ЕВРОПЕЙСКИ ПАРЛАМЕНТ 2009 - 2014

Документ за разглеждане в заседание

A7-0335/2012

17.10.2012

ДОКЛАД

относно кибернетична сигурност и отбрана
(2012/2096(INI))

Комисия по външни работи

Докладчик: Tunne Kelam

PR_INI

СЪДЪРЖАНИЕ

Страница

ПРЕДЛОЖЕНИЕ ЗА РЕЗОЛЮЦИЯ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ

относно кибернетична сигурност и отбрана

(2012/2096(INI))

Европейският парламент,

– като взе предвид доклада относно изпълнението на Европейската стратегия за сигурност, приет от Европейския съвет на 11 и 12 декември 2008 г.,

– като взе предвид Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство, приета в Будапеща на 23 ноември 2004 г.,

– като взе предвид заключенията на Съвета относно защитата на критичната информационна инфраструктура от 27 май 2011 г. и предходните заключения на Съвета относно кибернетичната сигурност,

– като взе предвид съобщението на Комисията „Програма в областта на цифровите технологии за Европа („Digital Agenda for Europe“)“ от 19 май 2012 г. (COM(2010)0245),

– като взе предвид Директива 2008/114/ЕО на Съвета от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита[1],

– като взе предвид неотдавнашното съобщение на Комисията относно създаването на Европейски център по киберпрестъпност като приоритет на стратегията за вътрешна сигурност (COM(2012)0140),

– като взе предвид своята резолюция от 10 март 2010 г., озаглавена „Прилагането на Европейската стратегия за сигурност и на Общата политика за сигурност и отбрана“[2],

– като взе предвид своята резолюция от 11 май 2011 г. относно развитието на общата политика за сигурност и отбрана след влизането в сила на Договора от Лисабон[3],

– като взе предвид резолюцията си от 22 май 2012 г. относно стратегията за вътрешна сигурност на Европейския съюз[4],

– като взе предвид своята резолюция от 27 септември 2011 г. относно предложението за регламент на Европейския парламент и на Съвета за изменение на Регламент (ЕО) № 1334/2000 за въвеждане на режим на Общността за контрол на износа на

[1] ОВ L 345, 23.12.2008 г., стр. 75.
[2] Приети текстове, P7_TA(2010)0061.
[3] Приети текстове, P7_TA(2011)0228.
[4] Приети текстове, P7_TA(2012)0207.

стоки и технологии с двойна употреба[5],

– като взе предвид своята резолюция от 12 юни 2012 г. относно защитата на критичната информационна инфраструктура – постижения и предстоящи стъпки: за постигане на сигурност в световното кибернетично пространство[6],

– като взе предвид резолюцията на Съвета на ООН по правата на човека от 5 юли 2012 г., озаглавена „Насърчаване, защита и упражняване на правата на човека в интернет“[7], която признава значението на защитата на правата на човека и свободното движение на информация онлайн,

– като взе предвид заключенията на срещата на върха в Чикаго от 20 май 2012 г.,

– като взе предвид дял V от Договора за ЕС,

– като взе предвид член 48 от своя правилник,

– като взе предвид доклада на комисията по външни работи (A7-0335/2012),

А. като има предвид, че в днешния глобализиран свят за ЕС и държавите членки е от съществено значение да могат да разчитат на сигурно киберпространство и безопасна употреба на информационните и цифровите технологии и на устойчиви и надеждни информационни услуги и свързаните с тях инфраструктури;

Б. като има предвид, че информационните и комуникационните технологии се използват и като инструменти за репресия; като има предвид, че контекстът, в който се използват те, определя до голяма степен влиянието, което те могат да окажат като сила или за положително развитие, или за репресия;

В. като има предвид, че кибернетичните предизвикателства, заплахи и атаки нарастват с драматична бързина и представляват сериозна заплаха за сигурността, отбраната, стабилността и конкурентоспособността на националните държави, както и на частния сектор; като има предвид, че поради това такива заплахи не следва да бъдат считани за проблем на бъдещето; като има предвид, че естеството на повечето силно видими и разрушителни кибернетични инциденти вече е политически мотивирано; като има предвид, че макар че в преобладаващата си част кибернетичните инциденти продължават да бъдат примитивни, заплахите за критичните активи стават все по-сложни и налагат задълбочена защита;

