Prof. dr hab. Jacek Sobczak
Akademia Ekonomiczno-Humanistyczna w Warszawie
Sędzia Sądu Najwyższego w stanie spoczynku
ORCID: 0000-0002-2231-8824
jmwsobczak@gmail.com

Dr hab. Ksenia Kakareko, prof. UW
Katedra Prawa Mediów
Wydział Dziennikarstwa, Informacji i Bibliologii
Uniwersytet Warszawski
ORCID: 0000-0003-3707-4479
k.kakareko@uw.edu.pl

Dr hab. Maria Gołda-Sobczak, prof. UAM
Instytut Kultury Europejskiej UAM w Gnieźnie
ORCID: 0000-0002-3854-7007
mgolsob@amu.edu.pl

AKT W SPRAWIE CYBERSOLIDARNOŚCI. UNIJNA REAKCJA NA CYBERZAGROŻENIA I INCYDENTY W CYBERBEZPIECZEŃSTWIE

Streszczenie

W kwietniu 2023 r. Komisja Europejska zaproponowała rozporządzenie mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty (akt w sprawie cybersolidarności). Działania zbrojne prowadzone w Europie ujawniły skalę zależności państwa od technologii cyfrowej i niestabilność przestrzeni cyfrowej. Wywołała ona gwałtowny wzrost cyberataków, które są szczególnie destrukcyjne, gdy są wymierzone w infrastrukturę krytyczną – taką jak energia, zdrowie lub finanse – w coraz większym stopniu uzależnioną od technologii, co sprawia, że jest ona bardziej wydajna, ale również bardziej podatna na zakłócenia cybernetyczne. W tym kontekście Komisja zaproponowała rozporządzenie dotyczące aktu w sprawie cybersolidarności, które ma być odpowiedzią na pilną potrzebę zwiększenia solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty.

Słowa kluczowe: cyberbezpieczeństwo, solidarność, cyberataki, incydenty, cyberzagrożenia, infrastruktura krytyczna.

WSTĘP

W dniu 19 grudnia 2024 r. zostało wydane rozporządzenie Parlamentu Europejskiego i Rady (EU) 2025/38[1]. Określając w rozdziale pierwszym tego rozporządzenia jego przedmiot i cele, stwierdzono, że ustanawia ono środki mające zwiększyć zdolność Unii w zakresie wykrywania oraz przygotowania się i reagowania na cyberzagrożenia i incydenty. Służyć temu winna ustanawiana z mocy rozporządzenia ogólnoeuropejska sieć centrum cyberbezpieczeństwa (europejskiego systemu cyberostrzeżeń) a obok niej mechanizm cyberkryzysowego wsparcia państw członkowskich w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie oraz incydenty na dużą skalę[2]. Wskazano jednocześnie zadania jakie winien pełnić europejski system cyberostrzeżeń (art. 3 ust. 2 rozporządzenia 2025/38) Zdefiniowano również pojęcie krajowych centrów cyberbezpieczeństwa, podkreślając, że utworzyć je mogą państwa unijne, które pragną uczestniczyć w europejskim systemie cyberostrzeżeń (art. 4). Istotne znaczenie rozporządzenie zdaje się przywiązywać do transgranicznych centrum bezpieczeństwa, które, jak przewidziano, winny tworzyć co najmniej trzy państwa członkowskie UE (art. 5).

Podkreślono rolę, jaką powinien spełnić mechanizm przeglądu incydentu w cyberbezpieczeństwie. Zadeklarowano, że rozporządzenie będzie służyć osiągnięciu takich ogólnych celów jakimi są wzmocnienie konkurencyjnej pozycji przemysłu i usług w Unii w odniesieniu do gospodarki cyfrowej oraz przyczynienie się do suwerenności technologicznej Unii i otwartej strategicznej autonomii w dziedzinie cyberbezpieczeństwa[3]. Wskazano także, że treść rozporządzenia pobudzi innowacje na rynku cyfrowym. Realizacja wspomnianych celów zapewni większą solidarność na poziomie Unii i wzmocni ekosystem cyberbezpieczeństwa.

Jako cele szczegółowe wskazano w rozporządzeniu dążenie do wzmocnienia wspólnych unijnych zdolności w zakresie skoordynowanego wykrywania cyberzagrożeń i incydentów. Ponadto regulacja rozporządzenia winny przyczynić się do zwiększenia gotowości podmiotów działających w sektorach kluczowych i krytycznych w całej unii oraz wzmocnić solidarność dzięki rozwijaniu skoordynowanego testowania gotowości i wzmocnienia zdolności reagowania na incydenty i poważne incydenty

[1] Dz.Urz.UE.L.2025. Nr 38. rozporządzenie Parlamentu Europejskiego i Rady (EU) 2025/38 z dnia 19 grudnia 2024 r. w sprawie ustanowienia środków mających na celu zwiększenie solidarności i zdolności Unii w zakresie wykrywania cyberzagrożeń i incydentów oraz przygotowania się i reagowania na takie cyberzagrożenia i incydenty oraz w sprawie zmian do Rozporządzenia (UE) 2021/694 (akt w sprawie cybersolidarności).

[2] Pod pojęciem europejskiego systemu cyberostrzeżeń rozporządzenie 2025/38 chce rozumieć ogólnoeuropejską sieć infrastruktury składającą się z krajowych centrów cyberbezpieczeństwa i transgranicznych centrów cyberbezpieczeństwa, przystępujących na zasadzie dobrowolności - aby wspierać rozwój zaawansowanych zdolności Unii w zakresie wykrywania, analizy i przetwarzania danych w odniesieniu do cyberzagrożeń oraz zapobiegania incydentom w Unii (art. 3 ust. 1 rozporządzenia 2025/38)

[3] W rozporządzeniu zawarowano, że jego treść nie będzie stanowić uszczerbku dla podstawowych funkcji państw członkowskich, w tym odnoszących się do integralności terytorialnej państwa, utrzymania porządku publicznego oraz ochrony bezpieczeństwa narodowego. W szczególności bezpieczeństwo narodowe pozostanie zakresie wyłączenej odpowiedzialności każdego państwa członkowskiego (art. 1 ust. 5 rozporządzenia 2025/38).

w cyberbezpieczeństwie. Dostrzeżono także, iż celem powinno być zwiększenie odporności Unii oraz osiągnięcie możliwości skutecznej reakcji na incydenty dotykający cyberbezpieczeństwa. Jako jeden z celów szczegółowych wskazano możliwość udostępnienia unijnego wsparcia w reagowaniu na incydenty w cyberbezpieczeństwie państwom trzecim stowarzyszonym w programie „Cyfrowa Europa”[4].

W części motywacyjnej rozporządzenia 2025/38 stwierdzono, że w odniesieniu do obszaru Unii, a także na poziomie globalnym rośnie skala i częstotliwość incydentów w cyberbezpieczeństwie, w tym ataków na łańcuchy dostaw, które mają na celu cyberszpiegostwo, instalacje oprogramowania szantażującego lub wywołanie zakłóceń. Podkreślono, że działania te stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. Wskazano dalej, że z uwagi na szybko zmieniający się krajobraz zagrożeń, możliwymi incydentami w obszarze cyberbezpieczeństwa, których skala jest wyjątkowo duża i które powodują poważne zakłócenia lub uszkodzenia infrastruktury krytycznej, zachodzi konieczność podwyższeni gotowości unijnych ram cyberbezpieczeństwa. Zauważono, że wspomniane zagrożenia te wykraczają poza rosyjską wojnę napastniczą przeciwko Ukrainie i prawdopodobnie będą się utrzymywać przez dłuższy czas, czego dowodzi wielość podmiotów mających swój udział w generowaniu obecnych napięć geopolitycznych. Wskazano, że takie incydenty mogą utrudniać świadczenie usług publicznych, ponieważ celem cyberataków jest częstokroć lokalna, regionalna lub krajowa infrastruktura i usługi publiczne. Skonstatowano, że władze lokalne są szczególnie podatne na zagrożenia z racji swoich ograniczonych zasobów. Zauważono, że incydenty te mogą również utrudniać prowadzenie działalności gospodarczej w sektorach kluczowych lub w sektorach krytycznych, powodować znaczne straty finansowe, podważać zaufanie użytkowników, wywoływać istotne szkody w gospodarce i systemach demokratycznych Unii. Skutkiem ich może być zagrożenie zdrowia, a nawet życia mieszkańców państw unijnych. Ponadto skonstatowano, że incydenty w cyberbezpieczeństwie są nieprzewidywalne, gdyż pojawiają się i ewoluują w szybkim tempie, a nie są ograniczone zwykle do konkretnego obszaru geograficznego. Mogą występować jednocześnie lub rozprzestrzeniać się błyskawicznie w wielu państwach. W efekcie potrzebna jest ścisła współpraca między sektorem publicznym, prywatnym oraz środowiskiem akademickim, społeczeństwem obywatelskim oraz środkami społecznego przekazu.

