Съвет на
Европейския съюз

Брюксел, 9 декември 2022 г.
(OR. en)

15623/22

Междуинституционално досие:
2022/0338(NLE)

PROCIV 149	ATO 102
ENV 1248	CSC 561
JAI 1617	ECOFIN 1279
SAN 650	CSCI 189
COSI 315	DATAPROTECT 346
CHIMIE 100	MI 912
ENFOPOL 619	CODEC 1916
RECH 645	COPS 581
CT 220	JAIEX 103
DENLEG 93	COPEN 430
COTER 297	IND 533
RELEX 1657	POLMIL 297
ENER 654	IPCR 116
HYBRID 116	DIGIT 231
TRANS 768	DISINFO 102
CYBER 397	CSDP/PSDC 848
TELECOM 512	MARE 71
ESPACE 125	POLMAR 78

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
До:	Делегациите
№ предх. док.:	13713/22, 15454/22
Относно:	ПРЕПОРЪКА НА СЪВЕТА относно координиран подход на равнището на Съюза за укрепване на устойчивостта на критичната инфраструктура

Приложено се изпраща на делегациите препоръката на Съвета относно координиран подход на равнището на Съюза за укрепване на устойчивостта на критичната инфраструктура, приета от Съвета на неговото 3920-о заседание, проведено на 8 декември 2022 г.

ПРИЛОЖЕНИЕ

ПРЕПОРЪКА (ЕС) 2022/… НА СЪВЕТА

от...

относно координиран подход на равнището 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 член 114 и член 292, първо и второ изречение от него,

като взе предвид предложението на Европейската комисия,

като има предвид, че:

1) С цел да се осигури функционирането на вътрешния пазар в интерес на всички държави членки и на Съюза като цяло е ясно да се определи и защити съответната критична инфраструктура, която предоставя основни услуги на този пазар, особено в ключови сектори като енергетиката, цифровата инфраструктура, транспорта и космическото пространство, както и критичната инфраструктура със значително трансгранично значение[1], чието нарушаване би могло да окаже значително въздействие върху други държави членки.

[1] Държавите членки следва да оценят тази целесъобразност в съответствие със своите национални практики и могат да го направят въз основа на оценка на риска и на въздействието или естеството на събитието, наред с други фактори.

2) Настоящата препоръка, която е необвързващ акт, показва политическата воля на държавите членки да си сътрудничат съвместно, и техния ангажимент към препоръчаните мерки, очертани в план от пет точки, изготвен от председателя на Европейската комисия, при пълно зачитане на компетентностите на държавите членки. Настоящата препоръка не засяга защитата на основните интереси на националната сигурност, обществената сигурност или отбраната на държавите членки и от никоя държава членка не следва да се очаква да обменя информация, която е в ущърб на тези интереси.

3) Въпреки че основната отговорност за гарантиране на сигурността и предоставянето на основни услуги от критичната инфраструктура се носи от държавите членки и от техните оператори на критични инфраструктури, е целесъобразно да се засили координацията на равнището на Съюза, особено предвид развитието на заплахите, които могат да окажат въздействие върху няколко държави членки едновременно, като например агресивната война на Русия срещу Украйна и хибридните кампании срещу държавите членки, или да засегнат устойчивостта и доброто функциониране на икономиката, вътрешния пазар и обществото на Съюза като цяло. Особено внимание следва да се обърне на критичната инфраструктура извън територията на държавите членки, като например подводната критична инфраструктура или морската енергийна инфраструктура.

4) В заключенията си от 20 и 21 октомври 2022 г. Европейският съвет категорично осъди актовете на саботаж срещу критичната инфраструктура, като например тези срещу газопроводите „Северен поток“, като посочи волята на Съюза да се справи с всяко умишлено прекъсване на критичната инфраструктура или други хибридни действия с единна и решителна реакция.

5) С оглед на бързо изменящата се обстановка на заплахи следва приоритетно да се предприемат мерки за повишаване на устойчивостта в ключови сектори като енергетиката, цифровата инфраструктура, транспорта и космическото пространство и в други имащи отношение към това сектори, определени от държавите членки. Тези мерки следва да се съсредоточат върху повишаването на устойчивостта на критичната инфраструктура, като се вземат предвид съответните рискове, особено каскадните ефекти, прекъсването на веригата на доставки, зависимостта, въздействието на изменението на климата, ненадеждните доставчици и партньори и хибридните заплахи и кампании, включително чуждестранното манипулиране на информация и вмешателство. Когато става въпрос за национална критична инфраструктура, с оглед на възможните последици, следва да се даде приоритет на критичната инфраструктура, която е със значително трансгранично значение. Държавите членки се насърчават спешно да осигурят такива мерки за повишаване на устойчивостта, когато е целесъобразно, като същевременно запазят подхода, изложен в развиващата се правна рамка.

