ЕВРОПЕЙСКА
КОМИСИЯ

Страсбург, 18.10.2022 г.
COM(2022) 551 final

2022/0338 (NLE)

Предложение за

ПРЕПОРЪКА НА СЪВЕТА

относно координиран подход на Съюза за укрепване на устойчивостта на критичната инфраструктура

(текст от значение за ЕИП)

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ПРЕДЛОЖЕНИЕТО

• Основания и цели на предложението

Сигурността е основна цел на Европейския съюз. Въпреки че държавите членки носят главната отговорност за защитата на гражданите, колективните действия на равнището на Съюза имат съществен принос за сигурността на ЕС като цяло. Координацията спомага за подобряване на устойчивостта, за увеличаване на бдителността и за укрепване на колективната ни реакция. В контекста на Съюза на сигурност на ЕС бяха предприети важни стъпки за изграждане на капацитет и възможности за предотвратяване, откриване и бързо реагиране на много заплахи за сигурността, както и за свързване на действията на участниците от публичния и частния сектор в общи усилия.

За да може ЕС да се справи с постоянно променящата се обстановка по отношение на заплахите е необходима постоянна бдителност и адаптиране. Военната агресия на Русия срещу Украйна породи нови рискове, често комбинирани в една хибридна заплаха. Един от тях е рискът от прекъсване на предоставянето на основни услуги от субекти, експлоатиращи критична инфраструктура в Европа. Това бе потвърдено от очевидния саботаж на газопроводите „Северен поток“ и други неотдавнашни инциденти. Обществото разчита в голяма степен както на физическата, така и на цифровата инфраструктура, и прекъсването на основни услуги, било то чрез конвенционални физически атаки или кибератаки, или чрез комбинация от двете, може да има сериозни последици за благосъстоянието на гражданите, нашите икономики и доверието в нашите демократични системи.

Освен това гарантирането на гладкото функциониране на вътрешния пазар е друга ключова цел на ЕС, включително когато става въпрос за основни услуги, предоставяни от субекти, експлоатиращи критична инфраструктура. Ето защо ЕС вече предприе редица мерки за намаляване на уязвимостта и повишаване на устойчивостта на критичните субекти по отношение както на рисковете в киберпространството, така и на тези извън него.

Необходими са спешни действия за увеличаване на капацитета на ЕС за справяне с потенциални атаки срещу критична инфраструктура, главно в самия ЕС, но когато е уместно, и в неговите непосредствени съседи.

Предложената препоръка на Съвета има за цел да засили подкрепата на ЕС за повишаване на устойчивостта на критичната инфраструктура и за осигуряване на координация на равнище ЕС по отношение на готовността и реакцията. Тя има за цел да увеличи максимално и да ускори работата за защита на активите, съоръженията и системите, които са необходими за функционирането на икономиката, и за предоставяне на основни услуги, на които гражданите разчитат, както и за смекчаване на въздействието на всяка атака чрез осигуряване на възможно най-бързото възстановяване. Въпреки че цялата подобна инфраструктура следва да бъде защитена, понастоящем приоритет следва да се отдаде на енергийния, цифровия, транспортния и космическия сектор, поради техния особено хоризонтален характер за обществото и икономиката, както и вследствие на настоящите оценки на риска.

ЕС играе особена роля по отношение на гарантирането на устойчивостта на инфраструктурата, която пресича сухоземни или морски граници и засяга интересите на няколко държави членки, или която се използва за предоставяне на основни

трансгранични услуги. Критичната инфраструктура от значение за няколко държави членки обаче може да се намира само в една държава членка или дори извън територията на държава членка, например в случай на подводни кабели или тръбопроводи. Ясното идентифициране на критичната инфраструктура и субектите, които я експлоатират, както и на рисковете, на които е изложена, и колективният ангажимент за тяхната защита са в интерес на всички държави членки и на ЕС като цяло.

Европейският парламент и Съветът вече постигнаха политическо съгласие за задълбочаване на законодателната рамка на ЕС, за да се подпомогне укрепването на устойчивостта на субектите, експлоатиращи критична инфраструктура. През лятото на 2022 г. бяха постигнати споразумения по Директивата относно устойчивостта на критичната инфраструктура („Директивата за УКС“)[1] и Директивата относно сигурността на мрежите и информационните системи („Директивата за МИС 2“)[2]. Те ще представляват значително увеличаване на способностите в сравнение със съществуващата законодателна рамка, Директива 2008/114/ЕО от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита (Директива за ЕКИ“)[3] и Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза („Директивата за МИС“)[4]. Очаква се новото законодателство да влезе в сила в края на 2022 г. или началото на 2023 г., а транспонирането и прилагането следва да бъдат приоритизирани от държавите членки в съответствие с правото на Съюза.

При това положение и като се има предвид потенциалната неотложност за справяне със заплахите, произтичащи от военната агресия на Русия срещу Украйна, стъпките, очертани в новото законодателство, следва, когато е възможно, да бъдат приложени с приоритет. Засилването още сега на взаимното сътрудничество ще спомогне и за създаването на импулс за ефективно прилагане, когато новото законодателство влезе изцяло в сила.

Резултатът би бил вече да се премине отвъд настоящата рамка, както по отношение на дълбочината на действие, така и по отношение на броя на обхванатите сектори. С новата Директива за УКС се предлага нова рамка за сътрудничество, както и задължения за държавите членки и критичните субекти, насочени към укрепване на физическата устойчивост спрямо природни и причинени от човека заплахи от страна на субекти, извън киберпространството, които предоставят основни услуги на вътрешния пазар, като се посочват единадесет сектора[5]. С Директивата за МИС 2 ще се въведе широк секторен обхват на задълженията в областта на киберсигурността. Тя ще съдържа ново изискване за държавите членки да включат, когато е уместно, подводните кабели в своите стратегии за киберсигурност.

Законодателството изисква от Комисията да поеме съществена координираща роля. Съгласно Директивата за УКС Комисията има поддържаща и улесняваща роля, която трябва да изпълнява с подкрепата и участието на Групата за устойчивост на критичните

---

1 COM(2020)829 final
2 COM(2020) 823 final
3 ОВ L 345, 23.12.2008 г.
4 ОВ L194, 19.7.2016 г.
5 Енергетика, транспорт, цифрова инфраструктура, банково дело, инфраструктура на финансовия пазар, здравеопазване, питейна вода, отпадъчни води, публична администрация, космическо пространство и храни

субекти, създадена с посочената директива, и следва да допълва дейностите на държавите членки чрез разработване на най-добри практики, материали с насоки и методики. Що се отнася до киберсигурността, в заключенията си от лятото на 2022 г. относно състоянието на киберсигурността на ЕС Съветът прикани Комисията, върховния представител и групата за сътрудничество за МИС да работят по оценките на риска и сценариите от гледна точка на киберсигурността. Такава координация може да вдъхнови подход спрямо други ключови критични инфраструктури.

На 5 октомври 2022 г. председателят Фон дер Лайен представи план от 5 точки, в който се определя координиран подход към предстоящата работа, която е необходимо да бъде извършена. Основните му елементи бяха: повишаване на подготвеността; работа с държавите членки с цел извършване на стрес тестове на критичната им инфраструктура, като се започне с енергийния сектор и се продължи с други високорискови сектори; увеличаване на капацитета за реагиране, по-специално чрез Механизма за гражданска защита на Съюза; пълноценно използване на спътниковия капацитет за откриване на потенциални заплахи; и засилване на сътрудничеството с НАТО и ключови партньори относно устойчивостта на критичната инфраструктура. В плана от 5 точки се подчертава значението на влизането в сила на законодателството, по което вече има политическо съгласие.

Предложената препоръка на Съвета приветства този подход, за да се структурира подкрепата за държавите членки и да се координират усилията им за повишаване на осведомеността относно рисковете, подготвеността и реагирането на настоящите заплахи. Във връзка с това се свикват срещи на експерти, за да се обсъди устойчивостта на субектите, експлоатиращи критична инфраструктура, в очакване на влизането в сила на Директивата за УКС и създадената с нея Група за устойчивост на критичните субекти.

