II

(Незаконодателни актове)

ПРЕПОРЪКИ

ПРЕПОРЪКА (ЕС) 2021/1086 НА КОМИСИЯТА

от 23 юни 2021 година

за изграждането на съвместно киберзвено

ЕВРОПЕЙСКАТА КОМИСИЯ,

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

като има предвид, че:

(1) Киберсигурността е от съществено значение за успеха на цифровата трансформация на икономиката и обществото. ЕС е ангажиран да инвестира на безпрецедентно равнище, за да гарантира, че гражданите, предприятията и публичните органи имат доверие на цифровите инструменти.

(2) С пандемията от COVID-19 нарасна значението на свързаността, както и зависимостта на Европа от стабилни мрежи и информационни системи и стана ясна необходимостта от защита на цялата верига на доставки. Надеждните и сигурни мрежи и информационни системи са особено важни за субектите на първа линия в борбата с пандемията, например болници, медицински агенции и производители на ваксини. Координирането на усилията на ЕС за предотвратяване, откриване, възпиране, смекчаване и реагиране на най-тежките кибератаки срещу такива субекти би могло да предотврати загубата на човешки живот и опитите за подкопаване на способността на ЕС да се справи с пандемията по възможно най-бързия начин. Освен това укрепването на способността на ЕС да противостои на кибератаките допринася за напредъка на глобалното, отворено, стабилно и сигурно киберпространство.

(3) Изправени пред трансграничния характер на заплахите за киберсигурността и непрекъснатото увеличаване на по-сложните, повсеместни и целенасочени атаки ([1]), съответните институции и участници в областта на киберсигурността следва да увеличат способността си да реагират на такива заплахи и атаки, като използват съществуващите ресурси и координират по-добре усилията си. Всички съответни участници в ЕС трябва да бъдат подготвени да реагират колективно и да обменят информация на принципа „необходимост от споделяне“, а не „необходимост да се знае“.

(4) Въпреки значителния напредък, постигнат чрез сътрудничеството между държавите членки в областта на киберсигурността, особено чрез групата за сътрудничество („групата за сътрудничество за МИС“) и мрежата от екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС), създадена съгласно Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета ([2]), все още не съществува обща платформа на ЕС, където ефективно и безопасно да се обменя информацията, събрана в различни общности за киберсигурност, и където оперативните способности могат да бъдат координирани и мобилизирани от съответните участници. В резултат на това е налице опасност киберзаплахите и киберинцидентите да бъдат разглеждани изолирано, което води до ограничена ефективност и повишена уязвимост. Също така липсва канал на равнище ЕС за техническо и оперативно сътрудничество с частния сектор както по отношение на споделянето на информация, така и по отношение на подкрепата за реагиране на инциденти.

([1]) Доклад на ENISA относно картината на заплахите през 2020 г.; Европол, Оценка на заплахата от организирана престъпност, ползваща се от интернет (IOCTA), 2020 г.

([2]) 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).

(5) Съществуващите рамки и структури и наличните ресурси и експертен опит в държавите членки и съответните институции, органи и агенции на ЕС предлагат солидна основа за колективен отговор на заплахи, инциденти и кризи в областта на киберсигурността ([3]). Съществуваща структура включва, от оперативна гледна точка, концепция за координирана реакция при широкомащабни инциденти и кризи, свързани с киберсигурността („концепцията“) ([4]), мрежата на ЕРИКС и мрежата на Европейската организация за връзка при киберинциденти („EU CyCLONe“) ([5]), както и Европейския център за борба с киберпрестъпността („EC3“) и съвместната експертна група на по киберпрестъпността към Агенцията на Европейския съюз за сътрудничество и обучение в областта на правоприлагането („Европол“) и Протокола за реагиране при извънредни ситуации на правоприлагащите органи в ЕС („EU LE ERP“). Групата за сътрудничество за МИС, Центърът на ЕС за анализ на информация (INTCEN) и инструментариумът за кибердипломация ([6]) и свързаните с киберотбраната проекти, стартирани в рамките на постоянното структурирано сътрудничество (ПСС) ([7]), също допринасят за политическото и оперативното сътрудничество между различните общности за киберсигурност. В духа на засиления си мандат Европейската агенция за киберсигурност (ENISA) е натоварена да подпомага оперативното сътрудничество ([8]) по отношение на киберсигурността на мрежите и информационните системи, ползвателите на тези системи и други лица, засегнати от киберзаплахи и киберинциденти. Чрез интегрираните договорености на ЕС за реакция на политическо равнище при кризи (ИРПК), ЕС е в състояние да координира политическия си отговор на значителни кризи, включително в случай на широкомащабни кибератаки.

(6) Все още не съществува обаче механизъм за използване на наличните ресурси и осигуряване на взаимопомощ между киберобщностите, отговорни за сигурността на мрежите и информационните системи, за борбата с киберпрестъпността, за провеждането на кибердипломация и, където е уместно, за киберотбрана в случай на криза. Не съществува и всеобхватен механизъм на равнище ЕС за техническо и оперативно сътрудничество във връзка със ситуационната осведоменост, подготовката и реакцията между всички общности за киберсигурност. Също така следва да се постигнат полезни взаимодействия между правоприлагащите и разузнавателните общности чрез Европол и INTCEN.

(7) Комисията, Върховният представител на Съюза по въпросите на външните работи и политиката на сигурност (върховният представител), държавите членки и съответните институции, органи и агенции на ЕС признават значението на анализа на силните и слабите страни, пропуските и припокриванията на настоящата архитектура на киберсигурността, която беше изградена през последните години. В консултация с държавите членки и с участието на върховния представител Комисията разработи концепция за съвместно киберзвено в отговор на този анализ и като важен елемент от стратегията на ЕС за Съюза на сигурност ([9]), цифровата стратегия ([10]) и стратегията за киберсигурност ([11]).

([3]) Европейската организация за връзка при киберинциденти („EU CyCLONe“) беше създадена от държавите членки в отговор на препоръката, с която беше представена концепцията. Това е мрежа от национални експерти по оперативното управление и управлението на кризи, която Комисията предложи да бъде кодифицирана чрез Директивата относно мерките за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148, COM(2020) 823 final, 2020/0359 (COD) предложена през декември 2020 г.

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

([5]) Настоящата препоръка взема предвид последващия доклад от оперативното учение по концепцията (Blue OLEx) от 2020 г., и по-специално обобщението на председателя на стратегическата дискусия по политиката относно съвместното киберзвено.

([6]) Заключения на Съвета относно рамка за съвместен дипломатически отговор на ЕС срещу зловредни кибердейности („Инструментариум за кибердипломация“) от 19 юни 2017 г. (9916/17).

([7]) По-специално проектите по линия на ПСС относно „екипите за бързо реагиране при кибератаки и за взаимопомощ в областта на киберсигурността“, координирани от Литва, и относно „координационния център в областта на киберсигурността и информацията“, координирани от Германия.

