Вторник, 3 октомври 2017 г.

P8_TA(2017)0366

Борбата с киберпрестъпността

Резолюция на Европейския парламент от 3 октомври 2017 г. относно борбата с киберпрестъпността (2017/2068(INI))

(2018/C 346/04)

Европейският парламент,

— като взе предвид членове 2, 3 и 6 от Договора за Европейския съюз (ДЕС),

— като взе предвид членове 16, 67, 70, 72, 73, 75, 82, 83, 84, 87 и 88 от Договора за функционирането на Европейския съюз (ДФЕС),

— като взе предвид членове 1, 7, 8, 11, 16, 17, 21, 24, 41, 47, 48, 49, 50 и 52 от Хартата на основните права на Европейския съюз,

— като взе предвид Международната конвенция за правата на детето от 20 ноември 1989 г.,

— като взе предвид Факултативния протокол към Конвенцията за правата на детето относно търговията с деца, детската проституция и детската порнография от 25 май 2000 г.,

— като взе предвид Декларацията и Плана за действие от Стокхолм, приети на Първия световен конгрес срещу търговската сексуална експлоатация на деца, Глобалния ангажимент от Йокохама, приет на Втория световен конгрес срещу търговската сексуална експлоатация на деца, Ангажимента от Будапеща и плана за действие, приети на подготвителната конференция за Втория световен конгрес срещу търговската сексуална експлоатация на деца,

— като взе предвид Конвенцията на Съвета на Европа от 25 октомври 2007 г. за закрила на децата срещу сексуална експлоатация и сексуално насилие;

— като взе предвид резолюцията си от 20 ноември 2012 г. относно защитата на децата в света на цифровите технологии ([1]),

— като взе предвид своята резолюция от 11 март 2015 г. относно сексуалното насилие на деца онлайн ([2]),

— като взе предвид рамково решение 2001/413/ПВР на Съвета от 28 май 2001 г. относно борбата срещу измамите и фалшифицирането на непаричните платежни средства ([3]),

— като взе предвид Конвенцията от Будапеща за престъпления в кибернетичното пространство от 23 ноември 2001 г. ([4]) и Допълнителния протокол към нея,

— като взе предвид Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 г. относно създаване на Европейската агенция за мрежова и информационна сигурност ([5]),

([1]) ОВ C 419, 16.12.2015 г., стр. 33.
([2]) ОВ C 316, 30.8.2016 г., стр. 109.
([3]) ОВ L 149, 2.6.2001 г., стр. 1.
([4]) Съвет на Европа, European Treaty Series, брой 185, 23.11.2001 г.
([5]) ОВ L 77, 13.3.2004 г., стр. 1.

Вторник, 3 октомври 2017 г.

— 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 Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 г. относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации ([2]),

— като взе предвид Директива 2011/93/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 ([3]),

— като взе предвид Съвместното съобщение от 7 февруари 2013 г. до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите на Комисията и заместник-председателя на Комисията / върховен представител на Съюза по въпросите на външните работи и политиката на сигурност, озаглавено „Стратегия на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство“ (JOIN(2013)0001),

— като взе предвид Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за отмяна на Рамково решение 2005/222/ПВР на Съвета ([4]),

— като взе предвид Директива 2014/41/ЕС на Европейския парламент и на Съвета от 3 април 2014 г. относно Европейска заповед за разследване по наказателноправни въпроси ([5]) („Директивата за ЕЗР“),

— като взе предвид решението на Съда на Европейския съюз от 8 април 2014 г. ([6]) по преюдициално запитване, с което Директивата за запазване на данни се обявява за недействителна,

— като взе предвид резолюцията на Европейския парламент от 12 септември 2013 г. относно стратегията на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство ([7]),

— като взе предвид съобщението на Комисията от 6 май 2015 г., озаглавено „Стратегия за цифров единен пазар за Европа“ (COM(2015)0192),

— като взе предвид съобщението на Комисията от 28 април 2015 г., озаглавено „Европейска програма за сигурност“ (COM(2015)0185), и последващите доклади за напредъка по създаването на ефективен и истински Съюз на сигурност,

— като взе предвид доклада на конференцията относно юрисдикцията в киберпространството, проведена на 7 и 8 март 2016 г. в Амстердам,

— като взе предвид Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) ([8]),

([1]) ОВ L 345, 23.12.2008 г., стр. 75.
([2]) ОВ L 201, 31.7.2002 г., стр. 37.
([3]) ОВ L 335, 17.12.2011 г., стр. 1.
([4]) ОВ L 218, 14.8.2013 г., стр. 8.
([5]) ОВ L 130, 1.5.2014 г., стр. 1.
([6]) ECLI:EU:C:2014:238.
([7]) ОВ C 93, 9.3.2016 г., стр. 112.
([8]) ОВ L 119, 4.5.2016 г., стр. 1.

— като взе предвид Директива (ЕС) 2016/680 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни от компетентните органи за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказания и относно свободното движение на такива данни, и за отмяна на Рамково решение 2008/977/ПВР на Съвета ([1]),

— като взе предвид Регламент (ЕС) 2016/794 на Европейския парламент и на Съвета от 11 май 2016 г. относно Агенцията на Европейския съюз за сътрудничество в областта на правоприлагането (Европол) ([2]),

— като взе предвид решението на Комисията от 5 юли 2016 г. относно подписването на договорно споразумение относно публично-частно партньорство за промишлени изследвания и иновации в областта на киберсигурността между Европейския съюз, представляван от Комисията, и организация на заинтересовани страни (C(2016)4400),

— като взе предвид Съвместното съобщение до Европейския парламент и Съвета от 6 април 2016 г. на Комисията и заместник-председателя на Комисията / върховен представител на Съюза по въпросите на външните работи и политиката на сигурност, озаглавено „Съвместна рамка за борба с хибридните заплахи — ответни действия на Европейския съюз“ (JOIN(2016)0018),

— като взе предвид съобщението на Комисията, озаглавено „Европейската стратегия за по-добър интернет за децата“ (COM(2012)0196) и доклада на Комисията от 6 юни 2016 г., озаглавен „Окончателна оценка на многогодишната програма на ЕС за защита на децата при използването на интернет и други комуникационни технологии („По-безопасен интернет“)“ (COM(2016)0364),

— като взе предвид съвместното изявление на Европол и ENISA от 20 май 2016 г. относно законосъобразното наказателно разследване, зачитащо защитата на данните от XXI век,

— като взе предвид заключенията на Съвета от 9 юни 2016 г. относно Европейската съдебна мрежа по въпросите на киберпрестъпността,

— като взе предвид Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза ([3]),

— като взе предвид становището на ENISA от декември 2016 г., озаглавено „Криптирането — силното криптиране защитава нашата цифрова идентичност“,