Засиленото сътрудничество с ключови партньори и съседни и други заинтересовани трети държави относно устойчивостта на субектите, експлоатиращи критична инфраструктура, ще бъде от съществено значение, по-специално чрез структурирания диалог между ЕС и НАТО относно устойчивостта.

Акцентът на настоящата препоръка е укрепването на капацитета на Съюза за предвиждане, предотвратяване и реагиране на новите заплахи, произтичащи от военната агресия на Русия срещу Украйна. Поради това в предложените препоръки се поставя акцент върху справянето със свързаните със сигурността рискове и заплахи за критичната инфраструктура. При все това следва да се отбележи, че неотдавнашните събития също подчертаха належащата необходимост да се обърне по-голямо внимание на въздействието на изменението на климата върху критичните инфраструктура и услуги по отношение например на сезонно застрашеното и непредвидимо водоснабдяване за охлаждане на атомните електроцентрали, за водноелектрическата енергия и корабоплаването по вътрешните водни пътища, или на риска от материални щети на транспортната инфраструктура, които могат да причинят сериозни смущения в основните услуги. Тези опасения ще продължат да бъдат адресирани чрез подходящо законодателство и координация.

- **Съгласуваност с действащите разпоредби в тази област на политиката**

Настоящото предложение за препоръка на Съвета е в пълно съответствие с действащата и бъдещата правна рамка относно устойчивостта на субектите, експлоатиращи критична инфраструктура, съответно Директивата за ЕКИ и Директивата за УКС, тъй като има за цел, наред с другото, да улесни сътрудничеството между държавите членки в тази област и да подкрепи конкретни мерки за повишаване на устойчивостта срещу

настоящите непосредствени заплахи срещу субекти, експлоатиращи критична инфраструктура в ЕС.

С него също така се допълва Директивата за УКС, като държавите членки се приканват да дадат приоритет на навременното транспониране на директивата, чрез сътрудничество посредством срещи на експерти, свикани като част от обявения от Комисията план от 5 точки, и като се цели да се координира пътят към общ подход за провеждане на стрес тестове на критичната инфраструктура в ЕС.

Предложението е в съответствие и с Директивата за МИС и предстоящата Директива за МИС 2, която ще отмени Директивата за МИС, като призовава за ранно започване на работата по прилагането и транспонирането. В него са отразени също така съвместния призив от март 2022 г., направен в град Невер, Франция, както и заключенията на Съвета относно позицията на ЕС в киберпространството от май 2022 г. по отношение на искането на държавите членки към Комисията да разработи оценки на риска и сценарии за риска.

Предложението е в съответствие и с политиката на ЕС в областта на гражданската защита, когато в случай на сериозно прекъсване на операциите на критичната инфраструктура/критичните субекти държавите членки и трети държави могат да поискат помощ чрез Координационния център за реагиране при извънредни ситуации в рамките на Механизма за гражданска защита на Съюза. В случай на задействане на Механизма за гражданска защита на Съюза Координационният център за реагиране при извънредни ситуации е в състояние да координира и съфинансира разполагането в засегнатата държава на основно оборудване, материали и експертен опит, налични в държавите членки (отчасти в контекста на Европейския резерв за гражданска защита) и в рамките на rescEU. Помощта, която може да бъде предоставена при поискване, включва например горива, генератори, електроенергийна инфраструктура, капацитет за подслон, капацитет за пречистване на вода и капацитет за спешна медицинска помощ.

Предложението е в съответствие и с достиженията на правото на ЕС, свързани със сигурността на енергийните доставки.

Секторът на ядрената енергетика не е изрично включен в предложената препоръка на Съвета, с изключение например на свързаната с него инфраструктура (като преносните линии към атомни електроцентрали), която може да засегне сигурността на доставките. Специфични ядрени елементи са обхванати от съответното законодателство в областта на ядрената енергетика съгласно Договора за Евратом и/или националното законодателство[6]. Въз основа на поуките от аварията във Фукушима европейското законодателство в областта на ядрената безопасност беше подсилено и вследствие на това националните органи трябва редовно да извършват периодични прегледи на безопасността за всяка инсталация, за да се гарантира непрекъснатото спазване на най-високите изисквания за безопасност и да се набележат допълнителни подобрения на безопасността, както и шест годишни тематични партньорски проверки на равнище ЕС.

В Стратегията на ЕС за морска сигурност[7] и нейния план за действие[8] се подчертава променящият се характер на заплахите в морската област и се призовава за подновяване на ангажимента за защита на критичната морска инфраструктура, включително подводната, и по-специално морската транспортна, енергийна и

6 Съображение 9 от Директива 2008/114/ЕО на Съвета (Директива за ЕКИ)
7 11205/14
8 10494/18

комуникационна инфраструктура, наред с другото като се повиши осведомеността за морската среда чрез подобрена оперативна съвместимост и рационализиран обмен на информация.

Предложението е в съответствие и с други приложими секторни законодателни актове. Поради това изпълнението на настоящата препоръка следва да бъде съгласувано с конкретни мерки, които регулират или могат да регулират в бъдеще някои аспекти на устойчивостта на субектите, извършващи дейност в засегнати сектори, като например транспорта. Това включва други съответни инициативи, като например плана за действие в извънредни ситуации в областта на транспорта[9] или плана за действие при извънредни ситуации за гарантиране на доставките на храни и продоволствената сигурност по време на криза[10] и свързания с него Европейски механизъм за готовност и реакция в областта на продоволствената сигурност. В по-общ план препоръката следва естествено да се прилага при пълно зачитане на всички приложими правила на правото на ЕС, включително тези, определени в директивите за ЕКИ и МИС.

Предложението е в съответствие и със Стратегическия компас за сигурност и отбрана, в който се подчертава необходимостта от значително повишаване на устойчивостта и способността за борба с хибридните заплахи и кибератаките, както и необходимостта от укрепване на устойчивостта на държавите партньори и от сътрудничество с НАТО. То е в съответствие и с рамката за координиран отговор на ЕС на хибридните заплахи и кампании, засягащи ЕС, държавите членки и партньорите[11].

2. ПРАВНО ОСНОВАНИЕ, СУБСИДИАРНОСТ И ПРОПОРЦИОНАЛНОСТ

• Правно основание

Предложението се основава на член 114 от Договора за функционирането на Европейския съюз (ДФЕС), който включва сближаване на законодателствата с цел подобряване на функционирането на вътрешния пазар, заедно с член 292 от ДФЕС. Това е обосновано от факта, че предложената препоръка на Съвета има за основна цел да предвиди мерките, установени в новите директиви за УКС и МИС 2, които се основават и на член 114 от ДФЕС. В съответствие с логиката, обосноваваща използването на този член като правно основание за тези директиви, са необходими действия от страна на ЕС, за да се гарантира гладкото функциониране на вътрешния пазар, по-специално с оглед на трансграничния характер и обхвата на съответните услуги и потенциалните последици в случай на смущения, както и с оглед на съществуващите и бъдещите национални мерки, насочени към повишаване на устойчивостта на субектите, експлоатиращи критична инфраструктура, използвана за предоставяне на основни услуги на вътрешния пазар.

• Субсидиарност (при неизключителна компетентност)

Предприемането на мерки на европейско равнище в областта на устойчивостта на субектите, експлоатиращи критична инфраструктура, са оправдани, като се има предвид взаимозависимият трансграничен характер на отношенията между операциите на критичната инфраструктура и предоставяните основни услуги, както и

---

9 COM(2022)211

10 COM(2021)689

11 Съвет на Европейския съюз 10016/22, 21 юни 2022 г.

необходимостта от по-общ и координиран европейски подход, за да се гарантира, че съответните субекти са достатъчно устойчиви в настоящия геополитически контекст. Като има предвид, че много от общите предизвикателства, като например явният саботаж на газопроводите „Северен поток“, се решават преди всичко чрез национални мерки или от субекти, експлоатиращи критична инфраструктура, подкрепата на ЕС, включително съответните агенции, когато е целесъобразно, е необходима за увеличаване на устойчивостта, подобряване на бдителността и укрепване на колективния отговор на ЕС.

- **Пропорционалност**

Настоящото предложение е в съответствие с принципа на пропорционалност, предвиден в член 5, параграф 4 от Договора за Европейския съюз.