Г. като има предвид, че кибернетичното пространство, с почти два милиарда глобално взаимосвързани потребители, се е превърнало в едно от най-мощните и ефективни средства за разпространение на демократичните идеи и организиране на хората в усилията им да постигнат своите стремежи към свобода и да се борят с диктаторските режими; като има предвид, че използването на кибернетичното пространство от недемократични и авторитарни режими представлява нарастваща заплаха за правата на хората на свобода на изразяване и свобода на сдружаване;

[5] Приети текстове, P7_TA(2012)0406.
[6] Приети текстове, P7_TA(2012)0237.
[7] http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx.

като има предвид, че поради това е от съществено значение да се гарантира, че кибернетичното пространство ще остане открито за свободния обмен на идеи, информация и изразяване на мнение;

Д. като има предвид, че в ЕС и в държавите членки съществуват многобройни пречки от политическо, законодателно и организационно естество пред изграждането на всеобхватен и единен подход спрямо кибернетичната отбрана и кибернетичната сигурност; като има предвид, че липсват обща дефиниция, стандарти и общи мерки в чувствителната и уязвима област на кибернетичната сигурност;

Е. като има предвид, че споделянето и координацията между институциите на ЕС, както и с държавите членки и с външни партньори и между тях все още не са достатъчни;

Ж. като има предвид, че в ЕС и на международно равнище липсват ясни и хармонизирани определения на „кибернетична сигурност“ и „кибернетична отбрана“; като има предвид, че разбирането за кибернетичната сигурност и за други ключови термини е твърде различно в различните страни;

З. като има предвид, че ЕС все още не е разработил собствени съгласувани политики за защита на критичната информационна инфраструктура, за което е необходим мултидисциплинарен подход, като се засилва сигурността при същевременно зачитане на основните права;

И. като има предвид, че ЕС предложи различни инициативи за справяне с киберпрестъпността на гражданско равнище, включително създаването на нов Европейски център по киберпрестъпност, но въпреки това не разполага с конкретен план на ниво сигурност и отбрана;

Й. като има предвид, че изграждането на доверие между частния сектор, от една страна, и правоприлагащите органи, институциите в областта на отбраната и други компетентни институции, от друга страна, е от изключителна важност за борбата срещу киберпрестъпността;

К. като има предвид, че взаимното доверие в отношенията между държавните и недържавните участници е предпоставка за надеждна кибернетична сигурност;

Л. като има предвид, че по-голямата част от кибернетичните инциденти както в публичния, така и в частния сектор не се съобщават поради чувствителното естество на информацията и възможните вреди за имиджа на засегнатите компании;

М. като има предвид, че голям брой кибернетични инциденти се случват поради недостатъчната устойчивост и здравина на частната и публичната мрежова инфраструктура, слабо защитени или обезопасени бази данни и други недостатъци в критичната информационна инфраструктура; като има предвид, че само няколко държави членки считат защитата на своите мрежи и информационни системи и свързаните с тях данни за свое съответно задължение за полагане на грижа, което обяснява липсата на инвестиции в съвременни технологии за сигурност, обучение и разработване на подходящи насоки, и като има предвид, че голям брой държави

членки са зависими от технологии за сигурност от трети държави и следва да увеличат усилията си за намаляване на тази зависимост;

Н. като има предвид, че по-голямата част от извършителите на сериозни кибернетични атаки, които застрашават националната или международната сигурност и отбрана, никога не биват откривани и подложени на наказателно преследване; като има предвид, че не съществува нито международно договорена форма на реакция спрямо подкрепени от държавата кибернетични атаки към друга държава, нито яснота по въпроса дали това може да се счита за „casus belli“;

О. като има предвид, че Европейската агенция за мрежова и информационна сигурност (ENISA) участва като посредник за държавите членки с цел подкрепа на обмена на добри практики в областта на кибернетичната сигурност посредством препоръки за разработването, изпълнението и поддържането на стратегия за кибернетична сигурност, има подпомагаща роля в националните стратегии за кибернетична сигурност, националните планове за действие в извънредни ситуации, организирането на общоевропейски и международни обучения във връзка със защитата на критичната информационна инфраструктура (ЗКИИ) и разработването на сценарии за национални обучения;

