Съвет на
Европейския съюз

Брюксел, 20 октомври 2021 г.
(OR. en)

13048/21

CYBER 263
JAI 1117
TELECOM 384
CSC 362
CIS 116
RELEX 874
ENFOPOL 370
COPS 373
COSI 190
HYBRID 62
CSCI 133
POLGEN 177
DATAPROTECT 244

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
Дата:	19 октомври 2021 г.
До:	Делегациите
№ предх. док.:	12534/21
Относно:	Заключения на Съвета относно проучване на потенциала на инициативата за съвместно киберзвено – допълване на координираната реакция на ЕС при мащабни инциденти и кризи в областта на киберсигурността – Заключения на Съвета (19 октомври 2021 г.)

Приложено се изпращат на делегациите заключенията на Съвета относно проучване на потенциала на инициативата за съвместно киберзвено – допълване на координираната реакция на ЕС при мащабни инциденти и кризи в областта на киберсигурността, приети на заседанието на Съвета от 19 октомври 2021 г.

ПРИЛОЖЕНИЕ

Заключения на Съвета относно проучване на потенциала на инициативата за съвместно киберзвено – допълване на координираната реакция на ЕС при мащабни инциденти и кризи в областта на киберсигурността

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

КАТО ПРИПОМНЯ своите заключения относно:

– стратегията на ЕС за киберсигурност за цифровото десетилетие[1],

– координираната реакция на ЕС при мащабни инциденти и кризи в областта на киберсигурността[2],

– кибердипломацията[3],

– рамката за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството („инструментариум за кибердипломация“)[4],

– сигурността и отбраната[5],

– рамката за политиката на ЕС за кибернетична отбрана[6],

– изграждането на цифровото бъдеще на Европа[7],

– Решение за изпълнение (ЕС) 2018/1993 на Съвета от 11 декември 2018 г. относно договорености за интегрирана реакция на ЕС при политическа криза,

---

1 7290/21.
2 10086/18.
3 6122/15 + COR 1.
4 10474/17.
5 8396/21.
6 15585/14.
7 8711/20.

– Съвместното съобщение до Европейския парламент и Съвета „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“[8],

– капацитета за киберсигурност и изграждането на способности в ЕС[9],

1. НАБЛЯГА на значението на киберсигурността за изграждането на устойчива, цифрова и зелена Европа. ИЗТЪКВА, че киберсигурността е от първостепенна важност за просперитета и сигурността на ЕС и неговите държави членки, на неговите граждани, предприятия и институции, както и за поддържането на интегритета на нашите свободни и демократични общества.

2. ПРИЗНАВА трансграничното и междусекторното естество на много от заплахите за киберсигурността, както и рисковете и потенциалните последици от непрекъснатите кампании на все по-въздействащи, високотехнологични, целенасочени, сложни, настойчиви и/или всеобхватни злонамерени действия в киберпространството[10]. Пандемията от COVID-19 разкри още повече уязвимостта на нашите общества и вероятността от щети в резултат на мащабни киберинциденти за икономиката, демокрацията, основните услуги и критичната инфраструктура, особено в сектора на здравеопазването. Тя доведе и до нарастване на значението на свързаността и зависимостта на обществото от благонадеждни, внушаващи доверие и сигурни мрежови и информационни системи. В крайна сметка пандемията подчерта необходимостта от глобален, отворен, свободен, стабилен и сигурен интернет, както и от доверие в продуктите, процесите и услугите на информационните и комуникационни технологии (ИКТ) и тяхната сигурност, включително необходимостта да се гарантира устойчивостта на веригата на доставки.

---

8 14435/17 + COR 1.
9 7737/19.
10 ENISA Threat Landscape 2020.

3. ОТНОВО ИЗТЪКВА значението на киберустойчивостта и на по-задълбоченото развиване на рамката на ЕС за управлението на кризи в областта на киберсигурността[11] с цел ефективна и навременна реакция на равнището на ЕС спрямо мащабни инциденти и кризи в областта на киберсигурността, както и на по-нататъшното ѝ интегриране в съществуващите хоризонтални и секторни механизми на ЕС за реакция при кризи. ИЗТЪКВА ролята на Съвета и на интегрираните договорености на ЕС за реакция на политическо равнище при кризи (IPCR) за осигуряване на своевременна координация и реакция на политическо равнище на Съюза при кризи – независимо дали възникват в Съюза или извън него – и които са с широкообхватно въздействие или политическо значение. ИЗТЪКВА значението тези рамки и механизми да бъдат изпитвани на редовни учения.

