Съвет на
Европейския съюз

Брюксел, 7 септември 2023 г.
(OR. en)

12485/23
ADD 1

Междуинституционално досие:
2023/0318(NLE)

PROCIV 57
ENV 925
JAI 1084
SAN 494
COSI 140
CHIMIE 85
ENFOPOL 356
RECH 380
CT 133
DENLEG 38
COTER 153
RELEX 987
ENER 467
HYBRID 53
TRANS 329
CYBER 203
TELECOM 251
ESPACE 45
ATO 48
CSC 408
ECOFIN 839
CSCI 149
DATAPROTECT 216
MI 698
CODEC 1500
COPS 418
JAIEX 46
COPEN 292
IND 441
POLMIL 221
IPCR 55
DIGIT 160
DISINFO 62
CSDP/PSDC 608
MARE 18
POLMAR 47

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	6 септември 2023 г.
До:	Г-жа Thérèse BLANCHET, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2023) 526 final
Относно:	ПРИЛОЖЕНИЕ към Предложение за ПРЕПОРЪКА НА СЪВЕТА относно подробен план за координиран отговор на равнището на Съюза на смущения в критичната инфраструктура със значително трансгранично значение

Приложено се изпраща на делегациите документ COM(2023) 526 final.

Приложение: COM(2023) 526 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 6.9.2023 г.
COM(2023) 526 final

ANNEX

ПРИЛОЖЕНИЕ

към

Предложение за ПРЕПОРЪКА НА СЪВЕТА

относно подробен план за координиран отговор на равнището на Съюза на смущения в критичната инфраструктура със значително трансгранично значение

ПРИЛОЖЕНИЕ

В настоящото приложение се описват принципите, целите, основните участници, взаимодействието със съществуващите механизми за реакция при кризи и функционирането на подробен план за координиране на реакцията при значителни инциденти с критичната инфраструктура („подробен план за критичната инфраструктура“) и подобряване на сътрудничеството между държавите членки и съответните институции, органи, служби и агенции на Съюза по отношение на такива инциденти в съответствие с приложимите правила и процедури. Настоящият подробен план не засяга по никакъв начин ролята и функционирането на други механизми.

ЧАСТ I: ЦЕЛИ, ПРИНЦИПИ, УЧАСТНИЦИ И ДРУГИ ИНСТРУМЕНТИ

1. Цели

Подробният план за критичната инфраструктура има за цел да постигне следните три основни цели в отговор на значителен инцидент с критичната инфраструктура:

а) **Споделена ситуационна осведоменост**, тъй като правилното разбиране на значителния инцидент с критичната инфраструктура в държавите членки, неговия произход и потенциалните последици за всички заинтересовани страни на оперативно и стратегическо/политическо равнище е от съществено значение за подходящия координиран отговор.

б) **Координирана комуникация с обществеността**, тъй като тя спомага за смекчаване на негативните последици от значителен инцидент с критичната инфраструктура и за свеждане до минимум на разминаванията в съобщенията, предавани на обществеността в държавите членки и между тях. Ясната комуникация с обществеността също е важна за смекчаване на последиците от дезинформацията.

в) **Ефективен отговор**, тъй като засилването на отговора на държавите членки и сътрудничеството между тях и със съответните институции, органи, служби и агенции на Съюза допринасят за смекчаване на последиците от значителен инцидент с критичната инфраструктура и за бързото възстановяване на основните услуги по начин, който свежда до минимум уязвимостта на по-нататъшни значителни инциденти.

2. Принципи

Пропорционалност

Инцидентите, които причиняват смущения в критичната инфраструктура и/или предоставянето на основни услуги, често са под прага на значителен инцидент с критичната инфраструктура, както е посочено в точка 2 от настоящата препоръка. Като такива, те по принцип могат да бъдат решени ефективно на национално равнище. Поради това прилагането на подробния план за критичната инфраструктура се ограничава до значителни инциденти с критичната инфраструктура.

Субсидиарност

В съответствие с правото на Съюза държавите членки носят основната отговорност за реакция при смущения в критичната инфраструктура или прекъсване на основните услуги, предоставяни от критични субекти. Съответните институции, органи, служби и агенции на Съюза, както и Европейската служба за външна дейност (ЕСВД) обаче имат

важна допълваща роля в случай на значителен инцидент с критична инфраструктура с мащабно трансгранично значение, тъй като такъв инцидент може да засегне няколко сектора или дори всички сектори на икономическата дейност в рамките на вътрешния пазар, живота на гражданите, живеещи в Съюза, сигурността и международните отношения на Съюза.

Взаимно допълване

Подробният план за критичната инфраструктура отчита и отразява функционирането на съществуващите механизми за управление на кризи на равнището на Съюза, а именно договореностите на Съвета за интегрирана реакция при кризи (IPCR), вътрешния процес на Комисията за координация при кризи ARGUS, Механизма за гражданска защита на Съюза (МГЗС), подпомаган от Координационния център за реагиране при извънредни ситуации (ERCC), и механизма за реакция при кризи на ЕСВД. Той се основава и на секторни договорености, включително на разпоредбите за координирано управление на мащабни киберинциденти, предвидено в Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета[1], и на рамката, установена в подробния план за координирана реакция на мащабни трансгранични инциденти и кризи в областта на киберсигурността („подробен план в областта на киберсигурността“)[2], мрежата от звена за контакт в областта на транспорта[3] и европейското звено за координация при кризи в авиацията[4].