Нито съдържанието, нито форматът на настоящата предложена препоръка на Съвета не надвишават необходимото за постигане на нейните цели. Предложените действия са пропорционални на преследваните цели, тъй като зачитат прерогативите и задълженията на държавите членки съгласно националното право.

И накрая, предложението включва потенциален диференциран подход, който отразява различните вътрешни реалности на държавите членки по отношение на подготвеността и реагирането на физически заплахи за критичната инфраструктура.

- **Избор на инструмент**

За да се постигнат посочените по-горе цели, ДФЕС предвижда приемането от Съвета на препоръки, по-специално в член 292, въз основа на предложение на Комисията. Препоръката на Съвета е подходящ инструмент в този случай, като се има предвид и настоящият законодателен контекст, както е обяснено по-горе. Като правен акт, въпреки че е с необвързващ характер, препоръката на Съвета сигнализира ангажимента на държавите членки към включените мерки и предоставя солидна политическа основа за сътрудничество в тези области, като същевременно напълно зачита правомощията на държавите членки.

3. РЕЗУЛТАТИ ОТ ПОСЛЕДВАЩИТЕ ОЦЕНКИ, КОНСУЛТАЦИИТЕ СЪС ЗАИНТЕРЕСОВАНИТЕ СТРАНИ И ОЦЕНКИТЕ НА ВЪЗДЕЙСТВИЕТО

- **Консултации със заинтересованите страни**

При разработването на настоящото предложение бяха взети предвид становищата на експертите от държавите членки, изразени на срещата от 12 октомври 2022 г. Налице бе широк консенсус относно ползата от по-голяма координация на равнището на Съюза по отношение на готовността и реакцията в настоящия контекст на заплахи и за предварителни мерки по някои елементи от Директивата за УКС преди официалното ѝ приемане. Държавите членки изразиха готовност за обмен на опит и най-добри практики относно мерките и методиките за повишаване на устойчивостта на субектите, експлоатиращи критична инфраструктура. Държавите членки също така изразиха готовност за координиран подход към стрес тестовете на субектите, експлоатиращи критична инфраструктура, на доброволна основа и въз основа на общи принципи. Държавите членки посочиха, че субектите, експлоатиращи критична инфраструктура в секторите на енергетиката, цифровата инфраструктура и транспорта, следва да се считат за приоритетни за целите на настоящата препоръка, по-специално тези, които са от значение за няколко държави членки. Държавите членки приветстваха и

намерението на Комисията да свика допълнителни срещи на експерти от държавите членки през следващите седмици.

- **Подробно разяснение на отделните разпоредби на предложението**

Предложението за препоръка на Съвета гласи следното:

– В глава I се определят целта на предложението, какво обхваща то и приоритизирането на препоръчаните мерки.

– Глава II е съсредоточена върху мерките, които следва да бъдат предприети за подобряване на готовността както на равнището на Съюза, така и на равнището на държавите членки.

– Глава III обхваща засилената реакция както на равнището на ЕС, така и на равнището на държавите членки.

– Глава IV се отнася до международното сътрудничество и действията, които следва да бъдат предприети за повишаване на устойчивостта на субектите, експлоатиращи критична инфраструктура.

2022/0338 (NLE)

Предложение за

ПРЕПОРЪКА НА СЪВЕТА

относно координиран подход на Съюза за укрепване на устойчивостта на критичната инфраструктура

(текст от значение за ЕИП)

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) ЕС играе специална роля по отношение на инфраструктурата, която пресича границите и оказва въздействие върху интересите на няколко държави членки или която по друг начин се използва от субектите за предоставяне на основни трансгранични услуги. Такова предоставяне на услуги и критична инфраструктура от значение за няколко държави членки обаче може да се намира само в една държава членка или извън територията на държава членка, например в случай на подводни кабели или тръбопроводи. Ясното идентифициране на тази критична инфраструктура и на субектите, които я експлоатират, както и на рисковете, които ги заплашват, и колективният ангажимент за тяхната защита са в интерес на всички държави членки и на ЕС като цяло.

(2) Защитата на критичната инфраструктура в два сектора понастоящем се урежда от Директива 2008/114/ЕО на Съвета[12]. С посочената директива се създава процедура за установяване и означаване на европейски критични инфраструктури, както и общ подход за оценка на необходимостта от подобряване на защитата на тези инфраструктури, с цел да се допринесе за защитата на населението. Тя обхваща секторите на енергетиката и транспорта. С цел да се подобри устойчивостта на критичните субекти и услугите, които те предоставят, както и инфраструктурата, на която разчитат, нова директива относно устойчивостта на критичните субекти[13] („Директивата за УКС“) е в процес на приемане от законодателя на Съюза. Тя ще замени Директива 2008/114/ЕО, като ще обхваща повече сектори, включително цифровата инфраструктура.

---

12 Директива 2008/114/ЕО на Съвета от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита (ОВ L 345, 23.12.2008 г., стр. 75).

13 COM(2020)829

(3) Освен това Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза[14] се фокусира върху киберзаплахите. Тази директива ще бъде заменена с нова директива относно мерки за високо общо ниво на киберсигурност в Съюза[15] („Директива за МИС 2“), която също е в процес на приемане от законодателя на Съюза.

(4) С оглед на бързо изменящата се обстановка на заплахи, по-специално в контекста на очевидния саботаж на газовата инфраструктура „Северен поток 1 и 2“, субектите, експлоатиращи критична инфраструктура, са изправени пред особени предизвикателства по отношение на устойчивостта срещу враждебни действия и други предизвикани от човека заплахи, а свързаните с природните фактори и изменението на климата предизвикателства нарастват и могат да се съчетаят с враждебни действия. Поради това те трябва да предприемат, с подкрепата на държавите членки, подходящи мерки за повишаване на устойчивостта. Тези мерки следва да бъдат предприети и подкрепата да бъде предоставяна дори като се отиде по-далеч от мерките по Директива 2008/114/ЕО и Директива (ЕС) 2016/1148 и дори преди приемането, влизането в сила и транспонирането на новите директиви за УКС (Директива относно устойчивостта на критичните субекти) и МИС 2 (Директива за мрежовата и информационна сигурност).

(5) До приемането, влизането в сила и транспонирането на тези нови директиви Съюзът и държавите членки се насърчават, в съответствие с правото на Съюза, да използват всички налични инструменти, за да постигнат напредък и да спомогнат за укрепване на физическата устойчивост и киберустойчивостта на тези субекти и на критичната инфраструктура, която експлоатират, за да предоставят основни услуги на вътрешния пазар, т.е. услуги, които са от решаващо значение за поддържането на жизненоважни обществени функции, икономически дейности, общественото здраве и безопасност или околната среда. В това отношение понятието „устойчивост“ следва да се разбира като отнасящо се до способността на даден субект да предотвратява, защитава, реагира, устоява, смекчава, абсорбира, приспособява и да се възстановява от събития, които могат значително да нарушат или възпрепятстват предоставянето на въпросните основни услуги.

(6) За да се гарантира подход, който е както ефективен, така и възможно най-съгласуван с новата директива за УКС, мерките, съдържащи се в настоящата препоръка, следва да се отнасят до инфраструктура, определена от държава членка като критична инфраструктура, която обхваща както националната критична инфраструктура, така и европейската критична инфраструктура, независимо дали субектът, експлоатиращ критичната инфраструктура, вече е бил определен като критичен субект съгласно тази нова директива. За целите на настоящата препоръка терминът „критична инфраструктура“ следва да се разбира по съответния начин.

---

[14] Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

[15] COM(2020)823

(7) С оглед на съществуващите заплахи следва приоритетно да се предприемат мерки за повишаване на устойчивостта в ключовите сектори на енергетиката, цифровата инфраструктура, транспорта и космическото пространство, като тези мерки следва да се съсредоточат върху повишаването на устойчивостта на субектите, експлоатиращи критична инфраструктура, по отношение на породените от човека рискове. Когато става въпрос за национална критична инфраструктура, с оглед на възможните последици от настъпването на рисковете, следва да се даде приоритет на инфраструктура, която е с трансгранично значение.

