EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY

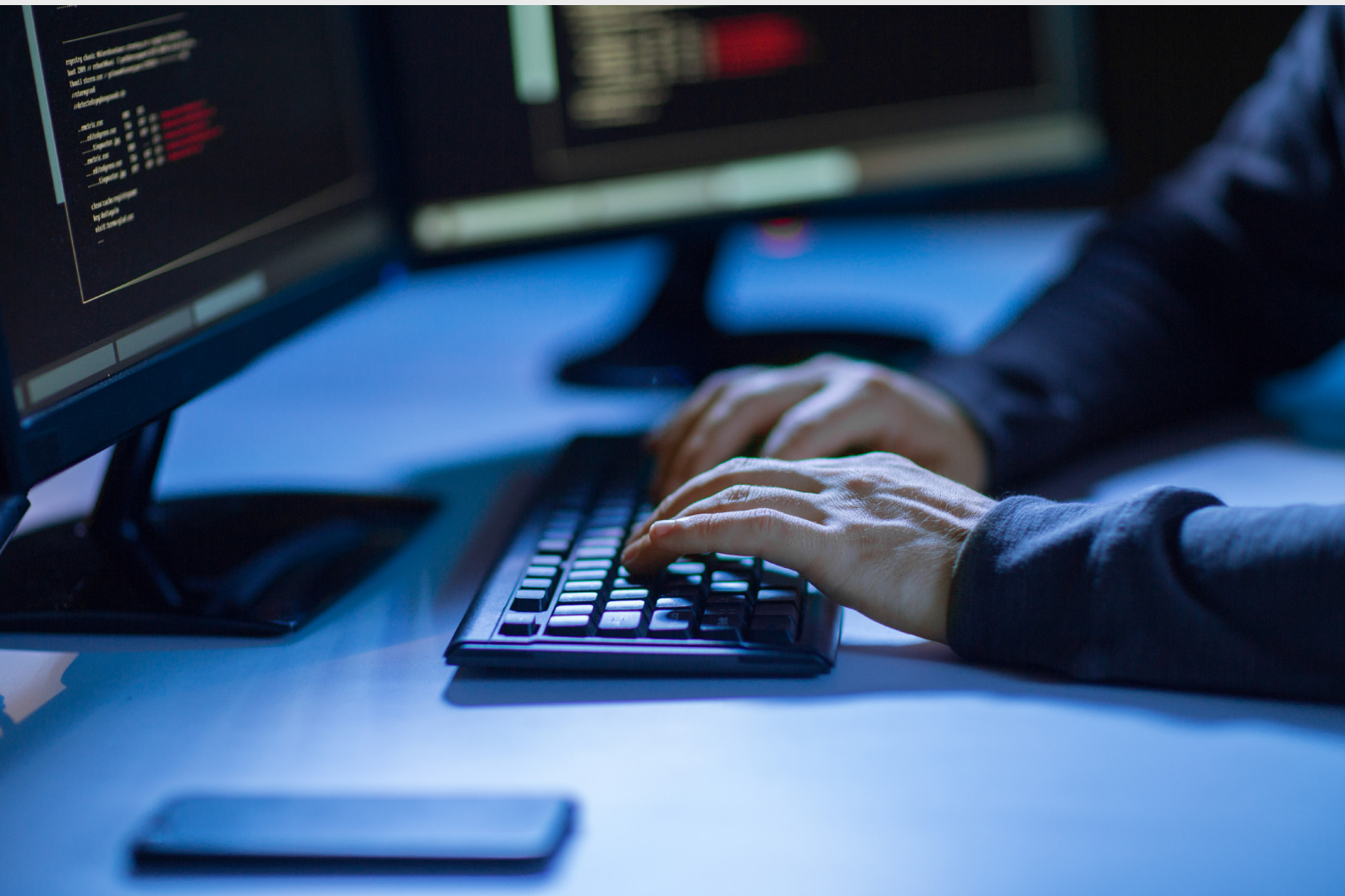
PL

2019

Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją

Dokument analityczny

Marzec 2019 r.



Informacje na temat niniejszego dokumentu:

Cel niniejszego dokumentu analitycznego – niebędącego sprawozdaniem z kontroli – polega na przedstawieniu w zarysie złożonych warunków, w jakich prowadzona jest unijna polityka cyberbezpieczeństwa, oraz wskazaniu zasadniczych wyzwań związanych ze skutecznym realizowaniem tej polityki. W dokumencie poruszono kwestie bezpieczeństwa sieci i informacji, cyberprzestępczości, cyberobrony i dezinformacji. Stanowi on jednocześnie wkład w przyszłe prace kontrolne w tym obszarze.

Trybunał przeanalizował wybrane ogólnodostępne informacje pochodzące z oficjalnych dokumentów, stanowisk i opracowań zewnętrznych. Prace przeprowadzono w okresie od kwietnia do września 2018 r., przy czym w dokumencie uwzględniono rozwój sytuacji aż do grudnia 2018 r. Uzupełniono je ankietą rozesłaną do krajowych organów kontroli państw członkowskich oraz wywiadami z przedstawicielami kluczowych zainteresowanych stron z unijnych instytucji oraz sektora prywatnego.

Rozpoznane przez Trybunał wyzwania pogrupowano w cztery szerokie kategorie: (i) ramy polityczne; (ii) finansowanie i wydatkowanie środków; (iii) budowanie cyberodporności; (iv) skuteczne reagowanie na cyberincydenty. Kluczowym sprawdzianem dla Unii pozostaje osiągnięcie wyższego poziomu cyberbezpieczeństwa w UE. Z tego względu na końcu każdego rozdziału zamieszczono szereg kwestii do dalszego rozważenia przez decydentów politycznych, prawodawców i specjalistów działających w omawianej dziedzinie.

Trybunał pragnie przy tej okazji podziękować za użyteczne informacje zwrotne, które otrzymał od służb Komisji, Europejskiej Służby Działań Zewnętrznych, Rady Unii Europejskiej, Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji, Europolu, Europejskiej Organizacji ds. Cyberbezpieczeństwa, a także krajowych organów kontroli z państw członkowskich.

Spis treści

Streszczenie

I Technologia otwiera przed nami nowe niezmierzone możliwości, a nowe produkty i usługi stają się nieodłącznym elementem codziennego życia. Jednocześnie rośnie ryzyko cyberprzestępstw i cyberataków, których społeczne i ekonomiczne oddziaływanie jest coraz większe. Trwające od 2017 r. starania Unii Europejskiej, by przyspieszyć realizację inicjatyw na rzecz podniesienia poziomu cyberbezpieczeństwa i zwiększenia autonomii cyfrowej, przypadają więc w szczególnie ważnym momencie.

II W niniejszym dokumencie analitycznym – który nie jest sprawozdaniem z kontroli i opiera się na ogólnodostępnych informacjach – przedstawiono w zarysie złożone i niejednorodne okoliczności prowadzenia polityki cyberbezpieczeństwa oraz wskazano zasadnicze wyzwania związane z jej skutecznym realizowaniem. Zakres dokumentu obejmuje unijną politykę cyberbezpieczeństwa, a także cyberprzestępczość i cyberobronę. Uwzględniono w nim również działania mające na celu zwalczanie dezinformacji. Rozpoznane przez Trybunał wyzwania pogrupowano w cztery szerokie kategorie: (i) ramy polityczne i prawne; (ii) finansowanie i wydatkowanie środków; (iii) budowanie cyberodporności; (iv) skuteczne reagowanie na cyberincydenty. Na końcu każdego rozdziału umieszczono szereg kwestii do rozważenia odnoszących się do tych wyzwań.

Ramy polityczne i prawne

III Wobec braku mierzalnych celów oraz niewielkiej ilości dostępnych wiarygodnych danych trudnym zadaniem jest opracowanie działań zgodnych z ogólnym zamiarem unijnej strategii w zakresie cyberbezpieczeństwa, polegającym na stworzeniu najbezpieczniejszego środowiska cyfrowego na świecie. Pomiary wyników przeprowadza się rzadko i dotychczas ocenie poddano jedynie niewielką liczbę obszarów polityki. Kluczowym wyzwaniem pozostaje zatem **zapewnienie rzetelnej rozliczalności i oceny** dzięki przejściu na kulturę organizacyjną ukierunkowaną na wyniki i powiązaną z ugruntowanymi praktykami oceny.

IV Ramy prawne pozostają niekompletne. **Luki w unijnych przepisach prawnych i niespójna transpozycja tych przepisów** mogą sprawić, że nie będzie można wykorzystać w pełni potencjału tkwiącego w prawodawstwie.

Finansowanie i wydatkowanie środków

V Wyzwaniem jest również **dostosowywanie poziomów inwestycji do celów**. Wymaga to nie tylko zwiększenia ogólnych inwestycji w cyberbezpieczeństwo – które w UE pozostają rozdrobnione i na niskim poziomie – lecz także wzmocnienia oddziaływania, w szczególności poprzez lepsze wykorzystanie rezultatów uzyskanych dzięki środkom na badania naukowe oraz za sprawą skutecznego ukierunkowania działań na przedsiębiorstwa typu start-up i finansowania tych przedsiębiorstw.

VI **Zyskanie jasnego obrazu wydatków unijnych** jest niezbędne do tego, by UE i państwa członkowskie wiedziały, jakie luki należy wyeliminować, aby osiągnąć założone cele. Ponieważ w budżecie UE nie wyodrębniono oddzielnych środków na strategię w zakresie cyberbezpieczeństwa, brak jest przejrzystych informacji, jakie środki przeznaczono na jakie cele.

VII W czasach, gdy polityczne priorytety związane z bezpieczeństwem zyskują na znaczeniu, **niedostatki odpowiednich zasobów w unijnych agencjach zajmujących się cyberprzestrzenią** mogą skutkować niespełnieniem przez UE ambicji w tej dziedzinie. Aby poradzić sobie z tym wyzwaniem, należy m.in. znaleźć sposoby na przyciągnięcie i zatrzymanie utalentowanych pracowników.

Budowanie cyberodporności

VIII Uchybienia w zarządzaniu w zakresie cyberbezpieczeństwa są powszechne w sektorach publicznym i prywatnym w UE, a także na szczeblu międzynarodowym. Osłabia to zdolność społeczności międzynarodowej do reagowania na cyberataki i ich zwalczania. Stanowi również przeszkodę w stosowaniu jednego spójnego podejścia w całej UE. Należy zatem **usprawnić zarządzanie w dziedzinie cyberbezpieczeństwa**.

IX Coraz bardziej odczuwalny w skali globalnej niedostatek umiejętności w zakresie cyberbezpieczeństwa sprawia, że niezwykle istotne są **rozwój kompetencji i podnoszenie poziomu świadomości** we wszystkich sektorach i grupach społecznych. Obecnie ogólnounijne standardy dotyczące szkolenia, certyfikacji i oceny ryzyka w cyberprzestrzeni mają jedynie ograniczony zakres.

X Stworzenie godnej zaufania cyberprzestrzeni ma kluczowe znaczenie dla zwiększenia ogólnej cyberodporności. Sama Komisja oceniła, że koordynacja działań wciąż jest niewystarczająca. Wyzwaniem pozostaje również **usprawnienie wymiany informacji i koordynowania działań** między sektorem publicznym i prywatnym.

Skuteczne reagowanie na cyberincydenty

XI Systemy cyfrowe stały się tak złożone, że zapobieżenie wszystkim atakom jest niemożliwe. Problem ten można rozwiązać, zapewniając **szybkie wykrywanie i reagowanie**. Tymczasem cyberbezpieczeństwo nie zostało jeszcze w pełni włączone w istniejące ogólnounijne mechanizmy koordynacji reagowania kryzysowego. Może to ograniczać zdolność Unii do reagowania na transgraniczne cyberincydenty na dużą skalę.

XII Podstawowym zagadnieniem jest **ochrona infrastruktury i funkcji społecznych o krytycznym znaczeniu**. Ponadto poważne wyzwanie stanowią potencjalne zakłócenia procesów wyborczych i kampanie dezinformacyjne.

XIII Obecne wyzwania związane z cyberzagrożeniami, którym musi stawić czoła UE, i ogólny rozwój sytuacji na świecie wymagają ciągłego zaangażowania ze strony UE i nieustannego, zdeterminowanego obstawania przy unijnych wartościach podstawowych.

Wstęp

01 Technologia otwiera przed nami nowe niezmierzone możliwości. W miarę jak nowe produkty i usługi rozpowszechniają się, stają się nieodłączną częścią codziennego życia. Niemniej z każdą kolejną zmianą rośnie zależność technologiczna społeczeństwa, a wraz z nią – znaczenie cyberbezpieczeństwa. Im więcej danych osobowych umieszcza się w internecie i im większa część życia toczy się w sieci, tym większe jest zagrożenie wszelkimi formami cyberprzestępczości lub cyberataków.

Czym jest cyberbezpieczeństwo?

02 Brak jest standardowej, powszechnie uznawanej definicji cyberbezpieczeństwa[1]. Ogólnie rzecz ujmując, są to wszystkie zabezpieczenia i środki przyjęte w celu ochrony systemów informacyjnych i ich użytkowników przed nieuprawnionym dostępem, atakiem lub szkodą, tak aby zapewnić poufność, integralność i dostępność informacji.

03 Na cyberbezpieczeństwo składa się zapobieganie cyberincydentom, ich wykrywanie, reagowanie na nie oraz przywracanie działalności po takich incydentach. Incydenty mogą być wywoływane umyślnie lub nieumyślne i obejmują np. niezamierzone ujawnienie informacji, ataki na przedsiębiorstwa i infrastrukturę krytyczną, kradzieże danych osobowych, a nawet zakłócanie przebiegu procesów demokratycznych. Mogą one wywierać istotne skutki na osoby fizyczne, organizacje i społeczności.

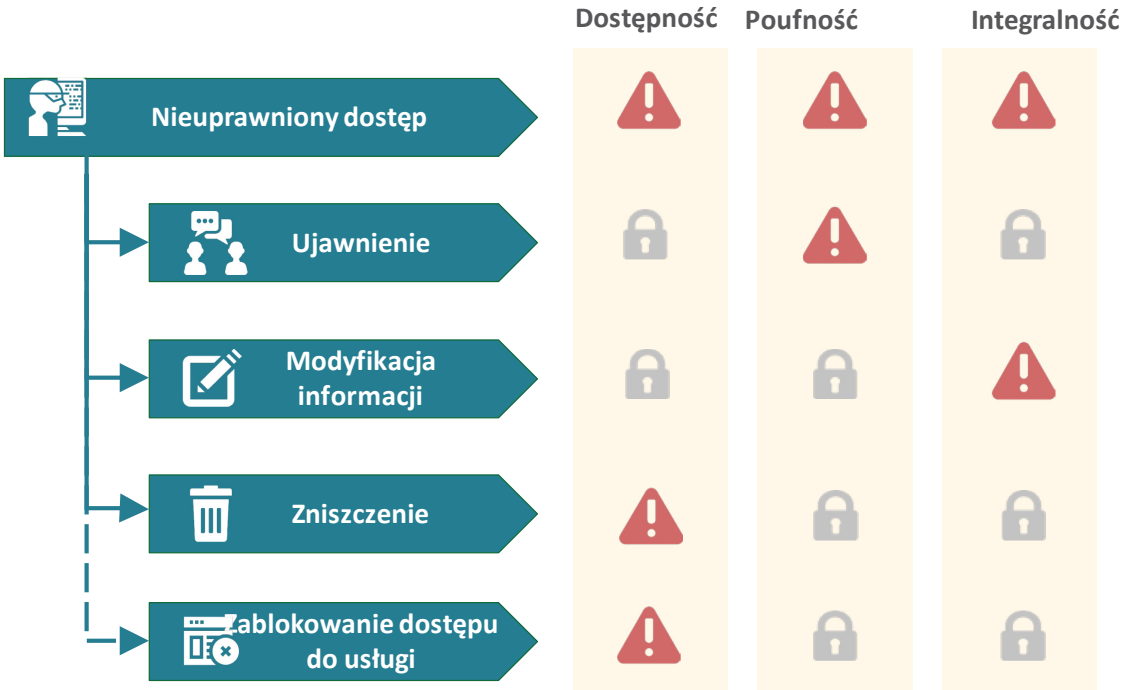
04 Jako termin stosowany w unijnych kręgach politycznych cyberbezpieczeństwo nie odnosi się wyłącznie do bezpieczeństwa sieci i informacji. Dotyczy wszelkich nielegalnych działań prowadzonych z wykorzystaniem technologii cyfrowych w cyberprzestrzeni, a zatem cyberprzestępstw takich jak uruchamianie ataków wirusów komputerowych czy oszustwa związane z płatnościami bezgotówkowymi. Niekiedy przedmiotem tych przestępstw jest zarówno funkcjonowanie samych systemów, jak i nielegalne treści, jak w przypadku rozpowszechniania w sieci materiałów prezentujących seksualne wykorzystywanie dziecka. Cyberbezpieczeństwo może się również odnosić do kampanii dezinformacyjnych mających wypływać na debaty w sieci oraz podejrzewanych przypadków zakłócania przebiegu wyborów. Ponadto Europol zwraca uwagę na łączenie zjawisk cyberprzestępczości i terroryzmu[2].

05 Za cyberincydenty odpowiadają różne rodzaje podmiotów – w tym państwa, grupy przestępcze i haktywiści – powodowanych różnymi motywami. Konsekwencje

tych incydentów są odczuwane na szczeblu krajowym, europejskim, a nawet globalnym. Niemniej niematerialny i w dużej mierze transgraniczny charakter internetu oraz wykorzystywane narzędzia i taktyki często utrudniają wykrycie sprawcy ataku (tzw. „problem przypisania odpowiedzialności").

06 Można wyodrębnić różne kategorie zagrożeń dla cyberbezpieczeństwa w zależności od tego, w jaki sposób wpływają one na dane – czy chodzi o ujawnienie, modyfikację, zniszczenie danych lub uniemożliwienie do nich dostępu – oraz tego, jakie podstawowe zasady dotyczące bezpieczeństwa zostały naruszone, jak pokazano na ***rys. 1*** poniżej. Niektóre przykłady ataków przedstawiono natomiast w ***ramce 1***. W miarę jak strategie ataków na systemy informatyczne stają się coraz bardziej zaawansowane, spada skuteczność mechanizmów obrony[3].

Rys. 1 – Rodzaje zagrożeń i zasady bezpieczeństwa naruszane w wyniku tych zagrożeń



Źródło: Europejski Trybunał Obrachunkowy, opracowanie na podstawie badania Parlamentu Europejskiego[4]. Kłódka oznacza brak oddziaływania na bezpieczeństwo; wykrzyknik oznacza zagrożenie dla bezpieczeństwa.

Ramka 1

Rodzaje cyberataków

Wraz z podłączeniem każdego nowego urządzenia do sieci lub połączeniem go z innymi urządzeniami zwiększa się tak zwana „płaszczyzna ataku". Gwałtownemu rozwojowi internetu rzeczy, przetwarzania w chmurze, dużych zbiorów danych i cyfryzacji przemysłu towarzyszy coraz większe narażenie na ataki, umożliwiające podmiotom działającym w złej wierze dosięgnięcie coraz większej liczby ofiar. Zróżnicowanie i coraz bardziej zaawansowany charakter cyberataków sprawiają, że nadążenie za rozwojem sytuacji staje się szczególnie trudne[5].

Złośliwe oprogramowanie ma na celu wyrządzenie szkody w urządzeniach lub sieciach. Może obejmować wirusy komputerowe, trojany, oprogramowanie typu ransomware, robaki komputerowe, oprogramowanie reklamowe i szpiegujące. Działanie **oprogramowania typu ransomware** polega na szyfrowaniu danych, tak aby uniemożliwić użytkownikom dostęp do plików do momentu, aż zostanie opłacony okup (ang. *ransom*), zazwyczaj w kryptowalucie, albo użytkownicy wykonają określone działanie. Zgodnie z danymi Europolu ataki typu ransomware są ogólnie najpowszechniejszym typem ataków, a liczba rodzajów takiego oprogramowania gwałtownie wzrosła w ostatnich latach. Coraz powszechniejsze stają się ponadto **rozproszone ataki typu „odmowa usługi"**, które uniemożliwiają dostęp do usług i zasobów, zalewając systemy ogromną ilością zapytań, których nie sposób obsłużyć. W 2017 r. niemal jedna trzecia podmiotów musiała stawić czoła atakom tego rodzaju[6].

Użytkownicy mogą paść ofiarą manipulacji i nieświadomie wykonać określoną czynność lub ujawnić poufne informacje. Takie oszustwa mogą być wykorzystywane do celów kradzieży danych lub cyberszpiegostwa i są znane pod nazwą **manipulacji z zakresu inżynierii społecznej**. Istnieją różne sposoby przeprowadzania tego rodzaju ataków. Jedną z powszechnie stosowanych metod jest **phishing**, polegający na przesyłaniu pocztą elektroniczną wiadomości sprawiających wrażenie, że pochodzą z wiarygodnych źródeł, tak aby skłonić użytkowników do ujawnienia informacji lub kliknięcia na łącza instalujące w urządzeniu złośliwe oprogramowanie. Ponad połowa państw członkowskich zgłosiła prowadzenie dochodzeń dotyczących ataków sieciowych[7].

Do najbardziej szkodliwych rodzajów zagrożeń należą **zaawansowane, trwałe zagrożenia** (ang. *advanced persistent threat* – APT). Podmioty dopuszczające się takich zaawansowanych ataków prowadzą długoterminowe monitorowanie i kradzież danych, przy czym niekiedy dążą również do wywołania zniszczeń. Atak jest tak pomyślany, by pozostać niewidocznym i niewykrytym przez możliwie jak najdłuższy okres. Ataki typu APT są często powiązane z określonymi państwami i ukierunkowane na szczególnie newralgiczne dziedziny, takie jak technologia, obronność i infrastruktura krytyczna. Cyberszpiegostwo ma odpowiadać za co najmniej jedną czwartą wszystkich cyberincydentów i większość związanych z nimi kosztów[8].

Na ile poważny jest problem cyberbezpieczeństwa?

07 Trudno zmierzyć jest wpływ niedostatecznego przygotowania na cyberataki ze względu na brak wiarygodnych danych. Gospodarcze skutki cyberprzestępczości zwiększyły się pięciokrotnie w latach 2013–2017[9]. Dotknęła ona zarówno rządy, jak i przedsiębiorstwa – i te małe, i duże. Znajduje to odbicie w przewidywanym wzroście składek na ubezpieczenia w dziedzinie cyberbezpieczeństwa, z 3 mld euro w 2018 r. do 8,9 mld euro w 2020 r.

08 Podczas gdy finansowe skutki cyberataków stają się coraz bardziej odczuwalne, istnieje zatrważająca rozbieżność między kosztem przeprowadzenia ataku oraz kosztami zapobiegania, wykrywania i usuwania szkód. Przykładowo przeprowadzenie rozproszonego ataku typu „odmowa usługi" może kosztować jedynie 15 euro miesięcznie, a tymczasem straty poniesione przez przedsiębiorstwa będące ofiarą ataku – włączywszy w to szkody wizerunkowe – są znacznie większe[10].

09 Choć 80% europejskich przedsiębiorstw spotkało się z co najmniej jednym incydentem w dziedzinie cyberbezpieczeństwa w 2016 r.[11], świadomość istnienia zagrożeń jest wciąż niepokojąco niska. Wśród przedsiębiorstw w UE 69% nie posiada żadnej wiedzy na temat własnego narażenia na cyberzagrożenia lub posiada taką wiedzę jedynie w podstawowym zakresie[12], a 60% nigdy nie szacowało potencjalnych strat finansowych[13]. Ponadto jak wynika z globalnego badania ankietowego, jedna trzecia podmiotów zapłaciłaby raczej hakerom okup niż inwestowała w bezpieczeństwo informacji[14].

10 Globalne ataki wywołane przez oprogramowanie typu ransomware Wannacry oraz oprogramowanie usuwające dane NotPetya łącznie dotknęły ponad 320 000 ofiar w około 150 krajach[15]. Incydenty te sprawiły, że globalnie uzmysłowiono sobie, jakim zagrożeniem są cyberataki. Przełożyło się na to na bardziej zdecydowane dążenie, by uwzględnić cyberbezpieczeństwo w głównym nurcie polityki. Co więcej, obecnie 86% obywateli UE uważa, że ryzyko zostania ofiarą cyberprzestępstwa rośnie[16].

Działania UE w zakresie cyberbezpieczeństwa

11 W 2001 r. UE zyskała status obserwatora w komitecie Konwencji Rady Europy o cyberprzestępczości (konwencji budapesztańskiej)[17]. Od tamtego czasu Unia dążyła, za sprawą prowadzonej polityki, prawodawstwa i wydatkowania środków, do zwiększenia własnej cyberodporności. Wobec rosnącej liczby znacznych cyberataków i cyberincydentów działania te nabierają od 2013 r. jeszcze większego tempa, jak

pokazano na *rys. 2*. Jednocześnie państwa członkowskie przyjęły pierwsze krajowe strategie w zakresie cyberbezpieczeństwa (a niektóre z nich zdążyły je już zaktualizować).

12 Główne unijne podmioty odpowiedzialne za cyberbezpieczeństwo opisano w *ramce 2* i *załączniku I*.

Ramka 2

Zaangażowane podmioty

Komisja Europejska dąży do zwiększenia zdolności w zakresie cyberbezpieczeństwa oraz zacieśnienia współpracy i wzmocnienia roli UE w tej dziedzinie, a także do włączenia tej kwestii do innych strategii politycznych UE. Głównymi dyrekcjami generalnymi odpowiedzialnymi za politykę w zakresie cyberbezpieczeństwa są DG **CNECT** (cyberbezpieczeństwo) oraz DG **HOME** (cyberprzestępczość), do których kompetencji należą odpowiednio jednolity rynek cyfrowy i unia bezpieczeństwa. DG **DIGIT** jest odpowiedzialna natomiast za bezpieczeństwo informatyczne systemów własnych Komisji.

