СЪВЕТ НА ЕВРОПЕЙСКИЯ СЪЮЗ

Брюксел, 22 юли 2013 г.
(OR. en)

12109/13

POLGEN 138
JAI 612
TELECOM 194
PROCIV 88
CSC 69
CIS 14
RELEX 633
JAIEX 55
RECH 338
COMPET 554
IND 204
COTER 85
ENFOPOL 232
DROIPEN 87
CYBER 15
COPS 276
POLMIL 39
COSI 93
DATAPROTECT 94

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
До:	Делегациите
№ предх. док.:	11357/13
Относно:	Заключения на Съвета във връзка със съвместното съобщение на Комисията и на върховния представител на Европейския съюз по въпросите на външните работи и политиката на сигурност относно Стратегията на Европейския съюз за киберсигурност: Отворено, безопасно и сигурно киберпространство

Приложено се изпращат на делегациите заключенията на Съвета във връзка със съвместното съобщение на Комисията и на върховния представител на Европейския съюз по въпросите на външните работи и политиката на сигурност относно Стратегията на Европейския съюз за киберсигурност: Отворено, безопасно и сигурно киберпространство, одобрени от Съвета по общи въпроси на 25 юни 2013 г.

ПРИЛОЖЕНИЕ

Заключения на Съвета във връзка със съвместното съобщение на Комисията и на върховния представител на Европейския съюз по въпросите на външните работи и политиката на сигурност
относно Стратегията на Европейския съюз за киберсигурност: Отворено, безопасно и сигурно киберпространство

Съветът на Европейския съюз,

1. КАТО ОТЧИТА, че киберпространството, което само по себе си има транснационален характер, се състои от взаимозависими мрежи и информационни инфраструктури, включително, наред с другото, интернет и телекомуникационните мрежи, представлява един от най-важните настоящи и бъдещи канали за осъществяване на потребностите, интересите и правата на гражданите и държавите членки на ЕС и носи незаменими ползи за икономическия растеж в ЕС,

2. КАТО ПОДЧЕРТАВА ролята и правата на отделните граждани, частния сектор и гражданското общество по въпросите на киберпространството и важната роля на ЕС в подкрепа и за запазване на отворено, безопасно и сигурно киберпространство на базата на основните ценности на ЕС, като демокрация, права на човека и върховенство на закона, за нашите икономики, администрации и общества, както и за безпрепятственото функциониране на вътрешния пазар,

3. КАТО ОТЧИТА необходимостта от подобряване на поверителността, наличността и целостта на мрежите и инфраструктурата, както и на съдържащата се в тях информация,

4. КАТО ПРИЗНАВА, че трябва да се въведат гаранции и да се вземат мерки за предотвратяване на заплахите, свързани с или нанасящи вреда на взаимозависимите мрежи и информационни инфраструктури, и за защита на киберпространството както в гражданската, така и във военната област,

5. КАТО ПОТВЪРЖДАВА ОТНОВО позицията на ЕС, че същите норми, принципи и ценности, към които ЕС се придържа в останалите области на живота, по-специално Хартата на основните права на Европейския съюз, следва да се прилагат и в киберпространството,

6. КАТО ОТЧИТА, че международното право, включително международните конвенции като Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство (Конвенция от Будапеща) и съответните конвенции в областта на международното хуманитарно право и правата на човека, като Международния пакт за граждански и политически права и Международния пакт за икономически, социални и културни права, предоставя правната рамка, приложима за киберпространството. Във връзка с това следва да се положат усилия тези правни инструменти да се спазват и в киберпространството; следователно ЕС не призовава за създаването на нови международни правни инструменти по въпросите на киберпространството,

7. КАТО ПОТВЪРЖДАВА, че към киберсигурността трябва да се прилага интегриран, мултидисциплинарен и хоризонтален подход, както и че предприеманите мерки следва да обхващат разнообразни въпроси, засягащи киберпространството,

8. КАТО ПРИПОМНЯ многобройните инициативи на ЕС и международни инициативи в областта на киберсигурността, в т.ч. посочените в приложението към настоящия документ,

9. КАТО ПРИПОМНЯ разпоредбите на член 222 от Договора за функционирането на Европейския съюз и взема под внимание продължаващите обсъждания по неговото прилагане,

10. КАТО СЪЗНАВА, че усилията за повишаване на киберсигурността трябва да се полагат не само в рамките на Европейския съюз, но и в трети държави, в т.ч. онези държави, от които действат организациите — извършители на киберпрестъпления, като същото важи и за борбата с киберпрестъпността,

С НАСТОЯЩОТО

11. ПРИВЕТСТВА съвместното съобщение на Комисията и на върховния представител на Европейския съюз относно Стратегията на Европейския съюз за киберсигурност.

