Съвет на
Европейския съюз

Брюксел, 6 юни 2025 г.
(OR. en)

9794/25

Междуинституционално досие:
2025/0036 (NLE)

CYBER 157
IPCR 42
RELEX 706
JAI 738
JAIEX 54
POLMIL 138
HYBRID 63
TELECOM 178
COSI 108

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
Дата:	6 юни 2025 г.
До:	Делегациите
Относно:	Препоръка на Съвета за концепция на ЕС относно управлението на кризи в областта на киберсигурността – Препоръка на Съвета, одобрена от Съвета на заседанието му от 6 юни 2025 г.

Приложено се изпраща на делегациите посочената по-горе препоръка на Съвета, одобрена от Съвета на заседанието му от 6 юни 2025 г.

ПРИЛОЖЕНИЕ

ПРЕПОРЪКА НА СЪВЕТА

за концепция на ЕС относно управлението на кризи в областта на киберсигурността

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взе предвид Договора за функционирането на Европейския съюз, и по-специално членове 114 и 292 от него,

като взе предвид предложението на Европейската комисия,

като има предвид, че:

(1) Цифровите технологии и глобалната свързаност са гръбнакът на икономическия растеж, конкурентоспособността и трансформацията на критичната инфраструктура на Съюза. Взаимосвързаната и все по-цифрова икономика все пак води и до увеличаване на риска от киберинциденти и кибератаки. Освен това увеличаването на геополитическото напрежение, конфликтите и стратегическото съперничество намира израз във въздействието, обема и сложността на злонамерените действия в киберпространството. Подобни действия могат да са част от хибридни кампании или военни операции. Те също така могат да засегнат пряко сигурността, икономиката и обществото на Съюза. Освен това те имат потенциал за разпространение, особено когато тези действия са насочени към държави — международни стратегически партньори, като държави кандидатки или съседни държави.

(2) Мащабен киберинцидент може да причини степен на смущение, надхвърляща способността на дадена държава членка да реагира на него, или да има значително въздействие върху повече от една държава членка. Такъв инцидент, в зависимост от неговата причина и въздействие, може да се разрасне и да се превърне в същинска криза, засягаща правилното функциониране на вътрешния пазар или представляваща сериозен риск за обществената сигурност и безопасност на субектите или гражданите в няколко държави членки или в Съюза като цяло. Ефективното управление на кризи е от съществено значение за поддържане на икономическата стабилност и защитата на европейските правителства, критичната инфраструктура, предприятията и гражданите, както и за приноса за международната сигурност и стабилност в киберпространството. Съответно управлението на киберкризи е неделима част от всеобхватната рамка на ЕС за управление на кризи.

(3) Като се имат предвид взаимозависимостите и взаимовръзките между ИКТ средата на субектите на Съюза и държавите членки, инцидент в субект на Съюза може да представлява риск за киберсигурността за държавите членки и обратно. Споделянето на съответната информация и координацията както по отношение на мащабни киберинциденти, така и по отношение на съществени инциденти, както са определени в член 3, точка 8 от Регламент (ЕС, Евратом) 2023/2841[1], е от решаващо значение в контекста на концепцията на ЕС относно управлението на кризи в областта на киберсигурността („концепцията за киберсигурността“).

[1] Регламент (ЕС, Евратом) 2023/2841 на Европейския парламент и на Съвета от 13 декември 2023 г. за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза (ОВ L, 2023/2841, 18.12.2023 г., стр. 1—27).

(4) В случай на криза, при която е задействана интегрирана политическа реакция на ЕС при криза (IPCR) съгласно Решение за изпълнение (ЕС) 2018/1993 на Съвета[2] („договореностите за IPCR“), концепцията за киберсигурността следва изцяло да е съобразена с договореностите за IPCR за координация и реакция. Политическата и стратегическата координация ще се осъществява в рамките на IPCR. Договореностите за IPCR са инструментът за хоризонтална координация и реакция на политическо равнище в Съюза. Съгласно договореностите за IPCR решението за задействане или прекратяване на IPCR се взема от председателството на Съвета на Европейския съюз. Докладите на интегрирания капацитет за ситуационна осведоменост и анализ (ISAA), изготвяни от службите на Комисията и Европейската служба за външна дейност (ЕСВД), подпомагат работата на IPCR както в режим за обмен на информация, така и в режим на пълно задействане.

(5) Държавите членки носят основната отговорност за управлението на киберинциденти и киберкризи. Потенциалният трансграничен и междусекторен характер на киберинцидентите обаче изисква държавите членки и съответните субекти на Съюза да си сътрудничат на техническо, оперативно и политическо равнище с цел ефективната им координация в рамките на Съюза. Управлението на киберкризи през целия цикъл включва подготвеност и споделена ситуационна осведоменост за предвиждане на мащабни киберинциденти, необходимите способности за откриване с цел установяване на необходимите инструменти за реакция и възстановяване за целите на смекчаването и овладяването на мащабни киберинциденти, както и способности за реагиране с цел избягване и предотвратяване на по-нататъшни инциденти.

[2] Решение за изпълнение (ЕС) 2018/1993 на Съвета от 11 декември 2018 г. относно договорености за интегрирана реакция на ЕС при политическа криза (ОВ L 320, 17.12.2018 г., стр. 28—34).

(6) В Препоръка (ЕС) 2017/1584 на Комисията[3] относно координирана реакция на мащабни киберинциденти и кризи се определят целите и способите на сътрудничеството между държавите членки и субектите на Съюза при реагиране на мащабни киберинциденти и киберкризи. В нея се обозначават съответните участници на техническо, оперативно и политическо равнище и се обяснява начинът, по който те са включени в съществуващите механизми на Съюза за управление на кризи, като договореностите за IPCR. Основните принципи, изложени в Препоръка (ЕС) 2017/1584, остават валидни, а именно субсидиарност, взаимно допълване и поверителност на информацията, както и подходът на три равнища (техническо, оперативно и политическо). Настоящата препоръка се основава на тези основни принципи и има за цел да замени Препоръка (ЕС) 2017/1584, като определи нова рамка на Съюза за управление на кризи в областта на киберсигурността.

(7) Някои определения, използвани в настоящата препоръка, се основават на определенията и термините, използвани в Директива (ЕС) 2022/2555[4]. Обхватът на настоящата препоръка обаче е различен от обхвата на Директива (ЕС) 2022/2555. С настоящата препоръка се определя рамката на Съюза за управление на киберкризи в контекста на цялостната подготвеност на ЕС за мащабни киберинциденти и киберкризи, произтичащи от такива инциденти — независимо от засегнатия сектор или субект. Доколкото е възможно, определенията се основават на определенията, съдържащи се в Директива (ЕС) 2022/2555.

---

[3] 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—58).

[4] 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 (Директива МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80—152).

(8) Необходима е актуализирана концепция за киберсигурността, за да се предоставят ясни и достъпни насоки, обясняващи какво представлява мащабен киберинцидент или киберкриза на равнището на Съюза, как се задейства рамката за управление на кризи и какви са ролите на съответните мрежи, участници и механизми на равнището на Съюза, както и взаимодействието между тези участници и механизми през целия цикъл на киберкризата. Концепцията за киберсигурността има за цел да подкрепи по-широката рамка на гражданско-военните отношения на ЕС в контекста на управлението на киберкризи, включително на фона на задълбочаването на отношенията между ЕС и НАТО, когато е възможно включително чрез приобщаващи, реципрочни и недискриминационни подобрени механизми за обмен на информация при управлението на киберкризи.

(9) Междусекторното управление на кризи на равнището на Съюза следва да бъде засилено, за да се даде възможност за интегрирана реакция при кризи, особено в случаите, когато мащабни киберинциденти и кризи пораждат физически последици. Настоящата препоръка допълва договореностите за IPCR и други механизми на Съюза за управление на кризи, включително общата система за бързо предупреждение ARGUS на Комисията, Механизма за гражданска защита на Съюза (МГЗС), подпомаган от Координационния център за реагиране при извънредни ситуации (ERCC), създаден в рамките на МГЗС с Решение № 1313/2013/ЕС на Европейския парламент и на Съвета относно Механизъм за гражданска защита на Съюза[5] (решение за МГЗС), механизма на ЕСВД за реакция при кризи (CRM), както и други процеси, като например описаните в инструментариума на ЕС за кибердипломация[6], инструментариума срещу хибридните заплахи[7] и преразгледания Протокол на ЕС за борба с хибридните заплахи[8]. Тя също така допълва и следва да бъде съгласувана с Препоръка (ЕС) 2024/4371 на Съвета относно подробен план за координиран отговор на равнището на Съюза на смущения в критичната инфраструктура със значително трансгранично значение[9] („подробен план на ЕС за критичната инфраструктура“), който обхваща физическата устойчивост, която не е свързана с киберсигурността, и има за цел да подобри координацията на реакцията на равнището на Съюза в тази област.

---

5 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—947).

6 Заключения на Съвета относно разработването на рамка за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството (9916/17).

7 Заключения на Съвета относно рамка за координиран отговор на ЕС на хибридни кампании, 22 юни 2022 г.

8 Съвместен работен документ на службите на Комисията — Протокол на ЕС за борбата с хибридните заплахи (SWD(2023) 116 final).

9 ОВ C, C/2024/4371, 5.7.2024 г.

(10) Европейската мрежа за връзка на организациите при киберкризи (EU-CyCLONe) е мрежата за координация на управлението на мащабни киберинциденти и кризи на оперативно равнище и в случай на междусекторни мащабни киберинциденти и киберкризи. За да не се усложняват допълнително съществуващите рамки, следва да се избягва създаването на секторни структури, които биха дублирали задачите на EU-CyCLONe. EU-CyCLONe следва да получава оперативна информация, свързана с киберсигурността, също и от секторите, и да я подава на политическото равнище.

(11) Държавите членки се насърчават да използват пълноценно наличните финансови ресурси за киберсигурност, предоставени по линия на съответните програми на Съюза. Следва да се гарантира, че тези програми налагат минимална административна тежест на кандидатите за финансиране, а участието на държавите членки в тези програми се улеснява чрез предоставяне на подходящи насоки за жизнеспособни възможности за финансова подкрепа.

(12) Настоящата препоръка допринася за по-широки действия за подготвеност, необходими на Съюза в контекста на междусекторни кризи, в съответствие с принципите, залегнали в стратегията на ЕС за Съюз на подготвеност, а именно интегриран подход, обхващащ всички опасности, всички равнища на управление и цялото общество, по-специално по отношение на подобряването на осведомеността за рисковете и заплахите и междусекторната реакция при кризи,

ПРИЕ НАСТОЯЩАТА ПРЕПОРЪКА:

I: Цел, обхват и ръководни принципи на рамката на ЕС за управление на киберкризи

Цел и обхват

(1) С настоящата препоръка за концепция на ЕС относно управлението на киберкризи („концепция за киберсигурността“) се определя рамката на Съюза за управление на киберкризи в контекста на цялостната подготвеност на ЕС за мащабни киберинциденти и киберкризи. Рамката отразява ролите както на държавите членки, така и на институциите, органите, службите и агенциите на Съюза („субектите на Съюза“) в рамките на съответната им компетентност, при пълно зачитане на националното право и вътрешните правила, за да се гарантират всеобхватни и координирани действия на равнището на Съюза.

(2) Концепцията за киберсигурността следва да се прилага в съответствие с подробния план на ЕС за критичната инфраструктура, по-специално в случай на инциденти, засягащи както физическата устойчивост, така и киберсигурността на критичната инфраструктура[10].

(3) В концепцията за киберсигурността се предоставят насоки за реагиране при мащабни киберинциденти или киберкризи и тя следва да се използва в допълнение към всички съответни секторни механизми за реагиране, като например изброените в приложение II. Съответните заинтересовани страни в областта на киберсигурността следва да помагат и да съдействат за постигането на целите на въпросните секторни механизми както на национално, така и на съюзно равнище.