W efekcie za konieczne uznano wzmocnienie pozycji przemysłu i usług w całej gospodarce cyfrowej w Unii oraz wsparcie transformacji cyfrowej poprzez podniesienie poziomu cyberbezpieczeństwa na jednolitym rynku cyfrowym. W części motywacyjnej rozporządzenia przypomniano, że zalecono to w trzech różnych propozycjach Konferencji w sprawie przyszłości Europy[5].

[4] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiający program „Cyfrowa Europa” oraz uchylający decyzję (UE) 2015/2240, Dz.Urz.UE.L. 2021, nr 166, str. 1.

[5] Zob. rezolucja Europejskiego Komitetu Regionów – Konferencja w sprawie przyszłości Europy z 12 lutego 2029 r., Dz. Urz. UE. C 2020, nr 145, str. 5; rezolucje Parlamentu Europejskiego w sprawie stanowiska Parlamentu Europejskiego dotyczącego konferencji w sprawie przyszłości Europy: z dnia 15 stycznia 2020 r (2019/2990 (RSP)) Dz .Urz. UE.C.2021r. nr 270, str.71; z dnia 18 czerwca 2020 r.(2020/2657(RSP)). Dz.U.UE.C.2021 nr 362, str.6; rezolucja Europejskiego Komitetu Ekonomiczno-Społecznego „Nowa narracja dla Europy” – Rezolucja

Uznano za niezbędne zwiększenie odporności obywateli oraz przedsiębiorstw w tym mikroprzedsiębiorstw, małych i średnich przedsiębiorstw, a także działań startupów i podmiotów obsługujących infrastrukturę krytyczną na rosnące cyberzagrożenia, które mogą mieć niszczące skutki społeczne i gospodarcze. Dostrzeżono potrzebę inwestycji w infrastrukturę i usługi, a także budowanie zdolności z myślą o rozwoju umiejętności w dziedzinie cyberbezpieczeństwa. Uznano za konieczne szybsze wykrywanie cyberzagrożeń oraz incydentów, a także reagowanie na nie[6].

Unia podjęła także szereg działań zmierzających do zmniejszenia podatności oraz zwiększenia odporności infrastruktury i podmiotów krytycznych na ryzyko cyberataktów[7]. Wśród nich wskazać należy rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)[8]. Istotną rolę pełnią także dyrektywy Parlamentu Europejskiego i Rady[9] oraz zalecenie Komisji (UE)

EKES-u w sprawie Konferencji w sprawie przyszłości Europy 27 kwietnia 2021 r., Dz. Urz. UE. C 2021, nr 286, str. 1; Na Konferencji zaproponowano, aby „UE zapewniła skuteczne i szybkie wdrożenie obowiązującego prawodawstwa oraz posiadała większe uprawnienia w zakresie zwiększania cyberbezpieczeństwa, zwalczania nielegalnych treści i przestępczości w cyberprzestrzeni, przeciwdziałania zagrożeniom cybernetycznym ze strony podmiotów niepaństwowych państw autorytarnych oraz usuwania skutków tych zagrożeń, a także przeciwdziałania dezinformacji". Ponadto podczas obrad Komisja przedstawiła unijną strategię cyberbezpieczeństwa. Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Konferencja w sprawie przyszłości Europy. Od wizji do konkretnych działań, 17 czerwca 2022 r., COM (2022) 404 final. Por. P. Burgoński, Konferencja w sprawie przyszłości Europy wobec zmian polityki równościowej i antydyskryminacyjnej, „Rocznik Integracji Europejskiej" 2022, nr 16, s.323-335.

[6] W rozporządzeniu zauważono, że państwa członkowskie Unii potrzebują pomocy w lepszym przygotowaniu się na poważne incydenty w cyberbezpieczeństwie, zwłaszcza na takie, które podejmowane są na dużą skalę. Wymagają także pomocy w reagowaniu na takowe incydenty i w rozpoczynaniu usuwania ich skutków. Skonstatowano, że w oparciu o istniejące struktury oraz w ścisłej współpracy z nimi Unia powinna także zwiększyć swoje zdolności w tych obszarach, w szczególności w zakresie zbierania i analizy danych dotyczących cyberzagrożeń i incydentów.

[7] Zob. w tym przedmiocie m.in. J. Sobczak, Cyberprzestrzeń jako obszar ochrony bezpieczeństwa narodowego w optyce dokumentów europejskich, w: P. Herbowski, D. Słapczyńska, D. Jagiełło (red.), „Pozyskiwanie informacji w walce z terroryzmem", Warszawa 2017, s. 42-55; J. Sobczak, W. Sobczak, Przestępczość w cyberprzestrzeni. Pomiędzy przepisami polskimi a międzynarodowymi, w: W. Kitler, K. Chałubińska-Jentkiewicz, K. Badzimirowska-Masłowska, „System bezpieczeństwa w cyberprzestrzeni RP", Warszawa 2018, s. 33-72; J. Sobczak, K. Kakareko, M. Gołda-Sobczak, Poszukiwanie unijnych standardów sztucznej inteligencji, „Cybersecurity and Law" 2023, nr 1 (9), s. 243-275; J. Sobczak, „Biała księga w sprawie sztucznej inteligencji" w systemie polityczno- prawnym Unii Europejskiej, w: R. Grabowski (red.) XXV lat Konstytucji Rzeczypospolitej Polskiej. Księga jubileuszowa dedykowana Profesor Halinie Ziębie-Załuckiej z okazji 70. Rocznicy urodzin, Toruń 2022, s. 527-548.

[8] Dz. Urz. UE.L., 2019 nr 151, str. 15.

[9] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz. Urz. UE. L 2013, nr 218, str. 8; dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii zmieniająca Rozporządzenie (UE)

2017/1584[10] Zauważyć należy, że w zaleceniu Rady z 8 grudnia 2022 r. w sprawie ogólnounijnego skoordynowanego podejścia do kwestii wzmocnienia odporności infrastruktury krytycznej wezwano państwa członkowskie do współpracy między sobą oraz współdziałania z Komisją i innymi właściwymi organami publicznymi, a także zainteresowanymi podmiotami w celu zwiększenia odporności infrastruktury krytycznej, wykorzystywanej do świadczenia usług kluczowych na rynku wewnętrznym[11].

W rozporządzeniu Parlamentu Europejskiego i Rady (EU) 2025/38 wskazano, że coraz większe ryzyko w cyberprzestrzeni i złożony krajobraz zagrożeń, w tym wyraźne niebezpieczeństwo rozprzestrzeniania się incydentów z jednego państwa członkowskiego na inne oraz państwa trzeciego na Unię, wymagają zwiększenia solidarności na poziomie Unii, aby skuteczniej wykrywać cyberzagrożenia i incydenty oraz lepiej przygotowywać się i reagować na nie, a także skuteczniej usuwać ich skutki. Taką możliwość widziano zwłaszcza w wzmocnieniu możliwości istniejących struktur. Ponadto w konkluzjach Rady z 23 maja 2022 r. w sprawie pozycji UE w kwestiach cyberprzestrzeni wezwano Komisję do przedstawienia wniosku dotyczącego nowego Funduszu Reagowania Cyberkryzysowego.

W rozporządzeniu przypomniano także, że we Wspólnym Komunikacie Komisji i Wysokiego Przedstawiciela Unii ds. Zagranicznych i Polityki Bezpieczeństwa z dnia 10 listopada 2022 r. do Parlamentu Europejskiego i Rady zatytułowanego „Polityka UE w zakresie cyberobrony”[12] zapowiedziano

nr 910/2014 i dyrektywę UE 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz. Urz. UE. L., 2022, nr 333, str. 80.