12. СЧИТА за съществено важно и спешно да се доразработи и прилага цялостен подход към политиката на ЕС за киберпространството, който:

- да защитава и насърчава спазването на правата на човека и да се базира на основните ценности на ЕС за демокрация, права на човека и върховенство на закона;

- да води до повишаване на благоденствието в Европа и на социалните и икономическите ползи от киберпространството, включително интернет;

- да насърчава ефективната и повишена киберсигурност на територията на ЕС и извън него;

- да води до напредък в усилията за преодоляване на цифровото разделение в световен план и да насърчава международното сътрудничество в областта на киберсигурността;

- да отразява ролята и правата на отделните граждани, частния сектор и гражданското общество по въпросите на киберпространството, в т.ч. засилване на публично-частното сътрудничество и обмен на информация,

И

13. ПРИКАНВА държавите членки, Комисията и върховния представител да работят съвместно, като зачитат съответните си области на компетентност и принципа на субсидиарност, за изпълнение на стратегическите цели, поставени в настоящите заключения.

Ценности

14. ПОДЧЕРТАВА, че човешките права на гражданите, включително свободата на изразяване и на неприкосновеност на личния живот трябва да се спазват винаги, когато се разработват политики и практики по въпросите на киберпространството, както и в законодателството, и отбелязва водените преговори за съгласуване на правна рамка на ЕС относно защитата на личните данни, която да може да действа ефективно в киберпространството.

15. ОТЧИТА, че ценностите и интересите, които се утвърждават и защитават в рамките на Съюза, следва да се насърчават и в неговите външни политики по въпросите на киберпространството.

16. ПРИЗОВАВА ЕС и неговите държави членки:

- да защитават единна и силна позиция по отношение на всеобщата приложимост на правата на човека и основните свободи, включително свободата на мнение, на изразяване, на информация, на събрания и сдружения в киберпространството;

- да установят начините за прилагане в киберпространството на сега действащите задължения.

17. ПРИКАНВА ЕС и неговите държави членки да поощряват цифровата грамотност и да съдействат на потребителите да повишават осведомеността си по отношение на индивидуалната си отговорност, когато публикуват лични данни в интернет.

18. ПОДЧЕРТАВА важната роля на ЕС за поддържане на модел с участието на множество заинтересовани страни при управлението на интернет.

19. ПРИКАНВА държавите членки да предприемат необходимите разумни мерки с цел да се гарантира, че всички европейски граждани имат достъп до интернет и са в състояние да се възползват от неговите предимства.

Благоденствие

20. ПРИКАНВА Комисията да положи конкретни усилия за насърчаване на цифровия единен пазар и да осъществи напредък по въпросите в тази област в рамките на Съюза и на международни форуми (например Световната търговска организация (СТО) и преговорите по Споразумението за информационните технологии), както и да гарантира пазарен достъп в тези сектори при договарянето на споразумения за зони за свободна търговия с трети държави.

21. ПОДЧЕРТАВА, че е важно законодателството в този сектор да е неутрално от гледна точка на технологиите и насърчава във възможно най-голяма степен неутралния характер на мрежата, за да не се нарушава конкуренцията посредством дискриминиране на трансграничната онлайн търговия и новите бизнес модели.

22. ПРИВЕТСТВА факта, че се признава необходимостта от инвестиции в научноизследователска и развойна дейност в областта на киберпространството като важна сфера, която би могла да осигури висококачествени работни места и икономически растеж.

23. ПОДЧЕРТАВА:

- решаващото значение на жизнеспособен сектор на ЕС на информационните и комуникационните технологии (ИКТ) и на сигурността на ИКТ за целите на укрепването на киберсигурността и ПРИКАНВА държавите членки и Комисията да проучат възможните мерки в подкрепа на неговото развитие, както и да докладват по този въпрос;

- че законодателството в подкрепа на киберсигурността следва да стимулира иновациите и растежа и да бъде насочено към защита на инфраструктурата и жизненоважните функции, които държавите членки считат за критични;

- че цифровата икономика е основен двигател на растежа, иновациите и заетостта, както и че киберсигурността е от ключово значение за защита на цифровата икономика;

- значението на национално равнище на защитата на критичната информационна инфраструктура.