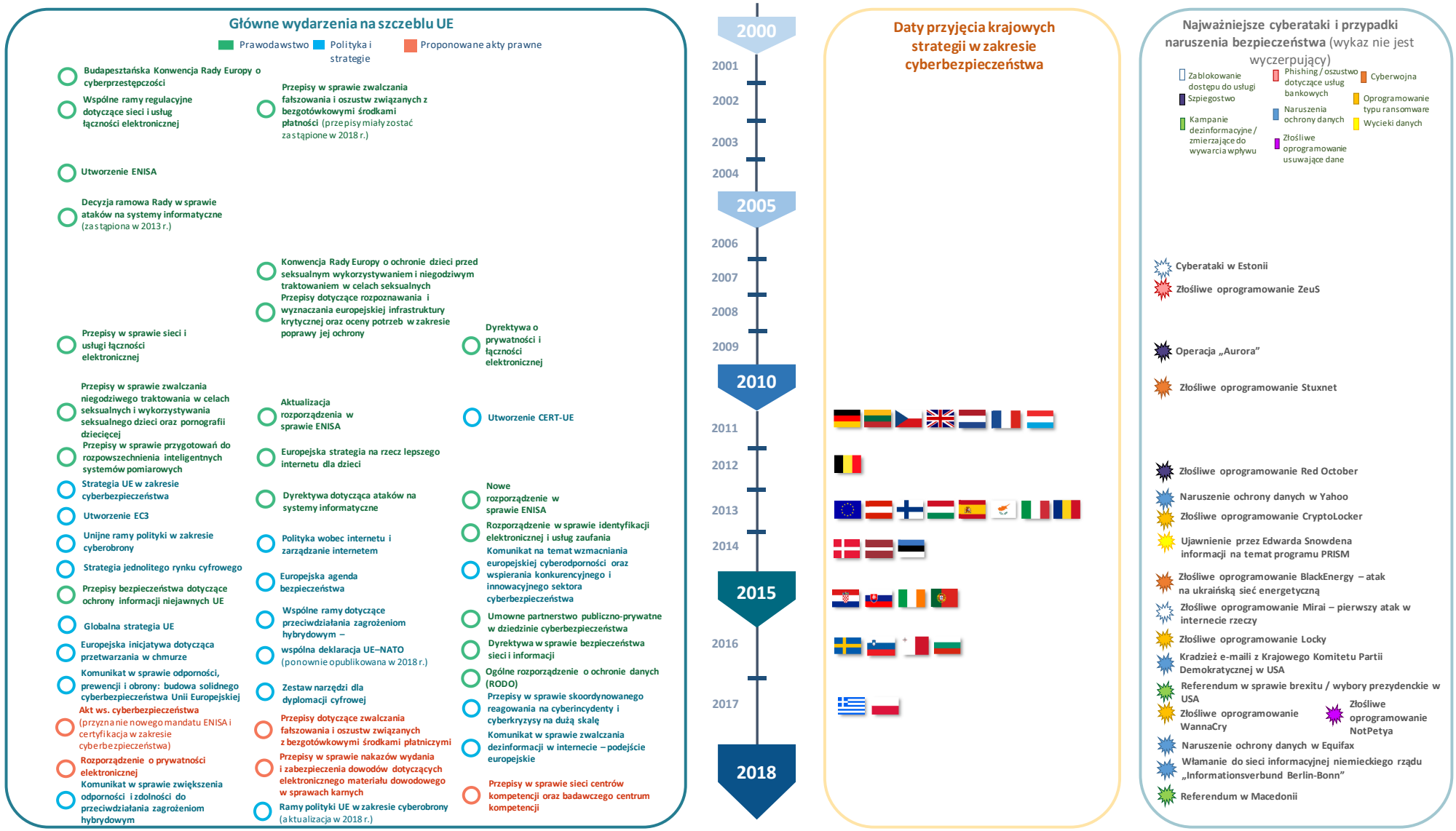
W realizowaniu tych zadań Komisję wspiera szereg agencji UE, w szczególności Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (**ENISA**), pełniąca funkcję unijnej agencji do spraw cyberbezpieczeństwa, głównego ciała doradczego działającego na rzecz kształtowania polityki, budowania zdolności i rozpowszechniania wiedzy. Działające przy Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością (**EC3**) utworzono w celu usprawnienia reakcji unijnych organów ścigania na przypadki cyberprzestępczości. W obrębie Komisji działa ponadto zespół reagowania na incydenty komputerowe (**CERT-UE**), wspierający wszystkie unijne instytucje, organy i agencje.

Europejska Służba Działań Zewnętrznych (ESDZ) zapewnia przywództwo w dziedzinie cyberobrony, cyberdyplomacji i komunikacji strategicznej, a w jej strukturach działają ośrodki wywiadowcze i analityczne. Celem **Europejskiej Agencji Obrony** jest budowanie zdolności w zakresie cyberobrony.

Państwa członkowskie są w pierwszym rzędzie odpowiedzialne za własne cyberbezpieczeństwo, a na szczeblu UE podejmują działania za pośrednictwem **Rady**, w ramach której działają liczne organy zajmujące się koordynacją działań i dzieleniem się informacjami (w tym Horyzontalna Grupa Robocza ds. Cyberprzestrzeni). **Parlament Europejski** pełni funkcję współprawodawcy.

Organizacje sektora prywatnego, w tym podmioty branżowe, organy zarządzające internetem i środowiska akademickie są partnerem w ramach prowadzonych działań i przyczyniają się do opracowywania i wdrażania polityki – w tym za pośrednictwem **umownego partnerstwa publiczno-prywatnego**.

Rys. 2 – Przyspieszenie działań w zakresie opracowywania inicjatyw politycznych i prawodawstwa (stan na 31 grudnia 2018 r.)



Źródło: Europejski Trybunał Obrachunkowy.

Inicjatywy polityczne

13 Unijne cyberśrodowisko jest złożone i wielowarstwowe. Obejmuje cały wachlarz obszarów polityki wewnętrznej, takich jak wymiar sprawiedliwości i sprawy wewnętrzne, jednolity rynek cyfrowy i strategie dotyczące badań naukowych. W polityce zewnętrznej kwestie dotyczące cyberbezpieczeństwa pojawiają się w dyplomacji i w coraz większym stopniu stanowią element kształtującej się unijnej polityki bezpieczeństwa.

14 Podstawą unijnej polityki w tej dziedzinie jest **strategia w zakresie cyberbezpieczeństwa z 2013 r.**[18] Ambicją strategii jest uczynienie środowiska cyfrowego w UE najbezpieczniejszym na świecie, a jednocześnie zapewnienie ochrony podstawowych wartości i wolności. Przyświeca jej pięć podstawowych celów: (i) zwiększenie odporności na cyberzagrożenia; (ii) ograniczenie cyberprzestępczości; (iii) opracowanie polityki obronnej i zdolności w dziedzinie cyberbezpieczeństwa; (iv) rozbudowa zasobów przemysłowych i technologicznych w zakresie cyberbezpieczeństwa; (v) ustanowienie międzynarodowej polityki w zakresie cyberprzestrzeni zgodnej z podstawowymi wartościami UE.

15 Strategia w zakresie cyberbezpieczeństwa jest powiązana z trzema później przyjętymi strategiami:

— Celem **Europejskiej agendy bezpieczeństwa** z 2015 r. jest usprawnienie ścigania przestępstw i reakcji wymiaru sprawiedliwości na przypadki cyberprzestępczości, zwłaszcza przez aktualizację obowiązujących strategii politycznych i przepisów[19]. Ma ona również pozwolić rozpoznać przeszkody dla prowadzenia postępowań karnych dotyczących cyberprzestępczości oraz ułatwić budowanie zdolności w tej dziedzinie.

— **Strategia jednolitego rynku cyfrowego**[20] z 2015 r. ma zapewnić lepszy dostęp do cyfrowych towarów i usług przez ustanowienie odpowiednich warunków, które pozwolą maksymalnie wykorzystać potencjał wzrostu gospodarki cyfrowej. Wzmocnienie bezpieczeństwa i zwiększenia zaufania online oraz cyfrowe włączenie obywateli mają w tym względzie zasadnicze znaczenie.

— **Globalna strategia**[21] UE z 2016 r. ma na celu umocnienie pozycji UE na świecie. Cyberbezpieczeństwo stanowi jeden z podstawowych filarów strategii. Strategia przewiduje odnowione zaangażowanie w kwestie dotyczące cyberprzestrzeni, współpracę z kluczowymi partnerami oraz dążenie do tego, by uwzględnić

problemy dotyczące cyberprzestrzeni we wszystkich obszarach polityki, a także dać odpór dezinformacji za pomocą komunikacji strategicznej.

16 W ostatnich latach, w miarę jak cyberprzestrzeń stawała się coraz bardziej zmilitaryzowana[22] i w coraz większym stopniu wykorzystywano ją w działaniach wojennych[23], zaczęto postrzegać ją jako piątą sferę prowadzenia wojny[24]. Cyberobrona ma chronić w cyberprzestrzeni systemy, sieci i infrastrukturę krytyczną przed atakami ze strony sił wojskowych lub za pomocą innych środków. **Ramy polityki w dziedzinie cyberobrony** przyjęto w 2014 r. i zaktualizowano w 2018 r.[25] W toku aktualizacji z 2018 r. wskazano sześć priorytetów, obejmujących rozwój zdolności w zakresie cyberobrony oraz ochronę sieci komunikacyjnych i informacyjnych wspólnej polityki bezpieczeństwa i obrony UE. Cyberobrona stanowi również część ram stałej współpracy strukturalnej (PESCO) oraz współpracy między UE i NATO.

17 W **unijnych wspólnych ramach dotyczących przeciwdziałania zagrożeniom hybrydowym** z 2016 r. podjęto kwestię cyberzagrożeń zarówno dla infrastruktury krytycznej, jak i dla indywidualnych użytkowników, zwracając przy tym uwagę, że cyberataki mogą przyjąć postać kampanii dezinformacyjnych w mediach społecznościowych[26]. W dokumencie zwrócono również uwagę na konieczność podniesienia poziomu świadomości i zacieśnienia współpracy między UE i NATO, co znalazło konkretny wyraz we wspólnych deklaracjach UE i NATO z 2016 r. i 2018 r.[27]

18 W 2017 r. Komisja przedstawiła nowy pakiet w dziedzinie cyberbezpieczeństwa w związku z coraz pilniejszą potrzebą zapewnienia ochrony cyfrowej. Pakiet obejmował nowy komunikat Komisji, aktualizujący strategię w zakresie cyberbezpieczeństwa z 2013 r.[28] i plan działania na rzecz szybkiej i skoordynowanej reakcji na wypadek dużego ataku oraz niezwłocznego wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji[29]. Ponadto w pakiecie znalazł się szereg wniosków ustawodawczych (zob. pkt ***22***).

Prawodawstwo

19 Od 2002 r. przyjęto szereg przepisów prawnych, które w mniejszym lub większym stopniu odnosiły się do cyberbezpieczeństwa.

20 Głównym filarem strategii w zakresie cyberbezpieczeństwa z 2013 r. i zasadniczym aktem prawnym w tej dziedzinie jest **dyrektywa w sprawie bezpieczeństwa sieci i informacji**[30] z 2016 r., będąca pierwszym ogólnounijnym aktem

prawnym w dziedzinie cyberbezpieczeństwa. Dyrektywa, której termin transpozycji upłynął w maju 2018 r., ma pozwolić państwom członkowskim na osiągnięcie minimalnego jednorodnego poziomu zdolności. W tym celu nakłada na te państwa obowiązek przyjęcia krajowych strategii w zakresie bezpieczeństwa sieci i informacji oraz utworzenia pojedynczych punktów kontaktowych i zespołów reagowania na incydenty bezpieczeństwa komputerowego (zwanych CSIRT)[31]. W dyrektywie ustanowiono ponadto wymogi dotyczące bezpieczeństwa i zgłaszania incydentów obowiązujące operatorów usług kluczowych w sektorach o krytycznym znaczeniu oraz dostawców usług cyfrowych.

21 Jednocześnie w 2016 r. weszło w życie **ogólne rozporządzenie o ochronie danych**[32] (RODO), a jego przepisy obowiązują od maja 2018 r. Celem rozporządzenia jest zapewnienie ochrony danych osobowych obywateli UE dzięki ustanowieniu zasad regulujących przetwarzanie i rozpowszechnianie tych danych. Przepisy rozporządzenia przyznają osobom, których dane dotyczą, pewne prawa, a na administratorów danych (dostawców usług cyfrowych) nakładają określone obowiązki dotyczące wykorzystania i przekazywania informacji. Nakładają również obowiązki w zakresie informowania w razie naruszenia przepisów i w niektórych przypadkach przewidują nakładanie kar finansowych. Na *rys. 3* pokazano, jak dyrektywa w sprawie bezpieczeństwa sieci i informacji oraz RODO uzupełniają się wzajemnie w zakresie własnych celów – wzmocnienia cyberbezpieczeństwa i zagwarantowania ochrony danych.

22 Omawiane obecnie projekty przepisów prawnych obejmują wniosek dotyczący aktu ws. cyberbezpieczeństwa, mający na celu wzmocnienie ENISA i ustanowienie ogólnounijnego mechanizmu certyfikacji[33], wniosek dotyczący rozporządzenia w sprawie nakazów wydania i zabezpieczenia dowodów w odniesieniu do elektronicznego materiału dowodowego[34] oraz wniosek dotyczący dyrektywy w sprawie elektronicznego materiału dowodowego[35]. Wniosek z 2018 r. dotyczący Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieci krajowych ośrodków koordynacji (zwanych dalej „siecią centrów kompetencji w dziedzinie cyberbezpieczeństwa oraz badawczym centrum kompetencji") stanowi część pakietu z 2017 r. dotyczącego cyberbezpieczeństwa[36].

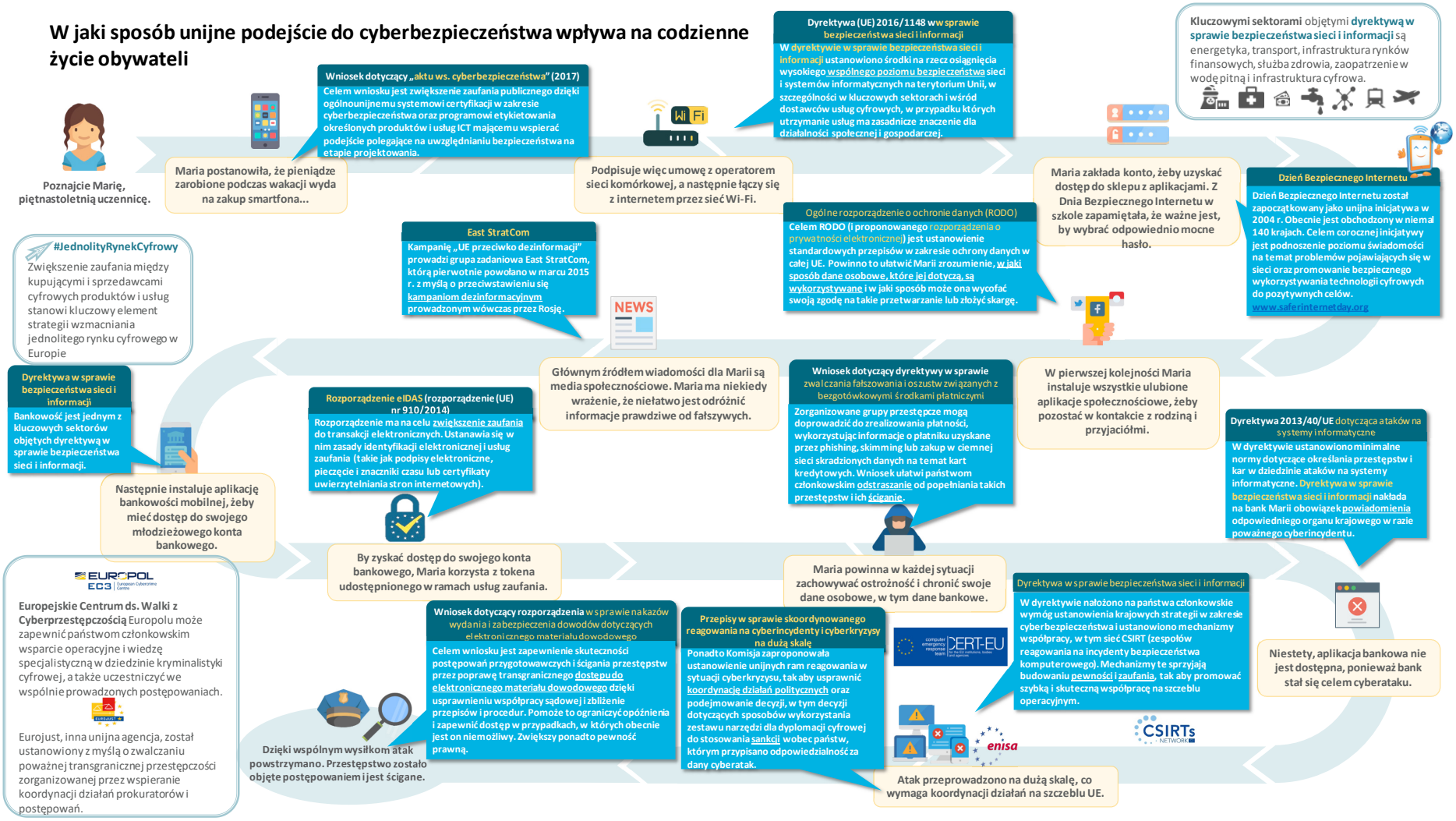
23 Zarysowanie ogólnego obrazu polityki i ram prawnych odnoszących się do cyberbezpieczeństwa oraz tego, w jaki sposób wpływają one na nasze codzienne życie, może być zadaniem trudnym.

24 Na *rys. 4* usiłowano przedstawić, jak różne akty prawne i inne inicjatywy wpływają na życie hipotetycznego unijnego obywatela.

Rys. 3 – W jaki sposób RODO i dyrektywa w sprawie bezpieczeństwa sieci i informacji uzupełniają się wzajemnie

Źródło: Europejski Trybunał Obrachunkowy.

Rys. 4 – W jaki sposób unijne podejście do cyberbezpieczeństwa wpływa na codzienne życie obywateli



Źródło: Europejski Trybunał Obrachunkowy.

Tworzenie ram politycznych i prawnych

25 Unijne cyberśrodowisko jest złożone i wielowarstwowe. Uczestniczy w nim wiele zainteresowanych stron (zob. ***załącznik I***). Koordynowanie wszystkich tych rozbieżnych elementów stanowi spore wyzwanie. Od 2013 r. podejmuje się wspólne wysiłki na rzecz zapewnienia spójności w dziedzinie cyberbezpieczeństwa w UE[37].

Wyzwanie 1 – Rzetelna ocena i rozliczalność

26 Jak zauważyła Komisja, prześledzenie relacji przyczynowo-skutkowej między strategią z 2013 r. i zaobserwowanymi zmianami jest trudne. Cele strategii z 2013 r. były sformułowane bardzo ogólnie i „raczej wyrażały wizję niż określały mierzalne cele”[38]. Wobec braku mierzalnych celów opracowanie działań dostosowanych do tych szerokich założeń stanowi wyzwanie. Zaktualizowane ramy polityki w zakresie cyberobrony z 2018 r. mają doprowadzić do ustanowienia celów określających minimalny zamierzony poziom cyberbezpieczeństwa i zaufania. Niemniej będą one ograniczone do cyberobrony; cele określające pożądany poziom odporności dla całej UE nie zostały wprowadzone.

27 Pomiary wyników przeprowadza się rzadko i dotychczas ocenie poddano jedynie niewielką liczbę obszarów polityki[39]. Wynika to po części z faktu, że wiele spośród wspomnianych działań – ustawodawczych i innych – zrealizowano niedawno, co utrudnia przeprowadzenie pełnej oceny oddziaływania. Trudność polega na określeniu rzetelnych kryteriów oceny, które pozwolą zmierzyć to oddziaływanie. Ponadto ogólnie rzecz ujmując, przeprowadzanie rygorystycznych ocen nie stało się jeszcze powszechną praktyką w dziedzinie cyberbezpieczeństwa. Konieczne jest zatem przyjęcie kultury organizacyjnej ukierunkowanej na wyniki i powiązanej z ugruntowanymi praktykami oceny oraz ujednoliconą sprawozdawczością. Obecny mandat ENISA nie obejmuje oceny i monitorowania sytuacji UE w zakresie cyberbezpieczeństwa ani gotowości w tej dziedzinie.

28 Możliwość kształtowania polityki w oparciu o dowody zależy od dostępności wiarygodnych danych oraz danych statystycznych, które ułatwiają monitorowanie i analizowanie tendencji i potrzeb. Brak obowiązkowego wspólnego systemu monitorowania przekłada się na niedostatek wiarygodnych danych. Wskaźniki często nie są dostępne, a przy tym trudno je zdefiniować[40]. W pewnych obszarach opracowano jednak szczegółowe wskaźniki pomiarowe, tak jak w przypadku cyklu polityki UE mającego na celu zwalczanie poważnej i zorganizowanej przestępczości.

29 Niewiele państw członkowskich regularnie gromadzi oficjalne dane na temat kwestii dotyczących cyberprzestrzeni, co utrudnia ewentualne porównania. UE dotychczas w niewielkim stopniu wskazywała na potrzebę zapewnienia skonsolidowanych danych statystycznych na szczeblu europejskim[41]. Niewiele jest też niezależnych ogólnounijnych analiz obejmujących kluczowe zagadnienia takie jak[42]: ekonomiczny wymiar cyberbezpieczeństwa, w tym aspekty behawioralne (niedostosowanie zachęt, asymetria informacyjna); analiza oddziaływania błędów popełnianych w dziedzinie cyberbezpieczeństwa oraz cyberprzestępczości; dane statystyczne na poziomie makro dotyczące tendencji w cyberprzestrzeni i oczekiwanych wyzwań; najlepsze rozwiązania pozwalające radzić sobie zagrożeniami.

30 Wobec braku szczegółowych celów i niewielkiej ilości wiarygodnych danych oraz jasno zdefiniowanych wskaźników dotychczasowa ocena postępów osiągniętych dzięki strategii była w dużej mierze jakościowa. W sprawozdaniach z postępów często opisuje się zrealizowane działania lub osiągnięte cele pośrednie, lecz nie towarzyszy temu rzetelny pomiar rezultatów. Ponadto nie określono jeszcze poziomów wyjściowych w odniesieniu do odporności systemów. Co więcej, ze względu na brak ustalonej definicji cyberprzestępstwa, znalezienie odpowiednich ogólnoeuropejskich wskaźników, które ułatwiałyby monitorowanie i ocenę, jest niemal niemożliwe.

31 Niezależny nadzór nad wdrażaniem polityki w zakresie cyberbezpieczeństwa jest różny w poszczególnych państwach członkowskich. Trybunał rozesłał do krajowych organów kontroli ankietę dotyczącą doświadczeń z prowadzenia kontroli w tym obszarze. Połowa wszystkich respondentów[43] nigdy nie przeprowadzała takich kontroli. Te podmioty natomiast, które takie kontrole prowadziły, koncentrowały się głównie na: zarządzaniu informacjami; ochronie infrastruktury krytycznej; wymianie informacji i koordynowaniu działań między głównymi zainteresowanymi stronami; gotowości na wypadek incydentów, powiadamianiu o incydentach i reagowaniu na nie. Wśród tematów w mniejszym stopniu objętych kontrolami znalazły się działania na rzecz rozpowszechniania wiedzy i luka w umiejętnościach cyfrowych. Rezultaty tych kontroli lub ocen nie zawsze były udostępniane publicznie ze względów dotyczących bezpieczeństwa publicznego. Wykaz sprawozdań z kontroli opublikowanych przez krajowe organy kontroli przedstawiono w ***załączniku III***.

32 Jako największe wyzwania związane z kontrolą działań państwa w tej dziedzinie wskazywano ograniczenia dotyczące umiejętności powiązanych z cyberprzestrzenią (zob. również pkt ***82–90***) oraz trudności w ocenie postępów w dziedzinie cyberbezpieczeństwa.

Wyzwanie 2 – Zaradzenie lukom w unijnych przepisach prawnych oraz niejednorodnej transpozycji tych przepisów

33 Tempo pojawiania się nowych technologii i zagrożeń daleko przerasta tempo opracowywania i wdrażania unijnego prawodawstwa. Unijne procedury nie zostały opracowane z myślą o realiach ery cyfrowej. W związku z tym kluczowe znaczenie ma ustanowienie innowacyjnych i elastycznych procedur pozwalających wprowadzić adekwatne ramy polityczne i prawne[44], tak aby lepiej przewidywać i kształtować przyszłość cyfrową[45].

34 Mimo dążeń do zapewnienia większej spójności ramy legislacyjne odnoszące się do cyberbezpieczeństwa pozostają niekompletne (pewne przykłady podano w ***tabeli 1***). Rozdrobnienie i luki utrudniają osiągnięcie ogólnych celów polityki i prowadzą do niewydajnego wykorzystania zasobów. Luki wskazane w ocenie strategicznej Komisji dotyczyły takich kwestii jak internet rzeczy i równomierne rozłożenie odpowiedzialności między użytkowników i dostawców produktów cyfrowych, a także części problemów, które nie zostały rozwiązane na gruncie dyrektywy w sprawie bezpieczeństwa sieci i informacji. Proponowany akt ws. cyberbezpieczeństwa ma zaradzić tym trudnościom dzięki promowaniu bezpieczeństwa na etapie projektowania w ramach ogólnounijnego systemu certyfikacji. Niektóre z zainteresowanych stron stoją na stanowisku, że wciąż brak jest jasno określonej branżowej polityki dotyczącej cyberprzestrzeni oraz wspólnego podejścia do cyberszpiegostwa[46].

Tabela 1 – Luki i niejednorodna transpozycja ram legislacyjnych (wykaz niewyczerpujący)

Jednolity rynek cyfrowy	o Obowiązująca dyrektywa w sprawie sprzedaży towarów konsumpcyjnych nie uwzględnia cyberbezpieczeństwa. Proponowane dyrektywy w sprawie treści cyfrowych[47] i sprzedaży internetowej[48] mają wyeliminować tę lukę. o Ramy prawne dotyczące obowiązków w zakresie staranności, które obowiązują w państwach członkowskich UE, mają ograniczony zakres i są zróżnicowane, co skutkuje niepewnością prawną i trudnością w korzystaniu ze środków ochrony prawnej[49]. o Polityki dotyczące ujawniania luk w oprogramowaniu opracowywane są w różnym tempie w poszczególnych państwach członkowskich, przy czym brak jest nadrzędnych ram prawnych na szczeblu UE, które umożliwiałyby przyjęcie skoordynowanego podejścia[50].
Zwiększenie bezpieczeństwa sieci i informacji	o Państwa członkowskie mają możliwość objęcia przepisami sektorów nieuwzględnionych w dyrektywie w sprawie bezpieczeństwa sieci i informacji[51]. Branża hotelarska, która nie jest objęta przepisami dyrektywy, może być wykorzystywana w zróżnicowanej działalności przestępczej, w tym do nielegalnego obrotu środkami odurzającymi, handlu ludźmi i nielegalnej migracji[52].
Walka z cyberprzestępczością	o Wiele państw członkowskich nie zdefiniowało jeszcze w przepisach krajowych pojęcia elektronicznego materiału dowodowego[53] (zob. również pkt ***22***). o Obowiązująca decyzja ramowa w sprawie oszustw związanych z płatnościami bezgotówkowymi nie uwzględnia w sposób jednoznaczny narzędzi dokonywania płatności bezgotówkowych takich jak waluty wirtualne, pieniądz elektroniczny i płatności mobilne ani nie obejmuje czynów takich jak phishing, przechwytywanie danych kart płatniczych (skimming) oraz posiadanie i udostępnianie informacji na temat płatnika[54]. o Dyrektywa w sprawie ataków na systemy informatyczne nie odnosi się bezpośrednio do nielegalnego pozyskiwania danych z wewnątrz organizacji (np. cyberszpiegostwa), co utrudnia ściganie przestępstw[55]. o W następstwie wyroku Trybunału Sprawiedliwości Unii Europejskiej w sprawie przechowywania danych[56] poszczególne państwa członkowskie przyjęły różne podejście do stosowania ram prawnych, co utrudnia ściganie przestępstw i mogło skutkować utratą poszlak śledczych i osłabieniem skutecznego ścigania działalności przestępczej w sieci[57].