— като взе предвид окончателния доклад на Групата за проучване на доказателства, локализирани в облака (Cloud Evidence Group), към Комитета по Конвенцията за престъпленията в кибернетичното пространство (T-CY), озаглавен „Достъп на наказателното правосъдие до електронни доказателства, локализирани в облака: Препоръки за размисъл от Комитета по Конвенцията за престъпленията в кибернетичното пространство (T-CY) от 16 септември 2016 г.,

— като взе предвид работата на съвместната работна група за действие в областта на киберпрестъпността (J-CAT),

— като взе предвид доклада на Европол от 28 февруари 2017 г. за оценка на заплахата от тежката и организираната престъпност (SOCTA), както и доклада от 28 септември 2016 г. за оценка на заплахата от организирана престъпност, ползваща се от интернет (IOCTA),

— като взе предвид съдебното решение на Съда на Европейския съюз по дело C-203/15 (решението TELE2) от 21 декември 2016 г. ([4]),

---

([1]) ОВ L 119, 4.5.2016 г., стр. 89.
([2]) ОВ L 135, 24.5.2016 г., стр. 53.
([3]) ОВ L 194, 19.7.2016 г., стр. 1.
([4]) Решение на Съда на Европейския съюз от 21 декември 2016 г. по дела Tele2 Sverige AB срещу Post- och telestyrelsen и Secretary of State for the Home Department срещу Tom Watson и други, C203/15, ECLI:EU:C:2016:970,

Вторник, 3 октомври 2017 г.

— като взе предвид Директива (ЕС) 2017/541 на Европейския парламент и на Съвета от 15 март 2017 г. относно борбата с тероризма и за замяна на Рамково решение 2002/475/ПВР на Съвета и за изменение на Решение 2005/671/ПВР на Съвета ([1]);

— като взе предвид член 52 от своя Правилник за дейността,

— като взе предвид доклада на комисията по граждански свободи, правосъдие и вътрешни работи и становището на комисията по вътрешния пазар и защита на потребителите (A8-0272/2017),

А. като има предвид, че киберпрестъпността нанася все повече значителни социални и икономически щети, като засяга основните права на физическите лица, създава заплахи за принципите на правовата държава в киберпространството и застрашава стабилността на демократичните общества;

Б. като има предвид, че киберпрестъпността е нарастващ проблем в държавите — членки на ЕС;

В. като има предвид, че оценката на заплахите от организираната престъпност, ползваща се от интернет, (IOCTA) за 2016 г. разкрива, че интензивността, сложността и мащабът на киберпрестъпността нарастват, че регистрираните случаи на киберпрестъпност в някои държави от ЕС надхвърлят случаите на традиционна престъпност, че тя обхваща и други области на престъпност, като например трафика на хора, че използването на инструментите за криптиране и анонимизиране за престъпни цели нараства и че атаките със софтуер за изнудване надхвърлят по брой заплахите с традиционния зловреден софтуер, например „троянските коне“;

Г. като има предвид, че през 2016 г. атаките срещу сървърите на Комисията са нараснали с 20 % в сравнение с 2015 г.;

Д. като има предвид, че уязвимостта на компютрите на атаки произтича от уникалното развитие на информационните технологии през годините, скоростта, с която нараства стопанската дейност онлайн, и липсата на действия от страна на правителствата;

Е. като има предвид, че е налице все по-разрастващ се черен пазар на компютризирано изнудване, използване на наети ботмрежи, хакерска дейност и крадени цифрови стоки;

Ж. като има предвид, че основният фокус на кибернетичните атаки продължава да бъде зловредният софтуер, като например „троянски коне“, насочени към банкови услуги, но също така се увеличава и броят и въздействието на атаките срещу системите за промишлен контрол и промишлените мрежи, които имат за цел унищожаване на критична инфраструктура и икономически структури и дестабилизиране на обществата, какъвто беше случаят с атаката със зловредния софтуер „WannaCry“ през май 2017 г., и поради това те представляват нарастваща опасност за сигурността, отбраната и други важни сектори; като има предвид, че в преобладаващата си част международните искания от страна на правоприлагащи органи за предоставяне на данни са свързани с измами и финансови престъпления, като след тях се нареждат проявите на придружена с насилие престъпност и тежките престъпления;

З. като има предвид, че макар непрекъснато нарастващата взаимосвързаност на хора, места и неща да носи много ползи, тя увеличава риска от киберпрестъпност; като има предвид, че устройства, свързани с интернет на нещата, включително интелигентни мрежи, свързани хладилници, автомобили, медицински инструменти или помощни медицински уреди, често не са толкова добре защитени като традиционните интернет устройства и следователно са идеална цел за киберпрестъпниците, особено поради факта, че режимът за актуализиране на сигурността на свързани устройства често е неравномерен или изцяло липсва; като има предвид, че устройства за „интернет на нещата“, станали обект на хакерска дейност, които разполагат с физически задействащи механизми или могат да контролират такива, могат да представляват конкретна заплаха за живота на хора;

И. като има предвид, че наличието на ефективна правна рамка за защита на данните е от съществено значение за изграждането на доверие в онлайн пространството, като позволява на потребителите и на предприятията да се възползват напълно от ползите от цифровия единен пазар и да предприемат действия срещу киберпрестъпността;

Й. като има предвид, че дружествата не могат да се справят сами с предизвикателството да направят свързания свят по-сигурен и че правителствата следва да допринасят за киберсигурността чрез регулиране и предвиждане на стимули, насърчаващи по-безопасното поведение на потребителите;

([1]) ОВ L 88, 31.3.2017 г., стр. 6.

К. като има предвид, че границите между киберпрестъпността, кибершпионажа, кибервойната, киберсаботажа и кибертероризма стават все по-неясни; като има предвид, че киберпрестъпленията могат да бъдат насочени към лица, публични или частни субекти и да обхващат широк спектър от правонарушения, включително нарушения на неприкосновеността на личния живот, нарушения на авторското право, сексуално насилие над деца онлайн, публично подбуждане към насилие и омраза, саботаж, шпионаж, финансови престъпления и измами, като измами при плащане, кражби и кражба на самоличност, както и незаконна намеса в системи;

Л. като има предвид, че в доклада за глобалните рискове за 2017 г. на Световния икономически форум мащабният инцидент със злоупотреба или кражба на данни се посочва като един от петте най-значими по степен на вероятност глобални риска;

М. като има предвид, че срещу значителен брой от киберпрестъпленията не се провежда съдебно преследване и те остават ненаказани; като има предвид значителния все още брой случаи, които не се регистрират, дългото време, необходимо за разкриване, което позволява на киберпрестъпниците да разработят множество входове/изходи или скрити възможности за проникване, затруднения достъп до електронни доказателства, проблемите при получаването на такива и тяхната допустимост в съда, както и сложните процедури и предизвикателствата по отношение на юрисдикцията, свързани с трансграничния характер на киберпрестъпленията;

