Съвет на
Европейския съюз

Брюксел, 20 ноември 2017 г.
(OR. en)

14435/17

CYBER 183
TELECOM 303
ENFOPOL 534
JAI 1055
MI 845
COSI 283
JAIEX 101
RELEX 989
IND 317
CSDP/PSDC 643
COPS 360
POLMIL 145

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
Дата:	20 ноември 2017 г.
До:	Делегациите
№ предх. док.:	13943/17 + COR 1
№ док. Ком.:	12210/17, 12211/17
Относно:	Заключения на Съвета относно Съвместното съобщение до Европейския парламент и Съвета: „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“ - Заключения на Съвета (20 ноември 2017 г.)

Приложено се изпращат на делегациите заключенията на Съвета относно Съвместното съобщение до Европейския парламент и Съвета „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“, приети от Съвета по общи въпроси на 20 ноември 2017 г.

ПРИЛОЖЕНИЕ

Заключения на Съвета относно съвместното съобщение до Европейския парламент и Съвета „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“

Съветът на Европейския съюз,

1. КАТО ПРИЗНАВА значението на киберсигурността за просперитета, растежа и сигурността на ЕС, както и за целостта на нашите свободни и демократични общества и за процесите, на които тези общества се основават в цифровата епоха, чрез закрила както на принципите на правовата държава, така и на човешките права и основните свободи на всеки човек;

2. КАТО ПОДЧЕРТАВА, че е необходимо към киберсигурността да се подхожда последователно на национално, европейско и световно равнище, тъй като киберзаплахите могат окажат въздействие върху нашата демокрация, просперитет, стабилност и сигурност;

3. КАТО ОТБЕЛЯЗВА, че високото равнище на устойчивост на киберпространството в целия ЕС е важно и за доверието в цифровия единен пазар и за по-нататъшното развитие на Европа на цифровите технологии;

4. КАТО ИЗТЪКВА ОТНОВО, че ЕС ще насърчава постоянно отвореното, глобално, свободно, мирно и сигурно киберпространство, в което правата на човека и основните свободи, и по-специално правото на свобода на изразяване, достъп до информация, защита на данните, неприкосновеност на личния живот и сигурност, както и основните ценности и принципи на ЕС, се зачитат и прилагат изцяло както в рамките на ЕС, така и в световен мащаб, и КАТО ИЗТЪКВА, че е от решаващо значение да се гарантира установяването на подходящ баланс между правата на човека и основните свободи и спазването на изискванията на политиката за вътрешна сигурност на ЕС[1],

5. КАТО ПРИЗНАВА, че международното право, включително Хартата на ООН в нейната цялост, международното хуманитарно право и правото в областта на правата на човека се прилагат и в киберпространството, и КАТО ПОДЧЕРТАВА, че е необходимо да продължат усилията за гарантиране на спазването на международното право в киберпространството;

[1] Док. 12650/17.

6. КАТО ПРИПОМНЯ своите заключения относно Стратегията на Европейския съюз за киберсигурност[2], управлението на интернет[3] укрепването на отбранителната способност на Европа срещу кибератаки[4], кибердипломацията[5] рамката за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството[6] повишаването на ефективността на наказателното правосъдие в киберпространството[7]; сигурността и отбраната в рамките на Глобалната стратегия на ЕС[8], Съвместната рамка за борба с хибридните заплахи[9], и относно междинния преглед на обновената стратегия за вътрешна сигурност на Европейския съюз за периода 2015—2020 г.[10];

7. КАТО ПРИЗНАВА, че рамката, предоставена с Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство (Конвенцията от Будапеща) създава солидна основа за група от различни държави за използването на ефективен правен стандарт за различните национални законодателства и за международното сътрудничество в борбата с киберпрестъпността;

8. КАТО ПРИЗНАВА необходимостта от подновен акцент върху прилагането на политическата рамка на ЕС за кибернетична отбрана от 2014 г. и от нейното актуализиране, така че въпросите на киберсигурността и отбраната да бъдат интегрирани в Общата политика за сигурност и отбрана (ОПСО) и в по-широката програма в областта на сигурността и отбраната;

9. КАТО ПРИЗНАВА, че конкурентоспособността на европейската икономика в световен мащаб е важен елемент за постигането на високо равнище на киберсигурност на национално равнище и в целия ЕС;

10. КАТО ПРИПОМНЯ, че съгласно член 4, параграф 2 от ДЕС националната сигурност остава единствено в рамките на отговорността на всяка държава членка.