(8) Съответно мерките, предвидени в настоящата препоръка, имат за основна цел да допълнят новите директиви за УКС и МИС 2, които се основават на член 114 от Договора за функционирането на Европейския съюз (ДФЕС), като предвиждат и допълват мерките, които ще бъдат посочени в тези нови директиви. Поради това и с оглед на трансграничния характер и значението на въпросните основни услуги и критична инфраструктура, както и на текущите и нововъзникващите различия в националните законодателства, които нарушават функционирането на вътрешния пазар, е целесъобразно настоящата препоръка да се основава и на член 114 от ДФЕС, заедно с член 292 от ДФЕС.

(9) Изпълнението на настоящата препоръка не следва да се разбира, че засяга текущите и бъдещите изисквания на правото на Съюза по отношение на някои аспекти на устойчивостта на съответните субекти и следва да съответства на тях. Тези изисквания са определени в общи инструменти като Директива 2008/114/ЕО и Директива (ЕС) 2016/1148 и новите директиви за УКС и МИС 2, които ги заменят, но също така и в някои специфични за сектора инструменти, като например в областта на транспорта, където, наред с другото, Комисията е предприела инициатива по отношение на плана за действие при извънредни ситуации в областта на транспорта[16]. В съответствие с принципа на лоялно сътрудничество настоящата препоръка следва да се прилага при пълно взаимно уважение и помощ.

(10) На 5 октомври 2022 г. Комисията обяви план от пет точки, в който се определя координиран подход за справяне с предстоящите предизвикателства, който включва работа по подготвеността чрез надграждане и предвиждане на приемането и влизането в сила на новата Директива за УКС, както и работа с държавите членки с цел извършване на стрес тестове на субекти, експлоатиращи критична инфраструктура, въз основа на общи принципи, като се започне с енергийния сектор. Чрез настоящата препоръка, която ще допринесе за този план, се приветства предложеният подход и се определя как той може да се превърне в действие.

(11) На фона на бързо изменящата се обстановка на заплахи и сегашната рискова среда, характеризираща се с породени от човека рискове, по-специално по отношение на критичната инфраструктура с трансгранично значение, от съществено значение е да се разполага с точна, актуална и пълна картина на най-важните рискове, пред които са изправени субектите, експлоатиращи критична инфраструктура. Поради това държавите членки следва да предприемат необходимите мерки за извършване или актуализиране на своите оценки на тези рискове. Въпреки че акцентът на настоящата препоръка е върху рисковете,

[16] COM(2022)211

свързани със сигурността, в допълнение следва да продължат усилията за справяне с изменението на климата и рисковете за околната среда, по-специално когато природните явления могат допълнително да изострят рисковете, породени от човека.

(12) Като се има предвид тази обстановка на заплахи, държавите членки следва да бъдат приканени да предприемат възможно най-скоро подходящи мерки за повишаване на устойчивостта на критичната инфраструктура, включително отиващи отвъд посочените оценки на риска, които впоследствие ще се изискват съгласно новата Директива за УКС.

(13) Като част от изпълнението на обявения от Комисията план от пет точки е необходимо да се координира работата чрез свикване на национални експерти, които да бъдат привлечени преди създаването на групата за устойчивост на критичните субекти с новата Директива за УКС, за да се даде възможност за сътрудничество между държавите членки и обмен на информация по отношение на устойчивостта на субектите, експлоатиращи критична инфраструктура. Това следва да включва сътрудничество и обмен на информация относно дейности като идентифициране на критичните субекти и инфраструктура, подготовка за разработването и насърчаването на общ набор от принципи за провеждане на стрес тестове и извличане на общи поуки от стрес тестовете, установяване на уязвимостите и възможните способности. Тези процеси следва също така да са от полза за устойчивостта на субектите, експлоатиращи критична инфраструктура, по отношение на рисковете, свързани с климата и околната среда. Тази работа ще даде възможност и за общо приоритизиране на работата по стрес тестовете, с акцент върху енергетиката, цифровата инфраструктура, транспорта и космическия сектор. Комисията вече започна да свиква тези експерти и да улеснява тяхната работа и възнамерява да продължи тази дейност. След като новата Директива за УКС влезе в сила и бъде създадена групата за устойчивост на критичните субекти, тази група следва да продължи работата по предвиждане в съответствие със задачите си съгласно Директивата относно УКС.

(14) Стрес тестовете следва да бъдат допълнени от изготвянето на подробен план за инциденти и кризи по критичната инфраструктура, в който се описват и определят целите и начините на сътрудничество между държавите членки и институциите, органите, службите и агенциите на ЕС в отговор на инциденти, свързани с критична инфраструктура, по-специално когато те водят до значителни нарушения в предоставянето на основни услуги за вътрешния пазар. За този подробен план следва да се използват съществуващите интегрирани договорености на ЕС за реакция на политическо равнище при кризи (IPCR), за да се координира реакцията, следва да е в съответствие и да се допълва взаимно с подробния план за мащабни киберинциденти и следва също така да предвиди постигане на съгласие по ключови послания за публична комуникация, като се има предвид, че комуникацията при кризи играе важна роля за смекчаване на отрицателните последици от инциденти и кризи при критичната инфраструктура.

(15) За да се осигури координиран и ефективен отговор на текущите и очакваните заплахи, Комисията ще предостави допълнителна подкрепа на държавите членки с цел повишаване на устойчивостта в контекста на тези заплахи, по-специално чрез предоставяне на съответната информация под формата на брифинги, ръководства и насоки, насърчаване на използването на финансирани от Съюза

проекти за научни изследвания и иновации, предприемане на необходимата дейност по предвиждане и оптимизиране на използването на активите за наблюдение на Съюза. ЕСВД, по-специално чрез Центъра на ЕС за анализ на информация, следва да предоставя оценки на заплахите.

(16) Съответните секторни агенции на Съюза и другите органи от значение следва също така да предоставят подкрепа по въпроси, свързани с устойчивостта, доколкото това позволяват съответните им мандати, определени в съответните инструменти на правото на Съюза. По-специално Агенцията на Европейския съюз за киберсигурност (ENISA) би могла да помага по въпроси, свързани с киберсигурността, Европейската агенция за морска безопасност (ЕАМБ) би могла да е от полза с експертния си опит в подпомагането на държавите членки чрез своята услуга за морско наблюдение по въпроси, свързани с морската сигурност и безопасност, Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) би могла да предоставя подкрепа във връзка със събирането на информация и разследванията при трансгранични действия в областта на правоприлагането, а Агенцията на Европейския съюз за космическата програма (EUSPA) и Сателитният център на ЕС (SatCen) могат да оказват подкрепа чрез операции в рамките на космическата програма на Съюза.

(17) Въпреки че основната отговорност за гарантиране на сигурността на критичната инфраструктура и засегнатите субекти се носи от държавите членки, е целесъобразно да се засили координацията на равнището на Съюза, особено с оглед на заплахите, които могат да окажат въздействие върху няколко държави членки едновременно, като например военната агресия на Русия срещу Украйна, или да засегнат устойчивостта и доброто функциониране на икономиката, единния пазар и обществата на Съюза.

(18) Настоящата препоръка не води до предоставяне на информация, чието разкриване противоречи на основните интереси на държавите членки в областта на националната сигурност, обществената сигурност или отбраната.

(19) С нарастващата взаимозависимост на физическите и цифровите инфраструктури злонамерените действия в киберпространството, насочени към критични области, могат да доведат до нарушаване или увреждане на физическата инфраструктура, а саботажът на физическата инфраструктура може да направи цифровите услуги недостъпни. С оглед на повишената заплаха, която представляват усъвършенстваните хибридни атаки, държавите членки следва също така да включат тези съображения в работата си по изпълнението на настоящата препоръка. С оглед на взаимовръзките между киберсигурността и физическата сигурност на операторите е важно работата по подготовката за транспонирането и прилагането на новата Директива за МИС 2 да започне възможно най-скоро, а също да напредва успоредно с това и работата съгласно новата Директива за УКС.

(20) В допълнение към повишаването на готовността е важно също така да се подобрят способностите за бърза и ефективна реакция в случай на възникване на рискове, засягащи предоставянето на основни услуги, предоставяни от субекти, експлоатиращи критична инфраструктура. Поради това настоящата препоръка следва да съдържа мерките, които следва да бъдат предприети както на равнището на държавите членки, така и на равнището на Съюза, включително засилено сътрудничество и обмен на информация в контекста на Механизма за

гражданска защита на Съюза и използване на съответните активи на космическата програма на Съюза.

