Четвъртък, 12 септември 2013 г.

4. Отправя искане към Комисията да окаже подкрепа на държавите членки за намаляване на разликата в заплащането на жените и мъжете с най-малко 5 % годишно, така че до 2020 г. разликата в заплащането на жените и мъжете да бъде премахната изцяло;

5. Отчита, че един многостепенен, многостранен подход изисква Комисията да оказва подкрепа на държавите членки при насърчаването на добри практики и при прилагането на политики за преодоляване на разликата в заплащането на жените и мъжете;

6. Настоятелно призовава Комисията да преразгледа незабавно Директива 2006/54/ЕО и да предложи изменения към нея в съответствие с член 32 от директивата и въз основа на член 157 от ДФЕС, като следва подробните препоръки, отправени в приложението към резолюцията на Европейския парламент от 24 май 2012 г.;

7. Възлага на своя председател да предаде настоящата резолюция на Съвета, Комисията и правителствата на държавите членки.

P7_TA(2013)0376

Стратегия на ЕС за киберсигурност: открито, безопасно и сигурно кибернетично пространство

Резолюция на Европейския парламент от 12 септември 2013 г. относно стратегията на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство (2013/2606(RSP))

(2016/C 093/16)

Европейският парламент,

— като взе предвид съвместното съобщение на Европейската комисия и върховния представител на Европейския съюз по въпросите на външните работи и политиката на сигурност от 7 февруари 2013 г., озаглавено „Стратегията на Европейския съюз за киберсигурност — Отворено, безопасно и сигурно киберпространство“ (JOIN(2013)0001);

— като взе предвид предложението на Комисията от 7 февруари 2013 г. за директива относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза (COM(2013)0048),

— като взе предвид съобщенията на Комисията от 19 май 2010 г., озаглавено „Програма в областта на цифровите технологии за Европа“ (COM(2010)0245) и от 18 декември 2012 г., озаглавено „Програма в областта на цифровите технологии за Европа: цифровите технологии — двигател на европейския икономически растеж“ (COM(2012)0784),

— като взе предвид съобщението на Комисията от 27 септември 2012 г., озаглавено „Оползотворяване на потенциала на изчисленията в облак в Европа“ (COM(2012)0529),

— като взе предвид съобщението на Комисията от 28 март 2012 г., озаглавено „Борбата с престъпността дигиталната ера: създаване на Европейски център по киберпрестъпност (COM(2012)0140) и заключенията на Съвета от 7 юни 2012 г.,

— като взе предвид Директива „2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 година атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета ([1]),

— 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 ([2]),

([1]) ОВ L 218, 14.8.2013 г., стр. 8.
([2]) ОВ L 345, 23.12.2008 г., стр. 75.

— като взе предвид Директива 2011/92/ЕС на Европейския парламент и на Съвета от 13 декември 2011 г. относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография и за замяна на Рамково решение 2004/68/ПВР на Съвета ([1]),

— като взе предвид Стокхолмската програма ([2]) в областта на политиката на свобода, сигурност и правосъдие, съобщението на Комисията „Установяване на пространство на свобода, сигурност и правосъдие за гражданите на Европа: План за действие за изпълнение на Програмата от Стокхолм“ (COM(2010)0171) и съобщението на Комисията „Стратегията за вътрешна сигурност на ЕС в действие: пет стъпки към една по-сигурна Европа“ (COM(2010)0673), и своята резолюция от 22 май 2012 г. относно стратегия за вътрешна сигурност на Европейския съюз ([3]),

— като взе предвид съвместното предложение на Комисията и върховния представител за решение на Съвета относно договореностите за прилагането от страна на Съюза на клаузата за солидарност (JOIN(2012)0039),

— като взе предвид Рамковото решение на Съвета 2001/413/ПВР от 28 май 2001 г относно борбата срещу измамите и фалшифицирането на непаричните платежни средства ([4]),

— 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 ([5]) и заключенията на Съвета от 27 май 2011 г. относно съобщението на Комисията, озаглавено „Постижения и предстоящи стъпки за постигане на сигурност в световното кибернетично пространство“ (COM(2011) 0163),

— като взе предвид резолюцията си от 11 декември 2012 г. относно доизграждането на цифровия единен пазар ([6]),