---

2 Док. 12109/13 и док. 6225/13 (Съвместно съобщение до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите: Стратегия на Европейския съюз за киберсигурност Отворено, безопасно и сигурно киберпространство (COM JOIN(2013) 1 final).

3 Док. 16200/14 и док. 6460/14 (Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите: „Политиката по отношение на интернет и управлението му. Ролята на Европа за определяне на бъдещото управление на интернет“ (COM(2014) 72 final).

4 Док. 14540/16 и док. 11013/16 (Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите: Укрепване на отбранителната способност на Европа срещу кибератаки и изграждане на конкурентен и иновативен сектор на киберсигурността (COM 2016(410) final).

5 Док. 6122/15.

6 Док. 9916/17.

7 Док. 10007/16.

8 Док. 9178/17.

9 Док. 7688/16 (Съвместно съобщение до Европейския парламент и Съвета: Съвместна рамка за борба с хибридните заплахи — ответни действия на Европейския съюз).

10 Док. 12650/17.

С НАСТОЯЩОТО

11. ПРИВЕТСТВА Съвместното съобщение до Европейския парламент и Съвета: „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“ за това, че набелязва амбициозна цел за повишаване на киберсигурността в ЕС. Съобщението допринася и за стратегическата автономност на ЕС, както е посочено в заключенията на Съвета относно глобалната стратегия за външната политика и политиката на сигурност на Европейския съюз[11], като се стреми към изграждането на Европа на цифровите технологии, която ще бъде по-сигурна, вдъхваща доверие, осъзнаваща своите силни страни, конкурентоспособна, отворена към света, зачитаща общите ценности на Съюза относно отворения, свободен, мирен и сигурен глобален интернет – а оттук и постигаща по-високо ниво на устойчивост с цел предотвратяване, възпиране, разкриване и реагиране при киберзаплахи, и способна да реагира колективно при киберзаплахи, засягащи целия ЕС, и

12. ПРИКАНВА държавите членки, институциите, агенциите и органите на ЕС да работят заедно, като зачитат съответните си области на компетентност и принципите на субсидиарност и пропорционалност, за изпълнение на стратегическите цели, поставени в тези заключения, и

13. ПОДЧЕРТАВА, че е необходимо ЕС, неговите държави членки и частният сектор да осигурят достатъчно финансиране, при зачитане на наличните ресурси, в подкрепа на изграждането на устойчивост на киберпространството и на усилията за научни изследвания и развитие в областта на киберсигурността в целия ЕС, както и да укрепват сътрудничеството за предотвратяване, възпиране, разкриване и реагиране при киберзаплахи и да бъдат в състояние да реагират колективно на кибернетични инциденти в голям мащаб и на злонамерени кибернетични дейности в целия ЕС;

[11] Док. 13202/16.

Глава I

ОСИГУРЯВАНЕ НА ЕФЕКТИВНА УСТОЙЧИВОСТ НА КИБЕРПРОСТРАНСТВОТО В ЕС И НА ДОВЕРИЕ В ЦИФРОВИЯ ЕДИНЕН ПАЗАР

14. ПОДЧЕРТАВА, че всяка държава членка носи основната отговорност за подобряване на собствената си киберсигурност и за осигуряването на реагиране при кибернетични инциденти и кризи, докато ЕС може да осигури значителна добавена стойност в подкрепа на сътрудничеството между държавите членки. В този контекст ИЗТЪКВА необходимостта всички държави членки да осигурят нужните ресурси за националните органи, отговарящи за киберсигурността, за да се гарантира предотвратяването, разкриването и реагирането при кибернетични инциденти и кризи в целия Съюз;

15. ПОДЧЕРТАВА, че е необходимо, когато е възможно, да се използват съществуващите механизми, структури и организации на равнището на ЕС;

16. ПРИВЕТСТВА:

- постигнатия напредък в транспонирането на директивата за МИС от държавите членки и ИЗТЪКВА необходимостта от пълно и ефективно прилагане до май 2018 г., както е предвидено в тази директива[12];
- извършеното в рамките на групата за сътрудничество за МИС за задълбочаване на стратегическото сътрудничество и обмена на информация между държавите членки;
- извършеното в рамките на мрежата на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС), по-специално за укрепване на оперативното сътрудничество между държавите членки, изграждането на доверие при обмена на информация в отговор на мащабни кибернетични инциденти и, въз основа на националните заключения от държавите членки, при предоставянето на елементи за обща ситуационна осведоменост на европейско равнище;
- извършеното в рамките на договорното публично-частно партньорство в областта на киберсигурността.

[12] Без да се засяга компетентността на държавите членки за транспонирането на директивата за МИС, по-специално по отношение на операторите на основни услуги.

17. ПРИВЕТСТВА факта, че в Съвместното съобщение се потвърждава, че солидното и надеждно криптиране е от изключително значение за надлежното гарантиране на правата на човека и на основните свободи в ЕС, както и за общественото доверие в цифровия единен пазар, като същевременно отчита необходимостта правоприлагащите органи да разполагат с достъп до данните, необходими за техните разследвания, и също, че сигурната цифрова идентификация и комуникация играят ключова роля за гарантирането на ефективна киберсигурност в ЕС;

18. ПРИВЕТСТВА планираното в Съвместното съобщение увеличаване на амбицията при редовното провеждане на общоевропейските учения в областта на киберсигурността, въз основа на опита от ученията Cyber Europe, съчетаващи реагиране на различни равнища, тъй като това ще бъде важен елемент от подобряването на подготвеността на държавите членки и на институциите на ЕС за реагиране при мащабни кибернетични инциденти;

19. ПРИЗОВАВА ЕС и неговите държави членки да провеждат редовни стратегически учения в областта на киберсигурността в различните състави на Съвета, въз основа на опита от EU CYBRID 2017, и

20. Без да се засяга крайният резултат от законодателния процес:

- ПРИВЕТСТВА предложението за интензивен и постоянен мандат на Агенцията на ЕС за мрежова и информационна сигурност (ENISA) с основна цел да подкрепя и развива по-тясно сътрудничество между държавите членки, да повишава техния капацитет и доверието в Европа на цифровите технологии;

- ПОТВЪРЖДАВА ОТНОВО, че бъдещата агенция следва да разчита на опита и експертните познания в рамките на държавите членки и на ЕС и да подкрепя последователното разработване и прилагане на съществуващите и бъдещи политики и регламенти в областта на киберсигурността в ЕС, като същевременно се гарантира, че всички правомощия на ENISA биват развивани, така че да допълват правомощията на държавите членки;

- ПОТВЪРЖДАВА ОТНОВО целта за повишаване на доверието в Европа на цифровите технологии посредством по-голямо доверие в цифровите решения и иновациите, включително интернет на нещата, електронната търговия и електронното управление, по-специално по отношение на Европейска рамка за сертифициране на киберсигурността, която да бъде на световно равнище[13]. Това изискване е от решаващо значение за насърчаване на доверието и на сигурността на цифровите продукти и услуги, защитата на критичната инфраструктура, данните на правителствата, гражданите и стопанските субекти и стои в основата на приемането на подхода „сигурност още при проектирането“ на продукти, услуги и процеси в рамките на цифровия единен пазар;

- ИЗТЪКВА, че законодателната работа по укрепване на сертифицирането на киберсигурността на равнище ЕС ще трябва да отговори на потребностите на пазара и потребителите, да надгражда върху опита на съществуващите в ЕС капацитет за и процеси на сертифициране (например рамката на Групата на висшите служители по сигурността на информационните системи SOG-IS) и да установи рамка, способна на бързо адаптиране към бъдещите развития в областта на цифровите технологии;