(21) В отговор на поканата, отправена от Съвета в неговите заключения относно позицията на ЕС в киберпространството[17], Комисията, върховният представител на Съюза по въпросите на външните работи и политиката на сигурност („върховният представител“) и групата за сътрудничество, създадена с Директива (ЕС) 2016/1148 („групата за сътрудничество за МИС“), в координация със съответните граждански и военни органи и агенции и съществуващи мрежи, включително EU CyCLONe, провеждат оценка на риска и изготвят сценарии за риска от гледна точка на киберсигурността в ситуация на заплаха или възможна атака срещу държави членки или държави партньори. Тази дейност е съсредоточена върху критични сектори, включително енергетиката, цифровата инфраструктура, транспорта и космическото пространство.

(22) В съвместния призив на министрите на държавите членки от Невер[18] и в заключенията на Съвета относно позицията на ЕС в киберпространството също се призовава за укрепване на устойчивостта на комуникационната инфраструктура и мрежи в Съюза, като се отправят препоръки към държавите членки и Комисията въз основа на оценка на риска. Понастоящем тази оценка на риска се извършва от групата за сътрудничество за МИС с подкрепата на Комисията и ENISA и в сътрудничество с Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС). В оценката на риска и анализа на пропуските се разглеждат рисковете от кибератаки за различните подсектори на комуникационните инфраструктури, включително стационарни и мобилни инфраструктури, сателити, подводни кабели, интернет маршрутизация и т.н., като по този начин се осигурява основа за работата по настоящата препоръка. Тази оценка на риска ще предостави информация за текущата междусекторна оценка на риска в кибернетичното пространство и сценариите, поискани от Съвета в заключенията на Съвета от 23 май 2022 г.

(23) Тези две дейности ще бъдат съгласувани и координирани с дейността по изготвяне на сценарии, съсредоточени върху гражданската защита в контекста на широк спектър от природни и причинени от човека бедствия, включително събития, свързани с киберсигурността, и тяхното въздействие върху реалния живот, които понастоящем се разработват от Комисията и държавите членки съгласно Решение № 1313/2013/ЕС на Европейския парламент и на Съвета[19]. В интерес на ефикасността, ефективността и последователността настоящата препоръка следва да се прилага, като се вземат предвид резултатите от тези дейности.

(24) В инструментариума на ЕС за киберсигурност на 5G технологиите[20] се определят съответните мерки и планове за смекчаване на последиците с цел укрепване на сигурността на 5G мрежите. С оглед на зависимостта на много основни услуги от 5G мрежите и взаимосвързания характер на цифровите екосистеми е от съществено значение всички държави членки спешно да

---

17 Позиция в киберпространството:Съветът одобрява заключения — Consilium (europa.eu)

18 https://www.regeringen.se/494477/contentassets/e5f13bec9b1140038eed9a3d0646f8cf/joint-call-to-reinforce-the-eus-cybersecurity-capabilities.pdf

19 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).

20 5g_eu_toolbox_72D70AC7-A9E7-D11D-BE17B0ED8A49D864_64468.pdf

постигнат изпълнението на мерките, препоръчани в инструментариума, и по-специално да приложат съответните ограничения по отношение на високорисковите доставчици за ключови активи, определени като критични и чувствителни в координираната на равнището на ЕС оценка на риска.

(25) С цел незабавно укрепване на готовността и капацитета за реагиране при сериозни киберинциденти Комисията създаде краткосрочна програма за подкрепа на държавите членки чрез допълнително финансиране, отпуснато на ENISA. Обхванатите услуги ще включват действия за подготвеност, като например тестване на проникването на критични субекти с цел установяване на уязвимости. С програмата също така ще се засилят възможностите за подпомагане на държавите членки в случай на сериозен инцидент, засягащ критични субекти. Това е първа стъпка в съответствие със заключенията на Съвета относно позицията в киберпространството, в които от Комисията се изисква да представи предложение за фонд за извънредни ситуации в киберпространството. Държавите членки следва да се възползват в пълна степен от тези възможности в съответствие с приложимите изисквания.

(26) Глобалната подводна кабелна мрежа за данни и електронни комуникации е от съществено значение за глобалната свързаност и свързаността в рамките на ЕС. Поради значителната дължина на тези кабели и инсталирането им на морското дъно, е изключително трудно да се наблюдават под водата повечето кабелни участъци. Споделената юрисдикция и други въпроси, свързани с юрисдикцията, засягащи тези кабели, представляват особен случай за европейското и международното сътрудничество в областта на защитата и възстановяването на инфраструктурата. Поради това е необходимо текущите и планираните оценки на риска по отношение на цифровите и физическите инфраструктури, които са в основата на цифровите услуги, да бъдат допълнени със специални оценки на риска и варианти за мерки за смекчаване на риска по отношение на подводните кабели. Поради това Комисията ще извърши проучвания за тази цел и ще сподели констатациите си с държавите членки.

(27) Определените в настоящата препоръка приоритетни сектори на енергетиката и транспорта могат да бъдат засегнати и от рискове, свързани с цифровата инфраструктура. Такова въздействие може да съществува например по отношение на енергийните технологии с цифрови компоненти. Сигурността на свързаните вериги на доставки е важна за непрекъснатостта на предоставянето на основни услуги и за стратегическия контрол на критичната инфраструктура, управлявана от субекти в енергийния сектор. Тези обстоятелства следва да бъдат взети предвид, когато се предприемат мерки за повишаване на устойчивостта на субектите, експлоатиращи критична инфраструктура, в съответствие с настоящата препоръка.

(28) Поради нарастващото значение на космическата инфраструктура и на космическите услуги за свързаните със сигурността дейности е от съществено значение да се гарантират устойчивостта и защитата на космическите активи и услуги на Съюза в рамките на ЕС, но също така и в рамките на настоящата препоръка, да се използват по-структурирано космическите данни и услуги, предоставяни от космическите системи и програми за наблюдение и защита на критичната инфраструктура в други сектори. Предстоящата космическа стратегия на ЕС за сигурност и отбрана ще предложи подходящи действия в това отношение, които следва да бъдат взети предвид при изпълнението на настоящата препоръка.

(29) Сътрудничеството на международно равнище е необходимо и с цел ефективно справяне с рисковете за устойчивостта на субектите, експлоатиращи критична инфраструктура, в Съюза или в съответните трети държави, или в международни води. Поради това държавите членки следва да бъдат приканени да си сътрудничат с Комисията и върховния представител, за да предприемат определени стъпки за постигането на тази цел, като се разбира, че всички такива стъпки се предприемат само в съответствие със съответните им задачи и отговорности съгласно правото на Съюза, по-специално разпоредбите на Договорите на ЕС относно външните отношения.

(30) Както е посочено в съобщението „Принос на Комисията към европейската отбрана“[21], в подкрепа на Стратегическия компас за сигурност и отбрана — За Европейски съюз, който защитава своите граждани, ценности и интереси и допринася за международния мир и сигурност[22], Комисията ще направи оценка на базовите критерии на ЕС за хибридна устойчивост по сектори в сътрудничество с върховния представител и държавите членки, като набележи пропуските и нуждите, както и стъпките за преодоляването им до 2023 г. Тази инициатива следва да предостави информация за работата по настоящата препоръка, като спомогне за засилване на обмена на информация и координацията на действията за по-нататъшно укрепване на устойчивостта, включително на критичната инфраструктура.

(31) Стратегията на ЕС за морска сигурност от 2014 г. и нейният план за действие призоваха за по-голяма защита на критичната морска инфраструктура, включително подводната, и по-специално морската транспортна, енергийна и комуникационна инфраструктура, наред с другото чрез повишаване на осведомеността за морската среда чрез подобрена оперативна съвместимост и рационализиран обмен на информация (задължителен и доброволен). Стратегията и планът за действие понастоящем се актуализират и ще включват засилени действия, насочени към защита на критичната морска инфраструктура. Тези действия следва да предоставят информация и да допълват настоящата препоръка.