— като взе предвид своята резолюция от 22 ноември 2012 г. относно кибернетичната сигурност и отбрана ([7]),

— като взе предвид своята позиция от 16 април 2013 г. на първо четене относно предложението за Регламент на Европейския парламент и на Съвета относно Европейската агенция за мрежова и информационна сигурност (ENISA) (COM(2010)0521) ([8]),

— като взе предвид своята резолюция от 11 декември 2012 г. относно стратегия за цифрова свобода в рамките на външната политика на ЕС ([9]),

— като взе предвид Конвенцията на Съвета на Европа относно престъпленията в кибернетичното пространство от 23 ноември 2001 г.,

— като взе предвид международните задължения на Съюза, по-конкретно произтичащите от Общото споразумение по търговията с услуги,

— като взе предвид член 16 от Договора за функционирането на Европейския съюз (ДФЕС) и Хартата за основните права на Европейския съюз, по-конкретно членове 6, 8 и 11 от нея,

— като взе предвид продължаващите преговори относно трансатлантическото партньорство в областта на търговията и инвестициите между Европейския съюз и Съединените американски щати,

— като взе предвид член 110, параграф 2 от своя правилник,

A. като има предвид, че нарастващите киберпредизвикателства, под формата на все по-усъвършенствани заплахи и атаки, представляват значителна опасност за сигурността, стабилността и икономическия просперитет на държавите членки, както и на частния сектор и обществото като цяло; като има предвид, че по тази причина защитата на нашето общество и икономика ще бъде постоянно увеличаващо се предизвикателство;

([1]) ОВ L 335, 17.12.2011 г., стр. 1.
([2]) ОВ C 115, 4.5.2010 г., стр. 1.
([3]) Приети текстове, P7_TA(2012)0207.
([4]) ОВ L 149, 2.6.2001 г., стр. 1.
([5]) Приети текстове, P7_TA(2012)0237.
([6]) Приети текстове, P7_TA(2012)0468.
([7]) Приети текстове, P7_TA(2012)0457.
([8]) Приети текстове, P7_TA(2013)0103.
([9]) Приети текстове, P7_TA(2012)0470.

Четвъртък, 12 септември 2013 г.

Б. като има предвид, че киберпространството и киберсигурността следва да са сред стратегическите стълбове на политиките в областта на сигурността и отбраната на ЕС и на всяка държава членка; като има предвид, че е от съществено значение да се гарантира, че киберпространството остава открито за свободния обмен на идеи и информация, и за свободното изразяване на мнение;

В. като има предвид, че електронната търговия и интернет услугите са жизненоважни за интернет и са от изключително значение за постигане на целите на стратегията „Европа 2020“, която е от полза както за гражданите, така и за частния сектор, като има предвид, че Съюзът трябва да реализира изцяло потенциала и възможностите, които предлага интернет при по-нататъшното развитие на единния пазар, включително на цифровия единен пазар;

Г. като има предвид, че посочените в съвместното съобщение относно стратегия за киберсигурността в Европейския съюз включва постигането на кибернетична устойчивост, намаляване на киберпрестъпността, разработване на политика за кибернетична отбрана и кибернетични способности, която да е свързана с общата политика за сигурност и отбрана и да установява последователна международна политика за кибернетичното пространство за ЕС;

Д. като има предвид, че в голяма степен мрежовите и информационните системи в Съюза са взаимно свързани; като има предвид, че с оглед глобалния характер на интернет, много инциденти с мрежовата и информационната сигурност прехвърлят националните граници и притежават потенциал да подкопаят функционирането на вътрешния пазар и доверието на потребителите в цифровия единен пазар;

Е. като има предвид, че киберсигурността в Съюза, както и в останалата част на света е толкова силна, колкото най-слабото й звено, и че смущенията в един сектор или държава членка оказват въздействие върху друг сектор или държава членка, като разпространението на отрицателните последици засяга икономиката на Съюза като цяло;

Ж. като има предвид, че към април 2013 г. само 13 държави членки официално приеха национални стратегии в областта на киберсигурността; като има предвид, че между държавите членки продължават да съществуват основни различия по отношение на подготвеността им, сигурността, стратегическата им култура и способност да разработят и прилагат национални стратегии в областта на киберсигурността, и като има предвид, че следва да бъде извършена оценка на посочените различия;