- ИЗТЪКВА, че при разширяването на сертифицирането на киберсигурността в ЕС следва да бъде обхванат целият спектър от изисквания за сигурност, включително най-високите изисквания, налагащи да се демонстрира съпротива срещу способностите на нападателите. Ключови фактори за успеха ще бъдат гарантирането на надежден, прозрачен и независим процес за сертифициране на сигурността, за да се насърчава предоставянето на надеждни и сигурни устройства, софтуер и услуги в рамките на цифровия единен пазар и извън него; признаването на съответния експертен опит на европейската промишленост, правителствата и специалистите по оценката посредством европейски и световни стандарти[14]; зачитане на ролята на държавите членки в процеса на сертифициране, що се отнася до оценката на по-високи нива на сигурност, и по-специално във връзка с основните нужди в областта на сигурността и оценката на уменията. Тази рамка за сертифициране следва също да гарантира, че всяка схема за сертифициране за целия ЕС е пропорционална на нивото на увереност, необходимо за използването на съответните ИКТ продукти, стоки и/или услуги, и че позволява трансгранична търговия за предприятия от всякакъв мащаб за разработване и продажба на нови продукти, както на пазара в ЕС, така и извън него.

---

13 Посредством глобални стандарти, разработени в съответствие с духа на СТО – Кодекс на добрите практики относно ТПТ.

14 Посредством европейски и глобални стандарти, разработени в съответствие с духа на СТО – Кодекс на добрите практики относно ТПТ.

21. ПРИВЕТСТВА намерението за създаване на мрежа от центрове за компетентност в сферата на киберсигурността, за да се стимулира разработването и внедряването на технологии за киберсигурност и да се даде допълнителен тласък на иновациите за промишлеността на ЕС на световната сцена при разработването на технологии от следващо поколение и на революционни технологии, като изкуствен интелект, квантови изчисления, блокова верига и сигурна цифрова идентичност;

22. ИЗТЪКВА, че е необходимо мрежата от центрове за компетентност в сферата на киберсигурността да бъде приобщаваща за всички държави членки и техните съществуващи центрове за върхови постижения и компетентности, както и да се обърне специално внимание на взаимното допълване и във връзка с това ОТБЕЛЯЗВА планирания европейски център за киберсигурност и научни изследвания, чиято ключова роля следва да бъде поставянето на акцент върху взаимното допълване и избягването на припокриване в рамките на мрежата от центрове за компетентност в сферата на киберсигурността и с други агенции на ЕС;

23. ИЗТЪКВА, че мрежата от центрове за компетентност в сферата на киберсигурността следва да разглежда спектър от въпроси от научните изследвания до промишлеността и следователно следва да допринася, наред с другото, за постигането на целта за стратегическа автономност на Европа;

24. С оглед на предложената мрежа от центрове за компетентност в сферата на киберсигурността ПОТВЪРЖДАВА ОТНОВО, че е е необходимо ЕС, чрез своите държави членки, да развива европейски капацитет за оценка на надеждността на криптирането, използвано в продуктите и услугите, предоставяни на гражданите, стопанските субекти и правителствата в рамките на цифровия единен пазар, като същевременно признава, че криптографските политики са ключов аспект от националната сигурност и че този въпрос е от компетентността на държавите членки;

25. ПРИКАНВА всички съответни заинтересовани страни да повишат инвестициите в приложения за киберсигурност на нови технологии, за да допринесат за гарантирането на кибесигурността във всички сектори на европейската икономика;

26. ИЗТЪКВА, че е важно да се предоставят услуги за киберсигурност за всички институции на ЕС по надежден и координиран начин и в условия на доверие, и ПРИЗОВАВА КОМИСИЯТА и другите институции на ЕС да продължат да развиват CERT-EU в съответствие с тези цели, както и да гарантират адекватни ресурси за това;

27. ПРИВЕТСТВА призива за признаване на важната роля на изследователите на сигурността, които са трети страни, за откриването на слабости в съществуващи продукти и услуги и ПРИЗОВАВА държавите членки да споделят добри практики за координирано разкриване на уязвимите места;

28. ИЗТЪКВА отговорността на всеки един за киберсигурността и ПРИКАНВА ЕС и неговите държави членки да утвърждават цифровите умения и медийната грамотност, които помагат на потребителите да защитават своята цифрова информация онлайн и да повишават своята осведоменост относно рисковете при публикуване на лични данни в интернет;