Освен това подробният план за критичната инфраструктура се основава на структурите и механизмите, създадени с Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета[5], и следва да се прилага в съответствие с тях, по-специално по отношение на сътрудничеството между компетентните органи и Комисията, както и в рамките на Групата по въпросите на устойчивостта на критичните субекти. В него са взети предвид и отговорностите на съответните институции, органи, служби и агенции на Съюза съгласно приложимата за тях правна рамка. Дейностите за реакция при кризи, свързани с критичната инфраструктура, се допълват други механизми за управление на кризи на равнището на Съюза, на национално и на секторно равнище, които подпомагат многосекторната координация.

Поверителност на информацията

В подробния план за критичната инфраструктура е отчетена важността на опазването на поверителността на класифицираната и чувствителната некласифицирана информация, свързана с критичната инфраструктура и критичните субекти.

---

[1] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (ОВ L 333, 27.12.2022 г., стр. 80).

[2] Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи (ОВ L 239, 19.9.2017 г., стр. 36).

[3] Съобщение на Комисията — План за действие в извънредни ситуации за транспорта (COM/2022/211 final).

[4] Създадено съгласно член 19 от Регламент за изпълнение (ЕС) 2019/123 на Комисията от 24 януари 2019 г. за определяне на подробни правила за прилагане на мрежовите функции за управление на въздушното движение (УВД).

[5] Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета (ОВ L 333, 27.12.2022 г., стр. 164).

3. Участници

Всяка държава членка и съответните институции, органи, служби и агенции на Съюза, посочени в букви а)—д) по-долу, в съответствие с приложимите за тях правила и процедури, вземат решение за съответния(те) участник(ци) за всеки значителен инцидент с критичната инфраструктура в зависимост от засегнатия(те) сектор(и) и вида на инцидента.

а) Държави членки

— компетентни органи (напр. органите, отговарящи за критичната инфраструктура, съответните секторни органи, единните звена за контакт, определени или създадени съгласно член 9, параграф 2 от Директива (ЕС) 2022/2557, органите, определени или създадени съгласно член 9, параграф 1 от Директива (ЕС) 2022/2557);

— когато е целесъобразно, Европейската мрежа за връзка на организациите при кибернетични кризи (EU-CyCLONe), както е посочено в член 16 от Директива (ЕС) 2022/2555;

— групата за сътрудничество, както е посочено в член 14 от Директива (ЕС) 2022/2555;

— когато е целесъобразно, други заинтересовани страни, включително субекти или лица от частния сектор, като например оператори на критична инфраструктура, включително тези, които са определени като критични субекти;

— министрите, отговарящи за устойчивостта на критичната инфраструктура, и/или министъра(ите), отговарящ(и) за сектора или секторите, които са най-силно засегнати от въпросния значителен инцидент с критичната инфраструктура.

б) Съвета

— ротационното председателство;

— съответните работни групи, като например работна група „Гражданска защита“, включително подгрупата „Устойчивост на критичните субекти“ (PROCIV-CER), и председателят(ите) на съответната(ите) работна(и) група(и) в зависимост от засегнатия(ите) сектор(и) и естеството на инцидента, като например хоризонталната работна група по въпроси на кибернетичното пространство и хоризонталната работна група „Повишаване на устойчивостта и борба с хибридните заплахи“;

— Корепер, Комитетът по политика и сигурност и IPCR, подпомагани от Генералния секретариат на Съвета.

в) Комисията, включително експертните групи на Комисията

— определена водеща служба (в зависимост от засегнатия сектор), подпомагана от ERCC като оперативен център, който работи денонощно 7 дни в седмицата, за управление на реакцията при кризи и генерална дирекция „Миграция и вътрешни работи“ като отговорна служба в района, а в случай на междусекторен инцидент — генерална дирекция „Миграция и вътрешни работи“ и други съответни служби на Комисията;

— генерална дирекция „Комуникации“ и службата на говорителя;

—Европейски орган за готовност и реакция при извънредни здравни ситуации (HERA);

— групата по въпросите на устойчивостта на критичните субекти, председателствана от представител на Комисията (генерална дирекция „Миграция и вътрешни работи“), създадена с Директива (ЕС) 2022/2557, и, когато е целесъобразно, други съответни експертни групи и комитети;

— ERCC, създаден съгласно МГЗС с Решение № 1313/2013/ЕС на Европейския парламент и на Съвета[6] (оперативен център за управление на извънредни ситуации, който работи денонощно 7 дни в седмицата, съгласно МГЗС, разположен в генерална дирекция „Европейска гражданска защита и европейски операции за хуманитарна помощ“);

— групата за сътрудничество, както е посочено в член 14 от Директива (ЕС) 2022/2555;

— центърът за ситуационна осведоменост и анализ в областта на киберсигурността;

— Комитетът за здравна сигурност, както е посочен в член 4 от Регламент (ЕС) 2022/2371[7];

— Генералният секретариат на Комисията (секретариатът на ARGUS) и (заместник-) генералният секретар (процесът по ARGUS), генерална дирекция „Човешки ресурси“ (дирекция „Сигурност“);

— други съответни експертни групи на Комисията, които я подпомагат при координирането на мерките в извънредна или кризисна ситуация;

— други мрежи за управление на кризи, включително секторни (например мрежата от звена за контакт в областта на транспорта, управлявана от генерална дирекция „Мобилност и транспорт“, междуинституционалната оперативна група за киберкризи[8], европейското звено за координация при кризи в авиацията);

— председателят и/или отговорният заместник-председател/член на Комисията.