(32) Държавите членки следва да вземат предвид пълния потенциал на програмата на Съюза за научни изследвания в областта на сигурността, по-специално като използват нейния специален приоритет за критичната инфраструктура, по-конкретно в рамките на програмите, финансирани от фонд „Вътрешна сигурност“, както и други потенциални възможности за финансиране на равнището на Съюза, по-специално Европейския фонд за регионално развитие, доколкото конкретните мерки отговарят на изискванията ѝ за допустимост. REPowerEU може също така да предложи възможности за финансиране за устойчивост. Всяко такова използване на възможностите, предлагани от финансирането от Съюза, трябва да се извършва в съответствие с приложимите правни изисквания.

ПРИЕ НАСТОЯЩАТА ПРЕПОРЪКА:

ГЛАВА I: ЦЕЛ, ОБХВАТ И ПРИОРИТИЗИРАНЕ

---

21 com_2022_60_1_en_act_contribution_european_defence.pdf (europa.eu)

22 Съвет на ЕС, 7371/22, 21 март 2022 г.

(1) С настоящата препоръка държавите членки се приканват да предприемат спешни и ефективни мерки и да си сътрудничат лоялно, ефикасно, солидарно и координирано помежду си, с Комисията и с други съответни публични органи, както и със съответните субекти, за да се повиши устойчивостта на критичната инфраструктура, използвана за предоставяне на основни услуги на вътрешния пазар.

(2) Мерките, посочени в настоящата препоръка, се отнасят до инфраструктура, определена от държава членка като критична инфраструктура, включително като европейска критична инфраструктура.

(3) При изпълнението на настоящата препоръка следва да се даде приоритет на повишаването на устойчивостта по отношение на породените от човека рискове на субектите, извършващи дейност в секторите на енергетиката, цифровата инфраструктура, транспорта и космическото пространство, както и на критичната инфраструктура, на която тези субекти извършват дейност, която е с трансгранично значение.

ГЛАВА II ПОВИШЕНА ПОДГОТВЕНОСТ

Действия на равнището на държавите членки

(4) Държавите членки се приканват да извършват или актуализират оценки на риска по отношение на устойчивостта на субектите, експлоатиращи европейска критична инфраструктура, определена в транспортния и енергийния сектор съгласно Директива 2008/114/ЕО, и да се стремят към сътрудничество помежду си по отношение на тези оценки на риска и на произтичащите от тях мерки за повишаване на устойчивостта, когато това е целесъобразно и в съответствие с посочената директива.

(5) Освен това и с цел да се постигне висока степен на устойчивост на субектите, експлоатиращи критична инфраструктура, държавите членки следва да засилят подготвителната работа, за да транспонират и приложат възможно най-скоро новата Директива за УКС, като:

а) ускорят приемането или актуализирането на национални стратегии за повишаване на устойчивостта на субектите, експлоатиращи критична инфраструктура, с оглед да се реагира на настоящата заплаха. Съответните части на стратегиите следва да бъдат съобщени на Комисията;

б) извършат или актуализират оценки на риска в съответствие с променящия се характер на настоящите заплахи по отношение на устойчивостта на субектите, експлоатиращи критична инфраструктура в съответните сектори, различни от енергетиката, цифровата инфраструктура, транспорта и космическото пространство, и когато е възможно в секторите, попадащи в обхвата на новата Директива за УКС, а именно банковото дело, инфраструктурата на финансовия пазар, цифровата инфраструктура, здравеопазването, питейната вода, отпадъчните води, публичната администрация, космическото пространство, както и производството, преработката и разпространението на храни, като се взема предвид потенциалният хибриден характер на съответните заплахи, включително верижните последици и последиците от изменението на климата;

в) информират Комисията за видовете рискове, установени по сектори и подсектори, и за резултатите от оценките на риска, което могат да направят с помощта на общ образец за докладване, разработен от Комисията в сътрудничество с държавите членки;

г) ускорят процеса на установяване и определяне на критични субекти, като с приоритет са критичните субекти, които:

д) използват критична инфраструктура, която е физически свързана между две или повече държави членки;

е) са част от корпоративни структури, свързани с критични субекти в други държави членки или имащи отношение към тях;

ж) са установени като такива в една държава членка и предоставят основни услуги във или на шест или повече държави членки и следователно са от особено европейско значение, и съответно информират Комисията;

з) сътрудничат помежду си, по-специално когато става въпрос за критични субекти и основни услуги и критична инфраструктура с трансгранично значение, най-вече като провеждат съвместни консултации за целите на точка 5, буква г) и се информират взаимно в случай на инцидент със значително или потенциално значително трансгранично отрицателно въздействие, като същевременно информират Комисията, както е целесъобразно;

и) засилят подкрепата за определени критични субекти с цел да се подобри тяхната устойчивост, което може да включва предоставяне на насоки и методики, организиране на учения за изпитване на тяхната устойчивост и предоставяне на консултации и обучение на техния персонал, както и предоставяне на възможност за цялостни проверки на лицата с чувствителни функции, в съответствие със законодателството на Съюза и националното законодателство, като част от мерките на критичните субекти за управление на сигурността на служителите;

й) ускорят определянето или създаването на единно звено за контакт в компетентния орган, което да изпълнява функция за връзка с цел осигуряване на трансгранично сътрудничество, свързано с устойчивостта на субектите, експлоатиращи критична инфраструктура, с единните звена за контакт на други държави членки.

(6) Държавите членки се насърчават да провеждат стрес тестове на субектите, експлоатиращи критична инфраструктура. По-специално държавите членки се приканват да повишат своята готовност и тази на съответните субекти в енергийния сектор и да провеждат стрес тестове в този сектор, когато е възможно, като следват съвместно договорените на равнището на Съюза принципи, като същевременно гарантират ефективна комуникация със съответните субекти. Стрес тестове в други приоритетни сектори, а именно цифровата инфраструктура, транспорта и космическото пространство, когато е необходимо, могат да бъдат разгледани впоследствие, като надлежно се вземат предвид инспекциите във въздушния и морския подсектор съгласно правото на Съюза и като се вземат предвид съответните разпоредби на секторното законодателство.

(7) Държавите членки се приканват да сътрудничат, когато е целесъобразно и в съответствие с правото на Съюза, със съответните трети държави по отношение на устойчивостта на субектите, експлоатиращи критична инфраструктура с трансгранично значение.

(8) Държавите членки се приканват да използват, в съответствие с приложимите изисквания, потенциалните възможности за финансиране на равнището на Съюза и на национално равнище, за да се повиши устойчивостта на субектите,

експлоатиращи критична инфраструктура в Съюза, включително например по трансевропейските мрежи, срещу пълния набор от значителни заплахи, по-специално в рамките на програмите, финансирани по линия на фонд „Вътрешна сигурност“ и Европейския фонд за регионално развитие, при условие че отговарят на съответните критерии за допустимост, и Механизма за свързване на Европа, включително разпоредбите относно устойчивостта спрямо изменението на климата. Финансирането по линия на Механизма за гражданска защита на Съюза може също да се използва за тази цел в съответствие с приложимите изисквания, по-специално за проекти, свързани с оценки на риска, инвестиционни планове или проучвания, изграждане на капацитет или подобряване на базата от знания. REPowerEU може също така да предложи възможности за финансиране на устойчивостта.

(9) Що се отнася до комуникационната и мрежовата инфраструктура в Съюза, групата за сътрудничество за МИС следва, като действа в съответствие с член 11 от Директива (ЕС) 2016/1148 и впоследствие член 14 от Директивата за МИС 2, да ускори текущата си работа по целева оценка на риска и следва да представи първите препоръки в началото на 2023 г. Тази работа следва да се извършва, като се гарантира съгласуваност и взаимно допълване с работата, извършвана от групата за сътрудничество за МИС в областта на сигурността на веригата за доставки на информационни и комуникационни технологии, както и от други съответни групи, като например групата за устойчивост на критичните субекти, която ще бъде създадена съгласно новата Директива за УКС, и надзорния форум, който ще бъде създаден съгласно новия Регламент относно оперативната устойчивост на цифровите технологии във финансовия сектор (DORA)[23].