([8]) С член 7 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019 г., стр. 15) се изисква Агенцията да подкрепя оперативното сътрудничество между държавите членки, институциите, органите, службите и агенциите на Съюза и между заинтересованите страни. Това включва подкрепа за държавите членки за оперативното сътрудничество в рамките на мрежата на ЕРИКС, изготвяне на редовен задълбочен доклад за техническото състояние на киберсигурността в ЕС относно инцидентите и киберзаплахите и допринасяне за разработването на съвместна реакция на равнището на Съюза и на равнището на държавите членки при мащабни трансгранични инциденти или кризи. Освен това ENISA допринася за дейностите по обучение на Европейския колеж по сигурност и отбрана (ЕКСО).

([9]) Съобщение на Комисията до Европейския парламент, Европейския съвет, Европейския икономически и социален комитет и Комитета на регионите: относно Стратегията на ЕС за Съюза на сигурност, COM(2020)605 final

([10]) Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите: Изграждане на цифровото бъдеще на Европа, COM(2020) 67 final.

([11]) Съвместно съобщение до Европейския парламент и Съвета: Стратегия на ЕС за киберсигурност за цифровото десетилетие, JOIN/2020/18 final

(8) При криза държавите членки следва да могат да разчитат на солидарността на ЕС под формата на координирана помощ, включително от четирите киберобщности, а именно гражданската, правоприлагащата ([12]), дипломатическата, и, където е уместно, отбранителната. Степента на намеса на участниците от една или повече общности може да зависи от естеството на мащабен инцидент или криза и следователно от вида на мерките за противодействие, необходими в отговор на инцидента. Когато се сблъскваме с киберзаплахи, инциденти и кризи, добре обучените експерти и техническото оборудване са от съществено значение и могат да допринесат за избягване на сериозни щети и за ефективно възстановяване. Следователно ясно определените технически и оперативни способности, на първо място експерти и оборудване, готови да бъдат ангажирани от държавите членки при необходимост, са в основата на съвместното киберзвено. В тази платформа участниците ще имат уникалната възможност да изграждат и координират тези способности чрез екипите на ЕС за бързо реагиране в областта на киберсигурността, като същевременно осигуряват съответните полезни взаимодействия с вече съществуващите киберпроекти, осъществявани в рамките на ПСС.

(9) Съвместното киберзвено осигурява виртуална и физическа платформа и не изисква създаването на допълнителен самостоятелен орган. Създаването му не би следвало да засегне компетенциите и правомощията на националните органи за киберсигурност и съответните субекти на Съюза. Съвместното киберзвено следва да бъде основано на меморандуми за разбирателство между участниците в него. То следва да доразвива и добавя стойност към съществуващите структури, ресурси и способности като платформа за сигурно и бързо оперативно и техническо сътрудничество между органите на ЕС и органите на държавите членки. То следва също така да обедини всички общности за киберсигурност — гражданската, правоприлагащата, дипломатическата и отбранителната. Участниците в платформата следва да имат оперативна или поддържаща роля. Оперативните участници следва да включват ENISA, Европол, екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС („CERT-EU“), Комисията, Европейската служба за външна дейност (включително INTCEN), мрежата на ЕРИКС и EU-CyCLONe. Участниците с поддържаща роля следва да включват Европейската агенция по отбрана (EDA), председателя на групата за сътрудничество за МИС, председателя на Хоризонталната работна група по въпроси на кибернетичното пространство към Съвета и по един представител на съответните проекти по линия на ПСС ([13]). Тъй като държавите членки разполагат с оперативен капацитет и компетентност да реагират на широкомащабни киберзаплахи, инциденти и кризи, участниците в платформата следва да разчитат преди всичко на техния капацитет, с помощта на съответните субекти на Съюза, за постигане на своите цели.

(10) Съвместното киберзвено следва да даде нов тласък на процеса, започнат през 2017 г. с концепцията. То следва освен това да приведе в действие изложената в концепцията архитектура и да отбележи решителна стъпка към европейски механизъм за управление на кризи в областта на киберсигурността, в която рисковете се установяват, смекчават и преодоляват координирано и своевременно. С тази стъпка съвместното киберзвено следва да помогне на ЕС да реагира на актуални и бъдещи заплахи.

(11) С участието си в съвместното киберзвено оперативните участници и участниците с поддържаща роля следва да могат да си взаимодействат с по-широк кръг заинтересовани страни като част от Механизма на ЕС за реакция при кризи в областта на киберсигурността. Упражнявайки функциите си в рамките на своите мандати, участниците следва да се възползват от повишена готовност и по-широка ситуационна осведоменост, които обхващат всички аспекти на киберзаплахите и киберинцидентите, и да привлекат допълнителен експертен опит в областта на киберсигурността. Участниците следва например редовно да се включват в учения, включващи различни общности, да поемат ясно определена роля в плана на ЕС за реакция при инциденти и кризи в областта на киберсигурността, да придават повече видимост на своите дейности чрез споделена публична комуникация и да сключват споразумения за оперативно сътрудничество с частния сектор. Наред с това приносът към съвместното киберзвено следва да позволи на участниците да укрепят съществуващите мрежи, например мрежата на ЕРИКС и EU CyCLONe, като им предоставят сигурни инструменти за обмен на информация и по-добри способности за откриване (т.е. центрове за операции по сигурността) и им дават възможност да използват наличните оперативни способности на ЕС.

(12) Участниците в съвместното киберзвено следва да се съсредоточат върху техническото и оперативното сътрудничество, включително съвместни операции. Те следва да допринасят за това сътрудничество в степента, възможна съгласно техните мандати. Сътрудничеството следва да се основава на текущите усилия и да ги допълва. Според вида на съответното сътрудничество могат да се включат и допълнителни участници.

([12]) От значение и за съдебното сътрудничество.

([13]) Вж. бележка под линия 5. ЕСВД и EDA, в ролята си на секретариат на ПСС, ще поддържат връзка с координаторите на съответните проекти по линия на ПСС.

(13) Платформата следва да обединява технически и оперативни експерти по управление на кризи от държавите членки и органите на ЕС с цел координиране на ответните реакции на киберзаплахи, инциденти и кризи, като се използват съществуващите способности и експертен опит. Участващите в съвместното киберзвено експерти ще могат да наблюдават и защитават много по-голяма изложена на атака повърхност като използват както физическата, така и виртуалната платформа. За целта участниците следва да координират усилията си в случай на трансгранични инциденти и кризи, както и предоставянето на помощ на пострадали от инциденти държави чрез платформата.