(6) Защитата на европейската критична инфраструктура в енергийния и в транспортния сектор понастоящем се урежда от Директива 2008/114/ЕО на Съвета[2], а сигурността на мрежите и информационните системи в Съюза, с акцент върху киберзаплахите, е гарантирана от Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета[3]. С цел да се гарантира по-високо общо равнище на устойчивост и защитата на критичната инфраструктура, киберсигурността и финансовия пазар, съществуващата правна рамка се изменя и допълва с приемането на нови правила, приложими за критичните субекти (Директивата за УКС), по-строги правила за високо общо ниво на киберсигурност в Съюза (Директивата за МИС2) и нови правила, приложими за оперативната устойчивост на цифровите технологии във финансовия сектор (DORA).

7) Държавите членки следва, в съответствие с правото на Съюза и националното право, да използват всички налични инструменти, за да постигнат напредък и да спомогнат за укрепване на физическата и кибернетичната устойчивост. В това отношение критичната инфраструктура следва да се разбира като включваща съответната критична инфраструктура, установена от държава членка на национално равнище или определена като европейска критична инфраструктура съгласно Директива 2008/114/ЕО, както и критичните субекти, които трябва да бъдат установени съгласно Директивата за УКС, или субектите, които попадат в обхвата на Директивата за МИС2, когато е приложимо. Понятието за устойчивост следва да се разбира като отнасящо се до способността на дадена критична инфраструктура да предотвратява събития, да се защитава и да реагира при такива, да им устоява, да ги смекчава и поема, да се приспособява към тях или да се възстановява от такива събития, които нарушават или имат потенциал да нарушат значително предоставянето на основни услуги на вътрешния пазар, т.е. услуги, които са от решаващо значение за поддържането на жизненоважни обществени и икономически функции, обществената безопасност и сигурност, здравето на населението или околната среда.

---

2 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).

3 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).

8) За да се координира работата за постигане на по-високо общо равнище на устойчивост и защита на критичната инфраструктура, което ще бъде въведено с предстоящите нови правила, приложими за критичните субекти, следва да бъдат свикани национални експерти. Координираната работа ще даде възможност за сътрудничество между държавите членки и за споделяне на информация относно дейностите, като например разработването на методики за определяне на основните услуги, предоставяни от критичната инфраструктура. Комисията вече започна да свиква тези експерти и да улеснява тяхната работа, и възнамерява да продължи тази дейност. След като Директивата за УКС влезе в сила и бъде създадена Групата по въпросите на устойчивостта на критичните субекти съгласно посочената директива, тази група следва да продължи работата по прогнозиране в съответствие със задачите си.

9) Като се отчита променената обстановка на заплахите, потенциалът за провеждане на стрес тестове на критичната инфраструктура на национално равнище следва да бъде доразвит, тъй като такива тестове биха могли да бъдат полезни за повишаване на устойчивостта на критичната инфраструктура. Що се отнася до специфичното значение на енергийния сектор и последиците за целия Съюз, произтичащи от евентуалните смущения в него, този сектор би могъл да се възползва в най-голяма степен от провеждането на стрес тестове въз основа на общоприети принципи. Тези тестове попадат в сферата на компетентност на държавите членки, които следва да насърчават и подкрепят операторите на критична инфраструктура да провеждат такива тестове, когато те бъдат оценени като полезни и в съответствие с техните национални правни рамки.

10) За да се осигури координиран и ефективен отговор на текущите и очакваните заплахи, Комисията се насърчава да предостави допълнителна подкрепа на държавите членки, по-специално чрез предоставяне на съответната информация под формата на брифинги, незадължителни наръчници и насоки. Европейската служба за външна дейност (ЕСВД), по-специално чрез Центъра на ЕС за анализ на информация и неговото Звено за синтез на информацията за хибридните заплахи, с подкрепата на Дирекция „Разузнаване“ на Военния секретариат на Европейския съюз (ВСЕС) съгласно рамката на единното звено за анализ на разузнавателна информация (SIAC), следва да представя оценки на заплахите. Комисията се приканва освен това, в сътрудничество с държавите членки, да насърчава внедряването на финансирани от Съюза проекти за научни изследвания и иновации.

11) С нарастващата взаимозависимост на физическата и цифровата инфраструктура е възможно злонамерените действия в киберпространството, насочени срещу критични области, да доведат до нарушаване или увреждане на физическата инфраструктура, или до нейния саботаж, за да се доведе до недостъпност на цифровите услуги. Държавите членки се приканват да ускорят подготвителната работа за транспонирането и прилагането, възможно най-скоро, на новата правна рамка, приложима за критичните субекти, и на засилената правна рамка в областта на киберсигурността, като се основават на опита, натрупан в рамките на Групата за сътрудничество, създадена с Директива (ЕС) 2016/1148 (Групата за сътрудничество за МИС), като същевременно се вземат предвид сроковете за транспониране, а също и това, че тази работа следва да напредва успоредно и съгласувано.