(10) Групата за сътрудничество за МИС, която трябва да изпълнява задачите си в съответствие с член 11 от Директива (ЕС) 2016/1148 и впоследствие член 14 от Директивата за МИС 2, се приканва, с подкрепата на Комисията и ENISA, да даде приоритет на работата си по сигурността на цифровата инфраструктура и космическия сектор, включително чрез изготвяне на насоки за политиката и методики и мерки за управление на риска, свързан с киберсигурността, въз основа на подход, обхващащ всички опасности по отношение на подводните комуникационни кабели, в очакване на влизането в сила на Директивата за МИС 2, както и по разработването на насоки за мерки за управление на риска, свързан с киберсигурността, за операторите в космическия сектор с цел повишаване на устойчивостта на наземната инфраструктура в подкрепа на предоставянето на космически услуги.

(11) Държавите членки следва да използват пълноценно услугите за подготвеност в областта на киберсигурността, предлагани в рамките на програмата на Комисията за краткосрочна подкрепа, изпълнявана с ENISA, по-специално тестове на възможностите за проникване с цел да се идентифицират уязвимости, и в този контекст се насърчават да дадат приоритет на субектите, експлоатиращи критична инфраструктура в енергийния, цифровия и транспортния сектор.

[23] COM(2020) 595 final

(12) Държавите членки следва спешно да приложат мерките, препоръчани в инструментариума на ЕС за киберсигурността в областта на 5G[24]. Държавите членки, които все още не са въвели ограничения за високорисковите доставчици, следва да направят това незабавно, като се има предвид, че изгубеното време може да увеличи уязвимостта на мрежите в Съюза. Те следва също така да засилят физическата и нефизическата защита на критичните и чувствителните части на 5G мрежите, включително чрез строг контрол на достъпа. Освен това държавите членки, в сътрудничество с Комисията, следва да оценят необходимостта от допълнителни действия, включително правно обвързващи изисквания на равнището на Съюза, за да се гарантира постоянното равнище на сигурност и устойчивост на 5G мрежите.

(13) Държавите членки следва да приложат възможно най-скоро предстоящия мрежови кодекс за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия, като се основават на опита, натрупан при прилагането на Директивата за МИС, и на съответните насоки, изготвени от групата за сътрудничество за МИС, по-специално нейния референтен документ относно мерките за сигурност, предназначен за операторите на основни услуги.

(14) Държавите членки следва да разработят начини да използват „Галилео“ и/или „Коперник“ за наблюдение и да споделят съответната информация чрез експертите, свикани в съответствие с точка 15. Следва да се използват по подходящ начин възможностите, предлагани от правителствените сателитни комуникации на Съюза (GOVSATCOM) на космическата програма на Съюза за наблюдение на критичната инфраструктура и за подкрепа на реакцията при кризи.

Действия на равнището на Съюза

(15) Комисията възнамерява да засили сътрудничеството между експертите от държавите членки с цел да спомогне за повишаване на физическата устойчивост, различна от киберпространството, на субектите, експлоатиращи критична инфраструктура, по-специално като:

а) подготви разработването и насърчаването на общи инструменти за подпомагане на държавите членки при повишаването на тази устойчивост, включително методики и сценарии за риска;

б) подпомага разработването на общи принципи за провеждането на стрес тестовете, посочени в точка 6, от държавите членки, като се започне с тестове, съсредоточени върху причинените от човека рискове в енергийния сектор и впоследствие в други ключови сектори, като например цифровата инфраструктура, транспорта и космическото пространство; разгледа други значителни рискове и опасности; както и, когато е уместно, като подпомага и дава насоки относно провеждането на такива стрес тестове;

в) осигури сигурна платформа за събиране, преглед и споделяне на най-добри практики, изводи, направени вследствие на националния опит, и друга информация, свързана с устойчивостта, включително относно провеждането на стрес тестове и превръщането на резултатите от тях в протоколи и планове за действие при извънредни ситуации.

[24] https://op.europa.eu/bg/publication-detail/-/publication/7def1c03-da16-11eb-895a-01aa75ed71a1

Тези експерти следва да обърнат специално внимание на междусекторните зависимости и субектите, експлоатиращи критична инфраструктура с трансгранично значение, като тяхната работа следва да бъде продължена от групата за устойчивост на критичните субекти след нейното създаване.

(16) Държавите членки следва да участват пълноценно в засиленото сътрудничество, посочено в точка 15, включително като определят звена за контакт, които имат съответен експертен опит, и като споделят опит относно методиките, използвани за стрес тестовете, протоколите и плановете за действие при извънредни ситуации, разработени въз основа на тях. При обмена на информация се гарантират поверителността на информацията, както и сигурността и търговските интереси на критичните субекти, като се зачита сигурността на държавите членки. Това не включва предоставянето на информация, чието разкриване противоречи на основните интереси на държавите членки по отношение на националната сигурност, обществената сигурност или отбраната.

(17) Комисията ще подкрепя държавите членки, като предоставя наръчници и насоки, например като изготви наръчник за защита на критичната инфраструктура и обществените пространства срещу безпилотни летателни системи, както и инструменти за оценка на риска. ЕСВД, по-специално чрез Центъра на ЕС за анализ на информация и неговото звено за синтез на информацията за хибридните заплахи, се приканва да провежда брифинги относно заплахите за критичната инфраструктура в ЕС с цел подобряване на ситуационната осведоменост.

(18) Комисията ще подкрепя внедряването на резултатите от проекти, финансирани по програмите на Съюза за научни изследвания и иновации, относно устойчивостта на субекти, експлоатиращи критична инфраструктура. В рамките на бюджета, отпуснат за „Хоризонт Европа“ съгласно многогодишната финансова рамка за периода 2021—2027 г., Комисията възнамерява да увеличи предназначеното за тази устойчивост финансиране. Това следва да даде възможност за справяне с настоящите и бъдещите предизвикателства в тази област, като например осигуряването на устойчивост спрямо изменението на климата на критичната инфраструктура, без да се засягат средствата на друго финансиране за научни изследвания и иновации в областта на гражданската сигурност по линия на „Хоризонт Европа“. Комисията също така ще увеличи усилията си за разпространение на резултатите от съответните научноизследователски проекти, финансирани от Съюза.

(19) Групата за сътрудничество за МИС, със съдействието на Комисията и върховния представител, се приканва да засили, съобразно съответните си задачи и отговорности съгласно правото на Съюза, работата със съответните мрежи и граждански и военни органи при извършването на оценка на риска и разработването на сценарии за риска в областта на киберсигурността с първоначален акцент върху енергетиката, комуникациите, транспорта и космическата инфраструктура, както и на взаимозависимостите между секторите и държавите членки. При това следва да се вземат предвид свързаните рискове за физическата инфраструктура, на която разчитат тези сектори. Оценките на риска и сценариите следва да се извършват редовно и следва да допълват и надграждат съществуващи или планирани оценки на риска в тези сектори, като се избягва дублирането, и да предоставят информация за дискусиите относно начините за укрепване на цялостната

устойчивост на субектите, експлоатиращи критична инфраструктура, и за справяне с уязвимостите.

(20) Комисията ще ускори дейностите си за подпомагане на подготвеността на държавите членки и реагирането при мащабни киберинциденти, като по-специално:

а) ще извърши, в допълнение към съответните оценки на риска в контекста на мрежовата и информационната сигурност, всеобхватно проучване, включително картографиране, в което се прави преглед на подводната кабелна инфраструктура, която свързва държавите членки една с друга и Европа с останалия свят, на нейния капацитет и излишък, както и на уязвимостите, рисковете за достъпността на услугите и намаляването на риска. Констатациите следва да бъдат споделени с държавите членки;

б) ще подпомогне готовността на държавите членки и институциите, органите и агенциите на ЕС (EUIBA) да реагират при мащабни киберинциденти.

(21) Комисията ще засили работата по прогнозни изпреварващи действия, включително в рамките на Механизма за гражданска защита на Съюза в сътрудничество с държавите членки съгласно членове 6 и 10 от Решение № 1313/2013/ЕС и под формата на планиране на действия при извънредни ситуации в подкрепа на оперативната готовност на Координационния център за реагиране при извънредни ситуации.

