ZALECENIA

ZALECENIE KOMISJI (UE) 2017/1584

z dnia 13 września 2017 r.

w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę

KOMISJA EUROPEJSKA,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 292,

a także mając na uwadze, co następuje:

(1) Wykorzystanie technologii informacyjno-komunikacyjnych i uzależnienie od nich zyskały podstawowe znaczenie we wszystkich sektorach działalności gospodarczej, gdyż przedsiębiorstwa i obywatele są wzajemnie bardziej powiązani i uzależnieni w wymiarze międzysektorowym i transgranicznym niż kiedykolwiek wcześniej. Incydent cybernetyczny mający negatywne skutki dla organizacji w więcej niż jednym państwie członkowskim, a nawet dla całej Unii, i mogący spowodować poważne zakłócenia w funkcjonowaniu rynku wewnętrznego oraz – w szerszym wymiarze – w funkcjonowaniu sieci i systemów informatycznych mających zasadnicze znaczenie dla gospodarki, demokracji i społeczeństwa, to scenariusz, na który państwa członkowskie i instytucje UE muszą być dobrze przygotowane.

(2) Incydent cybernetyczny może zostać uznany za sytuację kryzysową na szczeblu Unii, jeżeli wywołane nim zakłócenia mają zbyt duży zakres, by państwo członkowskie, w którym doszło do tego incydentu, poradziło sobie z nim w pojedynkę, albo jeżeli dla dwóch lub większej liczby państw członkowskich ma on skutki o tak szerokim zakresie i o tak dużym znaczeniu technicznym lub politycznym, że wymaga on szybkiej koordynacji i reakcji na szczeblu politycznym Unii.

(3) Incydenty cybernetyczne mogą doprowadzić do kryzysu na szerszą skalę, odbijającego się negatywnie na sektorach działalności niezwiązanych z siecią i systemami informatycznymi ani z sieciami łączności; każda właściwa reakcja musi opierać się na ograniczających zagrożenie działaniach zarówno w domenie cyfrowej, jak i poza nią.

(4) Incydenty cybernetyczne są nieprzewidywalne, często pojawiają się i rozwijają w bardzo krótkim czasie, w związku z tym dotknięte ich skutkami podmioty i jednostki odpowiadające za reagowanie na incydenty i ograniczanie ich skutków muszą koordynować swoje działania w trybie pilnym. Ponadto incydenty cybernetyczne często nie są ograniczone do konkretnego obszaru geograficznego i mogą występować jednocześnie lub rozprzestrzeniać się błyskawicznie w wielu państwach.

(5) Skuteczne reagowanie na szczeblu UE na incydenty i kryzysy cybernetyczne na dużą skalę wymaga szybkiej i skutecznej współpracy między wszystkimi odpowiednimi zainteresowanymi stronami, a podstawowym warunkiem skutecznej reakcji jest gotowość i zdolności poszczególnych państw członkowskich do podejmowania określonych działań, a także skoordynowane wspólne działanie wspierane zdolnościami na szczeblu unijnym. Szybkie i skuteczne reagowanie na incydenty uzależnione jest więc od istnienia wcześniej ustanowionych i, w miarę możliwości, dobrze przećwiczonych procedur i mechanizmów współpracy, w których kluczowe podmioty na szczeblu krajowym i unijnym mają jasno określone role i obowiązki.

(6) W konkluzjach ([1]) w sprawie ochrony krytycznej infrastruktury teleinformatycznej z dnia 27 maja 2011 r. Rada wezwała państwa członkowskie UE, aby wzmocniły wzajemną współpracę „i przyczyniły się, na podstawie doświadczeń i wyników krajowych w zakresie zarządzania kryzysowego oraz we współpracy z ENISA, do opracowania europejskich mechanizmów współpracy na wypadek incydentu cybernetycznego, które zostaną przetestowane w ramach następnego ćwiczenia *Cyber Europe* w 2012 roku".

(7) W komunikacie z 2016 r. „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego" ([2]) zachęcono państwa członkowskie do maksymalnego wykorzystania mechanizmów współpracy ustanowionych dyrektywą w sprawie bezpieczeństwa sieci i informacji ([3]) oraz do zacieśnienia współpracy transgranicznej związanej z gotowością na

([1]) Konkluzje Rady w sprawie ochrony krytycznej infrastruktury teleinformatycznej „Osiągnięcia i dalsze działania na rzecz globalnego bezpieczeństwa cyberprzestrzeni", dokument 10299/11, Bruksela, 27 maja 2011 r.
([2]) COM(2016) 410 final z dnia 5 lipca 2016 r.
([3]) 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)..

wypadek incydentu cybernetycznego na dużą skalę. Dodano w nim, że skoordynowane podejście do współpracy w sytuacjach kryzysowych pomiędzy różnymi elementami ekosystemu cybernetycznego, które należałoby określić w planie działania, zwiększyłoby stopień gotowości, a taki plan działania powinien również zapewniać synergię i spójność z istniejącymi mechanizmami zarządzania kryzysowego.

(8) W konkluzjach Rady ([1]) dotyczących wspomnianego wyżej komunikatu państwa członkowskie wezwały Komisję do przedłożenia takiego planu (projektu) współpracy do rozważenia przez podmioty działające na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji i inne zainteresowane strony. We wspomnianej dyrektywie nie określono jednak ram współpracy unijnej w przypadku incydentów i kryzysów cybernetycznych na dużą skalę.

(9) Komisja zasięgnęła opinii państw członkowskich w ramach dwóch odrębnych warsztatów konsultacyjnych, które odbyły się w dniach 5 kwietnia i 4 lipca 2017 r. w Brukseli z udziałem przedstawicieli zespołów reagowania na incydenty komputerowe (CSIRT) z państw członkowskich, grupy współpracy powołanej dyrektywą w sprawie bezpieczeństwa sieci i informacji oraz działającej w Radzie Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni, jak również przedstawicieli Europejskiej Służby Działań Zewnętrznych (ESDZ), ENISA, działu EC3 w Europolu i Sekretariatu Generalnego Rady (SGR).

(10) Obecny plan działania na rzecz skoordynowanego reagowania na szczeblu unijnym na incydenty i kryzysy cybernetyczne na dużą skalę, załączony do niniejszego zalecenia, jest rezultatem wspomnianych konsultacji i stanowi uzupełnienie komunikatu „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego".

(11) W planie tym określono i opisano cele i tryby współpracy między państwami członkowskimi UE a unijnymi instytucjami, organami, jednostkami organizacyjnymi i agencjami (zwanymi dalej „instytucjami unijnymi") przy reagowaniu na incydenty i kryzysy cybernetyczne na dużą skalę, a także sposoby pełnego wykorzystania w istniejących mechanizmach zarządzania kryzysowego istniejących podmiotów odpowiedzialnych za bezpieczeństwo cybernetyczne na szczeblu unijnym.

(12) W przypadku kryzysu cybernetycznego w rozumieniu motywu 2 koordynacja reakcji na szczeblu politycznym Unii w Radzie oparta zostanie na zintegrowanych uzgodnieniach UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych ([2]) (ang. *Integrated Political Crisis Response*, IPCR); Komisja będzie korzystać z mechanizmu ARGUS ([3]) służącego do koordynacji działań na wysokim szczeblu w przypadku kryzysów międzysektorowych. Jeżeli sytuacja kryzysowa wiąże się z istotnymi kwestiami z zakresu polityki zewnętrznej lub wspólnej polityki bezpieczeństwa i obrony (WPBiO), uruchomiony zostanie mechanizm reagowania kryzysowego (ang. *Crisis Response Mechanism*, CRM) ([3]) Europejskiej Służby Działań Zewnętrznych (ESDZ).

(13) W pewnych obszarach w sektorowych mechanizmach zarządzania kryzysowego na szczeblu UE przewidziano współpracę w przypadku incydentów lub kryzysów cybernetycznych. Na przykład w ramach Europejskiego Globalnego Systemu Nawigacji Satelitarnej (GNSS) w decyzji Rady 2014/496/WPZiB ([4]) określono już role przydzielone Radzie, Wysokiemu Przedstawicielowi, Komisji, Agencji Europejskiego GNSS i państwom członkowskim w łańcuchu odpowiedzialności operacyjnej ustanowionym na potrzeby reagowania na zagrożenia dla Unii, państw członkowskich lub GNSS, w tym zagrożenie stwarzane przez ataki cybernetyczne. W związku z tym niniejsze zalecenie nie powinno naruszać funkcjonowania takich mechanizmów.

(14) Odpowiedzialność za reagowanie na incydenty lub kryzysy cybernetyczne na dużą skalę spoczywa w pierwszej kolejności na państwach członkowskich nimi dotkniętych. Komisja, Wysoki Przedstawiciel i inne instytucje lub służby unijne odgrywają jednak ważną rolę, wynikającą z prawa Unii lub z faktu, że incydenty i kryzysy cybernetyczne mogą mieć negatywne skutki dla wszystkich sektorów działalności gospodarczej w ramach jednolitego rynku, dla bezpieczeństwa i stosunków międzynarodowych Unii, a także dla samych instytucji.

(15) Na szczeblu UE do głównych podmiotów zaangażowanych w reagowanie na kryzysy cybernetyczne należą nowe struktury i mechanizmy ustanowione na podstawie dyrektywy w sprawie bezpieczeństwa sieci i informacji, a mianowicie sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) oraz stosowne agencje i jednostki organizacyjne, tj. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Europejskie Centrum ds. Walki z Cyberprzestępczością w Europolu (Europol/EC3), Centrum Analiz Wywiadowczych UE (INTCEN), Dyrekcja ds. Wywiadu w Sztabie Wojskowym UE (EUMS INT) oraz Centrum Sytuacyjne (SITROOM), działające wspólnie jako SIAC (pojedyncza komórka analiz wywiadowczych), a ponadto komórka UE ds. syntezy informacji o zagrożeniach hybrydowych (działająca przy INTCEN), zespół reagowania na incydenty komputerowe w instytucjach i agencjach UE (CERT-UE) oraz Centrum Koordynacji Reagowania Kryzysowego działające w Komisji Europejskiej.

(16) Współpraca państw członkowskich w zakresie reagowania na incydenty cybernetyczne na poziomie technicznym prowadzona jest za pośrednictwem sieci CSIRT ustanowionej dyrektywą w sprawie bezpieczeństwa sieci

([1]) Dokument 14540/16 z dnia 15 listopada 2016 r.
([2]) Więcej informacji na ten temat podano w sekcji 3.1 dodatku dotyczącego zarządzania kryzysowego, mechanizmów współpracy i podmiotów na szczeblu UE.
([3]) *Ibidem*.
([4]) Decyzja Rady 2014/496/WPZiB z dnia 22 lipca 2014 r. w sprawie aspektów wdrażania, działania i użytkowania europejskiego globalnego systemu nawigacji satelitarnej mających wpływ na bezpieczeństwo Unii Europejskiej (Dz.U. L 219 z 25.7.2014, s. 53).

i informacji. ENISA zapewnia tej sieci obsługę sekretariatu i aktywnie wspiera współpracę między poszczególnymi zespołami CSIRT. Krajowe CSIRT oraz CERT-UE podejmują współpracę i wymieniają się informacjami na zasadzie dobrowolności, w tym, w razie potrzeby, przy reagowaniu na incydenty cybernetyczne mające negatywne skutki dla jednego państwa członkowskiego lub większej ich liczby. Na wniosek przedstawiciela CSIRT jednego z państw członkowskich mogą one omówić oraz, w miarę możliwości, ustalić sposób skoordynowanej reakcji na incydent, który wykryto na obszarze jurysdykcji tego państwa członkowskiego. Odnośne procedury zostaną określone w standardowych procedurach operacyjnych (SOP) ([1]) sieci CSIRT.

(17) Do zadań sieci CSIRT należy również omawianie, analizowanie i określanie dalszych form współpracy operacyjnej, w tym kwestii związanych z kategoriami zagrożeń i incydentów, wczesnym ostrzeganiem, wzajemną pomocą oraz zasadami i trybami koordynacji, w przypadku gdy państwa członkowskie podejmują działania w reakcji na transgraniczne zagrożenia i incydenty.

(18) Zadaniem grupy współpracy, powołanej na mocy art. 11 dyrektywy w sprawie bezpieczeństwa sieci i informacji, jest udzielanie strategicznych wskazówek dotyczących działalności sieci CSIRT oraz omawianie zdolności i gotowości państw członkowskich, a także, na zasadzie dobrowolności, ocena krajowych strategii w zakresie bezpieczeństwa sieci i systemów informatycznych oraz skuteczności CSIRT oraz wskazywanie najlepszych praktyk.

(19) Osobnym obszarem prac prowadzonych przez grupę współpracy są wytyczne w zakresie zgłaszania incydentów, zgodnie z art. 14 ust. 7 dyrektywy w sprawie bezpieczeństwa sieci i informacji, dotyczące okoliczności, w których operatorzy usług kluczowych są zobowiązani do zgłaszania incydentów zgodnie z art. 14 ust. 3, oraz formatu i procedury takich zgłoszeń ([2]).