12) В допълнение към повишаването на готовността е важно също така да се подобрят способностите за бърза и ефективна реакция в случай на смущения на основните услуги, предоставяни от критична инфраструктура. Поради това настоящата препоръка съдържа мерки както на равнището на Съюза, така и на национално равнище, включително като подчертава подкрепящата роля и добавената стойност, които могат да бъдат постигнати чрез въвеждането на засилено сътрудничество и обмен на информация в контекста на Механизма за гражданска защита на Съюза (МГЗС), създаден с решение № 1313/2013/ЕС на Европейския парламент и на Съвета[4], и чрез използването на съответните активи на космическата програма на Съюза, създадена с Регламент (ЕС) 2021/696 на Европейския парламент и на Съвета[5].

13) Комисията, върховният представител на Съюза по въпросите на външните работи и политиката на сигурност („върховният представител“) и Групата за сътрудничество за МИС в сътрудничество със съответните граждански и военни органи и агенции и установените мрежи, включително Европейската мрежа за връзка на организациите при киберкризи (EU-CyCLONe), трябва да извършат оценка на риска и да разработят сценарии за риска. Освен това, като последваща мярка след съвместния призив на министрите на държавите членки от Невер, понастоящем се извършва оценка на риска от Групата за сътрудничество за МИС с подкрепата на Комисията и на Агенцията на Европейския съюз за киберсигурност (ENISA) и в сътрудничество с Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС). Тези два процеса ще бъдат съгласувани и координирани с процеса на изработване на сценарии в рамките на МГЗС, включително за събития, свързани с киберсигурността, и тяхното реално въздействие, който процес понастоящем се разработва от Комисията и държавите членки. В интерес на ефикасността, ефективността и последователността, както и за правилното прилагане на настоящата препоръка, се очаква резултатите от тези процеси да бъдат отразени на национално равнище.

---

4 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).

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

14) С цел незабавно укрепване на готовността и капацитета за реагиране при мащабни инциденти в областта на киберсигурността Комисията създаде краткосрочна програма за подкрепа на държавите членки чрез допълнително финансиране, отпуснато на ENISA. Предложените услуги включват наред с останалото действия за подготвеност, като например тестване на проникването в критични субекти с цел установяване на уязвимости. Програмата може също така да засили възможностите за подпомагане на държавите членки в случай на мащабен инцидент в областта на киберсигурността, засягащ критични субекти. Това е първа стъпка в съответствие със заключенията на Съвета от 23 май 2022 г. относно установяването на позицията на Европейския съюз в киберпространството („заключенията на Съвета относно позицията на ЕС в киберпространството“), в които от Комисията се изисква да представи предложение за фонд за извънредни случаи в сферата на киберпространството. Държавите членки следва да се възползват в пълна степен от тези възможности в съответствие с приложимите изисквания и се насърчават да продължат работата в областта на управлението на киберкризи в Съюза, по-специално чрез редовно наблюдение и преглед на напредъка, постигнат в изпълнението на пътната карта за управление на киберкризи, разработена наскоро в Съвета. Тази пътна карта е непрекъснато развиващ се документ и следва да бъде преразглеждана и актуализирана, когато е необходимо.

15) Глобалната мрежа от подводни комуникационни кабели е от съществено значение за глобалната свързаност и свързаността в рамките на ЕС. Поради значителната дължина на този тип 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 този тип кабели, представляват специфичен 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 цифровата и физическата инфраструктура, 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. Държавите членки приканват Комисията да извърши проучвания за тази цел и да сподели констатациите си с държавите членки.

16) Секторите на енергетиката и транспорта също могат да бъдат засегнати от заплахи, свързани с цифровата инфраструктура, например във връзка с енергийните технологии, включващи цифрови компоненти. Сигурността на свързаните с тях вериги на доставки е важна за непрекъснатостта на предоставянето на основни услуги и за стратегическия контрол на критичната инфраструктура в енергийния сектор. Тези обстоятелства следва да бъдат взети предвид, когато се предприемат мерки за повишаване на устойчивостта на критичната инфраструктура в съответствие с настоящата препоръка.

17) Поради нарастващото значение на космическата инфраструктура, свързаните с космоса наземни активи, включително производствените съоръжения, и космическите услуги за свързани със сигурността дейности, от съществено значение е да се гарантират устойчивостта и защитата на космическите и наземни активи и услуги на Съюза в рамките на ЕС. Поради същите причини е от съществено значение, в рамките на настоящата препоръка, да се използват по-структурирано космическите данни и услуги, които се предоставят от космически системи и програми за наблюдение и проследяване и за 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.

18) Сътрудничеството на международно равнище е необходимо и с цел ефективно справяне с рисковете за критичната инфраструктура, наред с другото, в международни води. Поради това държавите членки се приканват да си сътрудничат с Комисията и с върховния представител, за да предприемат определени стъпки за постигането на тази цел, като имат предвид, че всички такива стъпки се предприемат само съгласно съответните им задачи и отговорности според правото на Съюза, по-специално разпоредбите на Договорите относно външните отношения.

19) Както е посочено в съобщението на Комисията от 15 февруари 2022 г., озаглавено „Принос на Комисията към европейската отбрана“, 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“, Комисията ще направи оценка на базовите критерии 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.

