KOMISJA
EUROPEJSKA

Bruksela, dnia 6.9.2023 r.
COM(2023) 526 final

ANNEX

ZAŁĄCZNIK

do

wniosku dotyczącego ZALECENIA RADY

w sprawie planu skoordynowanego reagowania na szczeblu Unii na zakłócenia infrastruktury krytycznej o istotnym znaczeniu transgranicznym

ZAŁĄCZNIK

W niniejszym załączniku opisano zasady, cele, główne podmioty planu skoordynowanego reagowania na znaczące incydenty związane z infrastrukturą krytyczną („plan dotyczący infrastruktury krytycznej”), funkcjonowanie tego planu oraz jego wzajemne oddziaływanie z istniejącymi mechanizmami reagowania kryzysowego, jak również sposób poprawy współpracy między państwami członkowskimi a odpowiednimi instytucjami, organami, urzędami i agencjami Unii w odniesieniu do takich incydentów, zgodnie z mającymi zastosowanie przepisami i procedurami. Niniejszy plan w żaden sposób nie wpływa na rolę i funkcjonowanie innych ustaleń.

CZĘŚĆ I: CELE, ZASADY, PODMIOTY I INNE INSTRUMENTY

1. Cele

Plan dotyczący infrastruktury krytycznej służy osiągnięciu następujących trzech głównych celów w reakcji na znaczący incydent związany z infrastrukturą krytyczną:

a) **wspólnej orientacji sytuacyjnej**, ponieważ dobre zrozumienie znaczącego incydentu związanego z infrastrukturą krytyczną w państwach członkowskich, jego przyczyn i potencjalnych konsekwencji dla wszystkich zainteresowanych stron na poziomach operacyjnym i strategicznym/politycznym ma zasadnicze znaczenie dla odpowiedniej skoordynowanej reakcji;

b) **skoordynowanej komunikacji publicznej**, ponieważ pomaga ona łagodzić negatywne skutki znaczącego incydentu związanego z infrastrukturą krytyczną i minimalizować rozbieżności w komunikatach kierowanych do społeczeństwa w państwach członkowskich. Jasna komunikacja publiczna jest również ważna dla łagodzenia skutków dezinformacji;

c) **skutecznej reakcji**, ponieważ poprawa reagowania państw członkowskich i współpracy państw członkowskich między sobą oraz z odpowiednimi instytucjami, organami, urzędami i agencjami Unii przyczynia się do łagodzenia skutków znaczącego incydentu związanego z infrastrukturą krytyczną i umożliwia szybkie przywrócenie usług kluczowych w sposób minimalizujący podatność tej infrastruktury na dalsze poważne incydenty.

2. Zasady

Proporcjonalność

Incydenty zakłócające funkcjonowanie infrastruktury krytycznej lub świadczenie usług kluczowych często nie przekraczają progu pozwalającego uznać je za znaczący incydent związany z infrastrukturą krytyczną, określony w pkt 2 niniejszego zalecenia. W związku z tym, co do zasady, można się nimi skutecznie zajmować na szczeblu krajowym. Dlatego stosowanie planu dotyczącego infrastruktury krytycznej ogranicza się do znaczących incydentów związanych z infrastrukturą krytyczną.

Pomocniczość

Zgodnie z prawem Unii, główną odpowiedzialność za reagowanie na zakłócenia funkcjonowania infrastruktury krytycznej lub świadczenia usług kluczowych przez podmioty krytyczne ponoszą państwa członkowskie. Odpowiednie instytucje, organy, urzędy i agencje Unii oraz Europejska Służba Działań Zewnętrznych („ESDZ”) odgrywają jednak ważną rolę uzupełniającą w przypadku znaczącego incydentu związanego z infrastrukturą krytyczną

o istotnym znaczeniu transgranicznym, ponieważ taki incydent może mieć wpływ na szereg obszarów działalności w obrębie jednolitego rynku, bezpieczeństwa i stosunków międzynarodowych Unii lub nawet na wszystkie te obszary, na życie mieszkańców Unii oraz na bezpieczeństwo i stosunki międzynarodowe Unii.

Komplementarność

Plan dotyczący infrastruktury krytycznej uwzględnia i odzwierciedla funkcjonowanie istniejących mechanizmów zarządzania kryzysowego na szczeblu Unii, czyli zintegrowanych uzgodnień Rady dotyczących reagowania na szczeblu politycznym w sytuacjach kryzysowych („IPCR"), wewnętrznego procesu koordynacji kryzysowej Komisji „ARGUS", Unijnego Mechanizmu Ochrony Ludności („UMOL"), wspieranego przez Centrum Koordynacji Reagowania Kryzysowego („ERCC"), oraz mechanizmu reagowania kryzysowego ESDZ. Opiera się on również na ustaleniach sektorowych, w tym na przepisach dotyczących skoordynowanego zarządzania incydentami w cyberbezpieczeństwie na dużą skalę, przewidzianych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2555[1], oraz na ramach określonych w planie skoordynowanego reagowania na wypadek wystąpienia transgranicznych incydentów cybernetycznych na dużą skalę i kryzysów cybernetycznych („plan na rzecz cyberbezpieczeństwa")[2], na sieci punktów kontaktowych ds. transportu[3] oraz na Europejskiej Komórce Koordynacji Kryzysowej ds. Lotnictwa[4].

Plan dotyczący infrastruktury krytycznej opiera się ponadto na strukturach i mechanizmach ustanowionych w dyrektywie Parlamentu Europejskiego i Rady (UE) 2022/2557[5] i ma być stosowany zgodnie z nimi, w szczególności w zakresie współpracy właściwych organów między sobą, z Komisją oraz w ramach Grupy ds. Odporności Podmiotów Krytycznych. Uwzględnia się w nim również obowiązki odpowiednich instytucji, organów, urzędów i agencji Unii zgodnie z mającymi do nich zastosowanie ramami prawnymi. Działania w zakresie reagowania kryzysowego dotyczące infrastruktury krytycznej uzupełniają inne mechanizmy zarządzania kryzysowego na szczeblu unijnym, krajowym i sektorowym, które to mechanizmy wspierają koordynację międzysektorową.