г) ЕСВД

— единно звено за анализ на разузнавателна информация (SIAC), състоящо се от Центъра на ЕС за анализ на информация (IntCen) и дирекция „Военно разузнаване“ на ЕС (EUMS Int);

— център за реакция при кризи (CRC);

— върховният представител на Съюза по въпросите на външните работи и политиката на сигурност/заместник-председател на Комисията.

---

[6] Решение № 1313/2013/ЕС на Европейския парламент и на Съвета от 17 декември 2013 г. относно Механизъм за гражданска защита на Съюза (ОВ L 347, 20.12.2013 г., стр. 924).

[7] Регламент (ЕС) 2022/2371 на Европейския парламент и на Съвета от 23 ноември 2022 г. относно сериозните трансгранични заплахи за здравето и за отмяна на Решение № 1082/2013/ЕС (ОВ L 314, 6.12.2022 г., стр. 26).

[8] Неформална група, включваща съответните служби на Комисията, ЕСВД, Агенцията на Европейския съюз за киберсигурност (ENISA), CERT-EU и Европол, със съпредседатели от генерална дирекция „Съобщителни мрежи, съдържание и технологии“ и ЕСВД.

д) Съответните органи и служби на Съюза и съответните агенции на Съюза, като например Европол, в зависимост от засегнатия(те) сектор(и)[9].

4. Взаимодействие с други съответни механизми и инструменти за управление на кризи

Подробният план за критичната инфраструктура е гъвкав инструмент, в който са очертани различни действия, които биха могли да бъдат предприети частично или изцяло, като се използват различни съществуващи договорености, в зависимост от естеството и сериозността на значителния инцидент с критичната инфраструктура и от необходимостта от оперативна, стратегическа/политическа координация.

а) Протокол на ЕС за борбата с хибридните заплахи[10] („протокол на ЕС“)

Протоколът на ЕС се прилага в случай на хибридни заплахи[11], като в него са очертани процесите и инструментите, приложими в случай на такива заплахи или кампании.

В случай на значителен инцидент с критична инфраструктура с хибридно измерение протоколът на ЕС се прилага в допълнение към подробния план за критичната инфраструктура, когато е целесъобразно, например за специфична информация, анализ или комуникация относно хибридните аспекти на значителния инцидент с критичната инфраструктура и по отношение на сътрудничеството с външни партньори.

б) Подробен план за координирана реакция на мащабни трансгранични киберинциденти и кризи

Подробният план в областта на киберсигурността се прилага при мащабни инциденти с трансгранично значение, причиняващи смущения, които са прекалено мащабни, за да може засегнатата държава членка да се справи сама с тях, или при които техническите или политическите последици за две или повече държави членки или институции на ЕС са толкова значителни, че изискват своевременна координация и реакция на политическо равнище от Съюза.

В случай на значителен инцидент с критичната инфраструктура, който съвпада или изглежда, че е свързан с мащабен киберинцидент, съответните работни групи на Съвета определят подходяща координация на оперативно равнище, включително с EU-CyCLONe или чрез съвместно заседание на Групата по въпросите на устойчивостта на

---

[9] Като например Европол; в областта на транспорта: Агенцията за авиационна безопасност на Европейския съюз (ЕААБ), Европейската агенция по морска безопасност (ЕАМБ), Европейската железопътна агенция (ЕЖА); в областта на здравеопазването: Европейския център за профилактика и контрол върху заболяванията (ECDC) и Европейската агенция по лекарствата (ЕМА); в областта на енергетиката: Агенцията за сътрудничество между регулаторите на енергия (АСРЕ); в областта на космоса: Агенцията на Европейския съюз за космическата програма (EUSPA); в сектора на храните: Европейският орган по безопасност на храните (ЕОБХ); в областта на морското дело: Европейската агенция за контрол на рибарството (EFCA); в областта на киберинцидентите: Агенцията на Европейския съюз за киберсигурност (ENISA), екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС), екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU).

[10] Съвместен работен документ на службите — Протокол на ЕС за борбата с хибридните заплахи, SWD(2023) 116 final.

[11] Хибридните заплахи могат да се характеризират като смесица от принудителна и подривна дейност, конвенционални и неконвенционални методи, които могат да бъдат използвани по координиран начин от държавни или недържавни участници за постигане на конкретни цели, като същевременно остават под прага на официално обявена война, вж. протокола на ЕС относно хибридните заплахи.

критичните субекти с групата за сътрудничество. Целта на координацията е да се определи кой участник, инструмент(и) или механизъм(и) би(ха) могъл(и) да допринесе(ат) най-ефективно за реагиране на значителен инцидент с критичната инфраструктура, като се избягва дублиране и паралелни направления на работа.