20) В Стратегията на ЕС за морска сигурност от 2014 г. и нейния преразгледан план за действие се призовава за по-голяма защита на критичната морска инфраструктура, включително подводната, и по-специално на морската транспортна, енергийна и комуникационна инфраструктура, наред с другото чрез повишаване на морската осведоменост посредством 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 допълват настоящата препоръка.

21) Укрепването на устойчивостта на критичната инфраструктура допринася за по-широките усилия за борба с хибридните заплахи и кампании срещу Съюза и неговите държави членки. Настоящата препоръка се основава на съвместното съобщение до Европейския парламент и Съвета, озаглавено „Съвместна рамка за борба с хибридните заплахи — ответни действия на Европейския съюз“. Действие 1 от съвместната рамка, а именно проучването на хибридните рискове, играе ключова роля за установяване на уязвимостите, които потенциално засягат националните и общоевропейските структури и мрежи. Освен това изпълнението на заключенията на Съвета от 21 юни 2022 г. относно рамка за координиран отговор на ЕС на хибридни кампании ще осигури по-решителни координирани действия чрез прилагането на инструментариума на ЕС срещу хибридни заплахи във всички засегнати области,

ПРИЕ НАСТОЯЩАТА ПРЕПОРЪКА:

ГЛАВА I: ЦЕЛ, ОБХВАТ И ПРИОРИТЕТИ

1) В настоящата препоръка се определят редица целенасочени действия на равнището на Съюза и на национално равнище за подкрепа и повишаване на устойчивостта на критичната инфраструктура на доброволна основа, с акцент върху критичната инфраструктура със значително трансгранично значение и в определени ключови сектори като енергетиката, цифровата инфраструктура, транспорта и космическото пространство. Тези целенасочени действия се състоят от повишена готовност, по-добра реакция и международно сътрудничество.

2) Информацията, споделяна с оглед на изпълнението на целите на настоящата препоръка, която е поверителна съгласно правилата на Съюза и националните правила, както и съгласно правилата за търговската тайна, следва да се обменя с Комисията и с други имащи отношение органи само когато този обмен е необходим за правилното прилагане на настоящата препоръка. Настоящата препоръка не засяга защитата на основните интереси на националната сигурност, обществената сигурност или отбраната на държавите членки и от никоя държава членка не следва да се очаква да обменя информация, която противоречи на тези интереси.

ГЛАВА II: ПОВИШАВАНЕ НА ПОДГОТВЕНОСТТА

Действия на равнището на държавите членки

3) Държавите членки следва да обмислят подход, обхващащ всички опасности, когато актуализират своите оценки на риска или съществуващите еквивалентни анализи в съответствие с променящия се характер на текущите заплахи за тяхната критична инфраструктура, особено в набелязани ключови сектори, а когато е възможно, и във всички сектори, обхванати от предстоящата нова правна рамка, приложима за критичните субекти.

4) Държавите членки се приканват да ускорят подготвителната работа и да приемат мерки за повишаване на устойчивостта, когато е възможно, както е предвидено в предстоящата правна рамка, приложима за критичните субекти, със специален акцент върху сътрудничеството и съответния обмен на информация между държавите членки и с Комисията, върху набелязването на критичните субекти със значително трансгранично значение и върху засилването на подкрепата за установените критични субекти с цел подобряване на тяхната устойчивост.

5) Държавите членки следва да подкрепят обучението и ученията на експертите и споделянето между тях на най-добри практики и извлечени поуки. Държавите членки следва да насърчават експертите да участват в съществуващите платформи за обучение, както национални, така и международни, например в рамките на МГЗС.

6) Държавите членки следва да насърчават и да подкрепят операторите на критична инфраструктура, поне в енергийния сектор, да провеждат стрес тестове, като следват съвместно договорените принципи на равнището на Съюза, когато това е от полза. Стрес тестовете следва да оценяват устойчивостта на критичната инфраструктура срещу антропогенни враждебни заплахи. Поради това държавите членки следва да се стремят да набелязват съответната критична инфраструктура, която да бъде тествана, и да се консултират със съответните оператори на критична инфраструктура възможно най-скоро и не по-късно от края на първото тримесечие на 2023 г. Освен това държавите членки следва да подкрепят операторите на критична инфраструктура, така че те да предприемат тези тестове възможно най-скоро и да се стремят да ги приключат до края на 2023 г., в съответствие с националното право. Съветът възнамерява да направи оценка на положението със стрес тестовете до края на април 2023 г.

7) Поради бързо променящите се заплахи за критичната инфраструктура поддържането на високото ѝ ниво на защита е от жизненоважно значение. Държавите членки се насърчават да заделят достатъчно финансови ресурси, за да укрепят капацитета на своите съответни национални органи, и да ги подкрепят, за да могат да повишат устойчивостта на критичната инфраструктура. Държавите членки се насърчават също така да заделят достатъчно финансови ресурси за органите, отговарящи за управлението на мащабни инциденти в областта на киберсигурността, за да ги подкрепят и да гарантират, че техните екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) и компетентни органи са изцяло мобилизирани в мрежата на ЕРИКС и в мрежата CyCLONe съответно.