[10] Zalecenie Komisji (UE) 2018/1584 z dnia 13 września 2018 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę. Dz.Urz.UE.L.2017, nr 239, str. 36.

[11] Dz. Urz. UE. C 2023, nr 20, str. 1. W motywach zalecenia wskazano, że ochrona europejskiej infrastruktury krytycznej w sektorze energetycznym i transportowym jest obecnie regulowana dyrektywą Rady 2008/114/WE (Dz. Urz. UE. L 2008, nr 345, str.75), a bezpieczeństwo sieci i systemów informatycznych w całej Unii z naciskiem na zagrożenia dla cyberbezpieczeństwa zapewnia dyrektywa Parlamentu Europejskiego i Rady 2016/1148 (Dz. Urz. UE. L 2016, nr. 194, s.1). Wskazano w zaleceniu, że w celu zapewnienia wyższego wspólnego poziomu odporności i ochrony infrastruktury krytycznej, cyberbezpieczeństwa i rynku finansowego obowiązujące ramy prawne są zmieniane i uzupełniane przez przyjęcie nowych przepisów mających zastosowanie do podmiotów krytycznych (dyrektywa CER), wzmocnionych przepisów dotyczących wysokiego wspólnego poziomu cyberbezpieczeństwa w całej Unii (dyrektywa NIS 2) oraz nowych przepisów mających zastosowanie do operacyjnej odporności cyfrowej sektora finansowego (rozporządzenie DORA).Zauważyć należy, że dyrektywa NIS 2 została uchylona dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającą rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. 2022 r. nr 333, str. 80)

[12] Bruksela 10 listopada 2022, JOIN (2022) 49 final W tekście komunikatu przypomniano, że „W 2018 r. UE określiła cyberprzestrzeń jako sferę operacji wojskowych. W przyjętej w 2021 r. „wojskowej wizji i strategii dotyczącej cyberprzestrzeni jako obszaru operacyjnego” (EEAS(2021) 706 REV4) określono warunki ramowe i opisano cele, sposoby oraz środki potrzebne do wykorzystania cyberprzestrzeni jako sfery operacyjnej w celu wsparcia operacji UE w dziedzinie wspólnej polityki bezpieczeństwa i obrony (WPBiO)”. Wskazano także, że „Cyberobrona i wykorzystanie powiązanych zdolności obejmujących pełne spektrum operacji wojskowych w cyberprzestrzeni stanowi prerogatywę krajową poszczególnych państw członkowskich, a jednocześnie wymaga szerszego ekosystemu, w tym silnej bazy przemysłowej wspieranej przez rozwój zdolności na poziomie UE”.

inicjatywę na rzecz cybersolidarności UE. Wskazano, że celem tej polityki będzie wzmocnienie wspólnych unijnych zdolności w zakresie wykrywania, orientacji sytuacyjnej i reagowania oraz promowanie wprowadzenia unijnej infrastruktury centrów monitorowania bezpieczeństwa (SOC), wspieranie stopniowego tworzenia w Unii rezerwy do celów cyberbezpieczeństwa, opartej na usługach świadczonych przez zaufanych dostawców, wreszcie przeprowadzanie testów w krytycznych podmiotach pod kątem potencjalnej podatności na zagrożenia z wykorzystaniem unijnych ocen ryzyka[13].

Za konieczne uznano przyspieszenie wykrywania cyberzagrożeń i incydentów[14], zwłaszcza godzących w całą Unię, a także zwiększenie solidarności dzięki podniesieniu poziomu gotowości i zdolności państw członkowskich Unii do zapobiegania poważnym incydentom w cyberbezpieczeństwie oraz incydentom w cyberbezpieczeństwie o dużej skali Zauważono, że należy zadbać o szybkość reagowania na takie zagrożenia. Za niezbędne uznano stworzenie ogólnoeuropejskiej sieci centrów cyberbezpieczeństwa, czyli europejskiego systemu cyberostrzeżeń. Zmierzać to winno do zbudowania skoordynowanych zdolności w zakresie wykrywania i orientacji sytuacyjnej, a także do wzmocnienia zdolności Unii do wykrywania zagrożeń i udostępniania informacji w tym zakresie. Podkreślono potrzebę stworzenia mechanizmu cyberkryzysowego, który winien wesprzeć państwa członkowskie w przygotowaniu się na poważne incydenty w cyberbezpieczeństwie oraz na takowe incydenty o dużej skali. Celem musi być ograniczanie wpływu takich incydentów oraz usuwanie ich skutków, a także wspieranie użytkowników w reagowaniu na takowe incydenty.

W motywacyjnej części rozporządzenia Parlamentu Europejskiego i Rady (EU) 2025/38 podkreślono konieczność ustanowienia europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie na potrzeby

[13] We Wspólnym Komunikacie wskazano także na zauważone przez Europejską Organizację ds. Cyberbezpieczeństwa braki specjalistów z obszarów cyberbezpieczeństwa, postulując potrzebę utworzenia unijnej Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa. Podkreślono również kluczowe znaczenie partnerstwa Unii z NATO w obszarze cyberobrony i konieczność dalszych wspólnych działania na rzecz opracowania wspólnych rozwiązań w odpowiedzi na obecne zagrożenia i wyzwania. Podkreślono, że Europejski Instrument na rzecz Pokoju (EPF) będzie nadal wspierał starania UE na rzecz zwiększania zdolności obronnych, w tym zdolności w zakresie cyberobrony, krajów partnerskich – w szczególności w sąsiedztwie UE. Zadeklarowano wreszcie, że UE zagwarantuje w razie konieczności lepsze powiązanie wsparcia w zakresie cyberobrony z budowaniem zdolności w zakresie cyberbezpieczeństwa w sektorze cywilnym, w szczególności za pośrednictwem unijnej Rady ds. Budowania Zdolności Cyfrowych.

[14] W art. 2 rozporządzenia stwierdzono, że używane w jego tekście pojęcia: „incydentu" należy rozumieć zgodnie z art. 6 pkt 6 dyrektywy 2022/2555 (Dz. Urz. UE. L. 2022, nr 333, str. 80); „poważnego incydentu w cyberbezpieczeństwie" jako incydent spełniający kryteria określone w art. 23 ust. 3 dyrektywy 2022/2555, „poważnego incydentu" zgodnie z definicją zawartą w art. 3 pkt 8 rozporządzenia Parlamentu Europejskiego i Rady (UE, Euratom) 2023/2841 z dnia 13 grudnia 2023 r. w sprawie ustanowienia środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa w instytucjach, organach i jednostkach organizacyjnych Unii (Dz. U. UE. L. z 2023 r. poz. 2841); „incydentu równoważnego incydentowi w cyberbezpieczeństwie na dużą skalę" oznacza, w przypadku instytucji, organów i jednostek organizacyjnych Unii - poważny incydent, a w przypadku państw trzecich stowarzyszonych z programem "Cyfrowa Europa" - incydent, który powoduje poziom zakłóceń wykraczający poza zdolność reagowania danego państwa trzeciego stowarzyszonego z programem "Cyfrowa Europa"; „cyberzagrożenia" w rozumieniu art. 2 pkt 8 rozporządzenia 2019/881 (Dz. U. UE. L. z 2019 r. Nr 151, str. 15).

przeglądu i oceny konkretnych, poważnych incydentów w cyberbezpieczeństwie lub incydentów równoważnych incydentom w cyberbezpieczeństwie na dużą skalę. Działania zmierzające w tym kierunku powinny być, jak wskazano, prowadzone z należytym poszanowaniem, kompetencji państw członkowskich. Powinny one także uzupełniać, a nie pobierać działań wprowadzonych przez sieć CSIRT oraz europejską sieć organizacji łącznikowych ds. kryzysów cyberbezpieczeństwa (EU–CyCLONe), a także grupę współpracy (grupa współpracy NIS)[15].

W motywach rozporządzenia wskazano, że dla osiągnięcia wskazanych celów okazała się zmiana w niektórych obszarach rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/694[16] poprzez dodanie nowych celów operacyjnych związanych z europejskim systemem cyberostrzeżeń i mechanizmem cyberkryzysowym w zakresie obejmującym zagwarantowanie odporności, integralności i wiarygodności jednolitego rynku cyfrowego oraz zwiększenie zdolności w zakresie monitorowania cyberataków i cyberzagrożeń, a także reagowania na nie. Dostrzeżono przy tym potrzebę ustanowienia szczegółowych warunków na jakich można przyznawać wsparcie finansowe dla działań wdrażających europejski system cyberostrzeżeń i rezerwę cyberbezpieczeństwa UE. W kwestii zasad finansowych podkreślono, że mają do nich zastosowanie rozwiązania przyjęte przez Parlament Europejski i Radę na podstawie art. 322 TFUE ustanowione rozporządzeniem Parlamentu Europejskiego i Rady (UE, Euratom) 2024/2509[17].