(20) Orientowanie się w czasie rzeczywistym w sytuacji, podejmowanym ryzyku i w zagrożeniach oraz ich zrozumienie, uzyskane dzięki zgłoszeniom, ocenom, badaniom, dochodzeniom i analizom, jest niezbędne do podejmowania świadomych decyzji. Taka orientacja sytuacyjna – u wszystkich zainteresowanych stron – ma kluczowe znaczenie w zapewnianiu skutecznej i skoordynowanej reakcji. Orientacja sytuacyjna obejmuje informacje zarówno o przyczynach, jak i skutkach oraz źródle incydentu. Powszechnie przyjmuje się, że taką orientację można osiągnąć tylko w drodze wymiany i udostępniania przez zainteresowane strony informacji w odpowiednim formacie, przy użyciu wspólnej taksonomii do opisu incydentu oraz w sposób zapewniający odpowiedni poziom bezpieczeństwa.

(21) Reagowanie na incydenty cybernetyczne może przybierać różne formy, począwszy od określenia środków technicznych, mogących polegać na wspólnej analizie technicznych przyczyn incydentu (np. analizie złośliwego oprogramowania) przez dwa podmioty lub większą ich liczbę, lub określenia sposobów, za pomocą których organizacje mogą sprawdzić, czy padły ofiarami incydentu (np. oznaki naruszenia integralności systemu), po decyzje operacyjne dotyczące stosowania takich środków oraz – na szczeblu politycznym – decyzje o wykorzystaniu innych instrumentów, takich jak ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne ([3]) lub unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym ([4]), w zależności od charakteru incydentu.

(22) Zaufanie europejskich obywateli i przedsiębiorstw do usług cyfrowych ma kluczowe znaczenie dla dynamicznie rozwijającego się jednolitego rynku cyfrowego. W związku z tym komunikacja podczas sytuacji kryzysowej odgrywa szczególnie ważną rolę w ograniczaniu negatywnych skutków incydentów i kryzysów cybernetycznych. Komunikację można również wykorzystać w ramach wspólnej reakcji dyplomatycznej jako środek wpływania na zachowania (potencjalnych) sprawców działających z terytorium państw trzecich. Uspójnienie informacji publikowanych w celu ograniczenia negatywnych skutków incydentów i kryzysów cybernetycznych z informacjami publikowanymi w celu wywierania wpływu na sprawców ma zasadnicze znaczenie dla zapewnienia skuteczności reakcji politycznej.

(23) Informowanie obywateli o tym, w jaki sposób mogą ograniczyć negatywne skutki danego incydentu na poziomie indywidualnego użytkownika bądź organizacji (na przykład poprzez aktualizację oprogramowania lub podjęcie działań uzupełniających w celu uniknięcia zagrożenia) może być skutecznym środkiem ograniczania szkodliwości incydentu lub kryzysu cybernetycznego na dużą skalę.

(24) Komisja, korzystając z infrastruktury usług cyfrowych w zakresie bezpieczeństwa cybernetycznego w ramach instrumentu „Łącząc Europę", tworzy mechanizm w postaci platformy usług podstawowych, którą nazwano MeliCERTes, służący współpracy między CSIRT uczestniczących państw członkowskich, w celu poprawy poziomu ich gotowości, udoskonalenia ich współdziałania i reakcji na pojawiające się zagrożenia i incydenty cybernetyczne. Komisja, w drodze konkurencyjnych zaproszeń do składania wniosków o przyznanie dotacji ze środków instrumentu „Łącząc Europę", współfinansuje CSIRT w państwach członkowskich, aby zwiększyć ich zdolności operacyjne na szczeblu krajowym.

([1]) W opracowaniu; oczekuje się, że zostaną przyjęte do końca 2017 r.
([2]) Wytyczne te mają zostać opracowane do końca 2017 r.
([3]) Konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej"), dokument 9916/17.
([4]) Wspólny dokument roboczy służb „Unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym" („Unijny podręcznik taktyczny"), SWD(2016) 227 final z dnia 5 lipca 2016 r.

(25) Ćwiczenia w dziedzinie bezpieczeństwa cybernetycznego na szczeblu UE są niezbędne do stymulowania i poprawy współpracy między państwami członkowskimi a sektorem prywatnym. W tym celu od 2010 r. ENISA organizuje regularnie ćwiczenia w zakresie incydentów cybernetycznych na skalę ogólnoeuropejską („Cyber Europe").

(26) W konkluzjach Rady ([1]) w sprawie realizacji wspólnej deklaracji przewodniczącego Rady Europejskiej, przewodniczącego Komisji Europejskiej i Sekretarza Generalnego Organizacji Traktatu Północnoatlantyckiego zaapelowano o wzmocnienie współpracy w zakresie ćwiczeń w dziedzinie bezpieczeństwa cybernetycznego poprzez wzajemny udział pracowników w odpowiednich ćwiczeniach, w tym w szczególności ćwiczeniach „Cyber Coalition" oraz „Cyber Europe".

(27) Stale zmieniający się obraz zagrożeń i niedawne incydenty cybernetyczne są oznaką rosnącego ryzyka, na jakie narażona jest Unia, państwa członkowskie powinny zatem bez dalszych opóźnień, a w każdym razie przed końcem 2018 r., podjąć działania w oparciu o niniejsze zalecenie,

PRZYJMUJE NINIEJSZE ZALECENIE:

1. Państwa członkowskie i instytucje unijne powinny ustanowić unijne ramy reagowania w sytuacji kryzysu cybernetycznego, obejmujące cele i tryby współpracy przedstawione w planie działania, z uwzględnieniem określonych w nim zasad przewodnich.

2. W unijnych ramach reagowania w sytuacji kryzysu cybernetycznego należy w szczególności określić właściwe podmioty, instytucje unijne i organy państw członkowskich, na wszystkich niezbędnych poziomach – technicznym, operacyjnym, strategicznym/politycznym – oraz opracować, w stosownych przypadkach, standardowe procedury operacyjne zawierające opis trybu współpracy tych podmiotów w ramach unijnych mechanizmów zarządzania kryzysowego. Należy położyć nacisk na umożliwienie wymiany informacji bez zbędnej zwłoki i koordynowanie reakcji w obliczu incydentów i kryzysów cybernetycznych na dużą skalę.

3. W tym celu właściwe organy państw członkowskich powinny wspólnie wypracować dalsze szczegóły protokołów wymiany informacji i współpracy. Grupa współpracy powinna dzielić się doświadczeniami w tych kwestiach z odpowiednimi instytucjami unijnymi.

4. Państwa członkowskie powinny zapewnić, by ich krajowe mechanizmy zarządzania kryzysowego umożliwiały adekwatną reakcję na incydent cybernetyczny, jak również by określono w nich procedury konieczne do umożliwienia współpracy na szczeblu UE w oparciu o ramy unijne.

5. W odniesieniu do istniejących unijnych mechanizmów zarządzania kryzysowego, zgodnie z planem działania, państwa członkowskie, wraz ze służbami Komisji i ESDZ, powinny określić praktyczne wytyczne wdrożeniowe, dotyczące zintegrowania krajowych podmiotów i procedur zarządzania kryzysowego i bezpieczeństwa cybernetycznego z istniejącymi unijnymi mechanizmami zarządzania kryzysowego, a mianowicie IPCR i mechanizmem reagowania kryzysowego ESDZ. Państwa członkowskie powinny w szczególności zapewnić utworzenie odpowiednich struktur umożliwiających skuteczny przepływ informacji między swoimi krajowymi organami zarządzania kryzysowego a swoimi przedstawicielami na szczeblu UE, zaangażowanymi w funkcjonowanie unijnych mechanizmów kryzysowych.

6. Państwa członkowskie powinny w pełni wykorzystywać możliwości, jakie oferuje program infrastruktury usług cyfrowych (DSI) w zakresie bezpieczeństwa cybernetycznego w ramach instrumentu „Łącząc Europę", a także współpracować z Komisją w celu zapewnienia, by mechanizm współpracy w postaci platformy usług podstawowych, obecnie w opracowaniu, zapewniał niezbędne funkcje i spełniał wymogi w zakresie współpracy, również podczas kryzysów cybernetycznych.

7. Państwa członkowskie – przy wsparciu ENISA, a także w oparciu o wcześniejsze prace w tej dziedzinie – powinny współpracować przy opracowywaniu i przyjmowaniu wspólnej taksonomii i wzoru raportów sytuacyjnych na potrzeby opisu technicznych przyczyn i skutków incydentów cybernetycznych, aby dalej zacieśniać swoją współpracę techniczną i operacyjną w sytuacjach kryzysowych. Państwa członkowskie powinny zatem uwzględnić prowadzone przez grupę współpracy bieżące prace nad wytycznymi w zakresie zgłaszania incydentów, a w szczególności aspekty dotyczące formatów zgłoszeń krajowych.

8. Procedury określone we wspomnianych ramach powinny być testowane i w razie konieczności zmieniane w następstwie nowych doświadczeń zdobywanych przez państwa członkowskie w wyniku ich uczestnictwa w krajowych, regionalnych i unijnych inicjatywach, jak również ćwiczeniach z zakresu dyplomacji cyfrowej oraz ćwiczeniach NATO w dziedzinie bezpieczeństwa cybernetycznego. W szczególności procedury te powinny być przedmiotem testów w kontekście ćwiczeń „Cyber Europe" organizowanych przez ENISA. Ćwiczenia „Cyber Europe" 2018 będą stanowić pierwszą tego rodzaju okazję.

([1]) Dokument 15283/16 z dnia 6 grudnia 2016 r.

9. Państwa członkowskie i instytucje unijne powinny regularnie ćwiczyć w skali krajowej i ogólnoeuropejskiej swoją reakcję na incydenty i kryzysy cybernetyczne na dużą skalę, w tym, w razie potrzeby, swoją odpowiedź polityczną, również przy zaangażowaniu, w stosownych przypadkach, podmiotów z sektora prywatnego.

Sporządzono w Brukseli dnia 13 września 2017 r.

W imieniu Komisji

Mariya GABRIEL

Członek Komisji

ZAŁĄCZNIK

Plan skoordynowanego reagowania na wypadek wystąpienia transgranicznych incydentów cybernetycznych na dużą skalę i kryzysów cybernetycznych

WPROWADZENIE

Niniejszy plan ma zastosowanie w przypadku wystąpienia incydentów cybernetycznych, które powodują zakłócenia na skalę zbyt szeroką, aby dotknięte nimi państwo członkowskie zdołało się z nimi samodzielnie uporać, lub które dotykają co najmniej dwóch państw członkowskich bądź instytucji unijnych i mają tak szeroko zakrojony i znaczący wpływ o charakterze technicznym bądź politycznym, że wymagają terminowej koordynacji działań i reakcji na unijnym poziomie politycznym.

Incydenty cybernetyczne na tak dużą skalę uważa się za „kryzysy cybernetyczne".

W przypadku ogólnounijnej sytuacji kryzysowej z elementami zagrożenia cybernetycznego koordynacją reakcji na unijnym poziomie politycznym zajmuje się Rada, która korzysta ze zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR).

W obrębie Komisji koordynacja przebiega zgodnie z systemem wczesnego ostrzegania ARGUS.

Jeżeli sytuacja kryzysowa obejmuje istotny wymiar polityki zewnętrznej lub wspólnej polityki bezpieczeństwa i obrony, uruchamia się mechanizm reagowania kryzysowego ESDZ.

W niniejszym planie opisano, w jaki sposób należy w pełni wykorzystać te ugruntowane mechanizmy zarządzania kryzysowego w ramach istniejących jednostek zajmujących się bezpieczeństwem cybernetycznym na szczeblu unijnym i mechanizmy współpracy między państwami członkowskimi.

W ten sposób w planie działania uwzględniono szereg zasad przewodnich (zasady: proporcjonalności, pomocniczości, komplementarności i poufności informacji), przedstawiono zasadnicze cele współpracy (skuteczne reagowanie, wspólna orientacja sytuacyjna, informowanie społeczeństwa) na trzech poziomach (strategicznym i politycznym, operacyjnym i technicznym), mechanizmy i zaangażowane podmioty oraz działania niezbędne do osiągnięcia wspomnianych celów zasadniczych.

W projekcie nie uwzględniono w pełni pełnego cyklu zarządzania kryzysowego (zapobieganie/ograniczanie skutków, przygotowanie, reagowanie, odbudowa), lecz skupiono się na reagowaniu. Niektóre działania, zwłaszcza związane z uzyskaniem wspólnej orientacji sytuacyjnej, zostały jednak wzięte pod uwagę.

Należy również zauważyć, że incydenty cybernetyczne mogą być źródłem lub częścią większych kryzysów, uderzających w inne sektory. Z uwagi na fakt, iż można się spodziewać, że skutki większości kryzysów cybernetycznych objawią się w świecie fizycznym, każde właściwe reagowanie musi być oparte na działaniach ograniczających skutki w sferze cybernetycznej i niecybernetycznej. Działania w odpowiedzi na kryzys cybernetyczny należy koordynować z innymi mechanizmami zarządzania kryzysowego na szczeblu unijnym, krajowym lub sektorowym.

Plan działania nie zastępuje też i nie powinien naruszać istniejących mechanizmów sektorowych lub mechanizmów, ustaleń bądź instrumentów związanych z określonymi obszarami polityki, takimi jak ustanowione w odniesieniu do programu Europejskiego Globalnego Systemu Nawigacji Satelitarnej (GNSS) ([1]).