По-специално Комисията ще поеме следните ангажименти:

а) ще подкрепя работата в Координационния център за реагиране при извънредни ситуации, свързана с прогнозирането и междусекторната превенция, планирането на режима на подготвеност и реакция с цел предвиждане и подготовка за прекъсвания на предоставянето на основни услуги от субекти, експлоатиращи критична инфраструктура;

б) ще увеличи инвестициите в превантивни подходи и подготвеност на населението в случай на такива смущения, със специален акцент върху химически, биологични, радиологични и ядрени взривни вещества или други възникващи причинени от човека заплахи;

в) ще засили обмена на съответни знания и най-добри практики и ще подобри планирането и провеждането на дейности за развитие на капацитет, като например курсове за обучение и учения със субектите, експлоатиращи критична инфраструктура, чрез съществуващи структури и експертен опит, като например Мрежата на Съюза за знания в областта на гражданската защита.

(22) Комисията ще насърчава използването на средствата на ЕС за наблюдение („Коперник“ и „Галилео“) в подкрепа на държавите членки при мониторинга на критична инфраструктура и непосредствените околности, когато е целесъобразно, както и в подкрепа на други варианти за наблюдение, предвидени в космическата програма на Съюза.

(23) Когато е уместно и в съответствие със съответните им мандати, агенциите на Съюза и други съответни органи се приканват да предоставят подкрепа по въпроси, свързани с устойчивостта на субектите, експлоатиращи критична инфраструктура, по-специално:

а) Европол относно събирането на информация, криминалния анализ и подпомагането на разследванията при трансгранични действия по правоприлагане;

б) ЕАМБ по въпроси, свързани със сигурността и безопасността на морския сектор в Съюза, включително услуги за морско наблюдение по въпроси, свързани с морската сигурност и безопасност;

в) EUSPA по отношение на дейностите в рамките на космическата програма на Съюза;

г) ENISA по отношение на дейностите, свързани с киберсигурността.

ГЛАВА III: ПО-ДОБРА РЕАКЦИЯ

Действия на равнището на държавите членки

(24) Държавите членки следва:

а) да координират реакцията си и поддържат прегледа на междусекторното реагиране на значителни смущения в предоставянето на основни услуги от субекти, експлоатиращи критична инфраструктура в рамките на механизма на Съвета за реакция при кризи (IPCR), когато става въпрос за критична инфраструктура с трансгранично значение, на подробния план за координирана реакция при мащабни инциденти и кризи в областта на киберсигурността или на рамката за координиран отговор на ЕС на хибридни кампании в случай на хибридна кампания;

б) да засилят обмена на информация в рамките на Механизма за гражданска защита на Съюза с цел подобряване на ранното предупреждение и координиране на тяхната реакция в рамките на механизма в случай на такива значителни смущения, като по този начин се гарантира по-бърза реакция с посредничеството на Съюза, когато е необходимо;

в) да повишат готовността си да реагират чрез Механизма за гражданска защита на Съюза на такива значителни смущения, по-специално когато е вероятно те да имат значителни трансгранични или дори общоевропейски последици, както и междусекторни последици;

г) да поемат ангажименти към Комисията за по-нататъшното развитие на съответния капацитет за реагиране в рамките на Европейския резерв за гражданска защита (ECPP) и rescEU;

д) да приканват субектите, експлоатиращи критична инфраструктура, и съответните национални органи да подобрят капацитета на тези субекти за бързо възстановяване на основните работни параметри на предоставяните основни услуги;

е) да гарантират, че когато е необходимо възстановяването на критична инфраструктура, тя ще бъде устойчива спрямо пълния набор от значителни рискове, които могат да възникнат за нея, включително при неблагоприятни климатични сценарии.

(25) Държавите членки се приканват да ускорят подготвителната работа за транспонирането и прилагането на Директивата за МИС 2, като започнат незабавно да укрепват капацитета на националните екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) с оглед на новите задачи на ЕРИКС, както и на увеличения брой субекти от нови сектори, като

актуализират бързо своите стратегии за киберсигурност и приемат възможно най-скоро национални планове за реакция при инциденти и кризи в областта на киберсигурността.

Действия на равнището на Съюза

(26) Реакцията при значителни смущения в предоставянето на основни услуги от субекти, експлоатиращи критична инфраструктура, следва да се координира между експертите на държавите членки по отношение на устойчивостта на тези субекти и реакцията на такива смущения, което може да допринесе за функционирането на механизма на Съвета за реакция при кризи (IPCR).

(27) Комисията ще работи в тясно сътрудничество с държавите членки за по-нататъшното разработване на капацитет за реагиране при извънредни ситуации, включително експерти и запаси в rescEU в рамките на Механизма за гражданска защита на Съюза, с цел да се повиши оперативната готовност за справяне с непосредствените и непреките последици от значителните смущения в предоставянето на основни услуги от субекти, експлоатиращи критична инфраструктура.

(28) Като взема предвид променящата се картина на рисковете и в сътрудничество с държавите членки, в контекста на Механизма за гражданска защита на Съюза Комисията:

а) непрекъснато ще анализира и тества адекватността и оперативната готовност на съществуващия капацитет за реагиране;

б) редовно ще прави преглед на потенциалната необходимост от разработване на нов капацитет за реагиране на равнището на ЕС чрез rescEU;

в) допълнително ще засили междусекторното сътрудничество, за да се гарантира адекватна реакция на равнище ЕС, и ще организира редовни учения за тестване на това сътрудничество;

г) ще доразвие ERCC като междусекторен кризисен център на равнище ЕС за координиране на подкрепата за засегнатите държави членки.

(29) Комисията, в сътрудничество с върховния представител и в тясно сътрудничество с държавите членки и с подкрепата на съответните агенции на Съюза, ще разработи подробен план за инциденти и кризи с критичната инфраструктура, в който се описват и определят целите и начините на сътрудничество между държавите членки и институциите, органите, службите и агенциите на ЕС при реагирането на инциденти с критичната инфраструктура, по-специално когато те водят до значителни смущения в предоставянето на основни услуги за вътрешния пазар. За изготвянето на подробния план ще бъдат използвани съществуващите интегрирани договорености на ЕС за реакция на политическо равнище при кризи (IPCR), за да се координира реакцията.

(30) Комисията ще работи със заинтересованите страни и експертите по евентуални мерки за възстановяване при инциденти във връзка с инфраструктурата на подводните кабели, които мерки ще бъдат представени заедно с всеобхватното проучване, посочено в точка 20, буква а), както и по допълнителното разработване на планове за действие при извънредни ситуации, сценарии за риска и дейности за подобряване на устойчивостта на Съюза при бедствия в рамките на Механизма за гражданска защита на Съюза.

ГЛАВА IV: МЕЖДУНАРОДНО СЪТРУДНИЧЕСТВО

(31) Комисията и върховният представител ще подкрепят, когато е целесъобразно и в съответствие със съответните им задачи и отговорности съгласно правото на Съюза, държавите партньори по отношение на повишаването на устойчивостта на субектите, експлоатиращи критична инфраструктура на тяхна територия.

(32) Комисията и върховният представител, в съответствие със съответните си задачи и отговорности съгласно правото на Съюза, ще засилят координацията с НАТО по отношение на устойчивостта на критичната инфраструктура чрез структурирания диалог между ЕС и НАТО относно устойчивостта и ще създадат работна група за тази цел.

(33) Държавите членки се приканват да допринесат, в сътрудничество с Комисията и върховния представител, за по-бързото разработване и прилагане на инструментариума на ЕС за борба с хибридните заплахи и насоките за прилагане, посочени в заключенията на Съвета относно рамка за координиран отговор на ЕС на хибридни кампании[25], и впоследствие да ги използват, за да се гарантира пълното изпълнение на рамката за координиран отговор на ЕС на хибридни кампании, по-специално когато се обмислят и подготвят всеобхватни и координирани ответни действия на ЕС на хибридни кампании и хибридни заплахи, включително тези срещу субекти, експлоатиращи критична инфраструктура.

(34) Комисията ще обмисли участието на представители на трети държави, когато е уместно и целесъобразно, в рамките на сътрудничеството и обмена на информация между експерти от държавите членки в областта на устойчивостта на субектите, експлоатиращи критична инфраструктура.

[…]

Съставено в Страсбург на […] година.

За Съвета
Председател

[25] Заключения на Съвета относно рамка за координиран отговор на ЕС на хибридни кампании — Съвет на Европейския съюз (europa.eu)