Н. като има предвид, че Съветът в своите заключения от юни 2016 г. изтъкна, че предвид трансграничния характер на киберпрестъпността и общите заплахи пред киберсигурността, пред които е изправен ЕС, засиленото сътрудничество и обменът на информация между полицията и съдебните органи и експертите по киберпрестъпността са от решаващо значение за провеждането на ефективни разследвания в киберпространството и за получаването на електронни доказателства;

О. като има предвид, че директивата за запазване на данни е обявена за невалидна от Съда на ЕС с решението му от 8 април 2014 г., както и забраната за общо, неизбирателно и нецелево запазване на данни, потвърдена с произнасяне на Съда в решението му по дело TELE2 от 21 декември 2016 г., налага строги ограничения върху обработването на масиви от телекомуникационни данни, както и върху достъпа на компетентните органи до такива данни;

П. като има предвид, че в решението на Съда на ЕС ([1]) по дело Maximillian Schrems се подчертава, че масовото наблюдение е нарушение на основните права;

Р. като има предвид, че в борбата с киберпрестъпността трябва да се спазват същите процедурни и материалноправни гаранции и основни права, а именно по отношение на защитата на данните и свободата на словото, също както в борбата срещу всеки друг вид престъпност;

С. като има предвид, че децата използват интернет на все по-ранна възраст и са особено уязвими да станат жертва на сприятеляване с цел сексуална злоупотреба и други форми на сексуална експлоатация на деца в интернет (кибертормоз, сексуално насилие, сексуална принуда и изнудване), присвояване на лични данни, както и на опасните кампании, насочени към популяризиране на различни видове самонараняванията, както в случая „син кит“, и следователно се нуждаят от специална защита; като има предвид, че извършителите на онлайн правонарушения по-бързо могат да намерят и да се сприятелят с жертви посредством чатове, електронни съобщения, онлайн игри и сайтове на социални мрежи и че скритите мрежи с равноправен достъп (P2P) продължават да бъдат за извършителите на сексуални престъпления срещу деца централни платформи за достъп, комуникация, съхранение и обмен на материали относно сексуална експлоатация на деца и за проследяване на нови жертви, без да бъдат открити;

Т. като има предвид, че тенденцията на нарастване на сексуалното насилие и изнудване все още не е достатъчно изследвано или докладвани, главно поради естеството на престъплението, което причинява чувство на вина и срам у жертвите;

У. като има предвид, че насилието спрямо деца, упражнявано на живо от разстояние, се отчита като нарастваща заплаха; като има предвид, че насилието спрямо деца, упражнявано на живо от разстояние, очевидно е свързано с търговското разпространение на материали, показващи сексуална експлоатация на деца;

([1]) ECLI:EU:C:2015:650.

Ф. като има предвид, че в наскоро публикувано проучване на Националната агенция по престъпността в Обединеното кралство се констатира, че подбудите на млади хора, занимаващи се с хакерски дейности, са свързани в по-малка степен с пари и че те често атакуват компютърни мрежи, за да впечатлят приятелите си или да отправят предизвикателство към политическата система;

Х. като има предвид, че информираността относно рисковете, свързани с киберпрестъпността, се е увеличила, но предпазните мерки, предприети от страна на отделните потребители, публичните институции и предприятията, са недостатъчни, главно поради липсата на познания и ресурси;

Ц. като има предвид, че борбата с киберпрестъпността и незаконните действия онлайн не следва да засенчва положителните аспекти на свободно достъпното и отворено киберпространство, предлагащо нови възможности за споделяне на знания и насърчаване на политическото и социалното приобщаване в световен мащаб;

Общи съображения

1. подчертава, че рязкото увеличаване на софтуера за изнудване, ботмрежите и непозволеното увреждане на компютърни системи оказва въздействие върху безопасността на физическите лица, върху наличността и целостта на техните лични данни, както и върху защитата на неприкосновеността на личния живот и на основните свободи и върху надеждността на критичната инфраструктура, включително, но не само, върху снабдяването с енергия и електроенергия и финансовите структури, като например фондовите борси; припомня в този контекст, че борбата с киберпрестъпността представлява приоритет в рамките на Европейската програма за сигурност от 28 април 2015 г.;

2. подчертава необходимостта от осъвременяване на общите определения за киберпрестъпност, кибервойна, киберсигурност, кибертормоз и кибератаки, за да се гарантира, че институциите на ЕС и държавите — членки на ЕС използват общо законово определение;

3. подчертава, че борбата с киберпрестъпността следва да постави на първо и най-важно място защитата и укрепването на критичните инфраструктури и други устройства, свързани в мрежа, а не само да се изразява в осъществяване на репресивни действия;

4. отново изтъква значението на правните мерки, предприети на европейско равнище с цел хармонизиране на определенията за престъпленията, свързани с атаки срещу информационни системи и със сексуалната експлоатация на деца онлайн, и с цел задължаване на държавите членки да създадат система за запис, изготвяне и предоставяне на статистически данни за тези престъпления с оглед по-ефективно водене на борбата с тези видове престъпност;

5. призовава настоятелно онези държави членки, които все още не са направили това, да транспонират и приложат бързо и правилно Директива 2011/93/ЕС относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография; призовава Комисията да наблюдава стриктно и да гарантира нейното пълно и ефективно прилагане и да докладва своевременно своите заключения на Парламента и на компетентната парламентарна комисия, като същевременно замени Рамково решение 2004/68/ПВР на Съвета; подчертава, че на Евроюст и Европол трябва да бъдат предоставени съответни ресурси за подобряване на идентифицирането на жертвите, за борба с организираните мрежи от извършители на сексуално насилие и за ускоряване на разкриването, анализа и сезирането за материали, показващи насилие на деца както онлайн, така и офлайн;

6. изразява съжаление, че 80 % от дружества в Европа са преживели най-малко един инцидент, свързан с киберсигурността, и че кибератаките срещу предприятия често остават неразкрити или нерегистрирани; припомня, че според различни проучвания годишните разходи, които световната икономика понася във връзка с кибератаки, са значими; счита, че задължението за разкриване на пробиви в сигурността и за споделяне на информация за рисковете, въведено с Регламент (ЕС) 2016/679 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) и Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (Директива за мрежова и информационна сигурност (Директива за МИС)), ще спомогне за преодоляване на този проблем чрез предоставяне на подкрепа на предприятията, по-специално на МСП;

7. подчертава, че постоянно променящият се характер на сферата на киберзаплахите изправя всички заинтересовани страни пред сериозни правни и технологични предизвикателства; счита, че новите технологии не следва да се разглеждат като заплаха и признава, че технологичният напредък в областта на криптирането ще подобри цялостната сигурност на нашите информационни системи, включително като позволи на крайните потребители да защитават по-добре своите данни и комуникации; посочва обаче, че все още се наблюдават значителни пропуски в сигурността на комуникациите и че такива техники като многократното препращане на трафика между сървъри посредници и скритите мрежи могат да бъдат

