dokumentacji bezpieczeństwa, zostaną uznane za zrealizowane.

2. usługa musi zależeć od systemów informatycznych,
3. wystąpienie incydentu ma istotny skutek zakłócający dla świadczenia tej usługi.

Ocena istotności skutku zależy od tzw. progów istotności skutku zakłócającego, które zostały wyznaczone przez Radę Ministrów w rozporządzeniu[7].

Obowiązki operatorów usług kluczowych

Operator usługi kluczowej zobowiązany jest wdrożyć zarządzanie bezpieczeństwem w systemie informacyjnym, używanym do świadczenia usługi kluczowej. Ma także obowiązek **systematycznego szacowania ryzyka i dostosowania do niego środków bezpieczeństwa**. Ponadto opracowuje dokumentację dotyczą cyberbezpieczeństwa systemu informacyjnego, uaktualnia ją i przechowuje przez co najmniej 2 lata[8].

Obsługa incydentu jest obowiązkiem operatora. W związku z tym jest zobowiązany do:

- klasyfikowania incydentu na podstawie kryteriów określonych w rozporządzeniu[9],
- zgłoszenia **incydentu poważnego** do właściwego CSIRT, nie później niż **w ciągu 24 godzin** od momentu wykrycia,
- współdziałania z CSIRT w obsłudze incydentu, w tym zapewnienia dostępu do informacji oraz usunięcia podatności systemu.

W przypadku powołania **sektorowego zespołu cyberbezpieczeństwa**, operator dodatkowo przekazuje zgłoszenie do tego zespołu, współdziała z nim wysyłając niezbędne dane i zapewnia dostęp do informacji o rejestrowanych incydentach.

Do realizacji zadań określonych w ustawie, operator powołuje struktury wewnętrzne odpowiedzialne za cyberbezpieczeństwo. Możliwe jest także zawarcie umowy z podmiotem zewnętrznym, który świadczy takie usługi. **Ustawa dopuszcza więc outsourcing usług cyberbezpieczeństwa.** Warunki dla podmiotów świadczących usługi cyberbezpieczeństwa, a także dla wewnętrznych struktur operatorów, określa rozporządzenie z 10 września 2018 r[10].

Operator ma **obowiązek przeprowadzić raz na 2 lata[11] audyt bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej**. Pierwszy audyt powinien odbyć się w ciągu roku od doręczenia decyzji o uznaniu za operatora usługi kluczowej.

Operatorzy usług kluczowych nadzorowani są przez organy właściwe do spraw cyberbezpieczeństwa w zakresie obowiązków wynikających z ustawy. W ramach nadzoru organy właściwe mogą przeprowadzać kontrolę, a także nakładać kary pieniężne.

Dostawcy usług cyfrowych

Do usług cyfrowych (DSP – Digital Service Providers) zaliczane są: **internetowe platformy handlowe, usługi przetwarzania w chmurze i wyszukiwarki internetowe.** Z zakresu ustawy zostały wyjęte małe i mikroprzedsiębiorstwa[12].

Definicje DSP:

Internetowa platforma handlowa – usługa, która umożliwia konsumentom lub przedsiębiorcom zawieranie umów drogą elektroniczną z przedsiębiorcami na stronie internetowej platformy handlowej, albo na stronie internetowej przedsiębiorcy, który korzysta z usług świadczonych przez internetową platformę handlową.

Usługa przetwarzania w chmurze – usługa umożliwiającą dostęp do skalowalnego i elastycznego zbioru zasobów obliczeniowych do wspólnego wykorzystywania przez wielu użytkowników.

Wyszukiwarka internetowa – usługa, która umożliwia użytkownikom wyszukiwanie wszystkich stron internetowych lub stron internetowych w danym języku za pomocą zapytania przez podanie słowa kluczowego, wyrażenia lub innego elementu, przedstawiająca w wyniku odnośniki, odnoszące się do informacji związanych z zapytaniem[13].

Ze względu na transgraniczny charakter usług cyfrowych i międzynarodową specyfikę podmiotów świadczących tego rodzaju usługi, DSP zostały objęte lżejszą regulacją, niż operatorzy usług kluczowych.

Oprócz odpowiedniego zarządzania ryzykiem systemów informacyjnych, wykorzystywanych do świadczenia usługi cyfrowej, DSP mają obowiązek prowadzenia czynności umożliwiających wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów. **W przypadku wystąpienia istotnego incydentu, dostawca usługi cyfrowej musi przekazać informację do właściwego CSIRT nie później niż w ciągu 24 godzin od momentu wykrycia**.

Podobnie jak w przypadku operatorów usług kluczowych, DSP podlegają nadzorowi organów właściwych, które są uprawnione do kontrolowania i nakładania kar pieniężnych.

Podmioty publiczne

W skład krajowego systemu cyberbezpieczeństwa wchodzą również podmioty publiczne takie jak: Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, a także instytuty badawcze i spółki prawa handlowego, wykonujące zadania o charakterze użyteczności publicznej.

Zgodnie z treścią art. 21 **każdy z powyższych podmiotów ma obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa w zakresie zadań publicznych zależnych od systemów informacyjnych.**

Dodatkowo na każdym z podmiotów publicznych spoczywa obowiązek zarządzania incydentem w podmiocie publicznym, w tym zapewnienia jego obsługi. **Czas na zgłoszenie incydentu do właściwego CSIRT nie może przekroczyć 24 godzin od momentu wykrycia.**

Raportowanie incydentów

Trzy CSIRT poziomu krajowego

Ustawa wyznacza **trzy CSIRT poziomu krajowego: CSIRT NASK w strukturach Państwowego Instytutu Badawczego NASK, CSIRT GOV w strukturach Agencji Bezpieczeństwa Wewnętrznego oraz CSIRT MON w strukturach Resortu Obrony Narodowej.** Każdy CSIRT poziomu krajowego ma jasno określone *constituency* – zakres podmiotów, które zobowiązane są raportować i którym świadczy on wsparcie.

CSIRT MON koordynuje obsługę incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej i przedsiębiorstwa o szczególnym znaczeniu gospodarczo-obronnym[14]. CSIRT GOV koordynuje incydenty zgłaszane przez administrację rządową, Narodowy Bank Polski, Bank Gospodarstwa Krajowego oraz operatorów infrastruktury krytycznej[15]. CSIRT NASK koordynuje natomiast incydenty zgłaszane przez pozostałe podmioty, w tym m.in. operatorów usług kluczowych[16], dostawców usług cyfrowych i jednostki samorządu terytorialnego. Do CSIRT NASK incydenty mogą także zgłaszać osoby fizyczne, czyli zwykli obywatele. Można więc powiedzieć, że CSIRT NASK stanowi tzw. CERT ostatniej szansy (CERT *of last resort*[17]). W przypadku incydentów o charakterze terrorystycznym właściwe są CSIRT MON i CSIRT GOV (zgodnie z zapisami ustawy o działaniach antyterrorystycznych i ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego). W przypadku incydentów związanych z obronnością kraju zawsze właściwy jest CSIRT MON. Poniższy schemat przedstawia podział *constituency* pomiędzy trzy CSIRT poziomu krajowego.

Rys. 1. Podział *Constituency* pomiędzy trzy CSIRT poziomu krajowego

[7] Rozporządzenie Rady Ministrów z 11 września 2018 roku w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych.
[8] Z tego zapisu wyłączeni są operatorzy posiadający obiekty, instalacje, urządzenia lub usługi wchodzące w skład infrastruktury krytycznej, którzy posiadają zatwierdzony plan ochrony infrastruktury krytycznej wraz z dokumentacją.
[9] Rozporządzenie Rady Ministrów z 31 października 2018 w sprawie progów uznania incydentu za poważny.
[10] Rozporządzenie Ministra Cyfryzacji z 10 września 2018 roku w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.
[11] Wytyczne do audytu zostały określone w ustawie.
[12] Art. 104 Ustawy o swobodzie gospodarczej z dnia 2 lipca 2004 r. określa mikroprzedsiębiorcę jako przedsiębiorcę, który w co najmniej jednym z dwóch ostatnich lat obrotowych zatrudniał średniorocznie mniej niż 10 pracowników oraz osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz operacji finansowych, nieprzekraczający równowartości w złotych 2 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 2 milionów euro.
Art. 105 ustawy o swobodzie gospodarczej z dnia 2 lipca 2004 r. określa małego przedsiębiorcę jako przedsiębiorcę, który zatrudniał średniorocznie mniej niż 250 pracowników oraz osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz operacji finansowych nieprzekraczający równowartości w złotych 50 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 43 milionów euro
[13] Załącznik 2 do Ustawy o krajowym systemie cyberbezpieczeństwa.
[14] Podmioty te zostały określone w Rozporządzeniu Rady Ministrów z dnia 3 listopada 2015 r. w sprawie wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym.
[15] Zgodnie z Ustawą z 26 kwietnia 2007 roku o zarządzaniu kryzysowym.
[16] Niebędących operatorami infrastruktury krytycznej.
[17] Zgodnie z nomenklaturą ENISA, zawartą w dokumencie Deployment of Baseline Capabilities of National/ Governmental CERTs oznacza to, że w przypadku, kiedy jakiś podmiot nie jest w stanie uzyskać bezpośredniego kontaktu lub oczekiwanej pomocy od podmiotu, który jest zaangażowany w incydent bezpośrednio, zgłaszający przekazuje zapytanie do CSIRT „ostatniej szansy".

Wszystkie trzy CSIRT poziomu krajowego mają za zadanie współpracować z organami właściwymi, ministrem właściwym ds. informatyzacji oraz pełnomocnikiem ds. cyberbezpieczeństwa. Poza tym do ich zadań należy m.in. monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym; szacowanie ryzyka w skali kraju; przekazywanie informacji na temat incydentów i ryzyk innym podmiotom krajowego systemu cyberbezpieczeństwa; wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa oraz reagowanie na zgłoszone incydenty.

Ponadto CSIRT poziomu krajowego zapewniają zaplecze analityczne oraz badawczo-rozwojowe dla krajowego systemu cyberbezpieczeństwa. W tym zakresie m.in. prowadzą zaawansowaną analizę złośliwego oprogramowania i podatności, monitorują wskaźniki zagrożeń, oraz rozwijają narzędzia i metody do wykrywania i zwalczania zagrożeń cyberbezpieczeństwa.

CSIRT poziomu krajowego mogą także wykonywać niezbędne działania techniczne związane z analizą zagrożeń, koordynacją obsługi incydentu poważnego, istotnego i krytycznego. W trakcie obsługi incydentów mogą zawnioskować do organów właściwych o wezwanie operatora usługi kluczowej lub dostawcy usługi cyfrowej do usunięcia podatności.

Rodzaje incydentów

Ustawa wprowadza trzy poziomy incydentów.

Poziom pierwszy to wszystkie zdarzenia o niekorzystnym wpływie na cyberbezpieczeństwo.

Poziom drugi to incydenty poważne[18], występujące u operatorów usług kluczowych; incydenty istotne[19] występujące u dostawców usług cyfrowych oraz incydenty w podmiocie publicznym[20], występujące w podmiotach publicznych. Te incydenty są klasyfikowane przez operatorów usług kluczowych, dostawców usług cyfrowych i podmioty publiczne. Klasyfikacja odbywa się w oparciu o konkretne kryteria. W przypadku operatorów usług kluczowych kryteria wyznacza rozporządzenie Rady Ministrów z dnia 31 października 2018 r. w sprawie progów uznania incydentu za poważny, w przypadku dostawców usług cyfrowych są to progi wyznaczone w Rozporządzeniu Wykonawczym Komisji (UE) 2018/151[21].

Poziom trzeci to incydenty krytyczne[22]. Są to incydenty o dużej skali i niosące za sobą większe zagrożenie, niż te wymienione wcześniej. **Incydent jako krytyczny kwalifikuje właściwy CSIRT poziomu krajowego (CSIRT MON, CSIRT NASK lub CSIRT GOV)**. Poniższa tabela przedstawia poziomy incydentów.

Poziom incydentu	Definicja	Nadawanie klasyfikacji	Konieczność raportowania
Poziom pierwszy	incydent – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo	brak	brak
Poziom drugi	incydent poważny – powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej	operator usługi kluczowej	CSIRT GOV – operatorzy infrastruktury krytycznej CSIRT MON – podmioty podległe RON CSIRT NASK – pozostałe na podstawie kryteriów z rozporządzenia do ustawy o krajowym systemie cyberbezpieczeństwa
	incydent istotny – ma istotny wpływ na świadczenie usługi cyfrowej	dostawca usługi cyfrowej	CSIRT NASK
	incydent w podmiocie publicznym – powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego	podmiot publiczny	CSIRT GOV CSIRT NASK CSIRT MON (zgodnie z constituency)
Poziom trzeci	incydent krytyczny – skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi	CSIRT MON CSIRT GOV CSIRT NASK	tak, przy czym raportujący operator/ dostawca usługi nie zawsze będzie miał świadomość, że jest to incydent krytyczny (np. zaraportuje incydent poziomu drugiego, a właściwy CSIRT poziomu krajowego zmieni jego klasyfikację)

Tabela 1. Poziomy incydentów na podstawie Ustawy o krajowym systemie cyberbezpieczeństwa

Współpraca CSIRT poziomu krajowego

Ustawa zakłada ścisłą współpracę CSIRT poziomu krajowego. Jej elementem jest opracowanie procedur postępowania w przypadku incydentu, którego koordynacja wymaga zaangażowania więcej niż jednego CSIRT.

[18] Incydent poważny – incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej; Ustawa o krajowym systemie cyberbezpieczeństwa art. 2.7.

[19] Incydent istotny – incydent, który ma istotny wpływ na świadczenie usługi cyfrowej w rozumieniu art. 4 rozporządzenia wykonawczego Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiającego zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ (Dz. Urz. UE L 26 z 31.01.2018, str. 48), zwanego dalej „rozporządzeniem wykonawczym 2018/151"; Ustawa o krajowym systemie cyberbezpieczeństwa art. 2.8.

[20] Incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15; Ustawa o krajowym systemie cyberbezpieczeństwa art. 2.9.

[21] https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=CELEX%3A32018R0151

[22] Incydent krytyczny – incydent skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi, klasyfikowany przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV; Ustawa o krajowym systemie cyberbezpieczeństwa art. 2.6.

[23] Zgodnie z ustawą o zarządzaniu kryzysowym przewodniczącym RZZK jest premier, a jego członkami odpowiedni ministrowie działowi. Wprowadzenie formuły Zespołu ds. Incydentów Krytycznych pozwala na szybkie przekazanie informacji o tzw. incydentach krytycznych, czyli „skutkujących znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi" na poziom Rady Ministrów, za pośrednictwem RCB. Pozwoli to łatwiej zarządzać kryzysem, który najprawdopodobniej, w przypadku incydentów krytycznych, będzie miał także skutki kinetyczne.

Poza tym ustawa wprowadza formułę Zespołu ds. Incydentów Krytycznych, który jest organem pomocniczym w sprawach obsługi incydentów krytycznych. W jego skład wchodzą CSIRT poziomu krajowego oraz Rządowe Centrum Bezpieczeństwa jako sekretariat – taka formuła zapewnia współpracę z Rządowym Zespołem Zarządzania Kryzysowego (RZZK)[23]. Dodatkowo do udziału w pracach zespołu mogą być zaproszeni przedstawiciele organów właściwych.

Powołanie Zespołu ds. Incydentów Krytycznych służy wyznaczeniu CSIRT, który będzie wiodącym w obsłudze incydentu krytycznego oraz podziałowi zadań związanych z tą obsługą. Na posiedzeniu może też zostać podjęta decyzja o wystąpieniu z wnioskiem do Prezesa Rady Ministrów w sprawie zwołania Rządowego Zespołu Zarządzania Kryzysowego. *De facto* jest to więc ujęcie problematyki cyberbezpieczeństwa w ramy zarządzania kryzysowego w Polsce.

RODO, a obsługa incydentów

Ustawa o krajowym systemie cyberbezpieczeństwa uwzględnia nowe regulacje, które wprowadziło Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO/GDPR). Poszczególne CSRIT (MON, NASK, GOV), a także sektorowe zespoły bezpieczeństwa, przetwarzają dane osobowe pozyskane w związku z incydentami i zagrożeniami cyberbezpieczeństwa. Są to m.in. informacje o użytkownikach systemów informatycznych, telekomunikacyjnych urządzeniach końcowych czy dane operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów publicznych.

CSRIT oraz sektorowe zespoły bezpieczeństwa mogą przetwarzać tylko takie informacje, które są niezbędne do realizacji zadania, a dane mają zostać usunięte lub zanonimizowane maksymalnie 5 lat po zakończeniu obsługi incydentu, którego dotyczą.

Ustawa obliguje również do opublikowania na stronie internetowej m.in. namiarów na administratora danych osobowych, celu i podstawy prawnej przetwarzania, kategorii przetwarzanych danych, okresu ich przetwarzania czy źródła pochodzenia. Co ważne, podmioty muszą również poinformować o **ograniczeniach obowiązków i praw osób, których dotyczą dane osobowe.**

CSIRT mogą również przetwarzać informacje prawnie chronione, np. tajemnicę przedsiębiorstwa, jeśli jest to konieczne do realizacji ich zadań. Muszą jednak zachować tajemnicę informacji. Oznacza to, że ustawodawca skorzystał z art. 23 GDPR, umożliwiającego wyłączenie niektórych podmiotów z części przepisów rozporządzenia.

Obsługa incydentów a dostęp do informacji publicznej

Informacje o podatnościach, incydentach i ryzyku ich wystąpienia oraz zagrożeniach cyberbezpieczeństwa, **nie podlegają ustawie o dostępie do informacji publicznej.** Nie można więc wymagać od zespołów CSRIT, aby te przekazywały dane dotyczące incydentów w drodze dostępu do informacji publicznej. Takie rozwiązanie ma budować zaufanie w obrębie systemu. CSIRT MON, CSIRT NASK lub CSIRT GOV może jednak opublikować takie informacje w Biuletynie Informacji Publicznej, jeśli jest to **niezbędne, aby zapobiec incydentowi lub zapewnić jego obsługę.** Wcześniej taką decyzję należy skonsultować z operatorem usługi kluczowej lub dostawcą usługi cyfrowej, który zgłosił incydent.

Nadzór

Organy właściwe

Nadzór nad każdym z kluczowych sektorów gospodarki sprawuje organ właściwy ds. cyberbezpieczeństwa. 11 sektorów wymienionych w ustawie podlega kompetencji konkretnych ministrów działowych[24], zgodnie z poniższą tabelą:

Organ właściwy ds. cyberbezpieczeństwa	Sektor/podsektor
Minister właściwy ds. energii	Energia
Minister właściwy ds. transportu	Transport
Minister właściwy ds. gospodarki morskiej i minister właściwy ds. żeglugi śródlądowej	Transport wodny
Komisja Nadzoru Finansowego	Bankowy, Infrastruktura rynków finansowych
Minister właściwy ds. zdrowia	Ochrona zdrowia
Minister właściwy ds. gospodarki wodnej	Zaopatrzenie w wodę pitną i jej dystrybucja
Minister właściwy ds. informatyzacji	Infrastruktura cyfrowa
	Dostawcy usług cyfrowych
Minister Obrony Narodowej (podmioty podległe MON oraz przedsiębiorcy o szczególnym znaczeniu gospodarczo-obronnym)	Ochrona zdrowia
	Infrastruktura cyfrowa
	Dostawcy usług cyfrowych

Tabela 2. Organy właściwe dla poszczególnych sektorów

[24] Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. 1997 nr 141 poz. 943) ustala łącznie 28 działów administracji rządowej w Polsce. Dokument opisuje ich zakres oraz właściwość ministrów kierujących danymi działami.

Organami właściwymi są więc ministrowie właściwi dla konkretnych działów administracji, którzy na podstawie porozumienia mogą powierzyć realizację niektórych zadań jednostkom podległym lub nadzorowanym. **Oznacza to, że jeśli w danym sektorze funkcjonuje regulator sektorowy, może realizować funkcje organu właściwego, zamiast ministra.**

Zadaniem organu właściwego ds. cyberbezpieczeństwa jest analiza podmiotów w danym sektorze i **wydawanie decyzji, które z nich otrzymają status operatora usługi kluczowej.** Poza tym organ właściwy przygotowuje rekomendacje działań, które wzmocnią cyberbezpieczeństwo sektora, a także przeprowadza kontrole podległych mu operatorów.

Sektorowy zespół cyberbezpieczeństwa

Organy właściwe mają możliwość powołania sektorowych zespołów cyberbezpieczeństwa. To od organu właściwego dla danego sektora będzie zależało, czy zespół sektorowy zostanie powołany. Dużą zaletą działania takiego zespołu jest uwzględnienie specyfiki danego sektora, co pozwala dostosować wsparcie dla operatorów usług kluczowych. Zespół nie tylko przyjmuje zgłoszenia o incydentach i pomaga w ich obsłudze, ale również analizuje skutki, wypracowuje wnioski oraz współpracuje z właściwym CSRIT. Może też wymieniać informacje o incydentach poważnych z innymi krajami Unii Europejskiej.

Minister ds. informatyzacji

Minister właściwy ds. informatyzacji odpowiada za cywilne aspekty cyberbezpieczeństwa RP. Do jego zadań należy monitorowanie wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, rekomendowanie obszarów współpracy z sektorem prywatnym, prowadzenie działań informacyjnych na temat dobrych praktyk, programów edukacyjnych oraz szkoleń z poszerzania wiedzy i budowania świadomości w zakresie cyberbezpieczeństwa.

Poza tym to właśnie minister właściwy ds. informatyzacji zapewnia rozwój i utrzymanie systemu teleinformatycznego, którego zadaniem jest wsparcie podmiotów krajowego systemu cyberbezpieczeństwa. Prowadzi także Pojedynczy Punkt Kontaktowy (PPK). PPK odpowiada za współpracę z Komisją Europejską i przekazywanie corocznych raportów, współpracuje z innymi państwami członkowskimi w zakresie cyberbezpieczeństwa oraz koordynuje współpracę pomiędzy organami właściwymi w kraju.

Minister Obrony Narodowej

Do głównych zadań Ministra Obrony Narodowej należy prowadzenie międzynarodowej współpracy w dziedzinie cyberbezpieczeństwa pomiędzy Siłami Zbrojnymi Rzeczypospolitej Polskiej, a właściwymi organami NATO, UE i innych organizacji międzynarodowych. Minister odpowiada również za zapewnienie Siłom Zbrojnym RP zdolności do działań militarnych w cyberprzestrzeni, rozwijanie umiejętności Sił Zbrojnych RP dotyczących cyberbezpieczeństwa poprzez organizację specjalistycznych szkoleń, a także kierowanie obsługą incydentów w czasie stanu wojennego.

Sankcje

Ustawa wprowadza sankcje za nieprzestrzeganie przepisów. Operatorzy usług kluczowych i dostawcy usług cyfrowych mogą zostać ukarani karą pieniężną od 1000 zł do 1 000 000 zł. Kara jest nakładana w drodze decyzji administracyjnej przez organ właściwy do spraw cyberbezpieczeństwa, a wpływy pochodzące z kar stanowią dochód budżetu państwa.

Strategia i koordynacja polityki w zakresie cyberbezpieczeństwa

Strategia Cyberbezpieczeństwa RP

Ustawa nakłada obowiązek przyjęcia Strategii Cyberbezpieczeństwa RP. Projekt opracowuje minister właściwy ds. informatyzacji we współpracy z Pełnomocnikiem ds. Cyberbezpieczeństwa oraz innymi ministrami. Strategia przyjmowana jest uchwałą Rady Ministrów na 5 lat. Co 2 lata dokonywany jest jej przegląd.

Pełnomocnik i Kolegium ds. Cyberbezpieczeństwa

Ponieważ tematyka cyberbezpieczeństwa jest horyzontalna – dotyczy wielu ministerstw i agencji rządowych – w celu koordynacji polityki w skali państwa, ustawa wprowadza Kolegium ds. cyberbezpieczeństwa i Pełnomocnika ds. cyberbezpieczeństwa.

Pełnomocnik jest powoływany i odwoływany przez Prezesa Rady Ministrów w randze sekretarza lub podsekretarza stanu i podlega Radzie Ministrów. Do jego zadań należy:

- analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa;

- nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa;
- opiniowanie dokumentów rządowych, w tym projektów aktów prawnych, mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa;
- upowszechnianie nowych rozwiązań i inicjowanie działań zapewniających cyberbezpieczeństwo na poziomie krajowym;
- inicjowanie krajowych ćwiczeń cyberbezpieczeństwa;
- wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT.

Dodatkowo pełnomocnik prowadzi współpracę międzynarodową, wspiera badania naukowe i rozwój technologii z zakresu cyberbezpieczeństwa, a także działa na rzecz podnoszenia świadomości cyberbezpieczeństwa i bezpiecznego korzystania z Internetu.

Kolegium ds. Cyberbezpieczeństwa jest organem opiniodawczo-doradczym Rady Ministrów. Przewodniczy mu Prezes Rady Ministrów, a w jego skład wchodzą: minister właściwy do spraw wewnętrznych, minister właściwy do spraw informatyzacji, Minister Obrony Narodowej, minister właściwy do spraw zagranicznych, Szef Kancelarii Prezesa Rady Ministrów, Szef Biura Bezpieczeństwa Narodowego oraz minister odpowiedzialny za koordynację działalności służb specjalnych. W posiedzeniach kolegium uczestniczą dodatkowo Dyrektor Rządowego Centrum Bezpieczeństwa; Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca; Szef Służby Kontrwywiadu Wojskowego albo jego zastępca oraz Dyrektor NASK PIB.

Podsumowanie

Wdrożenie ustawy o krajowym systemie cyberbezpieczeństwa to wyzwanie zarówno dla administracji, jak i sektora prywatnego.