(4) В случай на междусекторна криза в целия ЕС с кибераспекти, за които се задейства IPCR, координацията на реакцията на политическо равнище на Съюза следва да се извършва от Съвета, като се използват договореностите за IPCR. Когато се задейства IPCR, мерките в рамките на концепцията за киберсигурността следва да подкрепят реакцията на ЕС на политическо равнище, като предоставят специфична подкрепа в областта на киберсигурността.

[10] Координацията в такива случаи се уточнява допълнително в част I, раздел 4 от приложението към подробния план на ЕС за критичната инфраструктура.

Ръководни принципи

(5) По отношение на управлението на киберкризи на равнището на Съюза се прилагат следните ръководни принципи:

а) *Пропорционалност*: повечето киберинциденти, засягащи държавите членки, попадат в обхвата на това, което може да се счита за национален или съюзен мащабен киберинцидент или киберкриза. В случай на киберинциденти и заплахи държавите членки си сътрудничат и обменят информация доброволно и редовно в рамките на мрежата от екипи за реагиране при инциденти с компютърната сигурност („мрежата на ЕРИКС“) и EU-CyCLONe в съответствие със стандартните оперативни процедури (СОП) на мрежите.

б) *Субсидиарност*: Държавите членки носят основната отговорност за реакцията и коригиращите действия при засягащ ги киберинцидент, мащабен киберинцидент или киберкриза. С оглед на потенциалните трансгранични последици Съветът, Комисията, върховният представител, Агенцията на Европейския съюз за киберсигурност (ENISA), Службата за киберсигурност за институциите, органите, службите и агенциите на Съюза (CERT-EU), Европол и всички други съответни субекти на Съюза следва да си сътрудничат през целия цикъл на кризата. Тази роля произтича от правото на Съюза и отразява начина, по който мащабните киберинциденти и киберкризи оказват въздействие върху един или повече сектори на икономическата дейност на единния пазар, върху сигурността и международните отношения на Съюза, както и върху самите субекти.

в) *Взаимно допълване*: в настоящата препоръка се отчитат изцяло съществуващите механизми за управление на кризи на равнището на Съюза, изброени в приложение II, по-специално договореностите за IPCR, ARGUS и механизма на ЕСВД за реагиране при кризи. В настоящата препоръка се вземат предвид правомощията на мрежата на ЕРИКС и EU-CyCLONe, както и Регламент (ЕС, Евратом) 2023/2841. Когато се задейства IPCR, работата на съответните мрежи, субекти и задействани секторни механизми следва да продължи и следва да допринася за политическата и стратегическата координация, която се осъществява в рамките на IPCR, и да я подкрепя.

г) *Поверителност на информацията*: всеки обмен на информация в контекста на настоящата препоръка следва да отговаря на приложимите правила за сигурност и защита на личните данни. Когато е целесъобразно, следва да се вземат предвид неформалните споразумения за неразкриване на информация, като например протокола за обмен на информация с цветен код за поверителност (Traffic Light Protocol) за обозначаване на чувствителна информация. За обмена на класифицирана информация, независимо от прилаганата схема за класифициране, следва да се използват съществуващите задължителни правила и споразумения относно обработката на класифицирана информация заедно с наличните акредитирани инструменти.

(6) В съответствие с посочените по-горе ръководни принципи държавите членки и субектите на Съюза следва да задълбочат сътрудничеството си при управлението на киберкризи, като насърчават взаимното доверие и се опират на съществуващите мрежи и механизми. За това сътрудничество, в рамките на концепцията за киберсигурността, допринася прилагането на членове 22 и 23 от Регламент (ЕС, Евратом) 2023/2841. По-специално планът за управление на киберкризи, изготвен въз основа на член 23 от Регламент (ЕС, Евратом) 2023/2841, наред с другото, спомага за редовния обмен на съответна информация между субектите на Съюза и с държавите членки и определя договореностите относно координацията и информационния поток между субектите на Съюза.

II: Определения

(7) За целите на настоящата концепция за киберсигурността се прилагат следните определения:

а) „инцидент“ означава събитие, което засяга отрицателно наличността, автентичността, цялостността или поверителността на съхранявани, пренасяни или обработвани данни или на услугите, предлагани или достъпни чрез мрежови и информационни системи;

б) „значителен инцидент“ означава инцидент, който:

а. е причинил или е в състояние да причини сериозно оперативно смущение в услугите или финансова загуба за засегнатия субект;

б. е засегнал или може да засегне други физически или юридически лица, като причини значителни имуществени или неимуществени вреди;

в) „мащабен киберинцидент“ означава инцидент, който причинява степен на смущение, надхвърляща способността на дадена държава членка да реагира на него, или който има значително въздействие върху най-малко две държави членки;

г) „киберкриза“ означава мащабен киберинцидент, разраснал се до същинска криза, непозволяваща правилното функциониране на вътрешния пазар или представляваща сериозен риск за обществената сигурност и безопасност на субектите или гражданите в няколко държави членки или в Съюза като цяло.

III. Национални структури и отговорности за управление на киберкризи

(8) Държавите членки носят основната отговорност за реакцията при мащабни киберинциденти или киберкризи, които ги засягат. Всяка държава членка, в съответствие с Директива (ЕС) 2022/2555, има един или повече органи за управление на киберкризи, както и един или повече ЕРИКС.

(9) С приемането на Директива (ЕС) 2022/2555 и други законодателни и незаконодателни инструменти в областта на киберсигурността държавите членки привеждат в съответствие своите рамки за киберсигурност чрез определяне на минимални правила за функционирането на координираната регулаторна рамка, определяне на механизми за ефективно сътрудничество между отговорните органи във всяка държава членка и осигуряване на ефективни средства за правна защита и мерки за правоприлагане, които са от ключово значение за ефективното изпълнение на посочените задължения.

(10) В съответствие с член 9, параграф 4 от Директива (ЕС) 2022/2555 държавите членки следва да приемат национални планове за реакция при мащабни киберинциденти и кризи. Тези планове включват, наред с другото, национални мерки за подготвеност, процедури за управление на киберкризи и национални процедури и договорености между националните органи и служби, за да се гарантира ефективното им участие и подкрепата им за координираното управление на мащабни киберинциденти и киберкризи на равнището на Съюза. Процедурите за управление на киберкризи включват и разпоредби за тяхното интегриране в общата рамка за управление на кризи на национално равнище и канали за обмен на информация.

(11) В съответствие с член 9, параграф 1 от Директива (ЕС) 2022/2555 държавите членки следва да гарантират съответствие със съществуващите рамки за общото управление на кризи на национално равнище. В случай на задействане на IPCR националните органи за управление на кризи следва, с цел информиране на IPCR, да събират информация от органите за управление на киберкризи и националните секторни механизми за управление на кризи.

(12) В съответствие с член 9, параграф 5 от Директива (ЕС) 2022/2555, по искане на засегната държава членка, EU-CyCLONe следва да обменя информация за съответните части от националните планове за реакция при мащабни киберинциденти и кризи, по-специално относно разпоредбите за гарантиране на ефективно участие и подкрепа на координираното управление на мащабни киберинциденти и киберкризи на равнището на Съюза с цел обмен на най-добри практики и преценка дали цялостната рамка ще функционира на практика.

(13) EU-CyCLONe и Междуинституционалният съвет по киберсигурност (МСК) се приканват да обменят информация, когато е целесъобразно, за съгласуваността на плана за управление на кризи, изготвен от МСК в съответствие с член 23 от Регламент (ЕС, Евратом) 2023/2841, с националните планове за реакция при мащабни киберинциденти и кризи.

(14) EU-CyCLONe, с подкрепата на ENISA в качеството ѝ на секретариат, следва да поддържа актуализиран списък на националните органи за управление на киберкризи с данни за контакт на длъжностните лица и изпълнителните служители на EU-CyCLONe и да го предоставя на членовете на EU-CyCLONe.

IV: Основни мрежи и участници в екосистемата на ЕС за управление на киберкризи

(15) Мрежата на ЕРИКС е основната техническа мрежа за обмен на съответна информация за инциденти, по-специално в обхвата на настоящата препоръка, съгласно съответните задачи, описани в член 15, параграф 3 от Директива (ЕС) 2022/2555. Тя допринася за изграждането на доверие между държавите членки и насърчава бързото и ефективно оперативно сътрудничество между държавите членки. Председателят на мрежата на ЕРИКС може да участва като наблюдател в МСК.

(16) CERT-EU е службата в областта на киберсигурността за всички субекти на Съюза. CERT-EU действа като координационен център за обмен на информация в областта на киберсигурността и за реагиране при инциденти за субектите на Съюза в съответствие с член 13 от Регламент (ЕС) 2023/2841. CERT-EU е член на мрежата на ЕРИКС и подпомага Комисията в EU-CyCLONe. CERT-EU функционира на техническо равнище и отговаря за координирането на управлението на съществени инциденти, засягащи субекти на Съюза.

(17) EU-CyCLONe работи като посредник между техническото и политическото равнище, по-специално по време на мащабни киберинциденти и киберкризи. Тази мрежа подкрепя координираното управление на мащабни киберинциденти и киберкризи на оперативно равнище и гарантира редовен обмен на съответната информация между държавите членки и институциите, органите, службите и агенциите на Съюза в съответствие с член 16 от Директива (ЕС) 2022/2555. Председателят на EU-CyCLONe може да участва като наблюдател в МСК.

(18) ENISA е агенцията на Съюза, изпълняваща задачите, възложени съгласно Регламент (ЕС) 2019/881[11], с цел постигане на високо общо ниво на киберсигурност в целия Съюз, включително чрез активна подкрепа за държавите членки и институциите, органите и агенциите на Съюза. ENISA осигурява, наред с другото, секретариата на мрежата на ЕРИКС и EU-CyCLONe, услугите за ситуационна осведоменост и подпомага държавите членки, като редовно организира учения в областта на киберсигурността на равнището на Съюза. В съответствие с Директива (ЕС) 2022/2555 и Регламент (ЕС) 2024/2847[12] ENISA получава информация за значителни трансгранични инциденти и активно използвани уязвимости, и за инциденти, засягащи цифрови продукти.

(19) Съветът на Европейския съюз (Съветът) е институцията с функции по определяне на политиките и координиране съгласно член 16 от Договора за Европейския съюз (ДЕС) и е натоварен с IPCR, тъй като IPCR се отнася до координацията и реакцията на политическо равнище на Съюза. Съветът действа чрез съставите на Съвета, Комитета на постоянните представители и съответните подготвителни органи на Съвета, по-специално Хоризонталната работна група по въпроси на кибернетичното пространство (HWPCI), както и когато е приложимо, чрез договореностите за IPCR.

---

11 Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15—69).

12 Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета от 23 октомври 2024 г. относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост) (ОВ L, 2024/2847, 20.11.2024 г., стр. 1—81).

(20) Комисията, в качеството си на институция, която отстоява общия интерес на Съюза и предприема подходящи инициативи за тази цел и която следи за прилагането на Договорите и на мерките, приети от институциите съгласно член 17 от ДЕС, отговаря за някои общи действия за подготвеност на равнището на Съюза и за определени действия за ситуационна осведоменост, включително управлението на ERCC и на Общата система за комуникация и информация при извънредни ситуации (CECIS), в съответствие с Решението за МГЗС. Тя улеснява съгласуваността и координацията на оперативно равнище между съответните действия на равнището на Съюза за реакция при кризи. С нея се провеждат консултации при решения за задействане или прекратяване на IPCR. Службите на Комисията, заедно с ЕСВД, изготвят докладите ISAA. Тя е член на EU-CyCLONe в случаите, когато потенциален или текущ мащабен киберинцидент има или е вероятно да окаже значително въздействие върху услугите и дейностите, попадащи в обхвата на Директива (ЕС) 2022/2555, и е наблюдател в останалите случаи. Тя е звеното за контакт на EU-CyCLONe в МСК. Наблюдател е в мрежата на ЕРИКС.