Постигане на устойчивост на киберпространството

24. ПРИВЕТСТВА целите в предложението на Комисията за директива, с която се определят мерки за засилване на:

    - мрежовата и информационната сигурност на територията на ЕС;

    - готовността и капацитета в областта на киберсигурността на национално равнище;

    - сътрудничеството между държавите членки и в рамките на ЕС, както и за поощряване на култура на управление на риска в публичния и частния сектор.

25. ПРИЗОВАВА всички институции, органи и агенции на ЕС, в сътрудничество с държавите членки, да предприемат необходимите действия за гарантиране на собствената си киберсигурност, като повишат сигурността си съобразно подходящите стандарти за сигурност в сътрудничество с ENISA за постигане на най-добри практики, в съответствие с Регламент (ЕС) № 526/2013[1].

26. ПРИПОМНЯ, че след едногодишна пилотна фаза и успешна оценка на неговата роля и ефективност беше създаден екип за незабавно реагиране при компютърни инциденти (CERT) за институциите, органите и агенциите на ЕС.

27. ПОДЧЕРТАВА първостепенното значение на ENISA в подкрепа на усилията на държавите членки и на Съюза за постигане на високо равнище на мрежова и информационна сигурност, по-специално чрез съдействие за изграждането на капацитет в държавите членки, и разработване на силен национален капацитет за поддържане на устойчивостта на киберпространството, европейски учения в областта на кибернетичната отбрана, както и усилията на Съюза в областта на научноизследователската и развойна дейност и стандартизацията, и ПРИКАНВА ENISA да си сътрудничи с други институции, органи и агенции на Съюза по въпросите, свързани с мрежовата и информационна сигурност, в съответствие с Регламент (ЕС) № 526/2013.

---

[1] ОВ L 165, 18.6.2013 г.

28. ИЗТЪКВА необходимостта в целия ЕС да се повиши устойчивостта на критичните инфраструктури и да се засили тясното сътрудничество и координация между заинтересованите участници, както и между гражданските и военните участници от ЕС, включително между публичния и частния сектор, при реагирането на инциденти и предизвикателства, свързани с киберсигурността, чрез инициативи като разработване на общи стандарти, повишаване на осведомеността, образование и обучение, текущ преглед и изпитване (или разработване) на механизми за ранно предупреждение и реагиране. За ефективното преодоляване на предизвикателствата, свързани с киберсигурността, включително управлението на инциденти, е необходимо също да се засили тясното сътрудничество и координация при реагирането на инциденти в киберпространството от страна на органите за отбрана, правоприлагане, киберсигурност и частния сектор,

29. ПРИКАНВА държавите членки

- да предприемат мерки, за да гарантират достигането на ефикасно национално равнище на киберсигурност, като разработват и прилагат подходящи политики, организационни и оперативни способности за защита на информационните системи в кибернетичното пространство, по-специално на тези, за които се приема, че са с критично значение,

- да установяват контакти с представители на промишлеността и академичните среди, за да се насърчава доверието като ключов елемент на националната киберсигурност, например чрез създаването на публично-частни партньорства,

- да подпомагат повишаването на осведомеността на всички равнища относно естеството на заплахите и основните положения от добрите цифрови практики,

- да подпомагат собствениците и доставчиците на ИКТ системи в защитата на собствените им системи и жизненоважните услуги, които те предоставят,

- да насърчават общоевропейското сътрудничество по въпросите на киберсигурността, по-специално като усъвършенстват общоевропейските учения по въпросите на киберсигурността,

- да гарантират ефективното сътрудничество и координация между държавите членки на равнище ЕС към обща оценка на заплахите,

- да укрепят и разширят сътрудничеството между държавите членки и потребителите от ЕС въз основа на съществуващите структури,

- да вземат предвид проблемите на киберсигурността в светлината на продължаващата работа по клаузата за солидарност.

Киберпрестъпност

30. ОТЧИТА Заключенията на Съвета по правосъдие и вътрешни работи от 6—7 юни 2013 г. за определяне на приоритетите на ЕС в борбата срещу тежката и организираната престъпност за периода 2014—2017 г., в които борбата с киберпрестъпността се посочва сред приоритетите,

31. ПОДЧЕРТАВА, че в Оценката на Европол на заплахата от тежка и организирана престъпност за 2013 г. киберпрестъпността се разглежда като престъпна област с нарастваща заплаха за ЕС под формата на широкомащабно нарушаване на сигурността на данните, онлайн измами и сексуална експлоатация на деца, като същевременно киберпрестъпността с цел натрупване на печалби се превръща във фактор за други престъпни дейности,