Dużym wyzwaniem jest organizacja systemu w poszczególnych sektorach, związana z ustanowieniem sektorowych zespołów cyberbezpieczeństwa oraz zmianami w prawie sektorowym. Organy właściwe muszą także zbudować kompetencje nadzorcze w zakresie cyberbezpieczeństwa, co może być niełatwe w związku z niedoborem specjalistów w tej dziedzinie.

Obowiązek raportowania incydentów to duża zmiana dla sektora prywatnego i wyzwanie dla administracji w zakresie opracowania konkretnych narzędzi – systemu teleinformatycznego, który w założeniu ma wspierać krajowy system cyberbezpieczeństwa.

Rozporządzenia wykonawcze do Ustawy o krajowym systemie cyberbezpieczeństwa

Ustawę o krajowym systemie cyberbezpieczeństwa uzupełnia szereg rozporządzeń wykonawczych, które doprecyzowują zapisy ustawowe. Są to:

1. **Rozporządzenie w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo** z 10 września 2018 roku. Rozporządzenie określa wytyczne dla operatorów usług kluczowych. Według zapisów ustawy mogą oni sami realizować zadania związane z zapewnieniem bezpieczeństwa świadczonych usług lub powierzyć je podmiotowi zewnętrznemu, świadczącemu usługi z zakresu cyberbezpieczeństwa.
2. **Rozporządzenie w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu dla świadczenia usług** z 11 września 2018 roku. Jest to najistotniejsze rozporządzenie, które daje organom właściwym podstawy do wyznaczenia operatorów usług kluczowych w sektorach objętych zapisami ustawy.
3. **Rozporządzenie w sprawie zakresu działania oraz trybu pracy Kolegium do Spraw Cyberbezpieczeństwa** z 2 października 2018 roku. Kolegium ds. Cyberbezpieczeństwa to organ opiniodawczo-doradczy Rady Ministrów w zakresie cyberbezpieczeństwa. W rozporządzeniu określono tryb pracy kolegium oraz obowiązki sekretarza, a także sposób przyjmowania przez kolegium stanowiska.
4. **Rozporządzenie w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu** z 12 października 2018.Rozporządzenie określa wymagania do audytu, który operatorzy usług kluczowych mają obowiązek przeprowadzić raz na 2 lata. Audyt może być przeprowadzony przez jednostkę oceniającą zgodność[25], co najmniej dwóch audytorów z odpowiednim doświadczeniem[26] albo co najmniej dwóch audytorów posiadających certyfikaty wymienione w rozporządzeniu.

[25] Jednostka oceniająca zgodność musi być akredytowana zgodnie z przepisami ustawy z dnia 13 kwietnia 2016 r. o systemach oceny zgodności i nadzoru rynku (Dz. U. z 2017 r. poz. 1398 oraz z 2018 r. poz. 650), w zakresie właściwym do podejmowanych ocen bezpieczeństwa systemów informacyjnych. (art. 15 ust. 2 pkt. 1 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.)

[26] Audytor powinien posiadać co najmniej trzyletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych lub co najmniej dwuletnią praktykę w zakresie audytu bezpieczeństwa systemów informacyjnych i legitymować się dyplomem ukończenia studiów podyplomowych w zakresie audytu bezpieczeństwa systemów informacyjnych, wydanym przez jednostkę organizacyjną, która w dniu wydania dyplomu była uprawniona, zgodnie z odrębnymi przepisami, do nadawania stopnia naukowego doktora nauk ekonomicznych, technicznych lub prawnych (art. 15 ust. 2 pkt. 2 ustawy o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r.)

5. **Rozporządzenie w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej z dnia 16 października 2018 roku. Operatorzy usług kluczowych są zobowiązani do opracowania, stosowania i aktualizowania dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Składa się ona z dokumentacji normatywnej i operacyjnej.**
6. **Rozporządzenie w sprawie progów uznania incydentu za poważny** z 31 października 2018 roku. Rozporządzenie określa progi klasyfikacji incydentów poważnych dla poszczególnych sektorów i podsektorów gospodarki. Raportowanie tych incydentów jest obowiązkowe.

Implementacja GDPR – nowa Ustawa o ochronie danych osobowych

Rozporządzenie Ogólne o Ochronie Danych Osobowych – General Data Protection Regulation

RODO/GDPR zostało przyjęte 27 kwietnia 2016 r. i zastąpiło Dyrektywę 95/46/WE z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Rozporządzenie w znaczący sposób zwiększa kontrolę osób fizycznych nad dotyczącymi ich danymi poprzez:

- wprowadzenie nowych uprawnień dla osób, których dane dotyczą: prawo do przenoszenia danych i prawo do bycia zapomnianym.
- rozszerzenie obowiązku informacyjnego, który administrator danych musi zrealizować wobec osoby, której dane dotyczą.
- uregulowanie kwestii profilowania– osoba, której dane dotyczą, w określonych przypadkach będzie miała teraz m.in. uprawnienie do żądania ludzkiej interwencji, tak aby dotycząca jej decyzja nie była oparta wyłącznie na algorytmie.
- wprowadzenie nowego rozwiązania związanego z ochroną danych osobowych w fazie projektowania oraz jako ustawienie domyślne – tzw. zasady Privacy by Design i Privacy by Default
  - Privacy by Design oznacza, że administrator danych ma obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, które uwzględniają stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wynikające z przetwarzania.
  - Privacy by Default oznacza, że administrator ma obowiązek wdrażać odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania.
- wprowadzenie podejścia opartego na ryzyku (ang. *risk-based approach*), w którym obowiązki w zakresie ochrony danych są zróżnicowane w zależności od ryzyka, jakie wynika z konkretnych czynności przetwarzania danych. Administrator danych sam decyduje więc, jakie organizacyjne i techniczne środki powinien zastosować dla ochrony danych osobowych.
- wprowadzenie obowiązkowego zgłaszania przez administratorów danych do właściwego organu nadzoru, w ciągu 72 godzin, w przypadków naruszeń, które mogą skutkować zagrożeniem praw i swobód osób, których dane zostały naruszone. Dodatkowo może także pojawić się obowiązek zawiadomienia osoby, której prawa lub swobody mogły zostać naruszone.
- wprowadzenie administracyjnych kar finansowych za nieprzestrzeganie przepisów: karze do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa), podlegają następujące naruszenia przepisów:
  - Naruszenie obowiązków administratora i podmiotu przetwarzającego wymienionych w RODO, jak np.: brak weryfikacji wyrażenia zgody przez opiekuna dziecka, które nie ukończyło jeszcze 16 roku życia, na przetwarzanie jego danych osobowych; brak prowadzenia rejestru operacji przetwarzania; brak powołania Inspektora Ochrony Danych w przypadkach obligatoryjnych; brak informowania organu nadzorczego o naruszeniach w zakresie ochrony danych osobowych; nieprzestrzeganie obowiązków związanych z certyfikacją przedsiębiorcy przez stosowny podmiot;

– Naruszenie obowiązków podmiotu certyfikującego wymienionych w RODO;

– Naruszenie obowiązków podmiotu monitorującego związanych z podjęciem stosownych działań w przypadku stwierdzenia naruszenia przez danego przedsiębiorcę zatwierdzonego kodeksu postępowania;

Karze do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (przy czym zastosowanie ma kwota wyższa), podlegają następujące naruszenia przepisów:

– Naruszenie podstawowych zasad przetwarzania, w tym warunków zgód na przetwarzanie określonych w RODO;

– Naruszenie praw osób, których dane są przetwarzane;

– Naruszenie przepisów dotyczących przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej;

– Nieprzestrzeganie nakazu tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy lub niezapewnienie dostępu organowi nadzorczemu;

– Naruszenie obowiązków wynikających z przepisów krajowych danego państwa członkowskiego, uchwalonych na podstawie RODO;

– Nieprzestrzeganie środków naprawczych nałożonych przez organ nadzorczy.

Wejście w życie RODO/GDPR i konieczność zapewnienia skutecznego stosowania jego przepisów było dużym wyzwaniem legislacyjnym. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2018 r. poz. 1000) nie powiela ani nie implementuje rozwiązań RODO, lecz uzupełnia nowe regulacje w zakresie ochrony danych osobowych, aby odpowiadały przepisom i standardom przyjętym na poziomie UE. Najważniejsze z nich dotyczą:

- Utworzenia urzędu Prezesa Urzędu Ochrony Danych Osobowych (PUODO), który zastąpił Generalnego Inspektora Ochrony Danych Osobowych (GIODO). Prezesa powołuje i odwołuje Sejm, za zgodą Senatu, na czteroletnią kadencję. Funkcję można pełnić maksymalnie dwie kadencje;
- Wprowadzenia jednoinstancyjnego postępowania administracyjnego przed PUODO;
- Ustanowienia Rady do Spraw Ochrony Danych Osobowych. Jest to ośmioosobowy organ doradczy PUODO, powoływany przez prezesa na dwuletnią kadencję;
- Nałożenia na administratorów danych osobowych i podmioty przetwarzające (procesorów), będące podmiotami publicznymi, obowiązku powołania do 31 lipca 2018[1] inspektora danych osobowych;
- Określenia warunków i trybu udzielania akredytacji podmiotowi certyfikującemu;
- Określenia sposobu zatwierdzania kodeksu postępowania;.
- Określenia trybu postępowania w sprawach o naruszenie zasad ochrony danych osobowych oraz trybu kontroli przestrzegania przepisów i zasady odpowiedzialności cywilnej i karnej;
- Ograniczenia, w stosunku do zapisów RODO/GDPR, wysokości administracyjnych kar pieniężnych nakładanych na niektóre jednostki budżetowe (jednostki sektora finansów publicznych, instytuty badawcze i NBP — do 100 tys. złotych, zaś instytucje kultury — do 10 tys.).

GDPR/RODO a zespoły CERT/CSIRT

Nowe prawo w zakresie danych osobowych jest także pewnego rodzaju wyzwaniem dla zespołów CSIRT. Zgodnie z treścią rozporządzenia, **mianem administratora określa się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.** Natomiast podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę organizacyjną lub inny podmiot, który **przetwarza dane osobowe w imieniu administratora.**

[1] Wyjątkiem są przypadki, gdzie powołano wcześniej ABI, czyli Administratorów Bezpieczeństwa Informacji, którzy z dniem wejścia w życie ustawy staną się inspektorami ochrony danych.

Zespół CSIRT jest więc administratorem w każdym momencie, gdy przetwarza dane osobowe. Jeśli zespół działa w imieniu organów ścigania lub innych zespół CSIRT (np. zapewnia pomoc techniczną), pełni rolę podmiotu przetwarzającego, ponieważ nie decyduje samodzielnie o celach i sposobach przetwarzania danych osobowych. Także udostępnianie i wymianę informacji pomiędzy zespołami CSIRT można uznać za przetwarzanie danych osobowych.

Oznacza to, że w zakresie zgłaszania incydentów zespoły typu CSIRT podlegają dwóm reżimom: temu wprowadzonemu przez Dyrektywę NIS i temu właściwemu RODO/GDPR. Poniższe tabele prezentują wymagania notyfikacji incydentów dla obu aktów prawnych RODO/GDPR.

RODO/GDPR

Rodzaj incydentu	Podmiot notyfikujący	Odbiorca zgłoszenia	Termin
Naruszenie danych osobowych	Podmiot przetwarzający	Administrator	Bez zbędnej zwłoki
Naruszenie danych osobowych	Administrator	Właściwy organ ochrony danych osobowych	Bez zbędnej zwłoki, w miarę możliwości do 72 godzin od momentu otrzymania zgłoszenia
Naruszenie danych osobowych z dużym ryzykiem zagrożenia dla praw i wolności osób fizycznych	Administrator	Właściwy organ ochrony danych osobowych oraz osoby, których dane dotyczą	Bez zbędnej zwłoki

Tabela 3. Notyfikacje naruszeń wg. RODO/GDPR

NIS

Rodzaj incydentu	Podmiot notyfikujący	Odbiorca zgłoszenia	Termin
Incydent mający znaczny wpływ na ciągłość usług kluczowych	Operatorzy usług kluczowych	Właściwy organ ochrony danych lub zespół CSIRT	Bez zbędnej zwłoki
Incydent mający znaczny wpływ na świadczenie usługi	Dostawcy usług cyfrowych	Właściwy organ ochrony danych lub zespół CSIRT	Bez zbędnej zwłoki

Tabela 3. Raportowanie incydentów wg. Dyrektywy NIS

W związku z tym, zespół CSIRT powinien przeprowadzić analizę, w jakim zakresie może przetwarzać dane osobowe w obrębie własnego *constituency*, a także czy jest procesorem (przetwarza dane osobowe) czy administratorem. Konieczne jest także dokumentowanie sposobu przetwarzania danych osobowych, dokładna analiza okresu i zasad przetwarzania danych roboczych czy anonimizacja danych osobowych. Natomiast w czasie procesu przekazywania danych osobowych konieczna będzie ocena nie tylko *constituency* swojego zespołu CSIRT, ale także CSIRT, któremu dane te mają być przekazywane.

Kompetencje CSIRT poziomu krajowego w tym zakresie reguluje Ustawa o krajowym systemie cyberbezpieczeństwa.

W poszukiwaniu „polskiej" sztucznej inteligencji (AI)

W 2018 roku polski rząd po raz pierwszy podjął prace nad tematem sztucznej inteligencji (AI). Jeszcze przed publikacją Komunikatu Komisji Europejskiej Sztuczna Inteligencja dla Europy[27], z inicjatywy Polski, Grupa Wyszehradzka (V4) przyjęła wspólne stanowisko w sprawie sztucznej inteligencji. Państwa V4 wezwały KE do dalszego zaangażowania w rozwój AI, podkreślając potencjał tej technologii dla europejskich przedsiębiorców. Jednocześnie wskazały konieczność pogłębionych analiz prawnych i ekonomiczno-społecznych aspektów ważnych dla rozwoju AI. Na poziomie UE zdefiniowanych zostało 9 priorytetów:

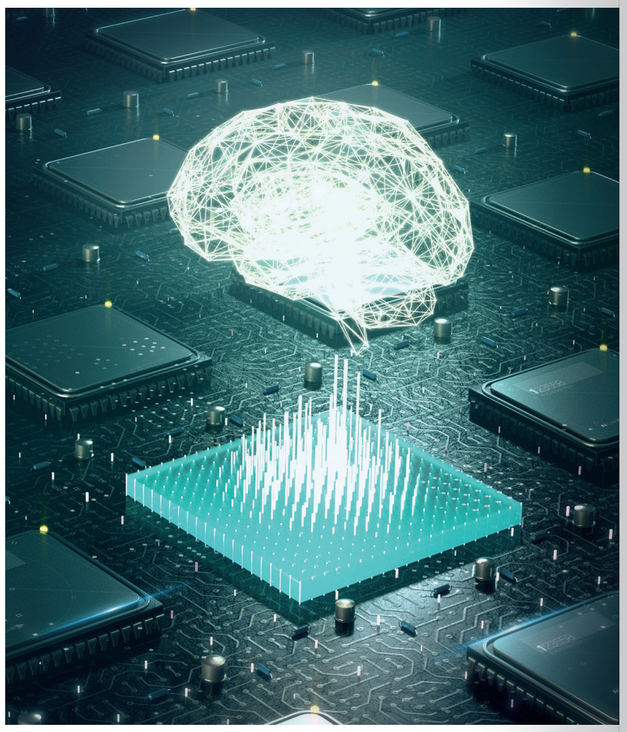
1. Włączenie sztucznej inteligencji do dyskusji na temat transformacji cyfrowej i uczynienie AI jednym z priorytetów UE do roku 2020 i na kolejne lata.
2. Uruchomienie ogólnoeuropejskiej inicjatywy w postaci wirtualnych magazynów danych (ma to umożliwić otwarcie danych przemysłowych i pozwolić przyspieszyć badania, rozwój oraz implementację sztucznej inteligencji).
3. Konieczność rozpoczęcia debaty na temat prawidłowego mechanizmu finansowania technologii cyfrowych.
4. Stworzenie tzw. „piaskownic regulacyjnych" na poziomie UE, które będą wspierać badania i rozwój w kluczowych sektorach, takich jak medycyna, prawo, rynki finansowe, usługi, rynek motoryzacyjny, rolnictwo, ochrona środowiska, gospodarka wodna czy przemysł żywnościowy.
5. Analiza wykorzystania technologii AI w reformie procesu podejmowania decyzji przez administrację państwową.
6. Konieczność wspierania edukacji i badań oraz tworzenie środowisk akademickich wspierających rozwój AI.
7. Utworzenie Europejskiego Obserwatorium Sztucznej Inteligencji.
8. Zapewnienie cyberbezpieczeństwa i zaufania.
9. Zbadanie wpływu sztucznej inteligencji na rynek pracy w Europie[28].

Kolejnym krokiem było utworzenie przy Ministerstwie Cyfryzacji czterech grup roboczych w zakresie sztucznej inteligencji: gospodarka oparta na danych, finansowanie badań i rozwoju, edukacja, etyka i prawo. Przez kilka miesięcy eksperci pracowali nad rekomendacjami, które przedstawiono ostatecznie na początku listopada 2018 jako **Założenia do strategii AI w Polsce.**

Dokument podsumowuje prace grup roboczych i przedstawia plan działań na lata 2018-2019, definiujący następujące priorytety:

- Opracowanie nowego programu kooperacyjnego dedykowanego AI w gospodarce.
- Utworzenie DIH (HUB cyfrowej innowacji)[29] w zakresie sztucznej inteligencji.
- Wspieranie organizacji pozarządowych w upowszechnianiu wiedzy o AI.
- Stworzenie ogólnodostępnego portalu edukującego na temat AI.
- Uruchomienie wirtualnego instytutu AI.
- Powołanie wirtualnej katedry prawa i etyki AI (przy Ministerstwie Cyfryzacji).
- Opracowanie katalogu kryteriów dla etyki w AI[30].

Na rok 2019 zapowiedziano prace nad krajową strategią w zakresie sztucznej inteligencji.



[27] Więcej na temat Komunikatu KE Sztuczna Inteligencja dla Europy na stronie 39.
[28] https://www.gov.pl/web/cyfryzacja/stanowisko-grupy-wyszehradzkiej-dotyczace-sztucznej-inteligencji
[29] Więcej informacji na temat DIH na stronie 43,
[30] https://www.gov.pl/web/cyfryzacja/sztuczna-inteligencja-polska-2118

Zmiany w Ustawie o usługach płatniczych

10 maja 2018 roku została przyjęta Ustawa o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw[31]. Jest to implementacja do porządku prawnego dyrektywy PSD2[32].

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE – Dyrektywa PSD2 została przyjęta w listopadzie 2015 roku. Zwiększa ochronę klientów oraz współpracę na europejskim rynku płatności poprzez:

- włączenie w zakres dyrektywy nieregulowanych wcześniej usług płatniczych,
- wyrównanie szans dla nowego rodzaju usług płatniczych,
- zwiększenie ochrony i bezpieczeństwa płatności poprzez m.in. silniejsze mechanizmy uwierzytelniania,
- zwiększenie konkurencyjności, a co za tym idzie zachętę do obniżenia cen dla klientów.

Dyrektywa PSD2 reguluje nowy rodzaj usług płatniczych, opartych o dostęp do „stron trzecich". Jest pewnego rodzaju rewolucją na rynku finansowym, ponieważ wprowadza obowiązek umożliwienia „stronom trzecim" świadczenia usług pośredniczących bez konieczności zawierania umowy pomiędzy instytucją prowadzącą rachunek (np. bankiem), a „stroną trzecią" (dostawcą usługi płatniczej).

Działanie stron trzecich

Klient zamiast logować się bezpośrednio do usług bankowości elektronicznej, loguje się do zewnętrznego dostawcy usług płatniczych („strona trzecia"). Następnie dostawca usług płatniczych loguje się w imieniu klienta, do instytucji prowadzącej jego rachunek (np. banku) i wykonuje operacje (np. inicjowanie płatności).

Najważniejszą kwestią uregulowaną w ustawie jest bezpieczeństwo dostawców usług płatniczych, którzy zostali zobowiązani do podjęcia środków ograniczających ryzyko oraz wprowadzenia mechanizmów kontroli, służących zarządzaniu ryzykiem naruszenia zasad bezpieczeństwa i ryzykiem operacyjnym.

Ustawa definiuje incydent jako „niespodziewane zdarzenie, które ma niekorzystny wpływ na integralność, dostępność, poufność, autentyczność lub ciągłość świadczenia usług płatniczych albo stwarza znaczne prawdopodobieństwo, że taki wpływ będzie mieć, lub serię takich zdarzeń"[33]. Dostawcy usług płatniczych zostali zobowiązani do niezwłocznego raportowania Komisji Nadzoru Finansowego (KNF) poważnych incydentów operacyjnych oraz incydentów związanych z bezpieczeństwem, w tym teleinformatycznych. Dodatkowo, jeśli taki incydent może mieć wpływ na interesy finansowe użytkowników, dostawca ma obowiązek ich o tym poinformować.

Dostawcy są także zobowiązani do przekazywania KNF rocznych danych na temat oszustw związanych z usługami płatniczymi.

Ponadto, ustawa wprowadza obowiązek silnego, zapewniającego ochronę poufności uwierzytelniania użytkownika w trzech przypadkach: kiedy uzyskuje on dostęp do swojego rachunku w trybie online, inicjuje elektroniczną transakcję płatniczą oraz, za pomocą zdalnego kanału, przeprowadza czynność, która może się wiązać z ryzykiem oszustwa, związanego z wykonywanymi usługami płatniczymi albo z innymi nadużyciami[34]. Przepisy te wejdą w życie 14 września 2019 roku.

[31] Ustawa ta zmienia także: ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, ustawę z dnia 29 sierpnia 1997 r. – Prawo bankowe, ustawę z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, ustawę z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami, ustawę z dnia 21 lipca 2006 r. o nadzorze nad rynkiem finansowym, ustawę z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych, ustawę z dnia 12 maja 2011 r. o kredycie konsumenckim, ustawę z dnia 5 sierpnia 2015 r. o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym, ustawę z dnia 15 grudnia 2017 r. o zmianie ustawy o podatku od towarów i usług oraz niektórych innych ustaw oraz ustawę z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.
[32] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającą dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającą dyrektywę 2007/64/WE (Dz. Urz. UE L 337 z 23.12.2015, str. 35).
[33] Art. 9 c Ustawy o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw.
[34] Art. 32 i Ustawy o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw.

Unia Europejska – Cyberbezpieczeństwo i rozwój nowoczesnych technologii w kontekście budowy Jednolitego Rynku Cyfrowego

Unia Europejska (UE) powstała w 1993 roku jako związek gospodarczo-polityczny. Od 2009 roku funkcjonuje jako organizacja międzynarodowa. W jej skład wchodzi 28 państw członkowskich. Najważniejsze organy to Komisja Europejska (KE) – władza wykonawcza, posiadająca inicjatywę ustawodawczą; Rada Unii Europejskiej – główny organ decyzyjny; oraz Parlament Europejski – wybierany w wyborach powszechnych organ władzy legislacyjnej.

Od 2015 roku UE wdraża Strategię Jednolitego Rynku Cyfrowego (*Digital Single Market* – DSM)[35]. Założeniem DSM jest usuwanie barier pomiędzy państwami członkowskimi, co według szacunków KE mogłoby przynieść unijnej gospodarce 415 mld euro rocznie[36]. Komisja szacuje, że zrealizowanie działań przedstawionych w Strategii DSM przyczyni się do wzrostu gospodarczego wewnątrz całej UE, ułatwiając jednocześnie codzienne funkcjonowanie pojedynczym obywatelom. Samo funkcjonowanie Jednolitego Rynku Cyfrowego przyczyni się natomiast do utworzenia wielu nowych miejsc pracy. Strategia DSM ma umożliwić państwom członkowskim jak najpełniejsze wykorzystanie rewolucji cyfrowej i szybki wzrost gospodarczy.

Strategia Jednolitego Rynku Cyfrowego dla Europy (A Digital Single Market Strategy for Europe) – Strategia DSM

6 maja 2015 roku Komisja Europejska opublikowała Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Strategia Jednolitego Rynku Cyfrowego dla Europy.

Dokument zakłada zniesienie ograniczeń regulacyjnych w kwestiach cyfrowych w taki sposób, aby możliwe było zbudowanie Wspólnego Europejskiego Rynku Cyfrowego. Ma to pomóc w szybszym rozwoju usług cyfrowych, a tym samym budować konkurencyjność europejskich firm. Jednym z działań związanych z DSM jest cyberbezpieczeństwo. Komisja podkreśla, że tylko bezpieczne usługi cyfrowe będą wykorzystywane przez obywateli.

Założenia strategii są oparte na trzech podstawowych filarach, do których została przydzielona lista konkretnych działań. Ich realizacja ma zapewnić wypracowanie jednolitych ram prawnych dla wspólnego rynku cyfrowego UE:

1. **Lepszy dostęp konsumentów i przedsiębiorców do towarów sprzedawanych przez Internet**
   - Wprowadzenie regulacji, mających ułatwić prowadzenie transgranicznego handlu elektronicznego;
   - Wprowadzenie transgranicznego doręczania paczek, którego jakość będzie wysoka, a koszty przystępne;
   - Zapobieganie nieuzasadnionemu blokowaniu geograficznemu, które ograniczało dostępność niektórych usług;
   - Lepszy dostęp do treści cyfrowych polegający na unowocześnieniu ram praw autorskich;
   - Zmniejszenie obciążeń i przeszkód związanych z podatkiem VAT przy sprzedaży ponad granicami;
2. **Środowisko, w którym sieci i usługi cyfrowe mogą się rozwijać**
   - Dostosowanie przepisów telekomunikacyjnych do odpowiednich potrzeb;
   - Przegląd ram prawnych dla usług medialnych (w tym platform internetowych i pośredników), tak aby były one odpowiednio przystosowane do realiów XXI w.;
   - Wzmocnienie zaufania do usług cyfrowych i przetwarzania danych osobowych oraz zwiększenie ich bezpieczeństwa;
3. **Cyfrowość jako siła napędowa wzrostu**
   - Budowanie gospodarki opartej na danych;
   - Zwiększenie konkurencyjności dzięki interoperacyjności i normalizacji w sektorach istotnych dla funkcjonowania jednolitego rynku europejskiego;
   - Kreowanie cyfrowego społeczeństwa sprzyjające włączeniu społecznemu.