4. ПРИПОМНЯ, че дейностите на равнището на ЕС при широкомащабни киберинциденти и кризи се провеждат в съответствие с принципите на субсидиарност, пропорционалност, взаимно допълване, избягване на дублирането и поверителност. ОТНОВО ИЗТЪКВА, че държавите членки носят основната отговорност за реагиране на засягащите ги мащабни инциденти и кризи в областта на киберсигурността. ПРИПОМНЯ, че е важно да се зачитат компетенциите на държавите членки и тяхната изключителна отговорност за националната сигурност в съответствие с член 4, параграф 2 от Договора за Европейския съюз, в това число в областта на киберсигурността.

5. Същевременно ПРИПОМНЯ, че е важно да се зачитат компетенциите и мандатите на институциите, органите и агенциите на ЕС. Върховният представител, Комисията и другите институции, органи и агенции на ЕС също имат важна роля, произтичаща от правото на Съюза, включително поради възможното въздействие на мащабните инциденти и кризи в областта на сигурността върху единния пазар, както и върху самото функциониране на институциите, органите и агенциите на ЕС.

[11] 10086/18.

6. ПОДЧЕРТАВА необходимостта при по-нататъшното развитие на рамката на ЕС за управление на кризи в областта на киберсигурността да се избягва ненужно дублиране и да се търси взаимно допълване и добавена стойност, както и да се гарантира синхрон със съществуващите механизми, инициативи, мрежи, процеси и процедури на национално и европейско равнище. ПРИДАВА ОСОБЕНО ЗНАЧЕНИЕ на рационализирането на съществуващите процеси и структури, за да се намали тяхната сложност и в интерес на сближаването в рамките на Съюза да се подобрят достъпността и способността за реагиране за търсещите помощ и солидарност.

7. ОТЧИТА приложимостта на международното право, включително на Устава на ООН в неговата цялост, на международното хуманитарно право и правото в областта на правата на човека в киберпространството, и НАСЪРЧАВА спазването на доброволните, необвързващи норми, правила и принципи на отговорно поведение на държавите в киберпространството, подкрепяни от всички държави – членки на ООН.

8. ПРИВЕТСТВА напредъка, постигнат през последните години в Съвета, по-специално в Хоризонталната работна група по въпроси на кибернетичното пространство (HWPCI) и други съответни работни групи на Съвета, както и в подемането на други инициативи за сътрудничество и обмен на информация между държавите членки, по-специално Групата за сътрудничество за МИС и мрежата на CSIRT, създадени с Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г., мрежата за връзка на организациите при кибернетични кризи (CyCLONe), както и съответните проекти на ЕС в областта на киберотбраната, изпълнявани в рамките на постоянното структурирано сътрудничество (ПСС)[12], Съвместната работна група за действие в областта на киберпрестъпността (J-CAT), Европейската съдебна мрежа по въпросите на киберпрестъпността (EJCN), доброволното участие на държавите членки в Ситуационния център на ЕС, както и координацията и сътрудничеството в контекста на инструментариума за кибердипломация.

---

[12] По-специално проектите „Екипи за бързо реагиране при кибератаки и екипи за взаимопомощ в областта на киберсигурността“, „Координационен център в областта на киберсигурността и информацията“, „Платформа за обмен на информация относно киберзаплахи и реагиране при инциденти“, координирани съответно от Литва, Германия и Гърция.

9. ПРИПОМНЯ съществуващите рамки за сътрудничество между институциите, органите и агенциите на ЕС, като структурираното сътрудничество между ENISA и CERT-EU, както и Меморандума за разбирателство между ENISA, Европейската агенция по отбрана (EDA), Европейския център за борба с киберпрестъпността към Европол (EC3) и CERT-EU. ИЗТЪКВА значението на постоянния редовен обмен на информация със Съвета относно по-нататъшното развитие на тези рамки за сътрудничество.

10. ПОДЧЕРТАВА значението на засилването на сътрудничеството и обмена на информация между различните киберобщности в рамките на ЕС и неговите държави членки на всички необходими равнища – техническо, оперативно и стратегическо/политическо – и на свързването на съществуващите механизми, мрежи, структури, процеси и процедури за управление на кризи в случаите, когато това подпомага и подобрява справянето с широкомащабни киберинциденти и кризи.

11. ПРИЗНАВА напредъка, постигнат от група държави членки в създаването на съвместна оперативна киберспособност „Екипи за бързо реагиране при кибератаки“ в рамките на ПСС, чиято цел е да се задълбочи доброволното сътрудничество в киберсферата чрез взаимопомощ, включително в отговор на широкомащабни киберинциденти и кризи.

12. ПРИЗНАВА опита и способността за реагиране по всяко време на правоприлагащата общност в областта на оперативното сътрудничество и сигурния обмен на информация срещу големи трансгранични кибератаки чрез Протокола за реагиране при извънредни ситуации на правоприлагащите органи в ЕС.