32. ПРИВЕТСТВА създаването на Европейския център по киберпрестъпност (EC3) към Европол и ПРИКАНВА държавите членки да използват EC3 в рамките на неговия мандат като средство за укрепване на сътрудничеството между националните агенции,

33. ПРИКАНВА Европол и Евроюст, в съответствие с мандата и компетентността си, да продължават да укрепват сътрудничеството си с всички заинтересовани страни, включително агенции на ЕС, Интерпол, общността на групите за бързо реагиране по въпросите на информационната сигурност (CERT) и частния сектор, в борбата с киберпрестъпността, включително чрез изтъкване на полезните взаимодействия и взаимното допълване,

34. ОЧАКВА своевременното ратифициране от всички държави членки на Конвенцията от Будапеща за престъпления в кибернетичното пространство,

35. ПРИЗОВАВА Комисията, Европол, CEPOL и ENISA да подпомагат обучението и повишаването на уменията в държавите членки, чиито правителства и правоприлагащи органи изпитват необходимост от изграждането на капацитет за борба с киберпрестъпността,

36. ПРИКАНВА Комисията:

- да подпомага държавите членки, по тяхно искане, при установяването на пропуски и укрепването на капацитета им за разследване на киберпрестъпността и борба с нея,

- да използва фонд „Вътрешна сигурност“, в рамките на осигурения бюджет (и при отчитане на останалите му приоритети), за да подпомага борбата на съответните органи с киберпрестъпността,

- да използва Инструмента за стабилност, за да разгърне борбата с киберпрестъпността, както и инициативи за изграждане на капацитет, в т.ч. полицейско и съдебно сътрудничество, в трети държави, от които действат организациите — извършители на киберпрестъпления,

- да улеснява координацията на програми за изграждане на капацитет, за да се избегне дублирането и да се осигурят полезни взаимодействия,

- да осигури информация относно напредъка във връзка с Глобалния алианс срещу сексуалното посегателство над деца в интернет,

- да продължи да улеснява наблюдението на политиката на ЕС, свързана с борбата с киберпрестъпността, по-специално предвид резултатите и стратегическата информация, предоставена от Европол (ЕС3),

- да продължи да улеснява сътрудничеството между отделните общности, по-специално като подпомага Европол (ЕС3).

Обща политика за сигурност и отбрана (ОПСО)

37. В рамките на ОПСО ИЗТЪКВА:

- спешната необходимост от изпълнение и постигане на напредък по свързаните с ОПСО аспекти за кибернетична отбрана на стратегията, за да се разработи рамка за кибернетична отбрана по целесъобразност, и от установяване на конкретни стъпки в това отношение, предвид също така подготвяния за декември 2013 г. дебат в Европейския съвет по въпросите на сигурността и отбраната. В ЕСВД следва да се определи единна точка за контакт, за да се направляват тези усилия,

- необходимостта от повишаване на капацитета на държавите членки за кибернетична отбрана, включително чрез разработването на общи стандарти, и повишаване на осведомеността чрез обучение и образование по въпросите на киберсигурността, посредством Европейския колеж по сигурност и отбрана, и допълнително усъвършенстване на възможностите за обучение и учения за държавите членки,

- изграждането по най-ефективен начин на необходимия капацитет на държавите членки за кибернетична отбрана, като се използват съществуващите механизми за обединяване и споделяне и полезните взаимодействия с по-широк кръг от политики на ЕС,

- необходимостта от научноизследователска и развойна дейност. Отдава се приоритет на насърчаването на държавите членки да разработват сигурни и устойчиви технологии за кибернетична отбрана при изявено участие на частния сектор и академичните среди, и на засилването на свързаните с киберсигурността аспекти на научноизследователските проекти на EDA въз основа на подход на сътрудничество и като добър пример за капацитет с двойна употреба, който ще се координира между EDA и Комисията съгласно европейската рамка за сътрудничество,

- че механизмите за ранно предупреждение и реагиране следва да се преразгледат и изпитат предвид новите заплахи за киберсигурността чрез диалог между ЕСВД, ENISA, EC3, EDA, Комисията и държавите членки, с цел да се постигнат полезни взаимодействия и да се установят връзки с отбранителната общност,

- необходимостта от провеждане и засилване на сътрудничеството между ЕС и НАТО в областта на кибернетичната отбрана, като се установят приоритети за непрекъснато сътрудничество между ЕС и НАТО в областта на кибернетичната отбрана при съществуващата рамка, включително участие на реципрочна основа в ученията и обучението в областта на кибернетичната отбрана,

- интегрирането на свързани с кибернетичната отбрана аспекти в цялостната политика за кибернетичното пространство.