(14) Изграждането на съвместното киберзвено изисква постепенен процес на мобилизиране и консолидиране на съществуващите рамки и структури, споменати в настоящата препоръка, включително механизмите за сътрудничество, установени в ръководените от държавите членки форуми (напр. мрежата на ЕРИКС, EU CyCLONe, Хоризонталната работна група по въпроси на кибернетичното пространство към Съвета, съвместната експертна група на по киберпрестъпността към Европол и свързаните с темата проекти по линия на ПСС), а от страна на институциите, органите и агенциите на ЕС — структурирано сътрудничество между ENISA и CERT-EU, както и на междуинституционалната група за обмен на информация в областта на киберсигурността. Рамките за хибридни заплахи и за гражданска защита ([14]) и секторните рамки ([15]) следва също да бъдат адекватно ангажирани. Необходимо е също така да се изгради структурирана връзка с ИРПК ([16]). Това ще позволи при криза събраната в Съвета информация да се предава бързо и ефективно на лицата, които вземат решения на политическо равнище.

(15) Поради това съвместното киберзвено следва да бъде изградено чрез постепенен и прозрачен процес, който трябва да бъде завършен през следващите две години. По тази причина целите, залегнали в настоящата препоръка, следва да се постигнат чрез четириетапен процес, както е описано в приложението към нея. В първите два етапа следва да бъде стартиран подготвителен процес, организиран и подкрепян от ENISA, който включва оперативни участници и участници в поддържаща роля на равнището на ЕС и на държавите членки, и който ще протече под ръководството на работна група, създадена от Комисията. Подготвителната работа следва да се опира на принципите на взаимна ангажираност, приобщаване и постигане на консенсус. Следва да се насърчава ангажирането на всички участници, което ще позволи да се изразят различни мнения и позиции и да се положат усилия за намиране на решения, които се ползват от възможно най-широка подкрепа. В зависимост от нуждите и при наличието на добра обосновка, графикът за различните етапи, указани в настоящата препоръка, може да бъде коригиран.

(16) На първия етап подготвителният процес следва да започне с определянето на съответните налични оперативни способности на ЕС и стартирането на оценка на ролите и задълженията на участниците в платформата. Вторият етап следва да включва разработването на план на ЕС за реагиране при инциденти и кризи, съгласуван с концепцията ([17]) и Протокола за реагиране при извънредни ситуации на правоприлагащите органи в ЕС, разгръщането на дейности, свързани с готовността и ситуационната осведоменост, в съответствие с Акта за киберсигурността и Регламента за Европол ([18]), и приключването на оценката на ролите и задълженията на участниците в платформата. Работната група следва да представи резултатите от тази оценка на Комисията и на върховния представител, които след това да ги представят на Съвета. Комисията и върховният представител следва да работят заедно, според съответните си области на компетентност, за изготвянето на съвместен доклад въз основа на тази оценка, и да приканят Съвета да одобри този доклад чрез заключения.

(17) След одобрение съвместното киберзвено ще започне да функционира с оглед на приключването на оставащите два етапа от процеса. На третия етап участниците следва да могат да задействат екипи за бързо реагиране на ЕС от съвместното киберзвено в съответствие с процедурите, определени в плана на ЕС за реагиране при инциденти и кризи, като използват и физическата, и виртуалната платформа и дават приноса си за различни аспекти на реагирането при инциденти (от публична комуникация до последващо възстановяване). И накрая, на четвъртия етап, заинтересованите страни от частния сектор, включително потребителите и доставчиците на решения и услуги в областта на киберсигурността, ще бъдат приканени да дадат своя принос за платформата, което ще позволи на участниците да подобрят обмена на информация и да усъвършенстват координирания отговор на ЕС при киберзаплахи и киберинциденти.

([14]) В този контекст съвместното киберзвено следва да установи полезни взаимодействия с Механизма за гражданска защита на ЕС (МГЗС) с цел подобряване на готовността и реагирането на европейско равнище в случай на множество бедствия и извънредни ситуации, които включват елемент на киберсигурност.

([15]) Например тази за финансовия сектор, предвидена в Регламент (ЕС) 2021/xx на Европейския парламент и на Съвета* [DORA].

([16]) Вж. съображение 5.

([17]) Вж. бележка под линия 3.

([18]) Регламент (ЕС) 2016/794 на Европейския парламент и на Съвета от 11 май 2016 г. относно Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) и за замяна и отмяна на решения 2009/371/ПВР, 2009/934/ПВР, 2009/935/ПВР, 2009/936/ПВР и 2009/968/ПВР на Съвета (ОВ L 135, 24.5.2016 г., стр. 53).

(18) До края на четириетапния процес участниците следва да изготвят доклад за дейността и напредъка в изпълнението на четирите етапа, определени в настоящата препоръка, като опишат постиженията и срещнатите трудности. Този доклад следва да бъде представен на Комисията и на върховния представител. Въз основа на доклада Комисията и върховният представител следва да извършат оценка на тези резултати и да направят заключения за бъдещето на съвместното киберзвено.

(19) Комисията, ENISA, Европол и CERT-EU следва да предоставят административна, финансова и техническа подкрепа на съвместното киберзвено, както е посочено в раздел IV от настоящата препоръка, доколкото позволяват бюджетните средства и наличните човешки ресурси. Укрепването на оперативния капацитет на съответните институции, органи и агенции на ЕС в областта на киберсигурността ще бъде от основно значение за осигуряването на ефективна подготовка и устойчивост на съвместното киберзвено. Комисията възнамерява да гарантира, че предстоящият регламент относно общите задължителни правила за киберсигурност за институциите, органите и агенциите на ЕС (октомври 2021 г.) осигурява правното основание за този принос в случая на CERT-EU.

(20) С оглед на засиления ѝ мандат съгласно Регламент (ЕС) 2019/881 („Акт за киберсигурността“) ENISA е в уникалната позиция да организира и подпомага подготовката на съвместното киберзвено, както и да допринася за неговото привеждане в действие. В съответствие с разпоредбите на Акта за киберсигурността, понастоящем ENISA създава бюро в Брюксел, който да подпомага структурираното ѝ сътрудничество със CERT-EU. Това структурирано сътрудничество, включително разположените в съседство офиси на двете агенции, осигурява полезна рамка за предстоящото съвместно киберзвено, включително създаването на неговото физическо пространство, което следва да бъде предоставено на разположение на участниците в случай на нужда, както и на персонала на други институции, органи и агенции на ЕС, имащи отношение към работата му. Физическата платформа следва да бъде съчетана с виртуална платформа, съставена от инструменти за сътрудничество и сигурно споделяне на информация. Тези инструменти ще използват богатството от информация, събрана чрез европейския киберщит ([19]), включително центровете за операции по сигурността и центровете за споделяне и анализ на информация (ISAC).