29. ПРИВЕТСТВА факта, че в Съвместното съобщение се поставя акцент върху образованието, кибернетичната хигиена и осведомеността в държавите членки и в ЕС;

30. ПРИЗОВАВА КОМИСИЯТА да предостави в кратки срокове оценка на въздействието и да предложи до средата на 2018 г. съответните правни инструменти за прилагане на инициативата за създаване на мрежа от центрове за компетентност в сферата на киберсигурността и на Европейски център за изследвания и компетентност в сферата на сигурността;

31. ПРИКАНВА държавите членки:

- да определят осведомеността в кибернетичната област като приоритет в информационните кампании и да утвърждават киберсигурността в академичните, общообразователните и професионалните учебни програми. Следва да се постави специален акцент върху образованието на младите хора и стимулирането на цифровите умения, за да се изградят професионалисти, подготвени за предизвикателствата в сферата на сигурността, икономиката и услугите;

- да активизират усилията си за създаване на специализирани програми на високо равнище в областта на киберсигурността с цел преодоляване на сегашния недостиг на специалисти по киберсигурност в ЕС;

- да създадат ефективна мрежа за сътрудничество на образователни звена за контакт (ЗК) под егидата на ENISA. Мрежата от ЗК следва бъде насочена към засилване на координацията и обмена на най-добри практики между държавите членки, свързани с образованието и осведомеността в сферата на киберсигурността, както и обучение, упражнения и изграждане на капацитет;

- да обмислят прилагането на правилата на директивата за МИС и в публичните администрации, които участват в ключови обществени или икономически дейности, ако вече не са обхванати от националното законодателство и бъде счетено за уместно, както и да предоставят обучение, свързано с киберсигурността, и в публичните администрации, като се има предвид ролята им в нашето общество и икономика.

Глава II

ИЗГРАЖДАНЕ НА КАПАЦИТЕТ НА ЕС ЗА ПРЕДОТВРАТЯВАНЕ, ВЪЗПИРАНЕ, УСТАНОВЯВАНЕ И РЕАГИРАНЕ НА ЗЛОНАМЕРЕНИ ДЕЙСТВИЯ В КИБЕРПРОСТРАНСТВОТО

32. ИЗТЪКВА, че един особено сериозен киберинцидент или криза може да бъде достатъчно основание държава членка да се позове на клаузата на ЕС за солидарност[15] и/или на клаузата за взаимна помощ[16];

33. ПРИВЕТСТВА приемането на рамката за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството, която допринася за предотвратяване на конфликти, за сътрудничество и стабилност в киберпространството чрез определяне на мерки в рамките на ОВППС, включително ограничителни мерки, които могат да бъдат използвани за предотвратяване и реагиране на злонамерени действия в киберпространството, и ПРИЗОВАВА ЕСВД и държавите членки редовно да използват тази рамка;

---

15 Член 222 от ДФЕС

16 Член 42, параграф 7 от ДЕС

34. ИЗТЪКВА необходимостта от ефикасен отговор на равнище ЕС на мащабни киберинциденти и кризи при зачитане на компетенциите на държавите членки, както и необходимостта да се включи киберсигурността в съществуващите механизми за управление на кризи на равнище ЕС[17]. За да се постигне това, ПРИЗОВАВА за даването на редовен отговор на равнище ЕС в случай на мащабни киберинциденти — от дипломатическо-стратегически до технически — въз основа на приложимите и при необходимост усъвършенствани рамки и процедури[18];

35. ИЗТЪКВА значението на добре интегрирания отговор и механизмите за обмен на информация между различните общности, които са от решаващо значение за гарантиране на киберсигурността в Европа, включително между съответните органи на ЕС и органите на държавите членки. Тези механизми трябва да бъдат изпитани и проверени като част от ученията в сферата на киберсигурността на равнище ЕС и при необходимост да бъдат официално регламентирани от съответни споразумения;

36. ОТБЕЛЯЗВА възможността да се разгледа, ако Комисията го представи, предложение за създаване на фонд за реагиране при извънредни ситуации, свързани с киберсигурността, наред с текущите усилия на държавите членки и при отчитане на наличните ресурси (особено в рамките на многогодишната финансова рамка на ЕС), за да се помогне на държавите членки да реагират на мащабни киберинциденти и да намаляват последиците им, при условие че преди инцидента дадената държава членка е въвела разумна система за киберсигурност, включително прилагане в пълна степен на директивата за МИС, и напълно развити рамки за управление на риска и за надзор на национално равнище;