П. като има предвид, че към юни 2012 г. само 10 държави – членки на ЕС, са приели официално национални стратегии за кибернетична сигурност;

Р. като има предвид, че кибернетичната отбрана е един от най-важните приоритети на Европейската агенция по отбрана, която създаде в рамките на Плана за развитие на способностите проектен екип по въпросите на кибернетичната сигурност, като мнозинството от държавите членки работят по събирането на опит и представянето на препоръки;

С. като има предвид, че инвестициите в изследванията в областта на кибернетичната сигурност и отбрана са от съществено значение за напредъка и за поддържането на високо равнище на кибернетична сигурност и отбрана; като има предвид, че разходите за научноизследователска и развойна дейност са намалели, вместо да достигнат договорените 2% от общите разходи за отбрана;

Т. като има предвид, че повишаването на осведомеността и образованието на гражданите по въпросите на кибернетичната сигурност следва да представлява основата на всяка цялостна стратегия за кибернетична сигурност;

У. като има предвид, че трябва да се постигне ясен баланс между мерките за сигурност и правата на гражданите в съответствие с ДФЕС, като например правото на неприкосновеност на личния живот, защита на данните и свобода на изразяване, като никое от тях не бъде жертвано за сметка на другото;

Ф. като има предвид, че е налице нарастваща нужда от по-добро зачитане и защита на правото на хората на неприкосновеност на личния живот, както е посочено в Хартата на ЕС и в член 16 от ДФЕС; като има предвид, че необходимостта от сигурност и защита на киберпространството е важна за институциите и военните органи на национално равнище, но никога не трябва да се използва като извинение,

за да се ограничават правата и свободите в кибернетичното и информационното пространство по какъвто и да било начин;

Х. като има предвид, че глобалният и транснационален характер на интернет налага нови форми на международно сътрудничество и управление с множество заинтересовани страни;

Ц. като има предвид, че правителствата все повече разчитат на частни участници за сигурността на тяхната критична инфраструктура;

Ч. като има предвид, че Европейската служба за външна дейност (ЕСВД) все още не е включила активно аспекта на кибернетичната сигурност в своите отношения с трети страни;

Ш. като има предвид, че Инструментът за стабилност засега е единствената програма на ЕС, която има за цел реакция при неотложни кризисни ситуации или глобални/трансрегионални предизвикателства пред сигурността, включително заплахи за кибернетичната сигурност;

Щ. като има предвид, че съвместният отговор – посредством работната група ЕС-САЩ по въпросите на кибернетичната сигурност и киберпрестъпността – на заплахите за кибернетичната сигурност е един от приоритетните въпроси в отношенията между ЕС и САЩ;

Действия и координация на ЕС

1. отбелязва, че кибернетичните заплахи и атаки срещу правителствените, административните, военните и международните органи представляват рязко нарастваща опасност и явление както в ЕС, така и в глобален мащаб, и че са налице съществени причини за загриженост, че държавни и недържавни субекти, особено терористични и престъпни организации, могат да атакуват критични информационни и комуникационни структури и инфраструктури на институциите на ЕС и държави членки, като имат потенциала да причинят значителни вреди, включително динамични последици;

2. във връзка с това подчертава необходимостта от глобален и координиран подход към тези предизвикателства на равнище ЕС чрез разработване на цялостна стратегия на ЕС за кибернетична сигурност, която да предостави обща дефиниция за кибернетичната сигурност и отбрана и за това, какво представлява кибернетична атака, свързана с отбраната, както и обща оперативна визия, и да вземе предвид добавената стойност на съществуващите агенции и органи, както и добрите практики на държавите членки, които вече разполагат с национални стратегии за кибернетична сигурност; подчертава изключителната важност на координирането и създаването на взаимодействия на равнището на Съюза, които да спомогнат за съчетаването на различни инициативи, програми и дейности от военно и гражданско естество; подчертава, че такава стратегия следва да гарантира гъвкавост и да бъде актуализирана редовно, така че да бъде приспособявана към бързо променящото се естество на киберпространството;