(21) Приетият от Съвета през 2018 г. протокол за реагиране на правоприлагащите органи в ЕС при извънредни ситуации във връзка с мащабни трансгранични кибератаки предоставя, в рамките на концептуалната рамка, централна роля на Европейския център за борба с киберпрестъпността (ЕС3) ([20]) на Европол. Този протокол позволява на правоприлагащите органи на ЕС да могат във всеки момент на денонощието да реагират, чрез бърза намеса и оценка, на мащабни трансгранични атаки с предполагаем злонамерен характер, както и защитен и своевременен обмен на възлова информация за ефективно координиране на ответните действия при трансгранични инциденти. С протокола, основан на протоколите за действие при обхванали ЕС кризи, се доразвива сътрудничеството с останалите институции на ЕС, а и с частния сектор — при кризисни ситуации. Правоприлагащите органи с подкрепата на Европол, когато е целесъобразно, следва да подпомагат съвместното киберзвено, като в съответствие с наказателното правораздаване и приложимите процедури за обработване на електронни доказателства предприемат необходимите стъпки по протежение на пълния цикъл на разследване. От създаването на ЕС3 през 2013 г. Европол предоставя оперативна подкрепа и улеснява оперативното сътрудничество в борбата срещу киберзаплахите. Европол следва да подкрепя платформата в рамките на мандата си и подхода за полицейски действия, основани на разузнавателна информация, както и да използва целия си натрупан експертен опит и всички продукти, инструменти и услуги, с които разполага, с оглед на дадения инцидент или кризисни мерки.

(22) С Директива 2013/40/ЕС относно атаките срещу информационните системи от държавите членки се изисква да разполагат с денонощно оперативно национално звено за контакт за обмен на информация по посочените в нея престъпни деяния. Мрежата от оперативни национални звена за контакт следва да подпомага съвместното киберзвено, като когато е целесъобразно приобщава правоприлагащите органи на държавите членки.

(23) Общността на ЕС за кибердипломация съдейства за насърчаването и опазването на едно глобално, отворено, стабилно и защитено киберпространство, както и за предотвратяването, възпирането и реагирането на атакуващи го злонамерени действия. През 2017 г. ЕС създаде рамка за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството („инструментариум за кибердипломация“). Настоящата рамка се вписва в една по-широка политика на ЕС за кибердипломация. Тя допринася за предотвратяването на конфликти и за по-стабилни международни отношения. Тя позволява на ЕС и на държавите членки да използват, когато е целесъобразно – в сътрудничество с международни партньори, всички мерки на общата външна политика и политика на сигурност (ОВППС) и съответните процедури за прилагането им, за да се насърчи сътрудничеството, да се ограничат заплахите и да се противостои на настоящото и потенциалното бъдещо злонамерено поведение в киберпространството. Общността за кибердипломация следва да си сътрудничи в рамките на съвместното киберзвено за получаване и предоставяне на подкрепа в случай на криза посредством пълния набор от дипломатически мерки, по-специално по отношение на комуникацията с обществеността, подпомагането на взаимна осведоменост за обстановката и встъпването в диалог с трети държави.

([19]) JOIN/2020/18 final, раздел 1.2.
([20]) Създаден по силата на Регламент (ЕС) 2016/794.

(24) В съответствие с концептуалната рамка върховният представител следва, в т.ч. чрез INTCEN, да подпомага съвместното киберзвено, като осигурява и споделя непрекъснат поток от разузнавателна информация за съществуващите и възникващите заплахи, в т.ч. за съответните стратегически аспекти на дадено събитие.

(25) С общността за киберотбрана ЕС и държавите членки се стремят да засилят капацитета си за противодействие на кибератаки, както и полезните взаимодействия, координацията и сътрудничеството — между съответните институции, органи и агенции на ЕС, с държавите членки и между самите държави членки, в т.ч. при мисиите и операциите по линия на общата политика за сигурност и отбрана (ОПСО). В основата на функционирането на общността стоят междуправителствено управление на равнище ЕС, националните структури за военно командване и капацитетът и ресурсите, предназначени за военна или двойна употреба. Предвид своеобразното естество на общността за киберотбрана обменът на информация между съвместното киберзвено и нея следва да се осъществява чрез специални опосредстващи механизми ([21]).

(26) Постоянното структурирано сътрудничество (ПСС) е нормативна уредба, въведена с Договора от Лисабон ([22]) и интегрирана през 2017 г. в уредбата на Съюза. Структурираното сътрудничество доведе до създаването по линия на ПСС на редица проекти за киберпространството, с което спомогна за изпълнението на ангажимент 11 ([23]) за „увеличаване на усилията за сътрудничество в киберотбраната, в сфери като обмена на информация, обучението и оперативното съдействие“. ЕСВД, в т.ч. Военният секретариат на ЕС и ЕАО, съставляват секретариата на ПСС, който осигурява единно звено за контакт в Съюза по всички въпроси на ПСС, в т.ч. подпомагане и координиране на функции във връзка с проектите по линия на ПСС (например оценяване на нови предложения за проекти, изготвяне на доклади за напредъка по проектите и др.). Представителите на съответните проекти по линия на ПСС следва да подпомагат съвместното киберзвено главно по отношение на осведомеността за дадена обстановка и готовността за реагиране.

(27) Чрез съвместното киберзвено участниците следва да приобщят по подходящ начин заинтересованите страни от частния сектор — както доставчици, така и ползватели на решения и услуги за киберсигурност, за да подпомагат европейската рамка за управление на киберкризи при надлежно спазване на нормативните изисквания за обмен на данни и защитеност на информацията. Доставчиците на услуги за киберсигурност следва да подпомагат инициативата, като обменят разузнавателни данни за заплахи и позволяват на екипите за реагиране при инциденти бързо да увеличават капацитета на звеното при мащабни атаки и кризи. Ползвателите на продукти и услуги за киберсигурност и най-вече обхванатите от Директивата за МИС следва да могат да търсят помощ и съвети чрез структурирани канали, свързани с центровете за споделяне и анализ на информация (ISAC) на равнище ЕС — каквито понастоящем липсват ([24]). Платформата би могла да допринесе и за засилване на сътрудничеството с международните партньори.

(28) За поддържането и усъвършенстването на осведомеността за обстановката са нужни върхови технически възможности за откриване и предотвратяване на проникване. Съвместното киберзвено следва да разчита на високо технологична мрежа, която е в състояние да анализира злонамерените заплахи и инцидентите с потенциално въздействие върху възловите комуникационни и информационни системи в Съюза. Това означава, че знанията за заплахите, извлечени от комуникационните мрежи, наблюдавани от национални, секторни и трансгранични ЦОС, следва да се използват, наред с другите източници на информация, в съвместното киберзвено, така че участниците да имат добра представа за заплахите в ЕС.

(29) Платформата следва да разполага с подходящо защитени комуникационни канали с оглед на обмена на оперативна информация, евентуално съдържаща поверителни материали. Тези канали биха могли да използват съществуващата инфраструктура, като например приложението за мрежа за сигурен обмен на информация (СИЕНА), използвано от Европол и правоприлагащите органи. Както бе обявено в стратегията за киберсигурност, използваният от институциите, органите и агенциите на ЕС инструментариум следва да се подчинява на нормите относно информационната сигурност, които Комисията скоро ще предложи.

([21]) По-специално чрез представителство в ЕСВД, с което ще се осигури съответстващо участие на общността за киберотбрана въз основа на доброволно национално участие.

([22]) Членове 42.6 и 46, и протокол № 10.

([23]) Всяка държава членка, участваща в ПСС, поема 20 индивидуални ангажимента, отнесени към петте ключови области, определени в член 2 от Протокол № 10 относно ПСС, приложен към Договора за Европейския съюз.