W części motywacyjnej rozporządzenia stwierdzono, że uczestnictwo państwa unijnych w europejskim systemie cyberostrzeżeń jest dobrowolne,

[15] Jednostki te zostały ustanowione na podstawie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniającej rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz. Urz. UE. L. 2022, nr 333, str. 80. Warto przypomnieć, że celem dyrektywy 2016/1148 (Dz. Urz. UE. L. 2016, nr 194, str.1) było zbudowanie zdolności w zakresie cyberbezpieczeństwa w całej Unii, łagodzenie zagrożeń dla sieci i systemów informatycznych, wykorzystywanych do celów świadczenia usług kluczowych podstawowych w najważniejszych sektorach oraz zapewnienie ciągłości takich usług w przypadku wystąpienia incydentów, co miało przyczynić się do bezpieczeństwa Unii oraz sprawnego funkcjonowania jej gospodarki i społeczeństwa. Wielokrotnie wskazywano, że dyrektywa 2016/1148, dzięki ustanowieniu Grupy Współpracy oraz sieci krajowych zespołów reagowania na incydenty bezpieczeństwa krajowego, przyczyniła się do współpracy państw unijnych, ujawniając jednocześnie, czego dowiódł przegląd dyrektywy, braki uniemożliwiające radzenie sobie z wyzwaniami w zakresie cyberbezpieczeństwa. Pamiętać nadal należy, że podstawą prawną tej dyrektywy stanowi art. 114 TFUE, którego celem jest ustanowienie i funkcjonowanie rynku wewnętrznego przez usprawnienie środków służących zbliżeniu przepisów krajowych. Przegląd dyrektywy 2016/1148 ujawnił istnienie znacznych rozbieżności w jej wdrażaniu przez państwa członkowskie Unii, zwłaszcza w odniesieniu do jej zakresu, którego ustalenie w znacznej mierze pozostawiono uznaniu państw członkowskich.

[16] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiający program „Cyfrowa Europa" oraz uchylający decyzję (UE) 2015/2240, Dz. Urz. UE. L. 2021, nr 166, str. 1.

[17] Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2024/2509 z dnia 23 września 2024 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, Dz.Urz.UE.L. 2024, str. 2509 Warto w tym miejscu wspomnieć, że zasady przyjęte w art. 322 TFUE obejmują także ogólny system warunkowości służący ochronie budżetu Unii ustanowiony rozporządzeniem Parlamentu Europejskiego i Rady (UE, Euratom) 2020/2092 z 16 grudnia 2020 w sprawie ogólnego systemu. Dz. Urz.UE.L. 2020.str. 433 I.

jednak każde z państw powinno wyznaczyć na poziomie krajowym jeden podmiot, którego zadaniem będzie koordynowanie działań w zakresie wykrywania cyberzagrożeń w państwie członkowskim. Te krajowe centra cyberbezpieczeństwa powinny pełnić funkcje punktu odniesienia i punktu dostępu na poziomie krajowym dla celów uczestnictwa w europejskim systemie cyberostrzeżeń oraz zapewniać, aby informacje dotyczące cyberzagrożeń, uzyskiwane od podmiotów publicznych i prywatnych były skutecznie i sprawnie udostępniane i gromadzone na poziomie krajowym. Krajowe centra winny także wspierać wymianę danych i informacji z odpowiednimi społecznościami sektorowymi i międzysektorowymi, w tym także z branżowymi ośrodkami wymiany i analizy informacji (ISAC). Taka ścisła i skoordynowana współpraca ma przy tym kluczowe znaczenia dla zwiększenia cyberodporności Unii, Jest ona szczególnie cenna w kontekście udostępniania danych wywiadowczych dotyczących cyberzagrożeń. Zauważono przy tym, że krajowe centra cyberbezpieczeństwa mogłyby w ramach takiej współpracy składać wnioski o konkretne informacje i otrzymywać je (motyw 14).

W motywach dostrzeżono także potrzebę ustanowienia transgranicznych centrów cyberbezpieczeństwa, które powinny zrzeszać krajowe centra co najmniej trzech państw członkowskich. Celem ich miałoby być zapewnienie pełnego osiągnięcia korzyści płynących z transgranicznego wykrywania zagrożeń, udostępniania informacji na ich temat i zarządzania nimi. Ogólnym celem transgranicznych centrów cyberbezpieczeństwa powinno być zwiększenie zdolności w zakresie analizy i wykrywania cyberzagrożeń oraz zapobiegania im, zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ogólnego systemu warunkowości służącego ochronie budżetu Unii (sic!)[18] (motyw 15). Państwo członkowskie wybrane przez Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (dalej: ECCC) ustanowione rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2021/887[19], w następstwie zaproszenia

[18] Rozporządzenie Parlamentu Europejskiego i Rady (EU, Euratom) 2020/2092 z dnia 16 grudnia 2020 w sprawie ogólnego systemu warunkowości służącego ochronie budżetu Unii, Dz.Urz.UE.L. 2020, nr 433 I/1.

[19] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/887 z 20 maja 2021 r. ustanawiające Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji, Dz.Urz.UE.L. 2021, nr 202, str. 1. W motywach tego rozporządzenia przypomniano, że Unia w 2016 r. przyjęła pierwsze środki w zakresie cyberbezpieczeństwa w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2026 r. w sprawie środków na rzecz wysokiego poziomu bezpieczeństwa sieci i systemu informatycznych na terytorium Unii, Dz.Urz.UE.L. 2016, nr 194, str. 1. Zauważono także, że we wrześniu 2017 Komisja i Wysoki Przedstawiciel przedstawili wspólny komunikat do Parlamentu Europejskiego i Rady (UE) „Odporność, prewencja i obrona: budowa solidnego bezpieczeństwa cybernetycznego Unii Europejskiej", aby jeszcze bardziej wzmocnić odporność, prewencję i reakcję Unii w przypadku cyberataków. Podkreślono także, że podczas Tallińskiego Szczytu Cyfrowego we wrześniu 2017 r. szefowie państw i rządów wezwali Unię, aby do 2025 r. stała się światowym liderem w dziedzinie cyberbezpieczeństwa w celu zapewnienia obywatelom, konsumentom i przedsiębiorstwu zaufanie, pewności i ochrony online oraz umożliwienia istnienia wolnego, bezpiecznego i podlegającego przepisom prawa Internetu, deklarując zamiar powszechniejszego korzystania z rozwiązań w zakresie otwartego oprogramowania i otwartych standardów przy przebudowie systemów i rozwiązań w zakresie technologii informacyjno-komunikacyjnych (ICT), dążąc do unikania uzależnienia od jednego dostawcy, w tym także

do wyrażenia zainteresowania w celu ustanowienia krajowego centrum cyberbezpieczeństwa lub zwiększenia jego zdolności powinno - wspólnie z ECCC – zakupić odpowiednie narzędzia, infrastrukturę lub usługi otrzymując dotację na obsługę narzędzi, infrastruktury i usług. Postępowanie w tym zakresie powinno być zgodne z art. 168 ust. 2 rozporządzenia (UE, Euratom) 2024/2509 oraz z zasadami finansowymi ECCC. Takie wybrane państwo członkowskie, mające utworzyć krajowe centrum cyberbezpieczeństwa, powinno zobowiązać się do złożenia wniosku o uczestnictwo w transgranicznym centrum cyberbezpieczeństwa w ciągu dwóch lat od daty nabycia narzędzi, infrastruktury lub usług, bądź od daty otrzymania finansowania w formie dotacji. W zależności od tego, co nastąpiło wcześniej.