(21) Върховният представител по въпросите на външните работи и политиката на сигурност (върховният представител), подпомаган от ЕСВД, ръководи общата външна политика и политика на сигурност (ОВППС) на Съюза и допринася с предложенията си за развитието на тази политика, включително на общата политика за сигурност и отбрана (ОПСО). Това включва дипломатически, разузнавателни и военни структури и механизми, по-специално единното звено за анализ на разузнавателна информация (SIAC) като единна входна точка за разузнавателни данни на държавите членки, Военния секретариат на ЕС (ВСЕС) като източник на военен експертен опит, инструментариума на ЕС за кибердипломация, както и мрежата от делегации на ЕС, които могат да допринесат за управлението на кризи от външно измерение. ЕСВД също така изготвя заедно с Комисията докладите ISAA.

(22) В приложение II се описват ролите и компетентностите на съответните участници на равнището на Съюза във връзка с управлението на киберкризи, включително основните мрежи и участници.

V: Подготовка за мащабни киберинциденти и киберкризи

Картографиране на заплахите

(23) Държавите членки и съответните субекти на Съюза следва да предприемат необходимите мерки за подобряване на ситуационната осведоменост, като приемат, че картината на заплахите и ситуационната осведоменост за специфични инциденти изискват отделни режими на работа. Държавите членки и съответните субекти на Съюза следва да работят заедно въз основа на проверени и надеждни данни, включително тенденции при инцидентите, тактики, техники и процедури, и на активно използвани уязвимости.

(24) При споделяне на информация на равнището на ЕС държавите членки следва да използват пълноценно съществуващите платформи за техническо и оперативно сътрудничество, като например използваните от мрежата на ЕРИКС и EU-CyCLONe.

(25) За да се подобри споделената ситуационна осведоменост и да се улесни оценката на въздействието на ЕС, EU-CyCLONe и мрежата на ЕРИКС, с подкрепата на ENISA, следва да използват вътрешно договорен механизъм за докладване, за да изготвят обзор на ЕС на техническите и оперативните дейности въз основа на информацията, събрана на национално равнище.

(26) EU-CyCLONe и мрежата на ЕРИКС следва:

а) да си сътрудничат за подобряване на обмена на информация между техническото и оперативното равнище и на ситуационната осведоменост като цяло;

б) да продължат да изграждат климат на доверие между своите членове и между мрежите;

в) да използват пълноценно наличните инструменти за обмен на информация с подкрепата на ENISA, да обмислят начините за подобряване на тези инструменти и да осигурят оперативната съвместимост на мрежите.

(27) EU-CyCLONe, мрежата на ЕРИКС и МСК следва да си сътрудничат, за да се гарантира ефективен обмен на съответна информация.

(28) ENISA, в качеството си на секретариат на мрежата на ЕРИКС и EU-CyCLONe, играе централна роля в подпомагането на държавите членки и институциите, органите и агенциите на Съюза за постигане на обща ситуационна осведоменост в рамките на ЕС на техническо и оперативно равнище в подкрепа на подготовката за мащабни киберинциденти и кризи.

(29) В съответствие с Директива (ЕС) 2022/2555 и Регламент (ЕС) 2019/881 държавите членки и съответните субекти на Съюза следва да се координират с частния сектор, включително общностите с отворен код и производителите, за да се подобри обменът на информация. По-специално ENISA следва да използва своята програма за партньорство в това отношение. Освен това държавите членки и съответните субекти на Съюза биха могли също да надграждат въз основа на съществуващите центрове за обмен и анализ на информация (ISAC) на европейско и национално равнище, за да увеличат капацитета в областта на киберсигурността и да реагират на киберинциденти, включително чрез съвместни срещи на частния сектор с EU-CyCLONe или мрежата на ЕРИКС.

(30) За да се подобри обменът на информация в рамките на мрежите и между тях и да се изяснят взаимните очаквания за подобен обмен, EU-CyCLONe, с подкрепата на ENISA като секретариат и след консултация с мрежата на ЕРИКС и групата за сътрудничество за МИС, следва, в срок от 24 месеца от приемането на настоящата препоръка, да постигне съгласие по обща съгласувана таксономия на нивата на сериозност на инцидентите. Тази таксономия следва да даде възможност за сравнение на сериозността на инцидентите в държавите членки, като се вземат предвид въздействието върху предоставянето на услуги, броят на засегнатите субекти и съответната им значимост, въздействието върху други услуги и инфраструктура, както и причинените парични, репутационни и политически вреди. Тя следва да се основава на съответните съществуващи скали или таксономии, като например таксономията за класифициране на инцидентите.

Техническо равнище

(31) Мрежата на ЕРИКС е платформата за техническо сътрудничество и обмен на информация между всички държави членки и чрез CERT-EU със субектите на Съюза.

(32) В съответствие с Директива (ЕС) 2022/2555 всеки ЕРИКС има за задача да наблюдава и анализира киберзаплахите, уязвимостите и инцидентите на национално равнище. ЕРИКС следва да обменят, както в рамките на мрежата на ЕРИКС, така и на двустранна основа, подходяща информация за инциденти, близки до инцидент положения, киберзаплахи, рискове и уязвимости, за да се постигне споделена ситуационна осведоменост.

(33) За да се засили оперативното сътрудничество на равнището на Съюза, мрежата на ЕРИКС следва да обмисли възможността да покани органи и агенции на Съюза, участващи в политиката в областта на киберсигурността, като например Европол, да участват в нейната работа.

(34) В съответствие с Регламент (ЕС, Евратом) 2023/2841 CERT-EU следва да събира, управлява, анализира и споделя информация с институциите, органите, службите и агенциите на Съюза относно киберзаплахи, уязвимости и инциденти в некласифицираната инфраструктура на ИКТ и когато е необходимо, да отправя конкретни предложения до МСК за насоки и препоръки към институциите, органите, службите и агенциите на Съюза. CERT-EU следва да си сътрудничи и да обменя информация с партньорите от държавите членки, включително чрез мрежата на ЕРИКС.

Оперативно равнище

(35) В съответствие с Директива (ЕС) 2022/2555 EU-CyCLONe следва да служи като платформа за сътрудничество между органите на държавите членки за управление на киберкризи и чрез Комисията със съответните субекти на Съюза с цел повишаване на равнището на подготвеност при управлението на мащабни киберинциденти и киберкризи и развиване на споделена ситуационна осведоменост за мащабни киберинциденти и киберкризи.

(36) В съответствие с Директива (ЕС) 2022/2555 и Регламент (ЕС) 2024/2847 ENISA получава информация за значителни трансгранични инциденти и активно използвани уязвимости и за инциденти, засягащи цифрови продукти. ENISA, която действа като секретариат, следва да предоставя съвети на мрежата на ЕРИКС и EU-CyCLONe с цел подпомагане на мрежите при решаването дали да се предприемат по-нататъшни действия и следва да допринася за споделената ситуационна осведоменост.

Политическо равнище

(37) Държавите членки и имащите отношение субекти на Съюза следва да наблюдават международните събития, които засягат киберсигурността (включително киберзаплахите, хибридните заплахи и чуждестранното манипулиране на информация и вмешателство (FIMI), включително дезинформацията, когато е уместно). Следва да се вземат предвид инициативи като съвместните доклади за кибероценка (JCAR), предоставените от SIAC анализи и други продукти от значение, предоставящи специализирана информация.

(38) Върховният представител следва да продължи да информира и да включва държавите членки в дипломатическите усилия на Съюза, свързани с киберзаплахите, особено в онези усилия, които включват държавни участници, ангажираността му с трети държави и международни организации, в т.ч. НАТО, и прилагането на дипломатически мерки, в т.ч. ограничителни мерки.

(39) Председателството на Съвета на Европейския съюз може да инициира страница за наблюдение на уебплатформата на IPCR, на която държавите членки и институциите и органите на ЕС могат да обменят информация относно евентуално развиваща се криза.

Общи учения

(40) В координация с върховния представител и подпомагана от ENISA, след консултация с EU-CyCLONe и мрежата на ЕРИКС, Комисията следва да изготви ефективна годишна постоянна програма за киберучения с цел подготовка за киберкризи и повишаване на организационната ефективност. В постоянната програма за киберучения следва да се вземат предвид ученията по Механизма за гражданска защита на Съюза (МГЗС) и други учения по механизми за реакция при кризи на равнището на Съюза, включително учението, очертано в подробния план на ЕС за критичната инфраструктура. Първата постоянна програма следва да бъде разработена в срок от 12 месеца след приемането на концепцията за киберсигурността, като последващите програми трябва да бъдат завършвани до 31 март всяка година. Постоянната програма следва да бъде представена на Съвета за информация.

(41) Постоянната програма следва да включва и учения, разработени въз основа на координирани от ЕС сценарии за оценки на риска. Тя следва да обхваща учения, в които са включени всички имащи отношение участници, по-специално частния сектор и НАТО.

(42) В ролята си на секретариат на мрежата на ЕРИКС и EU-CyCLONe, ENISA следва да гарантира систематичното събиране на поуки, извлечени от ученията, както и определянето и предлагането на начини за изпълнение на произтичащите от тях действия, за да се гарантира тяхното ефективно изпълнение и положително въздействие върху общата устойчивост на ЕС, включително съответните СОП.

(43) Всички участници и мрежи следва да подобрят координацията в случай на мащабен киберинцидент или киберкриза въз основа на поуките, извлечени от ученията. По-специално EU-CyCLONe и мрежата на ЕРИКС следва да се справят с установените по време на ученията предизвикателства, за да се подобри координацията, като се обърне по-специално внимание на предизвикателствата, свързани със сътрудничеството между мрежите, и ако е необходимо, СОП следва бързо да се адаптират.

(44) Групата за сътрудничество за МИС следва да покани мрежата на ЕРИКС, EU-CyCLONe и ENISA да представят поуките, извлечени от ученията, както и определянето на произтичащите от тях действия и предложения начин за изпълнението им.

(45) Съветът може да покани председателите на мрежата на ЕРИКС, EU-CyCLONe, групата за сътрудничество за МИС и ENISA да представят как са били приложени извлечените от ученията поуки.

(46) ENISA, в сътрудничество с Комисията и върховния представител, се приканва да организира учение за тестване на концепцията за киберсигурността по време на следващото учение „Cyber Europe“. Учението следва да включва всички имащи отношение участници, включително политическото равнище. ENISA се приканва да координира с председателството на Съвета на Европейския съюз участието на политическото равнище. Учението може да включва също така частния сектор и НАТО.

VI: Откриване на инцидент, който би могъл да се разрасне до мащабен киберинцидент или киберкриза

(47) Съгласно съответните си правомощия и въз основа на подхода, обхващащ всички опасности, всички участници следва да предоставят на съответните мрежи информация, показваща потенциален мащабен киберинцидент или киберкриза.

(48) В съответствие с Регламент (ЕС) 2025/38[13], когато трансграничните киберхъбове получат информация, свързана с потенциален или текущ мащабен киберинцидент, за целите на общата ситуационна осведоменост те следва да гарантират, че имащата отношение информация се предоставя своевременно на органите на държавите членки и на Комисията чрез EU-CyCLONe и мрежата на ЕРИКС.

[13] Регламент (ЕС) 2025/38 на Европейския парламент и на Съвета от 19 декември 2024 г. за определяне на мерки за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти, и за изменение на Регламент (ЕС) 2021/694 (Законодателен акт в областта на киберсолидарността) (ОВ L, 2025/38, 15.1.2025 г., ELI: http://data.europa.eu/eli/reg/2025/38/oj).