в) Механизъм за гражданска защита на Съюза и Координационен център за реагиране при извънредни ситуации

В съответствие с Решение № 1313/2013/ЕС относно Механизма за гражданска защита на Съюза оперативният отговор в рамките на МГЗС при действителни природни и причинени от човека бедствия или непосредствена заплаха от такива (включително такива, които включват смущения в критична инфраструктура) в рамките на Съюза и извън него се ръководи от ERCC — единния оперативен център на Комисията, който работи денонощно 7 дни в седмицата и управлява реакцията при кризи. В такива случаи ERCC може да осигури ранно предупреждение, уведомяване, анализ и подпомага обмена на информация, а в случай на задействане на МГЗС от държава членка — разгръщането на оперативна помощ и експерти в засегнатите райони. Освен това ERCC може да улесни секторната и междусекторната координация както на равнището на Съюза, така и между Съюза и съответните национални органи, включително тези, които отговарят за гражданската защита и устойчивостта на критичната инфраструктура.

г) Други секторни или междусекторни механизми и инструменти

Подробният план за критичната инфраструктура не дублира други секторни или междусекторни инструменти за управление на кризи или механизми за координация. Когато такива инструменти или механизми вече съществуват в засегнатия сектор, подробният план за критичната инфраструктура, в рамките на приложното си поле, може да се използва като допълнителен инструмент към секторните или междусекторните инструменти или механизми, но не ги замества. Нужно е да се осигури необходимата координация между различните участници, за да се избегне такова дублиране. Това може да бъде постигнато например в рамките на вътрешния процес на Комисията за координация при кризи ARGUS, подкрепен от ERCC, и/или на координационните срещи за IPCR.

ЧАСТ II: ОБМЕН НА ИНФОРМАЦИЯ И КООРДИНИРАН ОТГОВОР

Действията, описани по-долу, се състоят от начини на сътрудничество, а именно обмен на информация, координирана комуникация и реакция. Тази структура съответства на начините на работа на механизма на Съвета за координация при кризи IPCR и е отчетено в по-широк план потенциалното използване на вече съществуващите на равнището на ЕС механизми за координация при кризи. Тази структура показва как тези начини на сътрудничество биха се интегрирали в нея, ако се използват. Въпреки това повечето от тези действия могат да се извършват и самостоятелно: те не зависят от използването на този механизъм, а по-скоро го допълват. Действията са представени в хронологичен ред, като се отчита фактът, че в случай на мащабна криза, която представлява значителен инцидент с критичната инфраструктура, могат да бъдат предприети няколко действия едновременно и непрекъснато.

1. ОБМЕН НА ИНФОРМАЦИЯ

а) На оперативно равнище

Държавите членки, засегнати от значителен инцидент с критичната инфраструктура, прилагат свои собствени мерки за действие при извънредни ситуации, осигуряват

координация със съответните национални механизми за управление на кризи и участие на всички съответни национални, регионални и местни участници, според случая.

Когато е уместно по отношение на помощта в областта на гражданската защита, координацията между държавите членки и Комисията се осигурява чрез ERCC в рамките на МГЗС.

i) Обмен на информация и уведомяване от страна на националните компетентни органи

В допълнение към задълженията за уведомяване и информиране съгласно член 15 от Директива (ЕС) 2022/2557 националните компетентни органи, отговарящи за критичната инфраструктура в държавите членки, засегнати от значителен инцидент с критичната инфраструктура, споделят с ротационното председателство на Съвета и Комисията, чрез своите единни звена за контакт и без неоправдано забавяне, съответната информация, получена от оператора(ите) на критичната инфраструктура, критичните субекти или от други източници, както и информация относно механизмите за управление на кризи, които са били задействани. За Комисията ERCC осигурява денонощно 7 дни в седмицата оперативни контакти и капацитет и координира, наблюдава и подкрепя в реално време реакцията при извънредни ситуации на равнището на Съюза, като същевременно служи на държавите членки и на Комисията като оперативен център за реакция при кризи, насърчаващ междусекторен подход към управлението на бедствия.

Такъв обмен на информация се отнася до естеството на значителния инцидент с критичната инфраструктура, причината за него, наблюдаваното или очакваното въздействие на смущението върху критичната инфраструктура и предоставянето на основни услуги, последиците от инцидента в различни сектори и в трансграничен план и мерките за смекчаване на последиците, които вече са предприети или се предвиждат, на национално равнище или със съответните други държави членки и Комисията чрез съществуващите договорености, например договореностите за обмен на информация съгласно членове 9 и 15 от Директива (ЕС) 2022/2557. Това уведомяване се предоставя без да отклонява ресурсите на критичната инфраструктура или, в някои случаи, на критичния субект или на държавата членка от дейностите по справяне с инцидента, които трябва да имат приоритет.

За да се осигурят последващи действия, ERCC или нотифицираните служби на Комисията, отговарящи за сектора(ите), в който(ито) е възникнал значителният инцидент с критичната инфраструктура, информират звеното за контакт в генерална дирекция „Миграция и вътрешни работи“ и Генералния секретариат на Комисията. Междувременно, ако все още не е започнал, ERCC започва да наблюдава събитията, особено в случай на задействане на МГЗС от една или повече от засегнатите държави членки.

Ако информацията може да бъде от значение за справяне с измерение на киберсигурността или е свързана с киберинцидент, Комисията споделя съответната информация с EU-CyCLONe.

Националните компетентни органи съгласно Директива (ЕС) 2022/2557 си сътрудничат и да обменят информация с компетентните органи съгласно Директива (ЕС) 2022/2555 без неоправдано забавяне във връзка с киберинциденти и инциденти, засягащи критични субекти, включително мерките за киберсигурност и физическите мерки, предприети от критичните субекти.