Poufność informacji

Plan dotyczący infrastruktury krytycznej uwzględnia znaczenie ochrony poufności informacji niejawnych i szczególnie chronionych informacji jawnych związanych z infrastrukturą krytyczną i podmiotami krytycznymi.

3. Odpowiednie podmioty

Każde państwo członkowskie oraz odpowiednie instytucje, organy, urzędy i agencje Unii, o których mowa w lit. a)–e) poniżej, zgodnie z mającymi do nich zastosowanie zasadami i procedurami, ustalą – w odniesieniu do każdego znaczącego incydentu związanego

[1] 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) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dz.U. L 333 z 27.12.2022, s. 80).

[2] 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. L 239 z 19.9.2017, s. 36).

[3] Komunikat Komisji „Plan awaryjny dla transportu" (COM(2022) 211 final).

[4] Ustanowionej na mocy art. 19 rozporządzenia wykonawczego Komisji (UE) 2019/123 z dnia 24 stycznia 2019 r. ustanawiającego szczegółowe przepisy wykonawcze dotyczące funkcji sieciowych zarządzania ruchem lotniczym (ATM).

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (Dz.U. L 333 z 27.12.2022, s. 164).

z infrastrukturą krytyczną – odpowiednie podmioty, w zależności od rodzaju incydentu i od tego, których sektorów on dotyczy.

a) Państwa członkowskie

– właściwe organy (np. organy odpowiedzialne za infrastrukturę krytyczną, odpowiednie organy sektorowe, pojedyncze punkty kontaktowe wyznaczone lub ustanowione na podstawie art. 9 ust. 2 dyrektywy (UE) 2022/2557, organy wyznaczone lub ustanowione na podstawie art. 9 ust. 1 dyrektywy (UE) 2022/2557);

– w stosownych przypadkach – europejska sieć organizacji łącznikowych do spraw kryzysów cyberbezpieczeństwa („EU-CyCLONe"), o której mowa w art. 16 dyrektywy (UE) 2022/2555;

– Grupa Współpracy, o której mowa w art. 14 dyrektywy (UE) 2022/2555;

– w stosownych przypadkach – inne zainteresowane strony, w tym podmioty lub osoby z sektora prywatnego, takie jak operatorzy infrastruktury krytycznej, w tym operatorzy zidentyfikowani jako podmioty krytyczne;

– ministrowie odpowiedzialni za odporność infrastruktury krytycznej lub ministrowie odpowiedzialni za sektor lub sektory najbardziej dotknięte danym znaczącym incydentem związanym z infrastrukturą krytyczną.

b) Rada

– rotacyjna prezydencja;

– odpowiednie grupy robocze, takie jak Grupa Robocza ds. Ochrony Ludności, w tym podgrupa ds. odporności podmiotów krytycznych PROCIV-CER oraz przewodniczący odpowiednich grup roboczych w zależności od charakteru incydentu i tego, jakich sektorów dotyczy, takie jak horyzontalna Grupa Robocza ds. Cyberprzestrzeni i Horyzontalna Grupa Robocza ds. Wzmacniania Odporności i Przeciwdziałania Zagrożeniom Hybrydowym;

– Coreper, Komitet Polityczny i Bezpieczeństwa oraz IPCR, wspierane przez Sekretariat Generalny Rady.

c) Komisja, w tym grupy ekspertów Komisji

– wyznaczone służby odpowiedzialne (w zależności od sektora, którego dotyczy incydent) wspierane przez ERCC jako całodobowe centrum operacyjne odpowiedzialne za zarządzanie reagowaniem kryzysowym oraz przez Dyrekcję Generalną ds. Migracji i Spraw Wewnętrznych jako służbę odpowiedzialną w danym obszarze, a w przypadku incydentu międzysektorowego – przez Dyrekcję Generalną ds. Migracji i Spraw Wewnętrznych oraz inne odpowiednie służby Komisji;

– Dyrekcja Generalna ds. Komunikacji i służba rzecznika;

– Dyrekcja Generalna HERA, europejski Urząd ds. Gotowości i Reagowania na Stany Zagrożenia Zdrowia;

– Grupa ds. Odporności Podmiotów Krytycznych, której przewodniczy przedstawiciel Komisji (Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych), ustanowiona dyrektywą (UE) 2022/2557, oraz, w stosownych przypadkach, inne odpowiednie grupy ekspertów i komitety;

– ERCC ustanowione w ramach UMOL decyzją Parlamentu Europejskiego i Rady nr 1313/2013/UE[6] (całodobowe operacyjne centrum zarządzania kryzysowego w ramach UMOL w Dyrekcji Generalnej ds. Prowadzonych przez UE Operacji Ochrony Ludności i Pomocy Humanitarnej);

– Grupa Współpracy, o której mowa w art. 14 dyrektywy (UE) 2022/2555;

– centrum orientacji i analizy sytuacyjnej w zakresie cyberbezpieczeństwa;

– Komitet ds. Bezpieczeństwa Zdrowia, o którym mowa w art. 4 rozporządzenia (UE) 2022/2371[7];

– Sekretariat Generalny Komisji (sekretariat ARGUS) i (zastępca) sekretarza generalnego (proces ARGUS), Dyrekcja Generalna ds. Zasobów Ludzkich (Dyrekcja Bezpieczeństwa);

– inne odpowiednie grupy ekspertów Komisji wspierające Komisję w koordynowaniu środków w sytuacji nadzwyczajnej lub kryzysowej;

– inne sieci zarządzania kryzysowego, w tym sektorowe (np. sieć punktów kontaktowych ds. transportu zarządzana przez Dyrekcję Generalną ds. Mobilności i Transportu, międzyinstytucjonalna grupa zadaniowa ds. cyberkryzysów[8], Europejska Komórka Koordynacji Kryzysowej ds. Lotnictwa);

– przewodniczący lub odpowiedzialny wiceprzewodniczący/komisarz.

d) ESDZ

– pojedyncza komórka analiz wywiadowczych („SIAC”) złożona z Centrum Analiz Wywiadowczych („IntCen”) i Dyrekcji ds. Wywiadu w Sztabie Wojskowym UE („EUMS Int”);

– Centrum Reagowania Kryzysowego („CRC”);

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

e) Odpowiednie organy i urzędy Unii oraz odpowiednie agencje Unii, takie jak Europol, w zależności od tego, których sektorów dotyczy incydent[9].