З. като има предвид, че различните култури в областта на сигурността и липсата на правна рамка водят до разпокъсаност и представляват основен повод за притеснение по отношение на цифровия единен пазар; като има предвид, че липсата на хармонизиран подход към киберсигурността води до сериозни рискове за икономическия просперитет и за сигурността на трансакциите, и като има предвид, че това налага единни усилия и по-тясно сътрудничество между правителствата, частния сектор и правоприлагащите и разузнавателните агенции;

И. като има предвид, че киберпрестъпността се превръща във все по-скъпоструващ международен проблем, който към момента, по данни на Службата на ООН по наркотиците и престъпността струва на световната икономика близо 295 милиарда евро годишно;

Й. като има предвид, че международната организирана престъпност, като се възползва от напредъка на технологиите, продължава да прехвърля полето си на действие в киберпространството, където киберперстъпността драстично променя традиционната структура на групите на организираната престъпност; като има предвид, че в резултат на това организираната престъпност не е толкова локализирана и че е по-вероятно да се възползва от териториалността и различаващите се национални правни юрисдикции на световно равнище;

К. като има предвид, че при разследването на киберпрестъпността компетентните органи все още срещат редица пречки, сред които използването в кибернетичните транзакции на „виртуална валута“, която може да се използва за пране на пари, проблемите с териториалността и границите на юрисдикцията, недостатъчния капацитет на обмена на разузнавателна информация, липсата на обучен персонал и непоследователното сътрудничество с другите заинтересовани лица;

Л. като има предвид, че технологията е основа за развитието на киберпространството и постоянното адаптиране към технологичните промени е от съществено значение за подобряване на устойчивостта и безопасността на киберпространството на ЕС; като има предвид, че трябва да бъдат предприети мерки, за да се гарантира, че законодателството е синхронизирано с актуалното развитие на технологиите, като се позволи ефективното разкриване и преследване на киберпрестъпниците и защитата на жертвите на киберпрестъпността; като има предвид, че стратегията на

ЕС за киберсигурност трябва да включва мерки, фокусирани върху осведомеността, образованието, разработването на екипи за незабавно реагиране при компютърни инциденти, развитието на вътрешен пазар за продукти и услугите в областта на киберсигурността, както и насърчаването на инвестициите в изследванията, развитието и иновациите;

1. Приветства съвместното съобщение относно стратегията за киберсигурността в Европейския съюз и предложението за директива относно мерките за гарантиране на високо ниво на мрежова и информационна сигурност в Съюза;

2. Подчертава важното и нарастващо значение на интернет и киберпространството за политическите, икономическите и обществените трансакции, не само в рамките на Съюза, но и по отношение на други фактори по света;

3. Подчертава, че е необходимо да се развива политика на стратегическа комуникация относно киберсигурността в ЕС, ситуации на кибернетични кризи, стратегическо препозициониране, публично-частно сътрудничество и заплахи, както и препоръки към обществеността;

4. Припомня, че високо ниво на мрежова и информационна сигурност е необходимо не само за поддържане на услугите, които са от съществено значение за гладкото функциониране на обществото и икономиката, но също и за запазване на физическата неприкосновеност на гражданите чрез укрепване на ефикасността, ефективността и сигурното функциониране на критичните инфраструктури; подчертава, че редом с разглеждането на мрежовата и информационната сигурност, друг важен въпрос е и подобряването на физическата сигурност; подчертава, че инфраструктурата следва да е устойчива както на умишлени, така и на неумишлени смущения; в това отношение подчертава, че стратегията относно киберсигурността следва да наблегне повече на най-честите причини за неумишлени сривове в системата;

5. Подновява призива си към държавите членки да приемат национални стратегии относно киберсигурността, които да обхващат аспекти на техническите, координационните, човешките ресурси и предоставянето на финансиране и които да включват отделни правила относно ползите и отговорностите на частния сектор с цел да се гарантира навременно му участието и да се осигурят всеобхватни процедури за управление на риска, като и за защита на регулаторната среда;

6. Отбелязва, че единствено съчетанието между лидерска роля и политическа ангажираност от страна на институциите на Съюза и от държавите членки ще позволи достигането на високо ниво на мрежова и информационна сигурност в Съюза и ще допринесе за сигурното и гладкото функциониране на единния пазар;