Що се отнася до морската област, националните компетентни органи обмислят възможността за използване на общата среда за обмен на информация (CISE) за обмен на информация без неоправдано забавяне.

ii) Организиране на експертни срещи

Комисията свиква във възможно най-кратък срок Групата по въпросите на устойчивостта на критичните субекти, за да се улесни обменът на съответната информация между националните компетентни органи, отговарящи за критичната инфраструктура, и съответните институции, органи, служби и агенции на Съюза относно инцидента (естество, причина, въздействие и последици в различни сектори и в трансграничен план) и относно действията за реакция, включително смекчаващи мерки и техническа подкрепа за засегнатите държави членки. В зависимост от центъра на тежестта на инцидента съответните служби на Комисията ще бъдат тясно свързани със заседанието на Групата по въпросите на устойчивостта на критичните субекти с цел обмен на информация, събрана чрез съществуващите секторни инструменти. В случай на инциденти, при които киберсигурността е съчетана с физически аспекти, които не са свързани с киберсигурността, съответните служби на Комисията, CERT-EU и ЕСВД, когато е целесъобразно, уведомяват и се консултират възможно най-бързо в рамките на оперативната работна група за киберкризи, както и със съответните председатели на групата за сътрудничество, посочена в член 14 от Директива (ЕС) 2022/2555, и EU-CyCLONe, когато е целесъобразно, относно необходимостта от координационни дейности. Със съгласието на съответните председатели Комисията (генерална дирекция „Миграция и вътрешни работи“ и генерална дирекция „Съобщителни мрежи, съдържание и технологии“) може да предложи съвместно заседание на Групата по въпросите на устойчивостта на критичните субекти с Групата за сътрудничество с оглед на споделена ситуационна осведоменост и координиране на съответните реакции.

В случай на значителен междусекторен инцидент с критичната инфраструктура, който изисква или има вероятност да изисква управление на последствията на равнището на Съюза, Комисията може да свика междусекторни координационни срещи с участието на всички съответни заинтересовани страни.

В случай че значителен инцидент с критична инфраструктура засяга и трета държава, Комисията се консултира с компетентния орган на засегнатата трета държава и може да го покани на заседание на Групата по въпросите на устойчивостта на критичните субекти.

iii) Подкрепа от страна на Комисията и агенциите на Съюза

Когато е целесъобразно и като действа в съответствие с правомощията си, Европол представя доклад за ситуацията с инцидентите на равнището на Съюза. Другите агенции на Съюза, когато е целесъобразно и като действат в съответствие със съответните си правомощия, докладват съответната информация, с която се допринася за ситуационната осведоменост или за координирана реакция на значителния инцидент с критичната инфраструктура, на съответните си генерални дирекции, към които принадлежат, като последните от своя страна докладват на Комисията (генерална дирекция „Миграция и вътрешни работи“ в качеството ѝ на председател на Групата по въпросите на устойчивостта на критичните субекти).

Комисията може да допринесе за ситуационната осведоменост чрез използване на активите на космическата програма на Съюза[12], като „Коперник“, „Галилео“ и EGNOS, когато това е целесъобразно и в съответствие с приложимата правна рамка.

б) На стратегическо равнище

i) Изготвяне на доклади за ситуационна осведоменост

Въз основа на информацията, представена от националните компетентни органи по време на среща на Групата по въпросите на устойчивостта на критичните субекти или на съвместни срещи със съответните служби, експертни групи или мрежи, Комисията изготвя доклад за ситуационната осведоменост въз основа на приноса на компетентните национални органи и друга налична информация.

Когато е целесъобразно, в този доклад се вземат предвид резултатите от съответните оценки на риска, оценявания и сценарии на равнището на ЕС от гледна точка на киберсигурността, включително тези, извършени от Комисията, върховния представител на Съюза по въпросите на външните работи и политиката за сигурност и групата за сътрудничество.

В случай на задействане на IPCR този доклад може да допринесе за интегрирания капацитет за ситуационна осведоменост и анализ (ISAA), изготвен от службите на Комисията и ЕСВД.

Когато е целесъобразно, SIAC представя актуална оценка на инцидента, основана на разузнавателни данни.

ii) Задействане на механизмите на Съюза за координация при кризи и използване на инструментите на Съюза

ERCC започва да предоставя подкрепа за ситуационна осведоменост относно инцидента, когато това е целесъобразно, по-специално ако събитието предизвиква задействане на МГЗС[13]. Освен това засегнатите държави членки могат да поискат сателитни снимки на своята територия чрез услугата за управление на извънредни ситуации на „Коперник“.

Когато се прецени, че е целесъобразно да се обменя информация в рамките на Комисията с ЕСВД и съответните агенции на Съюза, водещата генерална дирекция или генерална дирекция „Миграция и вътрешни работи“, в координация с генералния секретариат, задейства вътрешния процес на Комисията за координация при кризи ARGUS фаза I, като открива събитие в ИТ инструмента Argus.