([24]) Няколко значими ISAC, които биха могли да участват в такъв обмен, са ISAC на европейската енергетика (EE-ISAC) или ISAC на европейските финансови институти (FI-ISAC).

(30) Комисията, главно чрез програмата „Цифрова Европа“, ще предвиди необходимите инвестиции за изграждането на физическата и виртуалната платформа, за изграждането и поддържането на защитени комуникационни канали и на капацитет за обучение, както и за усъвършенстването и разгръщането на капацитет за откриване на заплахи. От своя страна Европейският фонд за отбрана също би могъл да подпомогне финансирането на основни технологии и капацитет за киберотбрана, които биха засилили националната готовност за киберотбрана,

ПРИЕ НАСТОЯЩАТА ПРЕПОРЪКА:

I. **ЦЕЛ НА НАСТОЯЩАТА ПРЕПОРЪКА**

(1) С настоящата препоръка се набелязват действията за координиране, чрез съвместно киберзвено, на усилията на ЕС за предотвратяване, откриване, възпиране, възпрепятстване, реагиране и ограничаване на въздействието на мащабни киберинциденти и кризи. Във връзка с това в нея за държавите членки и съответните институции, органи и агенции на ЕС се определя и план-графикът за създаване и разгръщане на тази платформа.

(2) При мащабни киберинциденти и кризи държавите членки и съответните институции, органи и агенции на ЕС следва да координират усилията си чрез съвместно киберзвено, с помощта на което да впрегнат знанията и опита си за взаимно оказване на помощ ([25]). Съвместното киберзвено ще бъде и мястото на сътрудничество между участниците и частния сектор.

II. **ОПРЕДЕЛЕНИЯ**

(3) За целите на настоящата препоръка:

а) „План на ЕС за реагиране при киберинциденти и кризи“ означава съвкупността от роли, условия и процедури, с които се дооформя рамката на ЕС за реагиране при киберкризи, описана в точка 1 от препоръката на Комисията от 13 септември 2017 г. за координирана реакция при мащабни киберинциденти и кризи („концептуална рамка“).

б) „общности за киберсигурност“ означава съвместни граждански, правоприлагащи, дипломатически и отбранителни групи, представляващи както държавите членки, така и съответните институции, органи и агенции на ЕС, които обменят информация в преследване на общи цели, интереси и мисии във връзка с киберсигурността.

в) „участници от частния сектор“ означава представители на субекти от частния сектор, които предоставят или използват решения ([26]) и услуги ([27]) за киберсигурност.

г) „мащабен инцидент“ означава инцидент съгласно определението в член 4, параграф 7 от Директива (ЕС) 2016/1148, който има значително въздействие в най-малко две държави членки.

д) „интегриран доклад за състоянието на киберсигурността в ЕС“ означава доклад, в който се събират данни от участниците в съвместното киберзвено и който се съставя въз основа на определения в член 7, параграф 6 от Регламент (ЕС) 2019/881 доклад за техническото състояние на киберсигурността на ЕС.

е) „екип на ЕС за бързо реагиране за киберсигурност“ означава екип, съставен от признати експерти по киберсигурност, в частност от членовете на ЕРИКС на държавите членки, който с подкрепата на ENISA, CERT-EU и Европол има готовност да оказва от разстояние помощ на засегнатите от широкомащабни инциденти и кризи.

ж) „меморандуми за разбирателство“ означава споразумение, в което се определят редът и условията за сътрудничество, като в частност се определят ресурсите и процедурите за създаване и мобилизиране на екипите на ЕС за бързо реагиране за киберсигурност, както и тези за взаимопомощ.

([25]) В съответствие с подхода и принципите в Директива (ЕС) 2016/1148 и член 222 от ДФЕС, и без да се нарушава член 42, параграф 7 от Договора за Европейския съюз.

([26]) В т.ч. продавачи на софтуер.

([27]) В т.ч. разузнаване за заплахи.

III. **ЦЕЛ НА СЪВМЕСТНОТО КИБЕРЗВЕНО**

(4) Държавите членки и съответните институции, органи и агенции на ЕС следва да **координират на равнище ЕС ответните си действия** при мащабни киберинциденти и кризи, както и действията за възстановяване от тях. Такива координирани ответни действия следва в частност да се предприемат между оперативните участници — ENISA, Европол, CERT-EU, Комисията, Европейската служба за външна дейност (включително INTCEN), мрежата на ЕРИКС, EU-CyCLONe, и участниците с поддържаща роля — председателя на групата за сътрудничество за МИС, председателя на хоризонталната работна група на Съвета по въпросите на кибернетичното пространство и по един представител на съответните проекти по линия на ПСС ([28]). Оперативните участници следва да могат бързо и ефективно да мобилизират чрез съвместното киберзвено оперативни ресурси за взаимопомощ. За тази цел, при поискване от държава членка механизмите за взаимопомощ следва да бъдат координирани при съвместното киберзвено.

(5) С оглед на ефективността на координираната реакция изброените в точка 4 оперативни участници и участници с поддържаща роля следва, в границите на съответните си правомощия, да могат да обменят добри практики, да осигуряват непрекъснато **взаимна осведоменост за обстановката** и да имат необходимата степен на **готовност**. Тези участници следва да използват съществуващите процеси и експертния опит на различните общности за киберсигурност.

IV. **ОПРЕДЕЛЯНЕ НА ФУНКЦИОНИРАНЕТО НА СЪВМЕСТНОТО КИБЕРЗВЕНО**

(6) Държавите членки и съответните институции, органи и агенции на ЕС следва, въз основа на приноса на ENISA по член 7, параграф 7 от Регламент (ЕС) 2019/881, да **координират ответните си действия** при мащабни киберинциденти и кризи, както и действията за възстановяване от тях, чрез:

а) създаване, обучаване, изпитване и координирано разгръщане на **екипи на ЕС за бързо реагиране за киберсигурност**, като се използва предвиденото в член 7, параграф 4 от Регламент (ЕС) 2019/881 и в членове 3 и 4 от Регламент (ЕС) 2016/794;

б) координирано разгръщане на **виртуална и физическа платформа**, като се използва структурираното сътрудничество между ENISA и CERT-EU, залегнало в член 7, параграф 4 от Регламент (ЕС) 2019/881, която следва да служи като инфраструктура за подкрепа на техническото и оперативното сътрудничество между участниците и за набиране на съответния персонал и на други ресурси от участниците;

в) създаване и поддържане на опис **на оперативния и техническия капацитет в ЕС**, разгърнат в общностите за киберсигурност ([29]) в Съюза, с готовност да бъде впрегнат в действие при мащабни киберинциденти или кризи.

г) докладване до Комисията и върховния представител за натрупания опит при **оперативното сътрудничество по киберсигурност** вътре в самите общности за киберсигурност и между тях.