Źródło: Europejski Trybunał Obrachunkowy.

35 Stosowanie niektórych elementów prawodawstwa pozostaje nieobowiązkowe zarówno dla organów krajowych, jak i operatorów z sektora prywatnego. Przykładowo, w odniesieniu do grupy współpracy ocena krajowych strategii dotyczących bezpieczeństwa sieci i systemów informatycznych oraz skuteczności CSIRT jest nieobowiązkowa. Ponadto zgodnie z proponowanym w akcie ws. cyberbezpieczeństwa systemem certyfikacji stosowanie certyfikacji do produktów i usług ICT będzie dobrowolne.

36 W UE cyberbezpieczeństwo należy do kompetencji państw członkowskich. Niemniej UE powinna odegrać kluczową rolę w tej dziedzinie, zapewniając warunki dla zwiększenia zdolności państw członkowskich, dla wzajemnej współpracy tych państw oraz budowania zaufania. Zważywszy jednak na ogromne rozbieżności między poszczególnymi państwami członkowskimi pod względem potencjału i zaangażowania[58] przekazywanie informacji szczególnie chronionych (odnoszących się do bezpieczeństwa narodowego) pozostanie dobrowolne.

37 Niespójna transpozycja przepisów unijnego prawa w państwach członkowskich może poskutkować brakiem spójności prawnej i operacyjnej oraz sprawić, że nie będzie można wykorzystać w pełni potencjału tkwiącego w prawodawstwie. Przykładowo, poszczególne państwa członkowskie odmiennie interpretują to, w jaki sposób należy przeprowadzać kontrole produktów podwójnego zastosowania[59]. W rezultacie pewne przedsiębiorstwa z siedzibą UE mogą eksportować technologie i usługi, które następnie mogą być wykorzystywane do cyberinwigilacji i naruszeń praw człowieka za sprawą cenzury i przechwytywania przesyłanych danych. Parlament Europejski wyraził swoje zaniepokojenie w tej kwestii[60].

38 Ponadto ochrona prywatności i wolności wypowiedzi wymaga dostosowanej reakcji ustawodawczej, tak aby zapewnić prawidłową równowagę między ochroną wartości podstawowych i osiągnięciem kluczowych celów UE w zakresie bezpieczeństwa. Przykładowo, w jaki sposób należy zapewnić pełne szyfrowanie transmisji, a jednocześnie w jak najlepszy sposób wspierać ściganie przestępstw? Czy też w jaki sposób można osiągnąć cele RODO, uwzględniając przy tym wynikające z rozporządzenia konsekwencje dla ogólnodostępnych informacji na temat rejestratorów nazw domen lub posiadaczy bloków adresów IP? W jaki sposób może to negatywnie wpłynąć na czynności dochodzeniowe w ramach ścigania przestępstw[61]?

39 Samo prawodawstwo nie wystarczy, by zagwarantować odporność. Choć celem dyrektywy w sprawie bezpieczeństwa sieci i informacji jest osiągnięcie wysokiego poziomu bezpieczeństwa w całej UE, jednoznacznie przewiduje ona minimalną – a nie

maksymalną – harmonizację[62]. W miarę jak będzie zmieniała się cyberprzestrzeń, pojawiać się będą nowe zagrożenia.

Kwestie do rozważenia – ramy polityczne

- Jakie kluczowe działania należy podjąć, aby skłonić decydentów politycznych i prawodawców do przejścia w większym stopniu na kulturę organizacyjną ukierunkowaną na wyniki w dziedzinie cyberbezpieczeństwa, co powinno obejmować opracowanie definicji ogólnej odporności?

- W jaki sposób badania naukowe mogą lepiej przyczyniać się do wytworzenia koniecznych danych i danych statystycznych, które umożliwią rzetelną ocenę?

- W jaki sposób można dostosować unijne procedury legislacyjne, tak aby były bardziej elastyczne i większym stopniu uwzględniały tempo zmian technologicznych i pojawiania się zagrożeń?

- W jaki sposób praktyka opracowywania wskaźników pomiarowych (wskaźników, poziomów docelowych) w ramach cyklu polityki UE mogłaby zostać dostosowana, rozwinięta i powielona w odniesieniu do całego obszaru cyberprzestępczości?

- Czego krajowe organy kontroli mogą wzajemnie się od siebie nauczyć, jeśli chodzi o podejście do kontrolowania strategii i działań w zakresie cyberbezpieczeństwa?

- Jakie niespójności w transpozycji i wdrażaniu unijnych ram prawnych osłabiają skuteczną reakcję na luki w zakresie cyberbezpieczeństwa i cyberprzestępczość? Jak państwa członkowskie i instytucje unijne mogłyby najlepiej zaradzić temu problemowi?

    - Czy kontrole wywozu cyfrowych towarów i usług skutecznie zapobiegają naruszeniom praw człowieka poza UE?

Finansowanie i wydatkowanie środków

40 UE ma ambicje, by stać się najbezpieczniejszym środowiskiem cyfrowym na świecie. Do osiągnięcia tego celu konieczne są znaczne wysiłki wszystkich zainteresowanych stron, a ponadto solidne podstawy finansowe i należyte zarządzanie finansami.

Wyzwanie 3 – Dostosowanie poziomów inwestycji do celów

Zwiększenie zakresu inwestycji

41 Łączne globalne wydatki w dziedzinie cyberbezpieczeństwa szacuje się na ok. 0,1% PKB. W Stanach Zjednoczonych[63] odsetek ten wynosi ok. 0,35% (w tym w sektorze prywatnym). Przewidziane w budżecie amerykańskiego rządu federalnego na 2019 r. wydatki na ten cel wynoszą ok. 0,1% PKB, tj. ok. 21 mld dolarów[64].

42 W porównaniu ze Stanami Zjednoczonymi wydatki w UE były niewielkie, rozdrobnione i nie realizowano ich w ramach skoordynowanych programów prowadzonych przez rządy. Trudno uzyskać rzetelne dane liczbowe, ale szacuje się, że ze środków publicznych na cyberbezpieczeństwo w UE każdego roku wydaje się od 1 do 2 mld euro[65]. W niektórych państwach członkowskich wydatki te wyrażone jako odsetek PKB są równe jednej dziesiątej (lub nawet mniej) wydatków amerykańskich[66]. UE i państwa członkowskie muszą wiedzieć, ile środków łącznie przeznaczają na ten cel, aby móc wyeliminować istniejące luki.

43 Trudno uzyskać całościowy ogląd sytuacji wobec braku przejrzystych danych, co wynika z przekrojowego charakteru zagadnienia cyberbezpieczeństwa oraz tego, że często nie sposób rozróżnić wydatków ogólnych w obszarze IT i wydatków na potrzeby cyberbezpieczeństwa[67]. Zrealizowane przez Trybunał badanie ankietowe potwierdziło, że trudno zdobyć wiarygodne dane statystyczne na temat wydatków zarówno w sektorze publicznym, jak i prywatnym. Trzy czwarte spośród krajowych organów kontroli poinformowało, że nie posiada żadnego scentralizowanego przeglądu wydatków publicznych związanych z cyberprzestrzenią, a ani jedno z państw członkowskich nie nakłada na podmioty publiczne obowiązku odrębnego zgłaszania wydatków na cyberbezpieczeństwo w planach finansowych.

44 Szczególnym wyzwaniem w tej dziedzinie jest zwiększenie publicznych i prywatnych inwestycji w europejskie przedsiębiorstwa z branży cyberbezpieczeństwa.

Środki publiczne są często dostępne na początkowym etapie, ale w mniejszym stopniu na potrzeby etapów wzrostu i ekspansji[68]. Istnieje wiele unijnych inicjatyw w zakresie finansowania, ale nie są one wykorzystywane, w dużej mierze ze względu na biurokrację[69]. Ogólnie rzecz ujmując, unijne przedsiębiorstwa z branży cyberbezpieczeństwa radzą sobie gorzej od podobnych podmiotów spoza UE – jest ich mniej, a środki, które udaje im się pozyskać, są średnio znacznie niższe[70]. Zapewnienie skutecznego ukierunkowania działań na przedsiębiorstwa typu start-up oraz zagwarantowanie im środków mają więc zasadnicze znaczenie dla osiągnięcia przez UE celów polityki cyfrowej.

Zwiększenie oddziaływania

45 Wyeliminowanie luki inwestycyjnej w gospodarce cyfrowej powinno przynieść korzystne wyniki. Przykładowo, pomimo mocnej pozycji unijnego sektora badań naukowych i innowacji osiągane rezultaty są w niewystarczającym stopniu objęte patentami, wprowadzane do obrotu lub wykorzystywane na szerszą skalę, tak by można było wzmocnić odporność, konkurencyjność i autonomię cyfrową[71]. Kwestia ta staje się szczególnie widoczna, jeśli porównać UE z jej konkurentami na scenie międzynarodowej. To niedostateczne wykorzystanie rezultatów spowodowane jest szeregiem czynników[72], w tym:

- brak spójnej transnarodowej strategii, która pozwoliłaby na szersze stosowanie podejścia, tak aby dostosować się do większych potrzeb cyfrowych UE w zakresie konkurencyjności i zwiększonej autonomii;
- długość łańcucha wartości, która sprawia, że opracowane narzędzie wkrótce staje się przestarzałe;
- brak trwałości, ponieważ projekty zazwyczaj kończą się rozwiązaniem zespołu projektowego i przerwaniem wsparcia, w tym brakiem aktualizacji i łatek do oprogramowania.

46 Wniosek Komisji dotyczący utworzenia sieci centrów kompetencji w zakresie cyberbezpieczeństwa oraz badawczego centrum kompetencji stanowi próbę przezwyciężenia rozdrobnienia w obszarze badań nad cyberbezpieczeństwem oraz pobudzenia inwestycji na dużą skalę[73]. Ogółem w całej Unii istnieje ok. 665 ośrodków wiedzy specjalistycznej.

Wyzwanie 4 – Jasny obraz wydatków z budżetu UE

47 Scentralizowany ogląd wydatkowania środków ma duże znaczenie dla przejrzystości i usprawnienia koordynacji. Bez takiej wiedzy decydentom trudno jest ocenić, czy wydatki odpowiadają potrzebom związanym z osiągnięciem priorytetowych celów.

48 Nie ma odrębnego budżetu przeznaczonego na finansowanie wydatków w ramach strategii w zakresie cyberbezpieczeństwa. Na szczeblu UE wydatki te są finansowane z budżetu ogólnego UE przy współfinansowaniu ze strony państw członkowskich. W przeprowadzonej przez Trybunał analizie rozpoznano złożony zestaw co najmniej dziesięciu różnych instrumentów budżetu ogólnego UE, niemniej brak jest przejrzystych informacji, jakie środki przeznaczono na jakie cele (zob. ***załącznik II***).

49 Stworzenie jasnego obrazu wydatków w dziedzinie, która obejmuje wiele obszarów polityki, stanowi więc znaczące wyzwanie. Różne służby Komisji zarządzają różnymi programami wydatkowania, przy czym każda z nich ma własne cele, zasady i harmonogramy. Sytuacja dodatkowo komplikuje się, gdy w grę wchodzi współfinansowanie ze strony państw członkowskich, jak w przypadku Funduszu Bezpieczeństwa Wewnętrznego (części dotyczącej współpracy policyjnej)[74].

Dające się wyodrębnić wydatki na cyberbezpieczeństwo

50 W latach 2014–2018 Komisja wydała co najmniej 1,4 mld euro na wdrożenie wspomnianej strategii[75], przy czym największa część tej kwoty przypadła na program „Horyzont 2020”[76]. Finansowanie w ramach tego programu jest zasadniczo udostępniane za pośrednictwem programu dotyczącego bezpiecznych społeczeństw oraz programu pn. „Wiodąca pozycja w zakresie technologii prorozwojowych i przemysłowych”[77]. Trybunał wyszczególnił 279 projektów dotyczących cyberbezpieczeństwa, dla których zawarto umowy w okresie do września 2018 r. Łączne finansowanie ze środków UE w ramach tych programów wyniosło 786 mln euro[78]. Na ***rys. 5*** przedstawiono charakterystykę tych projektów w oparciu o przeprowadzoną analizę.

Rys. 5 – Projekty badawcze dotyczące cyberbezpieczeństwa, dla których zawarto umowy w ramach programu „Horyzont 2020” (w mln euro)

Źródło: Europejski Trybunał Obrachunkowy.

51 W 2016 r. ustanowiono umowne partnerstwo publiczno-prywatne, aby stymulować europejską branżę cyberbezpieczeństwa. Celem było udostępnienie 450 mln euro z programu „Horyzont 2020” w ramach partnerstwa i przyciągnięcie dodatkowych środków na kwotę 1,8 mld euro z sektora prywatnego do 2020 r. W okresie 18 miesięcy do 31 grudnia 2017 r. na partnerstwo z programu „Horyzont 2020” przeznaczono 67,5 mln euro, a sektor prywatny zainwestował środki na kwotę 1 mld euro[79].

52 Zwalczanie cyberprzestępczości jest ponadto wspierane za pośrednictwem Funduszu Bezpieczeństwa Wewnętrznego (części dotyczącej współpracy policyjnej). Wsparcie obejmuje badania, spotkania ekspertów i działania informacyjne, przy czym na te cele przeznaczono w latach 2014–2017 niemal 62 mln euro. Ponadto państwa członkowskie mogą otrzymywać w ramach zarządzania dzielonego dotacje na sprzęt, szkolenia, badania naukowe i gromadzenie danych. Z dotacji tych, obejmujących kwotę 42 mln euro, skorzystało 19 państw członkowskich.

53 W ramach programu „Sprawiedliwość”, którym zarządza DG ds. Sprawiedliwości i Konsumentów, przeznaczono środki o wartości 9 mln euro na wsparcie współpracy

sądowej i funkcjonowania traktatów o wzajemnej pomocy prawnej, ze szczególnym uwzględnieniem wymiany danych elektronicznych i informacji finansowych.

54 W dyrektywie w sprawie bezpieczeństwa sieci i informacji jednoznacznie stwierdza się, że CSIRT muszą mieć odpowiednie zasoby do skutecznej realizacji swoich zadań[80]. W latach 2016–2018 corocznie udostępniano 13 mln euro z instrumentu „Łącząc Europę". Państwa członkowskie mogły ubiegać się o te środki na potrzeby wsparcia wdrażania wymogów dyrektywy. Nie przeprowadzono badania, w którym określono by środki finansowe, których sieć CSIRT i grupa współpracy faktycznie potrzebują, by zapewnić odpowiednie oddziaływanie.

55 Niektóre elementy kosztów operacyjnych agencji odnoszą się jednoznacznie do działań związanych z cyberbezpieczeństwem lub cyberprzestępczością. Na podstawie ogólnodostępnych informacji trudno jest jednak określić jakiekolwiek dokładne dane liczbowe.

56 Konwencja budapesztańska (zob. pkt ***11***) stanowi podstawę unijnych wydatków zewnętrznych w omawianej dziedzinie. W latach 2014–2018 UE wydała ok. 50 mln euro na rzecz wzmocnienia cyberbezpieczeństwa poza swoimi granicami. Niemal połowę tej kwoty udostępniono za pośrednictwem Instrumentu na rzecz Przyczyniania się do Stabilności i Pokoju, przy czym jeden główny projekt – GLACY+ o wartości 13,5 mln euro – miał na celu wzmocnienie globalnych zdolności do opracowywania i wdrażania prawodawstwa dotyczącego cyberprzestępczości i zacieśnienia współpracy międzynarodowej[81]. Środki wydatkowane natomiast w ramach innych unijnych instrumentów finansowych były ukierunkowane w dużej mierze na obszar Bałkanów Zachodnich[82] oraz kraje objęte europejską polityką sąsiedztwa. Przykładowo, projekt Cybercrime@EaP z udziałem krajów Partnerstwa Wschodniego ma na celu usprawnienie współpracy międzynarodowej w zakresie cyberprzestępczości i elektronicznego materiału dowodowego.

Inne wydatki na cyberbezpieczeństwo

57 Wskazanie konkretnych wydatków na cyberbezpieczeństwo w ramach unijnych programów nie zawsze jest możliwe:

- środki programu „Horyzont 2020" udostępniano również za pośrednictwem Wspólnego Przedsięwzięcia „Podzespoły i układy elektroniczne w służbie wiodącej pozycji Europy" w odniesieniu do systemów cyberfizycznych. Niemniej kontrolerzy nie byli w stanie ustalić, jakie konkretnie wydatki dotyczyły cyberbezpieczeństwa

w ramach 27 projektów o łącznej wartości 437 mln euro zrealizowanych w latach 2015–2016;

- z europejskich funduszy strukturalnych i inwestycyjnych udostępniono do 400 mln euro na potrzeby cyberbezpieczeństwa i usług zaufania. Obejmuje to inwestycje w bezpieczeństwo i ochronę danych dokonane w celu zwiększenia interoperacyjności i wzajemnych połączeń infrastruktury cyfrowej, identyfikację elektroniczną, ochronę prywatności i usługi zaufania.

58 W planie operacyjnym na 2018 r. Europejski Bank Inwestycyjny ogłosił zamiar zwiększenia finansowania na rzecz technologii podwójnego zastosowania, cyberbezpieczeństwa i cywilnego sektora bezpieczeństwa do 6 mld euro w okresie trzech lat[83].

Perspektywy na przyszłość

59 Komponent nowego programu „Cyfrowa Europa” na lata 2021–2027 dotyczący cyberbezpieczeństwa[84] o wartości 2 mld euro ma wzmocnić unijną branżę cyberbezpieczeństwa i ochronę ogółu społeczeństwa, między innymi przez wspomaganie wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji. Proponowana sieć centrów kompetencji w dziedzinie cyberbezpieczeństwa oraz badawcze centrum kompetencji, mające na celu wprowadzenie usprawnionego podejścia, ma stać się głównym mechanizmem wydatkowania środków unijnych w ramach programu „Cyfrowa Europa”.

60 Wydatki na obronność z budżetu UE wzrosły ostatnio za sprawą Europejskiego programu rozwoju przemysłu obronnego, któremu w latach 2019 i 2020 przydzielone zostanie 500 mln euro[85]. Program ma być ukierunkowany na usprawnienie koordynacji i zwiększenie efektywności wydatkowania środków państw członkowskich na obronność dzięki zachętom na rzecz wspólnego rozwoju wyposażenia i technologii. Celem jest uruchomienie łącznych inwestycji w zdolności obronne na kwotę 13 mld euro po 2020 r. za pośrednictwem Europejskiego Funduszu Obronnego, przy czym część wydatków dotyczyć będzie cyberobrony[86].

Wyzwanie 5 – Przydzielenie agencjom UE odpowiednich zasobów

61 Trzy główne podmioty odgrywające najistotniejszą rolę w unijnej polityce w zakresie cyberbezpieczeństwa – ENISA, EC3 Europolu i CERT-UE (zob. ***ramka 2***) – borykają się z problemami dotyczącymi zasobów, i to w czasach, gdy polityczne priorytety związane z bezpieczeństwem zyskują na znaczeniu. Ze względu na obecne przydziały zasobów finansowych i kadrowych agencje UE mają trudności, by sprostać stawianym przed nimi oczekiwaniom[87].

62 Żądania agencji o przyznanie dodatkowych zasobów, by móc zaspokoić rosnące zapotrzebowanie, nie zostały w pełni zaspokojone, co może postawić pod znakiem zapytania osiągnięcie celów politycznych (w terminie). Przykładowo:

- ograniczone zasoby były jednym z czynników, który uniemożliwił ENISA pełne osiągnięcie celów w 2017 r.[88] W pakiecie z 2017 r. zaproponowano dodatkowe środki, które odpowiadałyby nowym uprawnieniom przyznanym ENISA.

- Tempo zatrudniania analityków i inwestowania w zdolności ICT w ramach EC3 Europolu nie odpowiadało rosnącemu zapotrzebowaniu[89]. Ponadto we Wspólnej Grupie Zadaniowej ds. Przeciwdziałania Cyberprzestępczości działającej w ramach EC3 Europolu pracują specjaliści z państw członkowskich i państw trzecich, którzy mają wspierać postępowania oparte na informacjach wywiadowczych. Niemniej koszty zatrudnienia tych specjalistów ponoszą w dużej mierze państwa delegujące, co zniechęca do zaangażowania większej ich liczby. Przewidziano tymczasowe zaangażowanie ekspertów do poszczególnych spraw z wykorzystaniem środków Europolu lub cyklu polityki UE, tak aby umożliwić udział większej liczby państw.

63 Niektóre z ograniczeń agencje nakładają na siebie same. Wielu pracowników CERT-UE i ENISA to pracownicy kontraktowi, w przypadku których procedury rekrutacyjne są zazwyczaj powolne. Inne ograniczenia natomiast – choćby w zakresie przyciągania i zatrzymywania utalentowanych pracowników – wynikają z niezdolności agencji do konkurowania z sektorem prywatnym pod względem zarobków lub ze słabych perspektyw rozwoju zawodowego, które te agencje oferują. W związku z powyższym w latach 2014–2016 ENISA zleciła podmiotom zewnętrznym większość prowadzonych prac[90].

64 Ograniczenia dotyczące personelu i koniecznych narzędzi mogą pociągać za sobą znaczące ryzyko, w szczególności w odniesieniu do gromadzenia informacji wywiadowczych na temat zagrożeń. Ilość danych ze źródeł jawnych i niejawnych

nieustannie rośnie. Wobec zalewu danych możliwości prowadzenia odpowiedniej analizy zagrożeń przez analityków mogą być zbyt ograniczone. Bez odpowiednich zdolności i narzędzi pozwalających z powodzeniem scalać i wzajemnie łączyć takie dane informacji tych nie będzie można skutecznie przekształcić w przydatne dane wywiadowcze na temat zagrożeń, które mogłyby być następnie wymieniane i analizowane w całej UE[91].

Kwestie do rozważenia – finansowanie i wydatkowanie środków

- W jaki sposób Komisja i prawodawcy mogą usprawnić wydatkowanie środków unijnych na cyberbezpieczeństwo i w bardziej systematyczny sposób powiązać te wydatki z jasno określonymi celami?
- W jaki sposób można całościowo zaradzić niedostatecznemu przydziałowi zasobów dla agencji UE, biorąc przy tym pod uwagę potrzeby i cele Unii?
- Jakie działania wskazano na szczeblu UE i państw członkowskich z myślą o ograniczeniu przeszkód dla MŚP w przyciąganiu kapitału inwestycyjnego na potrzeby rozwoju działalności?
- Jakie konkretne i trwałe rezultaty przynoszą środki programu „Horyzont 2020” w zakresie tworzenia rozwiązań w dziedzinie cyberbezpieczeństwa?
- Czy unijne działania z zakresu budowania potencjału mające zwiększyć zdolności poza granicami UE zapewniają respektowanie unijnych wartości?

Działania na rzecz społeczeństwa odpornego na cyberzagrożenia

65 Zarządzanie w zakresie cyberbezpieczeństwa obejmuje zarządzanie zagrożeniami i ryzykiem, zwiększenie zdolności i podnoszenie świadomości, koordynację działań i wymianę informacji na fundamencie wzajemnego zaufania.

Wyzwanie 6 – Usprawnienie zarządzania i wzmocnienie standardów

Zarządzanie w zakresie bezpieczeństwa informacji

66 Zarządzanie w zakresie bezpieczeństwa informacji polega na wprowadzaniu struktur i strategii mających na celu zapewnienie poufności, integralności i dostępności danych. Wykracza ono poza kwestie czysto techniczne i wymaga zapewnienia skutecznego przywództwa, solidnych procesów i strategii dostosowanych do celów organizacyjnych[92]. Częścią tej dziedziny zarządzania jest zarządzanie w zakresie cyberbezpieczeństwa, które dotyczy wszystkich rodzajów cyberzagrożeń, w tym ukierunkowanych, zaawansowanych ataków, włamań lub incydentów, które trudno wykryć i którym trudno zaradzić.

67 Modele zarządzania w zakresie cyberbezpieczeństwa są różne w poszczególnych państwach członkowskich, przy czym często w obrębie jednego państwa odpowiedzialność za cyberbezpieczeństwo spoczywa na wielu podmiotach. Różnice te mogą utrudniać współpracę konieczną, by reagować na transgraniczne incydenty o dużej skali oraz wymieniać informacje wywiadowcze na temat zagrożeń na szczeblu krajowym, nie wspominając o szczeblu unijnym. Przeprowadzone przez Trybunał badanie ankietowe krajowych organów kontroli wskazało, że za największe zagrożenia uznawano uchybienia w mechanizmach zarządzania w podmiotach publicznych oraz w zarządzaniu ryzykiem.

68 W sektorze prywatnym uchybienia w zarządzaniu w zakresie cyberbezpieczeństwa są powszechne, mimo że ewentualne konsekwencje dla podmiotów z tego sektora mogą być bardzo poważne. Niemal dziewięć na dziesięć podmiotów utrzymuje, że stosowane przez nie funkcje w zakresie cyberbezpieczeństwa nie spełniają w pełni ich potrzeb[93], a specjalistów ds. cyberbezpieczeństwa dzielą często od zarządu co najmniej dwa szczeble hierarchii[94].

69 Unijne dyrektywy dotyczące prawa spółek nie wprowadzają żadnego szczegółowego wymogu ujawniania cyberzagrożeń. W Stanach Zjednoczonych Komisja Papierów Wartościowych i Giełd niedawno wydała niewiążące wytyczne, które mają pomóc spółkom publicznym w ujawnianiu informacji na temat ryzyka i incydentów w dziedzinie cyberbezpieczeństwa[95]. Wspólny Komitet Europejskich Urzędów Nadzoru[96] ostrzegł przed wzrostem cyberzagrożeń i zachęcił instytucje finansowe do udoskonalenia zagrożonych systemów informatycznych oraz przeanalizowania nieodłącznych elementów ryzyka związanych z bezpieczeństwem informacji, łącznością z siecią i zlecaniem zadań podmiotom zewnętrznym[97].

70 Usprawnienie zarządzania w zakresie bezpieczeństwa informacji w MŚP jest szczególnie trudne, ponieważ w bardzo wielu przypadkach przedsiębiorstwa te nie są w stanie wdrożyć odpowiednich systemów. MŚP brak jest odpowiednich wytycznych na temat stosowania wymogów w zakresie bezpieczeństwa informacji i ochrony prywatności i ograniczania zagrożeń technologicznych[98]. Do najistotniejszych wyzwań należy zatem lepsze zrozumienie potrzeb tych przedsiębiorstw oraz zapewnienie im koniecznych zachęt i wsparcia.