Промишленост/Технологии

38. Като ОТЧИТА необходимостта Европа допълнително да развие промишлените и технологичните си ресурси, за да постигне подходящо равнище на диверсификация и доверие в мрежите и ИКТ системите, Съветът ИЗРАЗЯВА дълбоко задоволство от призива в Стратегията на ЕС за киберсигурност за Европа да се подпомага една силна промишлена политика, за да се насърчи надежден европейски сектор на ИКТ и в областта на киберсигурността и да се стимулира развитието на вътрешния пазар чрез научноизследователска и развойна дейност,

39. ПРИКАНВА държавите членки, Комисията и ENISA да активизират усилията за научноизследователска и развойна дейност в областта на ИКТ и киберсигурността, както и да повишат наличието на добре подготвени специалисти в тази сфера, което е от решаващо значение за стимулирането на конкурентоспособността на европейския сектор в областта на информационните и комуникационните технологии (ИКТ), услугите и сигурността и неговата способност да разработва надеждни и сигурни решения, поради което Съветът насърчава Комисията да използва рамковата програма за научни изследвания и иновации „Хоризонт 2020“,

40. ИЗТЪКВА факта, че развитието на публично-частни партньорства ще бъде инструмент от значение за повишаването на капацитета в областта на киберсигурността; и затова ПРИЗОВАВА Комисията да стимулира в рамките на „Хоризонт 2020“ полезните взаимодействия между операторите на критични инфраструктури, научните изследвания в областта на ИКТ и сигурността по въпроси на киберсигурността и киберпрестъпността и политиките на Съюза за вътрешна и външна сигурност,

41. ПРИЗОВАВА държавите членки и Комисията да предприемат конкретни мерки в подкрепа на киберсигурността на малките и средните предприятия, които са особено уязвими на заплахи в кибернетичното пространство, и насърчава държавите членки да разработят сигурни и устойчиви технологии за киберсигурност с участието и съдействието на частния сектор и академичните среди,

42. ПРИКАНВА Комисията да вземе под внимание съществуващите стандарти в областта на киберсигурността и ПОДЧЕРТАВА, че сътрудничеството и обменът на информация по отношение на стандартите — напр. за управление на риска — следва допълнително да се развият съвместно с държавите членки, промишлеността и други имащи отношение участници,

Международно сътрудничество по въпросите на кибернетичното пространство

43. ИЗТЪКВА отново ангажимента на ЕС да подпомага разработването на мерки за изграждане на доверие по въпросите на киберсигурността, повишаването на прозрачността и намаляването на риска от погрешно възприемане на поведението на дадена държава, като насърчава установяването на международни норми в тази област,

44. ПРИЗОВАВА Комисията и върховния представител, съгласно съответните процедури в Договорите:

- а) да утвърждават Конвенцията от Будапеща като модел за изготвянето на национално законодателство по въпросите на киберпрестъпността и като основа за международното сътрудничество в тази област, б) да насърчават зачитането на основните права в кибернетичното пространство и в) да използват пълноценно всички съществуващи средства за международно сътрудничество с цел разгръщане на борбата с киберпрестъпността, както и свързано полицейско и съдебно сътрудничество в трети държави, от които действат организациите — извършители на киберпрестъпления,

- да търсят експертния и практическия опит на държавите членки в политиката за кибернетичното пространство, извлечен от двустранен диалог/сътрудничество, за да разработят общи послания на ЕС по въпросите на киберсигурността, и да работят в тясна връзка с държавите членки по оперативните аспекти,

- в сътрудничество с държавите членки и съответните частни организации и представители на гражданското общество да използват пълноценно съответните инструменти на ЕС за оказване на помощ за изграждането на ИКТ капацитет, включително киберсигурност,

45. ПРИЗОВАВА държавите членки, Комисията и върховния представител да работят за постигането на съгласувана на равнище ЕС международна политика за кибернетичното пространство съгласно съответните процедури в Договорите, като:

- засилят диалога с ключови международни партньори и организации по начин, който гарантира, че всички държави членки имат възможност да използват пълноценно това сътрудничество,

- включат въпросите на кибернетичното пространство в ОВППС,

- подобрят координацията по световни въпроси на кибернетичното пространство и интегрират киберсигурността, включително мерките за изграждане на доверие и прозрачност, в цялостната рамка за развитие на отношенията с трети държави и международни организации, в т.ч. чрез засилена координация между държавите членки, Комисията и ЕСВД на провеждането на диалог и други дейности по въпросите на киберсигурността,