3. настоятелно призовава Комисията и върховния представител на Съюза по въпросите на външните работи и политиката на сигурност да разгледат възможността за сериозна кибернетична атака срещу държава членка в предстоящото си предложение относно правилата за прилагане на клаузата за солидарност (член 222 от ДФЕС); освен това счита, че макар да е необходимо кибернетичните атаки, застрашаващи националната сигурност, да бъдат дефинирани посредством обща терминология, те биха могли да бъдат обхванати от клаузата за взаимна отбрана (член 42, параграф 7), без да се нарушава принципът на пропорционалност;

4. подчертава, че ОПСО трябва да гарантира защитата на силите, провеждащи военни операции и цивилни мисии на ЕС, от кибернетични атаки; подчертава, че кибернетичната отбрана следва да стане активен капацитет на ОПСО;

5. подчертава, че всички политики на ЕС за кибернетична сигурност следва да се основават на защита и опазване на цифровата свобода, както и на зачитане на човешките права онлайн, и да бъдат разработвани така, че да ги осигуряват в максимална степен; изразява убеждението си, че Интернет и ИКТ следва да бъдат включени във външната политика и политиката на сигурност на ЕС с цел напредък на тези усилия;

6. призовава Комисията и Съвета да признаят недвусмислено цифровите свободи като основни права и като необходима предпоставка гражданите да се ползват от универсалните човешки права; подчертава, че при разработването на техните реакции на кибернетичните заплахи и атаки държавите членки следва да си поставят за цел никога да не излагат на риск правата и свободите на гражданите си и следва да предвидят в законодателствата си подходящо разграничение между гражданско и военно равнище на кибернетичните инциденти; призовава към предпазливост при прилагане на ограничения върху възможността гражданите да се възползват от инструментите на комуникационните и информационните технологии;

7. призовава Съвета и Комисията, заедно с държавите членки, да изготвят Бяла книга относно киберотбраната, като се установят ясни дефиниции и критерии, които да разделят нивата на кибернетичните атаки в гражданската и военната сфера съгласно техните мотиви и последствия, както и нивата на реакция, включително разследването, разкриването и съдебното преследване на извършителите;

8. вижда ясна необходимост от актуализиране на Европейската стратегия за сигурност с оглед да се идентифицират и да се намерят средства за преследване и изправяне пред съда на отделни, свързани с мрежата и подкрепяни от държавата извършители на кибернетични атаки;

На равнище ЕС

9. подчертава важността на хоризонталното сътрудничество и координация по въпросите на кибернетичната сигурност в рамките на институциите и агенциите на ЕС и между тях;

10. подчертава, че новите технологии представляват предизвикателство по отношение на начина, по който правителствата изпълняват своите традиционни основни задачи; отново потвърждава, че политиките, свързани с отбраната и сигурността, включително подходящият демократичен контрол, в крайна сметка са отговорност на правителството; отбелязва все по-значимата роля на частноправните субекти за изпълнение на задачите, свързани с отбраната и сигурността, често без необходимата прозрачност, отчетност или механизъм за контрол;

11. подчертава, че правителствата трябва да спазват основните принципи на международното публично и хуманитарно право, като например зачитането на държавния суверенитет и правата на човека, при използването на нови технологии в рамките на политиките за сигурност и отбрана; подчертава ценния опит на държави – членки на ЕС, като Естония в определянето и създаването на политики за кибернетична сигурност, както и за кибернетична отбрана;

12. признава необходимостта от оценка на цялостното равнище на кибернетичните атаки срещу информационните системи и инфраструктура на ЕС; в този контекст подчертава необходимостта от непрекъсната оценка на степента на подготвеност на институциите на ЕС да се справят с потенциални кибернетични атаки; подчертава по-специално необходимостта от засилване на критичната информационна инфраструктура;

13. подчертава също така необходимостта от предоставяне на информация относно уязвимите места, сигналите и предупрежденията за нови заплахи спрямо информационните системи;

14. отбелязва, че неотдавнашните кибернетични атаки срещу европейските информационни мрежи и правителствени информационни системи нанесоха значителни икономически щети и вреди по отношение на сигурността, размерът на които все още не е оценен в достатъчна степен;

15. призовава всички институции на ЕС да разработят във възможно най-кратки срокове свои стратегии за кибернетична сигурност и планове за действие в извънредни ситуации с оглед на техните собствени системи;