(49) Когато се наблюдава значителен инцидент, по-специално причиняващ непосредствено въздействие, той може да бъде съобщен на ЕРИКС или открит от него, както и от органите за управление на киберкризи на държавите членки или от други секторни органи. Държавите членки се насърчават да обменят информация, свързана с такъв инцидент, в рамките на мрежите, в които следва да се обмисли предприемането на подходящи действия. Задействането на мрежата на ЕРИКС и EU-CyCLONe може да бъде независимо едно от друго в зависимост от естеството на инцидента и необходимата реакция. И двете мрежи обаче се насърчават да продължат сътрудничеството помежду си въз основа на договорени процедурни правила. Решението за задействане се взема единствено и независимо от всяка съответна мрежа.

(50) Мрежата на ЕРИКС следва да консултира EU-CyCLONe относно това дали наблюдаван киберинцидент може да се счита за потенциален или текущ мащабен киберинцидент.

(51) Както е посочено в Директива (ЕС) 2022/2555, мрежата на ЕРИКС и EU-CyCLONe следва незабавно да установят процедурни правила в случай на потенциален или текущ мащабен киберинцидент, за да осигурят техническо-оперативна координация и навременна и подходяща информация за политическото равнище.

VII: Реагиране на мащабен киберинцидент или киберкриза на равнището на Съюза

Реакция при мащабен киберинцидент или киберкриза, за които IPCR не е в режим на пълно задействане

(52) Ефективната реакция на мащабни киберинциденти или киберкризи на равнището на ЕС зависи от ефективното техническо, оперативно и политическо сътрудничество в рамките на подход, който обхваща всички нива на управление, включително правоприлагането, когато е възможно.

(53) На всяко ниво участниците следва да извършват конкретни дейности за постигане на споделена ситуационна осведоменост и координирана реакция. Тези мерки гарантират правилното и ефективно разпространение на информацията.

(54) Реакцията следва да бъде съобразена с въздействието на мащабния киберинцидент или киберкриза. В съответствие с Директива (ЕС) 2022/2555 органите на държавите членки за управление на киберкризи следва да осигурят съгласуваност и координация на национално равнище между секторните действия в отговор на киберкризата.

(55) В случай на мащабен киберинцидент или киберкриза всички участници и мрежи следва да реагират в тясна координация, както следва:

а) на техническото равнище:

i. Засегнатите държави членки и техните ЕРИКС следва да си сътрудничат със засегнатите субекти, за да реагират на инциденти и да предоставят помощ, когато е приложимо;

ii. ЕРИКС следва да си сътрудничат чрез мрежата на ЕРИКС за споделяне на подходящата техническа информация за инцидента; ЕРИКС си сътрудничат в усилията си да анализират наличните технически артефакти и друга техническа информация, свързана с инцидента, с оглед на определяне на причините и възможните технически мерки за смекчаване на последиците;

iii. Когато ЕРИКС или орган за управление на киберкризи на държава членка узнае за значителен инцидент, те се насърчават да споделят информацията в рамките на мрежата на ЕРИКС или EU-CyCLONe.

iv. Мрежата на ЕРИКС, с подкрепата на ENISA, следва да изготви обобщение на националните доклади, предоставяни от ЕРИКС, което следва да бъде представено на EU-CyCLONe;

v. Когато даден киберинцидент има потенциала да се разрасне до мащабен киберинцидент или киберкриза, мрежата на ЕРИКС следва да сподели подходящата информация с EU-CyCLONe. EU-CyCLONe следва да използва тази информация, за да уведоми накратко Съвета;

vi. Мрежата на ЕРИКС следва да бъде в тесен контакт с Европол, за да се гарантира обменът на подходящата техническа информация. Мрежата на ЕРИКС и Европол следва да създадат звена за контакт за подобряване на обмена на информация, когато е уместно в случай на мащабен киберинцидент;

б) на оперативното равнище:

i. Държавите членки следва да смекчат въздействието на инцидента на национално равнище, като използват подходящи мерки;

ii. Мрежата на ЕРИКС следва да предоставя на EU-CyCLONe технически оценки на текущите инциденти, които могат да се използват от EU-CyCLONe;

iii. EU-CyCLONe следва да оценява последиците и въздействието на съответните мащабни киберинциденти и киберкризи и да предлага възможни мерки за смекчаване на последиците, и да подкрепя координираното управление на мащабни киберинциденти и киберкризи, както и да подпомага вземането на решения на политическо равнище;

iv. Ако мащабен киберинцидент с междусекторно въздействие изисква активирането на действия за реагиране на равнището на Съюза, по-специално съответните хоризонтални и секторни механизми за управление на кризи на равнището на Съюза, изброени в приложение II,

(a) в зависимост от вида на секторните механизми за управление на кризи на равнището на Съюза, съответните участници могат да призоват за задействане на посочения механизъм;

(b) в случай на задействане на такъв секторен механизъм съответните субекти подкрепят секторните субекти за смекчаване на въздействието на инцидента;

(c) Комисията следва да улесни потока от необходимата информация между звената за контакт за съответните хоризонтални и секторни механизми при кризи на равнището на Съюза, изброени в приложение II, и EU-CyCLONe, и следва да се стреми към интегриран междусекторен анализ и да предлага варианти за подходящ интегриран план за реагиране;

(d) в сътрудничество с върховния представител, когато е целесъобразно чрез EU-CyCLONe, Комисията следва да гарантира съгласуваност и координация на оперативните мерки на равнището на ЕС в киберпространството със съответните действия за реакция на равнището на Съюза, по-специално във връзка с исканията за помощ чрез МГЗС;

(e) ако е създадена страница за наблюдение на IPCR, информацията за инцидента, за неговото въздействие и за предприетите мерки следва да се споделя и сред държавите членки и субектите на Съюза чрез уебплатформата на IPCR;

v. Държавите членки могат да поискат услуги от Резерва за киберсигурност на ЕС съгласно член 15 от Регламент (ЕС) 2025/38. Без да се засягат бъдещи актове за изпълнение съгласно посочения регламент, услугите на Резерва за киберсигурност на ЕС следва да бъдат разгърнати в рамките на 24 часа от искането.

в) на политическото равнище:

i. Съветът може да поиска брифинги от основните заинтересовани страни, по-специално Комисията, върховния представител и EU-CyCLONe, с цел осигуряване на подходяща политическа и стратегическа реакция;

ii. Подкрепян от Комисията и върховния представител, Съветът би могъл да вземе решение относно подходящите мерки за реагиране на мащабния киберинцидент, включително относно възможните дипломатически отговори в съответствие с глава IX;

iii. Държавите членки могат да задействат допълнителни механизми или инструменти за управление на кризи в зависимост от естеството и въздействието на инцидента;

iv. Когато IPCR е в режим за обмен на информация, се задейства способността за подкрепа на ISAA, като се увеличава обменът на информация чрез уебплатформата на IPCR и се осигурява споделен обзор на състоянието. Докладите за състоянието от EU-CyCLONe и мрежата на ЕРИКС следва да останат основните инструменти, представящи общата ситуационна осведоменост съответно на оперативно и техническо равнище. Тези доклади могат да служат за основа на докладите ISAA;

v. В случай на инцидент, който изисква активиране на действия за реагиране на равнището на Съюза, по-специално съответните хоризонтални и секторни механизми за управление на кризи на равнището на Съюза, изброени в приложение II, в сътрудничество с Комисията и върховния представител Съветът следва да осигури съгласуваност и координация между реакцията при киберкриза и съответните действия за реагиране на равнището на Съюза;

vi. Когато са поискани подходящи механизми, по-специално услугите на Резерва за киберсигурност, службите на Комисията и ЕСВД, когато е целесъобразно, както и съответните органи на Съвета, по-специално HWPCI и хоризонталната работна група „Повишаване на устойчивостта и борба с хибридните заплахи“ (HWP-ERCHT), по целесъобразност, следва да координират разработването и изпълнението на мерките, както и подходящия процес на вземане на решения с допълнителните мерки, в съответствие с инструментариума срещу хибридни заплахи[14] в случай на злонамерени действия в киберпространството, които са част от по-широка хибридна кампания.

Реакция при мащабен киберинцидент или киберкриза, за които IPCR е в режим на пълно задействане

(56) Следва да бъдат изпълнени стъпките, изброени в раздел „*Реакция при мащабен киберинцидент или киберкриза, за които IPCR не е в режим на пълно задействане*“ по-горе.

(57) Когато IPCR е в режим на пълно задействане, докладите ISAA служат за осигуряване на обща ситуационна осведоменост на политическо равнище. Докладите за състоянието от EU-CyCLONe и мрежата на ЕРИКС следва да останат основните инструменти, представящи общата ситуационна осведоменост съответно на оперативно и техническо равнище. Тези доклади могат да служат за основа на докладите ISAA.

(58) В случай на мащабен киберинцидент или киберкриза, които водят до IPCR в режим на пълно задействане, всички участници следва да реагират в тясна координация чрез подход, включващ всички равнища на управление, както следва:

a) координацията на реакцията на политическо равнище на Съюза се извършва от Съвета, като се използват договореностите за IPCR;

---

14 Инструментариумът срещу хибридни заплахи представлява рамка за координирана реакция на хибридни кампании, засягащи ЕС и неговите държави членки, която включва например превантивни мерки, мерки за сътрудничество, за стабилност, ограничителни мерки и мерки за възстановяване и подкрепа за солидарност и взаимопомощ.

б) в сътрудничество с мрежата на ЕРИКС EU-CyCLONe следва да предостави ясна информация на политическото равнище относно въздействието, възможните последици и мерките за реакция и отстраняване на инцидента, включително чрез принос към докладите ISAA;

в) в допълнение към способността на ISAA председателството на Съвета на Европейския съюз ще свиква кръгли маси за IPCR, за да се даде възможност за политическа и стратегическа координация на реакцията на ЕС, с действия в рамките на концепцията за киберсигурността и работата на съответните секторни механизми, които да допринасят за работата на IPCR. Освен това кръглите маси могат да установят някои конкретни пропуски в реакцията и да приканят конкретни участници от ЕС да ги преодолеят и да докладват на бъдещи кръгли маси, за да се подпомогне политическата и стратегическата координация в рамките на IPCR;

г) председателството на Съвета на Европейския съюз следва да обмисли възможността да покани EU-CyCLONe на съответните заседания, включително на кръглите маси в рамките на договореностите за IPCR и други свързани заседания на Съвета;

д) органите на държавите членки за управление на кризи следва да гарантират съгласуваност и координация между секторните действия в отговор на киберкризи, подкрепяни от органите за управление на киберкризи;

е) възможните дипломатически отговори следва да бъдат обмислени и проведени в съответствие с глава IX.

VIII: Усилия за комуникация с обществеността

(59) Въпреки че комуникацията с населението на дадена държава членка относно текущ мащабен киберинцидент или киберкриза, включително като част от повишаването на осведомеността, е от национална компетентност, държавите членки, Комисията и върховният представител следва да се стремят да координират публичната си комуникация, доколкото е възможно. По целесъобразност може да бъде включена неформалната комуникационната мрежа при кризи на IPCR.

(60) За целите на подготовката за мащабни киберинциденти и киберкризи държавите членки и когато е целесъобразно, Комисията и CERT-EU се приканват да обменят информация относно своите комуникационни усилия в рамките на EU-CyCLONe и мрежата на ЕРИКС, включително най-добрите практики, като например съвети или кампании за повишаване на осведомеността. ENISA следва да предостави инструменти в подкрепа на такъв обмен и за осигуряване на лесен достъп.