7. Подчертава, че политиката на Съюза в областта на киберсигурността следва да предвижда сигурна и надеждна цифрова среда, основана и предназначена да гарантира защита и опазване в онлайн средата на свободите и спазването на основните права във вида, в който са установени в Хартата на ЕС и в член 16 от ДФЕС, по-конкретно правото на неприкосновеност на личния живот и на защита на данните; счита, че следва да бъде отделено специално внимание на закрилата на децата в онлайн средата;

8. Призовава държавите членки и Комисията да предприемат всички необходими действия, за да представят програми за обучение, имащи за цел да насърчат и подобрят осведомеността, уменията и образованието сред европейските граждани, по-конкретно по отношение на личната сигурност, като част от учебната програма за цифрово ограмотяване от ранна възраст; приветства инициативата за организиране на месец на европейската киберсигурност, с подкрепата на Европейската агенция за мрежова и информационна сигурност (ENISA) и в сътрудничество с публичните органи и частния сектор, с цел повишаване на осведомеността относно предизвикателствата от областта на мрежовите и информационните системи;

9. Счита, че образованието относно киберсигурността повишава осведомеността на европейското общество относно киберзаплахите, като по този начин насърчава отговорното използване на киберпространството и помага за развиването на кибернетични умения; признава ключовата роля на Европол и новия му Европейски център за борба с киберпрестъпността, както и на ENISA и Евроюст при осигуряване на дейности по обучение на равнището на ЕС относно използването на инструментите на международното съдебно сътрудничество и правоприлагането, засягащи различни аспекти на киберпрестъпността;

10. Потвърждава необходимостта от предоставяне на техническа консултация и правна информация, както и от съставяне на програми относно превенцията и борбата с киберпрестъпността; насърчава обучението на киберинженери, специализирани в защитата на критичната инфраструктура и информационните системи, както и на оператори на системи за контрол на транспорта и центрове за управление на трафика; подчертава спешната необходимост от въвеждане на схеми на редовно обучение по киберсигурност за лицата, заети на всички равнища в публичния сектор;

Четвъртък, 12 септември 2013 г.

11. Подновява призива си за предпазливост при прилагането на ограничения относно способността на гражданите да използват инструменти на комуникационни и информационни технологии и подчертава, че държавите членки следва да се стремят никога да не застрашават правата и свободите на гражданите, когато разработват отговори на киберзаплахи и кибератаки, и следва да имат подходящи законодателни средства за различаване на киберинциденти от граждански и военен характер;

12. Счита, че регулаторната намеса в областта на киберсигурността следва да е ориентирана към риска, да е фокусирана върху критичната инфраструктура, чието правилно функциониране е от висш обществен интерес и следва да се гради върху съществуващи, пазарно ориентирани усилия на промишлеността, за да се гарантира мрежова устойчивост; подчертава ключовата роля на сътрудничеството на оперативно равнище за укрепване на по-ефикасен обмен на информация относно киберзаплахите между публичните органи и частния сектор, както на равнището на Съюза, така и на национално равнище, и също така със стратегическите партньори на Съюза, с цел да се гарантира мрежовата и информационната сигурност чрез създаване на взаимно доверие, оценка и ангажираност, и обмен на опит; счита, че публично-частните партньорства следва да се основават на мрежова и технологична неутралност, и да се фокусират върху усилията за справяне с проблемите, оказващи значително обществено въздействие; призовава Комисията да насърчава всички участващи оператори на пазара да бъдат по-внимателни и по-отворени към сътрудничество с цел да помогнат на други оператори да защитят услугите си;

13. Признава, че разкриването и уведомяването за инциденти, свързани с киберсигурността, е от съществено значение за насърчаването на киберустойчивостта в Съюза; счита, че следва да бъдат установени пропорционални и необходими изисквания за разкриване на информация, за да бъде възможно уведомяването на националните органи за инциденти, свързани със значителни нарушения на сигурността, като по този начин ще улесни по-доброто проследяване на инциденти, свързани с киберпрестъпността, и ще позволи полагането на усилия за повишаване на осведомеността на всички равнища;

14. Насърчава Комисията и другите участници да въведат политики за киберсигурност и киберустойчивост, в които да бъдат включени стимули за насърчаване на високи равнища на киберсигурност и киберустойчивост;