16. призовава всички институции на ЕС да включат в своя анализ на риска и в плановете си за управление на кризи въпроса за управление на кибернетични кризи; освен това призовава всички институции на ЕС да осигурят обучения за повишаване на осведомеността относно кибернетичната сигурност за целия си персонал; препоръчва провеждане на кибернетични учения веднъж годишно по подобие на ученията за действие при извънредни ситуации;

17. подчертава важността на ефективното развитие на екип за незабавно реагиране при компютърни инциденти на ЕС (EU-CERT) и на национални екипи за незабавно реагиране при компютърни инциденти, както и на разработването на национални планове за действие в извънредни ситуации в случай на необходимост от предприемане на действия; приветства факта, че до май 2012 г. всички държави – членки на ЕС, създадоха национални екипи за незабавно реагиране при компютърни инциденти; настоятелно призовава за по-нататъшно развитие на националните

екипи за незабавно реагиране при компютърни инциденти и на екип за незабавно реагиране при компютърни инциденти на ЕС, които да са в състояние при необходимост да предприемат действия в рамките на 24 часа; подчертава необходимостта да се разгледа осъществимостта на публично-частните партньорства в тази област;

18. признава, че „Cyber Europe 2010“, първото паневропейско обучение относно защитата на критичната информационна инфраструктура, което бе проведено с участието на различни държави членки и водено от ENISA, се оказа полезно действие и пример за добра практика; подчертава също така необходимостта от възможно най-скорошно създаване на Предупредителна информационна мрежа за критичната инфраструктура на европейско равнище;

19. подчертава значението на паневропейските учения при подготовката за широкомащабни инциденти по мрежовата сигурност и определянето на единен набор от стандарти за оценка на заплахите;

20. призовава Комисията да проучи необходимостта от поща за кибернетична координация на ЕС;

21. счита, че предвид високите нива на квалификация, необходими както за осигуряване на подходяща защита на кибернетичните системи и инфраструктури, така и за атаките срещу тях, Комисията, Съветът и държавите членки следва да обмислят възможността за разработване на стратегия от типа „white hat“ („етични хакери“); отбелязва, че в тези случаи опасността от „изтичане на мозъци“ е висока, както и факта, че особено малолетните лица, осъдени за подобни атаки, имат голям потенциал както за реабилитация, така и за интеграция в агенциите и органите по отбраната;

Европейска агенция по отбрана (EDA)

22. приветства неотдавнашните инициативи и проекти, свързани с кибернетичната отбрана, по-специално относно събирането и картирането на данните, предизвикателствата и потребностите, свързани с кибернетичната сигурност и отбрана, и настоятелно призовава държавите членки към по-тясно сътрудничество, включително на военно равнище, с EDA по въпросите, свързани с киберотбраната;

23. подчертава важността за държавите членки на тясното сътрудничество с EDA във връзка с развитието на техните национални способности за кибернетична отбрана; изразява убеждението си, че изграждането на взаимодействия, обединяването и споделянето на европейско равнище са от съществено значение за ефективната кибернетична отбрана на европейско и национално равнище;

24. насърчава EDA да задълбочи сътрудничеството си с НАТО, националните и международните центрове за високи постижения, Европейския център по киберпрестъпност в рамките на Европол, с което да допринесе за съкращаване на времето за реакция в случай на кибератаки, и особено със съвместния център за високи научни постижения по киберотбрана (CCDCOE), да се концентрира върху изграждането на капацитет и обучението, както и върху обмена на информация и

практики;

25. отбелязва с безпокойство, че само една държава членка е постигнала равнището от 2 % разходи за научноизследователска и развойна дейност в областта на отбраната до 2010 г. и че пет държави членки не са похарчили нищо за научноизследователска и развойна дейност през 2010 г.; призовава EDA, заедно с държавите членки, да обединят ресурси и да инвестират ефективно в съвместна научноизследователска и развойна дейност, по-специално по отношение на кибернетичната сигурност и отбрана;