Zasady przewodnie

W pracy na rzecz osiągnięcia celów, określaniu niezbędnych działań i przypisywaniu ról oraz zakresu odpowiedzialności odnośnym podmiotom lub mechanizmom zastosowano następujące zasady przewodnie, których należy zatem przestrzegać przy przygotowywaniu przyszłych wytycznych wykonawczych.

Proporcjonalność: Przeważająca większość incydentów cybernetycznych uderzających w państwa członkowskie mieści się w kategorii znacznie niższej niż wszystko, co mogłoby zostać uznane za kryzys na szczeblu krajowym, nie mówiąc już o szczeblu europejskim. Podstawą współpracy państw członkowskich w odpowiedzi na tego rodzaju incydenty jest sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) ustanowiona dyrektywą w sprawie bezpieczeństwa sieci i informacji ([2]). Krajowe zespoły współpracują i wymieniają się informacjami na zasadzie dobrowolności i codziennie, w razie potrzeby, reagując na incydenty cybernetyczne, które uderzają w co najmniej jedno państwo członkowskie, zgodnie ze standardowymi procedurami operacyjnymi (SPO) sieci CSIRT. Dlatego w planie należy w pełni wykorzystywać te standardowe procedury i uwzględnić w nim wszelkie dodatkowe konkretne działania odnoszące się do kryzysu cybernetycznego.

([1]) Decyzja 2014/496/WPZiB.
([2]) Dyrektywa (UE) 2016/1148.

Pomocniczość: Zasada pomocniczości ma kluczowe znaczenie. Na państwach członkowskich spoczywa główna odpowiedzialność za reagowanie w przypadku uderzających w nie incydentów cybernetycznych na dużą skalę bądź kryzysów cybernetycznych. Komisja, Europejska Służba Działań Zewnętrznych i inne unijne instytucje, urzędy, agencje oraz organy mają jednak do odegrania ważną rolę. Rola ta jest jasno określona w ramach zintegrowanych uzgodnień UE dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR), ale wynika również z przepisów prawa unijnego bądź po prostu z faktu, że incydenty i kryzysy cybernetyczne mogą mieć wpływ na wszystkie obszary działalności w obrębie jednolitego rynku, bezpieczeństwa i stosunków międzynarodowych Unii oraz samych instytucji.

Komplementarność: W planie działania w pełni uwzględniono istniejące mechanizmy zarządzania kryzysowego na szczeblu unijnym, a mianowicie zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR), system ARGUS, mechanizm reagowania kryzysowego ESDZ, włączono do niego nowe struktury i mechanizmy ustanowione dyrektywą w sprawie bezpieczeństwa sieci i informacji (dyrektywą NIS), a mianowicie sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT), a także stosowne agencje i jednostki organizacyjne, tj. Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), Europejskie Centrum ds. Walki z Cyberprzestępczością w Europolu (Europol/EC3), Centrum Analiz Wywiadowczych UE (INTCEN), Dyrekcję ds. Wywiadu w Sztabie Wojskowym UE (EUMS INT) oraz Centrum Sytuacyjne (SITROOM) w INTCEN, działające wspólnie jako SIAC (pojedyncza komórka analiz wywiadowczych); komórkę UE ds. syntezy informacji o zagrożeniach hybrydowych (działającą przy INTCEN); oraz zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE). Dzięki temu plan powinien również zapewnić, aby ich współdziałanie i współpraca osiągnęły maksymalny poziom komplementarności i możliwie najmniejsze nakładanie się działań.

Poufność informacji: Wszelka wymiana informacji w ramach planu działania musi być zgodna z obowiązującymi zasadami bezpieczeństwa ([1]), ochrony danych osobowych i kodu poufności TLP ([2]). Przy wymianie informacji niejawnych, niezależnie od zastosowanego systemu klasyfikacji, należy korzystać z dostępnych akredytowanych narzędzi ([3]). W odniesieniu do przetwarzania danych osobowych przestrzegane będą mające zastosowanie przepisy unijne, w szczególności ogólne rozporządzenie o ochronie danych ([4]), dyrektywa o prywatności i łączności elektronicznej ([5]) oraz rozporządzenie ([6])„w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy, biura i agencje unijne i swobodnego przepływu tych danych".

Zasadnicze cele

Współpraca w ramach planu przebiega z uwzględnieniem trzech wspomnianych wyżej poziomów – politycznego, operacyjnego i technicznego. Na każdym z nich współpraca może obejmować zarówno wymianę informacji, jak też wspólne działania, a celem jej jest osiągnięcie poniższych celów zasadniczych.

— Umożliwienie skutecznego reagowania: Reagowanie może przybierać różne formy, od wskazania środków technicznych, które mogą dotyczyć co najmniej dwóch jednostek wspólnie badających techniczne przyczyny incydentu (np. analiza złośliwego oprogramowania), lub określenia sposobów, w jaki te organizacje mogą ocenić, czy zostały poszkodowane (np. oznaki naruszenia integralności systemu), do decyzji operacyjnych o zastosowaniu takich środków technicznych oraz – na poziomie politycznym – zadecydowania o uruchomieniu innych instrumentów, takich jak unijne działania dyplomatyczne w odpowiedzi na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej") bądź unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym – w zależności od incydentu.

— Wspólna orientacja sytuacyjna: Dostatecznie dobre rozumienie wydarzeń w miarę ich rozwoju przez wszystkie odnośne zainteresowane strony na wszystkich trzech poziomach (technicznym, operacyjnym, politycznym) ma decydujące znaczenie dla skoordynowanego reagowania. Orientacja sytuacyjna może obejmować elementy technologiczne dotyczące przyczyn, a także skutki i źródła incydentu. Ponieważ incydenty cybernetyczne mogą uderzać w różne sektory (finanse, transport, energia, ochrona zdrowia itp.), konieczne jest, aby stosowne informacje w odpowiednim formacie na czas docierały do wszystkich odnośnych zainteresowanych stron.

([1]) Decyzja Komisji (UE, Euratom) 2015/443 z dnia 13 marca 2015 r. w sprawie bezpieczeństwa w Komisji (Dz.U. L 72 z 17.3.2015, s. 41) oraz decyzja Komisji (UE, Euratom) 2015/444 z dnia 13 marca 2015 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 72 z 17.3.2015, s. 53); decyzja Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa z dnia 19 kwietnia 2013 r. w sprawie przepisów bezpieczeństwa mających zastosowanie do Europejskiej Służby Działań Zewnętrznych; decyzja Rady 2013/488/UE z dnia 23 września 2013 r. w sprawie przepisów bezpieczeństwa dotyczących ochrony informacji niejawnych UE (Dz.U. L 274 z 15.10.2013, s. 1).

([2]) https://www.first.org/tlp/

([3]) W czerwcu 2016 r. te kanały przekazywania informacji obejmowały system zarządzania informacjami niejawnymi (CIMS), algorytm kodowania ACID, bezpieczny system RUE do wytwarzania, wymiany i przechowywania dokumentów unijnych opatrzonych klauzulami niejawności oraz SOLAN. Inne sposoby przesyłania np. informacji niejawnych obejmują PGP i S/MIME.

([4]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 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).

([5]) Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.U. L 201 z 31.7.2002, s. 37).

([6]) Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.U. L 8 z 12.1.2001, s. 1) – w trakcie przeglądu.

— Zgoda co do kluczowych publicznych działań komunikacyjnych ([1]): Komunikacja w sytuacji kryzysowej odgrywa istotna rolę w ograniczaniu negatywnych skutków incydentów i kryzysów cybernetycznych, może być też jednak stosowana jako środek wywierania wpływu na zachowanie (potencjalnych) agresorów. Odpowiedni przekaz może też służyć do jasnego zasygnalizowania prawdopodobnych konsekwencji reakcji dyplomatycznej w celu wywarcia wpływu na zachowanie agresora. Dostosowanie publicznych działań komunikacyjnych, mających na celu ograniczanie negatywnych skutków incydentów, i kryzysów cybernetycznych oraz przekazów, służących do wywierania wpływu na agresora, ma zasadnicze znaczenie dla skuteczności reagowania politycznego. W obszarze bezpieczeństwa cybernetycznego szczególnie istotne jest rozpowszechnianie dokładnych możliwych do zastosowania informacji o tym, w jaki sposób społeczeństwo może ograniczać skutki incydentu (np. przez zastosowanie poprawki zabezpieczeń, podejmowanie działań uzupełniających w celu uniknięcia zagrożenia itp.).

WSPÓŁPRACA MIĘDZY PAŃSTWAMI CZŁONKOWSKIMI ORAZ MIĘDZY PAŃSTWAMI CZŁONKOWSKIMI A PODMIOTAMI UNIJNYMI NA POZIOMIE TECHNICZNYM, OPERACYJNYM I STRATEGICZNO-POLITYCZNYM

Skuteczne reagowanie na szczeblu unijnym na incydenty cybernetyczne na dużą skalę lub kryzysy cybernetyczne polega na skutecznej współpracy technicznej, operacyjnej i strategiczno-politycznej.

Na każdym poziomie zaangażowane podmioty powinny wykonywać określone działania na rzecz osiągnięcia trzech zasadniczych celów, którymi są:

— skoordynowana reakcja,

— wspólna orientacja sytuacyjna,

— publiczne działania komunikacyjne.

Podczas trwania incydentu lub kryzysu jednostki na niższym poziomie współpracy ostrzegają, informują i wspierają jednostki na poziomie wyższym; te z kolei zapewnią niższym poziomom wytyczne ([2]) i decyzje, w zależności od potrzeb.

Współpraca na poziomie technicznym

Zakres działań:

— postępowanie w odniesieniu do incydentu ([3]) podczas kryzysu cybernetycznego;

— monitorowanie incydentu i nadzór łącznie z ciągłą analizą zagrożeń i ryzyka.

Potencjalne zaangażowane podmioty

Na poziomie technicznym centralnym mechanizmem współpracy w ramach planu działania jest sieć CSIRT, której przewodniczy prezydencja i której sekretariat zapewnia ENISA.

— Państwa członkowskie:

  — właściwe organy i pojedyncze punkty kontaktowe powołane zgodnie z dyrektywą w sprawie bezpieczeństwa sieci i systemów informatycznych,

  — zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT).

— Organy/urzędy/agencje UE:

  — ENISA,

  — Europol/EC3,

  — CERT-UE.

([1]) Należy w tym miejscu zauważyć, że publiczne działania komunikacyjne mogą dotyczyć zarówno informacji o incydencie adresowanych do społeczeństwa jako całości, jak również przekazów, zawierających informacje o bardziej technicznym bądź operacyjnym charakterze, adresowanych do sektorów o krytycznym znaczeniu lub sektorów zaatakowanych. Może to wymagać wykorzystania poufnych kanałów komunikacyjnych i zastosowania specjalnych narzędzi technicznych lub platform. W każdym przypadku komunikacja z operatorami i przekaz informacji dla szerszego ogółu społeczeństwa w danym państwie członkowskim pozostaje w jego gestii i jest jego obowiązkiem. Dlatego też, zgodnie z przedstawioną wyżej zasadą pomocniczości, państwa członkowskie i krajowe CSIRT ponoszą ostateczną odpowiedzialność za informacje rozpowszechniane na terytorium danego państwa i kierowane do odbiorców objętych obszarem ich kompetencji.

([2]) „Zezwolenie na działanie" – w warunkach kryzysu cybernetycznego szybki czas reakcji ma kluczowe znaczenie dla określenia właściwych działań zaradczych. Aby zapewnić ten szybki czas reakcji, państwo członkowskie może dobrowolnie udzielić innemu państwu członkowskiemu „zezwolenia na działanie" niezwłocznie i bez konsultacji z wyższymi poziomami lub instytucjami unijnymi i bez przechodzenia przez wszystkie normalnie wymagane oficjalne kanały, jeśli nie jest to wymagane w danym wypadku (np. CSIRT nie musi zasięgać konsultacji z podmiotami wyższego szczebla, aby przekazać cenne informacje do CSIRT w innym państwie członkowskim).

([3]) „Postępowanie w przypadku incydentu" oznacza wszystkie procedury umożliwiające wykrywanie i analizowanie incydentu, ograniczenie jego skutków oraz reagowanie na niego.

— Komisja Europejska:

  — Centrum Koordynacji Reagowania Kryzysowego (ERCC: działająca nieprzerwanie służba operacyjna zlokalizowana w DG ECHO) oraz wyznaczona służba odpowiedzialna (do wyboru między DG CNECT i DG HOME w zależności od charakteru danego incydentu), Sekretariat Generalny (ARGUS), DG HR (dyrekcja ds. bezpieczeństwa), DG DIGIT (operacje w zakresie bezpieczeństwa IT),

  — w przypadku innych agencji UE ([1]) odpowiednia macierzysta DG w Komisji lub ESDZ (pierwszy punkt kontaktowy).

— ESDZ:

  — SIAC (pojedyncza komórka analiz wywiadowczych: EU INTCEN i EUMS INT),

  — Centrum Sytuacyjne UE i wskazana służba właściwa pod względem geograficznym lub tematycznym,

  — komórka UE ds. syntezy informacji o zagrożeniach hybrydowych (część Centrum Analiz Wywiadowczych UE (INTCEN) – bezpieczeństwo cybernetyczne w kontekście hybrydowym).