8) Държавите членки се приканват, в съответствие с приложимите изисквания, да използват потенциалните възможности за финансиране на равнището на Съюза и на национално равнище, за да повишат устойчивостта на критичната инфраструктура в Съюза за себе си, както и да насърчават операторите на критична инфраструктура да се възползват от тези възможности за финансиране, включително например за трансевропейските мрежи, срещу пълния набор от значителни заплахи, по-специално в рамките на програмите, финансирани от фонд „Вътрешна сигурност“, създаден с Регламент (ЕС) 2021/1149 на Европейския парламент и на Съвета[6], от Европейския фонд за регионално развитие, създаден с Регламент (ЕС) № 1301/2013 на Европейския парламент и на Съвета[7], както и по линия на МГЗС и плана REPowerEU на Комисията. Държавите членки се насърчават също така да използват по най-добрия начин резултатите от съответните проекти в рамките на научноизследователски програми, като например „Хоризонт Европа“, създадена с Регламент (ЕС) 2021/695 на Европейския парламент и на Съвета[8].

---

6 Регламент (ЕС) 2021/1149 на Европейския парламент и на Съвета от 7 юли 2021 г. за създаване на фонд „Вътрешна сигурност“ (ОВ L 251, 15.7.2021 г., стр. 94).

7 Регламент (ЕС) № 1301/2013 на Европейския парламент и на Съвета от 17 декември 2013 г. относно Европейския фонд за регионално развитие и специални разпоредби по отношение на целта „Инвестиции за растеж и работни места“ и за отмяна на Регламент (ЕО) № 1080/2006 (ОВ L 347, 20.12.2013 г., стр. 289).

8 Регламент (ЕС) 2021/695 на Европейския парламент и на Съвета от 28 април 2021 г. за създаване на Рамковата програма за научни изследвания и иновации „Хоризонт Европа“, за определяне на нейните правила за участие и разпространение на резултатите и за отмяна на регламенти (ЕС) № 1290/2013 и (ЕС) № 1291/2013 (ОВ L 170, 12.5.2021 г., стр. 1).

9) Що се отнася до комуникационната и мрежовата инфраструктура в Съюза, Групата за сътрудничество за МИС се приканва, като действа в съответствие с член 11 от Директива (ЕС) 2016/1148, да ускори текущата си работа въз основа на съвместния призив на министрите на държавите членки от Невер по целева оценка на риска и следва да представи първите препоръки във възможно най-кратък срок. Тази оценка на риска следва да предостави информация за текущата междусекторна оценка на риска в кибернетичното пространство и сценариите, поискани в заключенията на Съвета относно позицията на ЕС в киберпространството. Освен това тази работа следва да се извършва, като се осигури съгласуваност и взаимно допълване с работата, извършвана от Групата за сътрудничество за МИС в областта на сигурността на веригата за доставки в сферата на информационните и комуникационните технологии, както и от други съответни групи.

10) Групата за сътрудничество за МИС се приканва също така, с подкрепата на Комисията и ENISA, да продължи работата си по сигурността на цифровата инфраструктура, включително по отношение на подводната инфраструктура, а именно подводните комуникационни кабели. Групата се приканва също така да започне работа по космическия сектор, включително чрез изготвяне, когато е необходимо, на политически насоки и методики за управление на риска по отношение на киберсигурността, основани на обхващащ всички опасности подход и на основан на риска подход за операторите в космическия сектор с цел повишаване на устойчивостта на наземната инфраструктура, подпомагаща 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, например 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 секторите на енергетиката, цифровата инфраструктура и транспорта.

12) Държавите членки следва да използват пълноценно Европейския център за експертни познания в областта на киберсигурността (ECCC). Държавите членки следва да насърчават своите национални координационни центрове да работят проактивно с членовете на общността в областта на киберсигурността, за да изградят капацитет на равнището на Съюза и на национално равнище с цел по-добра подкрепа на операторите на основни услуги.

13) Важно е държавите членки да постигнат прилагането на мерките, препоръчани в инструментариума на ЕС за киберсигурност на 5G технологиите, и по-специално да въведат ограничения за високорисковите доставчици, като се има предвид, че загубата на време може да увеличи уязвимостта на мрежите в Съюза, както и да засилят физическата и нефизическата защита на критичните и чувствителните части от 5G мрежите, включително чрез строг контрол на достъпа. Освен това държавите членки, в сътрудничество с Комисията, следва да оценят необходимостта от допълнителни действия, за да се гарантира постоянно равнище на сигурност и устойчивост на 5G мрежите.

14) Държавите членки, заедно с Комисията и ENISA, следва да се съсредоточат върху изпълнението на заключенията на Съвета от 17 октомври 2022 г. относно сигурността на веригата за доставки на ИКТ.

15) Държавите членки следва да вземат предвид предстоящия мрежови кодекс за свързаните с киберсигурността аспекти на трансграничните потоци на електроенергия[...], като се основават на опита, натрупан при прилагането на Директива (ЕС) 2016/1148, 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.

16) Държавите членки следва да разработят начини да използват „Коперник“, „Галилео“ и Европейската геостационарна служба за навигационно покритие (EGNOS) за наблюдение, за да споделят съответната информация с 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 предвижданото и реакцията при кризи.