Държави членки

26. призовава всички държави членки без по-нататъшно отлагане да разработят и завършат съответните си национални стратегии за кибернетична сигурност и отбрана и да осигурят солидна регулаторна среда и среда за определяне на политики, всеобхватни процедури за управление на риска и подходящи подготвителни мерки и механизми; призовава ENISA да подпомага държавите членки; изразява своята подкрепата за ENISA в разработването на Ръководство за добри практики в областта на добрите практики и препоръките за това, как да се разработва, изпълнява и поддържа стратегия за кибернетична сигурност;

27. насърчава всички държави членки да създадат определени единици за кибернетична сигурност и кибернетична отбрана в рамките на своята военна структура с цел да осъществяват сътрудничество с подобни органи в други държави – членки на ЕС;

28. насърчава държавите членки да въведат специализирани съдилища на регионално равнище, които да имат за цел по-ефективно санкциониране на атаките срещу информационните системи; подчертава необходимостта от насърчаване на адаптирането на националните законодателства, което ще позволи приспособяването им към развитието на техниките и начините на използването им;

29. призовава Комисията да продължи да работи по съгласуван и ефикасен европейски подход, за да избягва излишни инициативи, като насърчава и подкрепя държавите членки в усилията им да разработят механизми за сътрудничество и да подобряват обмена на информация; счита, че между държавите членки следва да бъде установено едно минимално равнище на задължително сътрудничество и споделяне;

30. настоятелно призовава държавите членки да разработят национални планове за действие в извънредни ситуации и да включат управлението на кибернетични кризи в плановете за управление на кризи и анализ на риска; подчертава освен това значението на подходящото обучение по основна кибернетична сигурност за всички служители в публичните субекти и по-специално на предлагането на специално обучение на членовете на съдебните институции и органите за сигурност в центрове за обучение; призовава ENISA и други съответни органи да подпомагат държавите членки при осигуряване обединяването и споделянето на ресурси, както и за избягване на дублирането;

31. настоятелно призовава държавите членки да превърнат научноизследователската и развойна дейност в един от основните стълбове на кибернетичната сигурност и

отбрана и да насърчават обучението на инженери, специализирани в защитата на информационните системи; призовава държавите членки да изпълнят своя ангажимент за увеличаване поне до 2 % на разходите за научноизследователска и развойна дейност в областта на отбраната, по-специално по отношение на кибернетичната сигурност и отбрана;

32. призовава Комисията и държавите членки да предложат програми за насърчаване на общото безопасно използване на интернет, информационните системи и комуникационните технологии и за повишаване на осведомеността за него както сред частните, така и сред корпоративните потребители; предлага Комисията да стартира публична паневропейска образователна инициатива във връзка с това и призовава държавите членки да включат обучение по кибернетична сигурност в училищните програми от възможно най-ранна възраст;

Публично-частно сътрудничество

33. подчертава решаващата роля на значимото и допълващо се сътрудничество в областта на кибернетичната сигурност между публичните органи и частния сектор както на равнище ЕС, така и на национално равнище, с цел създаване на взаимно доверие; съзнава, че по-нататъшното подобряване на надеждността и ефективността на съответните публични институции ще допринесе за изграждането на доверие и за споделянето на информация от критично значение;

34. призовава партньорите от частния сектор при разработването на нови продукти, устройства, услуги и приложения да обмислят решения за заложена още при проектирането сигурност и стимули за онези, които разработват нови продукти, устройства, услуги и приложения със заложена при проектирането сигурност като основна характеристика; призовава при сътрудничеството с частния сектор да съществуват минимални стандарти за прозрачност и механизми за търсене на отговорност с цел предотвратяване и борба с кибернетичните атаки;

35. подчертава, че защитата на критичната информационна инфраструктура е включена в Стратегията за вътрешна сигурност на ЕС в контекста на повишаване на степента на сигурност за гражданите и предприятията в кибернетичното пространство;

36. призовава за създаването на постоянен диалог с тези партньори относно най-доброто използване и устойчивостта на информационните системи и споделянето на отговорността, необходимо за сигурното и правилно функциониране на тези системи;

37. счита, че държавите членки, институциите на ЕС и частният сектор, в сътрудничество с ENISA, следва да предприемат стъпки за увеличаване на сигурността и целостта на информационните системи, за предотвратяване на атаки и за минимизиране на последиците от атаките; подкрепя Комисията в усилията ѝ да изготви минимални стандарти за кибернетична сигурност и системи за сертифициране за компаниите, както и да осигури правилните стимули за насърчаване на усилията на частния сектор за повишаване на сигурността;