71 Brak spójnych międzynarodowych ram zarządzania w zakresie cyberbezpieczeństwa osłabia zdolność społeczności międzynarodowej do reagowania na cyberataki i ograniczania ich oddziaływania. Z tego względu istotne jest wypracowanie konsensusu dotyczącego takich ram zarządzania, które najlepiej odzwierciedlałyby unijne interesy i wartości[99]. Starania na rzecz wprowadzenia wiążących międzynarodowych standardów dotyczących cyberprzestrzeni stają się coraz trudniejsze, czego widomym znakiem była niemożność osiągnięcia konsensusu w grupie ekspertów rządowych ONZ w 2017 r. co do sposobu, w jaki prawo międzynarodowe powinno być stosowane do reakcji państw na cyberincydenty.

72 Aby usprawnić realizację programu dotyczącego zarządzania cyberprzestrzenią, UE ustanowiła ponadto sześć partnerstw cyfrowych w celu prowadzenia regularnych dialogów politycznych mających zbudować zaufanie i stworzyć wspólne obszary współpracy[100]. Działania te przyniosły umiarkowane wyniki; ogólnie rzecz ujmując nie można jeszcze uznać UE za „znaczący podmiot w dziedzinie cyberbezpieczeństwa" na scenie międzynarodowej, choć na pewno Unia wzmocniła swoją pozycję[101].

Bezpieczeństwo informacji w instytucjach UE

73 Każda z instytucji UE ma swoje zasady zarządzania bezpieczeństwem informacji. Komisja świadczy innym instytucjom i agencjom pomoc w tej dziedzinie na podstawie

podpisanego porozumienia międzyinstytucjonalnego. Instytucje i organy UE uznają potrzebę spójnego rozwijania zdolności w zakresie cyberprzestrzeni oraz podejścia do zarządzania ryzykiem. Komisja, Rada i ESDZ mają w 2020 r. przedstawić Horyzontalnej Grupie Roboczej ds. Cyberprzestrzeni sprawozdanie w sprawie zarządzania i postępów w zwiększaniu przejrzystości i harmonizacji zarządzania w zakresie cyberbezpieczeństwa w instytucjach i agencjach UE[102].

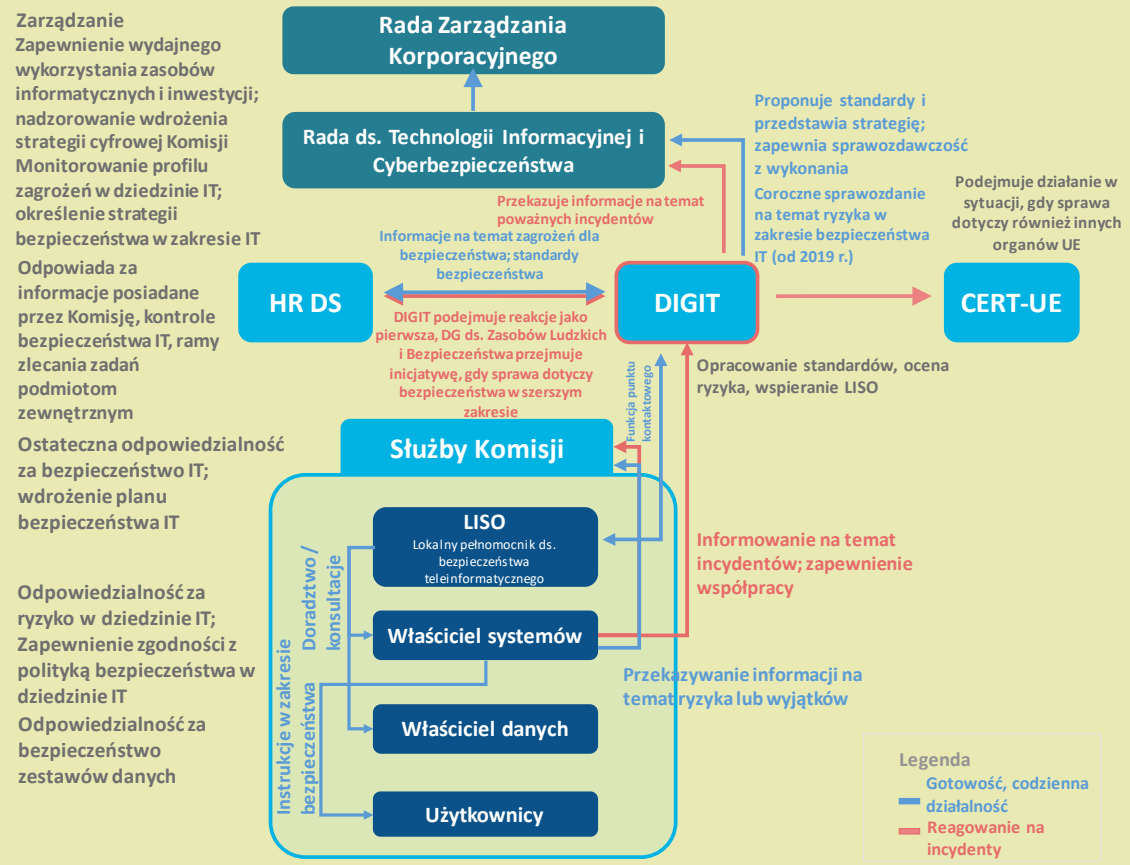
74 Za bezpieczeństwo infrastruktury i usług informatycznych w obrębie Komisji odpowiada Dyrekcja Generalna ds. Informatyki (DIGIT) (zob. ***ramka 3***). Główne cele strategii cyfrowej Komisji w zakresie bezpieczeństwa informatycznego są następujące: uwzględnienie tego bezpieczeństwa w procesach zarządzania; zapewnienie skutecznej i racjonalnej pod względem kosztów infrastruktury i odporności; rozszerzenie zakresu wykrywania i reagowania na incydenty oraz integracja zarządzania bezpieczeństwem i zarządzania informatycznego[103]. Zgodnie z umową o świadczeniu usług Komisja gwarantuje aktywne utrzymanie niemal całego oprogramowania oraz korzystanie wyłącznie z programów objętych wsparciem ze strony sprzedawców[104].

75 Znaczenie ochrony instytucji rozciąga się na unijne misje i struktury WPBiO działające na całym świecie. Jednym z priorytetów unijnych ram polityki w zakresie cyberobrony (zaktualizowanych w 2018 r.) jest wzmocnienie ochrony systemów informacyjnych i komunikacyjnych WPBiO stosowanych przez podmioty unijne. W strukturach ESDZ rozpoczęła działanie wewnętrzna rada ds. cyberzarządzania. Pierwsze spotkanie rady odbyło się w czerwcu 2017 r.[105]

Ramka 3

Ochrona systemów informacyjnych Komisji

Około 1 300 systemów i 50 000 urządzeń, które są użytkowane w Komisji, stanowi cel ciągłych cyberataków. Jak przedstawiono na rysunku poniżej, odpowiedzialność w dziedzinie IT jest rozproszona. Bezpieczeństwo informacji i systemów informatycznych opierają się na wspólnym planie informatycznym ustanowionym przez DIGIT. Rada ds. Technologii Informacyjnej i Cyberbezpieczeństwa działa jako *de facto* dyrektor ds. bezpieczeństwa systemów informacyjnych w Komisji. Zapewnia ona hierarchiczne powiązanie między poziomem operacyjnym bezpieczeństwa IT z wyższymi kadrami zarządzającymi w Komisji, które reprezentuje Rada Zarządzania Korporacyjnego.



Źródło: Europejski Trybunał Obrachunkowy na podstawie decyzji Komisji[106].

Głównym zadaniem DG ds. Zasobów Ludzkich i Bezpieczeństwa jest ochrona pracowników oraz zasobów Komisji, a także informacji będących w jej posiadaniu. Dyrekcja ta przeprowadza również postępowania wyjaśniające w dziedzinie bezpieczeństwa, których przedmiot wykracza poza samo bezpieczeństwo informatyczne. Działalność dyrekcji stanowi więc wkład w działania kontrwywiadowcze i z zakresu zwalczania terroryzmu.

DIGIT jest odpowiedzialna za bezpieczeństwo IT. W strukturach dyrekcji działa zespół reagowania na incydenty komputerowe (CERT-UE). Zespół ten, utworzony w 2011 r., dysponuje rocznym budżetem w wysokości ok. 2,5 mln euro i liczy 30 pracowników. Pełni on funkcję służby interwencyjnej, która reaguje jako pierwsza w przypadku dowolnego incydentu w dziedzinie bezpieczeństwa informacji obejmującego wiele instytucji.Nie funkcjonuje on jednak całodobowo przez siedem dni w tygodniu. CERT-UE prowadzi platformę wymiany informacji. W 2018 r. CERT-UE podpisał niewiążący protokół ustaleń z ENISA, EC3 oraz Europejską Agencją Obrony z myślą o zacieśnieniu współpracy i usprawnieniu koordynacji. Zawarł również techniczne porozumienie z systemem reagowania na incydenty komputerowe NATO.

Ocena ryzyka i zagrożeń

76 Solidna i ciągła ocena ryzyka i zagrożeń stanowi istotne narzędzie dla podmiotów zarówno sektora publicznego, jak i prywatnego. Nie znaczy to jednak, że istnieje jedno standardowe podejście na potrzeby klasyfikowania i identyfikowania cyberzagrożeń lub oceny ryzyka. W rezultacie treść ocen znacznie się różni, co stanowi przeszkodę dla przyjęcia spójnego ogólnounijnego podejścia do cyberbezpieczeństwa[107]. Ponadto oceny często opierają się na tych samych źródłach lub wręcz innych ocenach zagrożeń, co skutkuje powielaniem w nieskończoność tych samych ustaleń[108] i może sprawić, że niewystarczająco wiele uwagi poświęci się innym zagrożeniom. Problem pogłębia utrzymujący się brak gotowości do dzielenia się informacji i niezgłaszanie niektórych incydentów.

77 Komórka UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych[109] działająca w ramach struktur ESDZ została utworzona z myślą o zwiększeniu świadomości sytuacyjnej i wsparciu procesu decyzyjnego dzięki wymianie analiz. Konieczne jest jednak zwiększenie wiedzy specjalistycznej w Komórce, w tym w zakresie cyberbezpieczeństwa. Jednocześnie CERT-UE przedstawia instytucjom, organom i agencjom UE sprawozdania i briefingi na temat cyberzagrożeń, które ich dotyczą.

78 W przeszłości ENISA zwracała uwagę, że w wielu państwach członkowskich stosowano jakościowe podejście do zagrożeń i że konieczne jest rozwinięcie modelowania cyberzagrożeń[110]. Zdolność w zakresie monitorowania na potrzeby analizy strategicznej poprawi ogólne zrozumienie tych zjawisk. Oceny zagrożeń nie mogą obejmować przy tym jedynie zagrożeń technologicznych, ale również zagrożenia ekonomiczne i polityczno-społeczne, tak aby zapewnić całościowy ogląd sytuacji. Powinny dotyczyć również czynników stojących za zagrożeniami i motywów poszczególnych podmiotów.

Zachęty

79 Wciąż istnieje zbyt mało zachęt o charakterze ekonomicznym i prawnym, które skłaniałyby podmioty do zgłaszania incydentów i wymiany informacji na ten temat. Wiele z nich z obawy przed nadszarpnięciem reputacji woli uporać się z cyberatakami dyskretnie lub zapłacić okup sprawcom. Trudno jeszcze ocenić, na ile dyrektywa w sprawie bezpieczeństwa sieci i informacji będzie skuteczna w zwiększeniu liczby zgłoszeń. Komisja oczekuje wymiernych usprawnień zwłaszcza na szczeblu krajowym, ale akt ws. cyberbezpieczeństwa zapewni ogólnounijne podejście[111].

80 Dzięki uwzględnieniu określonych standardów w zamówieniach publicznych organy publiczne – zakupując produkty i usługi cyfrowe w ramach takich zamówień lub finansowania programów lub badań naukowych – mogą znacząco wpłynąć na dostawców (np. wymagając przyjęcia określonych standardów technicznych, takich jak protokół internetowy IPv6, w celu ułatwienia walki z cyberprzestępczością). Obecnie jednak brak jest wspólnych zamówień publicznych dotyczących infrastruktury cyberbezpieczeństwa[112]. Komisja ma jeszcze wiele do zrobienia w tym względzie. Program „Cyfrowa Europa" proponowany w następnych wieloletnich ramach finansowych ma rozwiązać problem dotychczas ograniczonych inwestycji sektora publicznego w zakup najnowszych technologii w zakresie cyberbezpieczeństwa.

81 Działając w charakterze regulatora, Komisja może zagwarantować opracowanie odpowiednich standardów, które zostaną na dużą skalę wdrożone w celu poprawy bezpieczeństwa. Komisja i Europol współpracują z organami zarządzającymi internetem, takimi jak ICANN (zob. pkt ***38***) oraz RIPE-NCC[113], co ma kluczowe znaczenie dla ustanowienia odpowiednich struktur zwalczania cyberprzestępczości z myślą o wspieraniu organów ścigania i wymiaru sprawiedliwości.

Wyzwanie 7 – Podniesienie poziomu umiejętności i upowszechnienie wiedzy

82 ENISA zwróciła uwagę, że użytkownicy odgrywają zasadniczą rolę w zwalczaniu cyberataków oraz że podniesieniu poziomu umiejętności i świadomości oraz kształcenie są nieodzowne dla budowy cyberodpornego społeczeństwa[114]. Obywatele, którzy potrafią w porę dostrzec niepokojące symptomy i posługują się odpowiednimi technikami, mogą spowolnić ataki lub im zapobiec, zarówno w pracy, jak i w otoczeniu domowym.

83 Szczególnie niepokojąca jest rosnąca asymetria między wiedzą fachową konieczną do popełnienia cyberprzestępstwa lub przeprowadzenia cyberataku a umiejętnościami koniecznymi, by przed takim działaniem się obronić. Model „przestępstwa na zlecenie" zmniejszył bariery wejścia na rynek cyberprzestępczości: osoby nieposiadające wiedzy technicznej mogą obecnie wynająć botnety, zestawy do exploitów lub pakiety do ataków typu ransomware.

Szkolenia, umiejętności i budowanie potencjału

84 W skali globalnej coraz bardziej odczuwalny jest brak umiejętności w zakresie cyberbezpieczeństwa; niedostatek siły roboczej w tej dziedzinie wzrósł o 20% od 2015 r.[115] Tradycyjne kanały rekrutacyjne nie pozwalają zaspokoić zapotrzebowania, w tym w odniesieniu do stanowisk kierowniczych i interdyscyplinarnych[116]. Niemal 90% pracowników w dziedzinie cyberbezpieczeństwa na świecie to mężczyźni; utrzymujący się brak zróżnicowania płciowego w dalszej mierze ogranicza napływ utalentowanych osób[117]. Ponadto na uniwersytetach kwestie związane z cyberprzestrzenią są niedostatecznie uwzględniane w nietechnicznych programach studiów.

85 Konieczne jest prowadzenie szkoleń i kształcenie we wszystkich sektorach, wśród pracowników służby cywilnej, funkcjonariuszy organów ścigania, w organach wymiaru sprawiedliwości, siłach zbrojnych i wśród instruktorów. Przykładowo, sądy muszą być w stanie radzić sobie z szybko ewoluującymi technicznymi szczegółami dotyczącymi cyberprzestępczości i ofiar cyberprzestępstw[118]. Obecnie brak jest ogólnounijnych standardów dotyczących szkolenia i certyfikacji w tym zakresie[119]. Ważne jest również zapewnienie odpowiedniej kombinacji umiejętności w unijnych instytucjach. Bez tych umiejętności instytucje mogą nie być w stanie odpowiednio określić zakresu działań ani wskazać właściwych partnerów i potrzeb w zakresie bezpieczeństwa. Mogą też być niezdolne do zarządzania programami. Wszystko to może z kolei osłabić skuteczność unijnych programów lub utrudnić opracowywanie unijnej polityki.

86 Za politykę w zakresie kształcenia na szczeblu UE odpowiedzialne są wprawdzie państwa członkowskie, obecnie jednak realizowane jest już wiele działań szkoleniowych (zob. ***tabela 2***) i inicjatyw (zob. ***ramka 4***). UE może również ułatwić stosowanie ogólnounijnych standardów w programach nauczania we wszystkich stosownych dziedzinach[120]. Przykładowo, w dziedzinie kryminalistyki cyfrowej wspólne standardy szkoleniowe są konieczne, by utorować drogę do dopuszczalności dowodu w państwach członkowskich. Ze względu na transgraniczny charakter cyberprzestępczości zaangażowanych może być wiele jurysdykcji, co wymaga szkolenia na szczeblu UE. Tymczasem Cepol, agencja UE odpowiedzialna za szkolenia w dziedzinie ścigania, odnotował, że w ponad dwóch trzecich państw członkowskich funkcjonariuszom organów ścigania nie oferuje się regularnych szkoleń dotyczących cyberprzestępczości[121]. UE mogłaby również wskazać sposoby na stworzenie synergii w zakresie kształcenia i szkoleń między sektorem cywilnym a wojskowym[122]. ENISA ustaliła ponadto, że wprawdzie obecna oferta szkoleniowa w kluczowych sektorach jest rozbudowana, nie jest ona jednak wystarczająco ukierunkowana na kwestię odporności infrastruktury krytycznej[123].

Tabela 2 – Niektóre z unijnych inicjatyw szkoleniowych dotyczących cyberprzestrzeni

Projekty Europejskiej Agencji Obrony, np. wsparcie sektora prywatnego na rzecz ćwiczeń oraz projekt platform cybernetycznych	Sieć Europejskiego Kolegium Bezpieczeństwa i Obrony (zapewniająca szkolenia cywilno-wojskowe), w tym platforma kształcenia, szkolenia, oceny i ćwiczeń w zakresie cyberbezpieczeństwa	Szkolenia ENISA, obejmujące programy szkoleniowe w obszarach, w których brak jest oferty rynkowej
Programy szkoleniowe Europolu, Cepolu, ECTEG[124] – w tym model zarządzania szkoleniami i ramy kompetencji dla szkoleń (z uwzględnieniem certyfikacji)	Sieć centrów kompetencji oraz badawcze centrum kompetencji (proponowane)	Działania dotyczące szyfrowania zaproponowane w 11. sprawozdaniu z postępu prac nad stworzeniem unii bezpieczeństwa
Współpraca UE-NATO w dziedzinie szkolenia i kształcenia w zakresie cyberobrony	Program „wojskowy Erasmus”	Europejska sieć szkolenia kadr wymiaru sprawiedliwości

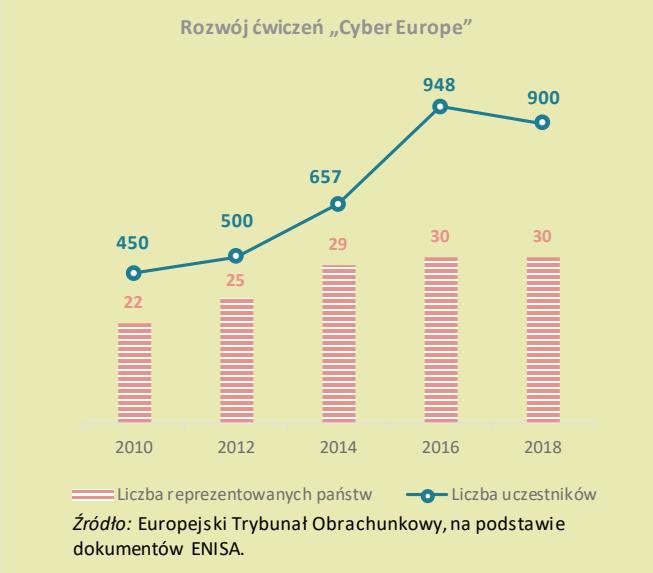
Źródło: Europejski Trybunał Obrachunkowy.

87 UE oddelegowała specjalistów ds. zwalczania terroryzmu i bezpieczeństwa do 17 delegatur, aby wzmocnić powiązania między wewnętrznym i zewnętrznym wymiarem bezpieczeństwa UE[125]. Niezależnie od ograniczeń związanych z zasobami, większa wiedza fachowa dotycząca cyberprzestrzeni mogłaby przyczynić się do wdrożenia odpowiednich projektów oraz wskazania synergii z innymi programami lub źródłami finansowania[126]. Mogłaby również zwiększyć znaczenie cyberbezpieczeństwa w dialogu politycznym, choć cyberbezpieczeństwo będzie musiało konkurować w tym zakresie z wieloma innymi priorytetami, takimi jak migracja, zorganizowana przestępczość i powracający zagraniczni bojownicy.

Ramka 4

Ćwiczenia

Ćwiczenia stanowią istotne elementy cyberkształcenia i cyberszkoleń. Są doskonałą okazją do wzmocnienia gotowości dzięki sprawdzeniu potencjału i pozwalają symulować reakcję w warunkach rzeczywistych oraz tworzyć sieci kontaktów roboczych. Od 2010 r. częstotliwość ćwiczeń znacząco wzrosła.



Źródło: Europejski Trybunał Obrachunkowy, na podstawie dokumentów ENISA.

Uczestnicy biorą w nich udział na miejscu lub zdalnie. Po ćwiczeniach przeprowadza się oceny, aby wyciągnąć wnioski z doświadczeń, choć nie są one jeszcze w pełni przyswajane jednocześnie na szczeblach strategicznym / politycznym, operacyjnym i technicznym[127].

Najistotniejsze ćwiczenia prowadzone przez UE i NATO – organizowane raz na dwa lata ćwiczenia „Cyber Europe” (o charakterze operacyjnym) i coroczne ćwiczenia „Locked Shields” (o charakterze technicznym) – gromadzą ponad 1 000 uczestników z ok. 30 uczestniczących państw. Oba te ćwiczenia są ukierunkowane na ochronę i utrzymanie infrastruktury krytycznej w symulowanych warunkach ataku. Oba zostały znacznie rozbudowane i obecnie uwzględniają aspekty strategii medialnych, prawnych i finansowych, tak aby poprawić świadomość sytuacyjną specjalistów zajmujących się tymi kwestiami w praktyce. Równocześnie prowadzone ćwiczenia PACE (o charakterze strategicznym) mają sprawdzać współdziałanie UE i NATO na wypadek pojawienia się zagrożeń hybrydowych.

Powyższe ćwiczenia nie są jedynymi organizowanymi na szczeblu międzynarodowym. ENISA organizuje coroczne zawody cyfrowe, w ramach których zespoły rywalizują ze sobą w rozwiązywaniu problemów związanych z bezpieczeństwem w obszarach takich jak bezpieczeństwo sieci i urządzeń mobilnych, zagadki kryptograficzne, inżynieria odwrotna, etyka i kryminalistyka. Pierwsze ćwiczenia na szczeblu ministerialnym, EU CYBRID, odbyły się we wrześniu 2017 r. i dotyczyły procesu podejmowania decyzji strategicznych. W 2018 r. uruchomiono ćwiczenia „Crossed Swords” pod egidą NATO w celu rozwinięcia aspektów ofensywnych wcześniejszych ćwiczeń „Locked Shields”. NATO organizuje ponadto ćwiczenia „Cyber Coalition”.

Kluczowym wyzwaniem w ramach tych inicjatyw jest zapewnienie aktywnego udziału wszystkich istotnych zainteresowanych stron i koordynacja wszystkich ćwiczeń, tak

aby uniknąć powielania działań i w skuteczny sposób dzielić się wnioskami z doświadczeń.

Świadomość

88 Obywatele często przyczyniają do rozprzestrzeniania ataków i rozpowszechniania dezinformacji, ponieważ mogą bez swojej wiedzy być narażeni na skutki występowania luk w niedrogich i powszechnie sprzedawanych urządzeniach i oprogramowaniu lub paść ofiarą manipulacji z zakresu inżynierii społecznej. Podnoszenie poziomu świadomości ma zatem kluczowe znaczenie dla zapewnienia cyberodporności, przy czym nie jest to w żadnym wypadku zadanie proste, ponieważ laikom trudno jest zrozumieć złożony charakter cyberbezpieczeństwa i powiązane zagrożenia.

89 Organizowany co roku europejski miesiąc świadomości w dziedzinie cyberbezpieczeństwa (European Cyber Security Awareness Month – ECSM) oraz Dzień Bezpiecznego Internetu są przykładami takich działań. Do tej pory do ECSM dołączyło siedem państw spoza UE[128]. Kampania Europolu „Powiedz NIE!" ma ograniczyć ryzyko tego, że dzieci padną ofiarą zmuszania do czynności seksualnych i wymuszeń seksualnych w sieci. Ograniczenie takiego ryzyka ma duże znaczenie, ponieważ obecnie niewiele ofiar zgłasza tego rodzaju przestępstwa policji[129]. Komisja przyznaje, że strategia w zakresie cyberbezpieczeństwa była jak do tej pory jedynie „częściowo skuteczna" w podnoszeniu poziomu świadomości wśród przedsiębiorstw i obywateli[130]. Związane jest to ze skalą zadania, ograniczonymi zasobami, niejednakowym zaangażowaniem wśród państw członkowskich oraz brakiem dowodów naukowych dotyczących tego, w jaki sposób najlepiej podnosić świadomość i mierzyć ją.

90 Wyzwaniem, przed którym stoi Komisja i stosowne agencje, jest zapewnienie, by działania mające na celu podnoszenie świadomości: były dobrze ukierunkowane i odpowiednio wypromowane; miały charakter integracyjny; odpowiadały profilowi zagrożeń; nie wywoływały niezamierzonych skutków takich jak „zmęczenie dbaniem o bezpieczeństwo"[131], a także aby w ramach tych działań opracowano metody i wskaźniki pozwalające ocenić ich skuteczność. Powinno to dotyczyć w równym stopniu samych unijnych instytucji, w których kultura organizacyjna ukierunkowana na podnoszenie poziomu świadomości wymaga poprawy[132].

Wyzwanie 8 – Lepsza wymiana informacji i koordynacja działań

91 Cyberbezpieczeństwo wymaga koordynacji działań sektora publicznego i prywatnego, zwłaszcza pod względem wymiany informacji i najlepszych praktyk. Zaufanie na wszystkich poziomach ma kluczowe znaczenie dla zapewnienia odpowiednich warunków sprzyjających transgranicznej wymianie informacji szczególnie chronionych. Słaba koordynacja może prowadzić do rozdrobnienia, powielania wysiłków i rozproszenia wiedzy specjalistycznej, skuteczna natomiast – przynieść wymierne sukcesy, takie jak zamknięcie serwisów sprzedażowych działających w ciemnej sieci[133]. Pomimo postępów osiągniętych w ostatnich latach, poziom zaufania jest wciąż „niewystarczający”[134] na szczeblu UE i w niektórych państwach członkowskich[135].