Действия на равнището на Съюза

17) Диалогът и сътрудничеството между определените от държавите членки експерти и с Комисията следва да бъдат засилени с оглед на повишаването на физическата устойчивост на критичната инфраструктура, по-специално като:

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

б) се подкрепят държавите членки при изпълнението на новата правна рамка, приложима за критичните субекти, включително чрез насърчаване на Комисията да приеме делегирания акт своевременно;

в) се подпомага провеждането на стрес тестовете, посочени в точка 6, въз основа на общи принципи, като се започне с такива тестове, съсредоточени върху антропогенните враждебни заплахи в енергийния сектор, а впоследствие и в други ключови сектори, както и като се подпомага и се дават консултации относно провеждането на такива стрес тестове при искане от някоя държава членка;

г) като се използва всяка сигурна платформа, след като бъде установена от Комисията, за събиране, преглед и споделяне на доброволна основа на най-добри практики, поуки от националния опит и друга информация, свързана с тази устойчивост.

В работата си тези определени експерти следва да обърнат специално внимание на междусекторните зависимости и на критичната инфраструктура със значително трансгранично значение, като тяхната работа следва да бъде продължена в Съвета и в Комисията, когато е уместно.

18) Държавите членки се приканват да използват всяка подкрепа, предлагана от Комисията, например посредством изготвянето на наръчници и насоки, като 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, с подкрепата на дирекция „Разузнаване“ на ВСЕС съгласно рамката на SIAC, се приканва да провежда брифинги относно заплахите за критичната инфраструктура в Съюза с цел подобряване на ситуационната осведоменост.

19) Държавите членки следва да подкрепят действия, предприети от Комисията, за внедряването на резултатите от проекти относно устойчивостта на критичната инфраструктура, финансирани по програмите на Съюза за научни изследвания и иновации. Съветът взема под внимание намерението на Комисията да увеличи финансирането за тази устойчивост в рамките на бюджета, отпуснат за „Хоризонт Европа“ съгласно многогодишната финансова рамка за периода 2021—2027 г., без това да е в ущърб на финансирането по линия на същата програма за други проекти за научни изследвания и иновации, свързани с гражданската сигурност.

20) Поради задачите, предвидени в заключенията на Съвета относно позицията на ЕС в киберпространството, Комисията, върховният представител и Групата за сътрудничество за МИС се приканват да засилят работата със съответните мрежи и граждански и военни органи и агенции, съобразно съответните си задачи и отговорности съгласно правото на Съюза, при извършването на оценка на риска и разработването на сценарии за риска в областта на киберсигурността, като вземат под внимание по-специално значението на енергетиката, цифровата инфраструктура, транспорта и космическата инфраструктура, както и взаимозависимостите между секторите и държавите членки. При това следва да се вземат предвид свързаните рискове за инфраструктурата, на която разчитат тези сектори. Когато това е от полза, оценките на риска и сценариите може 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 служат като основа за дискусиите относно начините за укрепване на цялостната устойчивост на субектите, експлоатиращи критична инфраструктура, и за справяне с уязвимостите.

21) Комисията се приканва, съгласно съответните си задачи в рамките на управлението на киберкризи, да ускори дейностите си за подкрепа на готовността и реакцията на държавите членки при мащабни киберинциденти, и по-специално:

а) с цел допълване на съответните оценки на риска в контекста на мрежовата и информационната сигурност да извърши всеобхватно проучване[9], което да направи преглед на подводната инфраструктура, а именно подводните комуникационни кабели, които свързват държавите членки, както и Европа в глобален план, като констатациите от това проучване следва да бъдат споделени с държавите членки;

б) да подкрепя готовността и реакцията на държавите членки и на институциите, органите и агенциите на Съюза на мащабни киберинциденти или на сериозни инциденти в съответствие с подсилената правна рамка за киберсигурността и други свързани с въпроса приложими правила[10];

в) да ускори основната концепция за фонда за извънредни ситуации в сферата на кибернетичното пространство с подходящо обсъждане с държавите членки.

22) Комисията се насърчава: да засили работата по прогнозни изпреварващи действия, включително сътрудничеството с държавите членки съгласно членове 6 и 10 от Решение № 1313/2013/ЕС, под формата на планиране на действия при извънредни ситуации в подкрепа на оперативната готовност и реакцията на Координационния център за реагиране при извънредни ситуации (ERCC) в случай на смущения в критичната инфраструктура; да увеличи инвестициите в превантивни подходи и готовност на населението; и да увеличи подкрепата, свързана с изграждането на капацитет в рамките на Мрежата на Съюза за знания в областта на гражданската защита.

---

9 Това проучване следва да включва набелязване на нейния капацитет и ограничения, уязвимости, заплахи и рискове за наличието на услуги, въздействието на прекъсването на (трансатлантическите) подводни кабели за държавите членки и Съюза като цяло и намаляването на риска, като същевременно отчита чувствителността на тази информация и необходимостта тя да бъде защитена.