38. призовава Комисията и правителствата на държавите членки да насърчават частния

сектор и участниците от гражданското общество да включат управлението на кибернетични кризи в своите планове за управление на кризи и анализ на риска; призовава освен това за въвеждане на обучение за повишаване на осведомеността относно важните въпроси на кибернетичната сигурност и кибернетичната хигиена за всички членове на своя персонал;

39. призовава Комисията, в сътрудничество с държавите членки и съответните агенции и органи, да разработят рамки и инструменти за една система за бърз обмен на информация, която да гарантира анонимност при докладване на кибернетични инциденти за частния сектор, да даде възможност на участниците от публичната сфера да бъдат постоянно информирани и да предоставя помощ, когато е необходимо;

40. подчертава необходимостта ЕС да улесни развитието на конкурентен и иновативен пазар за кибернетична сигурност в ЕС с цел да се даде по-добра възможност на МСП да работят в тази област, което ще допринесе за даване на тласък на икономическия растеж и за създаване на нови работни места;

Международно сътрудничество

41. призовава ЕСВД да предприеме активен подход по отношение на кибернетичната сигурност и да интегрира аспекта за кибернетичната сигурност във всички свои действия, особено по отношение на трети държави; призовава за ускоряване на сътрудничеството и обмена на информация за това, как да се подходи към въпросите на кибернетичната сигурност с трети държави;

42. подчертава, че доизграждането на цялостна стратегия на ЕС за кибернетична сигурност е предварително условие за създаването на ефективно международно сътрудничество в областта на кибернетичната сигурност, което се налага от трансграничната природа на кибернетичните заплахи;

43. призовава тези държави членки, които все още не са подписали или ратифицирали Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство (Конвенцията от Будапеща), да го направят без по-нататъшно отлагане; подкрепя Комисията и ЕСВД в техните усилия за популяризиране на конвенцията и нейните ценности сред трети държави;

44. съзнава необходимостта от международно договорена и координирана реакция спрямо кибернетичните заплахи; във връзка с това призовава Комисията, ЕСВД и държавите членки да поемат водеща роля на всички форуми, по-специално в ООН, като полагат усилия за постигане на по-широко международно сътрудничество и окончателно споразумение относно определяне на общо разбиране за нормите на поведение в кибернетичното пространство, както и да насърчават сътрудничеството за разработване на споразумения за контрол над кибероръжията;

45. насърчава обмена на знания с държавите от групата БРИКЮ и други държави с бързо развиващи се икономики в областта на кибернетичната сигурност, с цел да се проучат евентуални общи реакции на нарастващата кибернетична престъпност и кибернетичните заплахи и атаки както на гражданско, така и на военно равнище;

46. настоятелно призовава ЕСВД и Комисията да предприемат активен подход в рамките на съответните международни форуми и организации, по-специално на ООН, ОССЕ, ОИСР и Световната банка, с цел прилагане на съществуващото международно право и постигане на консенсус относно нормите за отговорно поведение на държавите по отношение на кибернетичната сигурност и отбрана и чрез координиране на позициите на държавите членки с оглед насърчаване на основните ценности и политики на ЕС в областта на кибернетичната сигурност и отбрана;

47. призовава Съвета и Комисията в рамките на своите диалози, отношения и споразумения за сътрудничество с трети държави, по-специално тези, които предвиждат сътрудничество или обмен в областта на технологиите, да настояват за минимални изисквания за предотвратяване и борба с кибернетичната престъпност и кибернетичните атаки, както и за минимални стандарти в областта на сигурността на информационната система;

48. призовава Комисията да улесни и подпомогне третите държави, ако е необходимо, в техните усилия да изградят своя капацитет за кибернетична сигурност и кибернетична отбрана;

Сътрудничество с НАТО

49. отново заявява, че въз основа на своите общи ценности и стратегически интереси ЕС и НАТО носят специална отговорност и притежават капацитет да се справят с нарастващите предизвикателства в сферата на кибернетична сигурност по-ефективно и в тясно сътрудничество чрез търсене на възможно допълване, без дублиране и при зачитане на съответните им отговорности;