W rozporządzeniu wskazano, że transgraniczne centra cyberbezpieczeństwa powinny działać jako centralne punkty, które umożliwiają szeroko zakrojone łączenie odpowiednich danych, w tym także danych wywiadowczych na temat cyberzagrożeń oraz pozwalają na rozpowszechnianie informacji o zagrożeniach w dużej i zróżnicowanej grupy zainteresowanych stron. Powinny także ściśle ze sobą współpracować, aby zapewnić synergię i komplementarność działań (motyw 19 i 20). Wspólna orientacja sytuacyjna odpowiednich organów jest, jak stwierdzono w motywach rozporządzenia, warunkiem koniecznym w gotowości i koordynacji całej Unii w odniesieniu do poważnych incydentów w cyberbezpieczeństwie i incydentów, w tym incydentów na dużą skalę. Przypomniano przy tej okazji, że dyrektywą 2022/2555 ustanowiono EU-CyCLONe, aby pomagać w skoordynowanym zarządzaniu na poziomie operacyjnym incydentami i sytuacjami kryzysowymi w cyberbezpieczeństwie na dużą skalę i zapewniać regularną wymianę odpowiednich informacji między państwami członkowskimi, a instytucjami, organami i jednostkami organizacyjnymi Unii. Tą dyrektywą ustanowiono również sieć CSIRT (zespołów reagowania na incydenty bezpieczeństwa komputerowego) mającą na celu promowanie szybkiej i skutecznej współpracy między wszystkimi państwami członkowskimi w płaszczyźnie cyberbezpieczeństwa (zob. art. 10-13). Wywiedziono dalej, że transgraniczne centra cyberbezpieczeństwa powinny działać w kierunku zwiększenia poziomu solidarności w sytuacjach, kiedy pojawiają się informacje dotyczące potencjalnego lub trwającego incydentu w odniesieniu do cyberbezpieczeństwa, zwłaszcza kiedy dotyczy on dużej skali.

Przypomniano przy tej okazji o potrzebie zapewnienia poufności informacji oraz o odpowiedzialności Komisji w ramach Unijnego Mechanizmu Ochrony Ludności (UMOL) ustanowionego decyzją Parlamentu Europejskiego i Rady 1313/2013/UE[20] oraz o odpowiedzialności za przedstawianie sprawozdań analitycznych na potrzeby zintegrowanych uzgodnień UE

rozwiązań i standardów opracowanych lub promowanych w ramach unijnych programów na rzecz interoperacyjności i standaryzacji takich jak ISA.

[20] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 13 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności Dz. Urz. UE. L 2013, nr 347, str.294.

dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (uzgodnienia IPCR) zgodnie z decyzją wykonawczą Rady UE 2018/1993[21].

Podmioty uczestniczące w europejskim systemie cyberostrzeżeń powinny zapewniać wysoki poziom interoperacyjności między sobą, w tym w stosownych przypadkach w odniesieniu do formatów danych, taksonomii, narzędzi przetwarzania i analityki danych. Powinny one również zapewnić bezpieczne kanały komunikacji, minimalny poziom bezpieczeństwa warstwy aplikacji, tablicę wskaźników orientacji sytuacyjnej oraz same wskaźniki (motyw 22)[22].

Kładąc nacisk na potrzebę umożliwienia prowadzonej na dużą skalę wymiany odpowiednich danych i informacji na temat cyberzagrożeń pochodzących z różnych źródeł w zaufanym i bezpiecznym środowisku, podmioty uczestniczące w europejskim systemie cyberostrzeżeń powinny być wyposażone w najnowocześniejsze i wysoce bezpieczne narzędzia, sprzęt i infrastrukturę oraz posiadać wykwalifikowany personel. Powinno to umożliwić poprawę zdolności zbiorowego wykrywania incydentów oraz terminowe ostrzeganie organów i odpowiednich podmiotów, w szczególności dzięki wykorzystaniu najnowszych technologii sztucznej inteligencji i analityki danych[23].

Duży nacisk położono w motywach rozporządzenia 2025/38 na zachowanie poufności i bezpieczeństwa informacji, uznając, że ma to zasadnicze znaczenie z punktu widzenia wszystkich trzech filarów niniejszego rozporządzenia: zachęcania do udostępniania informacji lub ich wymiany w kontekście europejskiego systemu cyberostrzeżeń, ochrony interesów podmiotów ubiegających się o wsparcie z mechanizmu cyberkryzysowego, lub zapewniania, aby zgłoszenia w ramach europejskiego mechanizmu przeglądu incydentów w cyberbezpieczeństwie umożliwiały zdobycie doświadczenia bez wywierania negatywnego wpływu na podmioty dotknięte incydentami. Podkreślono, że udział państw członkowskich i podmiotów w tych mechanizmach wymaga wzajemnego zaufania. Udostępnianie informacji, które zgodnie z przepisami unijnymi lub krajowymi mają status informacji poufnych, lub ich wymiana, powinny być ograniczone do tego, co jest istotne i proporcjonalne do celów tej wymiany. Podczas udostępniania informacji lub ich wymiany należy zachować ich poufność oraz chronić bezpieczeństwo i interesy handlowe każdego zainteresowanego podmiotu. Udostępnianie informacji lub ich wymiana na podstawie niniejszego rozporządzenia może się

[21] Decyzja wykonawcza Rady UE 2018/1993 z dnia 11 grudnia 2018 r. w sprawie zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych, Dz. Urz. UE. L 2018, nr 32, str. 28.

[22] Przy przyjmowaniu wspólnej taksonomii i opracowywaniu wzoru sprawozdań sytuacyjnych na potrzeby opisywania przyczyn wykrytych cyberzagrożeń i ryzyka w cyberprzestrzeni należy uwzględnić dotychczasowe prace w kontekście wykonywania dyrektywy (UE) 2022/2555 (Dz. Urz. UE. L., 2022, nr 333, str. 80).

[23] Udostępnianie informacji między uczestnikami europejskiego systemu cyberostrzeżeń powinno być, w myśl motywu 26 rozporządzenia 2025/38, zgodne z obowiązującymi wymogami prawnymi, w szczególności z unijnymi i krajowymi przepisami o ochronie danych, a także z unijnymi regułami konkurencji regulującymi wymianę informacji. Odbiorca informacji powinien wdrożyć - o ile konieczne jest przetwarzanie danych osobowych - środki techniczne i organizacyjne chroniące prawa i wolności osób, których dane dotyczą, oraz zniszczyć dane, gdy tylko przestaną one być niezbędne do określonego celu, oraz poinformować jednostkę udostępniającą dane o ich zniszczeniu.

odbywać z wykorzystaniem umów o zachowaniu poufności lub wytycznych dotyczących dystrybucji informacji, korzystając z kodów poufności.

W rozporządzeniu 2025/38 podjęto istotny problem uruchamiania rezerwy cyberbezpieczeństwa UE, wskazując, że konieczne są w tym przedmiocie szczegółowe zasady poufności. Wniosek o wsparcie winien być składany i oceniany, a wsparcie udzielane w kontekście kryzysu podmiotom działającym w sektorach wrażliwych. Podkreślono, że rezerwa cyberbezpieczeństwa UE może skutecznie funkcjonować, jeżeli użytkownicy i podmioty będą niezwłocznie udostępniali wszelkie informacje niezbędne do tego, aby każdy podmiot mógł odegrać wyznaczoną mu rolę w ocenie wniosków i uruchamianiu wsparcia. W związku z tym wszystkie takie informacje mogą być wykorzystywane lub udostępniane wyłącznie wtedy, gdy jest to konieczne dla działania rezerwy cyberbezpieczeństwa UE, a informacje poufne lub niejawne na podstawie prawa Unii i prawa krajowego mają być wykorzystywane i udostępniane wyłącznie zgodnie z tym prawem (motyw 28).

Zauważono w części motywacyjnej, że w związku z rosnącym ryzykiem i zwiększającą się liczbą incydentów mających wpływ na państwa członkowskie konieczne jest ustanowienie instrumentu wsparcia kryzysowego, a mianowicie mechanizmu cyberkryzysowego, aby poprawić odporność Unii na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę i incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę oraz uzupełnić działania państw członkowskich wsparciem finansowym w sytuacjach nadzwyczajnych na potrzeby gotowości, reagowania na incydenty i wstępnego przywrócenia funkcjonowania usług kluczowych. Ponieważ pełne usunięcie skutków incydentu jest kompleksowym procesem przywracania funkcjonowania podmiotu dotkniętego incydentem do stanu sprzed incydentu i może długo trwać oraz pociągać za sobą znaczące koszty, wsparcie z rezerwy cyberbezpieczeństwa UE powinno się ograniczać do wstępnego etapu procesu usuwania skutków, który pomaga przywrócić podstawowe funkcje systemów (motyw 29)[24].