Wspólna orientacja sytuacyjna:

— Jako element regularnej współpracy na poziomie technicznym służącej wzmocnieniu unijnej orientacji sytuacyjnej ENISA powinna regularnie przygotowywać techniczny raport sytuacyjny na temat bezpieczeństwa cybernetycznego w UE dotyczący incydentów i zagrożeń, oparty na publicznie dostępnych informacjach, swojej własnej analizie i sprawozdaniach przekazanych przez CSIRT państw członkowskich (na zasadzie dobrowolności) lub pojedyncze punkty kontaktowe powołane zgodnie z dyrektywą w sprawie bezpieczeństwa sieci i informacji, Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu i CERT-UE oraz – w stosownych przypadkach – Centrum Analiz Wywiadowczych UE (INTCEN) Europejskiej Służby Działań Zewnętrznych (ESDZ). Raport ten powinien zostać udostępniony odpowiednim organom Rady, Komisji, Wysokiemu Przedstawicielowi/wiceprzewodniczącemu Komisji oraz sieci CSIRT.

— W przypadku poważnego incydentu przewodniczący sieci CSIRT, z pomocą ENISA, przygotowuje raport sytuacyjny na temat incydentu cybernetycznego w UE ([2]), który jest przedkładany prezydencji, Komisji i Wysokiemu Przedstawicielowi/wiceprzewodniczącemu Komisji za pośrednictwem CSIRT państwa sprawującego rotacyjną prezydencję.

— *Wszystkie pozostałe agencje UE* składają raporty swoim macierzystym dyrekcjom generalnym, które z kolei przedkładają sprawozdania odpowiedzialnej służbie Komisji.

— *CERT-UE* przedkłada sprawozdania techniczne sieci CSIRT, instytucjom i agencjom UE (w stosownych przypadkach) oraz do systemu ARGUS (jeżeli został aktywowany).

— *Europol/EC3* ([3]) *i CERT-UE* zapewniają sieci CSIRT fachową analizę kryminalistyczną technicznych artefaktów oraz przedkładają jej inne informacje techniczne.

— Pojedyncza komórka analiz wywiadowczych ESDZ: w imieniu Centrum Analiz Wywiadowczych UE (INTCEN) komórka UE ds. syntezy informacji o zagrożeniach hybrydowych składa sprawozdanie odpowiednim wydziałom ESDZ.

Reagowanie:

— *Sieć CSIRT* prowadzi wymianę szczegółowych danych technicznych i analiz incydentu, takich jak adresy IP, oznaki naruszenia integralności systemu ([4]) itp. Takie informacje powinny zostać dostarczone bez zbędnej zwłoki do ENISA, najpóźniej jednak 24 godziny od wykrycia incydentu.

— Zgodnie z SPO sieci CSIRT jej członkowie współpracują w dążeniu do zanalizowania dostępnych artefaktów technicznych i innych informacji technicznych dotyczących incydentu, aby określić przyczynę i możliwe techniczne środki ograniczające skutki.

— ENISA pomaga CSIRT w ich działalności technicznej w oparciu o swoją wiedzę fachową i zgodnie ze swoim mandatem ([5]).

([1]) W zależności od charakteru i skutków incydentu w różnych sektorach działalności (finanse, transport, energia, ochrona zdrowia itp.) zaangażowane są właściwe agencje lub organy UE.

([2]) Raport sytuacyjny na temat incydentu cybernetycznego w UE jest agregacją raportów krajowych dostarczonych przez krajowe CSIRT. Format raportu powinien być opisany w standardowych procedurach operacyjnych (SPO) sieci CSIRT.

([3]) Zgodnie z warunkami i procedurami określonymi w ramach prawnych programu EC3.

([4]) Oznaka naruszenia integralności systemu (wskaźnik kompromitacji (IOC)) – w kryminalistyce informatycznej jest to artefakt zaobserwowany w sieci lub w systemie operacyjnym, który z dużym prawdopodobieństwem wskazuje na zainfekowanie komputera. Typowymi IOC są sygnatury wirusów i adresy IP, hasze MD5 plików złośliwego oprogramowania bądź URL lub nazwy domen i serwerów typu C&C (ang. *command and control*) do zarządzania botnetami.

([5]) Wniosek dotyczący rozporządzenia w sprawie Agencji UE ds. Bezpieczeństwa Cybernetycznego ENISA, uchylenia rozporządzenia (UE) nr 526/2013 oraz certyfikacji bezpieczeństwa cybernetycznego w zakresie technologii informacyjno-komunikacyjnych, 13 września 2017 r.

— CSIRT państw członkowskich koordynują swoje działania w ramach reagowania technicznego z pomocą ENISA i Komisji.

— Pojedyncza komórka analiz wywiadowczych ESDZ: w imieniu Centrum Analiz Wywiadowczych UE (INTCEN) komórka UE ds. syntezy informacji o zagrożeniach hybrydowych uruchamia proces gromadzenia dowodów w celu zebrania wstępnego materiału dowodowego.

Publiczne działania komunikacyjne:

— CSIRT opracowują poradniki techniczne ([1]) i ostrzeżenia dotyczące podatności na zagrożenia ([2]) i rozpowszechniają je w ramach swoich społeczności oraz wśród obywateli zgodnie z procedurami autoryzacyjnymi, mającymi zastosowanie w danym przypadku.

— ENISA ułatwia tworzenie i upowszechnianie wspólnych komunikatów sieci CSIRT.

— ENISA koordynuje swoje publiczne działania komunikacyjne z siecią CSIRT i służbami rzecznika prasowego Komisji.

— ENISA i EC3 koordynują swoje publiczne działania komunikacyjne w oparciu o wspólną świadomość sytuacyjną uzgodnioną przez państwa członkowskie. Oba podmioty koordynują swoje publiczne działania komunikacyjne ze służbami rzecznika prasowego Komisji.

— Jeżeli sytuacja kryzysowa obejmuje wymiar polityki zewnętrznej lub wspólnej polityki bezpieczeństwa i obrony, publiczne działania komunikacyjne należy koordynować z ESDZ i służbami rzecznika prasowego Wysokiego Przedstawiciela/wiceprzewodniczącego Komisji.

Współpraca na poziomie operacyjnym

Zakres działań:

— przygotowanie procesu decyzyjnego na poziomie politycznym,

— koordynacja zarządzania kryzysem cybernetycznym (w razie potrzeby),

— ocena skutków i wpływu na szczeblu unijnym i zaproponowanie możliwych środków zaradczych.

Potencjalne zaangażowane podmioty

— Państwa członkowskie:

  — właściwe organy i pojedyncze punkty kontaktowe powołane zgodnie z dyrektywą w sprawie bezpieczeństwa sieci i informacji,

  — CSIRT, agencje ds. bezpieczeństwa cybernetycznego,

  — inne krajowe organy sektorowe (w przypadku incydentu lub kryzysu o zasięgu ponadsektorowym).

— Organy/urzędy/agencje UE:

  — ENISA,

  — Europol/EC3,

  — CERT-UE.

— Komisja Europejska:

  — Sekretarz Generalny SG lub jego zastępca (procedura ARGUS),

  — DG CNECT/HOME,

  — organ Komisji ds. bezpieczeństwa,

  — inne DG (w przypadku incydentu lub kryzysu o zasięgu ponadsektorowym).

([1]) Porady o charakterze technicznym co do przyczyn incydentu i możliwych środków zaradczych.
([2]) Informacje o technicznych słabych punktach, które zostały wykorzystane w celu wywarcia negatywnego wpływu na systemy IT.

— ESDZ:

  — Sekretarz Generalny ds. reagowania kryzysowego lub jego zastępca i SIAC (EU INTCEN i EUMS INT),

  — komórka UE ds. syntezy informacji o zagrożeniach hybrydowych.

— Rada:

  — prezydencja (przewodniczący Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni lub COREPERU ([1])) wspierana przez Sekretariat Generalny Rady lub Komitet Polityczny i Bezpieczeństwa (KPiB) ([2]) oraz przy wsparciu ustaleń w ramach IPCR – jeżeli zostały aktywowane.

Orientacja sytuacyjna:

— wsparcie wytworzenia polityczno-strategicznych raportów sytuacyjnych (np. raport na temat zintegrowanej orientacji i analizy sytuacyjnej (ISAA) w przypadku aktywowania IPCR),

— działająca przy Radzie *Horyzontalna Grupa Robocza Rady ds. Cyberprzestrzeni* przygotowuje w stosownych przypadkach posiedzenia COREPER lub KPiB,

— w przypadku aktywowania IPCR:

  — prezydencja może zwołać posiedzenia okrągłego stołu w celu wsparcia jej przygotowań do posiedzeń COREPER lub KPiB, gromadzące odnośne zainteresowane strony z państw członkowskich, instytucje, agencje oraz strony trzecie, takie jak państwa spoza UE i organizacje międzynarodowe. Są to posiedzenia kryzysowe, mające na celu wskazanie wąskich gardeł i wysunięcie propozycji działań w odniesieniu do zagadnień przekrojowych,

  — *służba odpowiedzialna Komisji lub ESDZ* jako podmiot prowadzący zintegrowaną orientację i analizę sytuacyjną przygotowuje sprawozdanie na temat zintegrowanej orientacji i analizy sytuacyjnej zawierające materiały dostarczone przez ENISA, sieć CSIRT, Europol/EC3, EUMS INT, INTCEN oraz wszystkie pozostałe odnośne podmioty. Sprawozdanie na temat zintegrowanej orientacji i analizy sytuacyjnej stanowi ogólnounijną ocenę opartą na korelacji między incydentami technicznymi i oceną sytuacji kryzysowej (analiza zagrożeń, ocena ryzyka, pozatechniczne konsekwencje i skutki, pozacybernetyczne aspekty incydentu lub kryzysu itp.), która jest dostosowana do potrzeb poziomów operacyjnych i politycznych.

— W przypadku aktywowania systemu ARGUS:

  — ERT-UE i EC3 ([3]) wnoszą bezpośrednio wkład w wymianę informacji w ramach Komisji.

— W przypadku aktywowania mechanizmu reagowania kryzysowego ESDZ:

  — pojedyncza komórka analiz wywiadowczych zintensyfikuje gromadzenie informacji i dokona agregacji informacji ze wszystkich źródeł i przygotuje analizę i ocenę dotyczącą incydentu.

Reagowanie na żądanie z poziomu politycznego):

— Współpraca transgraniczna z pojedynczymi punktami kontaktowymi i właściwymi organami krajowymi (dyrektywa w sprawie bezpieczeństwa sieci i informacji) w celu łagodzenia konsekwencji i ograniczania skutków.

— Uruchomienie wszelkich technicznych środków zaradczych i koordynacja potencjału technicznego potrzebnego do powstrzymania lub ograniczenia wpływu ukierunkowanych ataków na systemy informatyczne.

— Współpraca i – w przypadku podjęcia takiej decyzji – koordynacja potencjału technicznego na rzecz wspólnego reagowania lub współdziałania zgodnie ze **standardowymi procedurami operacyjnymi sieci CSIRT**.

— Ocena potrzeby współpracy z odpowiednimi stronami trzecimi.

— (W przypadku aktywowania procedury ARGUS) Podejmowanie decyzji w ramach procedury ARGUS.

— (W przypadku aktywowania IPCR) Przygotowanie decyzji i koordynacja w ramach ustaleń IPCR.

— (W przypadku aktywowania MRK ESDZ) Wsparcie procesu decyzyjnego ESDZ przez mechanizm reagowania kryzysowego ESDZ, także z uwzględnieniem kontaktów z państwami trzecimi i organizacjami międzynarodowymi, a także wszelkie środki mające na celu ochronę misji i operacji w ramach WPBiO oraz delegatur UE.

([1]) Komitet Stałych Przedstawicieli lub COREPER (art. 240 Traktatu o funkcjonowaniu Unii Europejskiej – TFUE) odpowiada za przygotowywanie prac Rady Unii Europejskiej.

([2]) Komitet Polityczny i Bezpieczeństwa jest komitetem Rady Unii Europejskiej, zajmującym się wspólną polityką zagraniczną i bezpieczeństwa (WPZiB), wspomnianą w art. 38 Traktatu o Unii Europejskiej.

([3]) Zgodnie z warunkami i procedurami określonymi w ramach prawnych programu EC3.

Publiczne działania komunikacyjne:

— Uzgodnienie upublicznianych przekazów na temat incydentu.

— Jeżeli sytuacja kryzysowa obejmuje wymiar polityki zewnętrznej lub wspólnej polityki bezpieczeństwa i obrony, publiczne działania komunikacyjne należy koordynować z ESDZ i służbami rzecznika prasowego Wysokiego Przedstawiciela/wiceprzewodniczącego Komisji.

Współpraca na poziomie strategiczno-politycznym

Potencjalne zaangażowane podmioty:

— W imieniu państw członkowskich: ministrowie odpowiedzialni za bezpieczeństwo cybernetyczne.

— W imieniu Rady Europejskiej: Przewodniczący.