---

[6] Decyzja Parlamentu Europejskiego i Rady nr 1313/2013/UE z dnia 17 grudnia 2013 r. w sprawie Unijnego Mechanizmu Ochrony Ludności (Dz.U. L 347 z 20.12.2013, s. 924).

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2371 z dnia 23 listopada 2022 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylenia decyzji nr 1082/2013/UE (Dz.U. L 314 z 6.12.2022, s. 26).

[8] Nieformalna grupa obejmująca odpowiednie służby Komisji, ESDZ, Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), CERT-UE i Europol, której współprzewodniczą Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii oraz ESDZ.

[9] Np. Europol; w przypadku transportu: Agencja Unii Europejskiej ds. Bezpieczeństwa Lotniczego (EASA), Europejska Agencja Bezpieczeństwa Morskiego (EMSA), Agencja Kolejowa Unii Europejskiej (ERA); w przypadku sektora zdrowia: Europejskie Centrum ds. Zapobiegania i Kontroli Chorób (ECDC) i Europejska Agencja Leków (EMA); w przypadku sektora energii: Agencja ds. Współpracy Organów Regulacji Energetyki (ACER); w przypadku sektora przestrzeni kosmicznej: Agencja Unii Europejskiej ds. Programu Kosmicznego (EUSPA); w przypadku sektora spożywczego: Europejski Urząd ds. Bezpieczeństwa Żywności (EFSA); w przypadku sektora morskiego: Europejska Agencja Kontroli Rybołówstwa (EFCA); w przypadku cyberincydentów: Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), zespoły reagowania na

4. Wzajemne oddziaływanie planu oraz innych odpowiednich mechanizmów i instrumentów zarządzania kryzysowego

Plan dotyczący infrastruktury krytycznej jest elastycznym narzędziem określającym różne działania, które można podjąć częściowo lub w pełni z wykorzystaniem różnych istniejących ustaleń, w zależności od charakteru i powagi znaczącego incydentu związanego z infrastrukturą krytyczną oraz od potrzeby koordynacji operacyjnej lub strategicznej/politycznej.

a) Unijny protokół do celów przeciwdziałania zagrożeniom hybrydowym[10] („unijny protokół")

Unijny protokół ma zastosowanie w przypadku zagrożeń hybrydowych[11] i przedstawiono w nim zarys procesów i narzędzi mających zastosowanie w przypadku takich zagrożeń lub kampanii.

W przypadku znaczącego incydentu o wymiarze hybrydowym związanego z infrastrukturą krytyczną unijny protokół stosuje się, w stosownych przypadkach, jako uzupełnienie planu dotyczącego infrastruktury krytycznej, np. w odniesieniu do konkretnych informacji, analiz lub komunikacji na temat hybrydowych aspektów znaczącego incydentu związanego z infrastrukturą krytyczną oraz w odniesieniu do współpracy z partnerami zewnętrznymi.

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

Plan na rzecz cyberbezpieczeństwa ma zastosowanie do incydentów transgranicznych na dużą skalę, 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.

W przypadku znaczącego incydentu związanego z infrastrukturą krytyczną, który zbiega się z cyberincydentem na dużą skalę lub wydaje się z nim związany, odpowiednie grupy robocze Rady ustalają stosowną koordynację na szczeblu operacyjnym, z wykorzystaniem EU-CyCLONe lub w drodze wspólnego posiedzenia Grupy ds. Odporności Podmiotów Krytycznych z Grupą Współpracy. Celem koordynacji jest określenie, które podmioty, narzędzia lub mechanizmy mogłyby umożliwić najskuteczniejszą reakcję na znaczący incydent związany z infrastrukturą krytyczną, przy jednoczesnym unikaniu powielania działań i równoległych kierunków prac.

c) Unijny Mechanizm Ochrony Ludności i Centrum Koordynacji Reagowania Kryzysowego

Zgodnie z decyzją nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności reakcje operacyjne w ramach UMOL w przypadku wystąpienia lub groźby wystąpienia klęsk

---

incydenty bezpieczeństwa komputerowego (CSIRT), zespół reagowania na incydenty komputerowe w instytucjach, organach i agencjach UE (CERT-UE).

[10] Wspólny dokument roboczy służb „Unijny protokół do celów przeciwdziałania zagrożeniom hybrydowym", SWD(2023) 116 final.

[11] Zagrożenia hybrydowe można scharakteryzować jako połączenie działań odwetowych i destabilizujących, metod konwencjonalnych i niekonwencjonalnych, które mogą być stosowane w skoordynowany sposób przez podmioty państwowe lub niepaństwowe, aby osiągnąć konkretne cele, jednak metod tych ani działań nie można jeszcze uznać za oficjalnie wypowiedzianą wojnę, por. unijny protokół do celów przeciwdziałania zagrożeniom hybrydowym.