(61) В случай на мащабен киберинцидент или киберкриза държавите членки се приканват да споделят в рамките на EU-CyCLONe информация относно своите усилия за комуникация с обществеността с цел изграждане на обща осведоменост и координиране на действията. По собствена инициатива или по искане на Съвета EU-CyCLONe може да сподели със Съвета обзор на тези подходи.

IX: Дипломатически отговор и сътрудничество със стратегически партньори

(62) Върховният представител, в тясно сътрудничество с Комисията и с други съответни субекти на Съюза, следва:

а) да подпомага вземането на решения в Съвета, включително чрез анализи, доклади и предложения, относно използването на възможни мерки като част от инструментариума на ЕС за кибердипломация. Това ще предостави възможност за използването на пълния спектър от налични инструменти на Съюза за предотвратяване, възпиране и реагиране на злонамерени действия в киберпространството, укрепване на неговата кибернетична позиция и насърчаване на международния мир, сигурност и стабилност в киберпространството;

б) когато е установен съответен инцидент — да улеснява обмена на необходимата информация със стратегическите партньори, включително с НАТО, когато е уместно;

в) да подобрява координацията със стратегическите партньори, включително с НАТО, когато е уместно, в отговор на злонамерени действия в киберпространството от автори на постоянни заплахи, особено когато се използва инструментариумът за кибердипломация на ЕС, в съответствие с неговите насоки за прилагане.

(63) Държавите членки, върховният представител, Комисията и други съответни субекти в Съюза следва да си сътрудничат със стратегически партньори и международни организации, за да насърчават добрите практики и отговорното поведение на държавата в киберпространството и да гарантират бърза и координирана реакция в случай на потенциални или мащабни киберинциденти.

(64) Сътрудничеството между Европейския съюз и НАТО следва да се осъществява в съответствие с договорените ръководни принципи на приобщаване, реципрочност и прозрачност и при пълно зачитане на автономното вземане на решения в Съюза.

(65) Като вземат предвид съществуващите споразумения като техническото споразумение CERT-EU/NATO от 2016 г., Комисията и върховният представител следва да установяват звена за контакт с цел координация с НАТО в случай на киберкриза, за да обменят необходимата информация относно положението и използването на механизми за реакция при кризи, така че да подобрят сътрудничеството и ефективността на реакцията. За тази цел Съюзът следва да проучи начини за подобряване на обмена на информация с НАТО по приобщаващ, реципрочен и недискриминационен начин, по-специално чрез осигуряване на инструменти за сигурна комуникация, като същевременно се вземат предвид стандартите за обмен на информация на различните държави членки.

(66) Като част от постоянната програма на Съюза за киберучения, посочена в глава V по-горе, службите на Комисията и ЕСВД следва да обмислят организирането на учение на равнище персонал с НАТО, за да се тества сътрудничеството между граждански и военни субекти в случай на мащабен киберинцидент или киберкриза, когато държавите членки или съюзниците от НАТО очакват реакции на кибератака, засягаща тяхната сигурност. Ученията следва да се провежда по приобщаващ и недискриминационен начин и при пълно зачитане на договорените принципи на параметрите на сътрудничеството между ЕС и НАТО. Ученията следва да се проведе в рамките на ученията „EU Integrated Resolve“ (Паралелно и координирано учение, PACE). Следва да бъдат предприети всички необходими мерки, за да се гарантира участието на всички участници, посочени в концепцията за киберсигурността.

(67) Следва да се обмислят и съвместни киберучения на равнището на Съюза с държавите от Западните Балкани, Република Молдова, Украйна, както и с други стратегически партньори и единомислещи трети държави, в консултация със Съвета, Комисията и върховния представител.

X: Координация на управлението на киберкризи с военни участници на равнището на ЕС

(68) Държавите членки следва да продължат да укрепват сътрудничеството между гражданските и военните участници в киберпространството на национално равнище.

(69) EU-CyCLONe и мрежата на ЕРИКС следва да определят възможните начини и процедури за сътрудничество със съответните военни участници от ЕС, като например Конференцията на киберкомандирите на ЕС и оперативната мрежа за военни екипи за незабавно реагиране при компютърни инциденти (MICNET), за да се извлече полза от съвместна военна и гражданска гледна точка, по-специално чрез съвместни заседания. EU-CyCLONe и мрежата на ЕРИКС следва да информират Съвета за постигнатия напредък по отношение на това сътрудничество.

(70) Засегнатата държава членка се приканва да информира EU-CyCLONe, както и ЕСВД, ако съответните национални или многонационални военни способности за реагиране се използват в контекста на мащабен киберинцидент или киберкриза и предоставянето на тази информация се договаря взаимно между ползвателя и доставчика на такава способност за реагиране.

(71) Като част от постоянната програма на Съюза за киберучения, посочена в глава V по-горе, Комисията и върховният представител следва да обмислят организирането на съвместно учение с цел тестване на сътрудничеството между гражданските и военните участници в киберпространството в случай на мащабен киберинцидент, засягащ държавите членки.

XI: Възстановяване и извлечени поуки от дадена киберкриза

(72) Държавите членки, съответните субекти и мрежи на Съюза следва да си сътрудничат по време на фазата на възстановяване след киберкриза, за да се гарантира бързото възстановяване на основните функции. Правоприлагащите общности следва също да участват в такова сътрудничество, когато е уместно. На този етап сътрудничеството с частния сектор е от решаващо значение, особено за улесняване на възстановяването на данните и системите. Ефективната координация сред заинтересованите страни следва да даде приоритет на свеждането до минимум на смущенията и на гарантирането на непрекъснатост на дейността.

(73) Държавите членки, съответните субекти и мрежи на Съюза следва да работят заедно през етапа на възстановяване, като се основават на поуките, извлечени от киберкризи или управлявани киберинциденти в миналото, както и на докладите за инциденти, по-специално в контекста на Европейския механизъм за преглед на киберинциденти, създаден с Регламент (ЕС) 2025/38.

(74) EU-CyCLONe следва да предостави на мрежата ЕРИКС, на групата за сътрудничество за МИС и на Съвета изчерпателен списък на поуките, извлечени от киберкризи или управлявани киберинциденти в миналото, и на най-добри практики. ENISA следва да гарантира, че извлечените поуки са правилно отразени в бъдещите дейности за подготвеност и при обмислянето на планирането на бъдещи учения.

XII: Сигурна комуникация

(75) Въз основа на картографирането на съществуващите инструменти за сигурна комуникация[15], Комисията следва да предложи до края на 2026 г. оперативно съвместим набор от решения за сигурна комуникация. Съветът, Комисията, върховният представител, EU-CyCLONe и мрежата на ЕРИКС следва да постигнат съгласие по този набор от решения до края на 2027 г. За тези решения следва да допринасят действията в областта на сигурните комуникации, които институциите на ЕС биха могли да предприемат съгласно стратегията на ЕС за Съюз на подготвеност, и те следва да включват пълния набор от необходими начини на комуникация (глас, данни, видеоконферентна връзка, съобщения, сътрудничество и споделяне на документи и консултации). Решенията следва да отговарят на общо определени изисквания за защита на чувствителната некласифицирана информация. Следва да се използват решения, основани на отворен протокол с приложения с отворен код, подходящи за комуникация в реално време, управлявани от субект, който е местно лице на ЕС.

(76) Ако е необходимо, за целите на обмена на информация с ниво на класификация за сигурност RESTREINT UE/EU RESTRICTED, EU-CyCLONe и мрежата на ЕРИКС следва да могат да използват сигурни канали за комуникация, осигурени за институциите, органите и агенциите на ЕС за обмен на класифицирана информация помежду им и с държавите членки.

[15] Док. WK 862/2023.

(77) Без да се засяга бъдещата многогодишна финансова рамка, в Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ECCC), създаден съгласно Регламент (ЕС) 2021/887[16], следва да се обмисли финансиране чрез програмата „Цифрова Европа“, за да се подпомогнат държавите членки при внедряването на тези инструменти. Следва да се избягва всякакво дублиране на инвестиции в оперативно съвместими сигурни системи.

(78) По-специално субектите на ЕС и държавите членки следва да разработят действия в непредвидени случаи за тежки кризи, при които нормалните комуникационни канали, разчитащи на интернет или на телекомуникационни мрежи, са прекъснати или недостъпни.

(79) Следва да бъдат установени механизми за комуникация и обмен на информация между правоприлагащите органи и мрежите за киберсигурност, особено на техническо равнище, за постигане на ефективна реакция при кризи. При тези механизми следва да се зачита ролята на всяка страна и да се избягва намеса в текущите операции, както и да се гарантират резервни комуникации. Системата на ЕС за комуникации от критично значение (EUCCS), която е в процес на разработване, може да бъде от полза за съвместния отговор със съответните киберобщности.

XIII: Заключителни разпоредби

(80) В сътрудничество с мрежата на ЕРИКС и други основни участници в екосистемата на ЕС за управление на киберкризи, в срок от една година след публикуването на препоръката EU-CyCLONe с подкрепата на ENISA следва да разработи подробни технологични схеми, очертаващи информационните потоци между съответните участници, процесите на вземане на решения и докладите, разработени по време на управлението на мащабни киберинциденти или киберкризи, както е описано в настоящата препоръка. Технологичните схеми следва да включват различни режими и нива на сътрудничество. Те следва да бъдат актуализирани при необходимост.

---

[16] Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета от 20 май 2021 г. за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове (ОВ L 202, 8.6.2021 г., стр. 1—31).

(81) В подкрепа на ефективното прилагане на преразгледаната концепция за киберсигурността и въз основа на опита, придобит чрез съвместните киберучения, провеждани в рамките на този план, Съветът може да разработи при необходимост набор от насоки за изпълнение. Тези насоки биха могли да предложат решение на практическите предизвикателства, установени в хода на ученията, и да отстранят установените пропуски и липсващите връзки в координацията, комуникацията и оперативното взаимодействие.