Mechanizm cyberkryzysowy powinien zapewniać państwom członkowskim wsparcie uzupełniające ich własne środki i zasoby oraz inne istniejące możliwości wsparcia w przypadku reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę oraz wstępnego usuwania ich skutków, takie jak: usługi świadczone przez ENISA zgodnie z jej mandatem, skoordynowana reakcja i pomoc ze strony sieci CSIRT, wsparcie ze strony EU-CyCLONe na potrzeby zmniejszenia zagrożeń, a także wzajemna pomoc między państwami członkowskimi, w tym w kontekście art. 42 ust. 7 TUE i zespoły szybkiego reagowania na cyberincydenty w ramach stałej współpracy strukturalnej (PESCO)

[24] Wskazano w rozporządzeniu 2025/38, że mechanizm cyberkryzysowy powinien umożliwiać szybkie i skuteczne udzielanie pomocy w określonych okolicznościach i na jasnych warunkach oraz dokładne monitorowanie i ocenę sposobu wykorzystania zasobów. O ile podstawowa odpowiedzialność za zapobieganie incydentom i kryzysom spoczywa na państwach członkowskich, mechanizm cyberkryzysowy propaguje solidarność między państwami członkowskimi zgodnie z art. 3 ust. 3 Traktatu o Unii Europejskiej (TUE).

ustanowione na podstawie decyzji Rady (WPZiB) 2017/2315[25]. W mechanizmie tym należy uwzględnić potrzebę zapewnienia dostępności specjalistycznych środków wspierających gotowość, reagowanie na takie incydenty i usuwanie ich skutków w całej Unii i w państwach trzecich stowarzyszonych z programem "Cyfrowa Europa".

Wyraźnie zaznaczono w rozporządzeniu 2025/38, że pozostaje ono bez uszczerbku dla procedur i ram koordynowania reagowania kryzysowego na poziomie Unii, w szczególności dyrektywy (UE) 2022/2555, Unijnego Mechanizmu Ochrony Ludności ustanowionego decyzją Parlamentu Europejskiego i Rady nr 1313/2013/UE[26], uzgodnień IPCR oraz zalecenia Komisji (UE) 2017/1584[27]. Wsparcie z mechanizmu cyberkryzysowego może uzupełniać pomoc udzielaną w kontekście wspólnej polityki zagranicznej i bezpieczeństwa oraz wspólnej polityki bezpieczeństwa i obrony, w tym za pośrednictwem zespołów szybkiego reagowania na cyberincydenty, uwzględniając cywilny charakter mechanizmu cyberkryzysowego[28].

W części motywacyjnej rozporządzenia 2025/38 zwrócono uwagę, że w dyrektywie (UE) 2022/2555 zobowiązano państwa członkowskie do wyznaczenia lub ustanowienia co najmniej jednego organu ds. zarządzania kryzysowego w cyberbezpieczeństwie oraz do zapewnienia tym organom odpowiednich zasobów, aby organy te mogły efektywnie i skutecznie wykonywać powierzone im zadania. Zobowiązano w niej również państwa członkowskie do określenia zdolności, zasobów i procedur, które można wykorzystać w razie sytuacji kryzysowej, a także do przyjęcia krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę, w którym określa się cele i tryb zarządzania incydentami i zarządzania kryzysowego w cyberbezpieczeństwie na dużą skalę. Państwa członkowskie są również zobowiązane do ustanowienia co najmniej jednego CSIRT, który jest odpowiedzialny za obsługę incydentów zgodnie z wyraźnie określoną procedurą i obejmuje co najmniej sektory, podsektory i rodzaje podmiotów wchodzące w zakres stosowania tej dyrektywy, oraz do zapewnienia, aby CSIRT dysponowały odpowiednimi zasobami, tak aby mogły skutecznie realizować swoje zadania. Podkreślono, że rozporządzenie 2025/38 pozostaje bez uszczerbku dla roli Komisji w zapewnianiu przestrzegania przez państwa członkowskie obowiązków wynikających z dyrektywy (UE) 2022/2555.

[25] Decyzja Rady (WPZiB) 2017/2315 z dnia 11 grudnia 2017 r. w sprawie ustanowienia stałej współpracy strukturalnej (PESCO) oraz ustalenia listy uczestniczących w niej państw członkowskich (Dz. U. UE. L. z 2017 r. Nr 331, str. 57 z późn. zm.).

[26] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/EU z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz. U. UE. L. z 2013 r. Nr 347, str. 924 z późn. zm.).

[27] Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę (Dz. U. UE. L. z 2017 r. Nr 239, str. 36).

[28] W motywach rozporządzenia podkreślono, że wsparcie z mechanizmu cyberkryzysowego może uzupełniać działania realizowane w kontekście art. 42 ust. 7 Traktatu UE, w tym pomoc udzielaną przez jedno państwo członkowskie innemu państwu członkowskiemu lub stanowić część wspólnej reakcji Unii i państw członkowskich, lub w sytuacjach, o których mowa w art. 222 TFUE. Wykonywanie tego rozporządzenia powinno być również skoordynowane, w stosownych przypadkach, z wdrażaniem środków z zestawu narzędzi dla dyplomacji cyfrowej (motyw 31).

Mechanizm cyberkryzysowy powinien zapewniać pomoc w zakresie działań mających na celu zwiększenie gotowości, a także działań w zakresie reagowania na incydenty w celu złagodzenia skutków poważnych incydentów w cyberbezpieczeństwie i incydentów w cyberbezpieczeństwie na dużą skalę, wsparcia wstępnego usuwania ich skutków lub przywrócenia podstawowych funkcji usług świadczonych przez podmioty działające w sektorach kluczowych lub podmioty działające w innych sektorach krytycznych.

Za konieczne uznano w rozporządzeniu 2025/38 propagowanie spójnego podejścia oraz zwiększenie bezpieczeństwa w całej Unii i na jej rynku wewnętrznym. Stwierdzono, że w ramach działań w zakresie gotowości, należy w skoordynowany sposób wspierać testowanie i ocenę cyberbezpieczeństwa podmiotów działających w sektorach kluczowych określonych zgodnie z dyrektywą (UE) 2022/2555, w tym za pomocą ćwiczeń i szkoleń[29].

Mechanizm cyberkryzysowy powinien wspierać pomoc techniczną udzielaną przez jedno państwo członkowskie drugiemu państwu członkowskiemu dotkniętemu poważnym incydentem w cyberbezpieczeństwie lub incydentem w cyberbezpieczeństwie na dużą skalę. Udzielające takiej pomocy państwa członkowskie powinny mieć możliwość składania wniosków o pokrycie kosztów związanych z wysyłaniem zespołów ekspertów w ramach wzajemnej pomocy. Koszty kwalifikowalne mogą obejmować koszty podróży, zakwaterowania i diety dziennej ekspertów ds. cyberbezpieczeństwa.

Podkreślono w rozporządzeniu 2025/38, że w ramach mechanizmu cyberkryzysowego należy stopniowo tworzyć rezerwę cyberbezpieczeństwa UE składającą się z usług oferowanych przez zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa, aby wspierać reagowanie i wstępne usuwanie skutków w przypadku poważnych incydentów w cyberbezpieczeństwie, incydentów w cyberbezpieczeństwie na dużą skalę lub incydentów równoważnych incydentom w cyberbezpieczeństwie na dużą skalę mających wpływ na państwa członkowskie, instytucje, organy i jednostki organizacyjne Unii lub państwa trzecie stowarzyszone z programem "Cyfrowa Europa"[30]. Rezerwa cyberbezpieczeństwa UE powinna zapewniać dostępność i gotowość usług. W związku z tym powinna obejmować usługi, które są deklarowane z wyprzedzeniem, w tym na przykład gotowość do natychmiastowego i szybkiego reagowania. Usługi z rezerwy cyberbezpieczeństwa UE powinny służyć wspieraniu organów krajowych w udzielaniu pomocy dotkniętym incydentami podmiotom działającym w sektorach kluczowych lub dotkniętym incydentami podmiotom działającym w innych sektorach krytycznych jako uzupełnienie działań tych organów na poziomie krajowym. Usługi z rezerwy cyberbezpieczeństwa UE powinny również móc służyć zapewnieniu wsparcia instytucjom, organom i jednostkom