Ротационното председателство на Съвета на Съюза може да задейства договореностите за IPCR в режим на обмен на информация, който включва изготвянето на доклади ISAA от Комисията и ЕСВД с принос от националните компетентни органи и други източници, когато е целесъобразно. Дори без да се задейства IPCR, при определени условия ротационното председателство на Съвета или Комисията могат да инициират страница за наблюдение в уеб платформата на IPCR.

---

[12] Регламент (ЕС) 2021/696 на Европейския парламент и на Съвета от 28 април 2021 г. за създаване на космическа програма на Съюза и Агенция на Европейския съюз за космическата програма и за отмяна на регламенти (ЕС) № 912/2010, (ЕС) № 1285/2013 и (ЕС) № 377/2014 и на Решение № 541/2014/ЕС (ОВ L 170, 12.5.2021 г., стр. 69).

[13] Като например публикуването на продукти за медиен мониторинг, съобщения за гражданска защита, аналитични справки, ежедневни карти на ЕСНО, ежедневни бюлетини на ЕСНО и други персонализирани продукти.

Други (секторни) механизми и инструменти на Съюза за управление на кризи могат да бъдат задействани при спазване на съответните процедури, според случая. Комисията ще осигури координация между тези механизми и инструменти.

Ако физическият инцидент съвпада или изглежда, че е свързан с мащабен киберинцидент, както е определено в член 6, параграф 7 от Директива (ЕС) 2022/2555, ротационното председателство на Съвета може да използва подробния план в областта на киберсигурността, за да се определи подходяща координация на оперативно равнище, включваща, *inter alia,* EU CyCLONe и Групата по въпросите на устойчивостта на критичните субекти.

iii) Координация на комуникацията с обществеността

Държавите членки, засегнати от значителен инцидент с критичната инфраструктура, координират комуникацията си с обществеността във връзка с кризата във възможно най-голяма степен, като зачитат националните компетенции в това отношение. По целесъобразност може да бъде включена комуникационната мрежа при кризи за IPCR.

Въз основа на споделената ситуационна осведоменост Групата по въпросите на устойчивостта на критичните субекти и засегнатите държави членки подкрепят формулирането на договорени канали за комуникация с обществеността, когато е целесъобразно.

Европол и други съответни агенции на Съюза координират своите дейности по комуникация с обществеността със службата на говорителя на Комисията въз основа на споделена ситуационна осведоменост.

Ако значителният инцидент с критичната инфраструктура има външно, хибридно измерение или измерение, свързано с общата политика за сигурност и отбрана, комуникацията с обществеността се координира с ЕСВД и службата на говорителя на Комисията в съответствие с протокола на ЕС за борбата с хибридните заплахи[14].

2. РЕАКЦИЯ (ВКЛЮЧВАЩА НЕПРЕКЪСНАТИ ДЕЙСТВИЯ, ОПИСАНИ В РАЗДЕЛ „ОБМЕН НА ИНФОРМАЦИЯ“, И ДОПЪЛНИТЕЛНИ ДЕЙСТВИЯ НА СТРАТЕГИЧЕСКО/ПОЛИТИЧЕСКО РАВНИЩЕ)

а) На стратегическо равнище

i) Непрекъснато изготвяне на ситуационни доклади

Работната група на Съвета „Гражданска защита и устойчивост на критичните субекти“ (PROCIV-CER) се информира за изготвянето на ситуационен доклад на политическо/стратегическо равнище (например ISAA в случай на задействане на IPCR или споделения доклад за ситуационна осведоменост, изготвен от Комисията) и подготвя Корепер, в случай че последният все още не е свикан, или заседание на Комитета по политика и сигурност, според случая.

SIAC засилва контактите си с разузнавателните служби на държавите членки, обобщава информацията от всички източници и изготвя анализ и оценка на инцидента, както и редовни актуализации, ако е необходимо.

[14] Съвместен работен документ на службите — Протокол на ЕС за борбата с хибридните заплахи, SWD(2023) 116 final.

ii) Пълно задействане на механизмите на Съюза за координация при кризи и използване на инструментите на Съюза

В случай че председателят на Комисията задейства вътрешния процес на Комисията за координация при кризи ARGUS фаза II, в кратък срок се свиква(т) заседание(я) на Кризисния координационен комитет, в което(ито) участват съответните служби на Комисията, агенции и ЕСВД, когато е целесъобразно, за да се координират всички аспекти на значителния инцидент с критичната инфраструктура.

В случай че председателството на Съвета задейства IPCR в пълен режим:

— Ротационното председателство на Съвета призовава за своевременна неофициална кръгла маса, на която да заседават съответните национални, европейски и международни участници и на която представителят на Комисията, изпълняващ функциите на председател на Групата по въпросите на устойчивостта на критичните субекти (генерална дирекция „Миграция и вътрешни работи“), да докладва за предварително свиканата(ите) среща(и) на групата, допълнена от други служби на Комисията и ЕСВД, по целесъобразност.

— SIAC и съответните агенции на Съюза могат да бъдат поканени да представят на това заседание актуална информация за ситуацията във връзка със значителния инцидент с критичната инфраструктура.

Водещата служба за ISAA (водещата служба на Комисията или ЕСВД) изготвя доклада ISAA с участието на съответните служби на Комисията, съответните служби, органи и агенции на Съюза и националните компетентни органи. Държавите членки се приканват да предоставят информация за изготвянето на докладите ISAA чрез уеб платформата на IPCR.