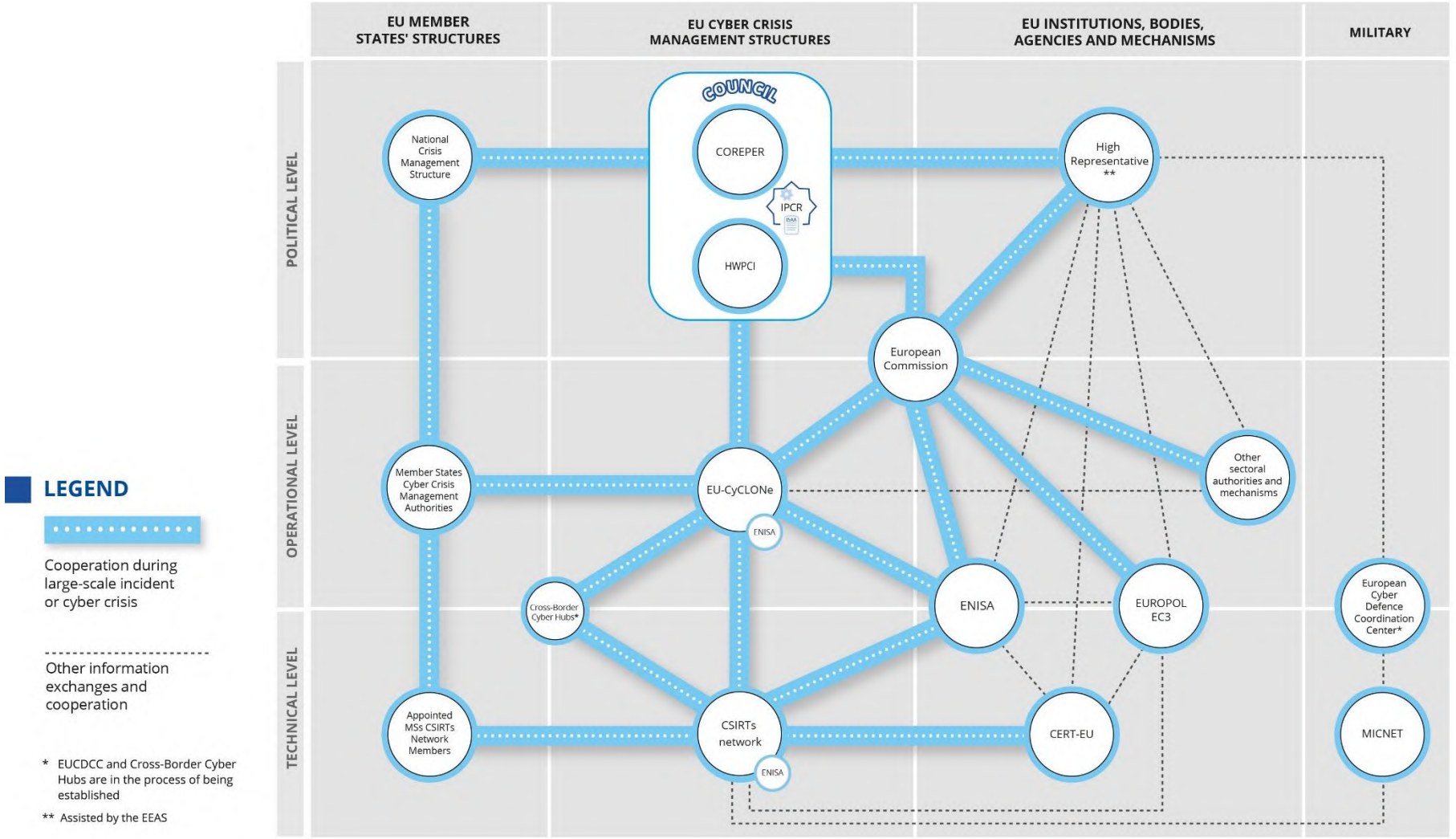
(82) Настоящата препоръка следва да се преразглежда от Комисията в сътрудничество с държавите членки поне веднъж на всеки четири години след публикуването ѝ. След всеки преглед Комисията следва да публикува доклад и да го представя на Съвета. Комисията и държавите членки следва да вземат предвид по-специално въздействието на променящата се картина на заплахите, резултатите от съвместните учения и законодателните промени — по-специално всички възможни промени, произтичащи от преразглеждането на Регламент (ЕС) 2019/881.

Съставено в Брюксел на […] година.

За Съвета

Председател

ПРИЛОЖЕНИЕ I — Концепция на Съюза за реакция при кризи в областта на киберсигурността



ПРИЛОЖЕНИЕ II — СЪОТВЕТНИ УЧАСТНИЦИ НА РАВНИЩЕТО НА СЪЮЗА (СУБЕКТИ И МРЕЖИ) И МЕХАНИЗМИ ЗА УПРАВЛЕНИЕ НА КРИЗИ

(1) Ангажимент на основните участници в целия жизнен цикъл на управлението на киберкризи (мащабни киберинциденти и киберкризи)

	Подготвеност	Установяване	Реагиране на мащабен киберинцидент или киберкриза			Комуникация с обществеността	Възстановяване и извлечени поуки
			на техническо равнище	на оперативно равнище	на политическо равнище		
Държави членки	X	X	X	X	X	X	X
Комисия	X			X	X	X	
Върховен представител, подпомаган от ЕСВД	X			X	X	X	
Съвет	X				X	X	X
ENISA	X		X	X			
CERT-EU	X	X	X	X		X	X
Мрежа на ЕРИКС	X	X	X				X
EU-CyCLONe;	X			X	X		X

(2) Роли и компетентности на съответните участници и механизми на равнището на Съюза (по азбучен ред) във връзка с управлението на киберкризи

Участник	Равнище	Роля и компетентност	Препратка
CERT-EU	Техническо/ оперативно	Координира на техническо равнище реакцията при криза и управлението на съществени инциденти, засягащи субекти на Съюза. Поддържа опис на наличния технически експертен опит, който би бил необходим при реагиране на инциденти в случай на съществени инциденти, и подпомага МСК в координирането на плановете на субектите на Съюза за управление на киберкризи в случай на съществени инциденти. Член на мрежата на ЕРИКС. Подкрепя Комисията в EU-CyCLONe относно координираното управление на мащабни киберинциденти и кризи. Действа като координационен център за обмен на информация и реагиране при инциденти в областта на киберсигурността, улеснява обмена на информация относно инциденти, киберзаплахи, уязвимости и близки до инцидент	Регламент (ЕС, Евратом) 2023/2841 Регламент (ЕС) 2025/38

Участник	Равнище	Роля и компетентност	Препратка
		положения между субектите на Съюза и партньори. Отправя искане за разгръщането на Резерва за киберсигурност на ЕС от името на субекти на Съюза. Сътрудничи с центъра на НАТО за киберсигурност въз основа на техническо споразумение между тях.	
Съвет на Европейския съюз	Политическо	Функции по определяне на политиките и координиране. Натоварен е с IPCR, което се отнася до координацията и реакцията на политическо равнище на Съюза.	Член 16 от Договора за Европейския съюз
Председателство на Съвета на Европейския съюз	Политическо	Взема решение (с изключение когато има позоваване на клаузата за солидарност съгласно член 222 от Договора за функционирането на Европейския съюз) дали да задейства или да прекрати IPCR, като се консултира по целесъобразност със засегнатите държави членки, както и с Комисията и ВП.	Член 16 от Договора за Европейския съюз Решение за изпълнение (ЕС) 2018/1993 на Съвета
Трансгранични киберхъбове	Техническо	Трансграничният киберхъб е многонационална платформа, създадена с писмено споразумение за консорциум, която обединява в	Регламент (ЕС) 2025/38

Участник	Равнище	Роля и компетентност	Препратка
		координирана мрежова структура националните киберхъбове от най-малко три държави членки и която е предназначена да засили мониторинга, откриването и анализа на киберзаплахи, да предотвратява инциденти и да подпомага изготвянето на разузнавателна информация за киберзаплахите, по-специално чрез обмен на подходящи данни и информация, анонимизирани, когато е целесъобразно, както и чрез споделяне на най-съвременни инструменти и съвместното развитие на способности за откриване на киберзаплахи, анализ, превенция и защита в доверителна среда; Тясно си сътрудничат с мрежата на ЕРИКС с цел обмен на информация. Предоставят информация, свързана с потенциален или продължаващ мащабен киберинцидент, на органите на държавите членки и на Комисията чрез EU-CyCLONe и мрежата на ЕРИКС.	

Участник	Равнище	Роля и компетентност	Препратка
Мрежа на ЕРИКС	Техническо	Допринася за изграждането на доверие и насърчава бързото оперативно сътрудничество между държавите членки. Представлява основната мрежа за обмен на относима информация за инциденти, близки до инцидент положения, киберзаплахи, рискове и уязвимости. По искане на потенциално засегнат от инцидент член Мрежата обменя и обсъжда информация във връзка с този инцидент и свързаните киберзаплахи. Мрежата може също да спомага за координирана реакция на инцидент, констатиран в рамките на юрисдикцията на отправил запитване член. Предоставя помощ на държавите членки при управлението на трансгранични инциденти и проучва допълнителни форми на сътрудничество, включително взаимопомощ. Получава информация от държавите членки относно техните	Директива (ЕС) 2022/2555 Регламент (ЕС) 2025/38

Участник	Равнище	Роля и компетентност	Препратка
		искания към Резерва за киберсигурност на ЕС.	
Конференция на киберкомандирите		Форум за киберкомандири на национално равнище в рамките на държавите членки за сътрудничество и обмен на жизненоважна информация относно текущи операции в киберпространството и стратегии за смекчаване на мащабни киберинциденти. Организира се от ротационното председателство на Съвета на Европейския съюз с подкрепата на Европейската агенция по отбрана (EDA), Европейската служба за външна дейност (ЕСВД) и Военния секретариат на Европейския съюз (ВСЕС).	Съвместно съобщение относно политиката на ЕС за киберотбрана (2022 г.)
Комисия	Оперативно/политическо	Изпълнителен орган на Европейския съюз. Осигурява безпроблемното функциониране на вътрешния пазар. Улеснява съгласуваността и координацията на съответните действия на равнището на Съюза за реакция при кризи. Определени общи действия на равнището на Съюза в	Член 17 от Договора за Европейския съюз Решение за изпълнение (ЕС) 2018/1993 Решение № 1313/2013/ЕС Директива (ЕС) 2022/2555

Участник	Равнище	Роля и компетентност	Препратка
		областта на подготвеността по линия на Решението за МГЗС, включително управление на координационния център за реагиране при извънредни ситуации и на общата система за комуникация и информация при извънредни ситуации. Наблюдател в EU-CyCLONe и член в случай на потенциален или текущ мащабен инцидент, който оказва или е вероятно да окаже значително въздействие върху услугите и дейностите, попадащи в обхвата на Директива (ЕС) 2022/2555. Наблюдател в мрежа на ЕРИКС. Цялостна отговорност за прилагането на Резерва за киберсигурност на ЕС. Звено за контакт в Междуинституционалния съвет по киберсигурност за споделяне с EU-CyCLONe на подходяща информация във връзка със съществени инциденти. Консултира председателството на Съвета във връзка с	Регламент (ЕС) 2025/38 Регламент (ЕС, Евратом) 2023/2841

Участник	Равнище	Роля и компетентност	Препратка
		решенията за задействане или прекратяване на IPCR (освен когато се прави позоваване на клаузата за солидарност съгласно член 222 от ДФЕС). Службите на Комисията изготвят, съвместно с ЕСВД, докладите ISAA.	
Агенция на Европейския съюз за киберсигурност (ENISA)	Техническо/оперативно	Изпълнява задачи с цел постигане на високо ниво на киберсигурност в целия Съюз, включително чрез активна подкрепа за държавите членки и институциите на Съюза Предоставя секретариат за мрежата на ЕРИКС и EU-CyCLONe. Изготвя редовно технически доклад за състоянието на киберсигурността в ЕС във връзка с инцидентите и киберзаплахите (с EC3 и CERT-EU и в тясно сътрудничество с държавите членки). Допринася за разработването на обща реакция на мащабни трансгранични инциденти или кризи най-вече чрез: - обобщаване и анализиране на доклади от национални източници; - осигуряване на подаване на информация	Директива (ЕС) 2022/2555 Регламент (ЕС) 2019/881 Регламент (ЕС) 2025/38 Регламент (ЕС) 2024/2847

Участник	Равнище	Роля и компетентност	Препратка
		между техническото, оперативното и политическото равнище; - при поискване, улесняване на справянето с инциденти; - предоставяне на подкрепа на субекти на Съюза по отношение на комуникацията с обществеността; - оказване на подкрепа, при поискване, на държавите членки по отношение на комуникацията с обществеността; - тестване на способностите за реагиране при инциденти и редовно организиране на учения в областта на киберсигурността. Действа като възлагащ орган, когато му е възложено частично или изцяло да управлява Резерва за киберсигурност на ЕС. Организира на всеки две години всеобхватно учение в областта на киберсигурността на равнището на Съюза с технически, оперативни или стратегически елементи. Изготвя доклад за преглед на инцидента в сътрудничество със съответната държава членка и други имащи отношение заинтересовани страни, за да оцени	