използвани от злонамерени потребители, включително терористи и извършители на сексуални престъпления срещу деца, хакери, спонсорирани от недобронамерени чужди държави или екстремистки политически или религиозни организации с престъпни цели, по-специално за прикриване на престъпните им дейности или идентичността им, което създава сериозни предизвикателства за разследванията;

8. изразява дълбока загриженост относно неотдавнашната глобална атака със софтуер за изнудване, която изглежда засегна десетки хиляди компютри в почти 100 държави и множество организации, включително Националната здравна служба (NHS) в Обединеното кралство — жертвата с най-високо положение на този масиран удар със зловреден софтуер; в този контекст признава важната работа на инициативата No More Ransom (NMR), която предоставя над 40 безплатни инструмента за декриптиране, позволяващи на жертвите на криптиращия вирус да декриптират засегнатите си устройства;

9. подчертава, че скритите мрежи и многократното препращане на трафика между сървъри посредници („onion-routing“) предоставят също така безплатно пространство на журналисти, организатори на политически кампании и защитници на правата на човека в някои държави, за да се избегне разкриването им от репресивни държавни органи;

10. отбелязва, че използването на инструменти и услуги за киберпрестъпления от престъпни и терористични мрежи все още е ограничено; подчертава обаче, че това вероятно ще се промени в светлината на засилващите се връзки между тероризма и организираната престъпност и широкото разпространение на огнестрелни оръжия и прекурсори на взривни вещества в скритите мрежи;

11. решително осъжда всяка намеса в системи, предприета или насочвана от чужда нация или нейни агенти с цел подриване на демократичните процеси в друга държава;

12. подчертава, че трансграничните искания за конфискуване на домейн, премахване на съдържание и достъп до данни за потребителите представляват сериозно предизвикателство, което изисква незабавно действие, тъй като свързаният с това залог е огромен; в този контекст подчертава, че международните рамки в областта на правата на човека, които се прилагат както онлайн, така и офлайн, представляват материалноправна отправна точка на глобално равнище;

13. призовава държавите членки да гарантират, че жертвите на кибератаки могат да се възползват изцяло от всички права, залегнали в Директива 2012/29/ЕС, и да увеличат усилията си за идентифициране на жертвите и услуги, ориентирани към жертвите, включително чрез продължаване на подкрепата за работната група на Европол по идентифициране на жертвите; призовава държавите членки, в сътрудничество с Европол, като въпрос с неотложен характер, да създадат свързани платформи с цел да се гарантира, че всички потребители на интернет знаят как да се обърнат за помощ, в случай че бъдат незаконно атакувани онлайн; призовава Комисията да изготви проучване във връзка с възможните последици от трансгранични киберпрестъпления въз основа на Директива 2012/29/ЕС;

14. подчертава, че докладът на Европол за оценка на заплахата от организирана престъпност, ползваща се от интернет, (IOCTA) за 2014 г. посочва необходимостта от по-ефикасни и ефективни правни инструменти, които да отчитат настоящите ограничения на процеса по договорите за правна взаимопомощ, и се застъпва за по-нататъшна хармонизация на законодателството в целия ЕС, където това е целесъобразно;

15. подчертава, че киберпрестъпността накърнява сериозно функционирането на единния цифров пазар, като намалява доверието в доставчиците на цифрови услуги, накърнява трансграничните сделки и нанася сериозен ущърб на интересите на потребителите на цифрови услуги;

16. подчертава, че стратегиите и мерките за киберсигурност могат да са надеждни и ефективни само ако се базират на основните права и свободи, залегнали в Хартата на основните права на Европейския съюз, и на основните ценности на ЕС;

17. подчертава, че съществува обоснована и категорична необходимост от защита на комуникациите между физически лица и между физически лица и публични и частни организации, за да се предотвратяват киберпрестъпления; подчертава, че силно развитата криптография може да спомогне за удовлетворяване на тази потребност; подчертава освен това, че ограничаването на използването или намаляването на силата на инструментите за криптиране ще създаде уязвимост, която може да бъде експлоатирана за престъпни цели, и ще понижи доверието в електронните услуги, което на свой ред ще бъде във вреда както на гражданското общество, така и на сектора;

18. призовава за план за действие за защита на правата на децата онлайн и офлайн в киберпространството и припомня, че в борбата с киберпрестъпността правоприлагащите органи трябва да обръщат специално внимание на престъпленията срещу деца; във връзка с това подчертава необходимостта от укрепване на съдебното и полицейското сътрудничество между

държавите членки и с Европол и неговия Европейски център за борба с киберпрестъпността (EC3) с цел предотвратяване на и борба с киберпрестъпността и по-специално със сексуалната експлоатация на деца онлайн;

19. настоятелно призовава Комисията и държавите членки да въведат всички правни и съдебни мерки за борба срещу явлението на онлайн насилието срещу жени и кибертормоза; призовава по-специално ЕС и държавите членки да обединят силите си за създаването на рамка на престъпленията, която да задължава онлайн корпорациите да заличават или да спират разпространението на позорящо, обидно и унизително съдържание; призовава също да се въведе психологическа подкрепа за жени, жертви на онлайн насилие, и момичета, които са били подложени на кибертормоз;

20. подчертава, че незаконното онлайн съдържание следва да се премахва незабавно чрез надлежен съдебен процес; подчертава ролята на информационните и комуникационни технологии, доставчиците на интернет услуги и доставчиците на хостинг услуги за осигуряването на бързо и ефикасно премахване на незаконно онлайн съдържание по искане на компетентния правоприлагащ орган;

Предотвратяване

21. призовава Комисията, в контекста на преразглеждането на европейската стратегия за киберсигурност, да продължи да установява уязвимите места в мрежовата и информационната сигурност на европейската критична инфраструктура, да стимулира развитието на устойчиви системи и да направи оценка на положението по отношение на борбата с киберпрестъпността в ЕС и държавите членки с цел да се постигне по-добро разбиране на тенденциите и развитието във връзка с престъпленията в киберпространството;

22. подчертава, че устойчивостта на кибератаки е от ключово значение за предотвратяване на киберпрестъпността и поради това следва да бъде основен приоритет; призовава държавите членки да предприемат проактивни политики и действия, насочени към защита на мрежите и критичната инфраструктура, и призовава за всеобхватен европейски подход към борбата с киберпрестъпността, който да е съвместим с основните права, защитата на данните, киберсигурността, защитата на потребителите и електронната търговия;

23. приветства в това отношение инвестирането на средства на ЕС в научноизследователски проекти като публично-частни партньорства (ПЧП) в областта на киберсигурността с цел насърчаване на европейската устойчивост на кибератаки чрез иновации и изграждане на капацитет; признава по-специално усилията, положени от ПЧП в областта на киберсигурността за разработване на подходящи ответни мерки за справяне със случаите на уязвимост, свързана с „нулев ден“;

24. във връзка с това подчертава важното значение на безплатния софтуер и на софтуера с отворен код; призовава за предоставяне на повече средства от ЕС специално за безплатен софтуер и софтуер с отворен код въз основа на научни изследвания на ИТ сигурността;