Działania związane z cyberbezpieczeństwem są prowadzone w ramach drugiego filaru.

[35] https://ec.europa.eu/digital-single-market/en
[36] http://europa.eu/rapid/press-release_IP-15-4919_en.htm

Implementacja Dyrektywy NIS

Rok 2018 upłynął, przede wszystkim, na pracach związanych z wdrożeniem Dyrektywy NIS[37]. Powołana w 2016 roku Grupa Współpracy[38] prowadziła prace zmierzające do koordynacji implementacji dyrektywy (państwa członkowskie miały na to czas do 9 maja 2018 roku). W ramach prac grupy przygotowano i opublikowano szereg dokumentów, które miały wesprzeć państwa członkowskie w tym procesie:

- Dokument na temat środków bezpieczeństwa dla operatorów usług kluczowych (*Reference document on security measures for Operators of Essential Services*)
- Dokument na temat notyfikacji incydentów dla operatorów usług kluczowych (*Reference document on incident notification for Operators of Essential Services (circumstances of notification)*)
- Kompendium wiedzy na temat cyberbezpieczeństwa wyborów (*Compendium on cyber security of election technology*)
- Taksonomia incydentów cyberbezpieczeństwa (*Cybersecurity incident taxonomy*)
- Wytyczne w zakresie notyfikacji incydentów dla operatorów usług kluczowych – formaty i procedury (*Guidelines on notification of Operators of Essential Services incidents (formats and procedures)*)
- Wytyczne w zakresie notyfikacji incydentów dla dostawców usług cyfrowych – formaty i procedury (*Guidelines on notification of Digital Service Providers incidents (formats and procedures)*)
- Wytyczne w zakresie identyfikacji operatorów usług kluczowych (współzależności międzypaństwowe) (*Reference document on the identification of Operators of Essential Services (modalities of the consultation process in cases with cross-border impact)*).[39]

Państwa członkowskie systematycznie rozwijają też współpracę w ramach sieci CSIRT[40].

Dyrektywa NIS – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii jest pierwszym ogólnoeuropejskim aktem prawnym w zakresie cyberbezpieczeństwa. Regulacja obejmuje dwa typy podmiotów: operatorów usług kluczowych – OUK (podmioty z sektorów energetyki, transportu, bankowości, finansów, zdrowia, zaopatrzenia w wodę pitną oraz infrastruktury cyfrowej) i dostawców usług cyfrowych – DUC (serwisy zakupowe, wyszukiwarki internetowe oraz usługi chmury obliczeniowej). Celem Dyrektywy NIS jest wzrost bezpieczeństwa teleinformatycznego zarówno w krajach członkowskich, jak i całej UE, poprzez:

- wprowadzenie obowiązkowego raportowania incydentów dla operatorów usług kluczowych oraz kontroli ex post dla dostawców usług cyfrowych
- obowiązek szacowania ryzyka w zakresie cyberbezpieczeństwa
- obowiązek desygnowania przez kraje członkowskie CSIRT (Computer Security Incident Response Team) przyjmującego zgłoszenia incydentów od OUK i DUC
- obowiązek ustanowienia w krajach członkowskich organów właściwych ds. cyberbezpieczeństwa, sprawujących nadzór nad OUK i DUC
- ustanowienie współpracy pomiędzy państwami członkowskimi poprzez powołanie Grupy Współpracy (mechanizm współpracy na poziomie politycznym) oraz sieci CSIRT (mechanizm współpracy na poziomie operacyjnym)

[37] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

[38] Grupa Współpracy (Cooperation Group) to mechanizm współpracy polityczno-strategicznej, powołany na mocy art. 11 Dyrektywy NIS. Celem jest wzmacnianie i budowanie współpracy pomiędzy państwami członkowskimi na poziomie strategicznym. W jej skład wchodzą przedstawiciele państw członkowskich, Komisji i ENISA. Sekretariat zapewnia Komisja.

[39] https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[40] Jest to mechanizm stworzony na podstawie art. 12 Dyrektywy NIS. W skład sieci CSIRT wchodzą przedstawiciele CSIRT państw członkowskich, CERT-EU i Komisja jako obserwator. Sekretariat prowadzi ENISA. Zadaniem sieci jest wzmacnianie współpracy operacyjnej pomiędzy państwami członkowskimi. Decyzją ministra właściwego ds. informatyzacji, Polskę w sieci CSIRT reprezentuje CERT Polska, znajdujący się w strukturze Państwowego Instytutu Badawczego NASK.

Negocjacje Cybersecurity Act

Jednym z najważniejszych wydarzeń 2018 roku były negocjacje ***Cybersecurity Act.*** Propozycja aktu została przedstawiona we wrześniu 2017, jako część tzw. pakietu cyberbezpieczeństwa. Częścią pakietu był także Komunikat KE *Odporność, prewencja i obrona: Budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej*. Dokument jest aktualizacją *Strategii bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń* z 7 lutego 2013.

Komunikat KE *Odporność, prewencja i obrona: Budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej* opiera się na trzech filarach, do których wyznaczono listę konkretnych działań:

Budowanie odporności UE na ataki cybernetyczne

- Wzmocnienie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA);
- Rozwój w kierunku jednolitego rynku bezpieczeństwa cybernetycznego;
- Pełne wdrożenie dyrektywy w sprawie bezpieczeństwa sieci i informacji (Dyrektywa NIS);
- Odporność dzięki szybkiemu reagowaniu w sytuacji kryzysowej;
- Tworzenie sieci ośrodków kompetencji w dziedzinie bezpieczeństwa cybernetycznego oraz Europejskiego Centrum Badań Naukowych i Kompetencji w dziedzinie Bezpieczeństwa Cybernetycznego;
- Budowanie silnej unijnej bazy umiejętności w zakresie cyberbezpieczeństwa;
- Propagowanie higieny cybernetycznej i świadomości zagrożeń;

Kształtowanie skutecznej unijnej prewencji cybernetycznej

- Identyfikacja podmiotów działających w złych intencjach;
- Doskonalenie reagowania przez organy ścigania;
- Publiczno-prywatna współpraca w zwalczaniu cyberprzestępczości;
- Doskonalenie reagowania politycznego;
- Kształtowanie prewencji w zakresie bezpieczeństwa cybernetycznego za pomocą potencjału obronnego państw członkowskich;

Wzmocnienie współpracy międzynarodowej w dziedzinie bezpieczeństwa cybernetycznego

- Cyberbezpieczeństwo w stosunkach zewnętrznych;
- Budowanie zdolności w obszarze bezpieczeństwa cybernetycznego
- Współpraca UE-NATO.

W komunikacie KE zapowiedziała także silne zbliżenie wojskowych i cywilnych kwestii związanych z cyberbezpieczeństwem.

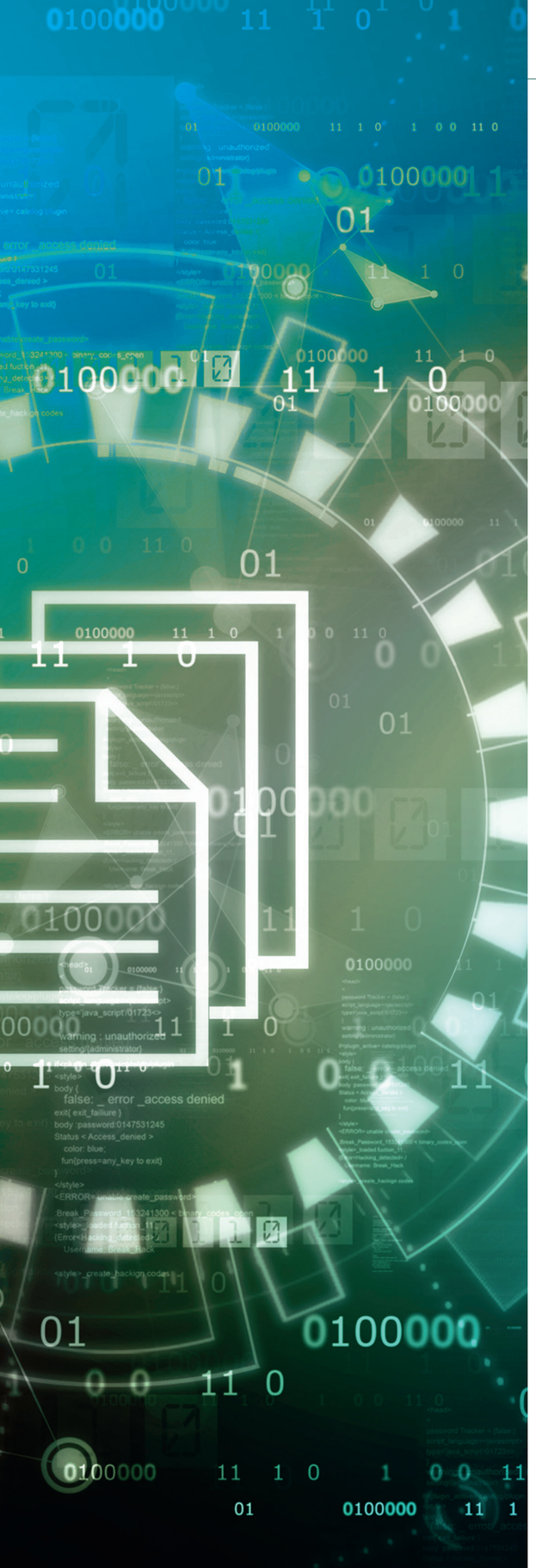
Porozumienie w sprawie pakietu Parlament Europejski i Komisja osiągnęły 10 grudnia 2018, natomiast oficjalna publikacja dokumentu przewidziana jest na marzec/kwiecień 2019. ***Cybersecurity Act*** (CA) to druga, po Dyrektywie NIS, regulacja prawna w zakresie cyberbezpieczeństwa na poziomie europejskim. Jej celem jest wzmacnianie odporności UE i krajów członkowskich na zagrożenia teleinformatyczne oraz budowa silnego systemu cyberbezpieczeństwa, tak aby wzmacniać Jednolity Rynek Cyfrowy.

CA składa się z dwóch części: nowego, permanentnego mandatu dla Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), której rola została znacznie wzmocniona, a także rozporządzenia tworzącego europejskie ramy certyfikacji cyberbezpieczeństwa dla produktów i usług ICT. Jest to bardzo istotna regulacja, która znacznie zmieni funkcjonujący obecnie model certyfikacji, zdominowany przez SOG-IS (Senior Official Group Information Security Systems)[41].

Rozporządzenie w sprawie certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjnych i komunikacyjnych

Rozporządzenie wprowadza **europejskie ramy certyfikacji w dziedzinie cyberbezpieczeństwa.** Regulacja określa mechanizm ustanawiania europejskich programów certyfikacji cyberbezpieczeństwa oraz potwierdzania, że dane produkty bądź usługi spełniają określone wymogi bezpieczeństwa. Efektem będzie **wzajemna uznawalność certyfikatów** na obszarze całej UE. KE zakłada również, że **certyfikacja spowoduje**

[41] Porozumienie SOG-IS zostało zawarte w 1997 roku, w odpowiedzi na decyzję Rady UE z marca 1992. Sygnatariusze porozumienia mogą samodzielnie oceniać i certyfikować produkty i usługi sektora IT, zgodnie z międzynarodową normą OSO/IEC 15408, która pozwala zweryfikować bezpieczeństwo systemów teleinformatycznych pod względem formalnym. Polska dołączyła do grupy państw sygnatariuszy porozumienia SOG-IS w 2017 roku.



wzrost zaufania konsumentów, bo będą oni mogli wybierać przetestowane i spełniające normy bezpieczeństwa urządzenia i rozwiązania. Przedsiębiorcy natomiast zaoszczędzą czas i pieniądze, ponieważ **nie będzie już konieczności ubiegania się o certyfikat w każdym kraju członkowskim**, w którym chcieliby oferować swoje usługi bądź produkty. Dodatkowo, te firmy które zainwestują w cyberbezpieczeństwo, uzyskają znaczną przewagę konkurencyjną.

Przyjęcie *Cybersecurity Act* oznacza także wyzwania dla tych państw członkowskich, które nie podejmowały dotąd żadnych kroków w kierunku stworzenia krajowego programu certyfikacji cyberbezpieczeństwa. W lepszej sytuacji znajdą się te państwa, które nie będą musiały budować odpowiednich kompetencji oraz infrastruktury potrzebnych np. do testowania certyfikowanego sprzętu od podstaw.

W proces certyfikacji na poziomie europejskim zaangażowane są Komisja Europejska, ENISA oraz Europejska Grupa Certyfikacji Cyberbezpieczeństwa.

Europejska Grupa Certyfikacji Cyberbezpieczeństwa (ECCG, *European Cybersecurity Certification Group*) to jeden z najważniejszych organów, który powołuje do życia CA. Grupa składa się z przedstawicieli krajowych organów certyfikacji cyberbezpieczeństwa lub innych właściwych organów krajowych. ECCG przewodniczy Komisja Europejska, która z pomocą ENISA zapewnia jej sekretariat. Głównym zadaniem ECCG jest współpraca z KE i ENISA poprzez doradztwo przy opracowywaniu programów certyfikacji. Poza tym grupa ma usprawniać współpracę między krajowymi organami certyfikacji.

Proces certyfikacji krok po kroku

Proces certyfikacji mogą zainicjować zarówno Komisja Europejska, jak i Europejska Grupa Certyfikacji Cyberbezpieczeństwa. Różnica polega na tym, że **ENISA musi przygotować propozycję europejskiego programu certyfikacji tylko na wniosek KE.** Jeśli o przygotowanie propozycji programu zawnioskuje ECCG, ENISA może taki wniosek odrzucić, podając uzasadnienie.

Krok 1: Przygotowanie propozycji programu

Za przygotowanie propozycji programu certyfikacji (tzw. program kandydat) odpowiada ENISA. Podczas prac Agencja ma obowiązek konsultacji „propozycji programu" ze wszystkimi interesariuszami oraz ustanowienia grupy roboczej, składającej się z ekspertów z państw członkowskich, która opracuje program. Wypracowana propozycja przekazywana jest do KE.

Dodatkowo pomoc i porady ekspertów zapewnia ECCG. Grupa wydaje również opinię na temat przygotowanej propozycji programu. Opinia ta nie jest wiążąca, a jej brak nie blokuje możliwości przekazania propozycji do Komisji Europejskiej. ENISA powinna jednak w jak największym stopniu uwzględnić opinię ECCG. Daje to sektorowi publicznemu wpływ na przygotowywanie europejskich programów certyfikacji.

Krok 2: Przyjęcie propozycji programu

Komisja, w oparciu o otrzymaną propozycję, **może przyjąć akty wykonawcze,** które ustanowią europejskie programy certyfikacji cyberbezpieczeństwa dla procesów, produktów i usług ICT.

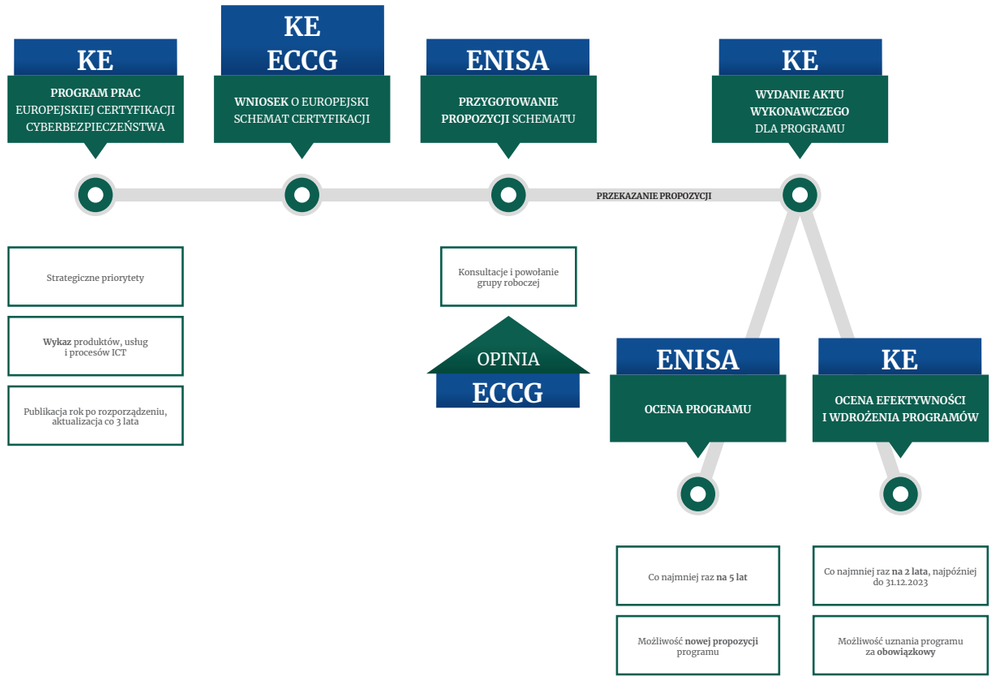
Krok 3: Przegląd programów certyfikacji

Co najmniej raz na 5 lat ENISA **ocenia przyjęte europejskie programy certyfikacji cyberbezpieczeństwa** pod względem ich użyteczności i aktualności. Komisja Europejska lub ECCG może zwrócić się do Agencji o opracowanie zmienionej propozycji programu.

Krok 4: Informacje o europejskich programach certyfikacji cyberbezpieczeństwa

Zadaniem ENISA jest utworzenie **specjalnej strony internetowej na temat certyfikacji cyberbezpieczeństwa.** Znajdą się tam m.in. informacje o aktualnych, wygasłych lub wycofanych programach, certyfikatach czy unijnych deklaracjach zgodności. Powinno się tam znaleźć również repozytorium linków do informacji dostarczanych przez producentów i dostawców z branży ICT.

Poniższy schemat przedstawia proces przygotowywania certyfikatu:



Rys. 2. Przygotowanie Europejskiego programu certyfikacji cyberbezpieczeństwa

Europejski program certyfikacji cyberbezpieczeństwa może określać **trzy poziomy bezpieczeństwa: podstawowy, istotny i wysoki.** Poziom uzasadnienia zaufania dla danego urządzenia czy usługi ICT, powinien być **proporcjonalny do poziomu ryzyka,** na który składa się m.in. prawdopodobieństwo wystąpienia incydentu oraz jego potencjalny wpływ.

Wydany na określonym poziomie certyfikat zapewnia, że produkty, usługi i procesy ICT spełniają odpowiednie wymogi bezpieczeństwa i zostały ocenione zgodnie z obowiązującymi na danym poziomie wytycznymi.

Poziom uzasadnienia zaufania	Ryzyko	Wymagana ocena
Podstawowy	znane podstawowe cyberzagrożenia	dokumentacja techniczna
Istotny	znane cyberzagrożenia, cyberatak prowadzony przez podmioty **o ograniczonych umiejętnościach i zasobach**	czy nie występują powszechnie znane podatności czy w produktach bądź usługach prawidłowo wdrożono niezbędne funkcjonalności bezpieczeństwa
Wysoki	cyberatak prowadzany przez osoby **o znaczących umiejętnościach i zasobach**	czy nie występują powszechnie znane podatności czy w produktach bądź usługach prawidłowo wdrożono niezbędne nowoczesne funkcjonalności bezpieczeństwa **odporność na zaawansowane ataki za pomocą testów penetracyjnych**

Tabela 5. Poziomy bezpieczeństwa i wymagana ocena wg. Cybersecurity Act

Europejski program certyfikacji cyberbezpieczeństwa zezwala także na przeprowadzenie **samooceny zgodności** (tzw. ocenę zgodności przez stronę pierwszą). Przeprowadza ją producent lub dostawca produktów i usług ICT na swoją **wyłączną odpowiedzialność**. Taka ocena może dotyczyć tylko produktów i usług na **podstawowym poziomie bezpieczeństwa**[42].

Obowiązkowa certyfikacja

CA wprowadza możliwość obowiązkowej certyfikacji dla tych produktów, procesów i usług ICT, które podczas przeglądu KE zidentyfikuje jako wymagające takiej certyfikacji. KE ma rozpocząć ocenę od sektorów szczególnie wrażliwych, wymienionych w załączniku II do Dyrektywy NIS: energetyka, transport, bankowość, infrastruktura rynków finansowych, służba zdrowia, zaopatrzenie w wodę pitną oraz infrastruktura cyfrowa. Ocenia się je najpóźniej dwa lata po przyjęciu pierwszego schematu.

Certyfikacja na poziomie krajowym – obowiązki państw członkowskich

O ile przygotowanie programów certyfikacji cyberbezpieczeństwa odbywa się na poziomie europejskim, o tyle sam **proces certyfikacji przebiega na poziomie krajowym**. CA nakłada na państwa członkowskie konkretne obowiązki, które mają pomóc w budowie sprawnego krajowego systemu certyfikacji cyberbezpieczeństwa. Aby móc przeprowadzić proces certyfikacji, konieczne jest powołanie:

1. Krajowego organu ds. certyfikacji cyberbezpieczeństwa (KOCC)

KOCC należy wyznaczyć **w ciągu 24 miesięcy od opublikowania rozporządzenia.** Można też porozumieć się z innym państwem i wyznaczyć organ, znajdujący się na jego terenie.

Krajowy organ certyfikacji pełni dwoistą rolę: **wydaje certyfikaty** (jednostka certyfikująca), oraz prowadzi **działania nadzorcze**. Obie te funkcje muszą być rozdzielone i **niezależne od siebie**. Krajowe organy muszą być również n**iezależne od podmiotów, które nadzorują**.

Do ich głównych zadań należy **monitorowanie zgodności** produktów, procesów i usług ICT z wymogami certyfikatów wydanych na ich terytoriach. Wspierają też krajowe jednostki akredytujące w **nadzorowaniu jednostek oceniających zgodność**. Aby realizować swoje zadania, mogą m.in. prowadzić audyty, nakładać sankcje, a nawet wycofać certyfikat, który jest niezgodny z europejskim programem certyfikacji.

Krajowe organy certyfikacji współpracują ze sobą oraz z KE, **uczestniczą również w pracach Europejskiej Grupy Certyfikacji Cyberbezpieczeństwa.** Podlegają też wzajemnej ocenie, czyli tzw. **przeglądowi partnerskiemu**.

[42] Wydawanie oświadczenia zgodności jest dobrowolne, chyba że inaczej stanowi unijne bądź krajowe prawo. Oświadczenie uznawane jest we wszystkich państwach członkowskich.

Odbywać się on będzie **co najmniej raz na pięć lat.** Prowadzą go przynajmniej dwa krajowe organy ds. certyfikacji cyberbezpieczeństwa z innych państw członkowskich oraz Komisja Europejska. W ocenie uczestniczyć może również ENISA.

2. Krajowej jednostki akredytującej

Na podstawie wcześniejszego rozporządzenia[43] każde państwo członkowskie wyznacza jedną krajową jednostkę akredytującą. W Polsce jest to Polskie Centrum Akredytacji, które **akredytuje jednostki oceniające zgodność,** gdy spełniają określone wymogi[44]. Akredytacja jest wydawana **maksymalnie na pięć lat** i może być przedłużana na tych samych warunkach, o ile organ oceny zgodności dalej spełnia wymogi.

3. Jednostek oceniających zgodność

Jednostki oceniające zgodność **mogą wystawiać certyfikaty dla podstawowego i istotnego poziomu bezpieczeństwa**, a po przekazaniu takiego zadania przez KOCC – nawet dla poziomu wysokiego.

Jeśli europejski certyfikat cyberbezpieczeństwa zostanie wydany przez krajowy organ ds. certyfikacji cyberbezpieczeństwa, wówczas to jego jednostka certyfikująca będzie akredytowana jako jednostka oceniająca zgodność.

Jeśli europejski program certyfikacji określa **specyficzne lub dodatkowe wymogi**, wówczas KOCC wyznacza jednostki oceniające zgodność, które spełniają te wymogi.

Krajowe schematy certyfikacji i certyfikaty cyberbezpieczeństwa

Cybersecurity Act wpłynie na funkcjonujące w niektórych państwach systemy certyfikacji. Nie oznacza to jednak, że wydane wcześniej krajowe certyfikaty przestaną obowiązywać. Nawet jeśli zostały objęte nowymi europejskimi programami certyfikacji, **zachowają ważność do daty wygaśnięcia określonej w przyznanym już certyfikacie.**

Jeśli zaś chodzi o krajowe programy certyfikacji cyberbezpieczeństwa, to te z nich które zostaną objęte europejskimi programami certyfikacji, **przestaną obowiązywać** od daty ustalonej w akcie wykonawczym danego europejskiego programu. Jeśli jednak krajowy program **nie został objęty** europejskim odpowiednikiem, nadal **będzie funkcjonować**.

Państwa członkowskie nie wprowadzają nowych krajowych programów certyfikacji cyberbezpieczeństwa dla produktów, procesów i usług ICT, które zostały już objęte europejskim programem certyfikacji.