- подобрят координацията между съответните подготвителни органи на Съвета (включително групата „Приятели на председателството по въпросите на киберпространството“),

- подпомагат изграждането на капацитет в трети държави чрез обучение и помощ за създаването на съответни национални политики, стратегии и институции, за да се даде възможност за пълно разгръщане на икономическия и социалния потенциал на ИКТ, като подпомагат разработването на устойчиви системи в тези държави и като ограничават рисковете за институциите на ЕС и държавите членки в кибернетичното пространство, като същевременно използват съществуващите мрежи и форуми за координация на политиката и обмен на информация,

Съответни роли и отговорности

46. ПРИЗОВАВА останалите заинтересовани участници — частния сектор, техническите и академичните общности, гражданското общество и отделни граждани, да поемат съответните роли и отговорности към едно отворено, свободно и сигурно кибернетично пространство,

47. ПРИЗОВАВА Комисията и върховния представител европейските дейности да бъдат разработени по начин, който е съвместим с националните структури, конституционното право и инициативите в областта на киберсигурността, за да се гарантира интегриран подход и избягване на дублирането,

И

48. ПРИЗОВАВА Комисията и върховния представител да изготвят доклад за напредъка по стратегията за киберсигурност, който да бъде представен на конференцията на високо равнище през февруари 2014 г.; и ПРЕДЛАГА компетентните подготвителни органи на Съвета да провеждат редовни заседания (по-специално групата „Приятели на председателството по въпросите на киберпространството“), за да съдействат за определянето на приоритети и стратегически цели на ЕС за кибернетичното пространство като част от цялостната политическа рамка, и да преразглеждат и подпомагат текущото изпълнение на стратегията,

49. При изпълнението на настоящите заключения на Съвета ще се използват единствено съществуващите фондове и финансови програми, без да се засягат преговорите по бъдещата финансова рамка, и затова Съветът ПРИКАНВА Комисията да представи финансирането на стратегията, като вземе под внимание предстоящите преговори с Европейския парламент.

ПРИЛОЖЕНИЕ КЪМ ПРИЛОЖЕНИЕТО

Документи за справка

1. Европейски парламент, Съвет и Комисия

   – Харта на основните права на Европейския съюз[2],

2. Европейски парламент и Съвет

   – Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 година относно създаване на Европейската агенция за мрежова и информационна сигурност[3],

   – Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 г. относно общата регулаторна рамка за електронните съобщителни мрежи и услуги (Рамкова директива), изменена с Директива 2009/140/ЕО[4],

3. Европейски парламент

   – Резолюция на Европейския парламент от 11 декември 2012 г. относно Стратегия за цифрова свобода в рамките на външната политика на ЕС,

   – Доклад на Европейския парламент от 2012 г. относно кибернетична сигурност и отбрана,

4. Съвет

   – Стокхолмска програма — Отворена и сигурна Европа в услуга и за защита на гражданите[5],

   – Сигурна Европа в един по-добър свят — европейска стратегия за сигурност, 12 декември 2003 г.[6],

---

2 ОВ C 364/1, 18.12.2010 г.
3 ОВ L 077, 13.3.2004 г.
4 ОВ L 108, 24.4.2002 г. и ОВ L 337/37, 18.12.2009 г.
5 Док. 17024/09 CO EUR PREP 3 JAI 896 POLGEN 229.
6 Док. 15849/03 PESC 783.

– Стратегия за вътрешна сигурност за Европейския съюз: „Към европейски модел за сигурност“[7],

– Директива 2008/114/ЕО на Съвета от 8 декември 2008 година относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита[8],

– Заключения на Съвета относно съобщението на Комисията за стратегията за вътрешна сигурност на Европейския съюз в действие[9],

– Заключения на Съвета във връзка със съобщението на Комисията относно защитата на критичната информационна инфраструктура „Постижения и предстоящи стъпки за постигане на сигурност в световното кибернетично пространство“[10],

– Заключения на Съвета за определяне на приоритетите на ЕС в борбата срещу тежката и организираната престъпност за периода 2014—2017 г.[11],

– Заключения на Съвета относно създаването на Европейски център по киберпрестъпност[12],

---

7 Док. 5842/2/10 JAI 90.

8 ОВ L 345, 23.12.2008 г.

9 Док. 6699/11 JAI 124.