25. отбелязва със загриженост, че липсват квалифицирани ИТ специалисти, работещи в областта на киберсигурността; настоятелно призовава държавите членки да инвестират в образование;

26. счита, че регулацията следва да играе по-голяма роля в управлението на рисковете за киберсигурността чрез подобрени продуктови и софтуерни стандарти за проектирането и последващите актуализации, както и чрез минимални стандарти за потребителски имена и пароли по подразбиране;

27. настоятелно призовава държавите членки да засилят обмена на информация чрез Евроюст, Европол и ENISA, както и споделянето на най-добри практики посредством Европейската мрежа на екипите за реагиране при инциденти с компютърната сигурност (CSIRT) и екипите за незабавно реагиране при компютърни инциденти (CERT) относно предизвикателствата, пред които те са изправени в борбата срещу киберпрестъпността, както и относно конкретни правни и технически решения за справяне с тази престъпност и за увеличаване на киберустойчивостта; във връзка с това призовава Комисията да насърчава ефективното сътрудничество и да подпомага обмена на информация с цел да бъдат предвиждани и управлявани потенциалните рискове съгласно предвиденото в Директивата за МИС;

28. изразява загриженост от констатацията на Европол, че по-голямата част от успешните атаки спрямо физически лица се дължи на липсата на цифрова хигиена и осведоменост сред потребителите, както и на недостатъчното внимание, което се отделя на мерките за техническа сигурност, като например сигурност при проектирането; подчертава, че потребителите са първите жертви на хардуера и софтуера със слаба сигурност;

29. призовава Комисията и държавите членки да започнат кампания за повишаване на осведомеността, която да включва всички съответни участници и заинтересовани страни, за да се създадат възможности за децата и да се предостави подкрепа на родителите, полагащите грижи лица и педагозите в разбирането и справянето с онлайн рисковете и защитата на безопасността на децата онлайн, да се подпомагат държавите членки при изготвянето на програми за предотвратяване на сексуалното насилие онлайн, да се насърчават кампании за повишаване на осведомеността относно отговорното поведение в социалните медии, както и да се насърчават основните интернет търсачки и мрежи на социалните медии да възприемат проактивен подход към защитата на безопасността на децата онлайн;

30. призовава Комисията и държавите членки да започнат кампании за повишаване на осведомеността и да насърчават добрите практики с цел да се гарантира, че гражданите, по-специално децата и други уязвими потребители, но също така централната администрация и местните органи, операторите от жизненоважно значение и участниците от частният сектор, по-специално МСП, са запознати с рисковете, свързани с киберпрестъпността, знаят как да се предпазят онлайн и как да защитят своите устройства; освен това призовава Комисията и държавите членки да насърчават практически мерки за сигурност, като например криптиране или други повишаващи сигурността и неприкосновеността на личния живот технологии и инструменти за анонимизация;

31. подчертава, че кампаниите за повишаване на осведомеността следва да бъдат съпътствани от образователни програми относно „информирано използване“ на инструментите на информационните технологии; насърчава държавите членки да включат киберсигурността, както и рисковете и последиците от използването на личните данни онлайн, в образователните програми на училищата; в този контекст подчертава усилията, положени в рамките на Европейската стратегия за интернет, по-подходящ за децата (Европейска стратегия за по-добър интернет за децата (ПИД) от 2012 г.);

32. подчертава неотложната необходимост борбата с киберпрестъпността да включва повече усилия за образование и обучение по въпросите на мрежовата и информационната сигурност (МИС) чрез въвеждане на обучение относно МИС, относно разработването на сигурен софтуер и защита на личните данни за студенти по компютърни науки, както и основно обучение по МИС за служителите в публични администрации;

33. счита, че застраховката срещу хакерски дейности в киберпространството може да представлява един от инструментите за стимулиране на действия в областта на сигурността както от страна на дружества, които са отговорни за проектирането на софтуер, така и от страна на потребителите, които да бъдат подтиквани да използват правилно софтуера;

34. подчертава, че предприятията следва да установяват уязвимите места и рискове посредством редовни оценки, да защитават своите продукти и услуги чрез незабавно отстраняване на съществуващите слабости, включително чрез политики за управление на програмите за коригиране на грешките (patches) и актуализация на защитата на данните, смекчаване на въздействието на атаките със софтуер за изнудване чрез стабилни системи за създаване на резервни копия и системно съобщаване на случаите на кибератаки;

35. настоятелно призовава държавите членки да създадат екипи за незабавно реагиране при компютърни инциденти (CERT), на които предприятията и потребителите да могат да съобщават за зловредни съобщения по електронната поща и уебсайтове, както е предвидено от Директивата за МИС, така че държавите членки да бъдат редовно информирани за инциденти, свързани със сигурността, и за мерки за борба с и смекчаване на риска за техните собствени системи; насърчава държавите членки да разгледат възможността за създаване на база данни за регистриране на всички видове киберпрестъпност и за наблюдение на развитието на свързаните с тях явления;

36. настоятелно призовава държавите членки да инвестират в мерки за по-голяма сигурност на тяхната критична инфраструктура и свързаните с нея данни, за да може тя да е устойчива на кибератаки;

Вторник, 3 октомври 2017 г.

Засилване на отговорността и задълженията на доставчиците на услуги

37. счита, че засиленото сътрудничество между компетентните органи и доставчиците на услуги е ключов фактор за ускоряване и рационализиране на процедурите за правна взаимопомощ и взаимно признаване в рамките на дадените от европейската правна рамка правомощия; призовава доставчиците на електронни съобщителни услуги, които не са установени в Съюза, да определят в писмена форма свои представители в Съюза;

38. подчертава отново, че що се отнася до интернета на предметите, производителите са ключовата отправна точка за затягането на режимите на отговорност, което ще доведе до по-добро качество на продуктите и до по-безопасна среда по отношение на външния достъп и до документирана възможност за актуализиране;

39. счита, че с оглед на иновативните тенденции и нарастващата достъпност на устройствата за интернет на предметите следва да се обърне специално внимание на сигурността на всички устройства, дори най-простите; счита, че е в интерес на производителите на хардуер и разработчиците на софтуер да инвестират в иновативни решения с цел превенция на киберпрестъпността и обмен на информация относно заплахите за киберсигурността; настоятелно призовава Комисията и държавите членки да насърчават подхода за сигурност при проектирането и настоятелно призовава сектора да включва решения за сигурност при проектирането във всички такива устройства; в този контекст насърчава частния сектор да прилага доброволни мерки, разработени въз основа на съответното законодателство на ЕС, като например Директивата за МИС, и синхронизирани с международно признатите стандарти с цел повишаване на доверието в сигурността на софтуера и устройствата, като например етикет за надеждност на интернет на предметите;