37. ОТЧИТА растящите връзки между киберсигурността и отбраната и ПРИЗОВАВА за укрепване на сътрудничеството в областта на кибернетичната отбрана, включително чрез насърчаване на сътрудничеството между гражданските и военните общности за реагиране при инциденти и за допълнително укрепване на киберсигурността на мисиите и операциите по линия на ОПСО;

---

17 Док. C/2017/6100 final

18 Док. 9916/17 и C/2017/6100 final.

38. ИЗТЪКВА необходимостта от евентуално пълноценно използване на предложените инициативи в областта на отбраната с цел ускоряване на разработването на подходящи кибернетични способности в Европа и ОТЧИТА възможностите за евентуално разработване на проекти в областта на кибернетичната отбрана в рамките на постоянното структурирано сътрудничество (ПСС), ако участващите в ПСС държави членки сметнат за необходимо, и ОТЧИТА ролята на европейската отбранителна технологична и индустриална база и по-широката база на гражданския сектор на киберсигурността за осигуряването на средства на държавите членки за защита на техните интереси, свързани с киберсигурността и отбраната;

39. ОТБЕЛЯЗВА предложението на Комисията да се създаде платформа за обучение и образование в областта на кибернетичната отбрана до края на 2018 г. и ИЗТЪКВА, че платформата следва да разшири възможностите за образование и обучение в държавите членки и да осигури взаимно допълване с други усилия и инициативи на ЕС, по-специално с Европейския колеж по сигурност и отбрана и Европейската агенция по отбрана;

40. ПРИЗОВАВА ЕС и неговите държави членки да реагират на заплахата от основаващи се на ИКТ кражби на интелектуална собственост, включително търговски тайни или друга поверителна бизнес информация, с цел да се осигурят конкурентни предимства на фирми или търговски сектори;

41. ОТЧИТА необходимостта от справяне с престъпленията в киберпространството, включително тези в „тъмната мрежа“ (Darkweb), сексуалната експлоатация на деца онлайн, както и с измамите и фалшифицирането на непарични платежни средства, по-специално чрез осигуряване на по-пълна разузнавателна информация, провеждане на съвместни разследвания и обмен на оперативна подкрепа;

42. ПРИВЕТСТВА дейността на ЕС и неговите държави членки за справяне с предизвикателствата, породени от системите, даващи възможност на престъпниците и терористите да използват средства за комуникация, до които компетентните органи нямат достъп, ИЗТЪКВА, че при тази дейност трябва да се има предвид, че сложното и надеждно криптиране е от първостепенно значение за киберсигурността и доверието в цифровия единен пазар и за гарантиране на зачитането на правата на човека и основните свободи;

43. ПОДЧЕРТАВА, че е важно на правоприлагащите органи да се предоставят инструменти, които да им позволяват да откриват, разследват и преследват киберпрестъпността, така че престъпленията в киберпространството да не остават незабелязани и безнаказани, и ПРИВЕТСТВА приноса на Европейската съдебна мрежа по въпросите на киберпрестъпността в борбата срещу престъпността чрез сътрудничеството между съдебните органи;

44. ИЗТЪКВА колко е важно да се осигури съгласувана позиция на ЕС за ефикасно определяне на решения за европейското и световното управление на интернет в рамките на общност с участието на множество заинтересовани страни, например за осигуряване на бързо достъпна и прецизна база данни на системата WHOIS за IP адреси и имена на домейни, за да се защитават способностите за правоприлагане и обществените интереси;

45. ИЗТЪКВА, че е важно да се ускори въвеждането на интернет протокола IPv6, което е решаващо за развитието на интернет на предметите в широк мащаб, както и за подобряване на определянето на престъпленията в киберпространството;