Wydawanie certyfikatów cyberbezpieczeństwa

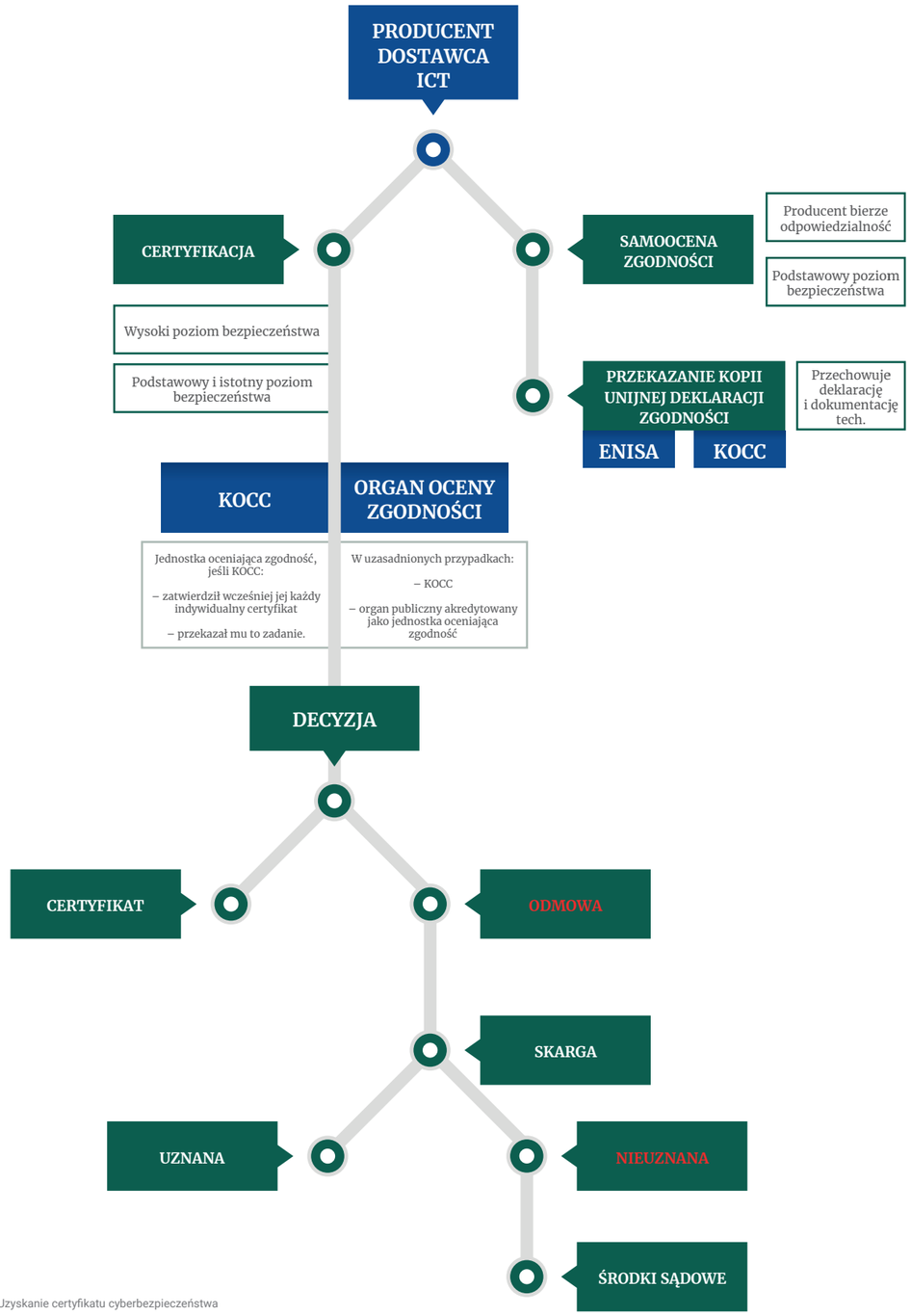
O tym, który organ może wydać europejski certyfikat cyberbezpieczeństwa, decyduje wymagany poziom bezpieczeństwa dla danego produktu bądź usługi ICT, określany przez program certyfikacji, zgodnie z poniższą tabelą.

Uzasadnienia zaufania	Kto wydaje certyfikat	Wyjątki
Podstawowy/ Istotny	Jednostki oceniające zgodność	Schemat może wskazywać, że certyfikat wydaje wyłącznie organ publiczny: krajowy organ certyfikacji cyberbezpieczeństwa organ publiczny akredytowany jako jednostka oceniająca zgodność
Wysoki	Krajowe organy ds. certyfikacji cyberbezpieczeństwa (KOCC)	Może to być jednostka oceniająca zgodność, jeśli KOCC: zatwierdził wcześniej każdy indywidualny certyfikat wydany przez ten organ oceny zgodności lub wcześniej przekazał mu to zadanie

Tabela 6. Wydawanie certyfikatów cyberbezpieczeństwa.

[43] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r. ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93
[44] Wymogi określa załącznik do powyższego rozporządzenia.

Poniższy schemat przedstawia proces uzyskania certyfikatu:



Rys. 3. Uzyskanie certyfikatu cyberbezpieczeństwa

Rozporządzenie przewiduje ustanowienie przez państwa członkowskie sankcji na wypadek naruszeń przepisów rozporządzenia i europejskich programów certyfikacji cyberbezpieczeństwa. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające.

Nowy mandat ENISA

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (*The European Union Agency for Network and Information Security* – ENISA) została założona w 2004 roku. Do tej pory mandat ENISA był czasowy, kończył się w czerwcu 2020 r. Przepisy, które wprowadza *Cybersecurity Act*, zapewniają ENISA stały i jasno sprecyzowany mandat, większy wpływ na ekosystem cyberbezpieczeństwa UE oraz większy niż dotąd budżet.

ENISA jest niezależnym ośrodkiem gromadzącym specjalistyczną wiedzę z zakresu cyberbezpieczeństwa, z siedzibą w Grecji. Głównym celem Agencji jest zapewnienie wysokiego poziomu cyberbezpieczeństwa w UE. Agencja wykonuje zadania powierzone jej na mocy przepisów unijnych i działa tak, aby nie powielać zadań realizowanych przez państwa członkowskie.

W momencie utworzenia w 2004 roku (Regulacja EC no. 460/2004), ENISA otrzymała mandat na 5 lat, ale był on przedłużany dwukrotnie w 2009 i 2011 roku. ENISA była jedyną agencją europejską z tymczasowym mandatem, który wygasał w czerwcu 2020 roku. W komunikacie z lipca 2016 Komisja Europejska zapowiedziała rewizję mandatu ENISA. Efektem był przygotowany akt legislacyjny, zaprezentowany 13 września 2017 roku w ramach tzw. "pakietu cybernetycznego".

Główne zadania ENISA to:

1. **Zaangażowanie w rozwój i wdrażanie polityki i prawa UE**

   ENISA ma wypracowywać niezależne opinie i analizy, zapewniać wkład do unijnej polityki i polityk sektorowych oraz prawa w dziedzinie cyberbezpieczeństwa. Agencja ma też wspierać państwa członkowskie w tworzeniu narodowych strategii cyberbezpieczeństwa, pomagać we wdrożeniu unijnych wytycznych w tym zakresie oraz przepisów prawnych dotyczących ochrony danych i prywatności.

2. **Wsparcie w budowaniu zdolności w zakresie cyberbezpieczeństwa**

   Nowym zadaniem Agencji jest pomoc państwom członkowskim, instytucjom unijnym, agencjom i organizacjom, w przeciwdziałaniu zagrożeniom teleinformatycznym. W tym zakresie ENISA współpracuje z zespołem CERT-EU[45]. ENISA wspiera również CSIRT krajowe w rozwoju ich kompetencji i wymianie doświadczeń, a także przynajmniej raz na dwa lata, organizuje unijne ćwiczenia cyberbezpieczeństwa (*CyberEurope*).

   Agencja ma też konkretne zadania, związane z implementacją Dyrektywy NIS: wspiera grupę współpracy w identyfikacji operatorów usług kluczowych działających transgranicznie, zapewnia sekretariat dla sieci CSIRT oraz wspiera współpracę krajowych CSIRT; ułatwia wymianę informacji między sektorami zdefiniowanymi jako kluczowe, opracowuje dobre praktyki dla sektorów (wytyczne i wskazówki).

3. **Zaangażowanie we współpracę na poziomie UE**

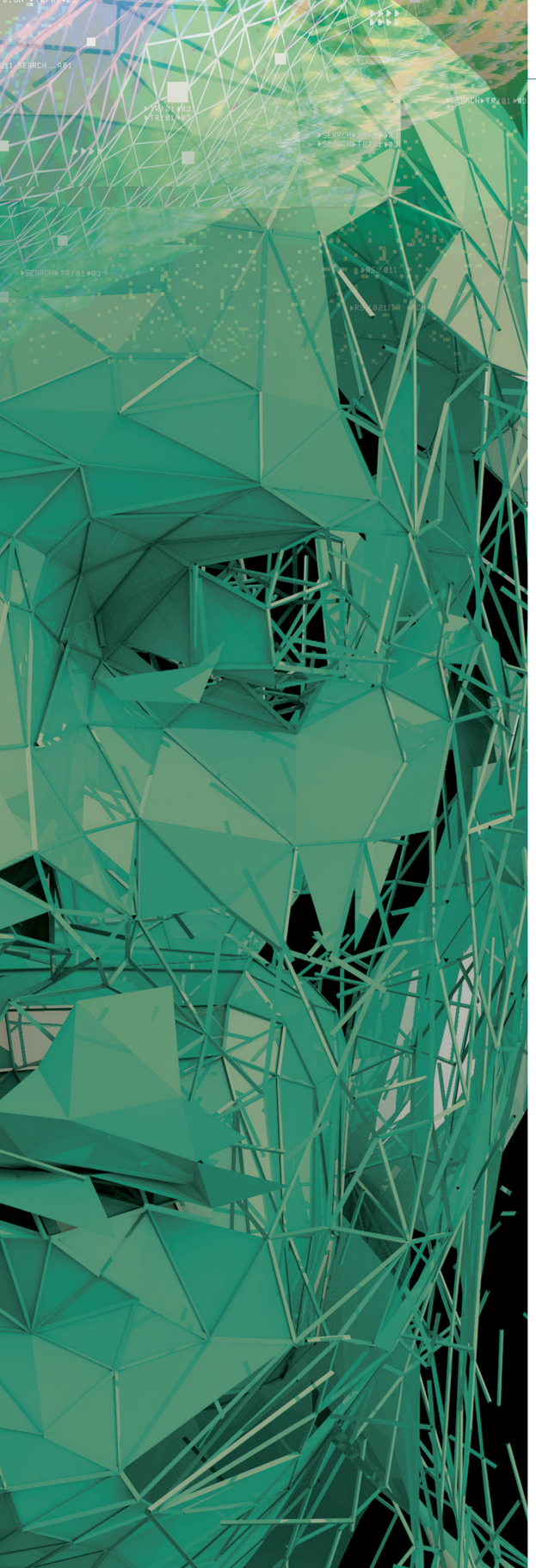
   Kolejnym nowym zadaniem, wzmacniającym rolę Agencji, jest wspieranie współpracy między państwami członkowskimi, instytucjami unijnymi, innymi agencjami UE oraz pozostałymi interesariuszami. W tym zakresie ENISA jest zaangażowana w budowanie synergii tych podmiotów z zespołem CERT-EU, służbami zajmującymi się cyberprzestępczością, organami nadzorującymi ochronę prywatności i danych osobowych; oferuje doradztwo w zakresie polepszania kompetencji CSIRT; wspiera państwa członkowskie w ocenie incydentów i analizie podatności; opracowuje, regularny raport dotyczący aktualnej sytuacji cyberbezpieczeństwa, z uwzględnieniem zagrożeń i incydentów zgłoszonych przez państwa członkowskie, sieć CSIRT, pojedyncze punkty kontaktowe, a także Europejskie Centrum Cyberprzestępczości (EC3) w Europolu; wspiera obsługę incydentów transgranicznych i zagrożeń cyberbezpieczeństwa na dużą skalę[46].

4. **Działania w obszarze certyfikacji cyberbezpieczeństwa produktów, usług i procesów ICT**

   W związku z wprowadzeniem europejskiego schematu certyfikacji, ENISA otrzymała szereg kompetencji i obowiązków w tym zakresie. Agencja ma wspierać i promować wdrażanie certyfikacji produktów, usług i procesów ICT poprzez monitorowanie aktualnych standardów, a także rekomendowanie odpowiednich norm i specyfikacji technicznych zgodnych z europejskimi schematami certyfikacji. W procesie europejskiej

[45] Zespół ds. Reagowania na incydenty komputerowe (CERT-EU) dla instytucji, agencji i organów UE. Zespół składa się z ekspertów ds. bezpieczeństwa IT z głównych instytucji UE (Komisja Europejska, Sekretariat Generalny Rady, Parlament Europejski, Komitet Regionów, Komitet Ekonomiczno-Społeczny). Ściśle współpracuje z innymi zespołami CERT w państwach członkowskich i poza nimi, a także z firmami zajmującymi się bezpieczeństwem IT.

[46] W tym zakresie ENISA agreguje sprawozdania z państw członkowskich, dba o efektywny przepływ informacji w sieci CSIRT, wspiera komunikację publiczną dotyczącą incydentów, a także testuje procedury reagowania na incydenty transgraniczne na poziomie unijnym.



certyfikacji to właśnie ENISA przygotowuje propozycję schematu, który następnie przekazuje do Komisji Europejskiej. Wraz z KE Agencja przewodniczy Grupie Interesariuszy ds. Certyfikacji Cyberbezpieczeństwa (*Stakeholer Cybersecurity Certification Group)*, która składa się z ekspertów reprezentujących interesariuszy[47]. Poza tym ENISA opracowuje i publikuje wytyczne i dobre praktyki w zakresie certyfikacji oraz wspiera budowę zdolności państw członkowskich w tym zakresie, na przykład organizując warsztaty czy konferencje.

5. **Zarządzanie i udostępnianie informacji z zakresu cyberbezpieczeństwa**

   Nowym zadaniem Agencji jest analizowanie rozwoju nowoczesnych technologii i ocenianie aktualnych trendów pod kątem społecznym, prawnym, ekonomicznym i wpływu innowacji na cyberbezpieczeństwo. ENISA przygotowuje analizy strategiczne incydentów, aby identyfikować zagrożenia oraz móc im zapobiegać. Zapewnia doradztwo, a także dostarcza wytyczne i najlepsze praktyki dla wzrostu poziomu cyberbezpieczeństwa infrastruktury krytycznej, operatorów usług kluczowych i dostawców usług cyfrowych.

6. **Działania z zakresu edukacji i zwiększania świadomości**

   W stosunku do wcześniejszego mandatu, rola ENISA w zakresie działań edukacyjnych została wzmocniona. Agencja dostarcza dobre praktyki i wskazówki obywatelom i organizacjom, a we współpracy z państwami członkowskimi organizuje regularne kampanie informacyjne. Co roku, w październiku, koordynuje Europejski Miesiąc Cyberbezpieczeństwa[48]. Wspiera również lokalne działania edukacyjne państw członkowskich.

7. **Zaangażowanie w badania i rozwój**

   Agencja wspiera budowę programu strategicznych badań i innowacji na poziomie unijnym w dziedzinie cyberbezpieczeństwa poprzez doradztwo w identyfikacji potrzeb i priorytetów badawczych, a na życzenie Komisji, uczestnictwo we wdrażaniu programów finansowania badań.

8. **Wspieranie współpracy międzynarodowej**

   ENISA angażuje się w budowę współpracy w zakresie cyberbezpieczeństwa między UE, państwami trzecimi i organizacjami międzynarodowymi. Jako obserwator bierze udział w ćwiczeniach międzynarodowych, ułatwia wymianę informacji i dobrych praktyk. Wraz z MSCG (*Member States Certification Group*) przygotowuje ekspertyzy dotyczące umów o wzajemnym uznawaniu certyfikatów bezpieczeństwa z państwami trzecimi.

[47] Członków grupy wybiera Komisja, na wniosek ENISA.

[48] Europejski Miesiąc Cyberbezpieczeństwa to cykliczna, odbywająca się co roku w październiku, inicjatywa Komisji Europejskiej, koordynowana przez ENISA. W 2018 roku odbyła się już 6 edycja ECSM. W Polsce kampanię koordynuje Państwowy Instytut Badawczy NASK.

Organizacja Agencji

Struktura administracyjna Agencji składa się z Zarządu, Rady Wykonawczej, Dyrektora Wykonawczego, Grupy Doradczej ENISA (ENISA Advisory Group) i Sieci Krajowych Urzędników Łącznikowych. Poniższa tabela prezentuje strukturę Agencji.

Zarząd	W skład zarządu wchodzi po jednym przedstawicielu z każdego państwa członkowskiego oraz dwóch przedstawicieli Komisji. Wszyscy mają prawo głosu, a każdy z nich wyznacza zastępcę, który reprezentuje go w razie nieobecności. Do Zarządu powoływane są osoby, które posiadają wiedzę z zakresu cyberbezpieczeństwa, a także kompetencje kierownicze i administracyjne. Zarząd podejmuje decyzje większością głosów. Wyjątkiem są głosowania dotyczące przyjęcia jednolitego dokumentu programowego[49], budżetu rocznego, mianowania/przedłużania kadencji/odwołania Dyrektora Wykonawczego, gdzie potrzebna jest większość dwóch trzecich głosów. Zarząd odpowiada za określenie ogólnego kierunku działań Agencji oraz przygotowanie propozycji budżetu, a także opracowuje roczne sprawozdanie z działalności ENISA, które jest potem przekładane Parlamentowi Europejskiemu, Komisji, Radzie i Trybunałowi Obrachunkowemu. Zarząd mianuje także Dyrektora Wykonawczego ENISA.
Przewodniczący Zarządu	Na czele Zarządu stoi Przewodniczący, który jest wybierany większością dwóch trzecich głosów na cztery lata, z możliwością jednokrotnego powtórzenia kadencji. Zarząd wybiera także jego zastępcę. Przewodniczący zwołuje posiedzenia Zarządu, co najmniej dwa razy w roku.
Rada Wykonawcza	Organem wspierającym Zarząd jest Rada Wykonawcza. Rada składa się z pięciu członków Zarządu i reprezentanta Komisji, mianowanych na cztery lata, z możliwością ponownej kadencji. Posiedzenia rady odbywają się przynajmniej raz na kwartał. Dyrektor Wykonawczy może brać w nich udział, jednak nie ma prawa głosu. Rada przygotowuje decyzje do głosowania Zarządu oraz wspiera Dyrektora Wykonawczego w ich wdrażaniu.
Dyrektor Wykonawczy	Agencją zarządza Dyrektor Wykonawczy, który w wykonywaniu swoich obowiązków jest niezależny i odpowiada przed Zarządem. Może on powoływać grupy robocze, składające się z ekspertów z państw członkowskich. Procedura powołania grup jest określona w wewnętrznych zasadach działania Agencji.
Grupa Doradcza ENISA (ENISA Advisory Group)	W ramach agencji działa Grupa Doradcza ENISA. Jest powoływana na dwuipółletnią kadencję przez Zarząd, na wniosek Dyrektora Wykonawczego. To grupa ekspertów reprezentujących różnych interesariuszy, takich jak dostawcy sieci oraz usług ICT, MŚP, operatorzy, grupy konsumenckie, przedstawiciele nauki oraz europejskich organizacji odpowiedzialnych za ochronę danych i egzekwowanie prawa. Grupie przewodniczy Dyrektor Wykonawczy lub osoba przez niego powołana. Zadaniem grupy jest doradzanie Agencji i Dyrektorowi Wykonawczemu.
Sieć Krajowych Urzędników Łącznikowych	W ramach ENISA funkcjonuje również Sieć Krajowych Urzędników Łącznikowych, w której skład wchodzi po jednym przedstawicielu z każdego państwa członkowskiego. Zadaniem sieci jest umożliwianie sprawnej wymiany informacji pomiędzy ENISA a państwami członkowskimi, wspieranie Agencji w promowaniu jej działalności, wytycznych i zaleceń, a także zapewnienie komunikacji pomiędzy ENISA a krajowymi ekspertami cyberbezpieczeństwa.

Tabela 7. Organizacja ENISA

[49] Jednolity dokument programowy zawiera roczny i wieloletni plan działań ENISA, w którym opisane są szczegółowe cele i oczekiwane wyniki, wraz ze wskaźnikami, które pozwolą ocenić działalność Agencji.

Współpraca z państwami członkowskimi, państwami trzecimi i organizacjami międzynarodowymi

ENISA może współpracować z państwami trzecimi lub organizacjami międzynarodowymi. Po uprzednim zatwierdzeniu przez Komisję, Agencja podejmuje zobowiązania robocze, które nie stanowią zobowiązań prawnych UE, ani państw członkowskich. ENISA współpracuje także z państwami trzecimi, które mają podpisane porozumienia z UE. W porozumieniach określa się charakter, zakres i sposób współpracy wraz z informacją o udziale w inicjatywach, wkładzie finansowym, zaangażowanym personelu itp. Współpraca z państwami trzecimi i organizacjami międzynarodowymi powinna odbywać się w obszarach właściwych dla ENISA i zgodnie ze strategią przyjętą przez Zarząd.

Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji – nowa propozycja KE

12 września 2018 roku Komisja Europejska przedstawiła propozycję rozporządzenia ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych wraz z siecią krajowych ośrodków koordynacji. Celem propozycji jest stymulowanie europejskiego ekosystemu technologicznego i przemysłowego oraz wzmacnianie współpracy w dziedzinie cyberbezpieczeństwa między różnymi branżami i środowiskami naukowymi. Zgodnie z propozycją KE, częścią nowego ekosystemu ma być Europejskie Centrum Cyberbezpieczeństwa, sieć krajowych ośrodków koordynacji oraz środowiska posiadające kompetencje w dziedzinie cyberbezpieczeństwa.

Europejskie Centrum Cyberbezpieczeństwa to nowa instytucja, której zadaniem będzie:

- ułatwianie i pomoc w koordynacji pracy sieci krajowych ośrodków koordynacji;
- zwiększanie możliwości i wiedzy oraz ulepszanie infrastruktury cyberbezpieczeństwa, z korzyścią dla przemysłu, sektora publicznego i środowisk naukowych;
- wnoszenie wkładu w powszechne wdrażanie w całej gospodarce nowoczesnych produktów i rozwiązań w dziedzinie cyberbezpieczeństwa;
- poprawa zrozumienia kwestii cyberbezpieczeństwa i ograniczanie niedoborów kwalifikacji w zakresie cyberbezpieczeństwa w UE;
- wzmacnianie badań naukowych i rozwoju w dziedzinie cyberbezpieczeństwa w UE;
- zacieśnienie współpracy między kręgami cywilnymi i obronnymi w odniesieniu do technologii i aplikacji podwójnego zastosowania w dziedzinie cyberbezpieczeństwa;
- zwiększanie synergii między wymiarem cywilnym i wymiarem obronnym cyberbezpieczeństwa w odniesieniu do Europejskiego Funduszu Obronnego.

Zasadniczą rolą centrum ma być dystrybuowanie funduszy europejskich w dziedzinie cyberbezpieczeństwa z poziomu europejskiego na poziom państw członkowskich. Dodatkowo centrum ma gromadzić wiedzę i kompetencje.

Zgodnie z propozycją KE, centrum składa się z:

- **Rady zarządzającej,** w której skład wchodzi po jednym przedstawicielu każdego państwa członkowskiego oraz pięciu przedstawicieli Komisji Europejskiej;
- **Dyrektora wykonawczego,** zatrudnianego przez centrum, a wybieranego i mianowanego przez radę zarządzającą z listy wskazanej przez Komisję Europejską;
- **Rady konsultacyjnej ds. przemysłowych i naukowych,** która liczy maksymalnie 16 członków. Jest mianowana przez radę zarządzającą spośród przedstawicieli podmiotów, będących częścią środowiska, posiadającego kompetencje w dziedzinie cyberbezpieczeństwa.

Sieć krajowych ośrodków koordynacji- ośrodki nominowane będą przez kraje członkowskie, a następnie akredytowane przez Komisję Europejską. Instytucje mają wspierać działania centrum. Poza tym zadania ośrodków są następujące:

- ułatwianie przemysłowi i innym podmiotom na szczeblu państwa członkowskiego udziału w projektach transgranicznych;
- określanie i eliminowanie, wspólnie z Centrum Kompetencji, stojących przed przemysłem wyzwań z zakresu cyberbezpieczeństwa w konkretnych sektorach;
- pełnienie roli krajowego punktu kontaktowego na potrzeby środowiska, posiadającego kompetencje w dziedzinie cyberbezpieczeństwa i Centrum Kompetencji;
- tworzenie synergii z odpowiednimi działaniami na szczeblu krajowym i regionalnym;

- wdrażanie działań, na które Centrum Kompetencji przyznało dotacje;
- promowanie i rozpowszechnianie przez sieć, środowisko posiadające kompetencje w dziedzinie cyberbezpieczeństwa i Centrum Kompetencji, odpowiednich wyników prac na szczeblu krajowym i regionalnym;
- ocena wniosków o włączenie do środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa, składanych przez podmioty, które mają siedzibę w tym samym państwie członkowskim co ośrodek koordynacji.

Środowiska posiadające kompetencje w dziedzinie cyberbezpieczeństwa będą współpracować z Europejskim Centrum i ropowszechniać fachową wiedzę. Jego członkowie mają pochodzić z różnych środowisk, tak aby reprezentować różne punkty widzenia. Będą to np. organizacje przemysłowe, akademickie, naukowe, non-profit oraz stowarzyszenia i podmioty publiczne. Warunkiem akredytacji na członka środowiska jest wykazanie się fachową wiedzą z zakresu cyberbezpieczeństwa w co najmniej jednej z dziedzin:

- badania naukowe;
- rozwój przemysłu;
- szkolenie i kształcenie.