В случай на значителен инцидент с критична инфраструктура от значение за международната сигурност службите на Комисията и ЕСВД могат да свикат заседание на структурирания диалог ЕС—НАТО по въпросите на устойчивостта, за да допринесат за споделена ситуационна осведоменост и обмен на информация относно мерките, предприети съответно от Съюза и НАТО.

iii) Комуникация с обществеността

Съветът подготвя общи послания за комуникацията с обществеността. Тази дейност може да се подкрепя от неформалната кризисна комуникационна мрежа, създадена чрез IPCR. Службата на говорителя на Комисията също подготвя послания за комуникация с обществеността, ако е целесъобразно.

Ако значителният инцидент с критичната инфраструктура има външно, хибридно измерение или измерение, свързано с общата политика за сигурност и отбрана, комуникацията с обществеността се координира с ЕСВД и службата на говорителя на Комисията.

iv) Подкрепа за държавите членки и ефективна реакция

Ротационното председателство може да свика заседание на PROCIV-CER в подкрепа на дейностите в рамките на IPCR, ако се задейства.

Държавите членки, засегнати от значителен инцидент с критичната инфраструктура, могат да поискат техническа подкрепа от други държави членки или от съответните институции, органи и агенции на Съюза чрез Групата по въпросите на устойчивостта на критичните субекти, например специфичен експертен опит за смекчаване на неблагоприятните последици от значителния инцидент с критичната инфраструктура.

Държавите членки, засегнати от значителен инцидент с критичната инфраструктура, могат също така да поискат техническа и/или финансова подкрепа от Комисията или от съответните агенции на Съюза. Комисията, в координация със съответните агенции на Съюза, оценява възможната подкрепа и задейства, когато е целесъобразно, технически мерки за смекчаване на последиците на равнището на Съюза в съответствие със съответните им процедури и координира техническия капацитет, необходим за спиране или намаляване на въздействието на значителния инцидент с критичната инфраструктура.

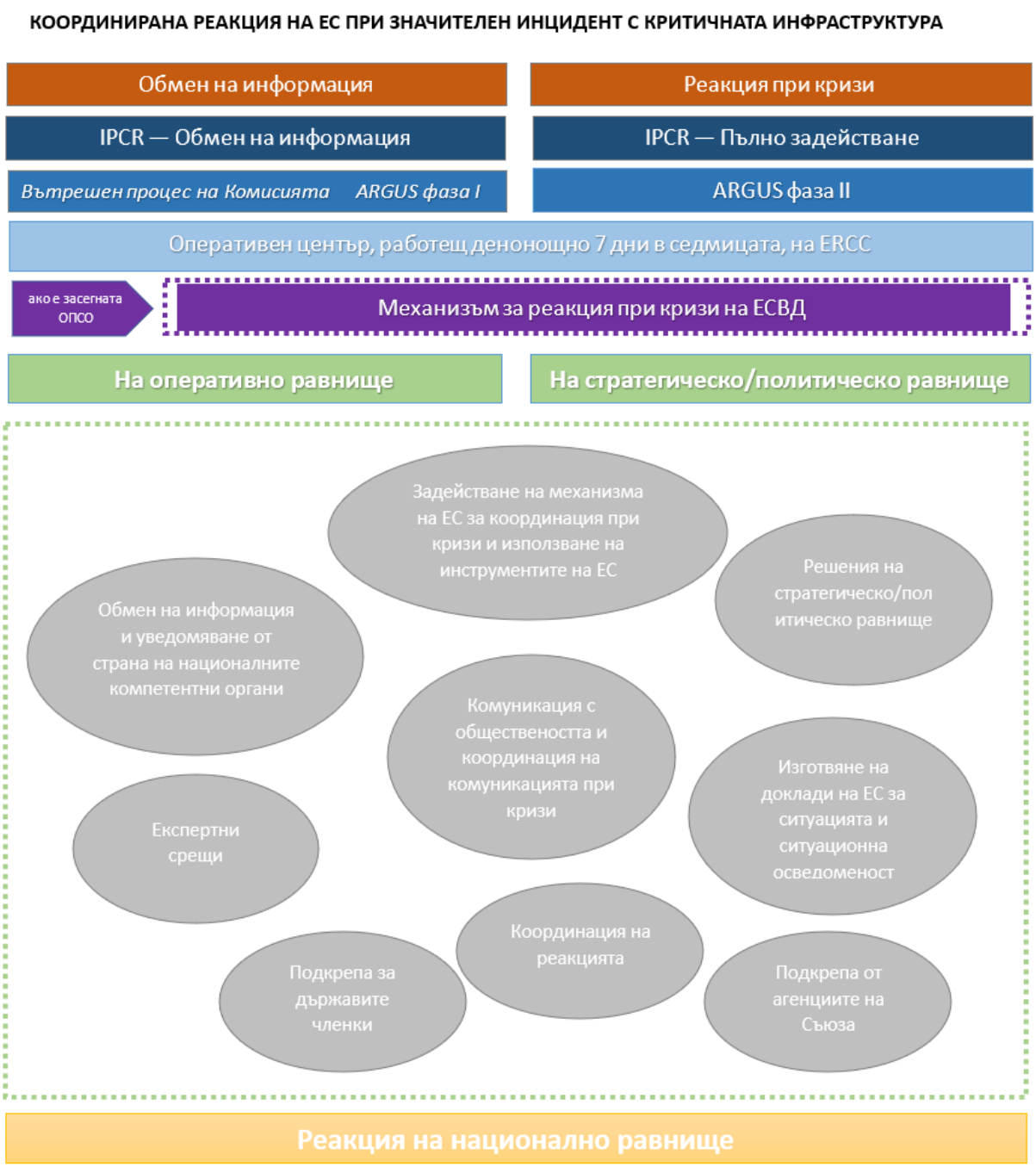
Конкретно в контекста на МГЗС засегнатите държави могат да поискат помощ чрез Общата система за спешна комуникация и информация („CECIS“), след което ERCC ще работи за координиране на оказването на помощ от държавите членки и участващите държави в МГЗС, както и чрез rescEU.