10 Специално внимание следва да се обърне и на всички дейности, подготвящи ефективна координирана реакция на равнището на Съюза в случай на трансграничен сериозен киберинцидент или свързана с него заплаха, които биха могли да имат системно въздействие върху финансовия сектор на Съюза, както е предвидено в новата правна рамка относно оперативната устойчивост на цифровите технологии.

23) Комисията следва да насърчава използването на средствата на Съюза за наблюдение („Коперник“, „Галилео“ и EGNOS) в подкрепа на държавите членки при мониторинга на критична инфраструктура и на непосредствените околности, когато е целесъобразно, както и в подкрепа на други варианти за наблюдение, предвидени в космическата програма на Съюза, като например рамките за осведоменост за ситуацията в космоса и капацитета на ЕС за космическо наблюдение и за проследяване.

24) 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 критичната инфраструктура, по-специално както следва:

а) Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) относно събирането на информация, анализа на престъпността и подкрепата за разследвания при трансгранични действия по правоприлагане и когато е уместно и целесъобразно, споделяне на резултатите с държавите членки;

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

в) Агенцията на Европейския съюз за космическата програма (EUSPA) и Сателитния център на ЕС (SATCEN) могат да съдействат чрез операции в рамките на космическата програма на Съюза;

г) по отношение на дейностите, свързани с киберсигурността, ЕССС, също и в сътрудничество с ENISA, би могла да подкрепя иновациите и промишлената политика в областта на киберсигурността.

ГЛАВА III: ПО-ДОБРА РЕАКЦИЯ

Действия на равнището на държавите членки

25) Държавите членки се приканват:

а) да продължат да координират реакцията си, когато е уместно, и да поддържат прегледа на междусекторната реакция при остри прекъсвания на основни услуги, предоставяни от критична инфраструктура. Това би могло да се направи в рамките на: бъдещ подробен план за координиран отговор на смущения в критичната инфраструктура със значително трансгранично значение; на съществуващите интегрирани договорености на ЕС за реакция на политическо равнище при кризи (IPCR) за координирането на политическия отговор, що се отнася за критична инфраструктура с трансгранично значение; на подробния план за мащабни инциденти и кризи в областта на киберсигурността съгласно Препоръка (ЕС) 2017/1584 на Комисията[11]; на EU-CyCLONe; на рамката за координиран отговор на ЕС на хибридни кампании и инструментариума на ЕС срещу хибридни заплахи в случай на хибридни заплахи и кампании; и на системата за бързо предупреждение в случай на дезинформация;

б) да засилят обмена на информация на оперативно равнище с ERCC в рамките на МГЗС с цел подобряване на ранното предупреждение и да координират своята реакция в рамките на МГЗС в случай на смущения на критичната инфраструктура със значително трансгранично значение, като по този начин се гарантира по-бърза реакция с посредничеството на Съюза, когато е необходимо;

в) да увеличат готовността си да реагират, когато е уместно, чрез съществуващи или подлежащи на разработване инструменти при такива значителни смущения, посочени в буква а);

---

[11] 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).

г) да се ангажират с по-нататъшното развитие на подходящ капацитет за реагиране в рамките на Европейския резерв за гражданска защита (ECPP) и rescEU;

д) да насърчават операторите на критична инфраструктура и съответните национални органи да увеличат капацитета си, за да могат бързо да възстановят базисните показатели на основните услуги, предоставяни от тези оператори на критична инфраструктура;

е) да насърчават операторите на критична инфраструктура, когато възстановяват своята критичната инфраструктура, да я изграждат така, че да бъде възможно най-устойчива, като вземат предвид пропорционалността на мерките с оглед на оценките на риска и разходите, до пълния набор от значителни рискове, които могат да се отнасят за нея, включително при неблагоприятни климатични сценарии.

26) Държавите членки се приканват, когато е възможно, да ускорят подготвителната работа, както е предвидено в засилената правна рамка относно киберсигурността, като се стремят да укрепят способностите на националните ЕРИКС с оглед на новите задачи на ЕРИКС, както и на увеличения брой субекти от нови сектори, като преразглеждат и актуализират своевременно своите стратегии за киберсигурност и приемат възможно най-скоро национални планове за реакция при киберинциденти и киберкризи.

27) Държавите членки се приканват да обмислят на национално равнище най-подходящите средства, за да се гарантира, че съответните заинтересовани страни са наясно с необходимостта от повишаване на устойчивостта на критичната инфраструктура чрез сътрудничество с надеждни доставчици и партньори. Важно е да се инвестира в допълнителен капацитет, особено в секторите, в които настоящата инфраструктура е в края на жизнения си цикъл, например подводна комуникационна кабелна инфраструктура, за да може да се осигури непрекъснатост на предоставянето на основни услуги в случай на смущения и да се намалят нежеланите зависимости.

28) Държавите членки се насърчават да обръщат внимание на проактивната стратегическа комуникация на национално равнище в контекста на борбата с хибридните заплахи и кампании, като се има предвид потенциалът, който противниците може да се стремят да ангажират при чуждестранно манипулиране на информацията и вмешателство, като оформят посланията около инциденти, насочени към критичната инфраструктура.