Akredytacji dokonuje Europejskie Centrum Komptencji. Jest ona poprzedzona wyznaczeniem danych organizacji na członków środowiska na mocy prawa krajowego, po tym jak krajowy ośrodek zweryfikuje kandydujące podmioty. Poza tym na członków środowiska mogą zostać powołane także organy, agencje i urzędy Unii Europejskiej.

Zadania członków środowiska posiadającego kompetencje w dziedzinie cyberbezpieczeństwa obejmują:

- wsparcie Centrum Kompetencji w wypełnianiu jego misji i osiąganiu celów oraz współpracę z właściwymi krajowymi ośrodkami koordynacji;
- udział w działaniach promowanych przez Centrum Kompetencji i krajowe ośrodki koordynacji;
- uczestniczenie w grupach roboczych, ustanowionych przez radę zarządzającą Centrum Kompetencji, w celu realizacji działań określonych w planie prac Centrum Kompetencji;
- wspieranie Centrum Kompetencji i krajowych ośrodków koordynacji w promocji projektów;
- rozpowszechnianie wyników działań i projektów prowadzonych przez społeczność.

Propozycja rozporządzenia w sprawie Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych budzi wiele kontrowersji. Przede wszystkim nie do końca uzasadniona wydaje się dominująca rola Komisji Europejskiej w radzie zarządzającej, a także uzależnienie prawa głosu w radzie dla państw członkowskich od funduszy wpłacanych na Centrum. Dodatkowo część zadań Centrum wyraźnie pokrywa się z nowym mandatem Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA).

Europejski kodeks łączności elektronicznej – reforma prawa telekomunikacyjnego

11 grudnia 2018 roku został przyjęty Europejski kodeks łączności elektronicznej[50](Kodeks). Projekt dyrektywy był procedowany od września 2016 roku. Jest to kompleksowa reforma regulacji telekomunikacyjnych (z 2009 roku) i **jeden z istotniejszych projektów w zakresie Jednolitego Rynku Cyfrowego**. Zmiany dotyczą dostępu do infrastruktury, regulacji widma radiowego oraz definicji i regulacji usług łączności elektronicznej. Dodatkowo Komisja Europejska zaproponowała nowy cel ram regulacyjnych: zapewnienie powszechnego dostępu i **wykorzystania łączności o bardzo dużej przepustowości.**

Dyrektywa zwiększa także cyberbezpieczeństwo sektora telekomunikacyjnego. Zgodnie z art.40, operatorzy mają obowiązek zapewniania właściwych środków technicznych i organizacyjnych w razie wystąpienia zagrożenia dla bezpieczeństwa sieci lub usług. Środki te mają być proporcjonalne do istniejącego ryzyka, tak aby minimalizować skutki zagrożeń. Dodatkowo przedsiębiorcy zobowiązani są do zapewnienia integralności usług i informowania organów właściwych w przypadkach naruszeń bezpieczeństwa. Żeby określić jak istotny jest wpływ zagrożenia bezpieczeństwa, uwzględnia się w szczególności następujące parametry:

- liczbę użytkowników, których dotyczy incydent związany z bezpieczeństwem,
- czas trwania incydentu,
- geograficzny zasięg obszaru dotkniętego incydentem,
- zakres funkcjonowania sieci lub usługi,
- wpływ na działalność ekonomiczną i społeczną.

Parametry te są zgodne z tymi wprowadzonymi przez Dyrektywę NIS, a co za tym idzie, przez Ustawę o Krajowym Systemie Cyberbezpieczeństwa .

[50] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiająca Europejski kodeks łączności elektronicznej.

Natomiast zgodnie z art. 41 Kodeksu właściwe organy krajowe mają prawo wymagać od przedsiębiorców:

- dostarczania informacji potrzebnych do oceny bezpieczeństwa i integralności ich usług i sieci, w tym dokumentów dotyczących polityki bezpieczeństwa;
- poddania się audytowi bezpieczeństwa przeprowadzanemu przez wykwalifikowany niezależny podmiot lub właściwy organ, a także udostępnienia właściwemu organowi wyników takiego audytu. Koszty audytu ponosi przedsiębiorstwo[51].

Negocjacje ePrivacy

Projekt rozporządzenia ePrivacy[52] został przedstawiony 10 stycznia 2017 roku. Rozporządzenie miało wejść w życie razem z RODO/GDPR i stanowić specjalną regulację w zakresie prywatności w Internecie (tzw. *lex specialis* do RODO). Negocjacje znacznie się jednak przedłużają.

Projekt regulacji obejmuje dostawców usług telekomunikacyjnych, dostawców Internetu oraz podmioty typu: Facebook, Messenger, Skype, Gmail, WhatsApp czy Viber. Rozporządzenie dotyczy także tych podmiotów, które mają siedzibę poza Unią Europejską, a świadczą usługi obywatelom któregoś z krajów UE.

Projekt rozszerza definicję marketingu internetowego oraz wprowadza ochronę zarówno dla osób fizycznych, jak i prawnych. Ważnym elementem jest zwiększenie przejrzystości plików *cookies* (służących do zapamiętywania preferencji i personalizowania stron internetowych), konieczność anonimizacji elektronicznych wiadomości wysyłanych przez użytkowników, a także objęcie ochroną metadanych, które dostarczają szczególnie chronione informacje takie jak lokalizacja, historia przeglądarki czy godzina połączenia i czas wysłania wiadomości.

Konkluzje Rady UE w sprawie szkodliwych działań w Internecie – dyplomacja UE w służbie cyberbezpieczeństwu

16 kwietnia 2018 roku Rada UE przyjęła Konkluzje w sprawie szkodliwych działań w Internecie[53]. Rada wyraziła zaniepokojenie faktem, że państwa trzecie oraz podmioty niepaństwowe zwiększają swoją gotowość oraz zdolność do realizacji celów poprzez szkodliwe działania w cyberprzestrzeni. Potępiła także wykorzystanie technologii informacyjnych i komunikacyjnych do szkodliwych działań. Wprost wskazano ataki WannaCry i NotPetya, które spowodowały znaczne szkody gospodarcze w UE i poza nią. Rada podkreśliła, że takie działania są niedopuszczalne. Zapowiedziano kontynuowanie prac nad dalszym rozwojem i wdrażaniem dobrowolnych, niewiążących norm i zasad działania państw w cyberprzestrzeni, m.in. w ramach ONZ i innych forów międzynarodowych.

Działania Rady są kontynuacją inicjatywy rozpoczętej w 2017 roku, kiedy to UE przyjęła ramy wspólnej unijnej reakcji dyplomatycznej (tzw. *diplomacy toolbox*, czyli zestaw narzędzi dla dyplomacji cyfrowej). Dokument przewiduje wykorzystanie unijnej dyplomacji, jako reakcji na szkodliwe działania w cyberprzestrzeni (proporcjonalnie do zakresu, skali, czasu trwania, intensywności, złożoności, zaawansowania i skutków działania)[54].

Sztuczna Inteligencja dla Europy

W 2018 roku Komisja Europejska dużo uwagi poświęciła zagadnieniom związanym ze sztuczną inteligencją (AI) i etycznymi aspektami jej rozwoju.

Komunikat Komisji Europejskiej Sztuczna Inteligencja dla Europy

25 kwietnia 2018 KE przedstawiła Komunikat w sprawie AI *(Sztuczna Inteligencja dla Europy)*. Dokument zakłada działania w dziedzinie technologii, etyki, prawa i ekonomii. AI została zidentyfikowana jako istotne wyzwanie strategiczne. KE podkreśla różnice w funduszach przeznaczanych na AI w Europie i na świecie – europejskie inwestycje w dziedzinie AI sięgają jedynie 2,4-3,2 mld euro, podczas gdy w Azji i Ameryce Północnej jest to odpowiednio 6,5-9,7 oraz 12,1-18,6 mld euro. Wyzwanie AI zostało zaadresowane w trzech aspektach:

1. **Zwiększenie zdolności technologicznej i przemysłowej UE oraz wykorzystanie sztucznej inteligencji w różnych dziedzinach gospodarki**

   Najważniejszym postulatem KE jest zwiększenie wydatków na AI, które do końca 2020 roku mają osiągnąć 20 mld euro. Dotyczą one jednak sektora prywatnego i publicznego, a KE przeznaczyła na inwestycje w zakresie sztucznej inteligencji jedynie 1,5 mld euro z funduszy Horyzontu 2020 (program wspierający rozwój i innowacje w Europie).

2. **Przygotowanie się do zmian społeczno-gospodarczych związanych z rozwojem sztucznej inteligencji**

   Rozwój sztucznej inteligencji przyczyni się do powstania nowych miejsc pracy, ale spowoduje także zanik niektórych znanych dziś zawodów. Dlatego Komisja zachęca do zmian w edukacji i planuje przygotować nowe schematy szkoleniowe wraz z sektorowym *blueprintem*, który uwzględni wyzwania stojące przed sektorami. Ponadto KE zapowiedziała kontynuację działań związanych z rozwojem umiejętności cyfrowych.

3. **Przygotowanie właściwych ram prawnych i etycznych dla rozwoju sztucznej inteligencji**

   Rozwój sztucznej inteligencji to także wyzwania w zakresie prawa i etyki. W związku z tym KE zapowiedziała opracowanie wytycznych w zakresie etyki oraz interpretacji dyrektywy odnoszącej się do odpowiedzialności za produkt.

Grupa ekspercka ds. Sztucznej Inteligencji

W czerwcu 2018 r. KE powołała grupę 52 ekspertów ds. AI. W jej skład weszli przedstawiciele ośrodków akademickich, biznesu i społeczeństwa obywatelskiego. Zadaniem grupy było opracowanie rekomendacji w zakresie rozwoju polityki sztucznej inteligencji. 18 grudnia grupa zaproponowała **Wytyczne w Zakresie Rozwoju i Wykorzystania Sztucznej Inteligencji** (*Ethics Guidelines for the Development and Use of Artificial Intelligence*)[55], w których opisała strukturę dla godnej zaufania AI. Dokument był przedmiotem konsultacji społecznych, a jego ostateczna wersja ma zostać opublikowana w marcu 2019 r.

Skoordynowany Plan dla Sztucznej Inteligencji

7 grudnia 2018 r. KE opublikowała Skoordynowany Plan dla Sztucznej Inteligencji[56]. Dokument podejmuje siedem głównych zagadnień:

1. **Wspólne cele i wysiłek na rzecz AI**

   Komisja zaprezentowała ramy dla krajowych strategii sztucznej inteligencji i zachęciła kraje członkowskie, aby do połowy 2019 roku każde z nich przyjęło taką strategię. W dokumentach powinny się znaleźć m.in. informacje na temat funduszy przeznaczonych na rozwój AI. KE szczególnie zależy, żeby środki na rozwój AI w Europie, ze strony sektora publicznego i prywatnego, osiągnęły poziom 20 mld euro rocznie.

2. **Partnerstwa publiczno-prywatne, finansowanie start-upów oraz innowacyjnych małych i średnich przedsiębiorstw**

   KE podkreśliła konieczność ścisłej współpracy sektora prywatnego i publicznego, zwłaszcza w kontekście badań naukowych oraz tworzenia nowych technologii i zastosowań dla AI. Dlatego szczególny nacisk ma być położony na współpracę biznesu i ośrodków akademickich. Komisja przewidziała także, że w 2020 roku przeznaczy 100 mln euro na działalność start-upów i innowacyjnych firm w dziedzinie AI.

3. **Wzmacnianie wiarygodności AI i związanych z nią rozwiązań technologicznych**

   Aby wspierać współpracę pomiędzy najlepszymi zespołami badawczymi w Europie, KE zapowiedziała utworzenie sieci centrów doskonałości w zakresie badań nad AI. Dodatkowo KE planuje rozbudowanie *Digital Innovation Hub* w stronę sztucznej inteligencji, za kluczowe uznając sektory rolnictwa, inteligentnych miast i autonomicznych samochodów.

4. **Dostosowywanie programów i systemów szkolnych do wyzwań związanych z rozwojem sztucznej inteligencji**

   Rozwój nowoczesnych technologii sprawia, że konieczne jest nabywanie nowych kompetencji, zarówno przez osoby młode, uczące się, jak i te które funkcjonują już na rynku pracy. Dlatego ważne jest stymulowanie nauki przez całe życie oraz wykształcenie kadr, które będą odpowiadać za implementację rozwiązań z zakresu AI. Komisja zapowiedziała wspieranie programów magisterskich i doktorskich poprzez tworzenie programów badawczych.

5. **Budowa europejskiej przestrzeni danych niezbędnej dla AI w Europie**

   KE podkreśliła, że dalszy rozwój AI wymaga stworzenia odpowiedniej infrastruktury oraz dobrze funkcjonującego ekosystemu danych, opartego na zaufaniu. W 2020 r. Komisja będzie rozwijała wspólną bazę danych obrazów diagnostycznych z sektora zdrowia. Dodatkowo wspierane będą także rozwiązania AI w zakresie cyberbezpieczeństwa.

6. **Opracowanie wytycznych etycznych i zapewnienie ram prawnych sprzyjających innowacjom**

   KE zaznaczyła, że rozwój sztucznej inteligencji w Europie musi następować w sposób etyczny i zgodny z prawami człowieka. Dlatego w marcu 2019 roku przedstawiona zostanie ostateczna wersja Wytycznych w Zakresie Rozwoju i Wykorzystania Sztucznej Inteligencji.

[51] https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018L1972&from=it
[52] Rozporządzenie w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE.
[53] Council conclusions on malicious cyber activities, 7517/18.
[54] https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=uriserv%3AOJ.L_.2017.239.01.0036.01.ENG
[55] hhttps://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_draft_ethics_guidelines_18_december.pdf
[56] https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence

7. **Aspekty związane z bezpieczeństwem AI**

   Zdaniem Komisji niezwykle ważne jest rozpatrywanie aspektów bezpieczeństwa związanych z AI w trzech aspektach:

   - wspieranie sektora bezpieczeństwa przez rozwiązania z zakresu sztucznej inteligencji;
   - ochrona technologii AI przed atakami i zagrożeniami cyberbezpieczeństwa;
   - zaadresowanie potencjalnych nadużyć w zakresie wykorzystania sztucznej inteligencji

Dezinformacja

Rok 2018 był w Unii Europejskiej czasem wzmożonej aktywności w dziedzinie dezinformacji. Opublikowano cztery istotne dokumenty w tym zakresie.

Według Komórki UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych[57] (*EU Hybrid Fusion Cell*) największe zagrożenie dla Unii Europejskiej, w kontekście zaplanowanych na maj 2019 wyborów do Parlamentu Europejskiego, stanowi dezinformacja ze strony Federacji Rosyjskiej[58]. Do 2020 roku w państwach członkowskich odbędzie się łącznie ponad 50 wyborów krajowych, prezydenckich oraz lokalnych[59]. Tymczasem, w ocenie Komisji, w ostatnich latach kampanie dezinformacyjne miały wyraźny wpływ na wybory odbywające się na terytorium UE[60].

Komunikat KE: Zwalczanie dezinformacji w Internecie: podejście europejskie

Opublikowany 26 kwietnia dokument przedstawia zakres, skalę i analizę zjawiska, opisuje zagrożenia związane rozpowszechnianiem dezinformacji i proponuje konkretne działania przeciwdziałające temu zjawisku. Komunikat był następstwem raportu przedstawionego przez Grupę ekspertów tzw. „wysokiego szczebla" (*high-level group of experts* – HLEG) zatytułowanego „*A multi-dimensional approach to disinformation*"[61].

Główne obszary działania, na które zwraca uwagę Komisja, to:

1. **Bardziej przejrzysty, godny zaufania i odpowiedzialny ekosystem internetowy**

   KE wezwała platformy internetowe, aby bardziej zaangażowały się w zwalczanie dezinformacji w ramach samoregulacji poprzez utworzenie niezależnej europejskiej sieci podmiotów weryfikujących fakty.

2. **Bezpieczne i odporne procesy wyborcze**

   Komisja zapowiedziała szczególną troskę o bezpieczeństwo sieci i systemów informatycznych w związku z wyborami do Parlamentu Europejskiego w 2019 r.

3. **Wspieranie edukacji i umiejętności korzystania z mediów**

   Umiejętność weryfikacji faktów i krytycznego myślenia jest podstawą dla budowy odporności społeczeństwa na zjawisko *fake newsów*. Komisja podkreśliła wagę rozwoju edukacji cyfrowej, a także konieczność wzmacniania kompetencji korzystania z nowych mediów.

4. **Wsparcie dla wysokiej jakości dziennikarstwa jako istotnego elementu demokratycznego społeczeństwa**

   Konieczne jest wzmocnienie pozycji dziennikarzy, a także budowanie zaufania do osób pracujących w tym zawodzie. Dziennikarze nie powinni obawiać się nowoczesnych technologii, tylko używać ich do rozpowszechniania informacji popartych transparentnymi źródłami.

5. **Zwalczanie wewnętrznych i zewnętrznych zagrożeń wynikających z dezinformacji poprzez komunikację strategiczną**

   W 2015 r. powołano grupę zadaniową East Stratcom, która przeciwdziała kampaniom dezinformacyjnym prowadzonym przez Rosję. W 2016 r. powstała Komórka UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych w ramach Centrum Analiz Wywiadowczych. W 2017 roku utworzono również Europejskie Centrum ds. Zwalczania Zagrożeń Hybrydowych.

Kodeks postępowania w zakresie zwalczania dezinformacji *(Code of Practice on Disinformation)*

We wrześniu 2018 roku Komisja Europejska opublikowała kodeks postępowania w zakresie zwalczania dezinformacji. Dokument jest formą samoregulacji sektora biznesowego i został opracowany przez przedstawicieli platform internetowych, branży reklamowej i mediów, przy wsparciu środowisk akademickich i społeczeństwa obywatelskiego. Skupiono się na działaniach w pięciu głównych obszarach:

[57] Komórka UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych została utworzona w 2016 roku w ramach Centrum Wywiadowczego i Sytuacyjnego UE powołanego przy Europejskiej Służbie Działań Zewnętrznych. Komórka analizuje informacje dotyczące zagrożeń hybrydowych, a następnie rozsyła raporty i analizy do instytucji UE oraz państw członkowskich, dbając aby osoby decyzyjne były dobrze poinformowane o możliwych zagrożeniach. W kwestiach cyberzagrożeń komórka opiera się na informacjach otrzymywanych m.in. z CERT-EU.

[58] Action Plan against Disinformation, s. 4

[59] Action Plan against Disinformation, s. 2

[60] Information Manipulation, a challenge to our democracies. A raport by the Policy Planning Staff and the Institute for Strategic Research

[61] W skład grupy wysokiego szczebla ds. fake news i dezinformacji online wchodzi 39 ekspertów. Są to przedstawiciele m.in. organizacji medialnych, dziennikarzy, środowisk akademickich czy platform internetowych. Przewodniczącym grupy jest prof. dr Madeleine de Cock Buning z Uniwersytetu w Utrechcie. Grupa doradza Komisji Europejskiej, pomagając przyjrzeć się bliżej zjawisku fake news. Do jej zadań należy m.in. wsparcie KE w określaniu ról i obowiązków poszczególnych interesariuszy oraz formułowanie rekomendacji. Grupa powstała w styczniu 2018 roku, a raport „A multi-dimensional approach to disinformation" ukazał się w marcu 2018 roku. Pełna treść raportu dostępna jest na stronie https://publications.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1

- Transparentność sponsorowanych treści.
- Identyfikacja fałszywych kont i botów.
- Przejrzystość i możliwość weryfikacji algorytmów.
- Dostęp do różnorodnych źródeł informacji.
- Monitoring prowadzony przez instytucje badawcze i władze publiczne.

W październiku 2018 roku kodeks podpisały największe platformy internetowe. **Jeżeli po roku obowiązywania kodeksu okaże się, że jego wdrożenie i wpływ na walkę z dezinformacją są niezadowalające, KE może zaproponować dalsze działania, w tym o charakterze regulacyjnym.**

Komunikat KE w sprawie wolnych i uczciwych wyborów europejskich (Election Package)

We wrześniu KE zaproponowała środki, które pozwolą zwiększyć przejrzystość internetowych reklam politycznych oraz umożliwią nakładanie sankcji za nielegalne wykorzystywanie danych osobowych do świadomego wpływania na wyniki wyborów europejskich.

Zalecenia Komisji Europejskiej w tym zakresie to:

- **Utworzenie krajowej sieci współpracy w dziedzinie wyborów** (m.in. organy wyborcze, ścigania, ds. cyberbezpieczeństwa i ochrony danych) oraz **wyznaczenie krajowego punktu kontaktowego** w ramach europejskiej sieci współpracy w dziedzinie wyborów.
- **Zapewnienie większej przejrzystości umieszczanych w Internecie reklam politycznych** – europejskie i krajowe partie polityczne powinny udostępnić informacje o kampaniach reklamowych w Internecie (wydatki, kryteria pozycjonowania, kto stoi za kampanią). Jeśli tego nie zrobią, kraje członkowskie powinny nałożyć na nie sankcje.
- Ochrona sieci i systemów informatycznych przed cyberzagrożeniami.
- **Stosowanie unijnych przepisów o ochronie danych osobowych** – zwłaszcza w świetle rosnącego wpływu mikrotargetingu wyborców w oparciu o dane osobowe.
- **Zaostrzenie przepisów finansowania europejskich partii politycznych** – umożliwienie nakładania kar za naruszenie przepisów ochrony danych osobowych w celu świadomego wpływania na wyniki wyborów europejskich. Kary wynosiłyby 5 proc. rocznego budżetu danej europejskiej partii politycznej lub fundacji.
- Utworzenie sieci ośrodków kompetencji w dziedzinie cyberbezpieczeństwa.

Plan Działania Przeciwko Dezinformacji (*Action Plan Against Disinformation*)

5 grudnia 2018 roku ogłoszono Plan działania przeciwko dezinformacji. Komisja Europejska wskazuje w nim kroki, które powinny zostać zrealizowane przez unijne instytucje oraz państwa członkowskie przed wyborami do Parlamentu Europejskiego w 2019 r. Wśród najważniejszych zadań zawartych w planie wymienić można:

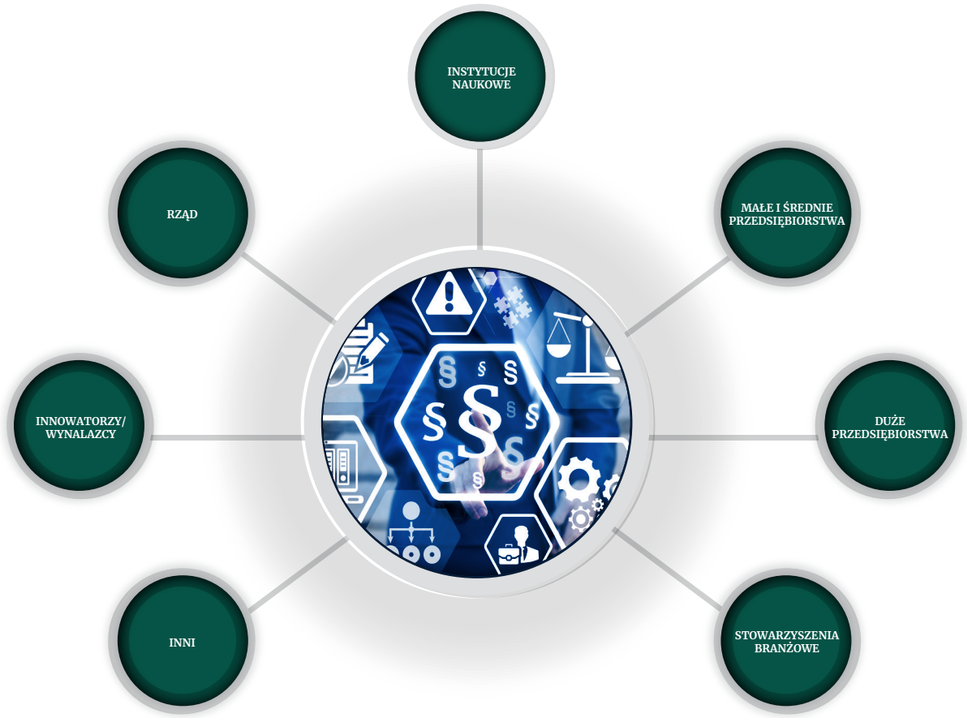
- **Wzmocnienie zespołów zadaniowych ds. komunikacji strategicznej** poprzez dodatkowy personel i niezbędne narzędzia (**zwiększenie budżetu na komunikację strategiczną z 1,9 mln euro w 2018 do 5 mln euro w 2019 roku**).
- Ustanowienie do marca 2019 r. **systemu szybkiego ostrzegania** (*Rapid Alert System*) przed kampaniami dezinformacyjnymi.
- Realizacja zapisów **kodeksu postępowania w zakresie zwalczania dezinformacji**.
- Wsparcie w **tworzeniu interdyscyplinarnych i niezależnych zespołów**, składających się z badaczy oraz specjalistów sprawdzających fakty.
- Zapewnienie skutecznego wdrażania rekomendacji pakietu wyborczego.

Digital Innovation Hubs – nowa koncepcja współpracy międzysektorowej

Digital Innovation Hub (DIH), czyli Huby Innowacji Cyfrowej to koncepcja KE, która powstawała w kilku etapach. Pierwszym była koncepcja Centrów Kompetencji (*Competence Centers*), które miały wytwarzać konkretną technologię tak, aby wspierać transformację cyfrową w Europie. Następnie, w drodze analiz, wypracowano koncepcję Hubów Innowacji Cyfrowej, które poza wytwarzaniem konkretnych produktów, mają za zadanie budować ekosystem cyfrowej innowacji poprzez jednoczenie różnych środowisk i sektorów, wymianę wiedzy, doświadczeń i technologii. W założeniach KE DIH ma pełnić następujące role:

- *one-stop-shop*: pomoc dla firm i doradztwo w zakresie procesów biznesowych, produkcyjnego zastosowania technologii cyfrowych itp.;
- centrum kompetencyjne, które działa jako pośrednik pomiędzy firmami a inwestorami oraz dostarcza firmom w regionie wiedzę, ekspertyzy i technologie;
- punkt kontaktowy w państwie, który wzmacnia innowacyjność i tworzy płaszczyznę do współpracy dla różnych interesariuszy[62].