— W imieniu Rady: rotacyjna prezydencja.

— W przypadku zastosowania środków w ramach „zestawu narzędzi dla dyplomacji cyfrowej": KPiB i Horyzontalna Grupa Robocza.

— W imieniu Komisji Europejskiej: Przewodniczący lub oddelegowany wiceprzewodniczący Komisji/komisarz.

— Wysoki Przedstawiciel Unii ds. Zagranicznych i Polityki Bezpieczeństwa/wiceprzewodniczący Komisji.

Zakres działań: Strategiczne i polityczne zarządzanie zarówno cybernetycznymi, jak i pozacybernetycznymi aspektami kryzysu z uwzględnieniem środków zgodnie z ramami wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne.

Wspólna orientacja sytuacyjna:

— Określenie skutków zakłóceń spowodowanych sytuacją kryzysową dla funkcjonowania Unii.

Reagowanie:

— Aktywacja dodatkowych mechanizmów/instrumentów zarządzania kryzysowego, zależnie od charakteru i wpływu incydentu. Mogą to być np. mechanizmy z zakresu ochrony ludności.

— Podjęcie działań w ramach wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne.

— Udostępnienie dotkniętych państwom członkowskim pomocy w sytuacjach kryzysowych, np. uruchomienie środków z funduszu pomocy w cybernetycznych sytuacjach kryzysowych ([1]), gdy zostanie ustanowiony.

— W stosownych przypadkach współpraca i koordynacja działań z organizacjami międzynarodowymi takimi jak Organizacja Narodów Zjednoczonych, Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE), a zwłaszcza NATO.

— Ocena bezpieczeństwa narodowego i skutki dla obronności.

Publiczne działania komunikacyjne:

Podejmowanie decyzji o wspólnej strategii komunikacyjnej skierowanej do opinii publicznej;

SKOORDYNOWANE Z PAŃSTWAMI CZŁONKOWSKIMI REAGOWANIE NA SZCZEBLU UNIJNYM W RAMACH USTALEŃ IPCR

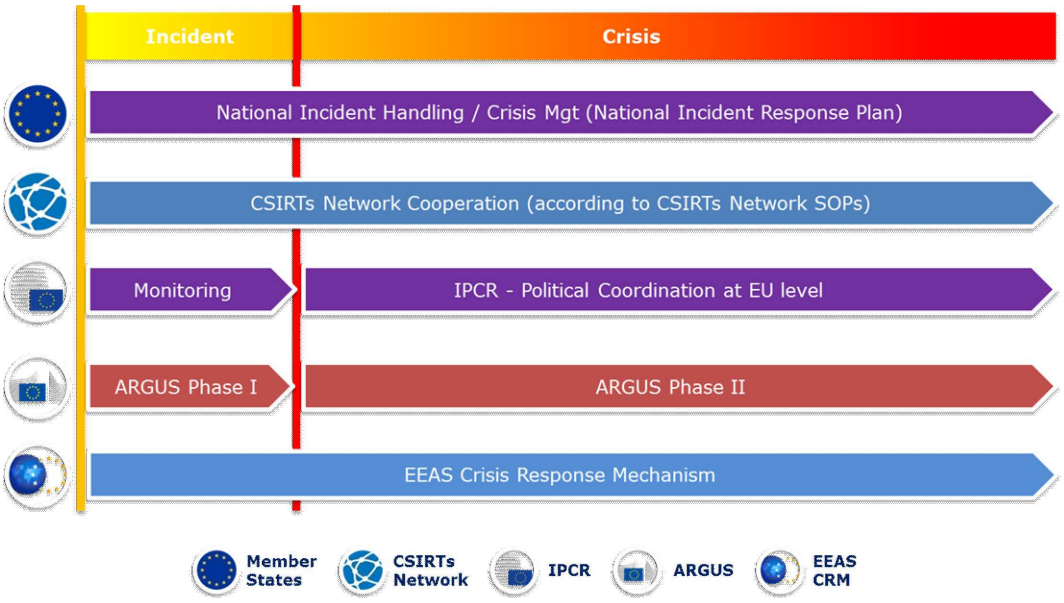
Zgodnie z zasadą komplementarności działań na szczeblu unijnym w niniejszej sekcji wprowadzono i omówiono w szczególności zasadniczy cel i zakres obowiązków oraz działań organów państw członkowskich, sieci CSIRT, ENISA, CERT-UE, Europol/EC3, INTCEN, komórki UE ds. syntezy informacji o zagrożeniach hybrydowych oraz działającej przy Radzie Horyzontalnej Grupy Roboczej ds. Cyberprzestrzeni w ramach procesu IPCR. Od podmiotów oczekuje się działania zgodnie z ustalonymi procedurami na szczeblu unijnym i krajowym.

Należy koniecznie zwrócić uwagę, że – jak przedstawiono na ilustracji 1 – niezależnie od aktywowania unijnych mechanizmów zarządzania kryzysowego działania na szczeblu krajowym oraz współpraca z siecią CSIRT (w razie potrzeby) odbywają się podczas trwania każdego incydentu/kryzysu zgodnie z zasadami pomocniczości i proporcjonalności.

([1]) Fundusz pomocy w cybernetycznych sytuacjach kryzysowych jest działaniem zaproponowanym we wspólnym komunikacie pt. Odporność, prewencja i obrona: budowanie silnego systemu bezpieczeństwa cybernetycznego dla UE, JOIN(2017) 450/1.

Ilustracja 1

Reagowanie na incydent/kryzys cybernetyczny na szczeblu unijnym



Wszystkie opisane poniżej działania muszą być przeprowadzane z zachowaniem standardowych procedur operacyjnych/zasad zastosowanych mechanizmów współpracy i zgodnie z ustalonymi mandatami i kompetencjami poszczególnych podmiotów i instytucji. Te procedury/zasady mogą wymagać pewnych uzupełnień lub zmian, prowadzących do osiągnięcia jak najlepszej współpracy i skutecznego reagowania na incydenty cybernetyczne na dużą skalę i kryzysy cybernetyczne.

Nie wszystkie wymienione niżej podmioty mogą być zobowiązane do podjęcia działań w każdym przypadku wystąpienia incydentu. W planie działania i odnośnych standardowych procedurach operacyjnych mechanizmów współpracy należy jednak przewidywać możliwość ich zaangażowania.

Z uwagi na zróżnicowanie stopnia potencjalnego wpływu incydentu lub kryzysu cybernetycznego na społeczeństwo wysoki poziom elastyczności w odniesieniu do zaangażowania podmiotów sektorowych na każdym poziomie i każde stosowne reagowanie będzie zależeć od działań zaradczych zarówno o charakterze cybernetycznym, jak i pozacybernetycznym.

Zarządzanie kryzysowe w sytuacji kryzysu cybernetycznego– włączenie bezpieczeństwa cybernetycznego do procesu IPCR

Ustalenia ICPR, opisane w standardowych procedurach operacyjnych IPCR ([1]), są zgodne na poszczególnych etapach z opisanymi poniżej krokami (zastosowanie niektórych z tych kroków zależy od sytuacji).

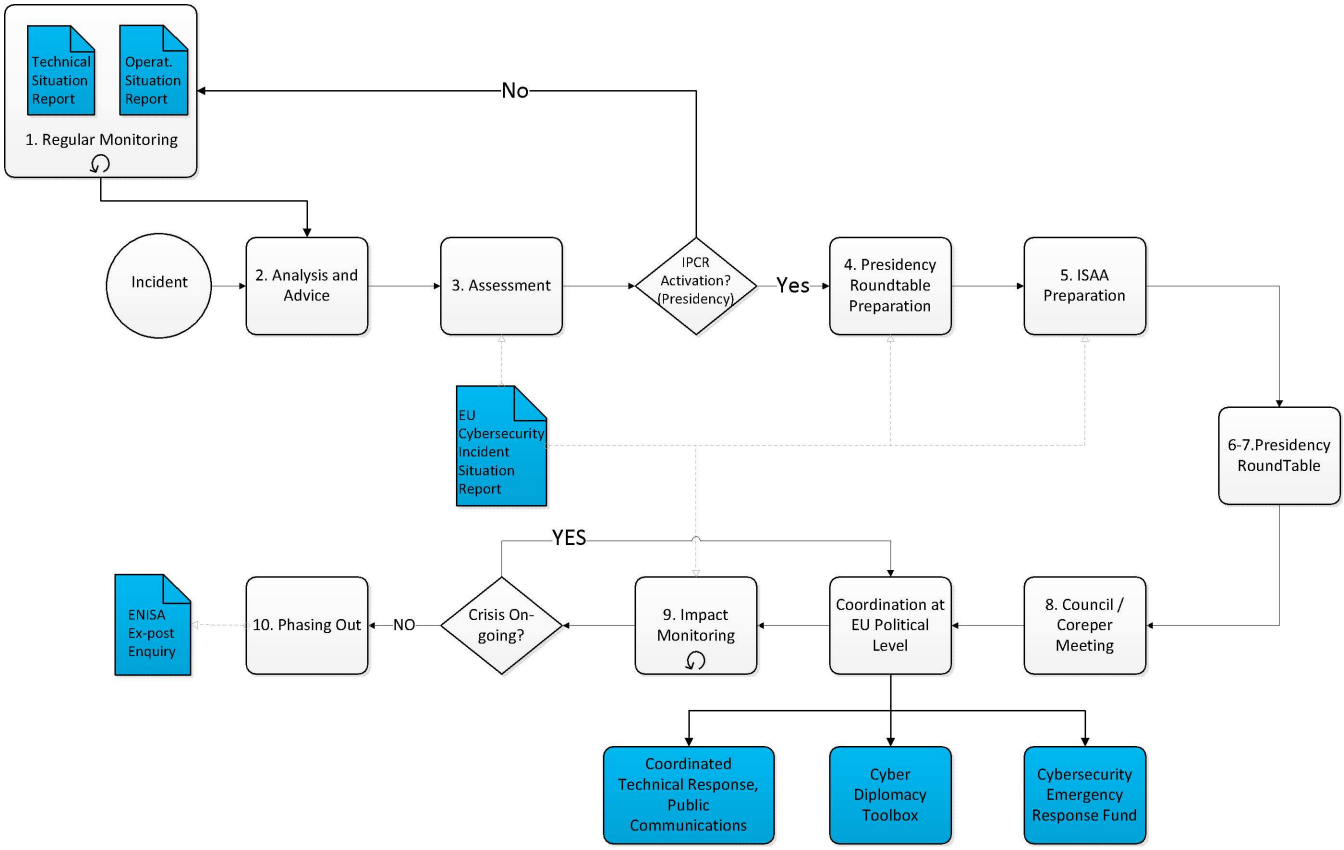
Na każdym etapie określa się działania odnoszące się do bezpieczeństwa cybernetycznego i podmioty. Dla wygody czytelnika na każdym etapie zamieszczono fragment standardowych procedur operacyjnych IPCR, po czym wyszczególniono działania nałożone niniejszym planem. Takie podejście (krok po kroku) pozwala również na jednoznaczne wskazanie istniejących **luk** w ramach niezbędnego potencjału i procedur, które to luki utrudniają skuteczne reagowanie na kryzysy cybernetyczne.

Na ilustracji 2 (poniżej ([2])) przedstawiono w formie graficznej przebieg procesu IPCR; nowo wprowadzone elementy są zaznaczone na niebiesko.

([1]) Z dokumentu 12607/15: „Standardowe procedury operacyjne IPCR", uzgodnionego przez grupę przyjaciół prezydencji i odnotowane przez COREPER w październiku 2015 r.
([2]) Obszerniejszą wersję ilustracji zamieszczono w dodatku.

Ilustracja 2

Elementy odnoszące się do bezpieczeństwa cybernetycznego w IPCR



Uwaga: Ze względu na charakter zagrożeń hybrydowych w cyberprzestrzeni, które mają pozostać poniżej progu rozpoznawalnego kryzysu, UE musi podejmować działania zapobiegawcze i służące zapewnieniu gotowości. Zadaniem komórki UE ds. syntezy informacji o zagrożeniach hybrydowych jest szybkie analizowanie odnośnych incydentów i informowanie odpowiednich struktur koordynujących. Regularne raportowanie przez tę komórkę może zapewnić decydentom sektorowym informacje sprzyjające zapewnieniu gotowości.

— **Etap 1 – Regularne monitorowanie sektorowe i ostrzeganie**: Istniejące regularne sektorowe raporty sytuacyjne i powiadomienia dostarczają prezydencji Rady wskazówek na temat rozwoju sytuacji kryzysowej i jej ewentualnych zmian.

  — **Stwierdzone luki**: Obecnie brak jest regularnych i skoordynowanych raportów sytuacyjnych z zakresu bezpieczeństwa cybernetycznego i powiadomień o incydentach (i zagrożeniach) cybernetycznych na szczeblu unijnym.