40. насърчава доставчиците на услуги да се присъединят към Кодекса за поведение за противодействие на незаконното използване на словото на омразата онлайн и насърчава Комисията и участващите дружества да продължат да си сътрудничат по този въпрос;

41. припомня, че Директива 2000/31/ЕО на Европейския парламент и на Съвета от 8 юни 2000 г. за някои правни аспекти на услугите на информационното общество, и по-специално на електронната търговия на вътрешния пазар ([1]) (Директива за електронната търговия)освобождава посредниците от отговорност за съдържанието само ако те имат неутрална и пасивна роля, що се отнася до съдържанието, което бива предавано и/или хоствано, но изисква също така бърза реакция за премахване или прекъсване на достъпа до съдържание, когато даден посредник е знаел действително за съществуването на нарушение или незаконна дейност или информация;

42. подчертава абсолютната необходимост от защита на базите данни в областта на правоприлагането от инциденти, свързани със сигурността, и незаконен достъп, тъй като това засяга физическите лица; изразява загриженост във връзка с екстериториалния обсег на правоприлагащите органи при достъпа до данни в контекста на наказателни разследвания и подчертава необходимостта от прилагане на строги правила по този въпрос;

43. счита, че въпросите, свързани с незаконни онлайн дейности, трябва да бъде решавани по бърз и ефикасен начин, включително чрез процедури за премахване на съдържание, ако то не е или е престанало да бъде необходимо за откриването, разследването и наказателното преследване; припомня, че когато премахването не е възможно, държавите членки могат да предприемат необходими и пропорционални мерки за блокиране на достъпа до такова съдържание от територията на Съюза; подчертава, че тези мерки трябва да са в съответствие със съществуващите правни и съдебни процедури, както и с Хартата, и също така трябва да бъдат предмет на подходящи предпазни мерки, включително възможността за съдебна защита;

44. подчертава ролята на доставчиците на цифрови услуги на информационното общество за осигуряването на бързо и ефикасно премахване на незаконно онлайн съдържание по искане на компетентния правоприлагащ орган и приветства напредъка, постигнат в тази насока, включително чрез приноса на интернет форума на ЕС; подчертава необходимостта от по-силен ангажимент и сътрудничество от страна на компетентните органи и доставчиците на услуги на информационното общество за постигане на бързо и ефективно премахване на съдържание от страна на сектора и избягване на блокирането на незаконно съдържание чрез правителствени мерки; призовава държавите членки да търсят правна отговорност на платформи, които не съответстват на изискванията; отново подчертава, че мерки за премахване на незаконно онлайн съдържание, за които се поставят определени условия, следва да се допускат единствено ако в националните процедурни правила е предвидена възможност потребителите да предявят правата си пред съда, след като научат за тези мерки;

45. подчертава, че в съответствие с резолюцията на Парламента от 19 януари 2016 г., озаглавена „Към Акт за единния цифров пазар“ ([2]), ограничената отговорност на посредниците е от съществено значение за защитата на отворения характер на интернет, основните права, правната сигурност и иновациите; приветства намерението на Комисията да предостави насоки относно процедурите за уведомяване и премахване, за да се окаже съдействие на онлайн платформите при изпълнението на

([1]) ОВ L 178, 17.7.2000 г., стр. 1.
([2]) Приети текстове, P8_TA(2016)0009.

техните отговорности и на правилата относно отговорността, определени в Директивата за електронната търговия (2000/31/ЕО), с цел да се увеличи правната сигурност и да се повиши доверието на потребителите; настоятелно призовава Комисията да представи законодателни предложения по тези въпроси;

46. призовава за прилагане на подхода „следвай парите“, както е посочено в резолюцията на Парламента от 9 юни 2015 г., озаглавена „Към обновен консенсус относно гарантиране на спазването на правата върху интелектуалната собственост: план за действие на ЕС“ ([1]), въз основа на регулаторната рамка на Директивата за електронна търговия и Директивата относно упражняването на права върху интелектуалната собственост;

47. подчертава решаващото значение на осигуряването на непрекъснато и специализирано обучение и психологическа подкрепа за модераторите на съдържание в частни и публични субекти, които отговарят за оценката на нежелателно или незаконно онлайн съдържание, тъй като те следва да се считат за лицата, които реагират първи в тази област;

48. приканва доставчиците на услуги да предвидят ясни видове сигнализиране, както и ясно определена административна инфраструктура, която да е в състояние да осигури бързо и подходящо проследяване на подадените сигнали;

49. приканва доставчиците на услуги да работят за засилване на дейностите за повишаване на осведомеността за онлайн рисковете, особено сред децата, чрез разработването на интерактивни инструменти и информационни материали;

Засилване на полицейското и съдебното сътрудничество

50. изразява загриженост, че значителен брой киберпрестъпления остават ненаказани; изразява съжаление, че използването на технологии като NAT CGN от доставчиците на интернет услуги сериозно вреди на разследванията, като прави технически невъзможно точното идентифициране на потребителя на даден IP адрес, а оттам и определянето на носителя на отговорността за онлайн престъпленията; подчертава необходимостта да се даде възможност на правоприлагащите органи да имат законен достъп до съответната информация при ограничените обстоятелства, когато този достъп е необходим и пропорционален поради съображения за сигурност и правосъдие; подчертава, че на съдебните и правоприлагащите органи трябва да бъде предоставен достатъчен капацитет за провеждане на законни разследвания;

51. настоятелно призовава държавите членки да не налагат никакви задължения на доставчиците на криптиране, които биха довели до отслабване или нарушаване на сигурността на техните мрежи и услуги, като например задължение за създаване или улесняване на скрити възможности за достъп („задни вратички“); подчертава, че трябва да бъдат предложени практически решения, както чрез законодателството, така и чрез непрекъснатото техническо развитие, когато откриването им е наложително за правосъдието и сигурността; призовава държавите членки да си сътрудничат, като се консултират със съдебните органи и Евроюст, при сближаването на условията за правомерно използване на средства за разследване онлайн;

52. подчертава, че законното прихващане може да бъде високоефективна мярка за борба с незаконното хакерство, при условие че е необходимо и пропорционално и че се спазват изцяло основните права, законодателството на ЕС в областта на защитата на данните и съдебната практика; призовава всички държави членки да използват възможностите за законно прихващане, насочено към заподозрени лица, да установят ясни правила относно процеса на даване на разрешения за законно прихващане, включително ограничения по отношение на употребата и продължителността на законния хакерски инструмент, да създадат механизъм за наблюдение и да осигурят ефективни правни средства за защита за лицата, към които са насочени хакерските дейности;

53. насърчава държавите членки да се ангажират със специалистите, работещи в областта на сигурността на ИКТ, и да го стимулира да поемат по-активна роля в „етичните хакерски дейности“ („white hat hacking“) и да докладват незаконно съдържание, като например материали, съдържащи сексуална злоупотреба с деца;

54. насърчава Европол да създаде система за подаване на анонимни сигнали от скритите мрежи, която ще позволи на отделни лица да сигнализират за незаконно съдържание, например изображения на материали, съдържащи сексуална злоупотреба с деца, като използват технически защитни мерки, подобни на тези, които се прилагат от много медийни организации, които използват такива системи, за да улеснят предаването на чувствителни данни на журналистите по начин, който позволява по-голяма степен на анонимност и сигурност, отколкото тази на традиционната електронна поща;

([1]) ОВ C 407, 4.11.2016 г., стр. 25.