Koncepcję DIH przedstawia poniższy schemat:



Rys. 4. Koncepcja Hubu Cyfrowej Innowacji

W 2017 roku KE prowadziła pilotaż, którego celem było przygotowanie kadr do budowy DIH w państwach Europy Środkowo-Wschodniej. W 2018 roku wciąż dyskutowano na temat tej koncepcji. Ustalono, że to państwa członkowskie będą zgłaszać DIH do KE (do tej pory można było aplikować samodzielnie, wypełniając ankietę na stronie KE). Komisja zakłada także, że DIH staną się głównymi ośrodkami dla rozwoju sztucznej inteligencji w Europie.

[62] https://ec.europa.eu/digital-single-market/en/digital-innovation-hubs

NASK Cyber POLICY

ONZ – brak konsensusu wobec implementacji prawa międzynarodowego w cyberprzestrzeni

Organizacja Narodów Zjednoczonych (ONZ) jest największą organizacją międzynarodową, obecnie zrzeszającą 193 państwa. Powołana w 1945 roku, działa na rzecz pokoju i bezpieczeństwa międzynarodowego. ONZ podejmuje problemy, przed którymi staje ludzkość w XXI wieku: zmiany klimatyczne, zrównoważony rozwój, prawa człowieka, terroryzm, pomoc humanitarna, zagrożenia zdrowia, równość płci, produkcja żywności, praworządność i wiele innych[63]. ONZ stanowi również płaszczyznę dialogu, umożliwiającą rządom znajdowanie obszarów porozumienia i współpracy. Organizacja składa się ze Zgromadzenia Ogólnego, Rady Bezpieczeństwa, Rady Gospodarczej i Społecznej, Rady Powierniczej, Międzynarodowego Trybunału Sprawiedliwości, a także innych organizacji, komitetów i grup powołanych w ramach ONZ.

Po raz pierwszy tematykę cyberbezpieczeństwa ONZ podjęła w 1990 roku, kiedy to wydano Rezolucję Zgromadzenia Ogólnego ONZ nr 45/121[64] dotyczącą przestępstw związanych z wykorzystaniem komputerów. Rezolucja podkreślała konieczność wprowadzenia przestępstw komputerowych do porządków legislacyjnych państw i była podstawą do wydania w 1994 roku poradnika International review of criminal policy – *United Nations Manual on the prevention and control of computer – related crime*, dotyczącego zapobiegania i kontroli cyberprzestępstw[65]. Od 1998 r. cyberbezpieczeństwo stało się stałym punktem obrad Walnego Zgromadzenia ONZ, a także tematem kilkunastu rezolucji wydanych nie tylko przez Walne Zgromadzenie, ale również organizacje działające w ramach ONZ, w szczególności Międzynarodowy Związek Telekomunikacyjny (*International Telecommunication Union* – ITU).

Rezolucje Walnego Zgromadzenia i Rady Gospodarczej i Społecznej ONZ:

- Rezolucja 55/63, styczeń 2001 – zawiera zapis, że państwa nie powinny udzielać schronienia przestępcom wykorzystującym technologie informacyjne
- Rezolucja 56/121, styczeń 2002 – dotyczy zwalczania przestępczego nadużycia technologii informacyjnych
- Rezolucja 57/239, styczeń 2003 – dotyczy globalnej kultury cyberbezpieczeństwa
- Rezolucja 58/32, grudzień 2003 – dotyczy rozwoju informatyzacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego
- Rezolucja 58/199, styczeń 2004 – dotyczy globalnej kultury cyberbezpieczeństwa i ochrony informacyjnej infrastruktury krytycznej
- Rezolucja 64/211, marzec 2010 – podsumowanie działań państw członkowskich na rzecz ochrony informacyjnej infrastruktury krytycznej
- Rezolucja Rady Gospodarczej i Społecznej ONZ 2011/33, lipiec 2011 – współpraca międzynarodowa na rzecz zapobiegania wykorzystywaniu dzieci z użyciem nowych technologii informatycznych

Rezolucje Międzynarodowego Związku Telekomunikacyjnego:

- Rezolucja 181, Guadalajara 2010 – terminologia dotycząca budowania zaufania i bezpieczeństwa w korzystaniu z technologii ICT
- Rezolucja 58, Dubai 2012 – zawierająca zachętę do tworzenia krajowych zespołów reagowania na incydenty komputerowe, szczególnie w krajach rozwijających się
- Rezolucja 45, Dubai 2014 – mechanizmy wzmacniania współpracy w zakresie cyberbezpieczeństwa, w tym przeciwdziałania i zwalczania spamu
- Rezolucja 130, Busan 2014 – wzmocnienie roli ITU w budowaniu zaufania i bezpieczeństwa w korzystaniu z technologii informacyjnych i komunikacyjnych
- Rezolucja 174, Busan 2014 – rola ITU w odniesieniu do międzynarodowych zagadnień polityki publicznej związanych z ryzykiem nielegalnego wykorzystania technologii informacyjnych i komunikacyjnych
- Rezolucja 179, Busan 2014 – rola ITU w ochronie dzieci w Internecie
- Rezolucja 50, Hammamet 2016 – dotycząca cyberbezpieczeństwa
- Rezolucja 52, Hammamet 2016 – dotycząca zwalczania spamu
- Rezolucja 67, Buenos Aires 2017 – rola sektora teleinformatycznego ITU w ochronie dzieci w Internecie
- Rezolucja 69, Buenos Aires 2017 – tworzenie krajowych zespołów reagowania na incydenty komputerowe, w szczególności w krajach rozwijających się

[63] Cele Organizacji Narodów Zjednoczonych zostały zapisane w art. 1 Karty Narodów Zjednoczonych. Treść Karty Narodów Zjednoczonych w języku polskim jest dostępna na stronie Ośrodka Informacji ONZ w Warszawie, pod adresem: http://www.unic.un.org.pl/dokumenty/karta_onz.php

[64] Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (A/45/756) http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/45/121

[65] UN. Centre for Social Development and Humanitarian Affairs; "International review of criminal policy". Nr 43-44, 1994; https://digitallibrary.un.org/record/162804

Grupa UN GGE – na ile prawo międzynarodowe ma zastosowanie w cyberprzestrzeni?

Najważniejsze traktaty z zakresu prawa międzynarodowego zostały przyjęte, kiedy Internet jeszcze nie funkcjonował. W związku z tym jednym z większych wyzwań w zakresie stosunków międzynarodowych jest stosowanie istniejącego prawa międzynarodowego w cyberprzestrzeni. W 2003 r. Walne Zgromadzenie ONZ zwróciło się do Sekretarza Generalnego z prośbą o analizę potencjalnych zagrożeń bezpieczeństwa informacji, a także publikację ewentualnych środków prewencji i możliwości współpracy, które pomogłyby zminimalizować te zagrożenia. Powołana została **Grupa ekspertów rządowych ds. rozwoju w dziedzinie informacji i telekomunikacji w kontekście bezpieczeństwa międzynarodowego** (*Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* – **UN GGE**). W latach 2003-2017 obradowało pięć grup GGE[67].

- Pierwsza grupa została zwołana w 2004 roku. Jej obrady zakończyły się fiaskiem i zamiast raportu, grupa opracowała jedynie krótkie sprawozdanie dotyczące kwestii proceduralnych.
- Kolejna grupa rozpoczęła pracę w 2009 roku. W wyniku jej prac powstał raport, który wzywał do współpracy między państwami, sektorem publicznym i prywatnym w celu zwiększenia cyberbezpieczeństwa. Raport zawierał również zalecenia z zakresu analizy ryzyka, wymiany informacji i najlepszych praktyk, takie jak dalszy dialog między państwami w celu obniżenia ryzyka cyberzagrożeń i ochrony infrastruktury krytycznej, budowa wzajemnego zaufania, stabilizacja i obniżenie ryzyka wynikającego z wykorzystywania przez państwa technologii ICT, również w kontekście konfliktów międzynarodowych[68].
- W latach 2012-2013 obradowała trzecia grupa GGE, a opublikowany raport przedstawiał znacznie dalej idące wnioski, niż poprzednie dokumenty. Eksperci podkreślili fakt, że **prawo międzynarodowe ma zastosowanie w cyberprzestrzeni. Działalność państw w Internecie**, również działalność infrastruktury informacyjno-komunikacyjnej, zlokalizowanej na terytorium danego państwa, **podlega zarówno Karcie Narodów Zjednoczonych[69], normom i zobowiązaniom dotyczącym suwerenności państwowej, jak i pozostałym przepisom prawa.** Oznacza to m.in., że ani państwa członkowskie, ani podmioty przez nie nadzorowane, **nie mogą wykorzystywać serwerów pośredniczących, tzw. serwerów proxy, w celach bezprawnych działań w cyberprzestrzeni.** Nie wolno również wspierać innych podmiotów dokonujących takich działań na ich terytorium.

Główne tezy raportu końcowego z 2013 roku

Zalecenia dotyczące norm i zasad postępowania państw:

- konieczność stosowania norm obowiązującego prawa międzynarodowego w cyberprzestrzeni, w tym Karty Narodów Zjednoczonych,
- przyjęcie międzynarodowego kodeksu postępowania w zakresie bezpieczeństwa informacji,
- poszanowanie praw człowieka i podstawowych wolności zawartych w prawie międzynarodowym przy podejmowaniu działań związanych z cyberbezpieczeństwem,

[67] Za każdym razem powoływano inny skład grupy. Pierwsza grupa, powołana w 2004 roku, liczyła 15 osób, kolejna, obradująca w 2009 roku, również 15 osób. W 2014 roku do grupy powołano już 20 ekspertów pod przewodnictwem przedstawiciela z Brazylii, w 2016 roku liczba ekspertów wzrosła do 25 osób; United Nations Groups of Governmental Experts, https://www.nti.org/learn/treaties-and-regimes/united-nations-groups-governmental-experts/#communications; Developments in the field of information and telecommunications in the context of international security, https://www.un.org/disarmament/topics/informationsecurity/

[68] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security; http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf

[69] Karta Narodów Zjednoczonych jest dokumentem powołującym do życia ONZ. Karta została podpisana 26 czerwca 1945 r. w San Francisco przez 50 krajów członkowskich, w tym 5 krajów założycielskich: Chiny, Francję, Stany Zjednoczone, Wielką Brytanię, ZSRR. W karcie zawarto wezwanie do przestrzegania, poszanowania i popierania praw człowieka, a także podkreślono wartość i godność jednostki. Zaznaczono również konieczność dbania o postęp społeczny i poprawę warunków życia wszystkich ludzi. Kraje, które podpisały kartę, zobowiązały się do przestrzegania jej postanowień. (źródło: Charter of the United Nations; United Nations portal; http://www.un.org/en/charter-united-nations/index.html)

- zintensyfikowanie prac przeciwko działalności przestępczej w cyberprzestrzeni,
- zakaz wykorzystywania serwerów proxy w celach bezprawnych działań w cyberprzestrzeni,
- włączenie społeczeństwa i sektora prywatnego w działania na rzecz zwiększenia poziomu cyberbezpieczeństwa.

- **W latach 2014-2015 powołano czwartą grupę GGE**. Opublikowany raport opierał się w dużej mierze na zaleceniach poprzednich grup, promujących otwartą i bezpieczną cyberprzestrzeń. Przede wszystkim podkreślono konieczność dalszej budowy bezpieczeństwa międzynarodowego w oparciu o nowoczesne technologie, zaangażowania sektora nauki i biznesu w działania zapewniające cyberbezpieczeństwo, a także potrzebę włączenia środowisk badawczych w analizy związane z rozwojem ICT. Walne Zgromadzenie przyjęło sprawozdanie w grudniu 2015 roku i wezwało państwa członkowskie do jego przestrzegania[70].
- **Ostatnia grupa UN GGE obradowała w latach 2016-2017**. Obrady 25 ekspertów pod przewodnictwem przedstawicieli z Niemiec odbyły się w czerwcu 2017 roku. Spotkanie zakończyło się brakiem konsensusu. Główne nieporozumienie pojawiło się w dialogu przedstawiciela Stanów Zjednoczonych i Kuby. Stany Zjednoczone oczekiwały od grupy wypracowania jasnych i konkretnych wytycznych stosowania prawa międzynarodowego w nowoczesnych technologiach, w tym prawa humanitarnego, prawa do samoobrony, a także prawa odpowiedzialności państwa i środków zaradczych. Aktualnie, zgodnie z prawem międzynarodowym, państwa mogą legalnie używać siły w ramach samoobrony w odpowiedzi na poważny atak zbrojny i proporcjonalnie do poniesionej szkody. Podobnie w przypadku prawa humanitarnego, które opiera się na rozróżnieniu między cywilami, a wojskowymi. W przypadku cyberataków niezwykle trudne jest wytypowanie pojedynczego sprawcy, poszkodowanych, cywilów i wojskowych. Zdaniem przedstawicieli Kuby, a nieoficjalnie wiadomo również, że podobne stanowisko zajęły Rosja i Chiny, zastosowanie tych przepisów w cyberprzestrzeni mogłoby prowadzić do jej militaryzacji. W czasie pracy grupy nie udało się wypracować stanowiska. Dotychczas ONZ nie wezwało do kontynuacji prac grupy[71].

Działania Międzynarodowego Związku Telekomunikacyjnego w zakresie Cyberbezpieczeństwa

Międzynarodowy Związek Telekomunikacyjny (*International Telecommunication Union – ITU*) jest jedną z wyspecjalizowanych organizacji ONZ, koncentrującą swoją działalność w obszarze technologii informacyjnych i komunikacyjnych. ITU, jako jedyna organizacja ONZ, zrzesza zarówno przedstawicieli sektora publicznego, jak i prywatnego. Członkami są 193 państwa członkowskie, organy regulacyjne, instytucje akademickie i ok. 700 firm z całego świata[72].

Przewodnik po opracowaniu Krajowej Strategii Cyberbezpieczeństwa

W 2018 roku ITU opublikowało „Przewodnik po opracowaniu Krajowej Strategii Cyberbezpieczeństwa" (*Guide to developing a national cybersecurity strategy*[73]). Dokument ma stanowić wsparcie dla państw, które przygotowują strategię. Opisano w nim poszczególne etapy, od identyfikacji potrzeb, poprzez analizy, opracowanie dokumentu, wdrożenie, aż do ewaluacji. Dodatkowo w przewodniku znajdują się przykłady dobrych praktyk w zakresie zarządzania, oceny ryzyka, infrastruktury krytycznej, rozwiązań prawnych i edukacyjnych. Dokument powstał przy wsparciu przedstawicieli organizacji międzynarodowych, sektora prywatnego, reprezentantów świata nauki, we współpracy z NATO, a także Europejską Agencją Bezpieczeństwa Sieci i Informacji (ENISA[74]). Etapy przygotowania strategii przedstawia poniższy rysunek.

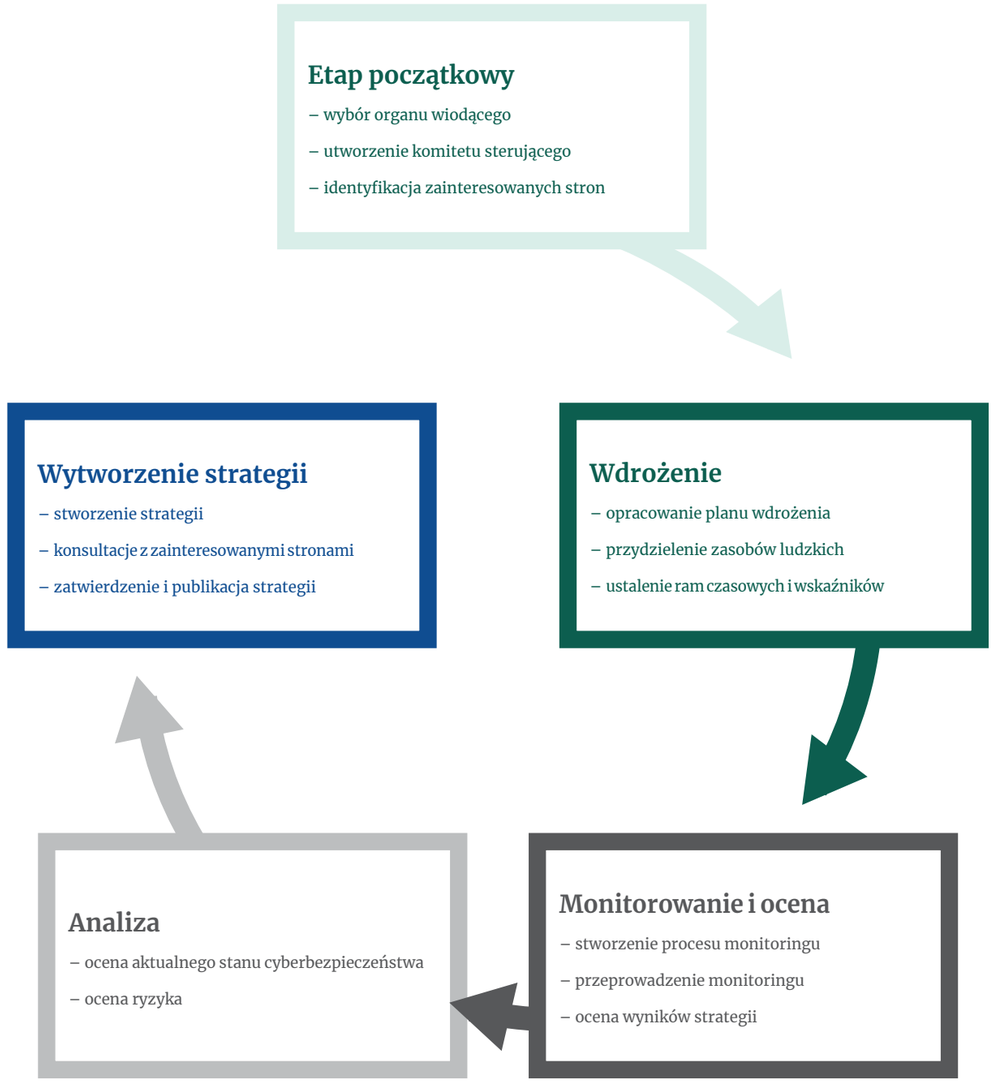
[70] James Martin Center for Nonproliferation Studies at the Middlebury Institute of International Studies at Monterey, "Developments in the Field of Information and Telecommunications in the Context of International Security"; https://www.nti.org/learn/treaties-and-regimes/united-nations-groups-governmental-experts/#communications)

[71] Korzak E., UN GGE on Cybersecurity: The End of an Era?, The Debate; https://thediplomat.com/2017/07/un-gge-on-cybersecurity-have-china-and-russia-just-made-cyberspace-less-safe/

[72] Więcej informacji na temat Międzynarodowego Związku Telekomunikacyjnego jest dostępnych na stronie internetowej: https://www.itu.int

[73] "Guide to developing a national cybersecurity strategy", International Telecommunication Union (ITU) 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

[74] We wrześniu 2018 r. ENISA przygotowała również narzędzie do ewaluacji krajowych strategii cyberbezpieczeństwa państw członkowskich, które składa się z prostych pytań umożliwiających ocenę kolejnych kroków wdrażania strategii, a także pomaga ustalić priorytety na przyszłość. To również wsparcie w realizacji założeń dyrektywy NIS. Wraz z publikacją narzędzia, ENISA zaktualizowała interaktywną mapę strategii krajowych. Źródło: ENISA launches the Cybersecurity Strategies Evaluation Tool; https://www.enisa.europa.eu/news/enisa-news/enisa-launches-the-cybersecurity-strategies-evaluation-tool



Rys. 5. Etapy przygotowania Krajowej Strategii Cyberbezpieczeństwa wg Przewodnika[75]

[75] "Guide to developing a national cybersecurity strategy", International Telecommunication Union (ITU) 2018, s. 17; https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Zasady wspierające przygotowanie krajowej strategii cyberbezpieczeństwa:

1. Określenie wizji

Strategia powinna wyznaczać jasną i spójną wizję społeczeństwa oraz zarządzania tym społeczeństwem. Im bardziej konkretna wizja, tym łatwiej wdrożyć strategię i koordynować współpracę zainteresowanych stron. Cele powinny być sformułowane tak, aby uwzględniały dynamikę rozwoju środowiska cyfrowego.

2. Kompleksowe podejście i odpowiednie priorytety

Cyberbezpieczeństwo jest zagadnieniem złożonym, dlatego ważne, aby zrozumieć wszystkie jego aspekty, wraz z warunkami danego kraju. W oparciu o analizę należy ustalić priorytety i cele strategii, a także harmonogram i zasoby niezbędne do jej wdrożenia. Priorytety strategii będą różne w zależności od kraju.

3. Włączenie wszystkich interesariuszy

Strategia powinna być rozwijana przy udziale zainteresowanych stron i z uwzględnieniem ich potrzeb. Cyberbezpieczeństwo jest tematem ważnym nie tylko dla administracji państwowej, ale również dla sektora prywatnego i obywateli. Dlatego też strategia powinna być wypracowywana we współpracy ze wszystkimi interesariuszami.

4. Uwzględnienie aspektów ekonomicznych i społecznych

Strategia powinna sprzyjać dobrobytowi gospodarczemu i społecznemu, maksymalizować wpływ technologii ICT na zrównoważony rozwój i integrację społeczną, a także prowadzić do budowy zaufania niezbędnego dla ochrony kraju przed zagrożeniami.

5. Uwzględnienie praw człowieka

Strategia powinna uwzględniać prawa człowieka, które są zawarte w Powszechnej Deklaracji Praw Człowieka[76], Międzynarodowym Pakcie Praw Obywatelskich i Politycznych[77] oraz innych ramach prawnych. Prawa człowieka w sferze offline powinny być respektowane także online.

6. Sformułowanie podejścia do zarządzania ryzykiem i odporności na incydenty

Wraz z rozwojem nowoczesnych technologii rośnie prawdopodobieństwo wystąpienia incydentów cyberbezpieczeństwa. Tego ryzyka nie można wyeliminować całkowicie, jednak można nim skutecznie zarządzać. Strategia powinna zachęcać do podejmowania działań, które minimalizują ryzyko, a także proponować plany naprawcze w przypadku wystąpienia incydentu.

7. Odpowiednie wykorzystanie instrumentów politycznych

Strategia powinna wykorzystywać dostępne instrumenty polityczne. Obejmują one prawodawstwo, regulacje, programy i mechanizmy zachęcające, programy edukacyjne, dzielenie się najlepszymi praktykami itp. Każdy z celów powinien mieć przyporządkowany najbardziej odpowiedni instrument polityczny, jednocześnie uwzględniający specyfikę i uwarunkowania danego kraju.

8. Jasne określenie przywództwa i podział ról

Strategia powinna być implementowana na poziomie rządowym, wraz z odpowiednim podziałem ról i obowiązków oraz z uwzględnieniem potrzeb kadrowo-finansowych. Ważne, aby wszystkie zaangażowane strony rozumiały swoje zadania i obowiązki. Należy także zapewnić rozliczalność strategii, a do każdego etapu przypisać odpowiednie zasoby.

9. Budowa zaufania

Zaufanie jest niezbędne, aby w pełni wykorzystać potencjał społecznych, politycznych i gospodarczych możliwości rozwoju nowoczesnych technologii. Strategia powinna zapewniać ochronę interesów każdej ze stron, a także bezpieczeństwo danych, systemów i świadczonych usług. Ważne, aby budowa wzajemnego zaufania nie była priorytetem jedynie dla państwa, ale także dla sektora prywatnego, organizacji pozarządowych i obywateli[78].

[76] Powszechna Deklaracja Praw Człowieka została uchwalona przez Trzecią Sesję Ogólnego Zgromadzenia ONZ w 1948 r. W deklaracji zawarto zbiór praw człowieka i zasad ich stosowania. Dokument stanowi jedno z największych osiągnięć ONZ. Źródło: Powszechna Deklaracja Praw Człowieka; http://www.unesco.pl/fileadmin/user_upload/pdf/Powszechna_Deklaracja_Praw_Czlowieka.pdf

[77] Międzynarodowy Pakt Praw Obywatelskich i Politycznych został uchwalony przez ONZ w 1966 r. W przeciwieństwie do Powszechnej Deklaracji Praw Człowieka, pakt posiada wiążący charakter prawny. Zawiera spis podstawowych praw i wolności człowieka, a także zobowiązania państwa w stosunku do obywateli. Powołuje do życia Komitet Praw Człowieka, który dba o przestrzeganie paktu. W tym samym roku ONZ uchwaliło także Międzynarodowy Pakt Praw Gospodarczych, Społecznych i Kulturalnych. Źródło: International Covenant on Civil and Political Rights (ICCPR); Information Platform humanrights.ch; https://www.humanrights.ch/en/standards/un-treaties/iccpr/

[78] "Guide to developing a national cybersecurity strategy", International Telecommunication Union (ITU) 2018, s. 30-34; https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-E.pdf

Sieć Zespołów Reagowania na Incydenty

ITU wspiera państwa członkowskie w tworzeniu krajowych zespołów reagowania na incydenty komputerowe (*National Computer Incident Response Teams* – CIRT[79]), których główną rolą jest koordynowanie obsługi cyberataków. W pierwszej kolejności przeprowadzana jest ocena gotowości państwa do wdrożenia krajowego CIRT. Kolejnymi krokami są pomoc w szkoleniu, planowaniu, wdrożeniu i działaniu zespołu. Po powołaniu CIRT, ITU oferuje wsparcie i możliwość dalszego rozwoju. Dotychczas udało się ocenić 75 krajów, a także stworzyć 18 zespołów CIRT, m.in. w Ugandzie, Zambii, Ghanie, Kenii, Cyprze.