[29] Wywiedziono, że w tym celu Komisja, po konsultacjach z ENISA, we współpracy z grupą współpracy NIS i EU-CyCLONe, powinna regularnie identyfikować odpowiednie sektory lub podsektory, które powinny kwalifikować się do otrzymania wsparcia finansowego na skoordynowane testowanie gotowości na poziomie Unii. Sektory lub podsektory należy wybierać spośród sektorów kluczowych wymienionych w załączniku I do dyrektywy (UE) 2022/2555. Skoordynowane testowanie gotowości powinno opierać się na wspólnych scenariuszach ryzyka i wspólnych metodykach. (motyw 34)

[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiający program „Cyfrowa Europa” oraz uchylający decyzję (UE) 2015/2240, Dz.Urz.UE.L. 2021, nr 166, str. 1.

organizacyjnym Unii na podobnych warunkach. Rezerwa cyberbezpieczeństwa UE mogłaby także wzmacniać konkurencyjną pozycję przemysłu i usług w Unii w całej gospodarce cyfrowej,

Komisja, w myśl postanowień rozporządzenia 2025/38, powinna ponosić ogólną odpowiedzialność za wdrożenie rezerwy cyberbezpieczeństwa UE. Biorąc pod uwagę rozległe doświadczenie ENISA w dziedzinie cyberbezpieczeństwa, ENISA jest najbardziej odpowiednią agencją do wdrożenia rezerwy cyberbezpieczeństwa UE. W związku z tym Komisja powinna powierzyć ENISA, częściowo lub - jeżeli uzna to za stosowne – w całości, obsługę rezerwy cyberbezpieczeństwa UE i zarządzanie nią. Powierzenie jej tych zadań powinno się odbyć zgodnie z przepisami rozporządzenia (UE, Euratom) 2024/2509[31], a w szczególności powinno być uzależnione od spełnienia odpowiednich warunków podpisania umowy o przyznanie wkładu. Wszelkie aspekty obsługi rezerwy cyberbezpieczeństwa UE i zarządzaniu nią, które nie zostały powierzone ENISA, powinny podlegać zarządzaniu bezpośredniemu przez Komisję, w tym przed podpisaniem umowy o przyznanie wkładu.

Państwa członkowskie powinny odgrywać kluczową rolę w tworzeniu i uruchamianiu rezerwy cyberbezpieczeństwa UE, a także w okresie po jej uruchomieniu. Ponieważ rozporządzenie (UE) 2021/694[32] jest odpowiednim aktem podstawowym dla działań wdrażających rezerwę cyberbezpieczeństwa UE, działania w ramach rezerwy cyberbezpieczeństwa UE należy uwzględnić w programach prac, o których mowa w art. 24 rozporządzenia (UE) 2021/694. Zgodnie z ust. 6 tego artykułu te programy prac mają być przyjmowane przez Komisję w drodze aktów wykonawczych zgodnie z procedurą sprawdzającą. Ponadto Komisja, w koordynacji z grupą współpracy NIS, powinna określić priorytety i ewolucję rezerwy cyberbezpieczeństwa UE.(motyw 45)

W rozporządzeniu 2025/38 stwierdzono, że dążąc do wesparcia ustanowienia rezerwy cyberbezpieczeństwa UE, ważne jest, aby Komisja zwróciła się do ENISA o przygotowanie propozycji programu certyfikacji cyberbezpieczeństwa w odniesieniu do usług zarządzanych w zakresie bezpieczeństwa na podstawie rozporządzenia (UE) 2019/881 w obszarach objętych mechanizmem cyberkryzysowy. Podkreślono, że chcąc wspierać osiągnięcie celów rozporządzenia 2025/38, które obejmują propagowanie wspólnej orientacji sytuacyjnej, zwiększanie odporności Unii oraz umożliwianie skutecznego reagowania na poważne incydenty w cyberbezpieczeństwie i incydenty w cyberbezpieczeństwie na dużą skalę, Komisja lub EU-CyCLONe powinny mieć możliwość zwrócenia się do ENISA, ze wsparciem sieci CSIRT i za zgodą danego państwa członkowskiego, o dokonanie przeglądu i oceny cyberzagrożeń, znanych możliwych do wykorzystania podatności oraz działań łagodzących w odniesieniu do konkretnego poważnego incydentu w cyberbezpieczeństwie lub incydentu w cyberbezpieczeństwie na dużą skalę. Wywiedziono, że po zakończeniu

[31] Rozporządzenie Parlamentu Europejskiego i Rady (UE, Euratom) 2024/2509 z dnia 23 września 2024 r. w sprawie zasad finansowych mających zastosowanie do budżetu ogólnego Unii, Dz.Urz.UE.L. 2024, str. 2509.

[32] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program Cyfrowa Europa oraz uchylające decyzję (UE) 2015/2240 (Tekst mający znaczenie dla EWG) (Dz. U. UE. L. z 2021 r. Nr 166, str. 1 z późn. zm.).

przeglądu i oceny incydentu ENISA powinna przygotować sprawozdanie z przeglądu incydentu we współpracy z zainteresowanym państwem członkowskim, odpowiednimi zainteresowanymi stronami, w tym z przedstawicielami sektora prywatnego, Komisją oraz innymi odpowiednimi instytucjami, organami i jednostkami organizacyjnymi Unii[33].

Warunki określone w niniejszym rozporządzeniu w odniesieniu do rezerwy cyberbezpieczeństwa UE i zaufanych dostawców usług zarządzanych w zakresie bezpieczeństwa powinny mieć zastosowanie do wsparcia udzielanego państwom trzecim stowarzyszonym z programem "Cyfrowa Europa". Państwa trzecie stowarzyszone z programem "Cyfrowa Europa" powinny mieć możliwość wystąpienia o wsparcie z rezerwy cyberbezpieczeństwa UE, w przypadku, gdy podmioty, które potrzebują wsparcia z rezerwy cyberbezpieczeństwa UE, są podmiotami działającymi w sektorach kluczowych lub podmiotami działającymi w innych sektorach krytycznych oraz w przypadku, gdy wykryte incydenty prowadzą do znaczących zakłóceń operacyjnych lub mogą mieć skutki uboczne w Unii. Państwa trzecie stowarzyszone z programem "Cyfrowa Europa" powinny kwalifikować się do otrzymania wsparcia tylko wtedy, gdy umowa, na podstawie której są one stowarzyszone z programem "Cyfrowa Europa", wyraźnie przewiduje takie wsparcie. Ponadto takie państwa trzecie powinny nadal kwalifikować się do wsparcia tylko tak długo, jak spełnione są trzy kryteria. Po pierwsze, państwo trzecie powinno w pełni przestrzegać odpowiednich postanowień tej umowy. Po drugie, biorąc pod uwagę komplementarny charakter rezerwy cyberbezpieczeństwa UE, państwo trzecie powinno było podjąć odpowiednie kroki, aby przygotować się na poważne incydenty w cyberbezpieczeństwie lub incydenty równoważne incydentom w cyberbezpieczeństwie na dużą skalę. Po trzecie, udzielenie wsparcia z rezerwy cyberbezpieczeństwa UE powinno być spójne z polityką Unii wobec tego państwa i ogólnymi stosunkami z tym państwem oraz z innymi politykami Unii w dziedzinie bezpieczeństwa. W kontekście swojej oceny zgodności z tym trzecim kryterium Komisja powinna konsultować się z Wysokim Przedstawicielem w kwestii dostosowania takiego wsparcia do wspólnej polityki zagranicznej i bezpieczeństwa.