Koordynowanie działań poszczególnych instytucji UE i państw członkowskich

92 Jednym z celów strategii w zakresie cyberbezpieczeństwa i struktur współpracy wprowadzonych na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji było zwiększenie wzajemnego zaufania między zainteresowanymi stronami. W ocenie strategii uznano, że stworzono fundamenty pod strategiczną i operacyjną współpracę na szczeblu UE[136]. Ogólnie koordynacja działań pozostaje jednak „niewystarczająca”[137]. Wyzwanie polega na zapewnieniu, by wymiana informacji nie tylko obejmowała istotne elementy, ale również pozwalała zyskać całościowy obraz sytuacji. Wypracowanie wspólnego podejścia w oparciu o uzgodnioną terminologię jest ważnym elementem tych starań (zob. ***ramka 5***).

93 W ocenie ENISA zwrócono jednak uwagę, że unijne podejście do kwestii cyberbezpieczeństwa nie obejmuje w wystarczającym stopniu koordynacji działań, co skutkuje brakiem synergii między działalnością ENISA i działaniami innych zainteresowanych stron. Mechanizmy współpracy wciąż nie są ugruntowane[138]. Akt ws. cyberbezpieczeństwa ma zaradzić temu problemowi przez przyznanie ENISA większej roli w zakresie koordynacji. Dążenie do zacieśnienia współpracy stało za podpisaniem w 2018 r. protokołu ustaleń przez ENISA, Europejską Agencję Obrony, EC3 Europolu oraz CERT-UE[139]. Priorytetem dla Komisji w nadchodzących latach będzie zapewnienie odpowiedniej spójności między inicjatywami politycznymi, potrzebami i programami inwestycyjnymi, tak aby przezwyciężyć rozdrobnienie i stworzyć synergię[140].

94 Sprawowanie funkcji koordynacyjnych powierzono różnym organom instytucjonalnym. Grupie roboczej w sprawie unii bezpieczeństwa przyznano kluczową

rolę w koordynowaniu działań różnych dyrekcji generalnych Komisji z myślą o wsparciu realizacji programu unii bezpieczeństwa[141]. Podgrupie grupy roboczej zajmującej się cyberbezpieczeństwem przewodniczy DG CNECT.

95 W obrębie Rady cyberbezpieczeństwem zajmuje się Horyzontalna Grupa Robocza ds. Cyberprzestrzeni, która zapewnia koordynację działań w odniesieniu do strategicznych i horyzontalnych kwestii związanych z cyberprzestrzenią oraz pomaga w przygotowaniu ćwiczeń i ocenie uzyskanych wyników. Współpracuje przy tym ściśle z Komitetem Politycznym i Bezpieczeństwa, który odgrywa zasadniczą rolę w podejmowaniu decyzji dotyczących wszelkich działań dyplomatycznych związanych z cyberprzestrzenią (zob. ***ramka 6*** w następnym rozdziale). Ponieważ kwestia cyberbezpieczeństwa ma charakter przekrojowy, jednoczesne uwzględnienie wszystkich istotnych interesów nie jest zadaniem prostym – w ostatnim czasie kwestiami dotyczącymi cyberbezpieczeństwa zajmowały się nie mniej niż 24 zespoły robocze i organy przygotowawcze[142].

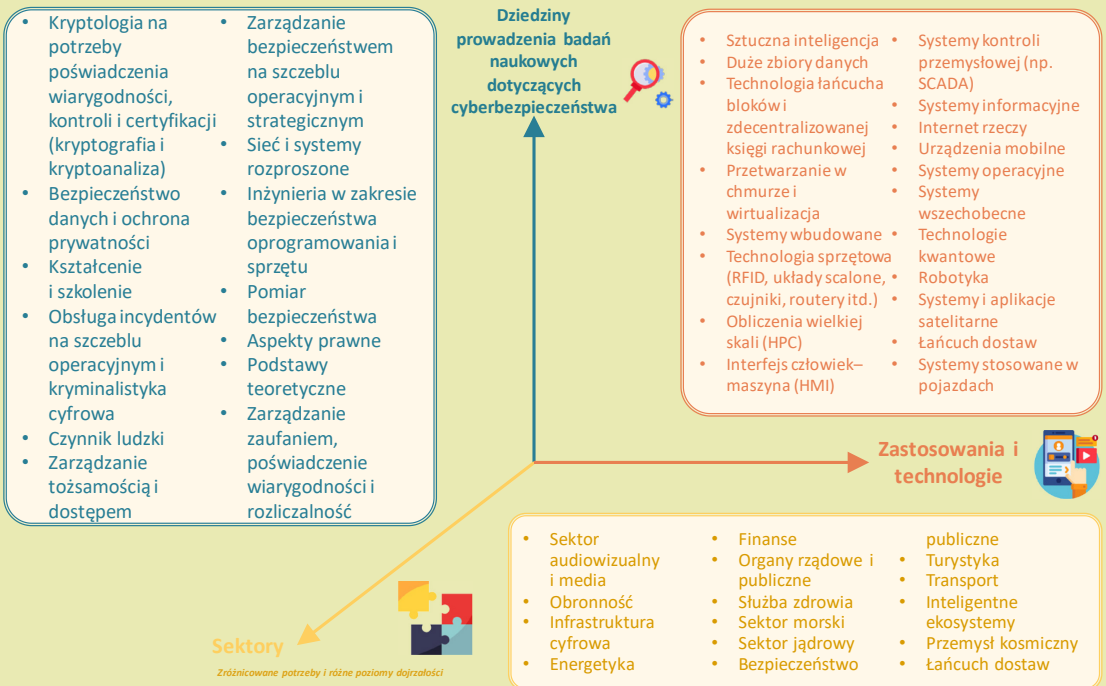
96 Dwa najnowsze wnioski ustawodawcze dotyczące wzmocnienia ENISA (z 2017 r.) oraz stworzenia sieci centrów kompetencji w dziedzinie cyberbezpieczeństwa i badawczego centrum kompetencji (z 2018 r.) mają w szczególności na celu zaradzenie rozdrobnieniu i powielaniu wysiłków. Głównym motywem ustanowienia sieci centrów kompetencji w dziedzinie cyberbezpieczeństwa oraz badawczego centrum kompetencji jest konieczność, by zapełnić lukę, której nie mogły wyeliminować struktury współpracy utworzone na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji. Struktury te nie miały na celu wspierania opracowywania najbardziej zaawansowanych technicznie rozwiązań.

Ramka 5

Dążenie do posługiwania się tym samym językiem cyfrowym: *spójność technologiczna*

Jednoznaczna terminologia korzystnie wpływa na świadomość sytuacyjną i ułatwia koordynację działań[143]. Pozwala precyzyjnie określić naturę zagrożenia i ryzyka.

Wspólne Centrum Badawcze Komisji niedawno opracowało zmienioną nomenklaturę badawczą na podstawie różnych standardów międzynarodowych[144]. Ma ona stać się punktem odniesienia, wykorzystywanym jako indeks przez podmioty badawcze w całej Europie.



Źródło: Europejski Trybunał Obrachunkowy, na podstawie informacji przekazanych przez Komisję Europejską.

Do niedawna unijne instytucje i agencje nie posługiwały się żadnymi wspólnymi definicjami. Sytuacja zaczyna się zmieniać. W ramach realizowanego planu działania grupa współpracy wypracowała nomenklaturę incydentów, tak aby ułatwić skuteczną współpracę transgraniczną.

Współpraca i wymiana informacji z sektorem prywatnym

97 Współpraca między organami publicznymi i sektorem prywatnym jest nieodzowna dla ogólnego podniesienia poziomu cyberbezpieczeństwa. Mimo tego w ocenie strategii w zakresie cyberbezpieczeństwa przeprowadzonej w 2017 r. Komisja stwierdziła, że wymiana informacji między prywatnymi zainteresowanymi stronami oraz między sektorem publicznym i prywatnym „wciąż nie była optymalna” ze względu na „brak zaufanych mechanizmów zgłaszania oraz zachęt do dzielenia się informacjami”[145], co utrudniało osiągnięcie celów strategicznych. Komisja zwróciła również uwagę na brak wydajnego mechanizmu współpracy, który pozwoliłby państwom członkowskim na wspólne działanie na rzecz strategicznego wzmocnienia trwałych zdolności przemysłowych na dużą skalę[146].

98 Ośrodki wymiany i analizy informacji to organizacje stworzone, by zapewnić platformę i zasoby na potrzeby wymiany informacji między sektorami publicznym i prywatnym oraz gromadzenia informacji na temat cyberzagrożeń. Mają one przyczynić się do budowania zaufania przez dzielenie się doświadczeniami, wiedzą i analizami, w szczególności na temat pierwotnych przyczyn, incydentów i zagrożeń. Krajowe i sektorowe ośrodki tego rodzaju istnieją w wielu państwach członkowskich, ale liczba takich ośrodków na szczeblu europejskim jest wciąż dość ograniczona[147]. Ponadto z ośrodkami tymi wiąże się szereg problemów (ograniczone zasoby, trudności w ocenie osiągniętych wyników, zapewnienie odpowiednich struktur na potrzeby zaangażowania zarówno sektora publicznego, jak i prywatnego, zapewnienie udziału organów ścigania), które będzie trzeba przezwyciężyć, jeśli ośrodki mają przyczynić się do wdrożenia dyrektywy w sprawie bezpieczeństwa sieci i informacji oraz budowania zdolności w zakresie bezpieczeństwa w wymiarze ogólnoeuropejskim[148].

99 Ścisła współpraca z sektorem prywatnym jest szczególnie istotna w zwalczaniu złożonych przypadków cyberprzestępstw, niemniej wyniki tej współpracy są różne w poszczególnych państwach członkowskich i zależą od poziomu wzajemnego zaufania[149]. EC3 Europolu ustanowił tymczasem liczne grupy doradcze z udziałem operatorów z sektora prywatnego, instytucji i agencji UE oraz innych organizacji międzynarodowych z myślą o usprawnieniu współpracy przez tworzenie sieci kontaktów, strategiczną wymianę informacji wywiadowczych i wspólne działania. Prace prowadzone są w oparciu o plany dostosowane do celów cyklu polityki UE[150]. Wykorzystanie szyfrowania do celów przestępczych jest kolejnym obszarem, w którym występuje wiele problemów wymagających pilnego zacieśnienia współpracy z sektorem prywatnym. EC3 Europolu analizuje obecnie możliwość zaangażowania we Wspólnej Grupie Zadaniowej ds. Przeciwdziałania Cyberprzestępczości (zob. pkt ***62***) specjalistów z sektora prywatnego i środowisk akademickich, na krótki czas i na potrzeby konkretnych spraw.

100 Brak wydajnych mechanizmów współpracy niekorzystnie wpływa na sektor cywilny i obronny, zarówno publiczny, jak i prywatny. Obszary, w których pojawiają się wspólne wyzwania, obejmują kryptografię, bezpieczne systemy wbudowane, wykrywanie złośliwego oprogramowania, techniki symulacji, ochronę sieci i systemów łączności oraz techniki uwierzytelniania. Promowanie współpracy cywilno-wojskowej oraz wspieranie badań naukowych i technologii (w szczególności przez wspieranie MŚP) stanowią dwa spośród priorytetów unijnych ram polityki w zakresie cyberobrony zaktualizowanych w 2018 r.

Kwestie do rozważenia – budowanie odporności

- W jaki sposób można zapewnić właściwą równowagę na szczeblu UE między koniecznością uwzględnienia polityki w zakresie cyberbezpieczeństwa w głównych strategiach politycznych a zapewnieniem wydajnej koordynacji działań między różnymi podmiotami i podziału obowiązków?

- W jakim stopniu unijne instytucje i agencje są przygotowane na kolejny duży atak skierowany bezpośrednio przeciwko nim?

- W jaki sposób unijne agencje zajmujące się cyberprzestrzenią mogą skuteczniej przyciągać utalentowanych pracowników?

- Jakie dalsze działania są konieczne w celu zapewnienia odpowiednich zdolności w unijnych instytucjach i agencjach, tak aby umożliwić przyjęcie spójnych ram oceny ryzyka i zagrożeń?

- W jaki sposób europejskie organy nadzoru (Europejski Urząd Nadzoru Bankowego, Europejski Urząd Nadzoru Giełd i Papierów Wartościowych oraz Europejski Urząd Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych) podejmują kwestię luk w zakresie cyberbezpieczeństwa nieodłącznie związanych z sektorem finansowym? Jakie wnioski dla innych sektorów można wyciągnąć z tych działań?

- Jak najlepiej – wobec ogólnego niedostatku wiedzy specjalistycznej – wykorzystać unijną pomoc techniczną na rzecz organów publicznych, aby w jak największym zakresie poprawić ogólną cyberodporność?

- W jaki sposób UE i państwa członkowskie mogą wziąć znaczący udział w międzynarodowych debatach, tak aby kształtować zarządzanie cyberprzestrzenią i odnośne standardy oraz promować unijne wartości?

- Jakie działania podnoszące poziom świadomości na szczeblu UE i państw członkowskich (w tym działania o charakterze zapobiegawczym) przynoszą faktyczne skutki i w jaki sposób UE może rozszerzyć ich zakres?

- Jaką rolę może odegrać UE w promowaniu zróżnicowania płciowego w dziedzinie cyberbezpieczeństwa?

- W jaki sposób UE i państwa członkowskie mogą wzmocnić synergię między sektorem cywilnym i wojskowym zgodnie z ramami polityki w zakresie cyberobrony zaktualizowanymi w 2018 r.?

Skuteczne reagowanie na cyberincydenty

101 Opracowanie skutecznej reakcji na cyberataki ma zasadnicze znaczenie dla możliwie jak najwcześniejszego powstrzymania takich działań. Jest szczególnie istotne, by sektory o krytycznym znaczeniu, państwa członkowskie i instytucje UE były w stanie reagować w sposób szybki i skoordynowany. W tym kontekście bardzo ważne jest wczesne wykrywanie.

Wyzwanie 9 – Skuteczne wykrywanie i reagowanie

Wykrycie i powiadomienie

102 Powszechnie stosowane narzędzia wykrywania pomagają zwalczyć ogromną większość ataków spotykanych na co dzień[151]. Niemniej systemy cyfrowe stały się tak złożone, że zapobieżenie wszystkim ewentualnym atakom jest niemożliwe. Zaawansowany charakter ataków sprawia, że często pozostają one przez dłuższy czas niewykryte. W związku z tym specjaliści twierdzą, że należy zwrócić szczególną uwagę na wczesne wykrywanie i obronę[152]. Tymczasem niektóre narzędzia służące do wykrywania – takie jak automatyzacja, uczenie się maszyn i analiza zachowania, mające na celu ograniczenie ryzyka oraz analizowanie zachowania systemu i wyciąganie wniosków – są wciąż w niewielkim stopniu wdrażane przez przedsiębiorstwa[153]. Wynika to po części z występowania „fałszywych trafień", gdy niegroźne działania zostają omyłkowo uznane za niebezpieczne.

103 Po tym, jak naruszenie bezpieczeństwa zostanie wykryte i przeanalizowane, należy szybko je zgłosić i przesłać powiązane informacje, tak aby inne podmioty publiczne i prywatne mogły podjąć działania zapobiegawcze, a stosowne organy – zapewnić wsparcie ofiarom ataku. Wiele podmiotów ma opory, by przyznać się, że padły ofiarą cyberataku, i przekazywać informacje na ten temat[154]. Równie kluczowe są wczesne zaangażowanie organów ścigania w początkową reakcję na podejrzenie cyberprzestępstwa oraz aktywna wymiana informacji z CSIRT.

104 Fakt, że wcześniej nie istniały wspólne unijne wymogi dotyczące powiadamiania o incydentach, mógł skutkować opóźnionym informowaniem o naruszeniach bezpieczeństwa i utrudniać reakcję. Zaradzić temu miało przyjęcie dyrektywy w sprawie bezpieczeństwa sieci i informacji (zob. pkt ***20***). Po ataku Wannacry z 2017 r.

Komisja stwierdziła, że system sieci CSIRT „nie jest jeszcze w pełni operacyjny”[155]. Wdrażanie dyrektywy nadal trwa i trudno jest obecnie ocenić, czy wytyczne opracowane przez grupę współpracy staną się skutecznym narzędziem przezwyciężania oporów w zakresie informowania o incydentach[156].

105 Na mocy obowiązujących przepisów unijnych operatorzy usług kluczowych działający w określonych sektorach podlegają licznym obowiązkom w zakresie powiadamiania (w tym powiadamiania konsumentów), co może osłabiać wydajność całego procesu. Przykładowo, operatorzy w sektorze finansowym i bankowości muszą przestrzegać zróżnicowanych kryteriów, standardów, progów i terminów dotyczących powiadamiania w różnych ramach prawnych: RODO, dyrektywa w sprawie bezpieczeństwa sieci i informacji, druga dyrektywa w sprawie usług płatniczych, EBC / Jednolity Mechanizm Nadzorczy, TARGET2 oraz rozporządzenie eIDAS[157]. Należy zatem koniecznie udoskonalić kwestię tych obowiązków, gdyż nie tylko stanowią one niepotrzebne obciążenie administracyjne, ale także ich niejednorodność może doprowadzić do fragmentarycznej sprawozdawczości.

Skoordynowana reakcja

106 Opracowywanie europejskich ram współpracy w sytuacji cyberkryzysu wciąż trwa. W związku z tym wprowadzono powiązany plan działania[158] (zob. pkt ***18***), aby uwzględnić kwestię cyberbezpieczeństwa w zintegrowanych uzgodnieniach UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych, poprawić świadomość sytuacyjną i zapewnić lepszą integrację z innymi unijnymi mechanizmami zarządzania kryzysowego[159]. Plan działania zakłada udział instytucji i agencji UE oraz państw członkowskich. Bezproblemowe zintegrowanie wszystkich tych mechanizmów reagowania kryzysowego jest zadaniem trudnym[160]. Obecnie brak jest wspólnej zabezpieczonej sieci łączności między instytucjami unijnymi, co stanowi poważne niedociągnięcie[161].

107 Zdolność UE do reagowania na cyberataki na szczeblu operacyjnym i politycznym w przypadku transgranicznych incydentów na dużą skalę określono jako „ograniczoną”, po części dlatego, że cyberbezpieczeństwa nie uwzględniono jeszcze w istniejących na szczeblu unijnym mechanizmach koordynacji reagowania kryzysowego[162]. Dyrektywa w sprawie bezpieczeństwa sieci i informacji nie rozwiązała tego problemu.

108 Niedawno zaproponowana reforma ENISA, w ramach której agencji ma zostać przyznana większa operacyjna rola w reagowaniu na incydenty w zakresie

cyberbezpieczeństwa na dużą skalę, nie znalazła poparcia państw członkowskich. Wolały one, by rolą agencji było wspieranie i uzupełnianie działań operacyjnych prowadzonych przez same państwa[163]. Na szczeblu państw członkowskich funkcjonuje już wiele CERT / CSIRT, ale zdolności tych poszczególnych zespołów znacznie się różnią. Stanowi to przeszkodę dla skutecznej współpracy transgranicznej koniecznej do zapewnienia reakcji na incydenty na dużą skalę[164].

109 Trybunał postarał się rozpoznać różne role przypisane różnym podmiotom wskazanym w planie działania, niemniej stwierdzono luki, które należy wyeliminować w miarę postępów we wdrażaniu. Jednym z obszarów, którym początkowo poświęcono niewystarczająco wiele uwagi, były organy ścigania, choć unijny protokół działań w zakresie egzekwowania prawa w sytuacjach kryzysowych wszedł w życie w grudniu 2018 r.[165] Kluczowe dla powodzenia działań jest, by plan działania miał charakter praktyczny, a każda z zaangażowanych stron wiedziała, jakie zadania ma wypełniać. Wymagać to będzie kompleksowego testowania w kolejnych latach.

110 Skuteczna reakcja wymaga czegoś więcej niż tylko ograniczenia szkód. Równie istotne jest również wskazanie odpowiedzialnych za ataki. Śledzenie i wskazywanie sprawców, przede wszystkim w przypadku ataków o charakterze hybrydowym, może być bardzo trudne ze względu na coraz powszechniejsze niewłaściwe wykorzystanie narzędzi anonimizacji, kryptowalut i szyfrowania. Zjawisko to jest znane pod nazwą problemu przypisania odpowiedzialności. Rozwiązanie tego problemu nie jest jedynie zagadnieniem technicznym, ale stanowi również wyzwanie dla wymiaru sprawiedliwości w sprawach karnych. Prawne i proceduralne różnice między krajami mogą utrudniać postępowania karne i ściganie przestępców. Zajęcie się problemem przypisania odpowiedzialności wymagać będzie bardziej sformalizowanej wymiany informacji na szczeblu operacyjnym z wykorzystaniem bardziej przejrzystych procedur przy udziale np. Europolu lub europejskiej sieci sądowej ds. cyberprzestępczości Eurojustu.

111 Na szczeblu politycznym opracowano zestaw narzędzi dla dyplomacji cyfrowej (zob. ***ramka 6***), aby ułatwić rozstrzyganie międzynarodowych sporów w cyberprzestrzeni za pomocą środków pokojowych. W ramach PESCO opracowywane są obecnie dwa projekty promujące zwiększoną wymianę informacji: utworzenie zespołów szybkiego reagowania na cyberincydenty oraz inicjatywa dotycząca pomocy wzajemnej w zakresie cyberbezpieczeństwa[166].

Ramka 6

Zestaw narzędzi dla dyplomacji cyfrowej

Ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni[167], czyli „zestaw narzędzi dla dyplomacji cyfrowej", stanowiły owoc konkluzji Rady w sprawie dyplomacji cyfrowej[168]. Dyplomacja cyfrowa ma na celu opracowanie i przyjęcie wspólnego kompleksowego podejścia do cyberprzestrzeni w oparciu o unijne wartości, praworządność, budowanie potencjału i partnerstwa, promowanie modelu zarządzania internetem zakładającego udział wielu stron oraz ograniczenie zagrożeń w dziedzinie cyberbezpieczeństwa i większą stabilność w stosunkach międzynarodowych.

Zestaw narzędzi pozwala UE i państwom członkowskim przygotować dyplomatyczną reakcję na szkodliwe działania w cyberprzestrzeni z pełnym wykorzystaniem działań dostępnych w ramach wspólnej polityki zagranicznej i bezpieczeństwa. Mogą one obejmować działania zapobiegawcze (np. podnoszenie świadomości, budowanie potencjału), działania w zakresie współpracy, zapewnienia stabilności, a także sankcje (np. zakazy podróżowania, embargo na broń, zamrożenie funduszy) oraz wsparcie reakcji podejmowanych przez państwa członkowskie[169]. U podstaw tej koncepcji leży przekonanie, że zacieśniona współpraca w zakresie zwalczania zagrożeń i jednoznaczne wskazanie konsekwencji wynikających ze wspólnej reakcji mogą zniechęcić do (ewentualnych) agresywnych zachowań.

Wszelkie wspólne działania UE w odpowiedzi na wrogie działania w cyberprzestrzeni będą proporcjonalne do zakresu, skali, czasu trwania, intensywności, złożoności, zaawansowania i skutków takich działań.

Kluczowe dla powodzenia zestawu narzędzi będzie, w jaki sposób zostanie on zintegrowany z planem działania oraz zintegrowanymi uzgodnieniami UE dotyczącymi reagowania na szczeblu politycznym w sytuacjach kryzysowych (zob. pkt ***106***), w jaki sposób zapewniona zostanie świadomość sytuacyjna dzięki szybkiej i nieprzerwanej wymianie informacji (w tym informacji pozwalających przypisać odpowiedzialność)[170], a także skutecznej współpracy. Równie istotna dla udanego wdrożenia zestawu narzędzi jest skuteczna i skoordynowana komunikacja. Do tej pory z zestawu narzędzi skorzystano dwukrotnie – w celu rozpoczęcia dialogu ze Stanami Zjednoczonymi po ataku Wannacry[171] oraz przy opracowywaniu konkluzji Rady potępiających szkodliwe działania w cyberprzestrzeni[172]. Operacjonalizacja narzędzi zawartych w zestawie wciąż trwa i w tej chwili trudno jest jeszcze ocenić, czy zestaw będzie skuteczny w osiąganiu wyznaczonych celów.

Wyzwanie 10 – Ochrona infrastruktury krytycznej i funkcji społecznych

Ochrona infrastruktury

112 Duża część unijnej infrastruktury krytycznej jest obsługiwana za pomocą systemów kontroli przemysłowej[173]. Wiele z nich zostało pomyślanych jako autonomiczne systemy, w niewielkim stopniu połączone ze światem zewnętrznym. W miarę jak elementy tych systemów podłączano do internetu, stawały się one bardziej narażone na ingerencję z zewnątrz. Utrzymywanie i aktualizowanie obecnych systemów może już nie być możliwe, niemniej ich modernizacja jest procesem kosztownym i długotrwałym. Starania na rzecz poprawy bezpieczeństwa infrastruktury krytycznej muszą więc obejmować modernizację systemów kontroli przemysłowej.

113 Coraz powszechniejsza cyfryzacja przemysłu (proces znany pod nazwą „Przemysłu 4.0") sprawia, że skutki incydentu na dużą skalę zaistniałego w jednym sektorze mogą, ze względu na efekt domina, być odczuwalne w innych. ENISA zwróciła uwagę na znaczenie rozpoznania skutków wzajemnych zależności między sektorami o krytycznym znaczeniu[174]. Jest to szczególnie istotne dla zrozumienia potencjalnego rozprzestrzeniania się incydentu i stanowi podstawę dla wypracowania odpowiednio skoordynowanej reakcji.

114 Dyrektywa w sprawie bezpieczeństwa sieci i informacji ma poprawić gotowość w kluczowych sektorach odpowiedzialnych za infrastrukturę krytyczną. Niemniej nie wszystkie sektory są objęte zakresem przepisów (zob. ***tabela 1***)[175], co „ogranicza skuteczność strategii"[176]. Szczególny niepokój w tym względzie budzi ochrona integralności demokratycznych wyborów przed ingerencją w infrastrukturę wyborczą i przed dezinformacją (zob. ***ramka 7***). Zasadniczym wyzwaniem, obok zmiany obowiązujących przepisów, jest zbadanie, w jaki sposób można zaangażować te sektory w skuteczne reagowanie na incydenty na dużą skalę.

115 Szczególnie narażone elementy infrastruktury krytycznej nie występują jedynie w Europie. Istotnym wyzwaniem dla Komisji jest zachęcenie krajów kandydujących do przyjęcia takich samych standardów jak obowiązujące w państwach członkowskich w obszarach takich jak przepisy dotyczące cyberprzestrzeni lub ochrona infrastruktury krytycznej.

Ramka 7

Ochrona funkcji społecznych o krytycznym znaczeniu – zwalczanie ingerencji w proces wyborczy

W maju 2019 r. ok. 400 mln wyborców weźmie udział w wyborach do Parlamentu Europejskiego. Będą to pierwsze wybory do PE od czasu wejścia w życie RODO. Wybory poprzedził szereg skandali związanych z niewłaściwym wykorzystaniem danych osobowych do indywidualnego dobierania reklamy politycznej (tzw. mikrotargetowania wyborców) oraz bezprecedensowymi skoordynowanymi kampaniami dezinformacyjnymi (tzw. fałszywymi informacjami). Komisja ostrzegła, że cyfrowa ingerencja w te wybory jest prawdopodobna[177]. Zwalczenie takiej ingerencji będzie wymagało przyjęcia podejścia zakładającego udział wszystkich organów państwowych i całego społeczeństwa.