Киберустойчивост

15. Отбелязва, че различните сектори и държави членки имат различна степен на способности и умения и че това възпрепятства развитието на сътрудничество, основано на доверието, и подкопава функционирането на единния пазар;

16. Счита, че изискванията за малките и средните предприятия следва да се ръководят от подход, основан на пропорционалността и съизмерен с риска;

17. Настоява за развиването на киберустойчивост за критичните инфраструктури и припомня, че предстоящите договорености за прилагането на клаузата за солидарност (член 222 от ДФЕС) следва да отчетат риска от кибератаки срещу държавите членки; призовава Комисията и върховния представител да вземат този риск предвид в своите съвместни интегрирани доклади за оценка на заплахата и риска, които ще излязат през 2015 г.;

18. Подчертава, че за гарантиране на неприкосновеността, наличността и поверителността по-специално на критичните услуги, идентификацията и категоризацията на критичната инфраструктура трябва да бъде актуализирана и трябва да бъдат определени необходимите минимални изисквания за сигурност за техните мрежи и информационни системи;

19. Признава, че предложението за директива относно мерки, с които да се гарантира високо общо равнище на сигурност на мрежите и на информацията в Съюза предвижда такива минимални изисквания за сигурност за доставчиците на услуги на информационното общество и операторите на критични инфраструктури;

20. Призовава държавите членки и Съюза да установят подходящи рамки за бърз двупосочен обмен на информация, които да гарантират анонимност за частния сектор и да предоставят постоянна информация на публичния, и при необходимост да осигуряват съдействие на частния сектор;

21. Приветства споменаването от страна на Комисията на идеята за създаване на култура за управление на риска по отношение на сигурността в кибернетичното пространство и призовава настоятелно държавите членки и институциите на Съюза да включат бързо управлението на кризи в киберпространството в техните планове за управление на кризи и за анализи на риска; освен това призовава правителствата на държавите членки и Комисията да насърчат представителите на частния сектор да включат управлението на кризи в киберпространството в техните планове за управление на кризи и за анализ на риска, както и да проведат обучение на своите служители във връзка с киберсигурността;

22. Призовава всички държави членки и институциите на Съюза да създадат мрежа от добре функциониращи екипи за незабавно реагиране при компютърни инциденти (CERT), които да работят денонощно 7 дни в седмицата; посочва, че националните екипи за незабавно реагиране при компютърни инциденти (CERT) следва да бъдат част от ефективна мрежа, в която съответната информация се обменя в съответствие с необходимите стандарти за доверие и поверителност; отбелязва, че инициативите за предпазване, които обединяват екипите за незабавно реагиране при компютърни инциденти и другите компетентни органи по сигурността, могат да служат като полезно средство за развиване на доверието в трансграничен и междусекторен аспект; признава колко е важно наличието на ефективно и ефикасно сътрудничество между екипите за незабавно реагиране при компютърни инциденти и правоприлагащите агенции в борбата срещу киберпрестъпността;

23. Подкрепя Европейската агенция за мрежова и информационна сигурност (ENISA) в упражняването на нейните задачи по отношение на мрежовата и информационната сигурност, по-специално чрез предоставянето на насоки и съвети на държавите членки, както и чрез подпомагане на обмена на най-добри практики и на развитието на среда на доверие;

24. Подчертава необходимостта промишлеността да приложи необходимите изисквания за киберсигурност по цялата верига на стойността за продуктите на ИКТ, които се използват в транспортните мрежи и информационните системи, да извърши съответното управляване на риска, да приеме стандарти и решения по отношение на сигурността, както и да разработи най-добри практики и да осъществи обмен на информация с оглед гарантиране на сигурни кибернетични системи за пренос;

Промишлени и технологични ресурси

25. Счита, че гарантирането на висока степен на мрежова и информационна сигурност играе централна роля за повишаване на конкурентоспособността както и на доставчиците на решения, свързани със сигурността, така и на потребителите в Съюза; счита, че независимо от факта, че индустрията в областта на сигурността на информационните технологии има значителен неизползван потенциал, частните, публичните и бизнес потребителите често остават неинформирани относно цената и ползите от инвестирането в киберсигурността, и по този начин продължават да бъдат уязвими по отношение на зловредни киберзаплахи; подчертава, че използването на екипите за незабавно реагиране при компютърни инциденти е уместен фактор в тази връзка;