W komunikacie Komisji z dnia 18 kwietnia 2023 r. w sprawie Akademii Umiejętności w dziedzinie Cyberbezpieczeństwa zwrócono uwagę na niedobór wykwalifikowanych specjalistów. Takie kwalifikacje są potrzebne do realizacji celów niniejszego rozporządzenia. Unia pilnie potrzebuje specjalistów posiadających umiejętności i kompetencje, aby zapobiegać cyberatakom, wykrywać i powstrzymywać je oraz bronić Unii, w tym jej najbardziej

[33] Sprawozdanie z przeglądu konkretnych incydentów, sporządzone we współpracy z zainteresowanymi stronami, w tym z sektorem prywatnym, powinno służyć ocenie przyczyn i skutków incydentu po jego wystąpieniu oraz działań łagodzących te skutki. Szczególną uwagę należy zwrócić na spostrzeżenia i doświadczenia przekazywane przez dostawców usług zarządzanych w zakresie bezpieczeństwa, którzy spełniają warunki najwyższej uczciwości zawodowej, bezstronności i wymaganej fachowej wiedzy technicznej zgodnie z wymogami niniejszego rozporządzenia. Sprawozdanie należy dostarczyć EU-CyCLONe, sieci CSIRT i Komisji oraz powinno być ono użyte do wnoszenia wkładu w ich prace, a także w prace ENISA. W przypadku gdy incydent dotyczy państwa trzeciego stowarzyszonego z programem "Cyfrowa Europa", Komisja powinna udostępnić sprawozdanie także Wysokiemu Przedstawicielowi (motyw 50).

krytycznej infrastruktury, przed takimi atakami oraz zapewnić jej odporność. W tym celu należy zachęcać do współpracy zainteresowane strony, w tym z sektora prywatnego, środowiska akademickiego i sektora publicznego. Równie ważne jest tworzenie synergii na wszystkich terytoriach Unii w odniesieniu do inwestycji w kształcenie i szkolenie, aby promować tworzenie zabezpieczeń zapobiegających drenażowi mózgów lub powiększeniu luki kompetencyjnej w niektórych regionach bardziej niż w innych. Należy pilnie zlikwidować lukę kompetencyjną w zakresie cyberbezpieczeństwa, a w szczególności zmniejszyć dysproporcję kobiet i mężczyzn w zawodach związanych z cyberbezpieczeństwem, aby promować obecność i udział kobiet w projektowaniu administracji cyfrowej.

W rozporządzeniu 2025/38 stwierdzono, że uwzględnia ono zobowiązanie zapisane we wspólnej deklaracji Parlamentu Europejskiego, Rady i Komisji z dnia 26 stycznia 2022 r. zatytułowanej "Europejska deklaracja praw i zasad cyfrowych w cyfrowej dekadzie"[34] do ochrony interesów demokracji Unii, obywateli, przedsiębiorstw i instytucji publicznych przed ryzykiem w cyberprzestrzeni i cyberprzestępczością, w tym przed naruszaniem ochrony danych oraz kradzieżą tożsamości lub manipulowaniem tożsamością.

W rozporządzeniu 2025/38 uznano, że w celu uzupełnienia niektórych, innych niż istotne elementów zawartych w jego treści, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w celu określenia rodzajów i liczby służb reagowania wymaganych dla rezerwy cyberbezpieczeństwa UE. Za szczególnie ważne uznano, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa[35]. W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach

[34] Dz. U. UE. C. z 2023 r. Nr 23, str. 1. W motywach tej deklaracji wskazano m.in., że „unijna wizja transformacji cyfrowej jest ukierunkowana na człowieka, wzmacnia pozycję jednostek i wspiera innowacyjne przedsiębiorstwa. W decyzji w sprawie programu polityki "Droga ku cyfrowej dekadzie" do 2030 r. określono konkretne cele cyfrowe oparte na czterech głównych punktach (umiejętności cyfrowe, infrastruktury cyfrowe, cyfryzacja przedsiębiorstw i usług publicznych). Unijna droga do transformacji cyfrowej naszych społeczeństw i gospodarki obejmuje w szczególności otwartą suwerenność cyfrową, poszanowanie praw podstawowych, praworządności i demokracji, włączenie społeczne, dostępność, równość, zrównoważony rozwój, odporność, bezpieczeństwo, poprawę jakości życia, dostępność usług oraz poszanowanie praw i aspiracji wszystkich osób. Transformacja powinna przyczyniać się do rozwoju dynamicznej, zasobooszczędnej i sprawiedliwej gospodarki i społeczeństwa w UE”. Warto także zauważyć, że odwołano się w treści tego dokumentu do "Deklaracji z Tallina w sprawie administracji elektronicznej" oraz "Deklaracji berlińskiej w sprawie społeczeństwa cyfrowego i administracji cyfrowej opartej na wartościach". Przypomniano, że państw członkowskie UE zaapelowały w "Deklaracji lizbońskiej - celowa demokracja cyfrowa" o model transformacji cyfrowej, który wzmacnia ludzki wymiar ekosystemu cyfrowego, a podstawą tego modelu jest jednolity rynek cyfrowy. Zaapelowały również o model transformacji cyfrowej, który zapewni wykorzystanie technologii w obliczu potrzeby podjęcia działań w dziedzinie klimatu i ochrony środowiska.

[35] Dz. Urz. UE L 2026, Nr 123, s. 1.

grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

Wskazano także, że w celu zapewnienia jednolitych warunków wykonywania rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze na potrzeby doprecyzowania szczegółowych ustaleń dotyczących przyznawania usług wsparcia z rezerwy cyberbezpieczeństwa UE. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[36].

Omawiane rozporządzenie jest aktem nowym, który wejdzie w życie zgodnie z treścią jego art. 26 w dniu 6 lutego 2025 r. (20 dnia po opublikowaniu w Dzienniku Urzędowym UE, co nastąpiło 15 stycznia 2025 r.). Nie doczekał się on jak dotąd bardziej szczegółowych omówieni, a tym bardziej analiz w literaturze naukowej. Jego treść wydaje się niezwykle niepokojąca, gdyż dowodzi, iż państwa członkowskie Unii Europejskiej winny się liczyć w najbliższym czasie z incydentami, w tym także poważnymi i takimi, których skala jest duża. Obawiać się należy, że rozsądne rozwiązania, zawarte w treści tego aktu normatywnego, będą, jak to się często w prawie unijnym zdarza, wprowadzane z ociąganiem i z wątpliwościami zgłaszanymi przez niektóre państwa i środowiska. Konsekwencje takiej sytuacji i takich postaw mogą okazać się wręcz tragiczne.

Bibliografia

Burgoński P., Konferencja w sprawie przyszłości Europy wobec zmian polityki równościowej i antydyskryminacyjnej, „Rocznik Integracji Europejskiej" 2022, nr 16.

Sobczak J., Cyberprzestrzeń jako obszar ochrony bezpieczeństwa narodowego w optyce dokumentów europejskich, w: P. Herbowski, D. Słapczyńska, D. Jagiełło (red.), Pozyskiwanie informacji w walce z terroryzmem, Warszawa 2017.

Sobczak J., Sobczak W., Przestępczość w cyberprzestrzeni. Pomiędzy przepisami polskimi a międzynarodowymi, w: W. Kitler, K. Chałubińska-Jentkiewicz, K. Badzimirowska-Masłowska, System bezpieczeństwa w cyberprzestrzeni RP, Warszawa 2018.

Sobczak J., Kakareko K., Gołda-Sobczak M., Poszukiwanie unijnych standardów sztucznej inteligencji, „Cybersecurity and Law" 2023, nr 1 (9).

Sobczak J., „Biała księga w sprawie sztucznej inteligencji" w systemie polityczno-prawnym Unii Europejskiej, w: R. Grabowski (red.) XXV lat Konstytucji Rzeczypospolitej Polskiej. Księga jubileuszowa dedykowana Profesor Halinie Ziębie-Załuckiej z okazji 70. Rocznicy urodzin, Toruń 2022.

[36] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz. Urz. UE L 2011, Nr 55, s. 13).

CYBERSOLIDARITY ACT
EU RESPONSE TO CYBER THREATS AND CYBER SECURITY INCIDENTS

Abstract

In April 2023. the European Commission proposed a regulation to enhance solidarity and capabilities within the Union to detect, prepare for and respond to cyber security threats and incidents (the Cybersolidarity Act). The military action conducted in Europe has revealed the scale of the state's dependence on digital technology and the instability of the digital space. It has triggered a surge in cyber attacks, which are particularly destructive when targeting critical infrastructure - such as energy, health or finance - that is increasingly dependent on technology, making it more efficient but also more vulnerable to cyber disruption. In this context, the Commission has proposed a Cybersolidarity Act Regulation to respond to the urgent need to enhance solidarity and capabilities within the Union to detect, prepare for and respond to cyber security threats and incidents.

Keywords: cyber security, solidarity, cyber attacks, cyber threats, incidents, critical infrastructure.