Действия на равнището на Съюза

29) Комисията се приканва да работи в тясно сътрудничество с държавите членки за по-нататъшно развитие на съответните органи, инструменти и капацитет за реагиране с цел повишаване на оперативната готовност за справяне с непосредствените и непреките последици от значителни смущения на съответните основни услуги, предоставяни чрез критична инфраструктура, по-специално експерти и ресурси, налични чрез ECPP и rescEU в рамките на МГЗС, или бъдещи екипи за бързо реагиране при хибридни заплахи.

30) Като взема предвид променящата се картина на заплахите и в сътрудничество с държавите членки, в контекста на МГЗС Комисията се приканва:

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

б) редовно да наблюдава и да набелязва потенциално значителни пропуски в капацитета за реагиране в рамките на ECPP и rescEU;

в) допълнително да засили междусекторното сътрудничество, за да се гарантира адекватна реакция на равнището на Съюза, и да организира редовни обучения или учения за тестване на това сътрудничество заедно с една или повече държави членки;

г) да доразвие ERCC като междусекторен кризисен център на равнището на Съюза за координиране на подкрепата за засегнатите държави членки.

31) Съветът се ангажира да започне работа с оглед на одобряването на подробен план за координирана реакция при смущения в критичната инфраструктура със значително трансгранично значение, в който да се описват и определят целите и начините на сътрудничество между държавите членки и институциите, органите, службите и агенциите на Съюза при реагирането на инциденти, свързани с такава критична инфраструктура. Съветът очаква проекта на Комисията за такъв подробен план, който се основава на подкрепата и приноса на съответните агенции на Съюза. Подробният план трябва да е напълно съгласуван и оперативно съвместим с преразгледания оперативен протокол на Съюза за борба с хибридните заплахи (EU Playbook) и да взема предвид съществуващия подробен план за координирана реакция при мащабни трансгранични инциденти и кризи в областта на киберсигурността[12] и мандата на EU-CyCLONe, предвиден в Директивата за МИС2, и да избягва дублирането на структури и дейности. В подробния план следва напълно да се зачитат съществуващите договорености за IPCR за координиране на реакцията.

[12] Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи.

32) Комисията се приканва да се консултира със съответните заинтересовани страни и експерти относно подходящи мерки във връзка с евентуални значителни инциденти по отношение на подводната инфраструктура, които ще бъдат представени заедно с всеобхватното проучване, посочено в точка 20, буква а), както и да доразработи плановете за действие при извънредни случаи, сценариите за риска и целите за устойчивостта на Съюза при бедствия, определени в Решение № 1313/2013/ЕС.

ГЛАВА IV: МЕЖДУНАРОДНО СЪТРУДНИЧЕСТВО

Действия на равнището на държавите членки

33) Държавите членки следва да си сътрудничат, когато е целесъобразно и в съответствие с правото на Съюза, със съответни трети държави по отношение на устойчивостта критичната инфраструктура със значително трансгранично значение.

34) Държавите членки се насърчават да си сътрудничат с Комисията и върховния представител с цел ефективно да се справят с рисковете за критичната инфраструктура в международни води.

35) Държавите членки се приканват да допринесат, в сътрудничество с Комисията и с 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 от 21 юни 2022 г. относно рамка за координиран отговор на ЕС на хибридни кампании, 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 планират и подготвят всеобхватни и координирани ответни действия на Съюза на хибридни кампании и хибридни заплахи, включително такива срещу оператори на критична инфраструктура.

Действия на равнището на Съюза

36) Комисията и върховният представител се приканват да подкрепят, когато е целесъобразно и съгласно съответните си задачи и отговорности според правото на Съюза, съответни трети държави за повишаване на устойчивостта на критичната инфраструктура на тяхна територия, и по-специално на критичната инфраструктура, която е физически свързана с тяхната територия и с тази на държава членка.

37) Комисията и върховният представител, съгласно съответните си задачи и отговорности според правото на Съюза, ще засилят координацията с НАТО относно устойчивостта на критичната инфраструктура от общ интерес чрез структурирания диалог между ЕС и НАТО относно устойчивостта, при пълно зачитане на правомощията на Съюза и на държавите членки съгласно Договорите и ключовите принципи, ръководещи сътрудничеството между ЕС и НАТО, договорени от Европейския съвет, по-специално реципрочност, приобщаване и автономност при вземането на решения. В този контекст това сътрудничество ще бъде доразвито в рамките на структурирания диалог между ЕС и НАТО относно устойчивостта, залегнал в съществуващия механизъм между служителите на двете страни за изпълнението на съвместните декларации, като същевременно се гарантира пълна прозрачност и участие на всички държави членки.

38) Комисията се приканва, когато е необходимо и целесъобразно, да обмисли участието на представители на съответни трети държави в рамките на сътрудничеството и обмена на информация между държавите членки в областта на устойчивостта на критичната инфраструктура, която е физически свързана с територията на държава членка и с тази на трета държава.

Съставено в …

За Съвета

Председател