Infrastruktura wyborcza

Organizowanie wyborów jest zadaniem złożonym, a odpowiedzialność za zapewnienie integralności i ochrony procesu wyborczego spoczywa na państwach członkowskich. Ingerencja w wybory i infrastrukturę wyborczą może mieć na celu wpłynięcie na preferencje wyborców, frekwencję lub sam proces wyborczy, w tym faktyczne głosowanie oraz zestawianie i przekazywanie wyników głosowania. W wyborach do Parlamentu Europejskiego szczególnie istotne jest zapewnienie ochrony tzw. ostatniej mili (przekazywanie wyników głosowania ze stolic krajowych do Brukseli), zważywszy że nie ma ani nie przetestowano obecnie żadnego wspólnego podejścia w zakresie bezpieczeństwa dla tej procedury[178].

Pakiet wyborczy niedawno przedstawiony przez Komisję obejmował działania mające na celu wzmocnienie cyberbezpieczeństwa wyborów, takie jak wyznaczenie krajowych punktów kontaktowych do koordynacji działań i wymiany informacji w okresie poprzedzającym wybory. Szczególnie istotna jest wymiana najlepszych praktyk i wniosków z doświadczeń[179].

Systemów wyborczych nie uznaje się za część infrastruktury krytycznej[180]. Nie są one też objęte zakresem dyrektywy w sprawie bezpieczeństwa sieci i informacji. Pomimo tego grupa współpracy opracowała praktyczne wytyczne dotyczące bezpieczeństwa technologii wyborczych, aby wesprzeć organy publiczne. Spotkanie krajowych punktów kontaktowych przewidziano na początek 2019 r.[181] Ponadto zachęca się państwa członkowskie, by przeprowadziły oceny ryzyka dotyczące krajowych procesów wyborczych.

Dezinformacja

Dezinformacja stanowi coraz istotniejszy element ataków hybrydowych, które obejmują cyberataki i włamywanie się do sieci. Wykorzystuje się ją do wprowadzania podziałów w społeczeństwach, siania nieufności i podważania zaufania do procesów demokratycznych oraz w innych kwestiach (np. ruchy antyszczepionkowe lub zmiana klimatu). Dezinformacja szerzy się na coraz większą skalę, z coraz większą prędkością

i obejmuje coraz większy zakres tematów, stanowiąc istotne zagrożenie w dziedzinie bezpieczeństwa dla Unii.

UE podjęła ostatnio szereg działań mających na celu zwalczenie tego problemu. W 2015 r. utworzono w obrębie ESDZ grupę zadaniową East StratCom mającą rozwiązać problem rosyjskich kampanii dezinformacyjnych[182]. Specjaliści z zadowoleniem przyjęli prace grupy na rzecz promowania polityki UE, wspierania niezależnych mediów w regionie europejskiego sąsiedztwa oraz antycypowania, śledzenia i zwalczania dezinformacji[183]. Należy jednak pamiętać, że zasoby grupy roboczej pozostają ograniczone względem skali i złożoności kampanii dezinformacyjnych[184]. Należy zapewnić bardziej systematyczne współdziałanie między istniejącymi już strukturami unijnymi oraz usprawnić współpracę w zakresie komunikacji strategicznej[185]. W grudniu 2018 r. Rada Europejska poparła nowy plan działania[186].

Niedawno Komisja opracowała – opierając się na przedstawionym w kwietniu 2018 r. komunikacie w sprawie zwalczania dezinformacji w internecie[187] – dobrowolny kodeks postępowania w ramach samoregulacji[188], bazujący na istniejących instrumentach politycznych, do których stosowania zobowiązały się już platformy internetowe i branża reklamowa[189]. Działanie obejmuje pomoc w zwiększeniu wiarygodności treści oraz wspieranie wysiłków na rzecz zwiększenia umiejętności medialnych i informacyjnych. Uruchomiono również niezależną europejską sieć osób weryfikujących fakty.

Komisja stwierdziła, że jeśli ten kodeks postępowania nie będzie przestrzegany, mogą zostać wprowadzone dalsze środki regulacyjne. Określenie skuteczności tych środków będzie miało kluczowe znaczenie, zwłaszcza jeśli chodzi o wybór metody pomiaru postępów w poziomie zaufania, przejrzystości i rozliczalności.

Kolejnym wyzwaniem będzie znalezienie sposobów na usprawnienie wykrywania, analizy i narażenia na dezinformację[190]. Konieczne jest ponadto aktywne i strategiczne monitorowanie i analiza danych z otwartych źródeł[191]. Starania na rzecz lepszego zrozumienia środowiska zagrożeń powinny uwzględniać pojawiające się tendencje, takie jak tzw. deepfake (czyli fałszywe materiały wideo wytworzone za pomocą sztucznej inteligencji i głębokiego uczenia maszynowego), a także narzędzia konieczne do wykrycia tych zjawisk.

Zwiększenie autonomii

116 UE jest importerem netto produktów i usług w dziedzinie cyberbezpieczeństwa, co zwiększa ryzyko technologicznego uzależnienia od podmiotów spoza UE oraz powiązane narażenie[192]. W szczególności sytuacja ta osłabia bezpieczeństwo infrastruktury krytycznej w UE. Ponadto infrastruktura jest wspierana za

pośrednictwem złożonych globalnych łańcuchów dostaw. Zagrożenie jest jeszcze większe w sytuacji, gdy podmioty spoza UE zakupują europejskie przedsiębiorstwa działające w sektorze cyberbezpieczeństwa. Za monitorowanie bezpośrednich inwestycji zagranicznych odpowiadają państwa członkowskie i obecnie nie ma ogólnounijnego mechanizmu monitorowania w tej dziedzinie[193].

117 Większa autonomia strategiczna stanowi cel globalnej strategii Unii Europejskiej i komunikatu z 2017 r. pt. „Odporność, prewencja i obrona”[194]. Podjęcie wielorakich wyzwań wskazanych w niniejszym dokumencie pomoże w zwiększeniu tej pożądanej autonomii. Żadne pojedyncze działanie nie pozwoli osiągnąć tego celu.

Kwestie do rozważenia – skuteczna reakcja

- W jaki sposób dyrektywa w sprawie bezpieczeństwa sieci i informacji usprawniła proces powiadamiania o cyberincydentach w sektorach o krytycznym znaczeniu i poza tymi sektorami?
- W jakim stopniu instytucje UE wcieliły w życie mechanizmy koordynacji reagowania kryzysowego na wypadek cyberincydentu na dużą skalę?
- Na czym mogłaby polegać istotniejsze rola dyplomacji cyfrowej w ramach działań zewnętrznych UE?
- Czy obecne struktury i działania UE w zakresie zwalczania dezinformacji są proporcjonalne do skali i zjawiska problemu?

Uwagi końcowe

118 W ostatnich latach Unia Europejska i państwa członkowskie nadały cyberbezpieczeństwu wyższy priorytet w swoich działaniach z myślą o zwiększeniu ogólnej cyberodporności. Osiągnięcie wyższego poziomu cyberbezpieczeństwa w UE jest jednak przedsięwzięciem na ogromną skalę. W niniejszym dokumencie analitycznym Trybunał starał się wskazać niektóre z zasadniczych wyzwań związanych z unijną ambicją, by stworzyć najbezpieczniejsze środowisko cyfrowe na świecie.

119 Przeprowadzony przez Trybunał przegląd wskazuje, że do zapewnienia rzetelnej **rozliczalności i oceny** konieczne jest przejście na kulturę organizacyjną ukierunkowaną na wyniki i powiązaną z ugruntowanymi praktykami oceny. **Wciąż utrzymują się pewne luki w prawie, a obowiązujące przepisy nie są transponowane w sposób spójny przez państwa członkowskie**. Utrudnia to wykorzystanie pełnego potencjału tkwiącego w prawodawstwie. Inne rozpoznane wyzwanie dotyczy **dostosowania poziomów inwestycji do celów strategicznych**, co wymaga podniesienia tych poziomów i zwiększenia oddziaływania inwestycji. Zadanie to jest jeszcze trudniejsze w sytuacji, gdy UE i państwa członkowskie nie posiadają **jasnego obrazu wydatków unijnych** w dziedzinie cyberbezpieczeństwa. Odnotowuje się również **niedostatki odpowiednich zasobów w unijnych agencjach zajmujących się cyberprzestrzenią**, w tym trudności w przyciąganiu i zatrzymywaniu utalentowanych pracowników.

120 Dostępne badania wskazują, że **zarządzanie w dziedzinie cyberbezpieczeństwa można usprawnić**, tak aby stymulować zdolność społeczności międzynarodowej do reagowania na cyberataki i cyberincydenty. Jednocześnie należy zauważyć, że zapobieżenie wszystkim atakom nie jest możliwe. Z tego względu należy w pierwszej kolejności skoncentrować działania na **szybkim wykrywaniu i reagowaniu** oraz **ochronie infrastruktury i funkcji społecznych o krytycznym znaczeniu**, wraz z lepszą **wymianą informacji i koordynacją działań** między sektorami publicznym i prywatnym. Wreszcie, coraz bardziej odczuwalny w skali globalnej niedostatek umiejętności w zakresie cyberbezpieczeństwa oznacza, że równie istotne jest **podnoszenie umiejętności i świadomości** we wszystkich sektorach i grupach społecznych.

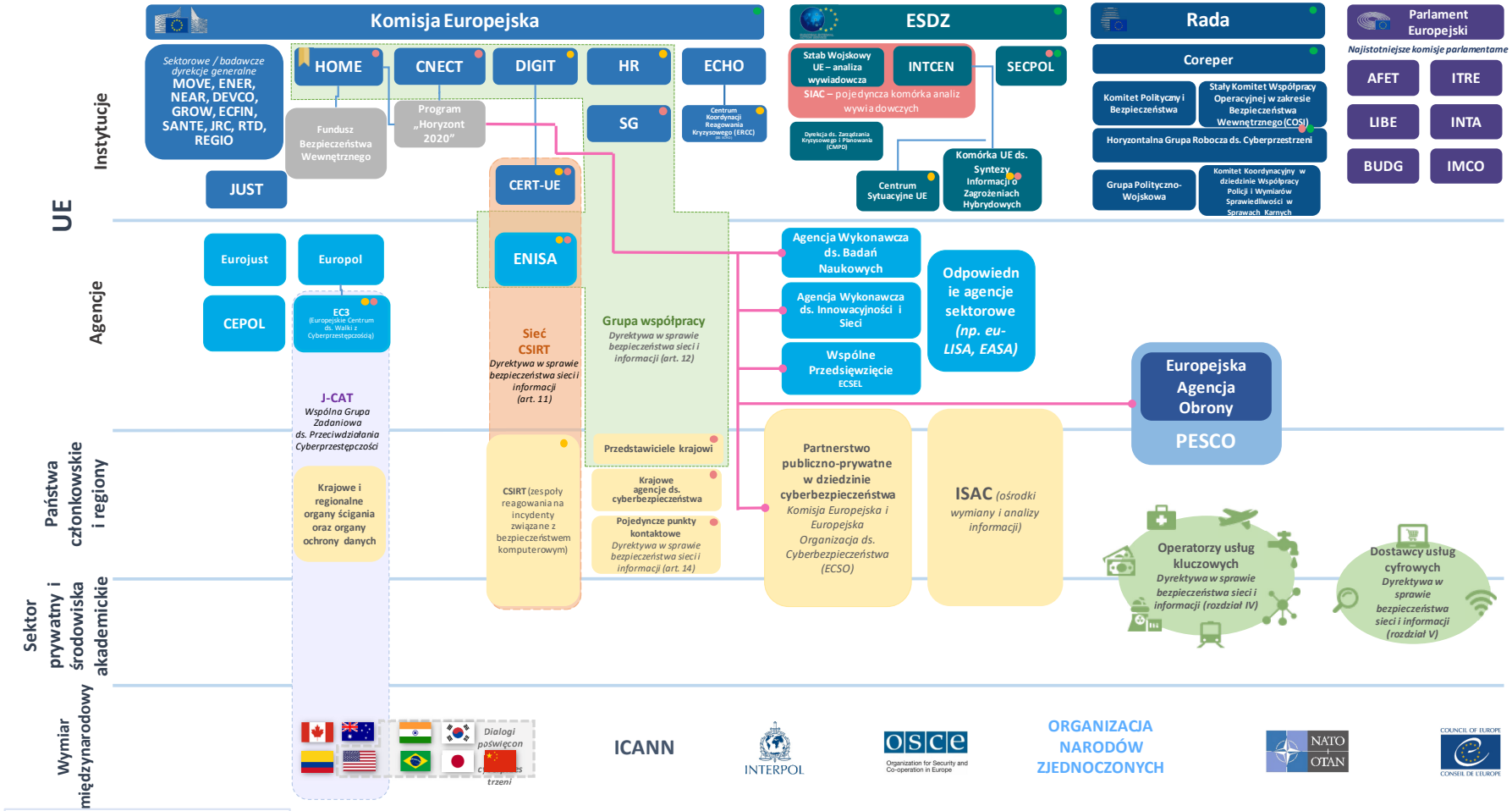
121 Te wyzwania związane z cyberzagrożeniami, którym musi stawić czoła UE, i ogólny rozwój sytuacji na świecie wymagają ciągłego zaangażowania ze strony UE i nieustannego, pełnego determinacji obstawania przy unijnych wartościach.

Niniejszy dokument zostały przyjęty przez Izbę III na posiedzeniu w dniu 14 lutego 2019 r.

W imieniu Europejskiego Trybunału Obrachunkowego

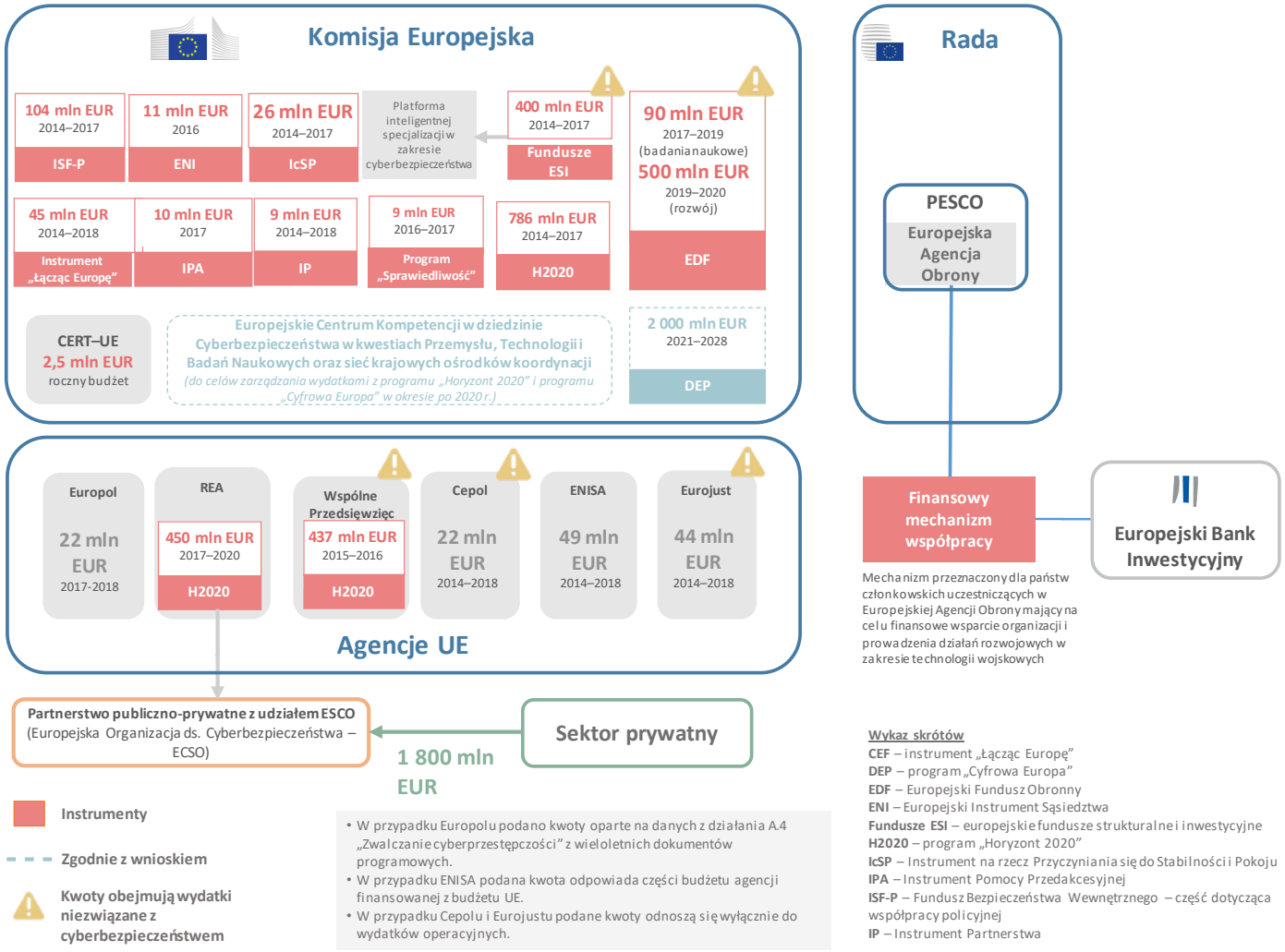
Klaus-Heiner Lehne
Prezes

Załącznik I — Złożone i wielowarstwowe środowisko obejmujące udział wielu podmiotów



Źródło: Europejski Trybunał Obrachunkowy.

Załącznik II — Unijne wydatki na cyberbezpieczeństwo od 2014 r.



Źródło: Europejski Trybunał Obrachunkowy na podstawie dokumentów Komisji i agencji UE.

Załącznik III — Sprawozdania organów kontroli działających w państwach członkowskich UE

Rodzaj dokumentu	Tytuł (wraz z łączem)	Rok publikacji	P. członk.
Kontrole zgodności	Nota z oceny przeprowadzonej w ramach kontroli wewnętrznej	2014	FR
	Sprawozdanie poświadczające rachunki ogólnego systemu zabezpieczenia społecznego (obrona, sprawy zagraniczne)	2016	FR
	Poświadczenie rachunków państwa	2016	FR
	Zapewnienie bezpieczeństwa i ochrona estońskich krajowych baz danych o krytycznym znaczeniu	Koniec 2018 r. / jeszcze nie opublikowano	EE
	Skuteczność wewnętrznych mechanizmów kontroli w zakresie ochrony danych osobowych w krajowych bazach danych	2008	EE
Kontrole wykonania zadań / kontrole gospodarnego wykorzystania środków	Sprawozdanie w sprawie łagodzenia skutków cyberataków	2013	DK
	Sprawozdanie RiR 2014:23 w sprawie bezpieczeństwa informacji w cywilnych organach administracji publicznej	2014	SE
	Sprawozdanie w sprawie przetwarzania przez organy rządowe niejawnych danych dotyczących osób fizycznych i przedsiębiorstw	2014	DK
	Krajowy program w zakresie cyberbezpieczeństwa	2014	UK
	Sprawozdanie przedłożone Komitetowi ds. Budżetu niemieckiego parlamentu federalnego zgodnie z art. 88 ust. 2 federalnego kodeksu budżetowego – konsolidacja IT, rząd federalny	2015	DE
	Sprawozdanie w sprawie dostępu do systemów informatycznych, które wspierają świadczenie usług kluczowych na rzecz duńskiego społeczeństwa	2015	DK
	Plaine de France – organ publiczny ds. planowania	2015	FR
	Sytuacja w zakresie cyberbezpieczeństwa na Litwie Wersja w języku litewskim Streszczenie przetłumaczone na język angielski	2015	LT
	Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP (w języku polskim)	2015	PL
	Sprawozdanie RiR 2015:21 w sprawie cyberprzestępczości – można poprawić wydajność działań policji i prokuratorów	2015	SE
	Luka w zakresie umiejętności cyfrowych w organach rządowych (badanie ankietowe)	2015	UK
	Sprawozdanie przedłożone parlamentowi federalnemu w sprawie finansów na szczeblu federalnym – pobór podatku od spadków	2016	BE
	Sprawozdanie w sprawie zarządzania bezpieczeństwem informatycznym w przypadku systemów powierzonych dostawcom zewnętrznym	2016	DK
	Sprawozdanie z kontroli dotyczące działalności pożyczkowej Instituto de Crédito Oficial za 2016 r.	2016	ES
	Kierowanie rządową siecią bezpieczeństwa	2016	FI

Rodzaj dokumentu	Tytuł (wraz z łączem)	Rok publikacji	P. członk.
	Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych	2016	PL
	Zapobieganie i przeciwdziałanie cyberprzemocy wśród dzieci i młodzieży	2016	PL
	Działania w zakresie bezpieczeństwa informacji w dziewięciu agencjach – Inne kontrole bezpieczeństwa informacji w organach państwowych. RiR 2016:8	2016	SE
	Ochrona informacji we wszystkich agendach rządowych	2016	UK
	Sprawozdanie w sprawie ochrony systemów informatycznych i danych dotyczących zdrowia w trzech duńskich regionach	2017	DK
	Nota w sprawie wyników prowadzonej równolegle międzynarodowej kontroli pn. „Skuteczność wewnętrznych mechanizmów kontroli w zakresie ochrony danych osobowych w krajowych bazach danych”	2017	EE
	Rozwiązania w zakresie cyberobrony	2017	FI
	Zarządzanie kwestią operacyjnej niezawodności urządzeń elektronicznych	2017	FI
	Sieć Izb Rolniczych (podsumowanie)	2017	FR
	Izba Przemysłowo-Handlowa Vaucluse (dokument sporządzony przez regionalną izbę obrachunkową regionu Prowansja-Alpy-Lazurowe Wybrzeże)	2017	FR
	Zapewnienie bezpieczeństwa i ochrona estońskich krajowych baz danych o krytycznym znaczeniu	Koniec 2018 r. / jeszcze nie opublikowano	EE
	Rozwój infrastruktury państwowej łączności elektronicznej Wersja w języku litewskim Streszczenie przetłumaczone na język angielski	2017	LT
	Kontrola dotycząca technologii informacyjnej –cyberbezpieczeństwo w podmiotach rządowych	2017	MT
	System rejestrów państwowych – bezpieczeństwo, funkcjonowanie i użyteczność	2017	PL
	Incydent WannaCry	2017	UK
	Oszustwa w internecie	2017	UK
	Sprawozdanie w sprawie ochrony przed atakami typu ransomware	2018	DK
	Szpital Arpajon (dokument sporządzony przez regionalną izbę obrachunkową w regionie Île-de-France)	2018	FR
	Zarządzanie państwowymi zasobami informatycznymi o znaczeniu krytycznym	2018	LT
	Przestępstwa elektroniczne	2019	LT
	Bezpieczeństwo teleinformatyczne Polski	2019	PL
	Baza danych organów publicznych	nd.	BE
Inne	Kwestionariusz w sprawie polityki w zakresie bezpieczeństwa i analizy ryzyka (w toku)	nd.	BE

Wykaz skrótów

CERT-UE – Zespół reagowania na incydenty komputerowe

CSIRT – Zespół Reagowania na Incydenty związane z Bezpieczeństwem Komputerowym

DG CNECT – Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii

DG HOME – Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych

DG JUST – Dyrekcja Generalna ds. Sprawiedliwości i Konsumentów

DIGIT – Dyrekcja Generalna ds. Informatyki

EC3 – Europejskie Centrum ds. Walki z Cyberprzestępczością Europolu

ECSEL – Wspólne Przedsięwzięcie „Podzespoły i układy elektroniczne w służbie wiodącej pozycji Europy”

ECSO – Europejska Organizacja ds. Cyberbezpieczeństwa

ENISA – Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji

ESDZ – Europejska Służba Działań Zewnętrznych

Fundusze ESI – europejskie fundusze strukturalne i inwestycyjne

JRC – Wspólne Centrum Badawcze

LISO – lokalny pełnomocnik ds. bezpieczeństwa teleinformatycznego

MŚP – małe i średnie przedsiębiorstwa

PESCO – stała współpraca strukturalna

RODO – ogólne rozporządzenie o ochronie danych

Trybunał – Europejski Trybunał Obrachunkowy

UE – Unia Europejska

WPBiO – wspólna polityka bezpieczeństwa i obrony

Glosariusz

Bezpieczeństwo informacji – zestaw procesów i narzędzi chroniących dane fizyczne i cyfrowe przed nieuprawnionym dostępem, wykorzystaniem, ujawnieniem, naruszeniem, modyfikacją, rejestracją lub zniszczeniem.

Bezpieczeństwo sieci – poddziedzina cyberbezpieczeństwa dotycząca ochrony danych przesyłanych za pomocą urządzeń w ramach tej samej sieci w celu zagwarantowania, że informacja nie zostanie przechwycona ani zmodyfikowana.

Botnet – sieć komputerów zainfekowana złośliwym oprogramowaniem i zdalnie kontrolowana, bez wiedzy użytkowników. Wykorzystywana do wysyłania spamu, wykradania informacji lub uruchamiania skoordynowanych cyberataków.

Cyberatak – próba naruszenia lub zniszczenia poufności, integralności lub dostępności danych lub systemów komputerowych z wykorzystaniem cyberprzestrzeni.

Cyberbezpieczeństwo – wszystkie zabezpieczenia i środki przyjęte w celu ochrony systemów informacyjnych i powiązanych danych przed nieuprawnionym dostępem, atakiem lub szkodą, tak aby zapewnić poufność, integralność i dostępność informacji.

Cyberincydent – wydarzenie, które w sposób pośredni lub bezpośredni szkodzi lub zagraża odporności lub bezpieczeństwu danego systemu informatycznego i danym przetwarzanym, przechowywanym lub przesyłanym przez ten system.

Cyberobrona – poddziedzina cyberbezpieczeństwa, która ma na celu obronę cyberprzestrzeni środkami wojskowymi i za pomocą innych odpowiednich działań, aby osiągnąć cele strategiczno-wojskowe.

Cyberodporność – zdolność do zapobiegania cyberatakom i incydentom, przygotowania się do nich, przetrwania ich, a także do przywrócenia działalności po cyberatakach i incydentach.

Cyberprzestępczość – różne rodzaje działalności przestępczej, w przypadku której komputery i systemy informatyczne stanowią podstawowe narzędzie przestępcze lub są głównym celem działania przestępczego. Obejmuje ona: tradycyjne przestępstwa (np. nadużycia finansowe, fałszerstwa i kradzież tożsamości), przestępstwa związane z treściami (np. dystrybucja w internecie pornografii dziecięcej lub nawoływanie do nienawiści rasowej) oraz przestępstwa typowe dla komputerów i systemów informatycznych (np. ataki na systemy informatyczne, w tym ataki prowadzące do zablokowania usług, oraz złośliwe oprogramowanie).