10 Док. 10299/11 TELECOM 71 DATAPROTECT 55 JAI 332 PROCIV 66. Това съобщение представлява последващо действие във връзка със съобщението на Комисията относно защитата на критичната информационна инфраструктура „Защита на Европа от широкомащабни кибернетични атаки и смущения: повишаване на готовността, сигурността и устойчивостта“ (док. 8375/09).

11 Док. 9849/13 JAI 407 COSI 62 ENFOPOL 151 CRIMORG 77 ENFOCUSTOM 89 PESC 569 RELEX 434.

12 Док. 10603/12 ENFOPOL 154 TELECOM 116.

– Предложение за директива на Европейския парламент и на Съвета относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета. Одобряване на окончателния компромисен текст с цел постигане на съгласие с Европейския парламент на първо четене[13],

– Заключения на Съвета относно европейската стратегия за по-добър интернет за децата[14],

– Заключения на Съвета относно борбата със сексуалната експлоатация на деца и детската порнография в интернет — повишаване на ефективността на полицейската дейност в държавите членки и трети държави[15],

– Заключения на Съвета относно глобален алианс срещу сексуалното посегателство над деца в интернет[16],

– Заключения на Съвета относно съгласувана работна стратегия и практически мерки в борбата с киберпрестъпността[17] и Заключения на Съвета относно план за действие за изпълнение на съгласуваната стратегия за борба с киберпрестъпността[18],

– Частичен общ подход на Съвета относно предложението на Комисията за регламент за установяване на „Хоризонт 2020“ — рамкова програма за научни изследвания и иновации (2014-2020 г.)[19],

– Съвместно действие на Съвета за създаване на Европейска агенция по отбрана[20],

---

13 Док. 11399/12 DROIPEN 79 TELECOM 126 CODEC 1673.

14 Док. 15850/12 AUDIO 111 JEUN 95 EDUC 330 TELECOM 203 CONSOM 136 JAI 766 GENVAL 81.

15 Док. 15783/2/11 REV 2 GENVAL 108 ENFOPOL 368 DROPIEN 119 AUDIO 53.

16 Док. 10607/12 +COR 1 GENVAL 39 ENFOPOL 155 DROIPEN 69 AUDIO 62 JEUN 46.

17 Док. 15569/08 ENFOPOL 224 CRIMORG 190.

18 Док. 5957/2/10 REV 2 CRIMORG 22 ENFOPOL 32.

19 Док. 10663/12 RECH 207 COMPET 364 IND 102 MI 398 EDUC 152 TELECOM 118 ENER 233 ENV 446 REGIO 75 AGRI 362 TRANS 187 SAN 134 CODEC 1511.

20 Док. 10556/04 COSDP 374 POLARM 17 IND 80 RECH 130 ECO 121.

– Съвместно предложение за решение на Съвета относно договореностите за прилагане от страна на Съюза на клаузата за солидарност[21],

– Заключения на Съвета относно медийната грамотност в цифрова среда[22],

– Права на човека и демокрация: Стратегическа рамка и план за действие на ЕС[23],

– Доклад относно изпълнението на Европейската стратегия за сигурност[24],

5. Комисия

– Програма в областта на цифровите технологии за Европа[25], която е една от седемте водещи инициативи на стратегията за интелигентен, устойчив и приобщаващ растеж „Европа 2020“[26], и Програма в областта на цифровите технологии за Европа: цифровите технологии — двигател на европейския икономически растеж[27], която пренасочва Програмата в областта на цифровите технологии,

– Съобщение относно защитата на правото на личен живот във взаимосвързания свят, Европейска рамка за защита на данните за 21-ви век[28],

– Съобщение „Борба с престъпността в дигиталната ера: създаване на Европейски център по киберпрестъпност“[29],

---

21 Док. 18124/12 CAB 39 POLGEN 220 CCA 13 JAI 946 COSI 134 PROCIV 225 ENFOPOL 430 COPS 485 COSDP 1123 PESC 1584 COTER 125 COCON 45 COHAFA 165.

22 Док. 15441/09 AUDIO 47 EDUC 173 TELECOM 233 RECH 380.

23 Док. 11855/12 COHOM 163 PESC 822 COSDP 546 FREMP 100 INF 110 JAI 476 RELEX 603.

24 Док. 17104/08 CAB 66 PESC 1687 POLGEN 139.

25 Док. 9981/1/10 TELECOM 52 AUDIO 17 COMPET 165 RECH 193 MI 168 DATA PROTECT 141.