żywiołowych i katastrof w Unii i poza nią spowodowanych przez człowieka (w tym związanych z zakłóceniami funkcjonowania infrastruktury krytycznej) prowadzi ERCC, które jest pojedynczym całodobowym centrum operacyjnym Komisji odpowiedzialnym za zarządzanie reagowaniem kryzysowym. W takich przypadkach ERCC może zapewniać wczesne ostrzeganie, powiadamianie, analizę i wspomaganie wymiany informacji, a w przypadku uruchomienia UMOL przez państwo członkowskie – wysyłać pomoc operacyjną i ekspertów do dotkniętych obszarów. ERCC może ponadto ułatwiać koordynację sektorową i międzysektorową zarówno na szczeblu Unii, jak i między Unią a odpowiednimi organami krajowymi, w tym organami odpowiedzialnymi za ochronę ludności i odporność infrastruktury krytycznej.

d) Inne mechanizmy i instrumenty sektorowe lub międzysektorowe

W planie dotyczącym infrastruktury krytycznej nie powiela się innych sektorowych lub międzysektorowych narzędzi zarządzania kryzysowego ani mechanizmów koordynacji. Jeżeli takie narzędzia lub mechanizmy istnieją już w danym sektorze, plan dotyczący infrastruktury krytycznej, zgodnie z jego zakresem stosowania, można wykorzystać jako narzędzie uzupełniające narzędzia lub mechanizmy sektorowe lub międzysektorowe, ale nie może on ich zastąpić. Należy zapewnić niezbędną koordynację działań poszczególnych podmiotów, aby uniknąć powielania tych działań. Można to osiągnąć na przykład w ramach wewnętrznego procesu koordynacji kryzysowej Komisji „ARGUS”, wspieranego przez ERCC, lub spotkań koordynacyjnych IPCR.

CZĘŚĆ II: WYMIANA INFORMACJI I SKOORDYNOWANA REAKCJA

Opisane poniżej działania podzielono wg sposobu współpracy na te związane z wymianą informacji, skoordynowaną komunikacją i reagowaniem. Struktura ta odpowiada trybom funkcjonowania mechanizmu koordynacji kryzysowej Rady w postaci IPCR i w szerszym ujęciu uwzględnia potencjalne wykorzystanie mechanizmów koordynacji kryzysowej, które już istnieją na szczeblu UE. Struktura ta pokazuje, jak włączyć w nie te sposoby współpracy, jeżeli będą one stosowane. Większość z tych działań można jednak również podjąć w sposób autonomiczny, gdyż nie zależą one od zastosowania tego mechanizmu, lecz go uzupełniają. Działania przedstawiono w porządku chronologicznym, należy jednak pamiętać, że w przypadku kryzysu na dużą skalę, który stanowi znaczący incydent związany z infrastrukturą krytyczną, kilka działań można podjąć jednocześnie i w sposób ciągły.

1. WYMIANA INFORMACJI

a) Na szczeblu operacyjnym

Państwa członkowskie dotknięte znaczącym incydentem związanym z infrastrukturą krytyczną stosują własne środki awaryjne i zapewniają koordynację z odpowiednimi krajowymi mechanizmami zarządzania kryzysowego oraz, w stosownych przypadkach, zaangażowanie wszystkich odpowiednich podmiotów krajowych, regionalnych i lokalnych.

W stosownych przypadkach, w odniesieniu do pomocy w zakresie ochrony ludności, koordynację państw członkowskich między sobą i z Komisją zapewnia się za pośrednictwem ERCC w ramach UMOL.

i) Wymiana informacji i zgłaszanie przez właściwe organy krajowe

Oprócz obowiązków w zakresie zgłaszania i informowania określonych w art. 15 dyrektywy (UE) 2022/2557 właściwe organy krajowe odpowiedzialne za infrastrukturę krytyczną w państwach członkowskich dotkniętych znaczącym incydentem związanym z tą

infrastrukturą przekazują Komisji i rotacyjnej prezydencji w Radzie, za pośrednictwem ich pojedynczych punktów kontaktowych, bez zbędnej zwłoki, istotne informacje otrzymane od operatorów infrastruktury krytycznej, od podmiotów krytycznych lub z innych źródeł, a także informacje dotyczące uruchomionych mechanizmów zarządzania kryzysowego. W przypadku Komisji ERCC zapewnia całodobowy kontakt i zdolności operacyjne oraz koordynuje, monitoruje i wspiera w czasie rzeczywistym reagowanie na sytuacje nadzwyczajne na szczeblu Unii, a jednocześnie służy państwom członkowskim i Komisji za operacyjne centrum reagowania kryzysowego, propagujące międzysektorowe podejście do zarządzania katastrofami.

Taka wymiana informacji dotyczy rodzaju znaczącego incydentu związanego z infrastrukturą krytyczną, jego przyczyny, zaobserwowanego lub szacowanego wpływu takiego zakłócenia na infrastrukturę krytyczną i na świadczenie usług kluczowych, konsekwencji incydentu w różnych sektorach i ponad granicami oraz środków łagodzących – już wprowadzonych albo planowanych – na szczeblu krajowym lub we współpracy z odpowiednimi innymi państwami członkowskimi i Komisją w ramach istniejących uzgodnień, np. ustaleń dotyczących wymiany informacji na podstawie art. 9 i 15 dyrektywy (UE) 2022/2557. Zgłoszenie to nie skutkuje przekierowaniem zasobów infrastruktury krytycznej lub, w niektórych przypadkach, zasobów podmiotu krytycznego lub państwa członkowskiego z działań podejmowanych w reakcji na incydent, które to działania należy traktować priorytetowo.

Aby zapewnić podjęcie działań następczych ERCC lub powiadomione służby Komisji odpowiedzialne za sektory, w których wystąpił znaczący incydent związany z infrastrukturą krytyczną, informują o nim punkt kontaktowy Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych i Sekretariat Generalny Komisji. Tymczasem ERCC rozpoczyna monitorowanie wydarzeń – jeżeli jeszcze tego nie zrobiło – zwłaszcza w przypadku uruchomienia UMOL przez co najmniej jedno z dotkniętych państw członkowskich.

Komisja udostępnia EU-CyCLONe wszelkie informacje, które mogą być istotne dla uwzględnienia wymiaru cyberbezpieczeństwa lub związane z cyberincydentem.

Właściwe organy krajowe, na podstawie dyrektywy (UE) 2022/2557, bez zbędnej zwłoki podejmują współpracę i wymieniają się informacjami z organami właściwymi na podstawie dyrektywy (UE) 2022/2555 w zakresie cyberincydentów i incydentów wpływających na podmioty krytyczne, w tym środków cyberbezpieczeństwa i środków fizycznych wprowadzonych przez podmioty krytyczne.