55. подчертава необходимостта от свеждане до минимум на рисковете за неприкосновеността на личния живот на интернет потребителите поради изтичане на данни от съответния софтуер за проникване или инструментите, използвани от правоприлагащите органи като част от техните законни разследвания;

56. подчертава, че съдебните и правоприлагащите органи трябва да разполагат с достатъчен капацитет и финансови средства, които да им позволят да реагират ефективно на киберпрестъпността;

57. подчертава, че разнообразието от отделни, териториално определени национални юрисдикции поражда трудности при определянето на приложимото право в случаи на транснационално взаимодействие и води до правна несигурност, като по този начин възпрепятства трансграничното сътрудничество, което е необходимо за ефективно справяне с киберпрестъпността;

58. подчертава необходимостта от разработване на практическа основа за общ подход на ЕС по отношение на юрисдикцията в киберпространството, изразена по време на неформалното заседание на министрите на правосъдието и вътрешните работи на 26 януари 2016 г.;

59. във връзка с това подчертава необходимостта от разработване на общи процедурни стандарти, които могат да определят териториални фактори, представляващи основание за приложимото право в киберпространството, и да определят кои действия по разследване могат да бъдат използвани независимо от географските граници;

60. признава, че такъв общ европейски подход, при който трябва да се спазват основните права и правото на неприкосновеност на личния живот, ще изгради доверие сред заинтересованите страни, ще съкрати забавянията при обработването на трансграничните искания за информация, ще установи оперативна съвместимост между разнородните участници и ще даде възможност за включване на изисквания за справедлив съдебен процес в оперативните рамки;

61. счита, че в дългосрочен план следва също така да бъдат разработени общи процедурни стандарти за компетентността за правоприлагане в киберпространството на световно равнище; в тази връзка приветства работата на Групата за доказателства, локализирани в облака, (Cloud Evidence Group) към Съвета на Европа;

Електронни доказателства

62. подчертава, че един общ европейски подход спрямо наказателното правосъдие в киберпространството е от приоритетно значение, тъй като той ще подобри прилагането на принципите на правовата държава в киберпространството и ще улесни получаването на електронни доказателства в наказателните производства, като също така ще допринесе за много по-бързо приключване на делата, отколкото понастоящем;

63. подчертава необходимостта от намиране на начини за по-бързо осигуряване и получаване на електронни доказателства, както и значението на тясното сътрудничество между правоприлагащите органи, включително чрез по-широко използване на съвместните екипи за разследване, трети държави и доставчици на услуги, извършващи дейност на европейска територия, в съответствие с Общия регламент относно защитата на данните ((ЕС) 2016/679), Директива (ЕС) 2016/680 (Директивата във връзка с полицейското сътрудничество) и съществуващите споразумения за правна взаимопомощ; подчертава, че е необходимо да се установят единни точки за контакт във всички държави членки и да се оптимизира използването на съществуващите точки за контакт, тъй като това ще улесни достъпа до електронни доказателства, както и споделянето на информация, ще подобри сътрудничеството с доставчиците на услуги и ще ускори процедурите по споразуменията за правна взаимопомощ;

64. признава, че сегашната фрагментирана правна рамка може да създаде предизвикателства за доставчиците на услуги, които се стремят да отговарят на искания за информация от страна на правоприлагащи органи; призовава Комисията да предложи европейска правна рамка за електронните доказателства, включително хармонизирани правила за определяне на статута на даден доставчик като национален или чуждестранен, и да наложи задължение на доставчиците на услуги да отговарят на искания за информация от други държави членки, които се основават на надлежно съдопроизводство и са в съответствие с европейската заповед за разследване (ЕЗР), като се взема предвид принципът на пропорционалност, за да се избегне неблагоприятното въздействие върху упражняването на свободата на установяване и свободата на предоставяне на услуги, и се осигуряват адекватни защитни мерки с оглед на установяването на правна сигурност, както и на повишаването на способността на доставчиците на услуги и на посредниците да отговорят на искания за информация от страна на правоприлагащите органи;

65. подчертава необходимостта рамката за електронните доказателства да включва достатъчно гаранции за правата и свободите на всички засегнати страни; подчертава, че това следва да включва изискване исканията за електронни доказателства да бъдат насочвани на първо място към администраторите или притежателите на лични данни, за да се осигури спазването на техните права и на правата на лицата, за които се отнасят личните данни (например законно признато право да искат запазване на поверителност, както и да потърсят правна защита в случай на непропорционален или незаконен поради

друга причина достъп); подчертава също така необходимостта да се гарантира, че правната рамка защитава доставчиците и всички други страни от искания за информация, които биха могли да създадат стълкновение на закони или да накърнят по друг начин суверенитета на други държави;

66. призовава държавите членки да приложат изцяло Директива 2014/41/ЕС относно Европейска заповед за разследване по наказателноправни въпроси („Директивата за ЕЗР“) за целите на ефективното обезпечаване и получаване на електронни доказателства в ЕС, както и да включат конкретни разпоредби, свързани с киберпространството, в своите национални наказателни кодекси, за да се улесни допустимостта на електронните доказателства в съда и да се дадат по-ясни насоки на съдиите по отношение на санкционирането на киберпрестъпленията;

67. приветства текущата работа на Комисията за създаване на платформа за сътрудничество със сигурен канал за комуникация за цифров обмен на Европейски заповеди за разследване (ЕЗР) и за електронни доказателства и отговори между съдебните органи на ЕС; приканва Комисията, съвместно с държавите членки, Евроюст и доставчиците на услуги, да провери и съгласува формулярите, инструментите и процедурите за искания за обезпечаване и получаване на електронни доказателства, за да се улесни установяването на автентичността, да се гарантира бързината на процедурите и да се повишат прозрачността и отчетността на процеса на обезпечаване и получаване на електронни доказателства; призовава Агенцията на Европейския съюз за обучение в областта на правоприлагането (CEPOL) да разработи модули за обучение относно ефективното използване на настоящите рамки за осигуряване и получаване на електронни доказателства; подчертава в този контекст, че съгласуването на политиките на доставчиците на услуги ще спомогне за намаляване на разнородността на подходите, по-специално що се отнася до процедурите и условията за предоставяне на достъп до исканите данни;