(7) С оглед на целите, заложени в член 7 от Регламент (ЕС) 2019/881 и член 3 от Регламент (ЕС) 2016/794, държавите членки и съответните институции, органи и агенции на ЕС следва да предприемат необходимото, така че съвместното киберзвено непрекъснато да осигурява сред отделните общности за киберсигурност, а и в рамките на самите такива общности, **взаимна осведоменост за обстановката** и **готовност** за реагиране на киберкризи. За тази цел държавите членки и съответните институции, органи и агенции на ЕС следва, в съответствие с Регламент (ЕС) 2019/881 и Регламент (ЕС) 2016/794, да създадат условия за провеждането на следните **поддържащи** операции:

а) събиране и проучване на цялата съответна информация и разузнавателни данни за заплахите, с оглед на съставянето на **интегриран доклад на ЕС за състоянието на киберсигурността**;

б) използване на подходящи и защитени **средства**, в съответствие с член 7, параграф 1 от Регламент (ЕС) 2019/881, за бърз обмен на информация сред участниците и с други субекти;

в) **обмен на необходимата информация и експертен опит**, за да се подготви Съюзът да управлява мащабни киберинциденти и кризи — със съдействието на ENISA, както е посочено в член 7, параграф 2 от Регламент (ЕС) 2019/881;

г) одобряване и изпитване на **национални планове за реагиране при киберинциденти и кризи** ([30]) — в съответствие с член 7, параграфи 2, 5 и 7 от Регламент (ЕС) 2019/881;

([28]) Координационен център за киберсигурност (Cyber and Information Domain Coordination Centre — CIDCC) и Екипи за бързо реагиране и взаимопомощ в областта на киберсигурността (Cyber Rapid Response Teams and Mutual Assistance in Cyber Security — CRRT).

([29]) Включително, когато е целесъобразно, общността за киберотбрана.

([30]) Предложена по силата на член 7, параграф 3 от Директивата относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148, COM(2020) 823 final, 2020/0359 (COD).

д) изготвяне, управление и изпитване, в т.ч. чрез учения и обучения в различни общности, на **плана на ЕС за реагиране при киберинциденти и кризи** — в съответствие с препоръката за концептуална рамка и член 7, параграф 3 от предложението на Комисията за преработена Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на киберсигурност в Съюза ([31]);

е) оказване на съдействие на участниците при свързването със **субекти от частния сектор** на споразумения за обмен на информация и на такива за оперативно сътрудничество, където сред предоставяните услуги са разузнаване за заплахи и реагиране при инциденти — със съдействието на ENISA, както е посочено в член 7, параграф 1 от Регламент (ЕС) 2019/881;

ж) установяване на структурирани полезни взаимодействия с националните, секторните и трансграничните **ресурси за наблюдение и откриване**, по-специално с оперативните центрове за сигурност;

з) оказване на съдействие на участниците при **управлението** на мащабни инциденти и кризи — в съответствие с подпомагащата роля на ENISA, както е посочено в член 7 от Регламент (ЕС) 2019/881. Тук спадат: съдействие за осигуряването на взаимна осведоменост за обстановката; подпомагане на дипломатическите действия; установяване на извършителите по политическа линия; установяване на извършителите, в т.ч. чрез Европол ([32]), при наказателни разследвания; съгласуване на комуникацията с обществеността; съдействие за възстановяването след инцидент.

(8) Държавите членки и съответните институции, органи и агенции на ЕС следва да изпълнят точки 6 и 7, като предприемат следното:

а) определят организационните аспекти на съвместното киберзвено и **ролите и задачите** във връзка с платформата на оперативните участници и участниците с поддържаща роля, така че да ѝ се осигури ефективно функциониране според изложените в приложението към настоящата препоръка аспекти и принципи;

б) сключват **меморандуми за разбирателство** за определяне на реда и условията за сътрудничество между участниците, посочени в точка 4.

(9) В изпълнение на член 7 от Регламент (ЕС) 2019/881 ENISA следва да координира и подпомага сътрудничеството на държавите членки и съответните институции, органи и агенции на ЕС в съвместното киберзвено, в т.ч. като осигури секретариат, организира заседанията и съдейства за провеждането на съответните действия в национален мащаб и на равнище ЕС. ENISA следва да създаде защитена виртуална платформа и физическо пространство за провеждане на заседанията, както и да подпомага провеждането на необходимите действия.

V. **ИЗГРАЖДАНЕ НА СЪВМЕСТНОТО КИБЕРЗВЕНО**

(10) Държавите членки и съответните институции, органи и агенции на ЕС следва да положат всички усилия, за да може съвместното киберзвено да започне да функционира на **30 юни 2022 г.** Към дадения момент оперативните участници следва да предоставят оперативен капацитет и експерти, които да бъдат сърцевината на екипите на ЕС за бързо реагиране за киберсигурност. Плановете за физическа и виртуална платформа следва да са отбелязали значителен напредък.

(11) Държавите членки и съответните институции, органи и агенции на ЕС следва да подпомагат функционирането на съвместното киберзвено и да положат всички усилия, за да му осигурят **до 30 юни 2023 г.** пълни оперативни възможности. Това следва да се извърши на четири последователни етапа, при всеки от които ще бъде предприето следното:

а) първи етап – до **31 декември 2021 г.**: оценка на организационните аспекти на съвместното киберзвено и определяне на наличния оперативен капацитет на ЕС;

б) втори етап – до **30 юни 2022 г.**: съставяне на планове за реагиране при инциденти и кризи и провеждане на съвместни действия за привеждане в готовност;

в) трети етап – до **31 декември 2022 г.**: начало на функционирането на съвместното киберзвено;

г) четвърти етап – до **30 юни 2023 г.**: обхващане на частния сектор в сътрудничеството в рамките на съвместното киберзвено и докладване за постигнатия напредък.

В приложението към настоящата препоръка са подробно описани действията, които трябва да се предприемат на всеки от четирите последователни етапа.

([31]) COM(2020) 823 final

([32]) В съответствие с Регламент (ЕС) 2016/794.

(12) При първите два етапа ENISA следва да организира и подпомага подготовката на съвместното киберзвено. С оглед на завършването на тази подготвителна работа службите на Комисията следва да свикат работна група, в чийто състав да влязат оперативните участници и участниците с поддържаща роля. Службите на Комисията следва да определят свой представител за съпредседател на работната група и да поканят за съпредседатели един представител, определен от върховния представител, който представител да участва в точките от дневния ред според съответната си компетентност, както и представител, избран от държавите членки.

(13) До края на втория етап работната група следва да приключи с оценката си на организационните аспекти на съвместното киберзвено и на ролите и задачите на оперативните участници в тази платформа. Работната група следва да представи резултатите от тази оценка на Комисията и на върховния представител. След това Комисията и върховният представител ще представят тази оценка на Съвета. Въз основа на тази оценка Комисията и върховният представител следва да изготвят съвместен доклад и да приканят Съвета да го одобри чрез заключения на Съвета.

(14) В началото на третия етап съвместното киберзвено следва вече да функционира.