W przypadku sektora morskiego właściwe organy krajowe rozważą możliwość wykorzystania wspólnego mechanizmu wymiany informacji („CISE") do udostępniania informacji bez zbędnej zwłoki.

ii) Organizacja spotkań ekspertów

Komisja jak najszybciej zwołuje Grupę ds. Odporności Podmiotów Krytycznych, aby ułatwić właściwym organom krajowym odpowiedzialnym za infrastrukturę krytyczną i odpowiednim instytucjom, organom, urzędom i agencjom Unii wymianę istotnych informacji na temat incydentu (jego charakteru, przyczyny, skutków i konsekwencji w różnych sektorach i ponad granicami) oraz na temat działań w zakresie reagowania, w tym środków łagodzących i wsparcia technicznego dla dotkniętych państw członkowskich. W zależności od tego, którego sektora incydent najbardziej dotyczy, odpowiednie służby Komisji będą ściśle zaangażowane w posiedzenie Grupy ds. Odporności Podmiotów Krytycznych w celu wymiany informacji zgromadzonych za pośrednictwem istniejących instrumentów sektorowych. W przypadku incydentów łączących aspekty cyberbezpieczeństwa i aspekty bezpieczeństwa fizycznego niezwiązane z cyberbezpieczeństwem odpowiednie służby

Komisji, CERT-UE i ESDZ w razie potrzeby zgłaszają te incydenty i jak najszybciej konsultują się między sobą w ramach grupy zadaniowej ds. cyberkryzysów, a także z odpowiednimi przewodniczącymi Grupy Współpracy, o której mowa w art. 14 dyrektywy (UE) 2022/2555, oraz – w stosownych przypadkach – z EU-CyCLONe w sprawie konieczności koordynacji działań. W porozumieniu z odpowiednimi przewodniczącymi Komisja (Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych oraz Dyrekcja Generalna ds. Sieci Komunikacyjnych, Treści i Technologii) może zaproponować wspólne posiedzenie Grupy ds. Odporności Podmiotów Krytycznych i Grupy Współpracy w celu wypracowania wspólnej orientacji sytuacyjnej i koordynowania odpowiednich reakcji.

W przypadku znaczącego międzysektorowego incydentu związanego z infrastrukturą krytyczną, który wymaga lub może wymagać zarządzania skutkami na szczeblu Unii, Komisja może zwołać międzysektorowe spotkania koordynacyjne z udziałem wszystkich odpowiednich zainteresowanych stron.

Jeżeli znaczący incydent związany z infrastrukturą krytyczną dotyczy również państwa trzeciego, Komisja konsultuje się z właściwym organem państwa trzeciego dotkniętego incydentem i może zaprosić go na posiedzenie Grupy ds. Odporności Podmiotów Krytycznych.

iii) Wsparcie ze strony Komisji i agencji unijnych

W stosownych przypadkach Europol, zgodnie ze swoim mandatem, przedstawia na szczeblu Unii raport sytuacyjny na temat incydentu. Inne agencje Unii, w stosownych przypadkach, zgodnie ze swoimi odpowiednimi mandatami, przekazują informacje, które są przydatne do opracowania orientacji sytuacyjnej lub skoordynowanej reakcji na znaczący incydent związany z infrastrukturą krytyczną, odpowiednim „macierzystym" dyrekcjom generalnym, które z kolei przekazują te informacje Komisji (Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych jako dyrekcji przewodniczącej Grupy ds. Odporności Podmiotów Krytycznych).

W stosownych przypadkach i zgodnie z mającymi zastosowanie ramami prawnymi Komisja może zbierać informacje na potrzeby orientacji sytuacyjnej z wykorzystaniem zasobów unijnego programu kosmicznego[12], takich jak Copernicus, Galileo i EGNOS.

b) Na szczeblu strategicznym

i) Sporządzanie sprawozdań z orientacji sytuacyjnej

Właściwe organy krajowe dzielą się informacjami na posiedzeniu Grupy ds. Odporności Podmiotów Krytycznych lub podczas wspólnych spotkań z odpowiednimi służbami, grupami ekspertów lub sieciami, a Komisja przygotowuje sprawozdanie z orientacji sytuacyjnej oparte na informacjach przekazanych przez właściwe organy krajowe oraz na innych dostępnych informacjach.

W stosownych przypadkach w sprawozdaniu tym uwzględnia się wyniki odpowiednich ocen, oszacowań i scenariuszy ryzyka na szczeblu UE w zakresie cyberbezpieczeństwa opracowanych na szczeblu UE, w tym przez Komisję, Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki Bezpieczeństwa oraz Grupę Współpracy.

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/696 z dnia 28 kwietnia 2021 r. ustanawiające Unijny program kosmiczny i Agencję Unii Europejskiej ds. Programu Kosmicznego oraz uchylające rozporządzenia (UE) nr 912/2010, (UE) nr 1285/2013 i (UE) nr 377/2014 oraz decyzję nr 541/2014/UE (Dz.U. L 170 z 12.5.2021, s. 69).

W przypadku uruchomienia IPCR sprawozdanie to może stanowić wkład w zintegrowaną orientację i analizę sytuacyjną („ISAA”) przygotowywaną przez służby Komisji i ESDZ.

W stosownych przypadkach SIAC przedstawia aktualną ocenę incydentu opartą na danych wywiadowczych.

ii) Uruchomienie unijnych mechanizmów koordynacji kryzysowej i wykorzystanie unijnych narzędzi

W stosownych przypadkach ERCC rozpoczyna udzielanie wsparcia w zakresie orientacji sytuacyjnej w związku z incydentem, w szczególności jeżeli zdarzenie powoduje uruchomienie UMOL[13]. Ponadto – za pośrednictwem usługi systemu Copernicus w zakresie zarządzania kryzysowego – dotknięte państwa członkowskie mogą zwrócić się o obrazy satelitarne swojego terytorium.