26. Вярва, че силното предлагане и търсене на решения за киберсигурност изисква извършването на адекватни инвестиции в академични ресурси, изследователска и развойна дейност, както и знания и капацитет за изграждане от страна на националните органи, занимаващи се с въпросите на ИКТ, за да може да бъдат стимулирани иновациите и да се осигури достатъчна осведоменост по отношение на рисковете, свързани с мрежовата и информационната сигурност, като това доведе до съгласувана европейска индустрия на сигурността;

27. Призовава институциите на Съюза и държавите членки да предприемат необходимите мерки за създаването на „единен пазар за киберсигурност“, на който потребители и доставчици ще бъдат в състояние да използват пълноценно предлаганите иновации, взаимодействия и комбинирани експертни умения и който позволява навлизането на МСП;

28. Насърчава държавите членки да разгледат възможността за извършването на съвместни инвестиции в европейската индустрия за киберсигурността, по сходен начин с този, по който това е било извършено за други индустрии, като сектора на авиацията;

Киберпрестъпност

29. Счита, че престъпните деяния в киберпространството могат да бъдат също толкова вредни за благоденствието на обществата, колкото престъпленията в реалния свят и че тези форми на престъпност често се подсилват взаимно и могат да бъдат наблюдавани например при сексуалната експлоатация на деца и организираната престъпност и изпирането на пари;

30. Отбелязва, че в някои случаи съществува връзка между законна и незаконна стопанска дейност; подчертава значението на връзката, улеснена от интернет, между финансирането на тероризма и тежката организирана престъпност; подчертава, че обществеността трябва да бъде информирана за сериозността на въвличането в киберпрестъпността и за възможността това, което на пръв поглед изглежда като „социално приемливо“ престъпление — като незаконното сваляне на филми, често да генерира големи суми пари за международните престъпни групировки;

Четвъртък, 12 септември 2013 г.

31. Изразява съгласие с Комисията във връзка с това, че същите норми и принципи, които се прилагат офлайн, се прилагат и онлайн и че борбата срещу киберпрестъпността трябва да бъде засилена с актуализирано законодателство и оперативен капацитет;

32. Счита, че предвид безграничния характер на киберпрестъпността съвместните усилия и предложеният експертен опит на равнището на Съюза, над равнището на отделните държави членки, са от особено значение и че на Евроюст, Европейския център по киберпрестъпността към Европол, екипите за незабавно реагиране при компютърни инциденти, университетите и изследователските центрове трябва следователно да бъдат предоставени подходящи средства и да се осигури капацитет за правилно функциониране в качеството на центрове за експертни умения, сътрудничество и обмен на информация;

33. Приветства енергично създаването на Европейски център по киберпрестъпността към Европол и насърчава бъдещото развитие на тази агенция и на нейната жизненоважна роля в координирането на своевременния и ефективен трансграничен обмен на информация и експертен опит, с цел подпомагане на предотвратяването, разкриването и разследването на киберпрестъпления;

34. Призовава държавите членки да гарантират, че гражданите могат лесно да получат достъп до информацията за киберзаплахите и за средствата за борба с тях; счита, че подобни насоки следва да включват информация относно това как потребителите могат да защитят своите лични данни в интернет, как да разпознаят и да докладват за случаите на „сприятеляване“, как да инсталират софтуер и защитни стени, как да управляват паролите и как да разпознават фалшивата идентичност (фишинг), примамването (фарминг) и други атаки;

35. Настоява държавите членки, които все още не са ратифицирали Конвенцията от Будапеща на Съвета на Европа за престъпления в кибернетичното пространство, да направят това незабавно; приветства разглежданата от Съвета на Европа тема за необходимостта от актуализиране на конвенцията в светлината на новите развития, за да се гарантира непрестанната ѝ ефикасност при разглеждането на въпросите, свързани с киберпрестъпността, и призовава Комисията и държавите членки да участват в това разискване; насърчава усилията за популяризиране ратификацията на конвенцията сред други държави и призовава Комисията насърчава това активно и извън Съюза;