46. НАСЪРЧАВА продължаващата работа по трансграничния достъп до електронни доказателства, по решаването на проблема със запазването на данни и по предизвикателствата за наказателното производство, пораждани от системи, даващи възможност на престъпниците и терористите да използват средства за комуникация, до които компетентните органи нямат достъп, като се има предвид необходимостта от зачитане на правата на човека и основните свободи и защита на данните;

47. ПРИЗОВАВА Комисията:

- до декември 2017 г. да представи доклад за напредъка относно изпълнението на практическите мерки за подобряване на трансграничния достъп до електронни доказателства;
- в началото на 2018 г. да представи законодателно предложение за подобряване на трансграничния достъп до електронни доказателства;

48. ПРИКАНВА Европол, ENISA и Евроюст:

- да продължат да укрепват сътрудничеството в борбата срещу киберпрестъпността помежду си и с други имащи отношение заинтересовани страни, включително общността на националните екипи за реагиране при инциденти с киберсигурността (ЕРИКС), Интерпол, частния сектор и академичните среди, като осигурят полезни взаимодействия и взаимно допълване в съответствие със съответните си правомощия и компетентности.

- да определят съвместно с държавите членки координиран подход за ответни мерки на ЕС в областта на правоприлагането при мащабни киберинциденти и кризи в допълнение към процедурите, описани в съответните рамки[19];

49. ПРИКАНВА ЕС и неговите държави членки да продължат да работят за:

- премахване на пречките пред разследването на престъпленията и ефективното наказателно правосъдие в киберпространството, както и за укрепване на международното сътрудничество и координация в борбата срещу престъпността в киберпространството;

- справяне с предизвикателствата, породени от анонимизирането на технологиите, като имат предвид, че сложното и надеждно криптиране е от първостепенно значение за киберсигурността и доверието в цифровия единен пазар;

- определяне на решения за управлението на интернет, които оказват въздействие върху способността на правоприлагащите органи за борба с престъпността в киберпространството

[19] Док. 9916/17 и C/2017/6100 final.

Глава III

УКРЕПВАНЕ НА МЕЖДУНАРОДНОТО СЪТРУДНИЧЕСТВО ЗА ОТВОРЕНО, СВОБОДНО, МИРНО И СИГУРНО ГЛОБАЛНО КИБЕРПРОСТРАНСТВО

50. ОТЧИТА, че гарантирането на киберсигурността е глобално предизвикателство, което изисква ефективно сътрудничество в световен мащаб между всички участници, и ОТЧИТА, че следва да се постави специален акцент върху подкрепата на демократичните ценности и принципите на отворено, свободно, мирно и сигурно киберпространство, и във връзка с това

51. ПРИЗОВАВА ЕС и неговите държави членки да насърчат създаването на стратегическа рамка за предотвратяване на конфликти, за сътрудничество и стабилност в киберпространството, която да се основава на прилагането на действащото международно право, и по-специално Устава на ООН в неговата цялост, разработването и въвеждането на всеобщи норми за отговорно поведение на държавите и регионални мерки за изграждане на доверие между държавите;

52. ОТЧИТА ролята на Организацията на обединените нации в по-нататъшното разработване на норми за отговорно поведение на държавите в киберпространството и припомня, че резултатите от обсъжданията на групата правителствени експерти към ООН в течение на годините са формулирали консенсусен набор от норми и препоръки[20], неколкократно одобрени от Общото събрание, които държавите следва да вземат като основа за отговорно поведение в киберпространството;

53. ОТЧИТА, че тези норми на отговорно поведение на държавите предполагат, че държавите не следва да позволяват съзнателно тяхната територия да бъде използвана за неправомерни в международен план действия, следва да отговарят на съответните искания за помощ от друга държава, чиято критична инфраструктура е обект на злонамерени действия в областта на ИКТ, произтичащи от тяхната територия, както и че държавите следва да предприемат подходящи мерки за защита на своята критична инфраструктура от заплахи в областта на ИКТ;

54. ОТЧИТА общите кибернетични заплахи и рискове, пред които са изправени ЕС, НАТО и съответните им държави членки, и ЗАЯВЯВА ОТНОВО, че е важно да продължи сътрудничеството между ЕС и НАТО в областта на киберсигурността и отбраната при пълно зачитане на принципите на приобщаване, реципрочност и автономност на ЕС при вземане на решения и в съответствие със заключенията на Съвета от 6 декември 2016 г. относно прилагането на Съвместната декларация на председателите на Европейския съвет и Европейската комисия и на генералния секретар на Организацията на Северноатлантическия договор[20];