W przypadku, gdy należy podzielić się informacjami zebranymi przez Komisję z ESDZ i odpowiednimi agencjami unijnymi, główna dyrekcja generalna lub Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych w koordynacji z Sekretariatem Generalnym uruchamia wewnętrzny proces koordynacji kryzysowej Komisji „ARGUS” – Faza I przez otwarcie zdarzenia w narzędziu informatycznym ARGUS.

Rotacyjna prezydencja Rady Unii Europejskiej może aktywować uzgodnienia IPCR w trybie wymiany informacji, co wiąże się z opracowywaniem sprawozdań ISAA przez Komisję i ESDZ w oparciu o informacje uzyskane od właściwych organów krajowych i, w stosownych przypadkach, z innych źródeł. Nawet, gdy IPCR nie zostaną aktywowane, rotacyjna prezydencja Rady lub Komisja mogą – pod pewnymi warunkami – uruchomić stronę monitorowania na platformie internetowej IPCR.

W stosownych przypadkach można uruchomić inne (sektorowe) unijne mechanizmy i narzędzia zarządzania kryzysowego zgodnie z odpowiednimi procedurami. Komisja zapewni koordynację między tymi mechanizmami i narzędziami.

Jeżeli incydent fizyczny zbiega się z cyberincydentem na dużą skalę lub wydaje się z nim związany, zgodnie z definicją z art. 6 ust. 7 dyrektywy (UE) 2022/2555, rotacyjna prezydencja Rady może wykorzystać plan na rzecz cyberbezpieczeństwa do ustalenia odpowiedniej koordynacji na szczeblu operacyjnym z udziałem m.in. EU CyCLONe i Grupy ds. Odporności Podmiotów Krytycznych.

iii) Koordynacja komunikacji publicznej

Państwa członkowskie dotknięte znaczącym incydentem związanym z infrastrukturą krytyczną koordynują w miarę możliwości swoją publiczną komunikację na temat kryzysu przy jednoczesnym poszanowaniu kompetencji krajowych w tym zakresie. W stosownych przypadkach można zaangażować sieć komunikacji kryzysowej IPCR.

W oparciu o wspólną orientację sytuacyjną Grupa ds. Odporności Podmiotów Krytycznych i państwa członkowskie dotknięte incydentem wspomagają w stosownych przypadkach opracowywanie wspólnie uzgodnionych komunikatów.

Europol i inne odpowiednie agencje Unii koordynują swoje publiczne działania komunikacyjne ze służbą rzecznika Komisji w oparciu o wspólną orientację sytuacyjną.

[13] Takie jak publikacja produktów monitorowania mediów, komunikatów dotyczących ochrony ludności, briefingów analitycznych, map dziennych ECHO, codziennych aktualizacji ECHO oraz innych produktów dostosowanych do indywidualnych potrzeb.

Jeżeli znaczący incydent związany z infrastrukturą krytyczną obejmuje wymiar polityki zewnętrznej, wymiar hybrydowy lub wymiar wspólnej polityki bezpieczeństwa i obrony, komunikację publiczną koordynuje się z ESDZ i służbą rzecznika Komisji zgodnie z unijnym protokołem do celów przeciwdziałania zagrożeniom hybrydowym[14].

2. REAGOWANIE (OBEJMUJĄCE CIĄGŁE DZIAŁANIA OPISANE W CZĘŚCIACH DOTYCZĄCYCH WYMIANY INFORMACJI ORAZ DODATKOWYCH DZIAŁAŃ NA SZCZEBLU STRATEGICZNYM/POLITYCZNYM)

a) Na szczeblu strategicznym

i) Ciągłe sporządzanie sprawozdań z orientacji sytuacyjnej

Grupa Robocza Rady ds. Ochrony Ludności – Odporność Podmiotów Krytycznych (PROCIV-CER) jest informowana o sporządzeniu polityczno-strategicznego sprawozdania z orientacji sytuacyjnej (np. ISAA w przypadku uruchomienia IPCR lub sprawozdania dotyczącego wspólnej orientacji sytuacyjnej przygotowanego przez Komisję) i przygotowuje posiedzenie Coreper, jeżeli nie zostało jeszcze zwołane, lub, w stosownych przypadkach, posiedzenie Komitetu Politycznego i Bezpieczeństwa.

SIAC intensyfikuje działania informacyjne skierowane do służb wywiadowczych państw członkowskich, agreguje informacje ze wszystkich źródeł oraz przygotowuje analizę i ocenę incydentu, a także, w razie konieczności, regularnie je aktualizuje.

ii) Pełne uruchomienie unijnych mechanizmów koordynacji kryzysowej i wykorzystanie unijnych instrumentów

Jeżeli przewodniczący Komisji uruchomi Fazę II wewnętrznego procesu koordynacji kryzysowej Komisji „ARGUS”, w krótkim czasie zwołuje się posiedzenia Komitetu Koordynacji Kryzysowej z udziałem odpowiednich służb Komisji, agencji i, w stosownych przypadkach, ESDZ na potrzeby koordynacji działań w odniesieniu do wszystkich aspektów znaczącego incydentu związanego z infrastrukturą krytyczną.

W przypadku uruchomienia przez prezydencję Rady IPCR w trybie pełnym:

– Rotacyjna prezydencja Rady apeluje o szybkie zorganizowanie nieformalnego okrągłego stołu z udziałem odpowiednich podmiotów krajowych, europejskich i międzynarodowych, podczas którego przedstawiciel Komisji pełniący funkcję przewodniczącego Grupy ds. Odporności Podmiotów Krytycznych (Dyrekcja Generalna ds. Migracji i Spraw Wewnętrznych) może złożyć sprawozdanie ze zwołanych wcześniej posiedzeń grupy, uzupełnione w stosownych przypadkach przez inne służby Komisji i ESDZ.

– Można poprosić SIAC i odpowiednie agencje unijne o przedstawienie na tym posiedzeniu aktualnej sytuacji w zakresie znaczącego incydentu związanego z infrastrukturą krytyczną.