Cyberprzestrzeń – niematerialne globalne środowisko, w którym za pośrednictwem sieci komputerowych i urządzeń technicznych odbywa się sieciowa komunikacja między ludźmi, oprogramowaniem i usługami.

Cyberśrodowisko – złożony zbiór współdziałających urządzeń, danych, sieci, osób, procesów i podmiotów oraz środowisko złożone z procesów i technologii wpływających na to współdziałanie i je wspierających.

Dane na temat dostępu – informacje na temat czynności logowania się i wylogowania się użytkownika w związku z dostępem do usługi, takie jak data, godzina i adres IP.

Dane osobowe – informacje dotyczące możliwej do zidentyfikowania osoby fizycznej.

Dezinformacja – możliwe do zweryfikowania nieprawdziwe lub wprowadzające w błąd informacje, tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną.

Dostępność – zapewnienie terminowego i wiarygodnego dostępu do informacji i korzystania z informacji.

Haktywiści – osoby fizyczne lub grupy, które uzyskują nieuprawniony dostęp do systemów informacyjnych lub sieci z myślą o osiągnięciu określonych celów politycznych lub społecznych.

Infrastruktura krytyczna – obiekty, usługi i zasoby fizyczne, w przypadku których zaburzenie funkcjonowania lub zniszczenia poważnie wpłynęłoby na funkcjonowanie gospodarki i społeczeństwa.

Infrastruktura wyborcza – obejmuje systemy informatyczne i bazy danych na potrzeby kampanii wyborczych, szczególnie chronione informacje na temat kandydatów, systemy rejestracji wyborców i systemy zarządcze.

Integralność – ochrona przed niewłaściwą modyfikacją lub zniszczeniem informacji oraz zagwarantowanie jej autentyczności.

Internet rzeczy – sieć przedmiotów codziennego użytku wyposażonych w układy elektroniczne, oprogramowanie i czujniki, tak że mogą one łączyć się i wymieniać dane za pośrednictwem internetu.

Kryptowaluta – zasób cyfrowy, który jest wytwarzany i wymieniany z wykorzystaniem technik szyfrowania, niezależnie od banku centralnego. Kryptowaluty są akceptowalnym środkiem płatniczym wśród członków społeczności internetowych.

Łatka na oprogramowanie – zestaw zmian w oprogramowaniu mający na celu aktualizację, naprawę lub usprawnienie działania, w tym usunięcie luk w zakresie bezpieczeństwa.

Manipulacje z zakresu inżynierii społecznej – w dziedzinie bezpieczeństwa informacji oznaczają one psychologiczną manipulację mającą sprawić, że użytkownicy wykonają określoną czynność lub ujawnią poufne informacje.

Model „przestępstwa na zlecenie" – model działalności przestępczej powszechnie występujący w nielegalnej gospodarce cyfrowej. Polega na zapewnianiu szerokiego zakresu usług i narzędzi komercyjnych pozwalających niewykwalifikowanym, niedoświadczonym cyberprzestępcom dokonywać cyberprzestępstw.

Oprogramowanie reklamowe – złośliwe oprogramowanie wyświetlające banery reklamowe lub wyskakujące okienka, w których zamieszcza się kod śledzący zachowania zainfekowanych użytkowników w internecie.

Oprogramowanie typu ransomware – złośliwe oprogramowanie, które uniemożliwia ofierze dostęp do systemu komputerowego lub sprawia, że nie można odczytać plików, zazwyczaj za sprawą szyfrowania. Atakujący szantażuje następnie ofiarę, uzależniając przywrócenie dostępu do systemu od opłacenia przez ofiarę okupu.

Phishing – praktyka polegająca na wysyłaniu pocztą elektroniczną wiadomości, które sprawiają wrażenie wiadomości pochodzących z wiarygodnego źródła, tak aby skłonić odbiorców do kliknięcia w łącza, za którymi kryje się złośliwe oprogramowanie, lub do udostępnienia danych osobowych.

Poufność – ochrona informacji, danych i zasobów przed nieuprawnionym dostępem lub ujawnieniem.

Przestępstwo wykorzystujące cybernarzędzia – tradycyjne przestępstwo popełnione na większą skalę dzięki wykorzystaniu systemów informatycznych.

Przestępstwo wymagające cybernarzędzi – przestępstwo, które można popełnić wyłącznie z wykorzystaniem urządzeń informatycznych.

Przetwarzanie w chmurze – zapewnienie zasobów informatycznych na żądanie – takich jak zdolność przechowywania, moce obliczeniowe lub zdolności do wymiany danych – za pośrednictwem sieci dzięki usługom hostingowym na zdalnych serwerach.

Rozproszony atak typu „odmowa usługi" – cyberatak uniemożliwiający właściwym użytkownikom dostęp do sieciowej usługi lub zasobu przez zalanie systemu ogromną ilością zapytań, których nie sposób obsłużyć.

Skimming – kradzież danych karty płatniczej lub kredytowej wprowadzonych online.

Systemy tradycyjne – przestarzałe lub nieaktualne systemy komputerowe, aplikacje i języki programowania, które wciąż są w użytku, ale w przypadku których aktualizacje i wsparcie sprzedawców – w tym wsparcie w zakresie bezpieczeństwa – mogą nie być dostępne.

Szyfrowanie – przekształcenie informacji gotowych do odczytu w niemożliwy do odczytania kod w celu ochrony danych. Aby odczytać informacje, użytkownik musi mieć dostęp do tajnego kodu lub hasła.

Treści cyfrowe – wszelkie dane – takie jak tekst, dźwięk, obraz lub wideo – przechowywane w formacie cyfrowym.

Usługi zaufania – usługi zwiększające moc prawną transakcji elektronicznej, takie jak podpisy elektroniczne, pieczęcie, znaki czasu, rejestrowane doręczenie i uwierzytelnianie stron internetowych.

Wektoryzacja tekstu – proces zamierzający do przekształcenia słów, zdań lub całych dokumentów w wektory cyfrowe, tak aby nadawały się one do wykorzystania w uczeniu się maszyn.

Zagrożenie hybrydowe – wrogie działania, w których przeciwnik wykorzystuje połączenie tradycyjnych i nietradycyjnych technik prowadzenia wojny (tj. metod wojskowych, politycznych, gospodarczych i technologicznych) do osiągnięcia siłowo własnych celów.

Zarządzanie podatnością na zagrożenia – integralna część bezpieczeństwa komputerów i sieci, polegająca na aktywnym zapobieganiu wykorzystaniu luk w systemach lub w oprogramowaniu lub ograniczaniu skutków takiego wykorzystania przez rozpoznawanie i klasyfikowanie tych luk oraz działania naprawcze.

Zestawy do exploitów – rodzaj zestawu narzędzi, który cyberprzestępcy stosują przy atakowaniu słabych punktów sieci i systemów informacyjnych do instalowania złośliwego oprogramowania i innych działań prowadzonych w złej wierze.

Złośliwe oprogramowanie – program komputerowy, który ma na celu uszkodzenie komputera, serwera lub sieci.

Złośliwe oprogramowanie usuwające dane – rodzaj złośliwego oprogramowania, które ma usunąć dane z dysku twardego zainfekowanego komputera.

[1] W projekcie unijnego aktu ws. cyberbezpieczeństwa zdefiniowano je jako „wszystkie działania niezbędne do ochrony przed zagrożeniami dla cyberbezpieczeństwa sieci i systemów informatycznych, ich użytkowników oraz osób, których zagrożenia te dotyczą". Akt ma zostać przyjęty przez Parlament Europejski i Radę z początkiem 2019 r.

[2] Europol, „Internet Organised Crime Threat Assessment 2017" [Ocena zagrożenia zorganizowaną przestępczością w internecie z 2017 r.].

[3] Europejska Organizacja ds. Cyberbezpieczeństwa (European Cyber Security Organisation – ESCO), „European Cybersecurity Industry Proposal for a contractual Public-Private Partnership" [Propozycja europejskiej branży zajmującej się cyberbezpieczeństwem dotycząca stworzenia umownego partnerstwa publiczno-prywatnego], czerwiec 2016 r.

[4] Parlament Europejski, „Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses" [Cyberbezpieczeństwo w Unii Europejskiej i poza jej granicami: przegląd zagrożeń i politycznych reakcji na te zagrożenia], badanie zlecone przez Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych PE, wrzesień 2015 r.

[5] ENISA, „ENISA Threat Landscape Report 2017" [Sprawozdanie ENISA z 2017 r. zawierające przegląd zagrożeń], 18 stycznia 2018 r.

[6] Europol, „Internet Organised Crime Threat Assessment 2018".

[7] Europol, tamże, 2018.

[8] European Centre for Political Economy, „Stealing Thunder: Will cyber espionage be allowed to hold Europe back in the global race for industrial competitiveness?" [Czy świat ubiegnie Europę – za sprawą cyberszpiegostwa Stary Kontynent miałby zostać w tyle w globalnym wyścigu o przemysłową konkurencyjność?], dokument okolicznościowy nr 2/18, luty 2018 r.

[9] Komisja Europejska, orędzie przewodniczącego o stanie Unii w 2017 r.

[10] Europol, „World's Biggest Marketplace selling internet paralysing DDoS attacks taken down" [Największy na świecie serwis sprzedaży paraliżujących działalność rozproszonych ataków typu „odmowa usługi" został zlikwidowany], komunikat prasowy, 25 kwietnia 2018 r.

[11] Europol, „Internet Organised Crime Threat Assessment 2017".

[12] Opracowane przez Komisję Europejską zestawienie danych na temat cyberbezpieczeństwa, wrzesień 2017 r.

[13] Koszty mogą obejmować: stracone przychody; koszty naprawy uszkodzonych systemów; potencjalne zobowiązania związane ze skradzionymi zasobami lub informacjami; zachęty na rzecz zatrzymania klientów; wyższe składki ubezpieczeniowe; zwiększone koszty ochrony (nowe systemy i nowi pracownicy, szkolenia); uregulowanie ewentualnych kosztów związanych z zapewnieniem zgodności lub zamknięciem sporów.

[14] NTT Security, „Risk:Value 2018 Report" [Sprawozdanie z 2018 r. na temat stosunku zagrożeń do wartości].

[15] Oprogramowanie typu ransomware Wannacry wykorzystywało luki w protokole Microsoft Windows pozwalające na zdalne przejęcie kontroli nad dowolnym komputerem. Po tym, jak luka została odkryta, Microsoft udostępnił odpowiednią łatkę. Niemniej oprogramowanie setek tysięcy komputerów nie

zostało zaktualizowane w porę i wiele z nich padło w konsekwencji ofiarą ataku. Źródło: A. Greenberg, „Hold North Korea Accountable For Wannacry—and the NSA, too" [Pociągnięcie Korei Północnej do odpowiedzialności za atak Wannacry – a także Narodowej Agencji Bezpieczeństwa], Wired, 19 grudnia 2017 r.

[16] Komisja Europejska, „Europeans' attitudes towards cybersecurity" [Postawy Europejczyków w kwestii cyberbezpieczeństwa], specjalne badanie Eurobarometr 464a, wrzesień 2017 r. Wyniki badania następczego mają zostać opublikowane z początkiem 2019 r.

[17] Konwencja budapesztańska jest wiążącym międzynarodowym zbiorem wytycznych dla państw opracowujących przepisy prawne w zakresie zwalczania cyberprzestępczości. Ustanawia ramy współpracy międzynarodowej między podmiotami państwowymi. Obecnie w ramach konwencji UE reprezentują Komisja, Rada Unii Europejskiej, Europol, ENISA i Eurojust.

[18] Komisja Europejska, „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" (JOIN(2013) 1 final z 7.2.2013).

[19] Komisja Europejska, „Europejska Agenda Bezpieczeństwa" (COM(2015) 185 final z 28.4.2015).

[20] Komisja Europejska, „Strategia jednolitego rynku cyfrowego dla Europy" (COM(2015) 192 final z 6.5.2015).

[21] ESDZ, „Wspólna wizja, wspólne działanie:Silniejsza Europa.Globalna strategia dla polityki zagranicznej i bezpieczeństwa Unii Europejskiej", czerwiec 2016 r.

[22] Centrum Studiów nad Polityką Europejską, „Strengthening the EU's Cyber Defence Capabilities – Report of a CEPS Task Force" [Zwiększenie unijnych zdolności w zakresie cyberobrony – sprawozdanie grupy roboczej Centrum Studiów nad Polityką Europejską], listopad 2018 r.

[23] Stany Zjednoczone, Zjednoczone Królestwo i Australia wskazały Koreę Północną jako miejsce pochodzenia złośliwego oprogramowania będącego przyczyną ataku typu ransomware Wannacry. Pierwotnie zostało ono jednak opracowane i było przechowywane przez amerykańską Narodową Agencję Bezpieczeństwa w celu wykorzystania luk w systemie Windows. Źródło: A. Greenberg, tamże, Wired, 19 grudnia 2017 r. W następstwie ataków Microsoft potępił przetrzymywanie informacji na temat luk w oprogramowaniu i ponowił apel o ustanowienie „cyfrowej konwencji genewskiej".

[24] Obok lądu, morza, powietrza i przestrzeni kosmicznej.

[25] Ramy polityki UE w zakresie cyberobrony (aktualizacja 2018 r.) (14413/18) z dnia 19 listopada 2018 r.

[26] Komisja Europejska / Europejska Służba Działań Zewnętrznych, „Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej" (JOIN(2016) 18 final z 6.4.2016).

[27] Wspólne deklaracje przewodniczącego Rady Europejskiej, przewodniczącego Komisji oraz sekretarza generalnego Organizacji Traktatu Północnoatlantyckiego z dnia 8 lipca 2016 r. i z dnia 10 lipca 2018 r.

[28] Komisja Europejska / Europejska Służba Działań Zewnętrznych, „Odporność, prewencja i obrona:budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej" (JOIN(2017) 450 final z 13.9.2017).

[29] 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 (Dz.U. L 194 z 19.7.2016, s. 1).

[30] 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.

[31] Są one włączone do struktur współpracy ustanowionych na mocy dyrektywy, sieci CSIRT (w której uczestniczą CSIRT wyznaczone przez państwa członkowskie UE i CERT-UE, przy czym usługi sekretariatu świadczy ENISA) oraz grupy współpracy (która wspiera i ułatwia współpracę strategiczną i wymianę informacji między państwami członkowskimi, przy czym w tym wypadku usługi sekretariatu świadczy Komisja).

[32] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. L 119 z 4.5.2016, s. 1).

[33] Komisja Europejska, wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie „Agencji UE ds. Cyberbezpieczeństwa" ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt w sprawie cyberbezpieczeństwa") (COM(2017) 477 final z 13.9.2017).

[34] Komisja Europejska, wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych (COM(2018) 225 final z 17.4.2018).

[35] Komisja Europejska, wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady ustanawiającej zharmonizowane przepisy dotyczące mianowania przedstawicieli prawnych w celu gromadzenia dowodów na potrzeby postępowań karnych. (COM(2018) 226 final z 17.4.2018).

[36] Komisja Europejska, wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego Europejskie Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa w kwestiach Przemysłu, Technologii i Badań Naukowych oraz sieć krajowych ośrodków koordynacji (COM(2018) 630 final z 12.9.2018).

[37] H. Carrapico i A. Barrinha, „The EU as a Coherent (Cyber)Security Actor?" [Czy UE stanowi spójny podmiot w dziedzinie (cyber)bezpieczeństwa?], *Journal of Common Market Studies*, vol. 55 nr 6, 2017.

[38] Komisja Europejska, tamże, SWD(2017) 295 final z 13.9.2017.

[39] Biuro Analiz Parlamentu Europejskiego, „Transatlantic cyber-insecurity and cybercrime. Economic impact and future prospects" [Brak cyberbezpieczeństwa i cyberprzestępczość w wymiarze transatlantyckim. Oddziaływanie ekonomiczne i perspektywy na przyszłość], PE 603.948, grudzień 2017 r.

[40] ENISA, „An evaluation framework for Cyber Security Strategies" [Ramy oceny dotyczące strategii w zakresie cyberbezpieczeństwa], 27 listopada 2014 r.

[41] Wyjątkiem w tym względzie jest art. 14 („Monitorowanie i statystyki”) dyrektywy Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i zastępującej decyzję ramową Rady 2005/222/WSiSW.

[42] Europejski Komitet Ekonomiczno-Społeczny, „Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks” [Cyberbezpieczeństwo – zapewnienie wiedzy i odporności w sektorze prywatnym w Europie wobec wzrostu ryzyka w cyberprzestrzeni], marzec 2018 r. Zespół roboczy CEPS-European Credit Research Institute, „Cybersecurity in Finance: Getting the policy mix right!” [Cyberbezpieczeństwo w sektorze finansowym – znalezienie właściwego połączenia rozwiązań politycznych], czerwiec 2018 r.

[43] Na ankietę odpowiedzi udzieliły 24 z 28 krajowych organów kontroli.

[44] Oznacza to podejście oparte na zasadach i neutralne pod względem technologicznym.

[45] Mechanizm doradztwa naukowego Komisji Europejskiej, opinia naukowa nr 2/2017, 24 marca 2017 r.

[46] L. Rebuffi, „EU Digital Autonomy: A possible approach” [Autonomia cyfrowa UE – możliwe podejście], Digma Zeitschrift für Datenrecht und Informationssicherheit, wrzesień 2018 r. European Centre for Political Economy, tamże, dokument okolicznościowy nr 2/18, luty 2018 r.

[47] Komisja Europejska, wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie niektórych aspektów umów o dostarczanie treści cyfrowych (COM(2015) 634 final z 9.12.2015).

[48] Komisja Europejska, wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie niektórych aspektów umów sprzedaży towarów zawieranych przez internet lub w inny sposób na odległość (COM(2015) 635 final z 9.12.2015).

[49] Cyber Security Raad, „European Foresight Cyber Security Meeting 2016: Public private academic recommendations to the European Commission about Internet of Things and Harmonization of duties of care” [Europejska konferencja analityczna poświęcona cyberbezpieczeństwu w 2016 r. – zalecenia sektorów publicznego i prywatnego oraz środowisk akademickich dla Komisji Europejskiej odnoszące się do internetu rzeczy i harmonizacji obowiązków w zakresie staranności], 2016.

[50] Centrum Studiów nad Polityką Europejską, „Software Vulnerability Disclosure in Europe:Technology, Policies and Legal Challenges – Report of a CEPS Task Force” [Ujawnianie luk w oprogramowaniu w Europie – technologia, polityka i wyzwania prawne – sprawozdanie grupy roboczej CEPS], czerwiec 2018 r.

[51] Komisja Europejska, „Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii” (COM(2017) 476 final/2 z 4.10.2017).

[52] Europol, tamże, 2017.

[53] Rada Unii Europejskiej, sprawozdanie końcowe na temat siódmej rundy wzajemnych ocen pt. „Praktyczne wdrażanie i funkcjonowanie europejskich polityk dotyczących zapobiegania cyberprzestępczości i jej zwalczania” (12711/1/17 REV 1 z 9.10.2017).

[54] Komisja Europejska, ocena skutków towarzysząca wnioskowi dotyczącemu dyrektywy w sprawie zwalczania fałszowania i oszustw związanych z bezgotówkowymi środkami płatniczymi (SWD(2017)

298 final z 13.9.2017). Porozumienie polityczne co do brzmienia nowych przepisów osiągnięto w grudniu 2018 r. i oczekuje się, że zostaną one przyjęte z początkiem 2019 r.

[55] Europol, tamże, 2017.

[56] Sprawa C-362/14 Maximillian Schrems przeciwko Data Protection Commissioner (Irlandia), 6 października 2015 r.

[57] Europol / Eurojust, „Common challenges in combating cybercrime" [Wspólne wyzwania w zwalczaniu cyberprzestępczości], 7021/17, 13 marca 2017 r.

[58] Komisja Europejska, „Ocena unijnej strategii z 2013 r. w zakresie cyberbezpieczeństwa" (SWD(2017) 295 final z 13.9.2017).

[59] Biuro Analiz Parlamentu Europejskiego, „Briefing: EU Legislation in Progress – Review of dual-use export controls" [Briefing. Postępy unijnego prawodawstwa – przegląd kontroli wywozu produktów podwójnego zastosowania], PE589.832.

[60] Rezolucja Parlamentu Europejskiego z dnia 8 września 2015 r. w sprawie „Prawa człowieka a technologia: wpływ systemów inwigilacji i nadzoru na prawa człowieka w państwach trzecich" (2014/2232(INI)). Towary i usługi podwójnego zastosowania, które obejmują oprogramowanie i technologie, mogą mieć zastosowania zarówno cywilne, jak i wojskowe.

[61] Ogólnodostępne informacje są przechowywane w bazie danych WHOIS, zarządzanej przez ICANN (Internetową Korporację ds. Nadanych Nazw i Numerów). ICANN prowadzi system nazw domen. Niewłaściwe wykorzystywanie nazw domen ułatwia cyberprzestępczość.

[62] Art. 3 dyrektywy w sprawie bezpieczeństwa sieci i informacji.

[63] Atlantic Council, „Risk Nexus: Overcome by cyber risks? Economic benefits and costs of alternate cyber futures" [Złożone ryzyko – rosnące brzemię ryzyka w cyberprzestrzeni. Korzyści i koszty ekonomiczne w alternatywnych scenariuszach rozwoju cyberprzestrzeni], 10 września 2015 r.

[64] Biały Dom, „Cybersecurity spending fiscal year 2019" [Wydatki na cyberbezpieczeństwo w roku budżetowym 2019].

[65] Komisja Europejska, dokument roboczy służb Komisji pt.„Ocena skutków towarzysząca wnioskowi dotyczącemu rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program »Cyfrowa Europa« na lata 2021–2027 (SWD(2018) 305 final z 6.6.2018).

[66] The Hague Centre for Strategic Studies, „Dutch investments in ICT and cybersecurity: putting it in perspective" [Niderlandzkie inwestycje w ICT i cyberbezpieczeństwo w szerszej perspektywie], grudzień 2016 r.

[67] Komisja Europejska, tamże, COM(2018) 630 final z 12.9.2018.

[68] Dział Prognoz Naukowych Biura Analiz Parlamentu Europejskiego, „Achieving a sovereign and trustworthy ICT industry in the EU" [Stworzenie suwerennej i godnej zaufania branży ICT w UE], grudzień 2017 r.

[69] European Digital SME Alliance, „Position Paper on European Cybersecurity Strategy: Fostering the SME ecosystem" [Stanowisko w sprawie europejskiej strategii w zakresie cyberbezpieczeństwa – promowanie ekosystemu MŚP], 31 lipca 2017 r.

[70] Dział Prognoz Naukowych Biura Analiz Parlamentu Europejskiego, tamże, grudzień 2017 r.

[71] Tamże.

[72] Komisja Europejska, „Ocena skutków dotycząca proponowanego badawczego centrum kompetencji oraz sieci krajowych ośrodków koordynacji" (SWD(2018) 403 final (część 1/4) z 12.9.2018).

[73] Komisja Europejska, tamże, COM(2018) 630 final z 12.9.2018.

[74] Sprawozdanie specjalne Europejskiego Trybunału Obrachunkowego nr 13/2018 pt. „Przeciwdziałanie radykalizacji postaw prowadzącej do terroryzmu".

[75] Dane liczbowe podane w tej części dokumentu pochodzą z ogólnodostępnych dokumentów Komisji, z wyjątkiem kwoty 42 mln euro wskazanej w pkt ***51***, którą Komisja podała Trybunałowi bezpośrednio.

[76] Program „Horyzont 2020" to unijny program w zakresie badań naukowych i innowacji o wartości 80 mld euro. Ma on wspierać Unię innowacji, której celem jest zagwarantowanie globalnej konkurencyjności UE.

[77] Wyzwanie społeczne 7 w ramach programu „Horyzont 2020" pn. „Bezpieczne i innowacyjne społeczeństwa – ochrona wolności i bezpieczeństwa Europy i jej obywateli".

[78] Trybunał przeanalizował projekty realizowane w ramach programu „Horyzont 2020" uwzględnione w bazie danych CORDIS. Trybunał przeprowadził wektoryzację tekstu dla opisu każdego projektu – korzystając przy tym z nomenklatury JRC dotyczącej cyberbezpieczeństwa (zob. ***ramka 5*** w następnym rozdziale) – w celu rozpoznania projektów, które są z dużym prawdopodobieństwem powiązane z cyberbezpieczeństwem. Następnie ręcznie sprawdzono i przeanalizowano otrzymane rezultaty.

[79] Europejska Organizacja ds. Cyberbezpieczeństwa, „ECS cPPP Progress Monitoring Report 2016–2017" [Sprawozdanie Europejskiej Organizacji ds. Cyberbezpieczeństwa z monitorowania postępów umownego partnerstwa publiczno-prywatnego za lata 2016–2017], 29 października 2018 r.

[80] Art. 9 ust. 2 dyrektywy w sprawie bezpieczeństwa sieci i informacji.

[81] GLACY+ (Global Action on Cybercrime+) to projekt dotyczący globalnych działań przeciwko cyberprzestępczości realizowany wspólnie z Radą Europy. W ramach projektu zapewnia się wsparcie 12 państwom w Afryce, regionie Azji i Pacyfiku, Ameryce Łacińskiej i regionie Karaibów, które następnie mogą stać się ośrodkami rozpowszechniania nabytej wiedzy w poszczególnych regionach.

[82] Europejski Ośrodek Strategii Politycznej (EOSP), ośrodek analityczny stworzony przez Komisję, zwrócił uwagę na ryzyko powstania „cyfrowego martwego pola", jeśli przepaść między UE i krajami sąsiedzkimi z Bałkanów Zachodnich będzie nadal rosła. Państwa takie jak Chiny i Rosja inwestują w tym regionie znaczne kwoty, co może skutkować marginalizacją UE jako podmiotu na regionalnej arenie cyfrowej. Źródło: EOSP, „Engaging with the Western Balkans: an investment in Europe's security" [Zaangażowanie na Bałkanach Zachodnich – inwestycja w bezpieczeństwo Europy], 17 maja 2018 r.

[83] Europejski Bank Inwestycyjny, „The EIB Group Operating Framework and Operational Plan 2018" [Ramy operacyjne i plan operacyjny Grupy EBI na rok 2018], 12 grudnia 2017 r. W momencie sporządzania niniejszego dokumentu brak było bardziej szczegółowych informacji.

[84] Komisja Europejska, wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego program „Cyfrowa Europa" na lata 2021–2027 (COM(2018) 434 final z 6.6.2018).

[85] Komisja Europejska, rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1092 z dnia 18 lipca 2018 r. ustanawiające Europejski program rozwoju przemysłu obronnego mający na celu wspieranie konkurencyjności i zdolności innowacyjnych przemysłu obronnego Unii (Dz.U. L 200 z 7.8.2018, s. 30). Ponadto w 2017 r. ustanowiono działanie przygotowawcze dotyczące badań w dziedzinie obrony na łączną kwotę 90 mln euro na lata 2017–2019, finansowane ze środków programu „Horyzont 2020". Trudno stwierdzić, czy kwota ta obejmuje jakieś wydatki związane z cyberprzestrzenią.