Globalny wskaźnik cyberbezpieczeństwa (*Global Cybersecurity Index* – GCI)

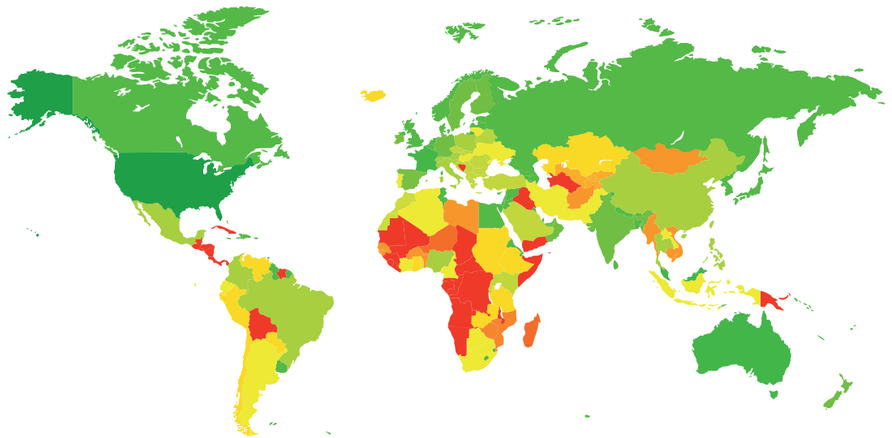
Globalny wskaźnik cyberbezpieczeństwa to inicjatywa ITU, która ma zwiększyć świadomość na temat cyberbezpieczeństwa. Wskaźnik mierzy zaangażowanie państwa i jego zdolność utrzymania bezpieczeństwa na poziomach krajowym, regionalnym i międzynarodowym. Ocena, prowadzona przez ekspertów ITU wraz z partnerami z sektora prywatnego, publicznego i naukowego, ma zidentyfikować aktualne problemy, wykryć luki i wskazać obszary do pracy[80]. Tworzony ranking ma również funkcję motywacyjną – ma zachęcać państwa do poprawy wyniku. W zestawieniu uwzględniono różne poziomy rozwoju cyberbezpieczeństwa, odzwierciedlone w ogólnym poziomie usług ICT. Koncepcja opiera się na założeniu, że im bardziej rozwinięte rozwiązania cyberbezpieczeństwa, tym wyższy poziom usług ICT.

Wskaźnik GCI mierzy przede wszystkim:

- Poziom zaangażowania w rozwój cyberbezpieczeństwa oraz jego wzrost w czasie;
- Postęp w zakresie cyberbezpieczeństwa w perspektywie globalnej;
- Postęp w perspektywie regionalnej;
- Zaangażowanie w inicjatywy i programy związane z cyberbezpieczeństwem.

W związku z uzyskanym wynikiem, państwa podzielono na 3 grupy, adekwatnie do poziomu zaangażowania w cyberbezpieczeństwo. Wyniki obrazuje mapa, na której kolorami zaznaczono poziom zaangażowania od najwyższego (zielony) do najniższego (czerwony).

Po raz pierwszy inicjatywa **Globalnego wskaźnika cyberbezpieczeństwa** została uruchomiona w 2013 roku. Po publikacji raportu w 2014 roku i zebraniu informacji zwrotnej, zaplanowano drugą edycję. Tym razem zaangażowano więcej partnerów (m.in. Bank Światowy, FIRST, INTERPPOL, UNICRI, UNODC itp.) i opracowano nowy model analizy danych, który zawierał 25 wskaźników, mierzonych na podstawie 157 pytań, badających poziom zaangażowania państw w odniesieniu do 5 filarów cyberbezpieczeństwa: środki prawne, środki techniczne, działania organizacyjne, budowanie zdolności, współpraca.



Rys. 6. Wskaźnik GCI na świecie (dane z grudnia 2018 roku)[81]

W 2018 po raz trzeci przeprowadzono analizę państw, zgodnie ze wskaźnikiem GCI[82]. Raport i najnowszy ranking zostaną opublikowane w 2019 roku.

[79] W zależności od instytucji stosuje się nazwę National Computer Incident Respone Teams – CIRT, Computer Emergency Response Team – CERT, albo Computer Security Incident Response Team – CSIRT.

[80] Global Cybersecurity Index (GCI) 2017; ITU, s. 13; https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

[81] Źródło: Global Cybersecurity Index (GCI) 2017; Figure 4.1.1: GCI Heat Map; ITU, s. 25, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

Działania Biura Narodów Zjednoczonych do spraw Narkotyków i Przestępczości w zakresie Cyberbezpieczeństwa (UNODC)

Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości (*United Nations Office on Drugs and Crime* – UNODC) zostało utworzone w 1997 r. UNODC działa na rzecz współpracy państw członkowskich w zwalczaniu przestępczości międzynarodowej, prowadzi prace badawcze i analityczne, wspiera wdrażanie traktatów międzynarodowych i lokalnego ustawodawstwa w zakresie zwalczania przestępczości.

UNODC zajmuje się również cyberprzestępczością, która może mieć charakter międzynarodowy albo dotyczyć ofiar w różnych częściach świata. Biuro promuje współpracę między państwami członkowskimi, a także wspiera budowę krajowych struktur i zdolności państw do zwalczania cyberprzestępczości. W szczególności wykorzystuje wiedzę ekspercką z systemów sądownictwa, wiedzę technologiczną, a także zdolności w zakresie edukacji, gromadzenia danych, prowadzenia badań i analiz[83].

UNODC prowadzi następujące inicjatywy, wspierające państwa w walce z cyberprzestępczością:

- **Globalny program dotyczący cyberprzestępczości** (*Global Programme on Cybercrime*) – program pomaga zapobiegać i zwalczać cyberprzestępczość poprzez zwiększanie skuteczności ścigania, koordynację krajowych służb, tworzenie ram prawnych, rozwój współpracy międzynarodowej i zwiększanie świadomości społecznej.
- **Grupa ekspertów ds. cyberprzestępczości** (*Open-ended Intergovernmental Expert Group Meeting on Cybercrime*) – grupa powołana do kompleksowego zbadania problemu cyberprzestępczości, zebrania danych na temat ustawodawstwa krajowego, dobrych praktyk, potrzebnej pomocy technicznej, a także zidentyfikowania obszarów wymagających wzmocnienia w zakresie działań lokalnych i międzynarodowych.
- **Repozytorium Cyberprzestępczości (***Repository Cybercrime*) – centralna baza przepisów prawa i zebranych doświadczeń dotyczących cyberprzestępczości[84].

Forum Zarządzania Internetem (IGF)

Forum Zarządzania Internetem (*Internet Governance Forum* – IGF) zostało powołane w 2006 roku. Jest miejscem dialogu na temat rozwoju sieci i platformą wymiany wiedzy[85]. Spotkania IGF organizowane są co roku i biorą w nich udział wszyscy członkowie WSIS (*World Summit on Information Society*). Do współpracy zapraszane są również organizacje i eksperci z różnych środowisk. Ważną częścią dyskusji na forum jest cyberbezpieczeństwo. Ostatnie spotkanie odbyło się w listopadzie 2018 r. w Paryżu.

Do 1998 roku Internetem zarządzała Agencja Zaawansowanych Projektów Badawczych przy Departamencie Obrony Stanów Zjednoczonych. Wiadomo było jednak, że należy uniezależnić Internet od rządowej agencji USA. Dlatego też powołano Internetową Korporację ds. Nadanych Nazw i Numerów (*Internet Corporation for Assigned Names and Numbers* – ICANN), która była odpowiedzialna za nadawanie i administrowanie adresami IP, a także za zarządzanie domenami i serwerami DNS. ICANN powołano na podstawie *Memorandum of Understanding*, zgodnie z którym korporacja stała się organizacją pozarządową, działającą na podstawie prawa stanu Kalifornia.

Zgodnie z założeniami powołanie ICANN miało być krokiem na drodze prywatyzacji zarządzania Internetem. Jednak zniesienie rządowych wpływów USA nigdy nie zostało w pełni osiągnięte. Międzynarodowy sprzeciw po raz pierwszy miał miejsce podczas Światowego Szczytu Społeczeństwa Informacyjnego, który odbył się w 2003 roku w Genewie i w 2005 roku w Tunisie. Przedstawiciele państw opowiedzieli się przeciwko amerykańskiej dominacji nad Internetem. Żądano, aby nadzór został przekazany w ręce organu reprezentującego interesy wszystkich, działającego pod egidą ONZ.

[82] Global Cybersecurity Index; https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx, Global Cybersecurity Index (GCI) 2017; ITU, s. 15-16; https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

[83] Cybercrime, http://www.unodc.org/unodc/en/cybercrime/index.html

[84] Repozytorium jest dostępne na stronie internetowej: https://sherloc.unodc.org/cld/v3/cybrepo/

[85] The Internet Governance Forum (IGF), Back ground paper, http://www.intgovforum.org/cms/2015/IGF.24.06.2015.pdf

W duchu kompromisu powołano Forum Zarządzania Internetem, które pełni rolę pomocniczą, jednak jest pozbawione uprawnień decyzyjnych. Ostatecznie ICANN pozostał organizacją non-profit, działającą na terenie USA i podlegającą tamtejszemu prawu[86]. Nadal jest instytucją nadzorującą światowe serwery DNS i domeny internetowe, część swoich obowiązków deleguje krajowym rejestratorom.

W ramach ICANN działa IANA (*Internet Assigned Numbers Authority*), która jest odpowiedzialna za koordynację sprawnego działania Internetu poprzez zarządzanie domenami, administrację globalnej puli adresów IP, a także utrzymywanie systemów numerowania protokołów internetowych. IANA nie angażuje się w politykę, a jedynie wdraża rozwiązania, nad którymi pieczę sprawuje ICANN[87].

Najważniejszym ciałem decyzyjnym ICANN jest Rada Dyrektorów, którą wybierają co roku wszyscy użytkownicy Internetu w dobrowolnym głosowaniu. Zgodnie z zasadami ICANN, każdy użytkownik może włączyć się w działalność organizacji i wyrazić swoją opinię[88].

W czasie forum, prezydent Francji Emmanuel Macron wezwał do wspólnego zaangażowania w bezpieczeństwo cyberprzestrzeni. Deklarację nazwaną ***Paris Call for Trust and Security in Cyberspace*** podpisały 64 państwa, 328 podmiotów sektora prywatnego i 129 organizacji pozarządowych. Wśród zobowiązań znalazły się m.in.:

- Zapobieganie szkodliwym działaniom online;
- Ochrona integralności Internetu;
- Współpraca w celu zapobiegania ingerencji w procesy wyborcze;
- Zapobieganie rozprzestrzenianiu się złośliwych programów i technologii;
- Poprawa cyberbezpieczeństwa produktów i usług, wzrost poziomu cyberhigieny;
- Współpraca w celu wzmocnienia międzynarodowych standardów w cyberprzestrzeni, a także ograniczenia ofensywnej działalności podmiotów niepaństwowych[89].

Panel Wysokiego Szczebla ds. Współpracy Cyfrowej

12 lipca 2018 roku Sekretarz Generalny ONZ powołał Panel Wysokiego Szczebla ds. Współpracy Cyfrowej (*Secretary-General's High-level Panel on Digital Cooperation*). Celem jest opracowanie propozycji wzmocnienia współpracy między rządami, sektorem prywatnym, społeczeństwem obywatelskim, organizacjami międzynarodowymi, środowiskiem akademickim i technicznym. Zadania panelu to m.in. podniesienie świadomości na temat transformacji cyfrowej w gospodarce, a także rozpoczęcie debaty nad kwestiami etycznymi oraz zmianami, jakie będą zachodzić w społeczeństwach w cyfrowej przyszłości.

Panel tworzy 20 niezależnych ekspertów z różnych środowisk, którzy działają we własnym imieniu. **Członkowie panelu po raz pierwszy spotkali się we wrześniu 2018 roku.** Wynikiem prac panelu ma być raport, zawierający praktyczne rekomendacje, analizę aktualnych trendów w technologiach cyfrowych, a także identyfikację luk i możliwości wzmocnienia współpracy międzynarodowej. Przewidywany czas pracy ekspertów to 9 miesięcy, co oznacza, że raport powinien zostać opublikowany w pierwszej połowie 2019 roku[90].

Portal ekspercki z zakresu *policy*

W grudniu 2018 roku UNIDIR[91] (*United Nations Institute for Disarmament Research*) uruchomił nowy portal internetowy, zawierający przegląd wiedzy z zakresu *policy* w tematyce cyberbezpieczeństwa. Portal gromadzi informacje dotyczące strategii cyberbezpieczeństwa wszystkich 193 państw członkowskich ONZ, organizacji międzynarodowych i regionalnych, a także dobrowolnie przekazane dane oraz dane z otwartych źródeł. Adres portalu: https://cyberpolicyportal.org/en/

[86] Morawski Ł., Unia Europejska wobec procesu zarządzania Internetem, Instytut Studiów Politycznych Polskiej Akademii Nauk, s. 114–120,

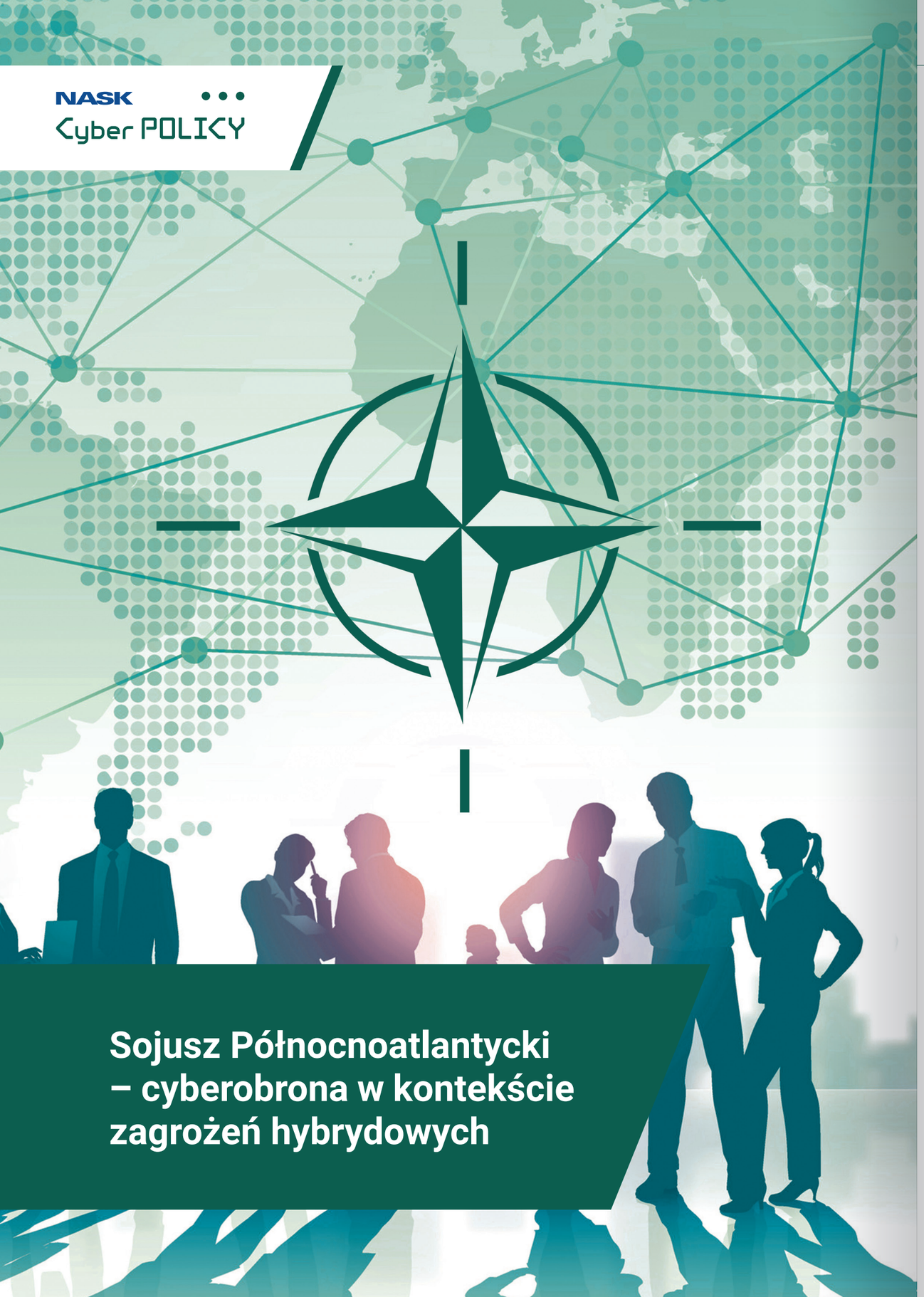
[87] IANA About us; https://www.iana.org/about

[88] Beginner's Guide to participating in ICANN; s. 2, https://www.icann.org/en/system/files/files/participating-08nov13-en.pdf

[89] Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace. France Diplomatie ; https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in

[90] Secretary-General's High-level Panel on Digital Cooperation; http://www.un.org/en/digital-cooperation-panel/

[91] United Nations Institute for Disarmament Research (UNIDIR) działa od 1980 r. Jest to Instytut Badań nad Rozbrojeniem ONZ, który prowadzi niezależne badania nad rozbrojeniem i pokrewnymi problemami, w szczególności kwestiami bezpieczeństwa międzynarodowego; http://www.unidir.org/about/the-institute



Sojusz Północnoatlantycki – cyberobrona w kontekście zagrożeń hybrydowych

Sojusz Północnoatlantycki (*North Atlantic Treaty Organization* – NATO) to układ wojskowy zrzeszający obecnie 29 państw. Został ustanowiony w 1949 roku, kiedy to w Waszyngtonie przedstawiciele 12 krajów podpisali Traktat Północnoatlantycki. Polska dołączyła do NATO 12 marca 1999 roku.

Celem istnienia NATO była obrona przed Związkiem Socjalistycznych Republik Radzieckich. Po jego rozpadzie Sojusz zaczął pełnić rolę stabilizacyjną. Wraz z rozwojem nowoczesnych technologii, cyberbezpieczeństwo staje się coraz istotniejszym tematem na forum NATO. Podczas szczytu w Warszawie w 2016 roku, Sojusz uznał cyberprzestrzeń za czwartą domenę prowadzenia działań bojowych. Obecnie NATO wkłada wiele wysiłku, aby zabezpieczyć swoje systemy i sieci oraz pomóc sojusznikom w zwiększeniu ich zdolności do skutecznej cyberobrony.

Organy odpowiedzialne w NATO za cyberbezpieczeństwo[96]

Wysokopoziomowy nadzór nad wdrażaniem polityki NATO w zakresie cyberobrony zapewnia **Rada Północnoatlantycka**[97] (NAC). Rada otrzymuje informacje o najpoważniejszych incydentach i cyberatakach, a także sprawuje główną funkcję w zarządzaniu kryzysowym związanym z cyberobroną.

Radzie podporządkowany jest **Komitet Cyberobrony NATO**[98] (NCDC, *NATO Cyber Defence Committee*), który pełni wiodącą rolę jeśli chodzi o politykę cyberobrony sojuszu. Komitet zapewnia również doradztwo państwom sprzymierzonym na poziomie eksperckim.

Na poziomie roboczym funkcjonuje **Rada NATO ds. Zarządzania Cyberobroną**[99] (NCDMB, *NATO Cyber Defence Management Board*), która odpowiada za koordynację cyberobrony w cywilnych i wojskowych organach NATO.

Ważną rolę pełni też **Komitet Konsultacyjny, Kontroli i Dowodzenia** (C3B, *Consultation, Control and Command Board*), który jest odpowiedzialny za konsultacje aspektów technicznych i wdrożeniowych w zakresie cyberobrony.

Ewolucja w podejściu NATO do cyberobrony

2002 – Cyberobrona pierwszy raz pojawiła się w agendzie sojuszu na szczycie w Pradze.

2007 – Zmasowany cyberatak na estońskie instytucje państwowe, banki oraz media.

2008 – Sojusz zatwierdził **pierwszą politykę dotyczącą cyberobrony** [92] (*NATO Cyber Defence Policy*), która została przyjęta podczas szczytu w Bukareszcie[93].

2008 – Konflikt między Rosją i Gruzją pokazał, że działania w cyberprzestrzeni mogą stanowić zagrożenie nie mniejsze niż konwencjonalne działania wojenne.

2010 – NATO przyjęło nową strategiczną koncepcję na szczycie w Lizbonie. Rada Północnoatlantycka otrzymała zadanie opracowania dogłębnej polityki cyberobrony NATO oraz planu jej wdrożenia[94].

2011 – Ministrowie obrony NATO zatwierdzili **drugą politykę dotyczącą cyberobrony**[95].

2012 – Cyberobrona została wprowadzona **do procesu planowania obrony NATO.**

2014 – Osiągnięto **pełną zdolność operacyjną NCIRC**, co zapewniło lepszą ochronę sieciom NATO.

2014 – Uruchomienie pierwszej inicjatywy, mającej na celu nawiązanie współpracy z sektorem prywatnym (*NATO Industry Cyber Partnership*).

2014 – Na szczycie w Walii państwa Sojuszu poparły nową politykę cyberobrony i zatwierdziły plan działania. Uznano, że **w cyberprzestrzeni obowiązuje prawo międzynarodowe**, a cyberobrona jest częścią podstawowego zadania NATO w zakresie obrony zbiorowej.

2016 – Na szczycie w Warszawie **państwa Sojuszu uznały cyberprzestrzeń za domenę operacji** – podobnie jak powietrze, ląd i morze. Podczas szczytu przyjęto także deklarację cyberbezpieczeństwa (***Cyber Defence Pledge***).

[92] Bucharest Summit Declaration; https://www.nato.int/cps/en/natolive/official_texts_8443.htm
[93] NATO's Cyber History (2008-2012); http://www.natolibguides.info/cybersecurity#s-lg-box-14363350
[94] Lisbon Summit Declaration; https://www.nato.int/cps/en/natolive/official_texts_68828.htm#cyber
[95] NATO Cyber Defence – Evolution; https://www.nato.int/cps/en/natohq/topics_78170.htm#

Szczyt NATO w Brukseli i utworzenie Centrum Operacji w Cyberprzestrzeni

Najważniejszym wydarzeniem w minionym roku był **szczyt NATO, który odbył się w lipcu w Brukseli**[100]. W deklaracji końcowej podkreślono, że Sojusz coraz częściej musi mierzyć się z cyberzagrożeniami, które stają się jeszcze bardziej złożone i niszczycielskie. Dlatego NATO musi być w stanie działać w cyberprzestrzeni równie skutecznie, co w pozostałych konwencjonalnych domenach operacji.

Najistotniejsze wnioski, które zawarto w deklaracji:

- Ogłoszenie **utworzenia Centrum Operacji w Cyberprzestrzeni** w ramach struktury dowodzenia NATO (*Cyberspace Operations Centre,* pkt 29). Nowe centrum, odpowiedzialne za operacje w cyberprzestrzeni, powinno osiągnąć pełną operacyjność w 2023 roku[101]. Ośrodek w Naczelnym Dowództwie Sojuszniczych Sił Europy (SHAPE) z siedzibą w Mons w Belgii ma się składać z zespołu 70 ekspertów, którzy będą mieli dostęp do wiedzy wywiadowczej oraz do informacji o cyberatakach pozyskiwanych w czasie rzeczywistym. Jest to krok w stronę stworzenia możliwości prowadzenia operacji w cyberprzestrzeni. Celem centrum będzie zapewnienie, że Naczelny Dowódca Sojuszniczy w Europie będzie wyposażony we wszystkie potrzebne narzędzia do podejmowania działań w cyberprzestrzeni.
- **Obrona przed działaniami hybrydowymi**, takimi jak cyberataki czy kampanie dezinformacyjne (pkt 2), które mogą być również wykorzystywane do ingerowania w demokratyczne procesy, np. wybory (pkt 6). NATO potwierdziło swój mandat obronny, jednocześnie zadeklarowało, że wykorzysta pełen zakres możliwości, aby odstraszać, bronić się i przeciwdziałać zagrożeniom w cyberprzestrzeni (pkt 20).
- Konieczność zapewnienia silnej krajowej obrony cyberprzestrzeni poprzez **realizację *Cyber Defence Pledge***. Implementacja tego zobowiązania ma kluczowe znaczenie dla zwiększenia cyberodporności państw członkowskich oraz kosztu cyberataku (pkt 20).
- Uzgodnienie, w jaki sposób NATO może korzystać z krajowych zdolności w domenie cyberprzestrzeni, **do prowadzenia misji i operacji**. Sojusznicy dostarczają swoje rozwiązania dobrowolnie, a ich wykorzystanie odbywa się w ramach silnego politycznego nadzoru (pkt 20).
- Poszczególni członkowie mogą suwerennie rozważyć, w stosownych przypadkach, **atrybucję cyberataku** oraz podjęcie skoordynowanej odpowiedzi (pkt 20).
- Konieczność prowadzenia dalszego **dialogu między NATO a UE** dla zacieśnienia współpracy w zakresie cyberbezpieczeństwa (pkt 70). W przeddzień brukselskiego szczytu przewodniczący Rady Europejskiej, przewodniczący Komisji Europejskiej oraz sekretarz generalny NATO podpisali wspólną deklarację w tej sprawie.