  — **Plan działania: Unijne monitorowanie sytuacji/raportowanie w zakresie bezpieczeństwa cybernetycznego**

    — **regularne techniczne raporty sytuacyjne na temat bezpieczeństwa cybernetycznego w UE**, dotyczące incydentów cybernetycznych i zagrożeń, będą opracowywane przez ENISA w oparciu o publicznie dostępne informacje, analizę własną i sprawozdania przekazane przez CSIRT państw członkowskich (na zasadzie dobrowolności) lub pojedyncze punkty kontaktowe powołane zgodnie z dyrektywą w sprawie bezpieczeństwa sieci i informacji, Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3) przy Europolu i CERT-UE oraz – w stosownych przypadkach – Centrum Analiz Wywiadowczych UE (INTCEN) Europejskiej Służby Działań Zewnętrznych (ESDZ). Raporty te powinny zostać udostępnione odpowiednim organom Rady, Komisji oraz sieci CSIRT,

    — w imieniu SIAC komórka UE ds. syntezy informacji o zagrożeniach hybrydowych powinna opracować **operacyjny raport sytuacyjny na temat stanu bezpieczeństwa cybernetycznego w UE**. Raport ten wspomaga też ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne,

    — oba raporty są rozpowszechniane wśród unijnych i krajowych zainteresowanych stron, aby poprawić poziom ich orientacji sytuacyjnej oraz wesprzeć proces decyzyjny i ułatwić transgraniczną współpracę regionalną.

Po wykryciu incydentu

— **Etap 2 – Analiza i doradztwo**: W oparciu o dostępne dane z monitorowania i ostrzeżenia służby Komisji, ESDZ i SGR informują się nawzajem o możliwym rozwoju wypadków, aby utrzymać gotowość do zapewnienia prezydencji doradztwa co do ewentualnej aktywacji IPCR (w całości lub w trybie wymiany informacji).

  — **Plan działania:**

    — w imieniu Komisji: DG CNECT, DG HOME, DG HR.DS oraz DG DIGIT, przy wsparciu ENISA, EC3 i CERT-UE,

    — ESDZ: Korzystając z prac Centrum Sytuacyjnego UE (SITROOM) oraz źródeł wywiadowczych, komórka UE ds. syntezy informacji o zagrożeniach hybrydowych zapewnia orientację sytuacyjną w zakresie faktycznych i potencjalnych zagrożeń hybrydowych uderzających w UE i jej partnerów, obejmujących zagrożenia cybernetyczne. Dlatego też w sytuacji gdy analiza i ocena wspomnianej komórki wskazują na istnienie potencjalnych zagrożeń skierowanych przeciwko państwu członkowskiemu lub krajom bądź organizacjom partnerskim, INTCEN przekazuje informacje (w pierwszej kolejności) na poziomie operacyjnym, zgodnie z ustalonymi procedurami. Na poziomie operacyjnym zostaną przygotowane zalecenia dla poziomu strategiczno-politycznego, obejmujące ewentualną aktywację ustaleń zarządzania kryzysowego w trybie monitorowania (np. mechanizm reagowania kryzysowego ESDZ lub aspekt monitorowania w ramach IPCR),

    — przewodniczący sieci CSIRT, z pomocą ENISA, przygotowuje raport sytuacyjny na temat incydentu cybernetycznego w UE ([1]), który jest przedkładany prezydencji, Komisji i Wysokiemu Przedstawicielowi/wiceprzewodniczącemu Komisji za pośrednictwem CSIRT państwa sprawującego rotacyjną prezydencję.

— **Etap 3 – Ocena sytuacji/decyzji w sprawie aktywacji IPCR**: Prezydencja ocenia potrzebę koordynacji politycznej, wymiany informacji i podejmowania decyzji na szczeblu unijnym. W tym celu prezydencja może zwołać nieformalne posiedzenie okrągłego stołu. Prezydencja określa wstępnie obszary wymagające zaangażowania COREPERU lub Rady. Stanowi to podstawę wskazówek do stworzenia raportów na temat zintegrowanej orientacji i analizy sytuacyjnej (ISAA). Po uwzględnieniu cech kryzysu, jego możliwych konsekwencji oraz związanych z nim potrzeb politycznych prezydencja podejmuje decyzję co do stosowności zwołania posiedzeń odnośnych grup roboczych Rady lub COREPERU bądź KPiB.

  — **Plan działania:**

    — uczestnicy okrągłego stołu:

      — służby Komisji i ESDZ będą doradzać prezydencji w ramach swoich obszarów kompetencji,

      — przedstawiciele państw członkowskich w Horyzontalnej Grupie Roboczej ds. Cyberprzestrzeni wspierani przez ekspertów krajowych (CSIRT, właściwe organy ds. bezpieczeństwa cybernetycznego, inne podmioty),

      — polityczno-strategiczne wskazówki na potrzeby raportów ISAA w oparciu o najnowsze raporty sytuacyjne na temat incydentu cybernetycznego w UE oraz dodatkowe informacje przedłożone przez uczestników okrągłego stołu,

      — odnośne grupy robocze i komitety:

        — Horyzontalna Grupa Robocza ds. Cyberprzestrzeni.

  Komisja, ESDZ i SGR, w pełnym porozumieniu i przy udziale prezydencji, mogą również podjąć decyzję o aktywowaniu IPCR w trybie wymiany informacji poprzez wygenerowanie strony kryzysowej, aby przygotować grunt pod ewentualną pełną aktywację.

— **Etap 4 – Aktywacja IPCR**/**gromadzenie i wymiana informacji**: Po aktywacji (w trybie wymiany informacji lub pełnej) na platformie internetowej IPCR generowana jest strona kryzysowa, umożliwiająca szczegółową wymianę informacji skoncentrowanych na kwestiach, które będą stanowić przyczynek do ISAA i wniosą wkład w przygotowanie dyskusji na poziomie politycznym. Wybór odpowiedzialnej służby ISAA (jedna ze służb Komisji lub ESDZ) zależy od danych okoliczności.

— **Etap 5 – Wytworzenie ISAA**: Inicjowane jest wytworzenie raportów ISAA. Komisja/ESDZ ogłosi raport zgodnie ze standardowymi procedurami operacyjnymi ISAA i może dalej wspierać wymianę informacji na platformie

([1]) Raport sytuacyjny na temat incydentu cybernetycznego w UE jest agregacją raportów krajowych dostarczonych przez krajowe CSIRT. Format raportu powinien być opisany w standardowych procedurach operacyjnych (SPO) sieci CSIRT.

internetowej IPCR lub kierować konkretne prośby o udzielenie informacji. Raporty ISAA są dostosowane do potrzeb poziomu politycznego (tj. COREPERU lub Rady) określonych przez prezydencję oraz sformułowanych w jej wskazówkach, dzięki czemu zapewniają one strategiczny ogląd sytuacji i rzeczową dyskusję na temat punktów porządku obrad określonych przez prezydencję Zgodnie ze standardowymi procedurami operacyjnymi ISAA od charakteru kryzysu cybernetycznego zależy, czy raport zostanie przygotowany przez którąś ze służb Komisji (DG CNECT, DG HOME), czy przez ESDZ.

W wyniku aktywacji IPCR prezydencja przedstawi konkretne obszary, na których należy się skoncentrować w ramach ISAA, aby zapewnić wsparcie koordynacji politycznej lub koordynacji procesu podejmowania decyzji w Radzie. Prezydencja określi też termin ogłoszenia raportu po konsultacjach ze służbami Komisji i ESDZ.

— **Plan działania:**

— Raport ISAA obejmuje materiały uzyskane od odpowiednich służb, w tym:

— sieci CSIRT: w formie raportu sytuacyjnego na temat incydentu cybernetycznego w UE,

— EC3, SITROOM, komórki UE ds. syntezy informacji o zagrożeniach hybrydowych, CERT-UE. Komórka UE ds. syntezy informacji o zagrożeniach hybrydowych wspomaga odpowiedzialną służbę ISAA i okrągły stół IPCR i w stosownych przypadkach dostarcza im materiały,

— unijnych agencji i organów sektorowych, zależnie od zagrożonych sektorów,

— organów państw członkowskich (innych niż CSIRT).

— Zbieranie materiałów do ISAA ([1]):

— Komisja i agencje UE: system informatyczny ARGUS będzie stanowić wewnętrzną sieć szkieletową na potrzeby ISAA. Agencje UE przekazują swoje materiały odpowiednim dyrekcjom macierzystym, które z kolei wprowadzają istotne informacje do systemu ARGUS. Służby Komisji i agencje zbierają informacje z istniejących sektorowych sieci, w których uczestniczą państwa członkowskie i organizacje międzynarodowe, oraz z innych odpowiednich źródeł.

— W imieniu ESDZ: Centrum Sytuacyjne UE wspomagane przez inne właściwe departamenty ESDZ zapewni wewnętrzną sieć szkieletową oraz pojedynczy punkt kontaktowy na potrzeby ISAA. ESDZ będzie zbierać informacje od państw trzecich oraz właściwych organizacji międzynarodowych.

— **Etap 6 – Przygotowanie nieformalnych posiedzeń okrągłego stołu zwołanych przez prezydencję**: Prezydencja, z pomocą Sekretariatu Generalnego Rady, określi termin, porządek obrad, uczestników oraz oczekiwane wyniki (możliwe rezultaty) nieformalnego posiedzenia okrągłego stołu. SGR będzie w imieniu prezydencji przekazywać na platformie internetowej IPCR istotne informacje, w szczególności zaś ogłosi zapis posiedzenia.

— **Etap 7 – Okrągły stół/działania przygotowawcze na potrzeby unijnej koordynacji politycznej/podejmowania decyzji**: Prezydencja zwoła nieformalne posiedzenie okrągłego stołu w celu dokonania przeglądu sytuacji oraz przygotowania przeglądu spraw, na które należy zwrócić uwagę COREPERU lub Rady. Nieformalne posiedzenie okrągłego stołu będzie również forum opracowania, przeglądu i omówienia wszystkich propozycji działań, które zostaną przekazane COREPEROWI/Radzie.

— **Plan działania:**

— działająca przy Radzie Horyzontalna Grupa Robocza ds. Cyberprzestrzeni przygotowuje posiedzenie COREPER lub KPiB.

— **Etap 8 – Koordynacja polityczna i podejmowanie decyzji na szczeblu COREPERU/Rady**: Wyniki posiedzeń COREPERU/Rady dotyczą koordynacji działań w ramach reagowania na wszystkich poziomach, decyzji co do zastosowania środków nadzwyczajnych, deklaracji politycznych itp. Decyzje te stanowią również zaktualizowane wskazówki polityczno-strategiczne do tworzenia kolejnych raportów ISAA.

— **Plan działania:**

— decyzja polityczna o koordynacji działań w reakcji na kryzys cybernetyczny jest wykonywana za pomocą działań (realizowanych przez odpowiednie podmioty) opisanych powyżej w sekcji 1: „Współpraca na poziomie technicznym, operacyjnym i strategiczno-politycznym" w odniesieniu do **reagowania** i **publicznych działań komunikacyjnych**,

— wytwarzanie ISAA jest kontynuowane w oparciu o współpracę na poziomie technicznym, operacyjnym i polityczno-strategicznym, w odniesieniu do **orientacji sytuacyjnej**, co również opisano wyżej w sekcji 1.

([1]) Standardowe procedury operacyjne ISAA.

— **Etap 9 – Monitorowanie wpływu**: Odpowiedzialna służba ISAA, z pomocą podmiotów wnoszących wkład do ISAA, przekazuje informacje na temat rozwoju sytuacji kryzysowej oraz wpływu na podejmowane decyzje polityczne. Taka pętla informacyjna wspomaga podlegający zmianom proces i wspiera decyzję prezydencji co do dalszego unijnego zaangażowania na poziomie politycznym lub wygaszania IPCR.

— **Etap 10 – Wygaszanie**: zgodnie z tą samą procedurą, którą zastosowano przy aktywacji, prezydencja może zwołać nieformalne posiedzenie okrągłego stołu w celu oceny potrzeby podtrzymania aktywności IPCR. Prezydencja może podjąć decyzję o zakończeniu lub obniżeniu poziomu aktywacji.

— **Plan działania:**

— ENISA może być zaproszona do przedłożenia wkładu do technicznego badania *ex post* incydentu lub do przeprowadzenia tego badana zgodnie z przepisami swojego mandatu.

DODATEK

1. ZARZĄDZANIE KRYZYSOWE, MECHANIZMY WSPÓŁPRACY I PODMIOTY NA SZCZEBLU UE

Mechanizmy zarządzania kryzysowego

Zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR) Zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR), przyjęte przez Radę w dniu 25 czerwca 2013 r. ([1]), zostały opracowane w celu ułatwienia terminowej koordynacji i reakcji na unijnym szczeblu politycznym w przypadku poważnego kryzysu IPCR wspomagają również koordynację na poziomie politycznym w reakcji na odwołanie się do klauzuli solidarności (art. 222 TFUE), jak określono w decyzji Rady 2014/415/UE z dnia 24 czerwca 2014 r. w sprawie uzgodnień dotyczących zastosowania przez Unię klauzuli solidarności. W standardowych procedurach operacyjnych (SPO) ([2]) IPCR ustanowiono proces aktywacji i kolejne działania, które należy podjąć.