Służba odpowiedzialna ds. ISAA (służba odpowiedzialna Komisji lub ESDZ) przygotowuje sprawozdanie ISAA z wykorzystaniem materiałów dostarczonych przez odpowiednie służby Komisji, odpowiednie urzędy, organy i agencje Unii oraz właściwe organy krajowe. Zachęca się państwa członkowskie do przekazywania informacji za pośrednictwem platformy internetowej IPCR na potrzeby sporządzania sprawozdań ISAA.

W przypadku gdy znaczący incydent związany z infrastrukturą krytyczną ma znaczenie dla bezpieczeństwa międzynarodowego, służby Komisji i ESDZ mogą zwołać posiedzenie

[14] Wspólny dokument roboczy służb „Unijny protokół do celów przeciwdziałania zagrożeniom hybrydowym”, SWD(2023) 116 final.

w ramach zorganizowanego dialogu UE–NATO na temat odporności, aby wnieść wkład we wspólną orientację sytuacyjną i wymienić się informacjami na temat środków zastosowanych odpowiednio przez Unię i przez NATO.

iii) Komunikacja publiczna

Rada przygotowuje wspólne komunikaty publiczne. Nieformalna sieć ds. komunikacji kryzysowej, ustanowiona w ramach IPCR, może wspierać te prace. W stosownych przypadkach również służba rzecznika Komisji przygotowuje komunikaty publiczne.

Jeżeli znaczący incydent związany z infrastrukturą krytyczną obejmuje wymiar polityki zewnętrznej, wymiar hybrydowy lub wymiar wspólnej polityki bezpieczeństwa i obrony, komunikację publiczną koordynuje się z ESDZ i służbą rzecznika Komisji.

iv) Wsparcie dla państw członkowskich i skuteczne reagowanie

Rotacyjna prezydencja może zwołać posiedzenie PROCIV-CER w celu wsparcia działań w ramach IPCR, jeżeli działania te zostały uruchomione.

Państwa członkowskie dotknięte znaczącym incydentem związanym z infrastrukturą krytyczną mogą – za pośrednictwem Grupy ds. Odporności Podmiotów Krytycznych – zwrócić się do innych państw członkowskich lub odpowiednich instytucji, organów i agencji Unii o wsparcie techniczne, np. o konkretną wiedzę fachową w celu złagodzenia niekorzystnych skutków znaczącego incydentu związanego z infrastrukturą krytyczną.

Państwa członkowskie dotknięte znaczącym incydentem związanym z infrastrukturą krytyczną mogą również zwrócić się o wsparcie techniczne lub finansowe do Komisji lub odpowiednich agencji unijnych. Komisja, we współpracy z odpowiednimi agencjami unijnymi, ocenia, jakiego wsparcia może udzielić, i w stosownych przypadkach uruchamia techniczne środki łagodzące na szczeblu Unii zgodnie z odpowiednimi procedurami oraz koordynuje zdolności techniczne niezbędne do powstrzymania lub ograniczenia wpływu znaczącego incydentu związanego z infrastrukturą krytyczną.

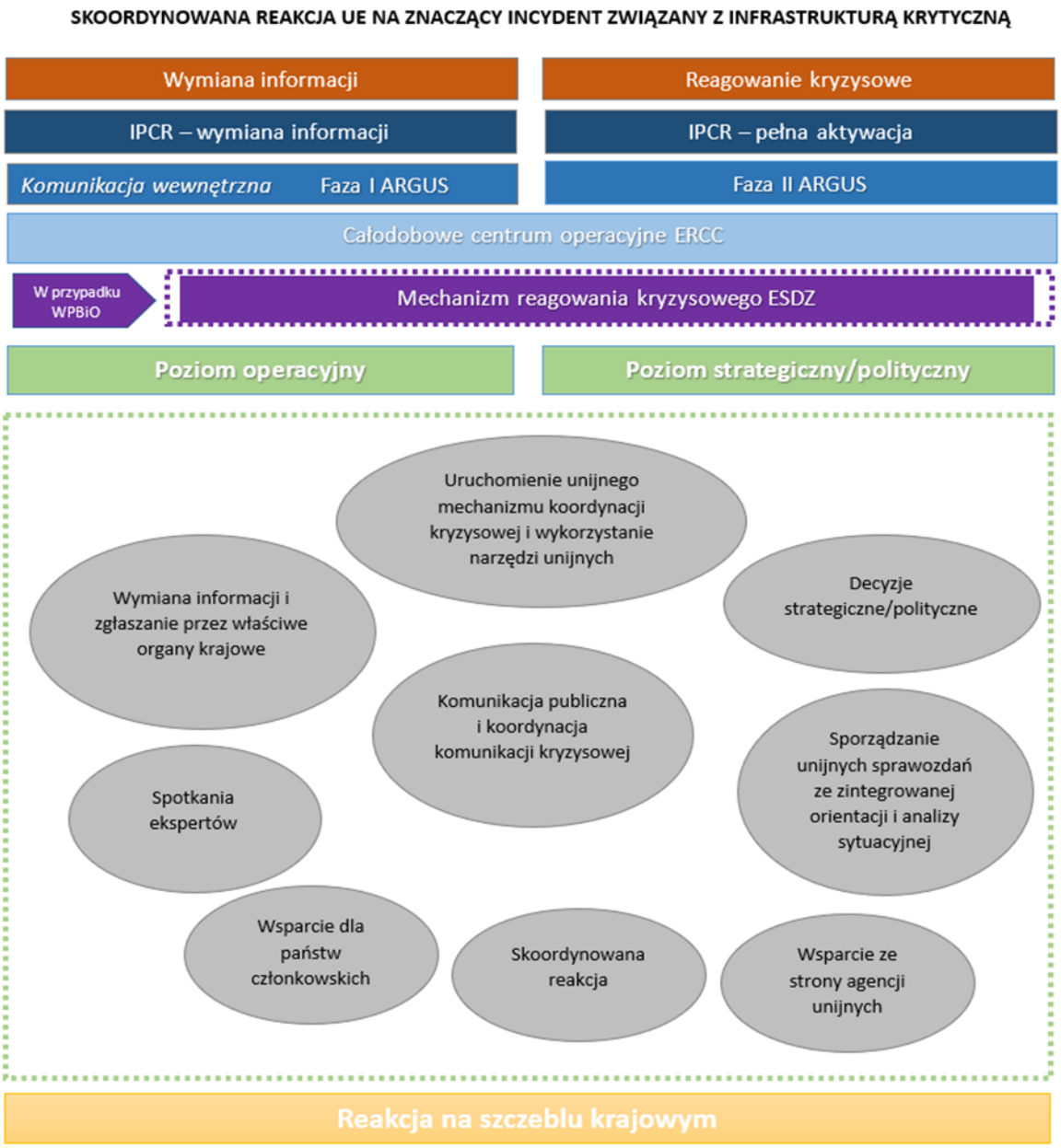
W szczególności w kontekście UMOL państwa dotknięte incydentem mogą zwrócić się o pomoc za pośrednictwem wspólnego systemu łączności i informacji w sytuacjach nadzwyczajnych („CECIS”), po czym koordynacją pomocy udzielanej przez państwa członkowskie i państwa uczestniczące w UMOL zajmie się ERCC; państwa te mogą się również zwrócić o pomoc za pośrednictwem „rescEU”.