Участник	Равнище	Роля и компетентност	Препратка
		причините, въздействието и смекчаването на последиците от даден инцидент (по искане на Комисията или EU-CyCLONe и с одобрението на засегнатата държава членка). Информира EU-CyCLONe, ако информацията, предоставена съгласно задълженията за докладване, произтичащи от Акта за киберустойчивостта, е от значение за координираното управление на мащабни киберинциденти и кризи на оперативно равнище.	
Европейска мрежа за връзка на организациите при киберкризи (EU-CyCLONe)	Оперативно	Подкрепя координираното управление на мащабни киберинциденти и кризи на оперативно равнище Осигурява редовен обмен на подходяща информация между държавите членки и институциите, органите, службите и агенциите на Съюза. Координира управлението на мащабни киберинциденти и кризи и подпомага процеса на вземане на решения на политическо равнище	Директива (ЕС) 2022/2555 Регламент (ЕС) 2025/38

Участник	Равнище	Роля и компетентност	Препратка
		във връзка с такива инциденти и кризи. Извършва оценка на последиците и въздействието на съответните мащабни киберинциденти и кризи и предлага възможни мерки за смекчаване на последиците. Обсъждане, по искане на засегната държава членка, на националните планове за реакция при мащабни киберинциденти и кризи. Разработва, заедно с ENISA и Комисията, образеца за улесняване на подаването на искания за подкрепа от Резерва за киберсигурност на ЕС. Получава информация от държавите членки относно техните искания към Резерва за киберсигурност на ЕС. Получава информация, свързана с потенциален или текущ мащабен киберинцидент от трансграничните киберцентрове или от мрежата на ЕРИКС.	
Върховният представител на Съюза по въпросите на външните работи и политиката на сигурност, подпомаган от	Политическо	Ръководи и координира усилията на Съюза за справяне с външните заплахи за сигурността в областта на	Решение 2010/427/ЕС на Съвета

Участник	Равнище	Роля и компетентност	Препратка
Европейската служба за външна дейност		хибридното и киберпространството Отговаря за инструментите на Съюза за кибердипломация и киберотбрана за възпиране и реагиране на външни заплахи, включително чрез използване на инструментариумите на Съюза против хибридни заплахи и за кибердипломация. Сътрудничи си с външни партньори, включително чрез участие в ОПСО. Осигурява подготвеност на Съюза и държавите членки относно ситуационната осведоменост и капацитета за реагиране на хибридни и киберзаплахи, например чрез практически учения, обучение и мрежи. Справя се с последиците за сигурността и отбраната, дължащи се на космическите активи на Съюза, особено в рамките на общата политика на Съюза за сигурност и отбрана (ОПСО). Подкрепя Конференцията на киберкомандирите на ЕС. Подкрепя оперативната мрежа	

Участник	Равнище	Роля и компетентност	Препратка
		на ЕС за военни екипи за незабавно реагиране при компютърни инциденти (MICNET). Консултира председателството на Съвета във връзка с решенията за задействане или прекратяване на IPCR (освен когато се прави позоваване на клаузата за солидарност съгласно член 222 от ДФЕС). ЕСВД, съвместно със службите на Комисията, изготвя докладите ISAA.	
Координационен център на ЕС за киберотбрана	Хоризонтално	Неговата първоначална цел е преди всичко да повиши споделената ситуационна осведоменост на Съюза и неговите държави членки за злонамерените действия в киберпространството, особено по отношение на военни мисии и операции в рамките на ОПСО.	Съвместно съобщение относно политиката на ЕС за киберотбрана (2022 г.)
Европол	Оперативно	Предоставя оперативна и техническа подкрепа на компетентните органи на държавите членки за предотвратяване и възпиране на киберпрестъпления. Подпомага компетентните органи на държавите членки, по тяхно искане, при реакцията срещу кибератаки с предполагаем престъпен произход.	Регламент (ЕС) 2016/794, включително всички изменения

Участник	Равнище	Роля и компетентност	Препратка
Междуинституционален съвет по киберсигурност		Изготвя план за управление на киберкризи с цел да окаже подкрепа на оперативно равнище при координираното управление на съществени инциденти, засягащи субекти на Съюза, и да допринесе за редовния обмен на подходяща информация. Координира приемането на плановете на отделните субекти на Съюза за управление на киберкризи Приема, въз основа на предложение на CERT-EU, насоки или препоръки относно сътрудничеството за реагиране при инциденти за значими инциденти, засягащи субекти на Съюза.	Регламент (ЕС, Евратом) 2023/2841
Оперативна мрежа за военни екипи за незабавно реагиране при компютърни инциденти (MICNET)	Техническо	Насърчава по-енергичен и координиран отговор на киберзаплахи, засягащи отбранителните системи в Съюза, включително тези, които се използват във военни мисии и операции по линия на ОПСО; подкрепя се от Европейската агенция по отбрана.	Съвместно съобщение относно киберотбраната (2022 г.)

Участник	Равнище	Роля и компетентност	Препратка
Единно звено за анализ на разузнавателна информация (SIAC)		Състои се от: 1) Центъра на ЕС за анализ на информация (EU INTCEN) и 2) дирекция „Разузнаване“ на Военния секретариат на ЕС (EUMS INT) SIAC. Предоставя стратегическа разузнавателна информация относно външната политика, тероризма, киберзаплахите и хибридните заплахи, и Обработва военната разузнавателна информация за мисии по линия на ОПСО и подкрепя операциите на Съюза в областта на отбраната и управлението на кризи. Под ръководството на върховния представител.	Член 38 и членове 42—46 от Договора за Европейския съюз.

(3) Съответни механизми и платформи за управление на кризи на равнището на Съюза

Механизъм	Хоризонтален/ секторен/специфичен за областта на киберсигурността	Описание	Препратка
Обща система за бързо предупреждение (ARGUS)	Хоризонтален	Процесът на координация на Комисията и общата система за предупреждение за съгласувана реакция в случай на сериозна трансгранична криза, изискваща действия на равнище ЕС. Той обединява всички съответни служби и кабинети за вземане на решения и координиране на мерките. Позволява на Комисията да обменя необходимата информация относно възникващи многосекторни кризи или предвидима или неизбежна опасност от такива, които изискват действие на равнището на Съюза.	Съобщение (2005) 662 на Комисията
Център на ЕСВД за реагиране при кризи (ЦРК)	Хоризонтален	Единното звено за контакт за всички свързани с кризи въпроси в ЕСВД, което притежава постоянна и налична 24 часа в денонощието,7 дни в седмицата способност за реагиране при кризи в извънредни ситуации, застрашаващи безопасността на персонала на делегациите на ЕС, и/или при кризи, засягащи граждани на Съюза в чужбина. То обединява експерти по сигурността, консулските операции и ситуационната осведоменост, като същевременно	Стратегически компас за сигурността и отбраната — За Европейския съюз, който защитава своите граждани, ценности и интереси и допринася за международния мир и сигурност (21 март 2022 г.)

Механизъм	Хоризонтален/ секторен/специфичен за областта на киберсигурността	Описание	Препратка
		разчита на отдадени специалисти на място в делегациите на Съюза.	
Подробен план за критичната инфраструктура	Хоризонтален	Координира реакцията на равнището на Съюза при смущения в критичната инфраструктура със значително трансгранично значение.	Препоръка C/2024/4371 на Съвета
Система за предупреждение в областта на киберсигурността	Специфичен за областта на киберсигурността	Гарантира усъвършенстване на способностите на Съюза за подобряване на възможностите за откриване, анализиране и обработване на данни във връзка с киберзаплахи и предотвратяване на инциденти в Съюза.	Регламент (ЕС) 2025/38
Инструментариум за кибердипломация (Рамка за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството)	Специфичен за областта на киберсигурността	Позволява съвместен дипломатически отговор на Съюза срещу злонамерени действия в киберпространството, допринасящ за предотвратяване на конфликти, смекчаване на заплахите за киберсигурността и по-голяма стабилност в международните отношения.	Заключения на Съвета от 19 юни 2017 г. Преразгледани насоки за изпълнение 10289/23, 8 юни 2023 г.
Резерв за киберсигурност на ЕС	Специфичен за областта на киберсигурността	Мобилизира експерти по киберсигурност и ресурси по време на кризи в подкрепа на усилията за реагиране в държавите членки, институциите, органите или агенциите на Съюза	Регламент (ЕС) 2025/38

Механизъм	Хоризонтален/ секторен/специфичен за областта на киберсигурността	Описание	Препратка
Мрежов кодекс относно специфични за сектора правила за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия	Секторен	Установява повтарящ се процес на оценки на рисковете за киберсигурността в електроенергийния сектор на равнището на Съюза, на равнището на държавите членки, на регионално равнище и на равнище субект. Съдържа разпоредби, специфични за управлението на кризи и сътрудничеството с ЕРИКС и EU-CyCLONe в случаите, когато мащабен киберинцидент оказва въздействие върху други сектори, зависещи от сигурността на доставките на електроенергия.	Делегиран регламент (ЕС) 2024/1366 на Комисията
Инструментариум срещу хибридни заплахи	Хоризонтален	Включва набор от разпоредби за осигуряване на обзор на наличното на равнището на ЕС в отговор на всички видове хибридни заплахи, тяхното координирано използване, осигуряване на съгласуваност на действията в различни области. Инструментариумът срещу хибридни заплахи спомага да се гарантира, че вземането на решения се основава на цялостна ситуационна осведоменост и на извлечените поуки	Заключения на Съвета относно рамка за координиран отговор на ЕС на хибридни кампании, 22 юни 2022 г. Насоки за прилагане на рамката за координиран отговор на ЕС на хибридни кампании, 14 декември 2022 г.

Механизъм	Хоризонтален/ секторен/спец ифичен за областта на киберсигурнос тта	Описание	Препратка
Екипи за бързо реагиране при хибридни заплахи (EU HRRT)	Хоризонтален	Като част от инструментариума срещу хибридни заплахи на ЕС екипите на ЕС за бързо реагиране при хибридни заплахи черпят от съответния секторен национален и граждански и военен експертен опит на ЕС с цел да осигурят съобразена и целенасочена краткосрочна помощ на държавите членки, мисиите и операциите в рамките на общата политика за сигурност и отбрана и държавите партньори при противодействието на хибридни заплахи и кампании.	Ръководна рамка за практическото създаване на екипи на ЕС за бързо реагиране при хибридни заплахи (21 май 2024 г.) Оперативни насоки за разгръщането на екипи за бързо реагиране при хибридни заплахи, одобрени от Корепер на 4 декември 2024 г.
IPCR	Хоризонтален	Подпомага бързото и координирано вземане на решения на политическо равнище на Съюза при сериозни и сложни кризи. Решението за задействане и прекратяване се взема от председателството на Съвета, което се консултира (освен когато е използвана клаузата за солидарност) със засегнатите държави членки, Комисията и ВП. Генералният секретариат на Съвета, службите на Комисията и ЕСВД могат също да се споразумеят, след консултации с председателството, да задействат IPCR в режим за обмен на информация.	Решение за изпълнение (ЕС) 2018/1993 на Съвета

Механизъм	Хоризонтален/ секторен/специфичен за областта на киберсигурността	Описание	Препратка
		Дискусиите се основават на докладите ISAA, изработени от службите на Комисията и ЕСВД. Тези доклади се основават на свързаните с въпроса информация и анализи, предоставени от държавите членки (например от съответните национални кризисни центрове) и от съответните агенции и органи на Съюза.	
Протокол за реагиране при извънредни ситуации на правоприлагащите органи в ЕС	Хоризонтален	Инструмент за подпомагане на правоприлагащите органи на Съюза при предоставянето на незабавна реакция на сериозни трансгранични кибератаки чрез бърза оценка, сигурен и навременен обмен на критична информация и ефективна координация на международните аспекти на техните разследвания.	Заключения на Съвета (26 юни 2018 г.) относно координирана реакция на ЕС на мащабни киберинциденти и кризи.
Екипи за бързо реагиране при кибератаки (CRRT) в рамките на постоянното структурирано сътрудничество (ПСС)	Специфичен за областта на киберсигурността	CRRT в рамките на ПСС са съвместно развита гражданско-военна способност за киберотбрана на държавите — членки на ЕС, за бързо реагиране на киберинциденти и киберкризи, както и за извършване на	Член 42, параграф 6, член 46 и протокол 10 от Договора за Европейския съюз.