13. ОТЧИТА продължаващото прилагане на рамката за съвместен дипломатически отговор на ЕС срещу злонамерени кибердействия („инструментариум за кибердипломация“). ПРИПОМНЯ, че всяка държава членка е свободна да взема суверенно решение, за всеки отделен случай, по отношение на определянето на дадена кибердейност като злонамерена. ПРИПОМНЯ, че мерките, предприети в рамките на съвместен дипломатически отговор на ЕС на злонамерени кибердействия, следва да се основават на взаимна ситуационна осведоменост, договорена между държавите членки. Центърът на ЕС за анализ на информация (EU INTCEN) играе централна роля като център за предоставяне на ситуационна осведоменост и оценка на заплахите по кибервъпроси за ЕС въз основа на доброволен принос от държавите членки в областта на разузнаването и без да се засягат областите им на компетентност.

14. ИЗТЪКВА ОТНОВО значението на взаимната помощ и солидарността в съответствие с член 42, параграф 7 от Договора за Европейския съюз и член 222 от Договора за функционирането на Европейския съюз и ПРИЗОВАВА за по-нататъшни учения с киберизмерение. ПРИПОМНЯ необходимостта да се обмисли съгласуването между рамката на ЕС за управление на кризи в областта на киберсигурността, инструментариума за кибердипломация и разпоредбите на горепосочените членове в случай на мащабен киберинцидент или криза. ПРИПОМНЯ още, че задълженията на държавите членки, произтичащи от член 42, параграф 7 от Договора за Европейския съюз, не засягат специфичния характер на политиката за сигурност и отбрана на някои държави членки. ПРИПОМНЯ също, че НАТО остава за държавите, които членуват в нея, основа за колективната им отбрана.

15. ОТЧИТА сътрудничеството между ЕС и НАТО в областта на киберсигурността и отбраната, включително обмена на информация между екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU) и екипа на НАТО за реагиране при компютърни инциденти (NCIRC), при пълно зачитане на принципите на прозрачност, реципрочност и приобщаване, както и на автономността за вземане на решения на двете организации.

16. ПРИЗНАВА значението на сътрудничеството, по целесъобразност, с частния сектор по отношение на ученията за обмен на информация и предоставянето на съответния експертен опит, както и на надеждните решения и услуги, включително например за подпомагане на реакцията при инциденти и за повишаване на ситуационната осведоменост между различните киберобщности.

17. ПОДЧЕРТАВА значението на сигурните канали за комуникация за обмена на класифицирана и чувствителна информация. ИЗТЪКВА необходимостта от по-нататъшен напредък.

Във връзка с това и като се има предвид гореизложеното,

18. ОТЧИТА Препоръката на Комисията за изграждането на съвместно киберзвено като инициатива, която да бъде разгледана при по-нататъшното разработване на рамката на ЕС за управление на кризи в областта на киберсигурността[13].

19. ПРИЗОВАВА ЕС и неговите държави членки да продължат усилията си за по-всеобхватна и ефективна рамка на ЕС за управление на кризи в областта на киберсигурността, като се основават на съществуващите механизми и на вече постигнатия напредък, и да вземат предвид потенциала на инициативата за съвместно киберзвено за допълване на тези механизми чрез поетапен подход. ПОДЧЕРТАВА, че един постепенен, прозрачен и приобщаващ процес ще бъде от съществено значение за повишаване на доверието и следователно от решаващо значение за по-нататъшното разработване на рамка на ЕС за управление на кризи в областта на киберсигурността. Този процес следва да зачита съществуващите роли, компетенции и мандати на държавите членки и институциите, органите и агенциите на ЕС, както и принципите, посочени в настоящите заключения, включително принципите на пропорционалност, субсидиарност, приобщаване, взаимно допълване, избягване на дублирането и поверителност на информацията. Същевременно ПОДЧЕРТАВА, че всяко евентуално участие във или принос на държавите членки към едно потенциално съвместно киберзвено ще има доброволен характер.

[13] C(2021) 4520 final (11155/21 и 11155/21 ADD1).

20. ИЗТЪКВА необходимостта от установяване на подходящи работни методи и управление, за да се даде възможност за включване и участие на всички държави членки в разискванията, разработването и ефективните процеси на вземане на решения относно рамката на ЕС за управление на кризи в областта на киберсигурността, включително относно потенциалната инициатива за съвместно киберзвено. ПРИЗОВАВА за зачитане на прерогативите на Съвета съгласно Договорите и на принципа на лоялно сътрудничество.