(15) ENISA и Комисията следва в съответствие с приложимите разпоредби за създаване на съответните работни програми да използват наличните ресурси по линия на програмите на ЕС за финансиране и най-вече програмата „Цифрова Европа“, за да предоставят на участниците в съвместното киберзвено допълнителни възможности за обучение, капацитет за комуникации и защитена инфраструктура за обмен на информация, които да позволяват обмен на класифицирана информация, в т.ч. между отделните общности.

VI. **ПРЕГЛЕД**

(16) Държавите членки следва да си сътрудничат с Комисията и върховния представител, в съответствие с техните области на компетентност, с цел до **30 юни 2025 г.** да бъде оценена ефективността и ефикасността на съвместното киберзвено, за да се изведат заключения за бъдещето му. При тази оценка следва да се вземе предвид приключването на горепосочените четири етапа.

Съставено в Брюксел на 23 юни 2021 година.

За Комисията
Thierry BRETON
Член на Комисията

ПРИЛОЖЕНИЕ

Етапи на изграждане на съвместното киберзвено

В настоящото приложение се описват по-подробно основните и допълнителните действия, необходими за създаването и привеждането в действие на съвместното киберзвено.

1. *Етап 1 – Оценка на организационните аспекти на съвместното киберзвено и определяне на наличните оперативни способности на ЕС*

ОСНОВНИ ДЕЙСТВИЯ

Оперативните участници в съвместното киберзвено, обединени в работна група, създадена от Комисията, и с подкрепата на ENISA, следва да съберат информация относно наличните оперативни способности, включително да съставят списък на наличните доказани специалисти, посочвайки съответния им експертен опит, на наличните инструменти, функции и активи за справяне с инциденти, съществуващите портфейли от обучения и учения, както и съществуващите продукти за анализ на разузнавателна информация. Въз основа на тази информация оперативните участници следва да изготвят **списък на наличните оперативни способности на ЕС**, готови за използване в случай на киберинциденти или кризи, по-специално чрез екипите на ЕС за бързо реагиране в областта на киберсигурността.

Работната група следва да започне оценка на **организационните аспекти** на съвместното киберзвено **и на ролите и отговорностите на оперативните участници в рамките на тази платформа**.

За да се придобие обща представа за способностите и да се постигне съгласие по процедурите, основните действия и, доколкото е възможно, допълнителните действия от първия етап следва да приключат до **31 декември 2021 г. [6 месеца след приемането]** .

2. *Етап 2 – Изготвяне на планове за реакция при инциденти и кризи и стартиране на съвместни дейности за готовност*

ОСНОВНИ ДЕЙСТВИЯ

Оперативните участници в работната група, след консултация с подпомагащите ги участници, следва да изготвят **плана на ЕС за реакция при инциденти и кризи в областта на киберсигурността** въз основа на националните планове за реакция при инциденти и кризи в областта на киберсигурността. Планът на ЕС за реакция при инциденти и кризи в областта на киберсигурността следва да включва цели за готовност на ЕС, установени процедури и сигурни канали за обмен на информация, включително начини за обработка на информацията, както и критерии за задействане на механизма за взаимна помощ въз основа на договорена таксономия за класификация на инцидентите и на списъка на съществуващите способности на ЕС.

До края на втория етап работната група следва да приключи с оценката си на организационните аспекти на съвместното киберзвено и на ролите и отговорностите на оперативните участници в рамките на тази платформа. Работната група следва да представи резултатите от тази оценка на Комисията и на върховния представител. Комисията и върховният представител следва да запознаят Съвета с оценката. Комисията и върховният представител следва да работят заедно, съгласно съответните си компетенции, за изготвянето на съвместен доклад въз основа на оценката и да приканят Съвета да одобри този доклад чрез заключения на Съвета.

ДОПЪЛНИТЕЛНИ ДЕЙСТВИЯ

Планът на ЕС за реакция при инциденти и кризи в областта на киберсигурността следва да надгражда върху основните елементи на националните планове за реакция при инциденти и кризи в областта на киберсигурността. В съответствие с предложението на Комисията за директива относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148 ([1]) държавите членки следва да приемат национални планове за реакция при инциденти и кризи в областта на киберсигурността. В националните планове, които евентуално могат да бъдат подложени на партньорска проверка, следва да се определят целите и условията за управление на широкомащабни киберинциденти и киберкризи. В националните планове следва да бъдат предвидени в частност, следните елементи:

а. цели на националните мерки и дейности за готовност;

б. роли и отговорности на националните компетентни органи на национално равнище;

в. национални процедури за управление на кризи и канали за обмен на информация;

г. набелязване на мерки за готовност, включително дейности по учения и обучение;

д. определяне на съответните заинтересовани страни от публичния и частния сектор и съответната инфраструктура;

е. национални процедури и договорености между съответните национални органи и служби, включително тези, които отговарят за всички киберобщности, за да се гарантира, че държавите членки участват ефективно и оказват подкрепа за координираното управление на широкомащабни киберинциденти и киберкризи на равнището на ЕС.

Въз основа на информацията, предоставена от държавите членки и институциите, органите и агенциите на ЕС, оперативните участници следва да извършат следните допълнителни действия в рамките на съвместното киберзвено:

а. изготвяне на първия интегриран доклад на ЕС за състоянието на киберсигурността въз основа на националните планове за реакция при инциденти и кризи в областта на киберсигурността;

([1]) COM(2020) 823 final 2020/0359 (COD), Брюксел, 16.12.2020 г.

б. изграждане на комуникационни способности и сигурни инструменти за обмен на информация;

в. подпомагане на приемането на протоколи за взаимопомощ между участниците;

г. организиране на учения и обучения за експерти от различни киберобщности, включени в списъка на наличните оперативни способности на ЕС;

д. разработване на многогодишен план за координиране на ученията.

При необходимост оперативните участници следва да се консултират с подпомагащите ги участници. ENISA, с подкрепата на Комисията, Европол и CERT-EU, следва да създаде условия за обмен на информация чрез изграждането на комуникационни способности и сигурни инструменти за обмен на информация.

За да се гарантира изготвянето на необходимите планове и започването на съвместните дейности, основните действия и, доколкото е възможно, допълнителните действия от втория етап следва да приключат до **30 юни 2022 г. [6 месеца след края на етап 1]** .

3. *Етап 3 – Привеждане в действие на съвместното киберзвено*

ОСНОВНИ ДЕЙСТВИЯ

След като Съветът одобри заключенията на Комисията относно доклада от втория етап, оперативните участници следва да координират разпределянето на задачите и отговорностите между **екипите на ЕС за бързо реагиране в областта на киберсигурността** в рамките на съвместното киберзвено и да създадат **физическа платформа**, позволяваща на екипите да извършват технически и оперативни дейности. Въз основа на подготвителната работа, извършена през втория етап, участниците следва да финализират плана на ЕС за реакция при инциденти и кризи в областта на киберсигурността. Оперативните участници следва да гарантират, че експертите и способностите, включени в списъка на наличните оперативни способности на ЕС, са на разположение и са готови да допринесат за дейността на екипите на ЕС за бързо реагиране в областта на киберсигурността.