50. подчертава необходимостта от обединяване и споделяне на практическо равнище, като има предвид допълващия се характер на подхода на ЕС и НАТО спрямо кибернетичната сигурност и отбрана; подчертава необходимостта от по-тясна координация, особено относно планирането, технологиите, обучението и оборудването по отношение на кибернетичната сигурност и отбрана;

51. призовава настоятелно всички съответни органи в ЕС, занимаващи се с кибернетична сигурност и отбрана, въз основа на съществуващите допълващи се дейности по развитието на отбранителна способност, да задълбочат своето практическо сътрудничество с НАТО с оглед обмен на опит и знания относно това, как да се изгради устойчивост за системите на ЕС;

Сътрудничество със Съединените американски щати

52. счита, че ЕС и САЩ следва да задълбочат взаимното си сътрудничество за противодействие на кибернетичните атаки и престъпления, тъй като това е приоритет на трансатлантическите отношения след срещата на високо равнище между ЕС и САЩ в Лисабон през 2010 г.;

53. приветства създаването на работна група ЕС–САЩ относно кибернетичната сигурност и кибернетичните престъпления, осъществено на срещата на високо

равнище между ЕС и САЩ през ноември 2010 г., и подкрепя усилията на тази група да включи въпросите на кибернетичната сигурност в трансатлантическия политически диалог;

54. приветства създаването съвместно от Комисията и правителството на САЩ, в рамките на работната група ЕС–САЩ, на обща програма и пътна карта за съвместни/синхронизирани трансконтинентални кибернетични учения през периода 2012/2013 г.; отбелязва първото кибернетично атлантическо учение през 2011 г.;

55. подчертава необходимостта както за САЩ, така и за ЕС, като най-големи източници на кибернетично пространство и потребители, да работят заедно за защита на правата и свободите на техните граждани да използват това пространство; подчертава, че макар националната сигурност да е първостепенна задача, кибернетичното пространство следва да бъде гарантирано, но също и защитено;

56. възлага на своя председател да предаде настоящата резолюция на Съвета, на Комисията, на върховния представител/заместник-председател, на EDA, ENISA и НАТО.

РЕЗУЛТАТ ОТ ОКОНЧАТЕЛНОТО ГЛАСУВАНЕ В КОМИСИЯ

Дата на приемане	10.10.2012 г.
Резултат от окончателното гласуване	+: 47 –: 3 0: 6
Членове, присъствали на окончателното гласуване	Bastiaan Belder, Franziska Katharina Brantner, Elmar Brok, Jerzy Buzek, Tarja Cronberg, Arnaud Danjean, Mário David, Ana Gomes, Andrzej Grzyb, Anna Ibrisagic, Liisa Jaakonsaari, Anneli Jäätteenmäki, Jelko Kacin, Ioannis Kasoulides, Tunne Kelam, Nicole Kiil-Nielsen, Евгени Кирилов, Maria Eleni Koppa, Wolfgang Kreissl-Dörfler, Eduard Kukan, Vytautas Landsbergis, Krzysztof Lisek, Sabine Lösing, Mario Mauro, Francisco José Millán Mon, Alexander Mirsky, María Muñiz De Urquiza, Annemie Neyts-Uyttebroeck, Norica Nicolai, Raimon Obiols, Kristiina Ojuland, Ria Oomen-Ruijten, Justas Vincas Paleckis, Bernd Posselt, Cristian Dan Preda, Fiorello Provera, José Ignacio Salafranca Sánchez-Neyra, Jacek Saryusz-Wolski, Werner Schulz, Sophocles Sophocleous, Laurence J.A.J. Stassen, Кристиан Вигенин, Sir Graham Watson, Karim Zéribi
Заместник(ци), присъствал(и) на окончателното гласуване	Charalampos Angourakis, Elena Băsescu, Jean-Jacob Bicep, Véronique De Keyser, Diogo Feio, Elisabeth Jeggle, Indrek Tarand, Sampo Terho, László Tőkés, Traian Ungureanu, Luis Yáñez-Barnuevo García
Заместник(ци) (чл. 187, пар. 2), присъствал(и) на окончателното гласуване	Joseph Cuschieri