Механизъм	Хоризонтален/ секторен/спец ифичен за областта на киберсигурнос тта	Описание	Препратка
		превантивни действия, като например оценки на уязвимостта и наблюдение на избори. Мисията на CRRT в рамките на ПСС е при поискване да предоставя подкрепа по въпроси на киберсигурността на държавите — членки на ЕС, институциите, органите и агенциите на ЕС, военните мисии и операции на ЕС по линия на ОПСО, както и на държавите партньори.	

Архитектура за реагиране на космически заплахи (STRA)	Секторен (Космически заплахи, включително свързани с киберсигурността)	Архитектура за реагиране на космически заплахи (STRA) относно отговорностите, които се упражняват от Съвета и върховния представител за предотвратяване на заплаха, произтичаща от разполагането, експлоатацията или използването на създадените системи и услугите, предоставяни в рамките на космическата програма на Съюза	Решение (ОВППС) 2021/698 на Съвета
Рамка за координация на системни киберинциденти (ЕС-РКСКИ)	Секторен	Рамка за комуникация и координация, която е в процес на разработване, с която се разглеждат и управляват потенциални системни киберсъбития във финансовия сектор. Тя ще се основава на една от предвидените роли на европейските надзорни органи (ЕНО) съгласно Регламент (ЕС) 2022/2554 за постепенно осигуряване на ефективна координирана реакция на равнището на Съюза в случай на съществен трансграничен инцидент, свързан с информационните и комуникационните технологии (ИКТ), или свързана с него заплаха със системно въздействие върху финансовия сектор на Съюза като цяло.	Препоръка на Европейския съвет за системен риск от 2 декември 2021 г. относно общоевропейската рамка за координация на системни киберинциденти за съответните органи (ESRB/2021/17)
Механизъм за гражданска	Хоризонтален	Осигурява сътрудничество за гражданска защита за подобряване на предотвратяването,	Решение 1313/2013.

защита на Съюза (МГЗС)		подготвеността и реакцията при бедствия.	
CISE — Обща среда за обмен на информация	Специфична за морския сектор, обхващаща седем сектора.	CISE е мрежа, която свързва системи на органи на ЕС/ЕИП, отговарящи за морското наблюдение. CISE дава възможност за обмен на подходяща информация през границите и различните сектори по безпроблемен и автоматизиран начин.	Стратегически компас за сигурността и отбраната — За Европейския съюз, който защитава своите граждани, ценности и интереси и допринася за международния мир и сигурност (21 март 2022 г.).

(4) Сектори с висока степен на критичност и други критични сектори съгласно Директива (ЕС) 2022/2555 и секторни механизми за управление на кризи на равнището на Съюза (когато е приложимо)		
Сектори	**Подсектор**	**Приложими секторни механизми за управление на кризи**
Енергетика	Електроенергия	Група за координация в областта на електроенергетиката
	Централизирано топлоснабдяване и студоснабдяване	Не се прилага
	Нефт	Група за координация в областта на нефта Групата на компетентните органи на ЕС по въпросите на добива на нефт и газ в крайбрежни води (EUOAG)
	Природен газ	Координационна група по природния газ
	Водород	Не се прилага
Транспорт	Въздушен	Европейско звено за координация при кризи в авиацията (EACCC)
	Железопътен	Не се прилага
	Воден	Европейска агенция за контрол на рибарството (EFCA) SafeSeaNet (SSN) Интегрирани морски услуги (ИМУ) Център за данни за разпознаване и проследяване на кораби на далечни разстояния (LRIT) Служби на ЕАМБ за морска подкрепа

	Автомобилен	Не се прилага
	Хоризонтален	Мрежата от звена за контакт в областта на транспорта, създадена с Плана за действие в извънредни ситуации в областта на транспорта (COM(2022) 211)
Банков сектор		ЕС-РКСКИ
Инфраструктури на финансовия пазар		ЕС-РКСКИ Европейски механизъм за финансово стабилизиране

Здравеопазване		Система за ранно предупреждение и реагиране (СРПР) Оперативен инструмент за извънредни ситуации в областта на общественото здраве (HEOF), Система за бързо предупреждение за тъкани, клетки и кръвни съставки (RATC/RAB) Рамка за извънредни ситуации в областта на общественото здраве Система за бързо предупреждение за химични инциденти (RASCHEM) Европейският портал за надзор върху заразните болести Орган за готовност и реакция при извънредни здравни ситуации (HERA) Система за анализ на здравни данни и генериране на медицински познания (MediSys) Изпълнителна ръководна група за медицинските изделия (MDSSG) Бързо предупреждение за фармакологична бдителност Работна група на ЕС в областта на здравеопазването (EUHTF) Комитет за здравна сигурност
Питейна вода		Не се прилага

Отпадъчни води		Не се прилага
Цифрова инфраструктура		Не се прилага
Управление на услугите в областта на ИКТ		Не се прилага
Публична администрация		Не се прилага
Космическо пространство		Архитектура за реагиране на космически заплахи (STRA)
Пощенски и куриерски услуги		Не се прилага
Управление на отпадъците		Не се прилага
Производство, изготвяне и дистрибуция на химикали		Система за бързо предупреждение за химични инциденти (RASCHEM)

Производство, преработка и разпространение на храни		Европейска система за мониторинг на културите, Откриване на горещи точки на аномалии в глобалното селскостопанско производство (ASAP), Европейска мрежа от информационни системи за здравето на растенията (EUROPHYT), Спешен ветеринарен екип на ЕС (EUVET) Система за бързо предупреждение за храни и фуражи (RASFF) Европейски механизъм за готовност и реакция при кризи в областта на продоволствена сигурност (EFSCM) Акт за извънредните ситуации и устойчивостта на вътрешния пазар (IMERA)
Производство	Медицински изделия	Не се прилага
	Компютри, електронни и оптични продукти	Не се прилага
	Машини и оборудване	Не се прилага
	Производство на моторни превозни средства, ремаркета и полуремаркета	Не се прилага
	Производство на друго транспортно оборудване	Не се прилага

Доставчици на цифрови услуги		Не се прилага
Научни изследвания		Не се прилага

ПРИЛОЖЕНИЕ III — Рамка на ЕС за управление на кризи в областта на киберсигурността и свързаните с нея инструменти

От 2017 г. насам Съюзът разработи своята рамка за киберсигурност чрез няколко инструмента, които съдържат разпоредби, свързани с управлението на кризи в областта на киберсигурността:

- Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[1],
- Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета[2],
- Регламент за изпълнение 2024/2690[3] на Комисията[3], Регламент (ЕС, Евратом) 2023/2841 на Европейския парламент и на Съвета[4],
- Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета[5],
- Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета[6], и
- Регламент (ЕС) 2025/38 на Европейския парламент и на Съвета (Законодателен акт за киберсолидарност)[7].

Специфичните секторни мерки при криза в областта на киберсигурността включват Делегиран регламент (ЕС) 2024/1366[8] на Комисията[8] и предстоящата Рамка за координация на системни киберинциденти (ЕС-РКСКИ) в контекста на Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета[9].

В Директива 2013/40[10] се предоставя позоваване на определението за престъпни дейности, свързани с кибератаки, и правилата на Съюза относно трансграничния достъп до електронни доказателства, по-специално Регламент (ЕС) 2023/1543 на Европейския парламент и на Съвета[11], чието прилагане значително ще улесни действията на правоприлагащите органи в тази област.

В политиката на ЕС в областта на киберотбраната[12] се посочват ролите на мрежата на ЕС, състояща се от оперативната мрежа за военни екипи за незабавно реагиране при компютърни инциденти (MICNET) и Конференцията на киберкомандирите на ЕС, и се предвижда създаването на Координационен център на ЕС за киберотбрана (КЦК на ЕС).

В някои от критичните сектори, изброени в приложения I и II към Директива (ЕС) 2022/2555, съществуват други, несвързани с киберпространството механизми за ситуационна осведоменост и за реакция при кризи.

В „Препоръка на Съвета относно подробен план за координиран отговор на равнището на Съюза на смущения в критичната инфраструктура със значително трансгранично значение“[13] се предвижда сътрудничество между съответните участници, когато даден инцидент засяга както физическите аспекти, така и киберсигурността на критичната инфраструктура.

[1] Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

[2] 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 (Директива МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

[3] Регламент за изпълнение (ЕС) 2024/2690 на Комисията от 17 октомври 2024 г. за определяне на правила за прилагане на Директива (ЕС) 2022/2555 по отношение на техническите и методологичните изисквания относно мерките за управление на риска в областта на киберсигурността и за доуточняване на случаите, в които даден инцидент се счита за значителен по отношение на доставчиците на DNS услуги, регистрите на имена на домейни от първо ниво, доставчиците на компютърни услуги „в облак“, доставчиците на услуги на центрове за данни, доставчиците на мрежи за доставяне на съдържание, доставчиците на управлявани услуги, доставчиците на управлявани услуги за сигурност, доставчиците на онлайн места за търговия, на онлайн търсачките и на платформите на услуги за социални мрежи и доставчиците на удостоверителни услуги (ОВ L, 2024/2690, 18.10.2024 г.). ELI: https://data.europa.eu/eli/reg/2024/2690/oj).

[4] Регламент (ЕС, Евратом) 2023/2841 на Европейския парламент и на Съвета от 13 декември 2023 г. за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза (ОВ L, 2023/2841, 18.12.2023 г., ELI: http://data.europa.eu/eli/reg/2023/2841/oj).

[5] Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета от 20 май 2021 г. за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове (ОВ L 202, 8.6.2021 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2021/887/oj).

[6] Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета от 23 октомври 2024 г. относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост) (ОВ L, 2024/2847, 20.11.2024 г., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

[7] Регламент (ЕС) 2025/38 на Европейския парламент и на Съвета от 19 декември 2024 г. за определяне на мерки за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти, и за изменение на Регламент (ЕС) 2021/694 (Законодателен акт в

областта на киберсолидарността) (ОВ L, 2025/38, 15.1.2025 г., ELI: http://data.europa.eu/eli/reg/2025/38/oj).

[8] Делегиран регламент (ЕС) 2024/1366 на Комисията от 11 март 2024 г. за допълнение на Регламент (ЕС) 2019/943 на Европейския парламент и на Съвета чрез установяване на мрежов кодекс относно специфични за сектора правила за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия (ОВ L, 2024/1366, 24.5.2024 г., ELI: http://data.europa.eu/eli/reg_del/2024/1366/oj).

[9] Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014, (ЕС) № 909/2014 и (ЕС) 2016/1011 (ОВ L 333, 27.12.2022 г., стр. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj).

[10] Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета (ОВ L 218, 14.8.2013 г., стр. 8, ELI: http://data.europa.eu/eli/dir/2013/40/oj).

[11] Регламент (ЕС) 2023/1543 на Европейския парламент и на Съвета от 12 юли 2023 г. относно европейските заповеди за предоставяне и европейските заповеди за запазване на електронни доказателства в рамките на наказателните производства и за изпълнението на наказания лишаване от свобода вследствие на наказателни производства и Директива (ЕС) 2023/1544 на Европейския парламент и на Съвета от 12 юли 2023 г. за установяване на хармонизирани правила относно определянето на определени форми на установяване и определянето на представители за целите на събирането на електронни доказателства по наказателни производства (ОВ L 191, 28.7.2023 г., стр. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj).

[12] JOIN(2022) 49 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022JC0049

[13] *ОВ C, C/2024/4371, 5.7.2024г.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C_202404371