[86] Trybunał planuje opublikować odrębny dokument analityczny na temat unijnej obronności w 2019 r.

[87] EC3 Europolu, ENISA, ESDZ, Europejska Agencja Obrony i CERT-UE zatrudniają łącznie 159 pracowników. Liczba ta nie uwzględnia pracowników zajmujących się cyberprzestrzenią pracujących w Komisji Europejskiej lub w państwach członkowskich. Źródło: Centrum Studiów nad Polityką Europejską, tamże, listopad 2018 r.

[88] Ocena ENISA, 2017.

[89] Europol wnioskował o zwiększenie rocznego zatrudnienia o 70 pracowników tymczasowych w ramach planu wieloletniego na okres 2018–2020, zatwierdzono tymczasem jedynie zwiększenie zatrudnienia o 26 pracowników. W projekcie kolejnego planu wieloletniego na lata 2019–2021 Europol uwzględnił ten ograniczony wzrost, „zakładając, że większe zapotrzebowanie na zasoby nie zostanie zaspokojone". Źródło: konsultacje w sprawie projektu programu wieloletniego na lata 2019–2021 przedłożonego grupie ds. wspólnej kontroli parlamentarnej, dokument A 000834, 1 lutego 2018 r.

[90] Ocena ENISA, 2017. W latach 2014–2016 80% budżetu operacyjnego ENISA wykorzystano na potrzeby udzielania zamówień na badania.

[91] ENISA, „Exploring the opportunities and limitations of current Threat Intelligence Platforms" [Analiza możliwości i ograniczeń obecnie stosowanych platform informacji wywiadowczych na temat zagrożeń], grudzień 2017 r.

[92] ISACA (organizacja wcześniej znana pod nazwą Information Systems Audit and Control Association), „Information Security Governance: Guidance for Boards of Directors and Executive Management" [Zarządzanie w zakresie bezpieczeństwa informacji – wytyczne dla zarządów i kadry zarządzającej], 2. wydanie, 2006.

[93] EY, „Cybersecurity regained: preparing to face cyber attacks.20th Global Information Security Survey 2017" [Odzyskać cyberbezpieczeństwo – przygotowania do odparcia cyberataków. 20. globalne badanie ankietowe dotyczące bezpieczeństwa informacji z 2017 r.], s. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy oraz H. Lung), „Hit or myth? Understanding the true costs and impact of cybersecurity programs" [Prawda czy fałsz? Analiza faktycznych kosztów i oddziaływania programów w zakresie cyberbezpieczeństwa], lipiec 2017 r.

[95] Komisja Papierów Wartościowych i Giełd, „Statement and Interpretive Guidance on Public Company Cybersecurity Disclosures" [Oświadczenie i wytyczne interpretacyjne w sprawie ujawniania przez spółki publiczne informacji dotyczących cyberbezpieczeństwa], 21 lutego 2018 r.

[96] Forum współpracy między Europejskim Urzędem Nadzoru Bankowego, Europejskim Urzędem Nadzoru Giełd i Papierów Wartościowych oraz Europejskim Urzędem Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych.

[97] Europejski Urząd Nadzoru Giełd i Papierów Wartościowych, „Joint Committee report on risks and vulnerabilities in the EU financial system" [Sprawozdanie Wspólnego Komitetu na temat zagrożeń i szczególnie narażonych elementów w ramach unijnego systemu finansowego], kwiecień 2018 r.

[98] ENISA, „Information security and privacy standards for SMEs: Recommendations to improve the adoption of information security and privacy standards in SMEs" [Standardy w zakresie bezpieczeństwa informacji i ochrony prywatności dotyczące MŚP – zalecenia na rzecz sprawniejszego przyjmowania standardów w zakresie bezpieczeństwa informacji i ochrony prywatności w MŚP], grudzień 2015 r.

[99] Odnosząc się do państw członkowskich UE, przedstawiciele mechanizmu doradztwa naukowego Komisji zwrócili uwagę na „istotny i wyjątkowy poziom zgodności co do podstawowych zasad i wartości, a także wspólne interesy strategiczne, które mogą stać się podstawą skutecznego unijnego zarządzania w zakresie cyberbezpieczeństwa". Źródło: opinia naukowa nr 2/2017 z 24 marca 2017 r.

[100] Stany Zjednoczone, Chiny, Japonia, Korea Południowa, Indie i Brazylia.

[101] Europejskie Kolegium Bezpieczeństwa i Obrony (T. Renard i A. Barrinha), „Handbook on cyber security, chapter 3.4 The EU as a partner in cyber diplomacy and defence" [Kompendium dotyczące cyberbezpieczeństwa. Rozdział 3.4 – UE jako partner w cyberdyplomacji i cyberobronie], 23 listopada 2018 r.

[102] Rada Unii Europejskiej, plan działania w celu wdrożenia konkluzji Rady w sprawie wspólnego komunikatu do Parlamentu Europejskiego i Rady pt.„Odporność, prewencja i obrona:budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej" 15748/17, 12 grudnia 2017 r.

[103] Komisja Europejska, „European Commission Digital Strategy: A digitally transformed, user-focused and data-driven Commission" [Strategia cyfrowa Komisji Europejskiej – w kierunku Komisji po transformacji cyfrowej, ukierunkowanej na użytkownika i funkcjonującej w oparciu o dane] (C(2018) 7118 final z 21.11.2018).

[104] Odpowiedź komisarz Mariyi Gabriel na pytanie poselskie wymagające odpowiedzi na piśmie (E-004294-17), 28 czerwca 2017 r.

[105] Rada Unii Europejskiej, roczne sprawozdanie w sprawie wdrożenia ram polityki w zakresie cyberobrony, 15870/17, 19 grudnia 2017 r.

[106] Zasady regulujące bezpieczeństwo systemów informacyjnych i komunikacyjnych Komisji określono w decyzjach 2015/443, 2015/444 oraz 2017/46. Decyzją Komisji C(2018) 7706 z dnia 21 listopada 2018 r. ustanowiono Radę ds. Technologii Informacyjnej i Cyberbezpieczeństwa, która stanowi połączenie wcześniej funkcjonujących Rady ds. Informatycznych i Rady Sterującej ds. Bezpieczeństwa Informacji.

[107] Europejski Komitet Ekonomiczno-Społeczny, tamże, marzec 2018 r.

[108] Parlament Europejski, tamże, wrzesień 2015 r.

[109] Komórkę UE ds. Syntezy Informacji o Zagrożeniach Hybrydowych utworzono w 2016 r. w Centrum Analiz Wywiadowczych UE w ESDZ. Otrzymuje ona i analizuje poufne i jawne informacje pochodzące od różnych zainteresowanych stron i dotyczące zagrożeń hybrydowych.

[110] ENISA, „National-level Risk Assessments: An Analysis Report" [Oceny ryzyka na szczeblu krajowym – sprawozdanie analityczne], listopad 2013 r.

[111] Komisja Europejska, ocena skutków dotycząca Agencji UE ds. Cyberbezpieczeństwa i aktu ws. cyberbezpieczeństwa (SWD(2017) 500 final (część 1/6) z 13.9.2017).

[112] Komisja Europejska, tamże, SWD(2018) 403 final z 12.9.2018.

[113] Centrum Koordynacji Sieci Résaux IP Européens (RIPE-NCC) stanowi regionalny rejestr internetowy dla Europy i nadzoruje przydzielanie i rejestrację zasobów numerów internetowych.

[114] ENISA, „EISAS Large-Scale Pilot Collaborative Awareness Raising for EU Citizens & SMEs" [Projekt pilotażowy na dużą skalę w ramach europejskiego systemu wymiany informacji i wczesnego ostrzegania (EISAS) dotyczący zespołowego upowszechniania wiedzy wśród obywateli i MŚP w UE], listopad 2012 r.

[115] Centre for Cyber Safety and Education w partnerstwie z Booz Allen Hamilton, Alta Associates oraz Frost & Sullivan, „2017 Global Information Security Workforce Study – Benchmarking Workforce Capacity and Response to Cyber Risk" [Globalne badanie siły roboczej zatrudnionej w sektorze bezpieczeństwa informacji z 2017 r. – analiza porównawcza zdolności pracowników i reakcji na cyberzagrożenia].

[116] Europejski Komitet Ekonomiczno-Społeczny, tamże, marzec 2018 r.

[117] Izba Lordów, Izba Gmin, Wspólny Komitet ds. Krajowej Strategii w zakresie Bezpieczeństwa, „Cyber Security Skills and the UK's Critical National Infrastructure. Second Report of Session 2017–19" [Umiejętności w zakresie cyberbezpieczeństwa i krajowa infrastruktura krytyczna w Zjednoczonym Królestwie. Drugie sprawozdanie w kadencji 2017–19], 16 lipca 2018 r.

[118] Europol / Eurojust, „Common challenges in combating cybercrime", 7021/17, 13 marca 2017 r.

[119] Europol/Eurojust, tamże, 7021/17, 13 marca 2017 r.

[120] Komisja Europejska, tamże, SWD(2018) 403 final z 12.9.2018.

[121] Cepol, decyzja Zarządu nr 33/2018/MB w sprawie jednolitego dokumentu programowego Cepol na lata 2020–2022 z dnia 20 listopada 2018 r.

[122] Przykładowo, współpraca między ESDZ, państwami członkowskimi, agencjami i organami takimi jak Cepol, europejska grupa ds. szkolenia i edukacji w zakresie cyberprzestępczości (ECTEG) oraz Europejskie Kolegium Bezpieczeństwa i Obrony (EKBiO).

[123] ENISA, „Stock-taking of information security training needs in critical sectors" [Podsumowanie potrzeb dotyczących szkoleń w zakresie bezpieczeństwa informacji w sektorach o krytycznym znaczeniu], grudzień 2017 r.

[124] Europejska grupa ds. szkolenia i edukacji w zakresie cyberprzestępczości.

[125] Komisja Europejska, trzynaste sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2018) 46 final z 24.1.2018).

[126] Na podstawie obserwacji zawartych w sprawozdaniu specjalnym nr 14/2018, tamże.

[127] Rezolucja Parlamentu Europejskiego z dnia 13 czerwca 2018 r. w sprawie cyberobrony (2018/2004(INI)). Rada Unii Europejskiej, tamże, 15870/17, 19 grudnia 2017 r.

[128] Szwajcaria, była jugosłowiańska republika Macedonii, Ukraina, Bośnia i Hercegowina, Kosowo (użycie tej nazwy nie wpływa na stanowiska w sprawie statusu Kosowa i jest zgodne z rezolucją Rady

Bezpieczeństwa ONZ 1244(1999) oraz z opinią Międzynarodowego Trybunału Sprawiedliwości w sprawie Deklaracji niepodległości Kosowa), Turcja i Stany Zjednoczone.

[129] Europol, „Internet Organised Crime Threat Assessment 2018".

[130] Komisja Europejska, tamże, SWD(2017) 295 final z 13.9.2017.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman i S. Furman, „Security Fatigue" [Zmęczenie dbaniem o bezpieczeństwo], *IT Professional*, vol. 18 nr 5, 2016, s. 26–32. Zob. również NIST.

[132] Komisja Europejska / Europejska Służba Działań Zewnętrznych, „Zwiększenie odporności i wzmocnienie zdolności reagowania na zagrożenia hybrydowe" (JOIN(2018) 16 final z 13.6.2018).

[133] Przykładowo, zamknięcie serwisów AlphaBay oraz Hansa w ramach wspólnych operacji prowadzonych przez FBI i niderlandzką policję krajową przy wsparciu Europolu. Były to dwa największe serwisy sprzedażowe wykorzystywane do obrotu nielegalnymi towarami takimi jak środki odurzające, broń palna i narzędzia do cyberprzestępczości, np. złośliwe oprogramowanie. Źródło: Europol, „Crime on the Dark Web: Law Enforcement coordination is the only cure" [Przestępczość w ciemnej sieci – jedynym panaceum jest koordynowanie działań organów ścigania], komunikat prasowy z 29 maja 2018 r.

[134] Komisja Europejska, SWD(2018) 403 final z 12.9.2018.

[135] Rada Unii Europejskiej, tamże, 12711/1/17 REV 1, 9 października 2017 r.

[136] Komisja Europejska, tamże, SWD(2017) 295 final z 13.9.2017.

[137] Komisja Europejska / Europejska Służba Działań Zewnętrznych, tamże (JOIN(2018) 16 z 13.6.2018).

[138] Komisja Europejska, SWD(2017) 500 final z 13.9.2017.

[139] Memorandum of Understanding – ENISA, EDA, Europol EC3, and CERT-EU [Protokół ustaleń – ENISA, Europejska Agencja Obrony, EC3 Europolu oraz CERT-UE], 23 maja 2018 r.

[140] Komisja Europejska, zaproszenie do składania ofert pn. „Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap" [Ustanowienie i prowadzenie programu pilotażowego dotyczącego sieci kompetencji w dziedzinie cyberbezpieczeństwa w celu opracowania i wdrożenia planu działania dla badań naukowych i innowacji w dziedzinie cyberbezpieczeństwa], 27 października 2017 r.

[141] Jean-Claude Juncker, pismo określające zadania komisarza właściwego do spraw unii bezpieczeństwa, 2 sierpnia 2016 r. Obrona nie należy do kompetencji grupy roboczej.

[142] Rada Unii Europejskiej, „EU cybersecurity roadmap" [Plan działania dotyczący cyberbezpieczeństwa w UE], 8901/17, 11 maja 2017 r.

[143] Friends of Europe, „Debating Security Plus: Crowdsourcing solutions to the world's security issues" [Debaty na temat bezpieczeństwa+ – pozyskiwanie wiedzy społecznościowej w celu znalezienia rozwiązań globalnych problemów w dziedzinie bezpieczeństwa], 5. wydanie, listopad 2017 r.

[144] Sprawozdania techniczne JRC, „European Cybersecurity Centres of Expertise Map: Definitions and Taxonomy" [Mapa europejskich centrów wiedzy specjalistycznej w dziedzinie cyberbezpieczeństwa – definicje i nomenklatura]. „Ocena skutków dotycząca proponowanego badawczego centrum kompetencji oraz sieci krajowych ośrodków koordynacji" (SWD(2018) 403 final z 12.9.2018).

[145] Komisja Europejska, tamże, SWD(2017) 295 final z 13.9.2017.

[146] Komisja Europejska, tamże, SWD(2018) 403 final z 12.9.2018.

[147] Przykładowo, w ośrodku European Financial Institutes ISAC (EU FI-ISAC) uczestniczą przedstawiciele sektora finansowego, krajowych CERT, agencji ścigania, ENISA, Europolu, Europejskiego Banku Centralnego, Europejskiej Rady ds. Płatności i Komisji Europejskiej.

[148] ENISA, „Information Sharing and Analysis Centres (ISACs) – Cooperative models" [Ośrodki wymiany i analizy informacji – modele współpracy], 14 lutego 2018 r.

[149] Rada Unii Europejskiej, tamże, 12711/1/17 REV 1, 9 października 2017 r.

[150] https://www.europol.europa.eu/empact.

[151] W badaniu przeprowadzonym w 2018 r. w 15 państwach przez Accenture ustalono, że udaje się zapobiec 87% ukierunkowanych cyberataków (zob. „2018 State of Cyber Resilience" [Sytuacja w zakresie cyberodporności w 2018 r.], 10 kwietnia 2018 r.]).

[152] P. Timmers, wpis na blogu pt. „Cybersecurity is Forcing a Rethink of Strategic Autonomy" [Cyberbezpieczeństwo zmusza do przemyślenia na nowo kwestii autonomii strategicznej], Oxford University Politics Blog, 14 września 2018 r.

[153] Caroline Preece, „Three reasons why cyber threat detection is still ineffective" [Trzy przyczyny, dla których wykrywanie cyberzagrożeń pozostaje nieskuteczne], IT Pro, 14 lipca 2017 r.

[154] Europejski Komitet Ekonomiczno-Społeczny, tamże, marzec 2018 r.

[155] Komisja Europejska, ósme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa (COM(2017) 354 final z 29.6.2017).

[156] Zob. różne publikacje grupy współpracy w zakresie bezpieczeństwa sieci i informacji.

[157] TARGET2 – transeuropejski zautomatyzowany błyskawiczny system rozrachunku brutto w czasie rzeczywistym (2. generacji); rozporządzenie eIDAS – rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym. Źródło: zespół roboczy CEPS–European Credit Research Institute, tamże, czerwiec 2018 r.

[158] Komisja Europejska, „Recommendation on Coordinated Response to Large Scale Cybersecurity Incidents and Crises" [Zalecenie dotyczące skoordynowanej reakcji na cyberincydenty i cyberkryzysy o dużej skali], C(2017) 6100 final, 13 września 2017.

[159] Komisja Europejska, tamże, SWD(2017) 295 final z 13.9.2017. Istnieje kilka mechanizmów zarządzania kryzysowego, w tym zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych, ARGUS (mechanizm reagowania kryzysowego Komisji), mechanizm reagowania kryzysowego ESDZ, Unijny Mechanizm Ochrony Ludności i unijny protokół działań w zakresie egzekwowania prawa w sytuacjach kryzysowych.

[160] Ponadto może to skutkować sięgnięciem po art. 42 ust. 7 Traktatu o Unii Europejskiej (klauzulę o wzajemnej pomocy) lub art. 222 Traktatu o funkcjonowaniu Unii Europejskiej (klauzulę solidarności).

[161] Komisja Europejska / Europejska Służba Działań Zewnętrznych, tamże (JOIN(2018) 16 z 13.6.2018). W grudniu 2018 r. media doniosły o rzekomym włamaniu do sieci łączności dyplomatycznej ESDZ, COREU (źródło: „New York Times", „Hacked European Cables Reveal a World of Anxiety About Trump, Russia

and Iran" [Na podstawie wykradzionych europejskich depesz dyplomatycznych rysuje się obraz międzynarodowej społeczności zaniepokojonej Trumpem, Rosją i Iranem], 18 grudnia 2018 r.). Sprawa jest obecnie objęta postępowaniem wyjaśniającym

[162] Dalszego zacieśnienia wymaga również współpraca w zakresie wczesnego ostrzegania i wzajemnej pomocy, zob. konkluzje Rady w sprawie skoordynowanego reagowania na szczeblu unijnym na cyberincydenty i cyberkryzysy na dużą skalę, 10085/18, 26 czerwca 2018 r.

[163] Biuro Analiz Parlamentu Europejskiego, „Briefing EU Legislation in Progress: ENISA and a new cybersecurity act" [Briefing. Postępy unijnego prawodawstwa – ENISA i nowy akt ws. cyberbezpieczeństwa], PE 614.643, wrzesień 2018 r.

[164] Europejski Komitet Ekonomiczno-Społeczny, tamże, marzec 2018 r.

[165] Rada Unii Europejskiej, „EU Law Enforcement Emergency Response Protocol (LE ERP) for Major Cross-Border Cyber-Attacks" [Unijny protokół działań w zakresie egzekwowania prawa w sytuacjach kryzysowych w przypadku dużych cyberataków transgranicznych], 14893/18, grudzień 2018 r.

[166] Zespoły szybkiego reagowania na cyberincydenty i pomoc wzajemna w zakresie cyberbezpieczeństwa; platforma wymiany informacji o cyberzagrożeniach i reagowaniu na cyberincydenty. Źródło: Rada Unii Europejskiej, „Permanent Structured Cooperation (PESCO) updated list of PESCO projects – Overview" [Stała współpraca strukturalna (PESCO) – zaktualizowany wykaz projektów PESCO – przegląd], 19 listopada 2018 r.

[167] Rada Unii Europejskiej, konkluzje w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne, 9916/17, 7 czerwca 2017 r.

[168] Rada Unii Europejskiej, konkluzje Rady w sprawie dyplomacji elektronicznej, 6122/55, 11 lutego 2015 r.

[169] Rada Unii Europejskiej, „Draft implementing guidelines for the Framework on a Joint Diplomatic Response to Malicious Cyber Activities" [Projekt wytycznych dotyczących wdrożenia ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni], 13007/17.

[170] Przypisanie odpowiedzialności za incydent pozostaje suwerenną decyzją polityczną, którą podejmują państwa członkowskie, przy czym nie wszystkie z działań przewidzianych w zestawie narzędzi wymagają takiego przypisania.

[171] Zestaw narzędzi nie doprowadził do wspólnego działania; pojedyncze państwa członkowskie przyjęły stanowisko Stanów Zjednoczonych.

[172] Rada Unii Europejskiej, konkluzje w sprawie szkodliwych działań w cyberprzestrzeni, 7925/18, 16 kwietnia 2018 r.

[173] Systemy komputerowe wykorzystywane do kontrolowania procesów w różnych branżach, takich jak przedsiębiorstwa użyteczności publicznej, produkcja przemysłowa i chemiczna, przetwórstwo żywności, systemy i węzły transportowe oraz usługi logistyczne.

[174] ENISA, tamże, grudzień 2017 r.

[175] Przykładowo, organy administracji publicznej, przemysł chemiczny i sektor energii jądrowej, przemysł wytwórczy, przetwórstwo żywności, turystyka, logistyka i ochrona ludności.

[176] Komisja Europejska, tamże, SWD(2017) 295 final z 13.9.2017.

[177] Przemówienie komisarz Jourovej na sesji plenarnej Parlamentu Europejskiego pt. „Increasing EU resilience against the influence of foreign actors on the upcoming EP election campaign" [Zwiększenie odporności UE wobec ingerencji podmiotów zagranicznych w zbliżającą się kampanię wyborczą do PE], 14 listopada 2018 r.

[178] Carnegie Endowment for International Peace, „Russian Election Interference: Europe's Counter to Fake News and Cyber Attacks" [Rosyjska ingerencja w proces wyborczy – odpowiedź Europy na fałszywe wiadomości i cyberataki], 23 maja 2018 r.

[179] Europejski Ośrodek Strategii Politycznej (L. Past), „Cybersecurity of Election Technology: Inevitable Attacks and Variety of Responses" [Cyberbezpieczeństwo technologii wyborczych – nieuniknione ataki i zróżnicowane odpowiedzi] w: „Election Interference in the Digital Age – Building Resilience to Cyber-Enabled Threats: A collection of think pieces of 35 leading practitioners and experts", 2018.

[180] Zgodnie z przepisami dyrektywy Rady 2008/114/WE w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony.

[181] Komisja Europejska, „Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament" [Zalecenie w sprawie sieci współpracy wyborczej, przejrzystości w internecie, ochrony przed cyberincydentami i przeciwdziałania kampaniom dezinformacyjnym w kontekście wyborów do Parlamentu Europejskiego], C(2018) 5949, 12 września 2018 r.

[182] Konkluzje Rady Europejskiej, EUCO 11/15, 20 marca 2015 r. Od tamtego czasu utworzono dwie dodatkowe grupy zadaniowe, do spraw Bałkanów Zachodnich i państw południowego sąsiedztwa.

[183] W sprawozdaniu Atlantic Council wezwano UE, by nałożyła na wszystkie państwa członkowskie wymóg oddelegowania ekspertów krajowych do grupy zadaniowej. Zob. D. Fried oraz A. Polyakova, „Democratic Defense Against Disinformation" [Demokracje bronią się przed dezinformacją], 5 marca 2018 r.

[184] Pierwotnie nie posiadała własnego budżetu, ale w 2018 r. Parlament Europejski przyznał grupie 1,1 mln euro na działanie przygotowawcze StratCom Plus.

[185] Carnegie Endowment for International Peace (E. Brattberg, T. Maurer), tamże, 23 maja 2018 r.

[186] Komisja Europejska, Wysoki Przedstawiciel Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa, plan działania na rzecz zwalczania dezinformacji (JOIN(2018) 36 final). Plan jest ukierunkowany na: zwiększenie zdolności instytucji Unii do wykrywania, analizowania i ujawniania dezinformacji; wzmocnienie skoordynowanej i wspólnej reakcji na dezinformację; mobilizowanie sektora prywatnego; podnoszenie świadomości i zwiększanie odporności społecznej.

[187] Komisja Europejska, „Zwalczanie dezinformacji w internecie: podejście europejskie" (COM(2018) 236 final z 26.4.2018).

[188] Nie należy mylić tego kodeksu z Kodeksem postępowania w zakresie zwalczania nielegalnego nawoływania do nienawiści w internecie.

[189] JRC, „The digital transformation of news media and the rise of disinformation and fake news" [Cyfrowa transformacja mediów informacyjnych i rozpowszechnienie się dezinformacji i fałszywych wiadomości], sprawozdania techniczne JRC, dokument roboczy JRC poświęcony gospodarce cyfrowej 2018-02, kwiecień 2018 r.

[190] ENISA, „Strengthening Network & Information Security & Protecting Against Online Disinformation (»Fake News«)" [Wzmocnienie bezpieczeństwa sieci i informacji oraz ochrona przed dezinformacją w internecie („fałszywymi wiadomościami")], kwiecień 2018 r.

[191] Europejski Ośrodek Strategii Politycznej (C. Frutos López), „ Responsibility to Support Electoral Organisations in Anticipating and Countering Cyber Threats" [Obowiązek wspierania organizacji wyborczych w prognozowaniu i zwalczaniu cyberzagrożeń] w: tamże, 2018.

[192] Komisja Europejska, tamże, SWD(2018) 403 final z 12.9.2018.

[193] Wniosek dotyczący rozporządzenia (COM(2017) 487 final z 13.9.2017) w sprawie monitorowania bezpośrednich inwestycji zagranicznych, przedstawiony we wrześniu 2017 r., obecnie przechodzi proces legislacyjny. Wniosek dotyczy zwłaszcza technologii o znaczeniu krytycznym, do których zaliczono sztuczną inteligencję, cyberbezpieczeństwo i produkty podwójnego zastosowania.

[194] Komisja Europejska / Europejska Służba Działań Zewnętrznych, tamże, JOIN(2017) 450 z 13.9.2018.

Zespół kontrolny Trybunału

Niniejszy dokument analityczny pt. „Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją” został przyjęty przez Izbę III – której przewodniczy członek Trybunału Bettina Jakobsen – zajmującą się obszarami wydatków dotyczącymi działań zewnętrznych, bezpieczeństwa i sprawiedliwości. Kontrolą kierował Baudilio Tomé Muguruza, członek Trybunału, a w działania kontrolne zaangażowani byli: Daniel Costa de Magalhães, szef gabinetu; Ignacio García de Parada, attaché; Alejandro Ballester Gallardo, kierownik; Michiel Sweerts, koordynator zadania, a także kontrolerzy: Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone i Silvia Monteiro Da Cunha oraz stażysta Johannes Bolkart. Wsparcie językowe zapewniła Hannah Critoph.

Od lewej: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY

Urząd Publikacji

EUROPEJSKI TRYBUNAŁ OBRACHUNKOWY
12 rue Alcide De Gasperi
1615 Luxembourg
LUKSEMBURG

Tel.: +352 4398-1

Formularz kontaktowy: eca.europa.eu/pl/Pages/ContactForm.aspx
Strona internetowa: eca.europa.eu
Twitter: @EUAuditors