В рамките на съответните си мандати и при поискване Европол и други съответни агенции на Съюза оказват подкрепа на държавите членки, засегнати от значителен инцидент с критичната инфраструктура, при разследването на инцидента.

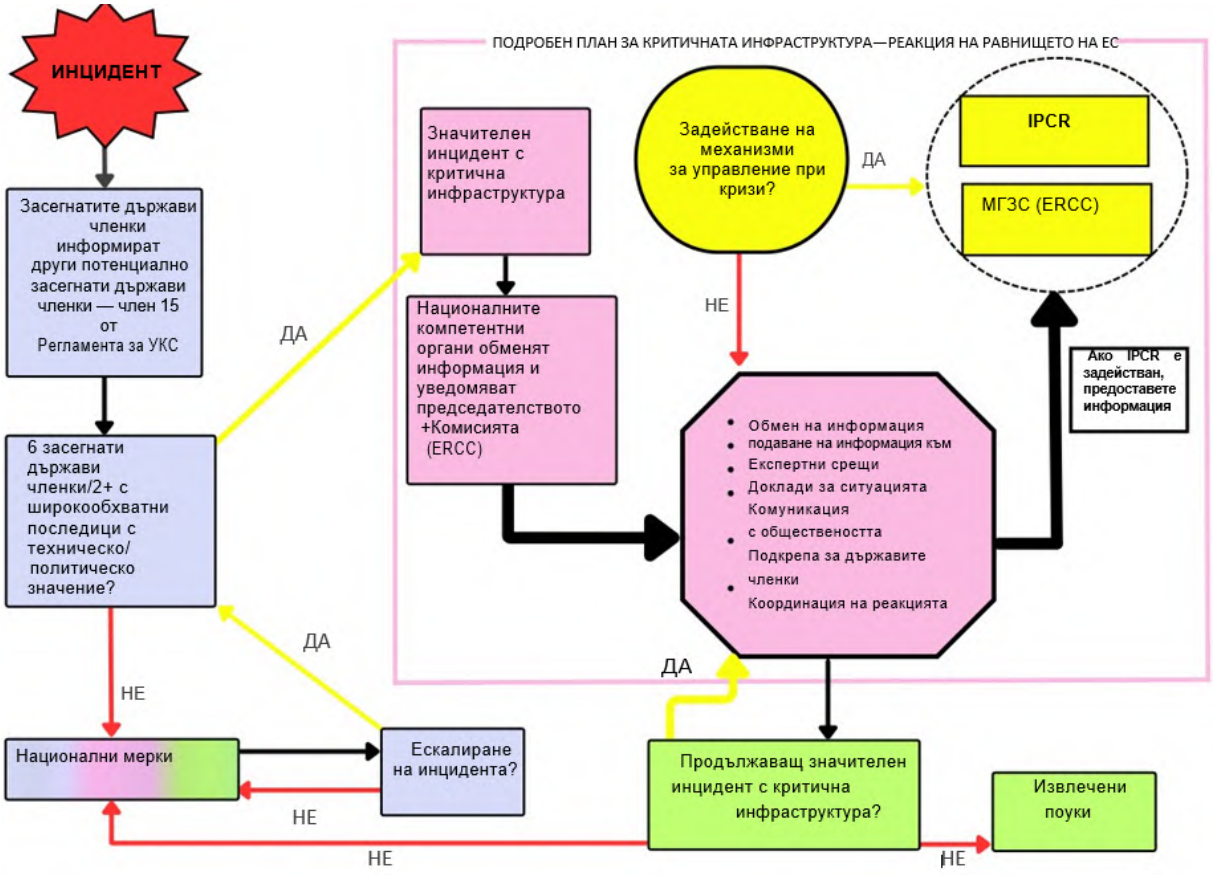
б) На политическо равнище

Председателството на Съвета би могло да прецени необходимостта от свикване на кръгли маси за IPCR, заседания на работните групи на Съвета, Корепер, Съвета и/или срещи на високо равнище за обмен на информация относно възможния произход и очакваните последици от значителния инцидент с критичната инфраструктура за държавите членки и за Съюза, за постигане на съгласие по общи насоки и за приемане на необходимите мерки за подпомагане на държавите членки, засегнати от значителния инцидент с критичната инфраструктура, и за смекчаване на последиците от него.

Диаграма 1: Схематичен преглед на подробния план за критичната инфраструктура



Диаграма 2: Вземане на решения в рамките на подробния план за критичната инфраструктура



ЛЕГЕНДА

Фази преди подробния план

Задействане на механизми за управление на кризи

Подробен план

Фази след подробния план