С цел изпълнение на плана на ЕС за реакция при инциденти и кризи в областта на киберсигурността участниците следва да изготвят годишна работна програма.

ДОПЪЛНИТЕЛНИ ДЕЙСТВИЯ

Съвместното киберзвено може да се използва от общността на кибердипломацията за съгласуване на публичната комуникация. Платформата може да даде възможност на участниците да допринесат за установяване на извършителите на политическо равнище, както и в контекста на наказателното правораздаване, извършвано от полицейските и съдебните органи. Освен това тя може да улесни възстановяването и да спомогне за структурирани полезни взаимодействия между националните и трансграничните способности за наблюдение и откриване.

За да се гарантира привеждането в действие на съвместното киберзвено, основните действия и, доколкото е възможно, допълнителните действия от трети етап следва да приключат до **31 декември 2022 г. [6 месеца след края на етап 2]** .

4. *Етап 4 – Разширяване на сътрудничеството в рамките на съвместното киберзвено към частни субекти и докладване за постигнатия напредък*

ОСНОВНО ДЕЙСТВИЕ

Участниците в съвместното киберзвено следва да изготвят доклад за дейността **относно постигнатия напредък в изпълнението на четирите етапа, очертани в препоръката, в който се описват постиженията и предизвикателствата в тази област**. Този доклад следва да включва статистическа информация относно дейностите за оперативно сътрудничество, извършени през четирите етапа. Докладът следва да бъде представен на Комисията и на върховния представител.

ДОПЪЛНИТЕЛНИ ДЕЙСТВИЯ

За да се разширят способностите и информацията, с които разполагат екипите на ЕС за бързо реагиране в областта на киберсигурността, участниците следва да гарантират, че съвместното киберзвено подпомага **сключването на споразумения за обмен на информация и за оперативно сътрудничество между участниците и субекти от частния сектор**, които предоставят, наред с другото, разузнавателна информация за заплахи и услуги, свързани с реакция при инциденти. Те следва също така да гарантират, че наред с други дейности съвместното киберзвено подпомага редовния диалог и дейностите по обмен на информация относно заплахите и уязвимите места с ползвателите на решения в областта на киберсигурността, най-вече със субектите, които попадат в обхвата на Директивата за МИС или участват в **центровете за споделяне и анализ на информация (ISAC) на равнище ЕС**.

Държавите членки следва да подкрепят субектите, които извършват дейност на тяхна територия, по-специално тези, попадащи в обхвата на Директивата за МИС, като им осигурят достъп и участие в публично-частния диалог в рамките на центровете за споделяне и анализ на информация на равнище ЕС.

За да се осигури подходящото участие на частния сектор, основните действия и, доколкото е възможно, допълнителните действия от четвърти етап следва да приключат до **30 юни 2023 г. [6 месеца след края на етап 3]**.

КАК БЪРЗО ДА СЕ МОБИЛИЗИРАТ ОПЕРАТИВНИТЕ СПОСОБНОСТИ НА ЕС

КОЙ ОСИГУРЯВА СПОСОБНОСТИ: Оперативните участници

КОЙ УПРАВЛЯВА СПОСОБНОСТИТЕ: Участници в рамките на съвместното киберзвено, в съответствие с договорените роли и отговорности

Етап	Цел	Задача	Основно действие	Допълнително действие
Етап 1 – Определяне До **31 декември 2021 г. [6 месеца след приемането]**	ГОТОВНОСТ	**Определяне на способностите**	**Оперативни участници съставят списък на наличните оперативни способности на ЕС.**	
Етап 2 — Подготовка До **30 юни 2022 г. [6 месеца след края на етап 1]**	ГОТОВНОСТ	**Определяне на съответните процедури и договорености за задействане на способностите в случай на необходимост**	**Въз основа на приетите национални планове оперативните участници подготвят плана на ЕС за реакция при инциденти и кризи в областта на киберсигурността (Рамка на ЕС за реакция при кризи в областта на киберсигурността съгласно концепцията)**	**Въз основа на доклада за техническото състояние на киберсигурността в ЕС оперативните участници изготвят интегрирани доклади за състоянието на киберсигурността в ЕС**
	ГОТОВНОСТ	**Възможности за провеждане на учения**		**Участниците организират съвместно учение и обучение (за различните киберобщности)** **Участниците изготвят многогодишен план за координиране на ученията.**
	ОСВЕДОМЕНОСТ ЗА СЪСТОЯНИЕТО НА КИБЕРСИГУРНОСТТА	**Създаване на инструменти за обмен на информация и искания за взаимопомощ**		**Участниците установяват сигурен и бърз обмен на информация**
СЪВМЕСТНОТО КИБЕРЗВЕНО Е ПРИВЕДЕНО В ДЕЙСТВИЕ Въз основа на подготвителната работа, извършена от участниците в работна група, която ще бъде създадена от Комисията				
Етап 3 – Въвеждане До **31 декември 2022 г. [6 месеца след края на етап 2]**	ГОТОВНОСТ	**Приемане на съответните процедури, договорености и меморандуми за разбирателство относно задействането на способностите в случай на необходимост**	**Оперативните участници финализират плана на ЕС за реакция при инциденти и кризи в областта на киберсигурността и планират неговото изпълнение чрез годишни работни програми.**	**Участниците подпомагат създаването на национални и трансгранични способности за наблюдение и откриване, включително създаването на центрове за операции по сигурността (ЦОС)**
	КООРДИНИРАНА РЕАКЦИЯ	**Разгръщане на способности в случай на необходимост**	**Оперативните участници координират оперативните екипи на ЕС за бързо реагиране в областта на киберсигурността чрез виртуалната и физическата платформа на съвместното киберзвено в Брюксел.**	**Участниците координират публичната комуникация и допринасят за установяване на извършителите на политическо равнище, както и в контекста на наказателното правораздаване, извършвано от полицейските и съдебните органи.**

Етап 4 – Разширяване на сътрудничеството и докладване До **30 юни 2023 г. [6 месеца след края на етап 3]**	ОСВЕДОМЕНОСТ ЗА СЪСТОЯНИЕТО НА КИБЕРСИГУРНОСТТА КООРДИНИРАНА РЕАКЦИЯ	**Осигуряване на възможност за разрастване чрез привличане на частния сектор за посрещане на възникващи нужди**	**Участниците представят доклад за дейността относно постигнатия напредък, в който, подкрепени със статистическа информация, се описват постиженията и предизвикателствата.**	**Участниците сключват споразумения за обмен на информация, както и споразумения за оперативно сътрудничество с доставчиците на киберсигурност** **Участниците сключват споразумения за обмен на информация с ползватели на киберсигурност, предимно субектите, попадащи в обхвата на Директивата за МИС, и участващи в центровете за споделяне и анализ на информация на равнище ЕС**