Киберотбрана

36. Подчертава, че киберпредизвикателствата,-заплахи и –атаки излагат на риск отбраната и интересите на националната сигурност на държавите членки и че гражданският и военен подход към задачата за опазване на критичната инфраструктура следва да доведе до максимална полза и за двете чрез полагането на усилия за постигане на взаимодействие;

37. Следователно призовава държавите членки да засилят своето сътрудничество с Европейската агенция по отбрана (ЕАО) с оглед изготвянето на предложения и инициативи за капацитет в киберотбраната, въз основа на неотдавнашните инициативи и проекти; подчертава необходимостта от засилване на изследователската и развойната дейност, в това число чрез обединяване и споделяне на ресурси;

38. Отново напомня, че изготвянето на всеобхватна стратегия за киберсигуронстта на равнище ЕС следва да отчете добавената стойност на съществуващите агенции и органи, както и добрите практики, натрупани от тези държави членки, които вече са въвели свои собствени национални стратегии за киберсигурност;

39. Призовава заместник-председателя/върховния представител да включи управлението на киберкризите в планирането на управлението на кризи и подчертава необходимостта държавите членки, в сътрудничество с ЕАО, да разработят планове за опазване на мисиите и операциите на ОПСО от кибератаки; призовава ги да сформират Европейска група за киберотбрана;

40. Подчертава доброто практическо сътрудничество с НАТО в областта на киберсигурността и необходимостта от засилване на това сътрудничество, по-специално чрез тясна координация в областта на планирането, технологиите, обучението и оборудването;

41. Призовава за полагането на усилия от страна на Съюза за осъществяване на обмен с международните партньори, в т.ч. с НАТО, за набелязване на сферите на сътрудничество, избягване на дублирането и допълване на действията, когато това е възможно;

Международна политика

42. Счита, че международното сътрудничество и диалогът играят съществена роля за създаването на доверие и прозрачност и за насърчаването на висока степен на мрежова свързаност и обмен на информация на световно равнище; следователно призовава Комисията и Европейската служба за външна дейност да съставят екип от кибердипломати, чиито отговорности да включват стимулирането на диалога с държави и организации със сходни виждания по въпроса; призовава за по-активно участие от страна на ЕС в богатия набор от международни конференции на високо равнище относно киберсигурността;

43. Счита, че трябва да бъде установен баланс между съревноваващите се цели на трансграничния трансфер на данни, защитата на личните данни и киберсигурността, в съответствие с международните задължения на Съюза, по-специално съгласно ГАТС;

44. Призовава заместник-председателя/върховния представител да включи измерението за киберсигурността в рамките на външните действия на ЕС, по-специално по отношение на трети държави, за да се засили сътрудничеството, обменът на опит и на информация във връзка с действията за справяне с въпроса за киберсигурността;

45. Призовава за полагането на усилия от страна на Съюза за осъществяване на обмен с международните партньори за набелязване на сферите на сътрудничество, избягване на дублирането и допълване на действията, когато това е възможно; призовава ЗП/ВП и Комисията да бъдат проактивни в международните организации и да координират позициите на държавите членки относно начините за ефективно популяризиране на решенията и политиките в кибернетичната сфера;

46. Счита, че следва да бъдат положени усилия, за да се гарантира, че съществуващите правни инструменти, по-специално Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство, се прилагат в киберпространството; следователно счита, че понастоящем не съществува необходимост от създаването на нови правни инструменти на международно равнище; приветства, обаче, международното сътрудничество за разработването на норми на поведение за киберпространството, в подкрепа на принципите на правовата държава в киберпространството; счита, че следва да се обмисли актуализирането на съществуващите правни инструменти, с цел в тях да бъдат отразени постиженията в сферата на технологиите; счита, че правните въпроси изискват задълбочено обсъждане по въпроса за съдебното сътрудничество и съдебното преследване при транснационални наказателни дела;

47. Счита, че по-конкретно работната група ЕС-САЩ относно киберсигурността и киберпрестъпленията следва да служи за инструмент, с който ЕС и САЩ да обменят по целесъобразност най-добри практики относно политиките в областта на киберсигурността; отбелязва в тази връзка, че областите, свързани с киберсигурността, като услугите, зависещи от сигурното функциониране на мрежовите и информационните системи, ще бъдат включени в предстоящите преговори на трансатлантическото партньорство в областта на търговията и инвестициите, което следва да бъде сключено по начин, който да защитава суверенитета на ЕС и независимостта на институциите му;