ARGUS: System koordynacji w sytuacji kryzysowej ustanowiony przez Komisję Europejską w 2005 r. w celu zapewnienia specjalnej procedury koordynacji w przypadku poważnego kryzysu o charakterze wielosektorowym. Jest on wspomagany przez ogólny system szybkiego ostrzegania (narzędzie informatyczne) o tej samej nazwie. W ramach systemu ARGUS przewiduje się dwa etapy; przy czym na etapie II (w przypadku poważnego kryzysu o charakterze wielosektorowym) zwoływane są spotkania Komitetu Koordynacji Kryzysowej (CCC) pod kierownictwem przewodniczącego Komisji lub komisarza, któremu powierzono to zadanie. CCC skupia przedstawicieli odnośnych dyrekcji generalnych Komisji, gabinetów i innych służb unijnych z zadaniem objęcia przewodnictwa i koordynowania reakcji Komisji na kryzys. Pod przewodnictwem zastępcy sekretarza generalnego CCC ocenia sytuację, rozważa warianty i podejmuje decyzje wykonawcze w odniesieniu do unijnych narzędzi i instrumentów w ramach kompetencji Komisji, a także zapewnia wykonanie tych decyzji ([3]) ([4]).

Mechanizm Reagowania Kryzysowego ESDZ: Mechanizm Reagowania Kryzysowego ESDZ jest zorganizowanym systemem, który umożliwia ESDZ reagowanie na sytuacje kryzysowe i wydarzenia nadzwyczajne o zewnętrznym charakterze lub istotnym wymiarze zewnętrznym – w tym na zagrożenia hybrydowe – potencjalnie lub rzeczywiście zagrażające interesom UE lub państw członkowskich. Dzięki zapewnieniu udziału właściwych urzędników Komisji oraz Sekretariatu Rady na posiedzeniach w ramach Mechanizmu Reagowania Kryzysowego ułatwione jest uzyskiwanie efektu synergii między wysiłkami dyplomatycznymi oraz działaniami w dziedzinie bezpieczeństwa i obrony a zarządzanymi przez Komisję instrumentami finansowymi i handlowymi oraz instrumentami współpracy. Komórka Kryzysowa może zostać aktywowana w czasie kryzysu.

Mechanizmy współpracy

Sieć CSIRT: Sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego skupia wszystkie krajowe i rządowe zespoły (CSIRT) oraz zespół reagowania na incydenty komputerowe w instytucjach i agencjach UE (CERT-UE). Celem tej sieci jest umożliwienie i usprawnienie wymiany informacji między CSIRT na temat zagrożeń i incydentów cybernetycznych, a także współpraca w zakresie reagowania na incydenty i kryzysy cybernetyczne.

Horyzontalna Grupa Robocza Rady ds. Cyberprzestrzeni: grupę roboczą powołano, aby zapewnić strategiczną i horyzontalną koordynację zagadnień polityki cybernetycznej w Radzie i może być ona zaangażowana zarówno w działalność prawodawczą, jak też działania o innym charakterze.

Podmioty

ENISA: Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji powołano w 2004 roku. Agencja ściśle współpracuje z państwami członkowskimi i sektorem prywatnym w celu zapewnienia doradztwa i rozwiązań w takich kwestiach, jak ogólnoeuropejskie ćwiczenia w zakresie bezpieczeństwa cybernetycznego, opracowanie krajowych strategii bezpieczeństwa cybernetycznego, współpracy CSIRT i rozwijania zdolności. ENISA współpracuje bezpośrednio z CSIRT w całej UE i stanowi sekretariat sieci CSIRT.

Centrum Koordynacji Reagowania Kryzysowego (ERCC): Centrum Koordynacji Reagowania Kryzysowego w Komisji (w ramach Dyrekcji Generalnej ds. Ochrony Ludności i Pomocy Humanitarnej – DG ECHO) wspiera i koordynuje szereg działań w dziedzinie zapobiegania, zapewnienia gotowości i reagowania przez siedem dni w tygodniu, 24 godziny na dobę. Uruchomione w 2013 r.Centrum działa jako centrum reagowania kryzysowego Komisji (w powiązaniu z innymi centrami kryzysowymi UE), w tym także jako działający nieprzerwanie główny punkt kontaktowy (IPCR 24/7).

([1]) 10708/13 w sprawie „Finalizacji procesu weryfikacji CCA: koordynacji działań w sytuacjach nadzwyczajnych i kryzysowych", przyjęta przez Radę w dniu 24 czerwca 2013 r.
([2]) 12607/15 „Standardowe procedury operacyjne IPCR", uzgodnione przez grupę przyjaciół prezydencji i odnotowane przez COREPER w październiku 2015 r.
([3]) Przepisy Komisji w sprawie ogólnego systemu szybkiego ostrzegania „ARGUS", COM(2005) 662 final, 23 grudnia 2005 r.
([4]) Decyzja Komisji 2006/25/WE, Euratom z dnia 23 grudnia 2005 r. zmieniająca regulamin wewnętrzny Komisji (Dz.U. L 19 z 24.1.2006, s. 20), w sprawie ustanowienia ogólnego systemu szybkiego ostrzegania „ARGUS".

Europol/EC3: Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3), które powstało w 2013 r. w ramach Europolu, wspiera reagowanie organów ścigania na przestępczość cybernetyczną w UE. EC3 oferuje operacyjne i analityczne wsparcie dochodzeń prowadzonych w państwach członkowskich i służy jako centralny węzeł informacji kryminalnych i wywiadowczych, wspomagając operacje i dochodzenia państw członkowskich przez analizę operacyjną, koordynację i wiedzę ekspercką, a także wysokospecjalistyczny potencjał technicznego i cyfrowego wsparcia kryminalistycznego.

CERT-UE: Zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE) ma za zadanie poprawę ochrony instytucji, organów i agencji przed atakami i zagrożeniami cybernetycznymi. Zespół jest częścią sieci CSIRT. CERT-UE dysponuje technicznymi porozumieniami w zakresie wymiany informacji na temat zagrożeń cybernetycznych z NATO CIRC, niektórymi państwami trzecimi i głównymi podmiotami gospodarczymi w dziedzinie bezpieczeństwa cybernetycznego.

Unijna wspólnota wywiadowcza obejmuje Centrum Analiz Wywiadowczych UE (**INTCEN**) oraz Dyrekcję ds. Wywiadu w Sztabie Wojskowym UE (EUMS INT) w ramach porozumienia w sprawie **pojedynczej komórki analiz wywiadowczych** (SIAC). Misja SIAC polega na dostarczaniu analiz wywiadowczych, wczesnym ostrzeganiu i zapewnianiu orientacji sytuacyjnej Wysokiemu Przedstawicielowi UE ds. Spraw zagranicznych i polityki bezpieczeństwa oraz Europejskiej Służbie Działań Zewnętrznych (ESDZ). SIAC oferuje swoje usługi różnym podmiotom decyzyjnym UE ds. wspólnej polityki zagranicznej i bezpieczeństwa (WPZiB), wspólnej polityki bezpieczeństwa i obrony (WPBiO) i zwalczania terroryzmu (CT), a także państwom członkowskim. EU INTCEN i EUMS INT nie są agencjami operacyjnymi i nie posiadają zdolności gromadzenia danych. Działalność wywiadowcza na poziomie operacyjnym pozostaje w gestii państw członkowskich. SIAC zajmuje się jedynie analizą strategiczną.

Komórka UE ds. syntezy informacji o zagrożeniach hybrydowych We wspólnym komunikacie w sprawie przeciwdziałania zagrożeniom hybrydowym z kwietnia 2016 r. wyznaczono komórkę UE ds. syntezy informacji (EU HFC) jako główny ośrodek analizy informacji na temat zagrożeń hybrydowych w UE, pochodzących ze wszelkich źródeł: jej mandat został zatwierdzony w grudniu 2016 r. przez Komisję w drodze konsultacji pomiędzy służbami. Ulokowana w INTCEN komórka wchodzi w skład SIAC i w związku z tym współpracuje z EUMS INT i ma w swoim stałym składzie wojskowego. Działanie hybrydowe polega na zamierzonym wykorzystaniu przez państwo lub podmiot niebędący państwem kombinacji wielu ukrytych lub jawnych, wojskowych lub cywilnych narzędzi i mechanizmów, takich jak ataki cybernetyczne, kampanie dezinformacyjne, działania szpiegowskie, presja ekonomiczna, wykorzystanie innych podmiotów lub inne działania wywrotowe. EU HCF współpracuje z rozległą siecią pojedynczych punktów kontaktowych (PoC), zarówno w Komisji, jak i w państwach członkowskich, aby zapewnić zintegrowaną reakcję/zaangażowanie całego sektora administracyjnego, wymagane do przeciwstawienia się różnorodnym wyzwaniom.

EU SITROOM: Centrum Sytuacyjne UE stanowi element Centrum Analiz Wywiadowczych UE (EU INTCEN) i zapewnia ESDZ zdolność operacyjną niezbędną do natychmiastowego i skutecznego reagowania na sytuacje kryzysowe. Jest to stała cywilno-wojskowa komórka dyżurna, która prowadzi ogólnoświatowe monitorowanie i zapewnia orientację sytuacyjną przez siedem dni w tygodni, 24 godziny na dobę.

Odnośne instrumenty

Ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne: Uzgodnione w czerwcu 2017 r. ramy stanowią element unijnego podejścia do dyplomacji cyfrowej, która przyczynia się do zapobiegania konfliktom, ograniczania zagrożeń dla bezpieczeństwa cybernetycznego oraz do wzrostu stabilności w stosunkach międzynarodowych. W ramach tych w pełni wykorzystuje się środki z obszaru wspólnej polityki zagranicznej i bezpieczeństwa, w tym w razie potrzeby środki ograniczające. Zastosowanie środków określonych w ramach współpracy powinno zachęcać do współpracy, sprzyjać ograniczaniu bezpośrednich i długofalowych zagrożeń i wpływać na zachowanie odpowiedzialnego sprawcy i potencjalnych agresorów w dalszej perspektywie.

2. KOORDYNACJA W PRZYPADKU KRYZYSU CYBERNETYCZNEGO W RAMACH UZGODNIEŃ IPCR – HORYZONTALNA WARSTWA KOORDYNACYJNA I POLITYCZNA ESKALACJA

Ustalenia IPCR mogą być (i są) wykorzystywane do rozwiązania kwestii technicznych i operacyjnych, ale zawsze z punktu widzenia politycznego/strategicznego.

W warunkach eskalacji IPCR można zastosować odpowiednio do poziomu kryzysu poprzez przejście od trybu „monitorowania" do trybu „wymiany informacji", który jest pierwszym poziomem aktywacji IPCR, oraz do „pełnej aktywacji IPCR".

Decyzję o aktywacji w trybie pełnym podejmuje aktualna prezydencja w Radzie UE. Komisja, ESDZ i SGR mogą aktywować IPCR w trybie wymiany informacji. W trybie monitorowania i wymiany informacji mogą zostać uruchomione różne poziomy wymiany informacji, przy czym w trybie wymiany informacji obowiązuje wytwarzanie

raportów ISAA. Przy pełnej aktywacji IPCR do zestawu działań dochodzą posiedzenia okrągłego stołu, w których uczestniczy prezydencja (z reguły przewodniczący COREPERU II lub ekspert w danej dziedzinie w randze radcy Stałego Przedstawicielstwa, wyjątkowo posiedzenia okrągłego stołu odbywały się na szczeblu ministerialnym).

Podmioty

Aktualna prezydencja (zwykle przewodniczący COREPERU) sprawuje przewodnictwo.

W imieniu Rady Europejskiej: gabinet Przewodniczącego,

W imieniu Komisji Europejskiej: poziom SGK/DG lub eksperci w danej dziedzinie.

W imieniu ESDZ: poziom zastępcy SGK/DG lub eksperci w danej dziedzinie.

W imieniu SGK: gabinet SG, zespół IPCR oraz odpowiedzialne DG.

Zakres działań: Nakreślenie wspólnego zintegrowanego obrazu sytuacji i zwiększenie wiedzy na temat wąskich gardeł lub niedociągnięć na każdym z trzech poziomów w celu ich rozwiązania na poziomie politycznym; przygotowanie decyzji do podjęcia w czasie posiedzenia, jeżeli wchodzą one w zakres kompetencji uczestników, lub wysunięcie propozycji działań, przekazywanych do COREPERU II i dalej do Rady.

Wspólna orientacja sytuacyjna:

(IPCR nieaktywowane): Strony IPCR na potrzeby monitorowania mogą zostać wygenerowane, aby umożliwić śledzenie rozwoju sytuacji, która może przerodzić się w kryzys z konsekwencjami dla UE.

(tryb IPCR „wymiana informacji"): Służba odpowiedzialna za ISAA przygotowuje raporty ISAA na podstawie danych przekazanych przez służby Komisji, ESDZ i państwa członkowskie (za pośrednictwem formularzy IPCR).

(pełna aktywacja IPCR): Oprócz raportów ISAA na nieformalnych posiedzeniach okrągłego stołu w sprawie IPCR spotykają się różne odnośne podmioty z państw członkowskich, Komisja, ESDZ, odnośne agencje itp., aby omawiać niedociągnięcia i wąskie gardła.

Współpraca i reagowanie:

Aktywacja/synchronizacja dodatkowych mechanizmów/instrumentów zarządzania kryzysowego, zależnie od charakteru i wpływu incydentu. Mogą to być na przykład: Unijny Mechanizm Ochrony Ludności, ramy wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne lub „Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym".