Изграждане на капацитет на европейско равнище

68. посочва, че инцидентите в последно време ясно показват изключителната уязвимост на ЕС — и по-специално на институциите на ЕС, националните правителства и парламенти, големите европейски дружества, европейските ИТ инфраструктури и мрежи — на високотехнологични атаки с използване на сложен и зловреден софтуер; призовава Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) непрекъснато да оценява равнището на заплаха и призовава Комисията да инвестира в ИТ капацитет, както и в защитата и устойчивостта на критичната инфраструктура на институциите на ЕС, за да се намали уязвимостта на ЕС на сериозни кибератаки, произхождащи от големите престъпни организации, организирани от определени държави нападения или терористични групи;

69. признава важния принос на Европейския център за борба с киберпрестъпността (EC3) към Европол и на Евроюст, както и на ENISA, в борбата срещу киберпрестъпността;

70. призовава Европол да подпомага националните правоприлагащи органи при създаването на сигурни и адекватни средства за предаване;

71. изразява съжаление относно факта, че понастоящем не съществуват никакви стандарти на ЕС за обучение и сертифициране; признава, че бъдещите тенденции в областта на киберпрестъпността изискват все по-високо равнище на експертни познания от специалистите; приветства факта, че съществуващите инициативи, като например Европейската група за обучение и образование в областта на киберсигурността, проекта „Обучение на обучаващите лица“ и дейностите по обучение в рамките на цикъла на политиката на ЕС за борба с организираната и тежката международна престъпност, вече проправят пътя към преодоляване на недостига на експертни познания на равнището на ЕС;

72. призовава CEPOL и Европейската мрежа за съдебно обучение да разширят предлагането на обучения, посветени на теми, свързани с киберпрестъпността, на компетентните правоприлагащи и съдебни органи в Съюза;

73. подчертава, че броят на случаите на киберпрестъпност, отнесени до Евроюст, се е увеличил с 30 %; призовава за разпределяне на достатъчно средства, като при необходимост бъдат създадени повече длъжности, за да се даде възможност на Евроюст да се справи с нарастващия обем работа във връзка с киберпрестъпността, както и да развие и засили допълнително подкрепата си за националните прокурори, работещи в областта на киберпрестъпността, при трансгранични случаи, включително чрез създадената наскоро Европейска съдебна мрежа по въпросите на киберпрестъпността;

74. отправя искане да бъде преразгледан мандатът на ENISA, както и да бъдат укрепени националните агенции по киберсигурността; призовава за укрепване на ENISA от гледна точка на задачите, ресурсите и персонала на агенцията; подчертава, че новия мандат следва да включва по-силни връзки с Европол и заинтересованите страни от сектора, за да се даде възможност на агенцията да окаже по-добра подкрепа на компетентните органи в борбата срещу киберпрестъпността;

75. изисква от Агенцията за основните права (FRA) да изготви практически и подробен наръчник, който да предоставя насоки на държавите членки относно надзора и контрола;

По-добро сътрудничество с трети държави

76. подчертава важността на тясното сътрудничество с трети държави в световната борба срещу киберпрестъпността, включително чрез обмен на най-добри практики, съвместни разследвания, изграждане на капацитет и правна взаимопомощ;

77. призовава държавите членки, които още не са направили това, да ратифицират и приложат Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство от 23 ноември 2001 г. (Конвенцията от Будапеща), както и допълнителните протоколи към нея, и в сътрудничество с Комисията да насърчават прилагането ѝ в рамките на съответните международни форуми;

78. подчертава своята сериозна загриженост относно работата в рамките на Комитета на Съвета на Европа по Конвенцията за престъпления в кибернетичното пространство относно тълкуването на член 32 от Конвенцията от Будапеща относно трансграничния достъп до съхраняваните компютърни данни („доказателства, локализирани в облака“) и се противопоставя на сключването на допълнителен протокол или насоки, предназначени да разширят обхвата на тази разпоредба извън рамките на настоящия режим, установен от тази конвенция, който вече представлява важно изключение от принципа на териториалност, тъй като това би могло да доведе до безпрепятствен достъп от разстояние от страна на правоприлагащи органи до сървъри и компютри, намиращи се в други юрисдикции, без да се прибягва до споразумения за правна взаимопомощ и други инструменти за съдебно сътрудничество, въведени с цел гарантиране на основните права на личността, включително защитата на личните данни и безпристрастния съдебен процес, и по-специално Конвенция № 108 на Съвета на Европа;

79. изразява съжаление във връзка с факта, че в областта на киберпрестъпността не съществуват правно обвързващи международни инструменти, и настоятелно призовава държавите членки и европейските институции да работят за създаване на спогодба по този въпрос;

80. призовава Комисията да предложи варианти за инициативи с цел подобряване на ефикасността и насърчаване на използването на споразуменията за правна взаимопомощ, за да се противодейства на поемането на извънтериториална компетентност от трети държави;

81. призовава държавите членки да осигурят достатъчен капацитет за обработването на исканията за правна взаимопомощ, свързани с разследвания в киберпространството, и да разработят подходящи програми за обучение за служителите, които отговарят за обработването на тези искания;

82. подчертава, че споразуменията за стратегическо и оперативно сътрудничество между Европол и трети държави улесняват както обмена на информация, така и практическото сътрудничество;

83. отбелязва факта, че най-голям брой искания за информация от страна на правоприлагащи органи са изпратени до САЩ и Канада; изразява загриженост, че процентът на оповестяване от големите доставчици на услуги от САЩ в отговор на искания за информация от страна на европейски органи на наказателното правосъдие е под 60 %, като признава, че съгласно глава V от Общия регламент относно защитата на данните споразуменията за правна взаимопомощ и другите международни споразумения са предпочитаният механизъм за осигуряване на достъп до лични данни;

84. призовава Комисията да предложи конкретни мерки за защита на основните права на заподозрените или обвиняемите лица при обмен на информация между европейските правоприлагащи органи и трети държави, по-специално гаранции по отношение на бързото получаване въз основа на съдебно решение на относими доказателства, свързана с абоната информация, както и подробни метаданни и данни за съдържание (ако не са криптирани) от правоприлагащите органи и/или доставчиците на услуги с оглед подобряване на правната взаимопомощ;

85. призовава Комисията, в сътрудничество с държавите членки, свързаните европейски органи и при необходимост с трети държави, да разгледа нови начини за ефективно осигуряване и получаване на електронни доказателства, съхранявани в трети държави, при пълно спазване на основните права и законодателството на ЕС в областта на защитата на данните, чрез ускоряване и рационализиране на използването на процедурите за правна взаимопомощ и където е приложимо, за взаимно признаване;

86. изтъква важността на Центъра на НАТО за реагиране на киберинциденти;

87. призовава всички държави членки да вземат участие в Световния форум за експертни киберпознания (GFCE), за да се улесни създаването на партньорства с цел изграждане на капацитет;

88. подкрепя помощта за изграждане на капацитет, предоставяна от ЕС на държавите от източното съседство, като се има предвид, че много кибератаки произхождат от тях;

o

o o

89. възлага на своя председател да предаде настоящата резолюция на Съвета и на Комисията.