48. Отбелязва, че уменията в областта на киберсигурността и способността за предотвратяване, разпознаване и ефективно противопоставяне на заплахите и злонамерените атаки, не са еднакво развити по света; подчертава, че усилията за засилване на киберустойчивостта и за провеждане на борба срещу киберзаплахите не трябва да се ограничават само сред единомислещите партньори, а следва също така да се насочат към региони с по-слабо развит капацитет, технически инфраструктури и правни рамки; счита, че в тази връзка координацията на екипите за незабавно реагиране при компютърни инциденти е от съществено значение; призовава Комисията да улесни и, при необходимост, да подпомогне третите държави, да изградят свой собствен капацитет за киберсигурност, чрез използването на подходящите средства;

Изпълнение

49. Призовава за редовни оценки на ефективността на националните стратегии за киберсигурност на най-високо политическо равнище, с цел да се гарантира адаптиране към новите световни заплахи и еднаква степен на киберсигурност в отделните държави членки;

50. Призовава Комисията да изготви ясна пътна карта, в която да бъдат определени сроковете за постигането на целите на равнището на Съюза, съгласно стратегията за киберсигурността, и тяхното оценяване; приканва държавите членки да постигнат съгласие относно подобен за осъществяването на националните дейности, съгласно тази стратегия;

Четвъртък, 12 септември 2013 г.

51. Призовава за представянето на редовни доклади от страна на Комисията, държавите членки, Европол и новосъздадения Европейски център по киберпрестъпността, Евроюст и Европейската агенция за мрежова и информационна сигурност, в които да бъде извършвана оценка на постигнатия напредък по набелязаните цели в стратегията за киберсигурността, в това число и ключовите показатели за постиженията, измерващи напредъка в прилагането;

o

o o

52. Възлага на своя председател да предаде настоящата резолюция на Съвета, на Комисията, на парламентите и правителствата на държавите членки, на Европол, на Евроюст и на Съвета на Европа.

P7_TA(2013)0377

Програма в областта на цифровите технологии за Европа: цифровите технологии — двигател на европейския икономически растеж

Резолюция на Европейския парламент от 12 септември 2013 г. относно Програма в областта на цифровите технологии за растеж, мобилност и заетост: време е за ускорени действия (2013/2593(RSP))

(2016/C 093/17)

Европейският парламент,

— като взе предвид съобщението на Комисията от 18 декември 2012 г., озаглавено „Програма в областта на цифровите технологии за Европа: цифровите технологии — двигател на европейския икономически растеж“ (COM(2012)0784),

— като взе предвид въпросите до Комисията и до Съвета относно „Програма в областта на цифровите технологии за растеж, мобилност и заетост: време е за ускорени действия“ (O-000085 — B7-0219/2013 и O-000086 — B7-0220/2013)

— като взе предвид Регламент (ЕС) № 531/2012 на Европейския парламент и на Съвета от 13 юни 2012 година относно роуминга в обществени мобилни съобщителни мрежи в рамките на Съюза ([1]),

— като взе предвид Решение № 243/2012/ЕС на Европейския парламент и на Съвета от 14 март 2012 г. за създаване на многогодишна програма за политиката в областта на радиочестотния спектър ([2]),

— като взе предвид продължаващите преговори относно Механизма за свързване на Европа и по-специално „Измененото предложение за регламент на Европейския парламент и на Съвета относно насоки за трансевропейските телекомуникационни мрежи и за отмяна на Решение № 1336/97/ЕО“ (COM(2013)0329),

— като взе предвид резолюцията си от 5 май 2010 г. относно определянето на нова програма за цифровите технологии за Европа: 2015.eu ([3])

— като взе предвид съобщението на Комисията от 27 септември 2012 г., озаглавено „Оползотворяване на потенциала на изчисленията в облак в Европа“ (COM(2012)0529),

— като взе предвид предложението от 25 януари 2012 г. за регламент на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (общ регламент относно защитата на данните) (COM(2012)0011),

---

([1]) ОВ L 172, 30.6.2012 г., стр. 10.
([2]) ОВ L 81, 21.3.2012 г., стр. 7.
([3]) ОВ C 81 E, 15.3.2011 г., стр. 45.