21. ПОДЧЕРТАВА значението на идентифицирането и включването на всички съответни киберобщности в рамките на ЕС и неговите държави членки, като същевременно се вземат предвид различните им роли и отговорности в различните видове мащабни киберинциденти и кризи. ПОДЧЕРТАВА важната роля на Съвета, по-специално чрез Хоризонталната работна група по въпроси на кибернетичното пространство, за изготвянето на политики и координацията по отношение на по-нататъшното развитие на рамката на ЕС за управление на кризи в областта на киберсигурността. Поради това ПРИКАНВА държавите членки, Комисията, Европейската служба за външна дейност (ЕСВД), EU INTCEN, CERT-EU, ENISA, Европол (EC3 - Европейски център за борба с киберпрестъпността), Евроюст (EJCN), Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ECCC), както и представителите на мрежата на CSIRT, мрежата CyCLONe, групата за сътрудничество за МИС, Европейската агенция по отбрана (EDA) и съответните проекти по линия на ПСС, както и други възможни заинтересовани страни, да участват в този процес. Евентуалното създаване на работна група, съгласно предложеното в препоръката на Комисията, би могло да бъде допълнително проучено, като се гарантира подходящо представителство на всички държави членки и като се действа под политическото ръководство на Съвета, която да служи като временен форум, обединяващ представители на всички съответни киберобщности в държавите членки и в рамките на ЕС. Тази работна група следва редовно да докладва за дейността си и да представя евентуални предложения на Съвета за обсъждане, одобрение и допълнителни насоки. Освен това могат да бъдат установени други форми на диалог в рамките на и между общностите, включително чрез работни срещи, семинари, съвместни обучения и учения.

22. ПОДЧЕРТАВА ролята на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ECCC) и Мрежата от национални координационни центрове във връзка с потенциалното съвместно киберзвено, особено като се има предвид неговата роля за значителното увеличаване на технологичния капацитет, технологичните решения, способностите и уменията на Съюза в областта на киберсигурността.

23. ПРИКАНВА ЕС и неговите държави членки да се ангажират с по-нататъшното разработване на рамката на ЕС за управление на кризи в областта на киберсигурността, включително чрез проучване на потенциала на инициативата за съвместно киберзвено, чрез установяване и определяне на процеса, в т.ч. на основни етапи и график, както и чрез изясняване на целите и възможните роли и отговорности. НАБЛЯГА НА необходимостта от приоритетно консолидиране на съществуващите мрежи и взаимодействия в рамките на всяка общност, както и от установяване на цялостно картографиране на възможните пропуски и потребности от обмен на информация в рамките на и между киберобщностите, както и в рамките на и между европейските институции, органи и агенции, и впоследствие да се постигне съгласие относно евентуалните основни цели и приоритети на едно потенциално съвместно киберзвено. Без да предопределя резултатът, ИЗТЪКВА необходимостта от съсредоточаване върху определянето на нуждите от обмен на информация, за да се изгради обща ситуационна осведоменост сред всички съответни общности. При установяването на пропуските и потребностите от обмен на информация, включително възможното използване на виртуални платформи, следва да продължи да се обръща необходимото внимание на сигурните комуникационни канали за обмен на класифицирана и чувствителна информация, като същевременно ИЗТЪКВА значението на използването на вече съществуващата инфраструктура. Въвеждането на постепенен подход има за цел да изгради доверие и основа за евентуални по-нататъшни стъпки, свързани с подобряване на готовността и оперативното сътрудничество. ПРИЗНАВА, че различните цели могат да изискват различни решения и ангажирането на различен набор от представители на съответните киберобщности в рамките на ЕС и неговите държави членки.

24. ПРИЗОВАВА за допълнително разглеждане на правното основание за потенциалното съвместно киберзвено по време на целия процес, включително оценка на задачите и ролите спрямо възложените на ENISA в препоръката в контекста на член 7 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. ПРИЗОВАВА за по-нататъшно обмисляне на отделните елементи на препоръката относно съвместното киберзвено, включително по отношение на идеята за екипите на ЕС за бързо реагиране в областта на киберсигурността, както и на плана на ЕС за реагиране при киберинциденти и кризи. ИЗТЪКВА СПЕЦИАЛНО, че потенциалното съвместно киберзвено трябва да зачита компетенциите, мандатите и законовите правомощия на своите евентуални бъдещи участници.

25. ПРИЗОВАВА ЕС и неговите държави членки да разгледат потенциала на инициативата за съвместно киберзвено, включително от гледна точка на институциите, органите и агенциите на ЕС, за да се допълнят текущите усилия на равнището на държавите членки. ПРИВЕТСТВА намерението на Комисията да засили устойчивостта на съответните институции, органи и агенции на ЕС чрез предстоящото си предложение за регламент относно общите задължителни правила за киберсигурност за институциите, органите и агенциите на ЕС.

26. В заключение ПОТВЪРЖДАВА ОТНОВО своя ангажимент за повишаване на киберустойчивостта и по-нататъшно развитие на рамката на ЕС за управление на кризи в областта на киберсигурността, и РЕДОВНО ЩЕ НАБЛЮДАВА напредъка и ще предоставя допълнителни насоки за допълване на рамката на ЕС за управление на кризи в областта на киберсигурността.