26 Док. 7110/10 CO EUR-PREP 7 POLGEN 28 AG 3 ECOFIN 136 UEM 55 SOC 174 COMPET 82 RECH 83 ENER 63 TRANS 55 MI 73 IND 33 EDUC 40 ENV 135 AGRI 74.

27 Док. 17963/12 TELECOM 262 MI 839 COMPET 786 CONSOM 161 DATAPROTECT 149 RECH 472 AUDIO 137 POLGEN 216.

28 Док. 5852/12 DATAPROTECT 8 JAI 43 MI 57 DRS 10 DAPIX 11 FREMP 6.

29 Док. 8543/12 ENFOPOL 94 TELECOM 72.

– Съобщение на Комисията „Оползотворяване на потенциала на изчисленията в облак в Европа“[30],

– Съобщение на Комисията относно защитата на критичната информационна инфраструктура — „Постижения и предстоящи стъпки за постигане на сигурност в световното кибернетично пространство“[31],

– Съобщение на Комисията относно защитата на критичната информационна инфраструктура „Защита на Европа от широкомащабни кибернетични атаки и смущения: повишаване на готовността, сигурността и устойчивостта“[32],

6. ООН

– Резолюция A/RES 57/239 на Общото събрание на ООН за създаването на световна култура за киберсигурност,

– Резолюция A/HRC/20/L.13 на Съвета на ООН по правата на човека от 29 юни 2012 г. относно утвърждаването, защитата и използването на правата на човека в интернет,

– Резолюция A/RES 67/27 на Общото събрание на ООН относно развитието в областта на информацията и далекосъобщенията в контекста на международната сигурност,

– Създаване на отворена междуправителствена експертна група по въпросите на киберпрестъпността със СНПООН съгласно Резолюция 65/230 на Общото събрание на ООН,

7. Съвет на Европа

– Конвенция на Съвета на Европа от 28 януари 1981 г. за защита на лицата при автоматизираната обработка на лични данни,

– Конвенция на Съвета на Европа от 23 ноември 2001 г. за престъпленията в кибернетичното пространство,

---

30 Док. 14411/12 TELECOM 170 MI 586 DATAPROTECT 112 COMPET 585.

31 Док. 8548/11 TELECOM 40 DATAPROTECT 27 JAI 213 PROCIV 38.

32 Док. 8375/09 TELECOM 69 DATAPROTECT 24 JAI 192 PROCIV 46.

8. Организация за сигурност и сътрудничество в Европа (ОССЕ)

– Решение № 1039 на Постоянния съвет, 26 април 2012 г.: Разработване на мерки за изграждане на доверие, за да се намалят рисковете от конфликт поради използването на информационни и комуникационни технологии,

– Решение № 4/12 на министрите, 7 декември 2012 г.: Усилията на ОССЕ за преодоляване на транснационалните заплахи,

– Отворена неофициална работна група на ОССЕ за изработването на набор от проектомерки за изграждане на доверие, за да се повиши междудържавното сътрудничество, прозрачността, предвидимостта и стабилността и да се намалят рисковете от погрешно възприемане, ескалация на напрежението и конфликт поради използването на ИКТ (Решение № 1039 на Постоянния съвет на ОССЕ, 26 април 2012 г.),

9. Конференции, инициативи и прояви

– Международна конференция по въпросите на кибернетичното пространство, проведена в Лондон на 1—2 ноември 2011 г. и последвана от Международна конференция по въпросите на кибернетичното пространство в Будапеща на 4—5 октомври 2012 г.,

– Съвместно симулационно учение с участието на ЕС и САЩ „Cyber Atlantic 2011“ и общоевропейски учения за действия при инциденти в кибернетичното пространство с участието на всички държави членки („Cyber Europe 2010“ и „Cyber Europe 2012“),

– Група *ad hoc* по ядрена сигурност, която разгледа и обсъди въпроса за компютърната сигурност/киберсигурността в окончателния си доклад[33],

[33] Док. 10616/12 AHGS 20 ATO 84.

10. Други

– Оценка на Европол на заплахата от тежка и организирана престъпност за 2013 г. (SOCTA)[34],

– Политика за сигурност по отношение на осигуреността на информацията[35] и насоки[36] относно защитата на мрежите.

---

[34] Док. 7368/13 JAI 200 COSI 26 ENFOPOL 75 CRIMORG 41 CORDROGUE 27 ENFOCUSTOM 43 PESC 286 JAIEX 20 RELEX 211.

[35] Док. 8408/12 CSCI 11 CSC 20.

[36] Док. 10578/12 CSCI 20 CSC 34.