55. ПРИЗОВАВА ЕС и неговите държави членки да подкрепят и насърчават разработването на регионални мерки за изграждане на доверие, което е основен елемент за укрепване на сътрудничеството, повишаване на прозрачността и намаляване на риска от конфликти. Въвеждането на мерки за изграждане на доверие в областта на киберсигурността в рамките на ОССЕ и други регионални структури ще увеличи предвидимостта на поведението на държавите и допълнително ще допринесе за стабилизиране на киберпространството;

56. ЗАЯВЯВА ОТНОВО, че ЕС ще продължава да подкрепя своите основни ценности за защитата на правата на човека и основните свободи, като се основава на насоките на ЕС относно правата на човека в областта на свободата в интернет. Освен това ЕС подчертава значението на участието на всички заинтересовани страни в управлението на интернет, включително академичните среди, гражданското общество и частния сектор;

57. ПРИЗОВАВА ЕС и неговите държави членки да насърчават изграждането на капацитет в киберпространството в трети държави, с отдаване на специален приоритет на съседните на ЕС и развиващите се страни, в които свързаността нараства бързо, с цел справяне с киберпрестъпността и изграждане на отбранителна способност срещу кибератаки в съответствие с основните ценности на ЕС. С цел постигане на напредък в усилията на ЕС в тази област следва да се създаде мрежа на ЕС за изграждане на киберкапацитет и да се разработят насоки на ЕС за изграждане на киберкапацитет, които да допълнят съществуващите механизми и структури;

[20] Док. 15283/16.

58. ПОДЧЕРТАВА постигнатия напредък в сътрудничеството между ЕС и НАТО в областта на кибернетичната отбрана и сигурност и неговото развитие в областта на обучението, образованието и концепциите, като същевременно се избягва ненужното дублиране на усилия при припокриване на изискванията и се насърчават оперативната съвместимост чрез изисквания относно кибернетичната отбрана, както и стандартите, и НАСТОЯВА да продължи сътрудничеството в ученията в областта на кибернетичната отбрана (на равнище персонал) и споделянето на добри практики по отношение на управлението на кризи, като същевременно се избягва ненужното дублиране на усилия при припокриване на изискванията, при пълно зачитане на политиката на ЕС за ученията и на принципите на приобщаване, реципрочност и автономност на ЕС при вземането на решения;

59. ОТЧИТА, че Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство — Конвенцията от Будапеща, предлага ефективен правен стандарт за информация на националните законодателства по въпросите на киберпрестъпността. ПРИЗОВАВА всички държави да изготвят подходяща национална правна рамка и да продължат сътрудничество си в действащата международна рамка, предлагана от Конвенцията от Будапеща;

60. ПРИПОМНЯ постиженията в провеждането на двустранни диалози на ЕС за кибернетичното пространство и призовава за по-нататъшни усилия, за да се улесни сътрудничеството с трети държави в областта на киберсигурността;

61. ПРИПОМНЯ, че ЕС разполага със солиден и правно обвързващ механизъм за контрол на износа въз основа на решенията и най-добрите практики, разработвани в рамките на международните режими за неразпространение, ОТБЕЛЯЗВА текущите обсъждания в Съвета за намиране на най-добрите начини за по-нататъшно подобряване на функционирането на този контрол и ПРИКАНВА държавите членки да продължат да разглеждат в съответните международни режими за контрол на износа (напр. Васенаарската договореност) критичните приложения в областта на киберсигурността на нови технологии, за да се осигури ефективен контрол на бъдещите критични технологии в областта на киберсигурността.

62. Като последващи действия във връзка със заключенията на Европейския съвет от 19 октомври 2017 г.[21] тези заключения ще се изпълняват посредством план за действие, който трябва да бъде приет от Съвета преди края на 2017 г. Планът за действие, като подлежащ на развитие документ, ще бъде редовно преразглеждан и актуализиран от Съвета.

---

[21] Док. EUCO 14/17.