Przekazywanie informacji w sytuacjach kryzysowych:

Sieć IPCR narzędzi komunikacji w sytuacjach kryzysowych może zostać uruchomiona przez prezydencję po konsultacjach z właściwymi służbami Komisji, Sekretariatu Generalnego Komisji i ESDZ w celu wsparcia wytwarzania wspólnych przekazów informacyjnych lub opracowania najskuteczniejszych narzędzi komunikacji.

3. ZARZĄDZANIE KRYZYSOWE W PRZYPADKU KRYZYSU CYBERNETYCZNEGO W RAMACH SYSTEMU ARGUS – WYMIANA INFORMACJI W RAMACH KOMISJI EUROPEJSKIEJ

W obliczu nieoczekiwanych sytuacji kryzysowych, które wymagały działania na szczeblu europejskim, tj. ataków terrorystycznych w Madrycie (w marcu 2004 r), tsunami w Azji Południowo-Wschodniej (w grudniu 2004 r.) i ataków terrorystycznych w Londynie (w lipcu 2005 r.), Komisja ustanowiła w 2005 r. system koordynacji ARGUS, wspomagany przez ogólny system szybkiego ostrzegania o tej samej nazwie [1] [2]. Jego zadaniem jest zapewnienie specjalnego **procesu koordynacji w sytuacjach kryzysowych** w razie poważnego kryzysu o charakterze wielosektorowym w celu umożliwienia w czasie rzeczywistym wymiany informacji związanych z kryzysem oraz zagwarantowania szybkiego podejmowania decyzji.

W systemie ARGUS określono dwa etapy, w zależności od powagi zdarzenia:

Etap I: służy do „wymiany informacji" w przypadku sytuacji kryzysowej na ograniczoną skalę

[1] Komisja Europejska, dnia 23 grudnia 2005 r., Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Ustalenia Komisji w sprawie bezpiecznego ogólnego systemu szybkiego ostrzegania „ARGUS", COM(2005) 662 final.

[2] Decyzja 2006/25/WE, Euratom.

Przykłady zgłoszonych niedawno w etapie I zdarzeń obejmują pożary lasów w Portugalii i Izraelu, atak w Berlinie w 2016 r., powodzie w Albanii, huragan Matthew na Haiti oraz suszę w Boliwii. Każda DG może otworzyć etap I w przypadku gdy uzna, że sytuacja w obszarze jej kompetencji jest na tyle poważna, że należy zagwarantować wymianę informacji lub z niej korzystać. DG CNECT lub DG HOME mogą na przykład otworzyć etap I w przypadku gdy uznają, że sytuacja cybernetyczna w obszarze ich kompetencji jest na tyle poważna, że należy zagwarantować wymianę informacji lub z niej korzystać.

Etap II: jest uruchamiany w przypadku poważnego kryzysu o charakterze wielosektorowym lub też w obliczu przewidywanej bądź nieuchronnej groźby dla Unii

Na etapie II uruchamia się specjalną procedurę koordynacyjną, która umożliwia Komisji podejmowanie decyzji i szybkie, skoordynowane i spójne reagowanie na najwyższym szczeblu w obszarze jej kompetencji i we współpracy z innymi instytucjami. Działania etapu II są przewidziane w odniesieniu do poważnego kryzysu o charakterze wielosektorowym lub też w obliczu przewidywanej bądź nieuchronnej groźby jego zaistnienia. Przykłady rzeczywistych wydarzeń objętych etapem II obejmują kryzys migracyjno-uchodźczy (2015 i nadal), potrójną katastrofę w elektrowni Fukushimie (2011) i wybuch wulkanu Eyjafjallajökull w Islandii (2010).

Etap II jest uruchamiany jest przez Przewodniczącego z jego własnej inicjatywy lub na wniosek jednego z członków Komisji. Przewodniczący może przydzielić odpowiedzialność polityczną za reakcję Komisji komisarzowi odpowiedzialnemu za służby, których kryzys najmocniej dotyczy, lub zachować ją dla siebie.

W ramach etapu II przewidziane są posiedzenia nadzwyczajne Komitetu Koordynacji Kryzysowej (CCC). Są one zwoływane w imieniu Przewodniczącego lub komisarza, któremu powierzono odpowiedzialność. Posiedzenia zwołuje SG za pomocą narzędzia informatycznego ARGUS. Komitet Koordynacji Kryzysowej jest specjalną strukturą operacyjną zarządzania kryzysowego, utworzoną w celu kierowania reakcją Komisji na sytuację kryzysową oraz jej koordynowania, skupiającą przedstawicieli wszystkich odpowiednich dyrekcji generalnych Komisji, gabinetów i innych służb unijnych. Komitetowi przewodniczy zastępca sekretarza generalnego. **CCC ocenia sytuację, rozważa warianty i podejmuje decyzje, a także zapewnia wykonanie decyzji i działań**, jednocześnie gwarantując spójność i konsekwencję reagowania. Wsparcie dla CCC zapewnia SG.

4. MECHANIZM REAGOWANIA KRYZYSOWEGO ESDZ

Mechanizm Reagowania Kryzysowego (MRK) ESDZ uruchamia się w razie zaistnienia poważnej sytuacji nadzwyczajnej, dotyczącej lub w inny sposób angażującej zewnętrzny wymiar UE. MRK jest aktywowany przez zastępcę sekretarza generalnego ds. reagowania kryzysowego po konsultacji z Wysokim Przedstawicielem/wiceprzewodniczącym Komisji lub Sekretarzem Generalnym. Zastępca sekretarza generalnego ds. reagowania kryzysowego może również zostać poproszony o uruchomienie mechanizmu reagowania kryzysowego przez Wysokiego Przedstawiciela/wiceprzewodniczącego komisji lub Sekretarza Generalnego bądź innego zastępcę SG lub jednostkę mediacji (MD).

MRK przyczynia się do spójności działań UE w reakcji na sytuacje kryzysowe w ramach strategii bezpieczeństwa. W szczególności MRK ułatwia uzyskiwanie efektu synergii między wysiłkami dyplomatycznymi oraz działaniami w dziedzinie bezpieczeństwa i obrony a zarządzanymi przez Komisję instrumentami finansowymi i handlowymi oraz instrumentami współpracy.

MRK jest powiązany z ogólnym systemem reagowania kryzysowego Komisji (ARGUS) oraz zintegrowanymi uzgodnieniami UE dotyczącymi reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR); dzięki temu w przypadku jednoczesnej aktywacji możliwe jest wykorzystanie efektu synergii. Centrum Sytuacyjne UE w ramach ESDZ działa jako główny ośrodek komunikacyjny między ESDZ a systemami reagowania kryzysowego w Radzie i Komisji.

Z reguły pierwszym działaniem związanym z zastosowaniem MRK jest zwołanie **posiedzenia kryzysowego** z udziałem członków kierownictwa wyższego szczebla ESDZ, Komisji i Rady, bezpośrednio dotkniętych daną sytuacją kryzysową. Uczestnicy posiedzenia kryzysowego oceniają krótkookresowe skutki sytuacji kryzysowej i mogą uzgodnić podjęcie natychmiastowych działań bądź aktywować Komórkę Kryzysową lub powołać platformę kryzysową. Kroki te mogą zostać podjęte w dowolnej kolejności.

Komórka Kryzysowa jest centrum sytuacyjnym na niewielką skalę, w którym przedstawiciele ESDZ oraz służb Komisji i Rady zaangażowanych w reagowanie na sytuację kryzysową gromadzą się, aby stale monitorować sytuację w celu zapewnienia centrali ESDZ wsparcia w podejmowaniu decyzji. Po aktywowaniu Komórka Kryzysowa funkcjonuje w trybie ciągłym (7 dni w tygodniu, 24 godziny na dobę).

Platforma kryzysowa skupia odnośne służby ESDZ, Komisji i Rady w celu dokonania oceny średnio- i długookresowych skutków sytuacji kryzysowych oraz uzgodnienia działań, które należy podjąć. Przewodnictwo sprawuje Wysoki Przedstawiciel/wiceprzewodniczący Komisji lub Sekretarz Generalny bądź zastępca sekretarza generalnego ds. reagowania kryzysowego. Platforma kryzysowa ocenia skuteczność działania UE w odniesieniu do kraju lub regionu objętego kryzysem, decyduje o zmianach środków lub podjęciu dodatkowych działań i omawia propozycje działań Rady. Platforma kryzysowa to posiedzenie *ad hoc*; dlatego nie jest w stanie ciągłej aktywacji.

Grupa zadaniowa składa się z przedstawicieli służb zaangażowanych w reagowanie i można ją uruchomić w celu śledzenia działań podejmowanych przez UE w ramach reagowania oraz ułatwienia ich realizacji. Grupa ta ocenia wpływ działań podejmowanych przez UE, przygotowuje dokumenty polityczne i materiały na temat wariantów, wnosi wkład w przygotowanie ram podejścia kryzysowego (PFCAs), ma udział w strategii w zakresie komunikacji i przyjmuje wszelkie inne ustalenia, które mogą ułatwić realizację unijnych działań w odpowiedzi na sytuację.

5. DOKUMENTY ŹRÓDŁOWE

Poniżej znajduje się wykaz dokumentów źródłowych wziętych pod uwagę przy opracowywaniu planu.

— *The European Cyber Crises Cooperation Framework* (Europejskie ramy współpracy w zakresie kryzysów cybernetycznych), wersja 1, 17 października 2012 r.

— *Report on Cyber Crisis Cooperation and Management* (Sprawozdanie na temat współpracy i zarządzania kryzysowego na wypadek kryzysu cybernetycznego), ENISA, 2014.

— *Actionable Information for Security Incident Response* (Praktyczne informacje na potrzeby reagowania na incydent cybernetyczny), ENISA, 2014.

— *Common practices of EU-level crisis management and applicability to cyber crises* (Wspólne praktyki zarządzania kryzysowego na szczeblu UE i ich zastosowanie w przypadku kryzysów cybernetycznych), ENISA, 2015.

— *Strategies for Incident Response and Cyber Crisis Cooperation* (Strategie reagowania na incydenty i współpraca na wypadek kryzysu cybernetycznego), ENISA, 2016.

— *EU Cyber Standard Operating Procedures* (Standardowe procedury operacyjne UE w obszarze cybernetyki), ENISA, 2016.

— *A good practice guide of using taxonomies in incident prevention and detection* (Przewodnik po dobrych praktykach stosowania taksonomii w zapobieganiu incydentom i ich wykrywaniu), ENISA, 2017.

— Komunikat „Wzmacnianie europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego", COM(2016) 410 final, 5.7.2016 r.

— Konkluzje Rady na temat wzmacniania europejskiego systemu odporności cybernetycznej oraz wspieranie konkurencyjnego i innowacyjnego sektora bezpieczeństwa cybernetycznego – konkluzje Rady (15 listopada 2016 r.), 14540/16.

— Decyzja Rady 2014/415/UE z dnia 24 czerwca 2014 r. w sprawie uzgodnień dotyczących zastosowania przez Unię klauzuli solidarności (Dz.U. L 192 z 1.7.2014, s. 53).

— Finalizacja procesu weryfikacji CCA: zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR), 10708/13, 7 czerwca 2013 r.

— Zintegrowana orientacja i analiza sytuacyjna (ISAA) – standardowe procedury operacyjne, DS 1570/15, 22 października 2015 r.

— Przepisy Komisji w sprawie ogólnego systemu szybkiego ostrzegania „ARGUS", COM(2005) 662 final, 23 grudnia 2005 r.

— Decyzja Komisji 2006/25/WE, Euratom z dnia 23 grudnia 2005 r. zmieniająca regulamin wewnętrzny Komisji (Dz.U. L 19 z 24.1.2006, s. 20).

— *ARGUS Modus Operandi* (Sposób działania systemu ARGUS), Komisja Europejska, 23 października 2013 r.

— Konkluzje Rady w sprawie ram wspólnej unijnej reakcji dyplomatycznej na szkodliwe działania cybernetyczne („zestaw narzędzi dla dyplomacji cyfrowej"), dokument 9916/17.

— *EU operational protocol for countering hybrid threats „EU Playbook"* (Unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym [„Unijny podręcznik taktyczny"]), SWD(2016) 227.

— Mechanizm reagowania kryzysowego ESDZ z dnia 8 listopada 2016 r. Ares(2017)880661. Wspólny dokument roboczy służb „Unijny protokół operacyjny do celów przeciwdziałania zagrożeniom hybrydowym" („Unijny podręcznik taktyczny"), SWD(2016) 227 final z dnia 5 lipca 2016 r.

— Wspólny komunikat do Parlamentu Europejskiego i Rady: Wspólne ramy dotyczące przeciwdziałania zagrożeniom hybrydowym – odpowiedź Unii Europejskiej, JOIN(2016) 18 final z dnia 6 kwietnia 2016 r.

— EEAS(2016) 1674 – Dokument roboczy Europejskiej Służby Działań Zewnętrznych – komórka UE ds. syntezy informacji o zagrożeniach hybrydowych – zakres zadań.

6. ELEMENTY ODNOSZĄCE SIĘ DO BEZPIECZEŃSTWA CYBERNETYCZNEGO W IPCR