W ramach swoich odpowiednich mandatów i na stosowny wniosek Europol i inne odpowiednie agencje Unii pomagają państwom członkowskim dotkniętym znaczącym incydentem związanym z infrastrukturą krytyczną zbadać ten incydent.

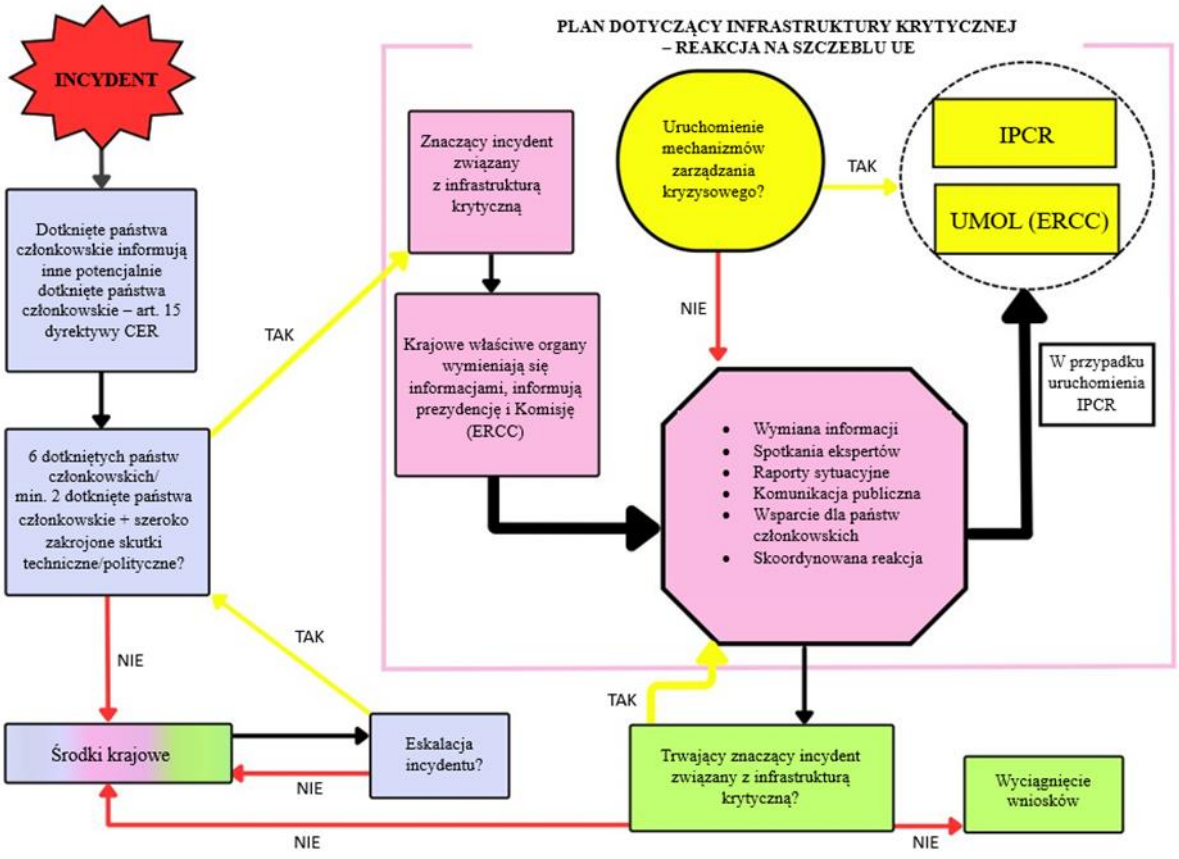
b) Na szczeblu politycznym

Prezydencja Rady może rozważyć konieczność zwołania posiedzeń okrągłego stołu grupy IPCR, posiedzeń grup roboczych Rady, Coreper, Rady Ministrów lub szczytów w celu wymiany informacji na temat możliwego źródła i spodziewanych konsekwencji znaczącego incydentu związanego z infrastrukturą krytyczną dla państw członkowskich i Unii, uzgodnienia wspólnych wytycznych oraz przyjęcia niezbędnych środków na potrzeby wsparcia państw członkowskich dotkniętych takim incydentem i złagodzenia jego skutków.

Wykres 1: Schematyczny przegląd planu dotyczącego infrastruktury krytycznej



Wykres 2: Podejmowanie decyzji w sprawie planu dotyczącego infrastruktury krytycznej



LEGENDA

Etapy poprzedzające uruchomienie planu działania

Uruchomienie mechanizmów zarządzania kryzysowego

Plan działania

Etapy po uruchomieniu planu działania