Implementacja *Cyber Defence Pledge*

Dokument przyjęty na szczycie w Warszawie w 2016 roku jest wynikiem dążenia Sojuszu do zwiększenia nacisku na cyberodporność na poziomie krajowym. Sojusznicy zobowiązali się do podniesienia swojego poziomu cyberbezpieczeństwa. Najważniejsze postanowienia to m.in.:

- Konieczność wzmocnienia cyberbezpieczeństwa krajowych sieci oraz infrastruktury.
- Dotrzymywanie kroku szybko rozwijającym się cyberzagrożeniom, tak aby państwa NATO były w stanie skutecznie bronić się w cyberprzestrzeni.
- Stosowanie prawa międzynarodowego w cyberprzestrzeni oraz współpraca z UE.
- Międzynarodowa współpraca poprzez edukację, szkolenia oraz wymianę informacji.

Pierwsza konferencja podsumowująca wdrażanie *Cyber Defence Pledge* odbyła się 15 maja 2018 r. w Paryżu. Sekretarz generalny NATO Jens Stoltenberg przyznał, że w ciągu niespełna dwóch lat od przyjęcia zobowiązania, **niemal każdy sojusznik poprawił swoje zdolności cyberobronne.** Liderem zmian w Europie jest Wielka Brytania, która zainwestowała 1,9 mld funtów za pośrednictwem narodowej strategii cyberbezpieczeństwa[102] (*National Cyber Security Strategy*). Druga w kolejności Francja zainwestowała 1,6 mld euro[103].

Realizacja *Cyber Defence Pledge* była oceniana również podczas szczytu NATO w Brukseli w lipcu 2018 roku. Poszczególne kraje poinformowały o poczynionych przez siebie postępach.

Rozwijanie zdolności cyberobrony NATO

W belgijskim Mons funkcjonuje jednostka **NATO *Computer Incident Response Capability*** (NCIRC), która zapewnia całodobowe wsparcie państwom Sojuszu. Zespół 200 ekspertów[104] odgrywa kluczową rolę w reagowaniu na wszelkie incydenty cyberbezpieczeństwa, mające wpływ na NATO. Nie tylko obsługuje i identyfikuje on incydenty, ale również dystrybuuje ważne informacje odnośnie wykrytych cyberzagrożeń.

NCIRC funkcjonuje w ramach **Agencji NATO ds. Komunikacji i Informacji** (*NATO Communications and Information Agency*), która prowadzi także inne inicjatywy z zakresu cyberobrony. Są to m.in. program współpracy z sektorem prywatnym (*NATO Industry Cyber Partnership*) czy zespoły szybkiego reagowania (*Rapid Reaction Team*).

NATO pomaga sojusznikom zwiększyć swoje zdolności cyberobrony poprzez:

- Udostępnianie w czasie rzeczywistym informacji o incydentach oraz dzielenie się najlepszymi praktykami, jak zwalczać zagrożenia w cyberprzestrzeni;
- Utrzymywanie zespołów szybkiego reagowania, które mogą pomagać sojusznikom;
- Opracowanie celów, których realizacja ułatwi wypracowanie wspólnego podejścia do budowania zdolności cyberobronnych sojuszników;
- Inwestowanie w edukację, szkolenia i ćwiczenia, takie jak Cyber Coalition.

Deklaracja w sprawie współpracy UE-NATO

W deklaracji z 10 lipca 2018 roku podtrzymano zobowiązanie do zacieśnienia współpracy, które zapoczątkowano w 2016 roku w Warszawie[105]. Wśród siedmiu głównych obszarów wskazano m.in. zwiększenie zdolności do reagowania na zagrożenia hybrydowe, takie jak cyberataki i dezinformacja, a także podniesienie poziomu cyberbezpieczeństwa[106].

Współpraca między NATO i UE odbywa się na kilku płaszczyznach. W 2016 roku obie organizacje podpisały techniczne porozumienie[107], które umożliwiło wymianę informacji oraz najlepszych praktyk między zespołami reagowania na cyberzagrożenia z NATO (NCIRC) oraz Unii Europejskiej (CERT-EU). Sekretarz generalny NATO, jako przykład dobrej współpracy, wymienił działania podczas ataków WannaCry i NotPetya w 2017 roku[108]. Reprezentacje obu organizacji biorą też udział we wspólnych ćwiczeniach, np. *Cyber Coalition czy Locked Shields.*

Ćwiczenia – podnoszenie zdolności współpracy pomiędzy członkami Sojuszu

NATO przeprowadza wiele ćwiczeń, starając się jak najlepiej przygotować do współczesnych wyzwań. Ćwiczenia mają nie tylko pomóc NATO w sprawdzeniu strategii oraz mechanizmów, ale służą również wzmacnianiu współpracy między członkami Sojuszu.

- ***Locked Shields*** to ćwiczenie organizowane co roku przez Sojusznicze Centrum Doskonalenia Obrony Cybernetycznej w Estonii (NATO *Cooperative Cyber Defence Centre of Excellence*, **CCDCOE**). 27 kwietnia 2018 roku wzięło w nim udział ponad 1000 ekspertów z 30 krajów. 22 zespoły trenowały obronę złożonych systemów informatycznych w przypadku cyberataków na dużą skalę. Łącznie przeprowadzono ponad 2500 ataków. Najlepszy okazał się zespół z NATO, który wyprzedził drużynę z Francji i Czech[109].
- Ćwiczenie ***Cyber Coalition*** odbyło się w Estonii między 26 a 30 listopada 2018 roku[110]. W jedenastej edycji uczestniczyło ponad 700 uczestników z 28 państw członkowskich oraz 4 partnerskich, a także z sektora prywatnego i środowisk akademickich. Ćwiczenie miało wzmocnić koordynację i współpracę między NATO i sojusznikami, a także poprawić ochronę cyberprzestrzeni Sojuszu oraz usprawnić prowadzenie w niej operacji wojskowych.

Ważne wydarzenia

- **Międzynarodowa Konferencja CyCon 2018**

  X Międzynarodowa Konferencja CyCon 2018 (*Conference on Cyber Conflict*, CyCon 2018) zorganizowana została 5 czerwca 2018 roku w Tallinie przez **CCDCOE**[111]. W wydarzeniu udział wzięło około 700 ekspertów z ponad 40 krajów. Konferencja odbyła się pod hasłem maksymalizacji efektów w cyberprzestrzeni. Debaty i prezentacje były okazją do zaprezentowania oryginalnych prac badawczych oraz spostrzeżeń renomowanych ekspertów. Materiały z konferencji są publikowane jako publikacje IEEE (*Institute of Electrical and Electronics Engineers*) i stanowią ważny wkład do światowej literatury technicznej.

- **Konferencja NIAS 2018 – *Cyber Security Symposium***

  NIAS to największa konferencja NATO dotycząca cyberbezpieczeństwa, która odbyła się 16-18 października 2018 roku w Belgii (*NIAS18: Securing NATO's Digital Endeavour*[112]). Podczas spotkania podkreślono rolę cyberbezpieczeństwa, którego zapewnienie stanowi konieczność dla każdej konwencjonalnej operacji Sojuszu. Możliwość bezpiecznej wymiany krytycznie ważnych informacji jest niezbędna, aby wojskowi dowódcy oraz przywódcy państw mogli podejmować właściwe decyzje we właściwym czasie. W 2018 roku konferencja zgromadziła ponad 1800 liderów i czołowych specjalistów cyberbezpieczeństwa.

[101] NATO Cyber Defence – Factsheet; https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf
[102] Why cyber space matters as much to NATO as land, sea and air defence; https://www.ft.com/content/9c3ae876-6d90-11e8-8863-a9bb262c5f53
[103] Cyber Defence Pledge Conference; https://www.nato.int/cps/en/natohq/opinions_154462.htm
[104] NATO Cyber Defence, Factsheet, December 2018; https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/20180213_1802-factsheet-cyber-defence-en.pdf
[105] EU-NATO Cooperation – Factsheet; https://cdn5-eeas.fpfis.tech.ec.europa.eu/cdn/farfuture/otambGc7_PZ7cDdMdQqQki4M3aTBIo6-efph8-K1vFI/mtime:1542899750/sites/eeas/files/eu-nato_cooperation_factsheet.pdf
[106] Joint Declaration on EU-NATO Cooperation; 2018 https://www.nato.int/cps/en/natohq/official_texts_156626.htm
[107] NATO and the European Union enhance cyber defence cooperation; https://www.nato.int/cps/en/natohq/news_127836.htm
[108] Cyber Defence Pledge Conference; https://www.nato.int/cps/en/natohq/opinions_154462.htm
[109] NATO Won Cyber Defence Exercise Locked Shields 2018; https://ccdcoe.org/nato-won-cyber-defence-exercise-locked-shields-2018.html
[110] Cyber Coalition helps prepare NATO for today's threats; https://www.nato.int/cps/en/natohq/news_160898.htm
[111] The 10th CyCon Hosts 700 Cyber Experts in Tallinn; https://ccdcoe.org/cycon/content/10th-cycon-hosts-700-cyber-experts-tallinn.html
[112] NIAS 18; http://nias2018.com

Dezinformacja – działania NATO StratCom COE

NATO dostrzega zagrożenia, jakie dla Sojuszu stanowią działania hybrydowe, takie jak cyberataki czy kampanie dezinformacyjne. Powagę tego rodzaju działań podkreślono m.in. w deklaracji z ostatniego szczytu NATO w Brukseli w 2018 roku[113]. Już w deklaracji ze szczytu w Walii, sojusznicy z zadowoleniem przyjęli ustanowienie **NATO Strategic Communications Centre of Excellence** (*NATO StratCom COE*). Jest to wielonarodowa organizacja wojskowa z akredytacją NATO, nie będąca jednak częścią struktury dowodzenia Sojuszu. Polska należy do współzałożycieli. Od czasu powstania, centrum jest jednym z wiodących ośrodków, budujących kompetencje w zakresie komunikacji strategicznej, w tym w walce z dezinformacją. Obecnie zrzesza jedenaście krajów, a trzy kolejne finalizują procedurę dołączenia[114]. Wśród publikacji przygotowanych w 2018 roku wymienić można:

- ***Russia's Footprint in the Nordic-Baltic Information Environment*[115]**

  Materiał dotyczy strategii dezinformacyjnej Rosji na obszarze państw bałtyckich i nordyckich. Analiza opisuje metodykę działania oraz cele, jakie chce osiągnąć Rosja w czterech obszarach:

  1. **Politycznym**: utrzymanie statusu supermocarstwa, uderzenie w zachodnie wartości i zaburzenie jedności zachodnich państw.
  2. **Informacyjnym**: utworzenie globalnego systemu informacyjnego, promującego rosyjską perspektywę oraz punkt widzenia.
  3. **Militarnym**: powstrzymanie ekspansji NATO w kierunku granic Rosji.
  4. **Ekonomicznym**: Arktyka jest priorytetowym obszarem gospodarczym dla Rosji.

- **Robotrolling**

  Robotrolling to kwartalny raport, który analizuje manipulacje w mediach społecznościowych na temat obecności NATO w krajach bałtyckich. Autorzy skupiają się na dezinformacji, prowadzonej przez konta zautomatyzowane (boty) oraz fałszywe (trolle). Analizy wskazały, że w 4 kwartale 2018 roku boty wytworzyły 46 proc. wiadomości w języku rosyjskim na temat obecności NATO w krajach nadbałtyckich i Polsce[116].

- ***Executive summary. Fake News: A Roadmap*[117]**

  Dokument odpowiada na pytania czym są tzw. *fake newsy* oraz dlaczego obecne środowisko informacyjne służy szybkiemu rozprzestrzenianiu się kampanii dezinformacyjnych. Autorzy wskazują jakie działania można podjąć, aby przeciwdziałać temu zjawisku.

- **Gra na Facebooku, która uczy dostrzegać dezinformację**

  Gra ma pomóc wyłapywać użytkownikom Facebooka tzw. *fake newsy*[118]. Gracze prowadzą własną firmę wydawniczą, zarabiają wirtualną walutę i zdobywają czytelników, publikując wiarygodne wiadomości. Pomaga im w tym ekran sprawdzania faktów, który zachęca graczy do weryfikowania źródeł i podpowiada, jak odróżnić informacje prawdziwe od fałszywych.

[113] Brussels Summit Declaration, pkt 2 i 21; https://www.nato.int/cps/en/natohq/official_texts_156624.htm
[114] NATO StratCom COE; https://www.stratcomcoe.org/about-us
[115] Russia's Footprint in the Nordic-Baltic Information Environment; https://www.stratcomcoe.org/russias-footprint-nordic-baltic-information-environment
[116] Robotrolling 2018/4; https://www.stratcomcoe.org/robotrolling-20184
[117] Executive summary. Fake News: A Roadmap; https://www.stratcomcoe.org/executive-summary-fake-news-roadmap
[118] Facebook game teaches how to spot disinformation; https://www.stratcomcoe.org/facebook-game-teaches-how-spot-disinformation

NASK
Cyber POLICY

OBWE – budowa zaufania i współpracy w cyberprzestrzeni

Organizacja Bezpieczeństwa i Współpracy w Europie, OBWE *(Organization for Security and Cooperation in Europe, OSCE)* działa na rzecz zapobiegania konfliktom w Europie. Powstała w 1995 roku i aktualnie zrzesza 57 państw, nie tylko europejskich[119]. Do jej głównych zadań należy kontrola zbrojeń, budowa zaufania, dbałość o prawa człowieka i mniejszości narodowych, działanie na rzecz demokracji i środowiska, a także zwalczanie terroryzmu.

OBWE odgrywa znaczącą rolę w podnoszeniu poziomu cyberbezpieczeństwa na świecie poprzez zmniejszanie ryzyka konfliktów między państwami. Ponieważ cyberprzestrzeń stanowi obecnie dodatkowy wymiar w złożonych relacjach międzypaństwowych, państwa członkowskie OBWE pracują nad budową wzajemnego zaufania, szczególnie w obszarze nowoczesnych technologii, poprzez konsultacje dotyczące potencjalnych incydentów cyberbezpieczeństwa, budowę platformy do wymiany poglądów i krajowych polityk cyberbezpieczeństwa, oraz współpracę zmniejszającą podatności na incydenty, np. w obszarze informacyjnej infrastruktury krytycznej.

Budowanie zaufania w cyberprzestrzeni: *OSCE confidence-building measures*

OBWE przygotowało listę 16 postulatów, których realizacja ma przyczynić się do zwiększania zaufania pomiędzy członkami (*OSCE confidence-building measures – CBM*). Koncepcja opiera się na założeniu, że najlepszym sposobem zapobiegania konfliktom jest stworzenie systemu bezpośredniej komunikacji, która pozwoli na wyjaśnianie nieporozumień i identyfikację możliwych punktów spornych.

Lista CBM z 2013 r.:

1. Państwa dobrowolnie przekażą informację na temat krajowych aspektów zagrożeń cyberbezpieczeństwa.
2. Państwa będą ułatwiać współpracę i wymianę informacji między krajowymi organami zajmującymi się cyberbezpieczeństwem.
3. Państwa zaangażują się w zmniejszanie ryzyka konfliktu politycznego lub militarnego, który może wynikać z nieporozumień i wykorzystywania technologii ICT.
4. Państwa będą wymieniać się informacjami na temat środków zapewniających otwarty, interoperacyjny i bezpieczny Internet.
5. OBWE będzie wykorzystywane jako platforma dialogu, wymiany dobrych praktyk, podnoszenia świadomości na temat budowania zdolności w zakresie cyberbezpieczeństwa.
6. OBWE zachęca państwa do ustanowienia nowoczesnych i efektywnych metod legislacyjnych, które będą wspierać współpracę i wymianę informacji między władzą, a instytucjami zajmującymi się zwalczaniem cyberprzestępczości.
7. Państwa dobrowolnie wymieniają się informacjami na temat krajowych strategii i polityk istotnych dla bezpieczeństwa ICT.
8. Państwa wyznaczą punkt kontaktowy w celu ułatwienia komunikacji i dialogu między sobą.
9. W celu zmniejszenia ryzyka nieporozumień, państwa uzgodnią wspólną terminologię związaną z bezpieczeństwem i stosowaniem technologii informacyjno-komunikacyjnych.
10. Państwa będą dobrowolnie wymieniać poglądy i informacje za pośrednictwem platformy kontaktowej OBWE.
11. Co najmniej 3 razy w roku będą się odbywać spotkania ekspertów, reprezentantów państw uczestniczących, w celu omówienia aktualnego stanu cyberbezpieczeństwa i zbadania rozwoju środków budowy zaufania w przyszłości.

[119] W skład OBWE wchodzą państwa z trzech kontynentów: Europy, Ameryki Północnej i Azji. Poza państwami członkowskimi do organizacji należy również 6 partnerów śródziemnomorskich i 5 azjatyckich; „Who we are"; https://www.osce.org/whatistheosce

W 2016 r. dodano poniższe punkty:

12. Państwa będą dobrowolnie dzielić się informacjami za pomocą różnych form współpracy, tj. seminariów, forów, spotkań przy okrągłym stole itp. Będą wymieniać między sobą wiedzę na temat procesów i mechanizmów, które zmniejszają ryzyko konfliktu wynikającego z wykorzystywania ICT. Zachęca się państwa do kontynuowania stabilnej, przejrzystej i przewidywalnej współpracy, uzupełniania w tym zakresie działań innych organizacji międzynarodowych (np. ONZ), uwzględniania potrzeb i wymagań wszystkich interesariuszy, a także zapraszania do współpracy środowisk akademickich, przedstawicieli biznesu, organizacji trzeciego sektora i społeczeństwa obywatelskiego.
13. Państwa będą dobrowolnie prowadzić działania informacyjne, wspierające dostęp do autoryzowanych środków komunikacji, w celu zmniejszania ryzyka nieporozumień i eskalacji konfliktów, a także wyjaśniające techniczne i prawne aspekty wykorzystywania technologii ICT.
14. Państwa będą promować partnerstwa publiczno-prywatne, a także wspierać wymianę dobrych praktyk z dziedziny cyberbezpieczeństwa i wykorzystywania technologii ICT.
15. Państwa będą dobrowolnie budować współpracę z organami zabezpieczającymi infrastrukturę krytyczną w celu oszacowania ryzyka i możliwych wyzwań związanych z cyberbezpieczeństwem.
16. Państwa będą zachęcać do zgłaszania luk w zabezpieczeniach, a także poinformują o dostępnych środkach zaradczych. Takie informacje mogą być również przekazywane między państwami poprzez autoryzowane kanały komunikacji i punkty kontaktowe[120].

CBM były jednym z tematów poruszanych podczas konferencji w Rzymie, która odbyła się we wrześniu 2018 r. Wzięło w niej udział 170 przedstawicieli 57 państw członkowskich OBWE, partnerów, organizacji pozarządowych, środowisk akademickich i biznesu. **Główna dyskusja dotyczyła możliwości łagodzenia ryzyka konfliktu wynikającego z użycia technologii ICT z wykorzystaniem opracowanych CBM.** Dodatkowo w trakcie konferencji uczestnicy mieli możliwość zaprezentować tematy związane z lokalnymi zagrożeniami cyberbezpieczeństwa. Skupiono się również na kwestii **zwiększania możliwości zwalczania incydentów przez państwa.** Ważną sugestią była zachęta do **budowy partnerstw publiczno-prywatnych**, dzięki którym państwa mogłyby skorzystać ze skutecznych rozwiązań sektora prywatnego, zwiększać wiedzę na temat cyberbezpieczeństwa, a także delegować zadania do firm zajmujących się cyberbezpieczeństwem[121].

Zwalczanie cyberprzestępczości – projekt edukacyjny w Europie Południowo-Wschodniej

We wrześniu 2017 r. OBWE uruchomiło projekt edukacyjny, którego celem jest rozwój wymiaru sprawiedliwości w zakresie cyberprzestępczości w Europie Południowo-Wschodniej. W ramach projektu zorganizowano serię szkoleń i warsztatów, m.in. na temat cyfrowych materiałów dowodowych, kryptowalut, Dark Webu, Forensics[122]. Projekt zakończy się w 2019 r. konferencją podsumowującą, na której zostaną wytyczone obszary wymagające szczególnej pracy i uwagi w przyszłości[123].

[120] Decision no. 1202 osce confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies, s. 1-4; https://ccdcoe.org/sites/default/files/documents/OSCE-160310-NewCBMs.pdf

[121] New technological features, policy engagement and public-private partnerships as ways to lower risks of cyber conflicts in focus at Rome conference, OSCE Newsroom; https://www.osce.org/chairmanship/397853

[122] OSCE-hosted training course for South-Eastern Europe on handling digital evidence by first responders completed in Tirana, OSCE Newsroom, 26.01.2018; https://www.osce.org/secretariat/368056; OSCE hosts regional training course on Live Data Forensics in Tirana, OSCE Newsroom; https://www.osce.org/secretariat/374089; OSCE hosts training course for South-Eastern Europe on Dark Web and virtual currencies in Tirana; OSCE Newsroom; https://www.osce.org/presence-in-albania/372201

[123] OSCE launches project on combating cybercrime and cyber-enabled crime in South-Eastern Europe, OSCE Newsroom; https://www.osce.org/secretariat/341141

O Autorach

Rafał Babraj – Specjalista ds. komunikacji i nowoczesnych technologii w zespole Analiz Strategicznych i Wpływu Nowoczesnych Technologii w NASK PIB. Specjalizuje się w analizach dotyczących dezinformacji i fałszywych informacji, przede wszystkim w kontekście polityki UE i NATO. Jego zainteresowania badawcze koncentrują się nad wpływem rozwoju nowoczesnych technologii na bezpieczeństwo informacji. Twórca projektu bezpiecznewybory.pl.

Doświadczenie zdobywał, pracując jako dziennikarz i redaktor stron internetowych, a także w biurach prasowych w administracji publicznej. Redaktor naczelny strony internetowej Mazowieckiego Urzędu Wojewódzkiego. Lider zespołu wprowadzającego standardy prostego języka w Ministerstwie Zdrowia, zaangażowany w prace nad rządowym portalem GOV.PL oraz odpowiedzialny za uruchomienie na nim strony resortu zdrowia. Absolwent Instytutu Edukacji Medialnej i Dziennikarstwa na Uniwersytecie Kardynała Stefana Wyszyńskiego w Warszawie.

Prywatnie pisarz oraz pasjonat literatury fantastycznej.

Justyna Balcewicz – Analityk ds. „czynnika ludzkiego w cyberbezpieczeństwie" i nowoczesnych technologiach w zespole Analiz Strategicznych i Wpływu Nowoczesnych Technologii w NASK PIB. Specjalizuje się w analizach z zakresu wpływu nowoczesnych technologii na rozwój społeczeństwa i związanych z tym wyzwaniami. Czynnie zaangażowana w prace grupy roboczej ds. edukacji, opracowującej wytyczne do powstania strategii Sztucznej Inteligencji dla Polski, działającej w Ministerstwie Cyfryzacji.

Doświadczenie zdobywała, pracując w firmach sektora energetycznego oraz w sektorze finansowym, gdzie zajmowała się monitoringiem transakcji podejrzanych o pranie brudnych pieniędzy. Wcześniej pracowała jako koordynator projektów unijnych finansowanych ze Szwajcarsko-Polskiego Programu Współpracy i Norweskiego Mechanizmu Finansowego.

Absolwentka Socjologii Instytutu Stosowanych Nauk Społecznych Uniwersytetu Warszawskiego oraz studiów w Wyższej Szkole Finansów i Zarządzania. Ekspert w zakresie relacji międzyludzkich i ich wpływu na funkcjonowanie społeczeństwa oraz rozwoju kompetencji cyfrowych w świecie nowoczesnych technologii. W wolnych chwilach pisarka powieści dla dzieci i młodzieży.

Magdalena Wrzosek – Kierownik Zespołu Analiz Strategicznych i Wpływu Nowoczesnych Technologii w NASK PIB, gdzie odpowiada za kwestie strategiczne, regulacyjne i organizacyjne związane z cyberbezpieczeństwem oraz rozwojem nowoczesnych technologii. Oficer Łącznikowy Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), koordynator Europejskiego Miesiąca Cyberbezpieczeństwa w Polsce. Twórca projektu CyberPolicy (*https://cyberpolicy.nask.pl*). Brała także udział w pracach międzyresortowego zespołu odpowiedzialnego za przygotowanie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 oraz założeń do Ustawy o krajowym systemie cyberbezpieczeństwa.

W latach 2014-2016 pracowała w Ministerstwie Cyfryzacji, gdzie odpowiadała m.in. za negocjacje Dyrektywy NIS, planowanie i koordynację europejskich ćwiczeń cybernetycznych Cyber Europe (edycja 2014 i 2016), współpracę międzynarodową oraz implementację zapisów Polityki Ochrony Cyberprzestrzeni RP.

Politolog, kulturoznawca, absolwentka Uniwersytetu Warszawskiego i Uniwersytetu w Konstancji w Niemczech. Studia podyplomowe z zarządzania projektami, zarządzania bezpieczeństwem informacji, prawa międzynarodowego i służby zagranicznej. Ukończyła także Europejskie Centrum Studiów nad Bezpieczeństwem im. Greaorge'a Marshall'a w Garmisch-Partenkirchen (Program on Cyber Security Studies (PCSS) oraz Seminar on Regional Security (SRS)). W 2016 roku brała udział w programie dotyczącym cyberbezpieczeństwa, organizowanym przez Departament Stanu USA International Visitor Leadership Program. Doktorantka Akademii Sztuki Wojennej w Warszawie.

NASK

Cyber POLICY

Grafiki zaprojektowane częściowo przez:

Harryartsrawpixel.com

rawpixel.com

Freepik.com

NASK

Cyber POLICY

NASK – Państwowy Instytut Badawczy

ul. Kolska 12, 01-045 Warszawa

Recepcja

+48 22 380 82 00

+48 22 380 82 01

nask@nask.pl

Sekretariat

+48 22 380 82 04

+48 22 380 82 01

nask@nask.pl