ЕВРОПЕЙСКА КОМИСИЯ

Брюксел, 28.3.2012 г.
COM(2012) 140 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО СЪВЕТА И ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ

Борбата с престъпността в дигиталната ера: създаване на Европейски център по киберпрестъпност

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО СЪВЕТА И ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ

Борбата с престъпността в дигиталната ера: създаване на Европейски център по киберпрестъпност

1. ВЪВЕДЕНИЕ: ОТГОВОРЪТ НА ЕВРОПА НА ПРЕСТЪПЛЕНИЯТА ОТВЪД ДЪРЖАВНИТЕ ГРАНИЦИ

Интернет се превърна в неделима и необходима част от нашето общество и икономика. Осемдесет процента от младите европейци поддържат връзка помежду си и със света чрез социалните мрежи онлайн[1] и приблизително 8 трилиона долара сменят притежателя си в глобален мащаб всяка година чрез електронната търговия[2]. Все по-голяма част от ежедневния ни живот и бизнес трансакциите се извършват онлайн и престъпната дейност също се преориентира – над един милион души в целия свят стават жертва на престъпления в кибернетичното пространство всеки ден[3]. Престъпната дейност онлайн варира от продажба на откраднати кредитни карти само за едно евро през кражба на идентичност и сексуално малтретиране на деца до сериозни атаки в кибернетичното пространство срещу институции и инфраструктура.

Престъпленията в кибернетичното пространство струват много скъпо на обществото. Според доклад, публикуван неотдавна, жертвите на престъпления в кибернетичното пространство по цял свят губят около 388 милиарда долара всяка година, което прави този род престъпления по-доходоносни от световната търговия с марихуана, кокаин и хероин взети заедно[4]. Въпреки че към подобна информация трябва да се подхожда предпазливо заради различните тълкувания на това какво се разбира под киберпрестъпност, което може да доведе до различни оценки на щетите, смята се, че киберпрестъпността е незаконна дейност, която носи високи печалби при нисък риск, става все по-разпространена и нанася все повече щети. В момент, когато стимулирането на икономическия растеж е от първостепенно значение, засилването на борбата срещу киберпрестъпността е от съществено значение за запазване на доверието на гражданите и бизнеса в безопасната онлайн комуникация и търговия. Това ще допринесе и за постигане на целите за растеж, заложени в стратегията „Европа 2020“[5] и Програмата в областта на цифровите технологии за Европа[6].

Свободата в интернет е ключовият фактор, който обяснява цифровата революция през последните години. Отвореното интернет пространство не познава национални граници, нито единна световна управленска структура. Но докато насърчаваме и

---

1 Евростат, Достъп и използване на интернет, 14 декември 2010 г.

2 McKinsey Global Institute, Интернет има значение: огромното въздействие на мрежата върху растежа, работните места и просперитета. Доклад от май 2011, достъпен на 8 февруари 2012 г.

3 Norton Cybercrime Report 2011, Symantec, 7 септември 2011 г., достъпен на 6 януари 2012 г.

4 Ibid.

5 „Европа 2020 — Стратегия за интелигентен, устойчив и приобщаващ растеж“, COM (2010) 2020, 3 март 2010 г.

6 Програма в областта на цифровите технологии за Европа; COM(2010) 245 окончателен, 26 август 2010 г.

защитаваме онлайн свободата в съответствие с Хартата на основните права на Европейския съюз, трябва да се стремим и да защитаваме гражданите от организираните престъпни групи, които искат да се възползват от тази отвореност. Нито едно друго престъпление не се простира до такава степен извън държавните граници както киберпрестъпленията и затова е необходимо правоприлагащите органи да възприемат координиран и съгласуван подход, надхвърлящ националните граници, като включат заинтересовани страни от публичния и частния сектор. Именно тук ЕС може и действително има съществен принос.

Европейският съюз разработи различни инициативи за борба с киберпрестъпността. Сред тях са Директива 2011 за борба срещу сексуалната експлоатация на деца онлайн и детската порнография, както и Директивата за атаките срещу информационните системи, която се съсредоточава върху санкционирането на използването на инструменти за извършване на престъпления в кибернетичното пространство, особено ботнет[7], и трябва да бъде приета през 2012 г. Европол засили дейностите си срещу киберпрестъпността, като изигра ключова роля в неотдавнашната операция „Спасение“, при която полицията арестува 184 предполагаеми извършители на сексуални престъпления срещу деца и идентифицира над 200 деца — жертви на малтретиране, при едно от най-мащабните по рода си разследвания на правоприлагащи агенции в световен мащаб. Благодарение на работата на анализаторите на Европол, които пробиха сигурността на ключов сървър от компютърната мрежа, бяха разкрити самоличността и действията на предполагаемите извършители.

Борбата срещу киберпрестъпността, в която основен правен инструмент е Конвенцията на Съвета на Европа за престъпления в кибернетичното пространство[8], продължава да бъде върховен приоритет. Това е посочено в цикъла на политиката на ЕС за борба с организираната и тежката международна престъпност[9] и представлява неделима част от усилията за разработването на ключова стратегия на ЕС за засилване на киберсигурността. ЕС работи в тясно сътрудничество с международни партньори, като например работната група ЕС-САЩ по кибернетичната сигурност и престъпленията в кибернетичното пространство.

Като се остави настрана този напредък, все още има някои препятствия пред ефективното разследване на престъпленията в кибернетичното пространство и наказателното преследване на извършителите на престъпления на европейско ниво. Те включват: границите на юрисдикция, недостатъчни способности за обмен на разузнавателни данни, технически трудности при проследяването на произхода на извършителите на престъпления в кибернетичното пространство, различен капацитет за разследване и анализ, недостиг на квалифицирани кадри и непоследователно

---

[7] Предложение за Директива на Европейския парламент и на Съвета относно атаките срещу информационните системи, COM (2010) 517 окончателен, 30 септември 2010 г. Ботнет са мрежи от компютри, които са били заразени от злонамерен софтуер, който може да бъде активиран от разстояние за извършване на определени действия, включително кибератаки.

[8] Конвенция на Съвета на Европа за престъпления в кибернетичното пространство, Будапеща, 23 ноември 2001г., известна още като Конвенцията от Будапеща. Конвенцията е придружена от *Допълнителен протокол* относно обявяването за престъпления на расистки и ксенофобски действия, извършени чрез информационни системи.

[9] Цикълът на политиката на ЕС за борба с организираната и тежката международна престъпност за периода 2011—2013 г. включва осем приоритета, един от които е да се засили борбата с киберпрестъпността и използването на интернет за престъпни цели от страна на организирани престъпни групи.

сътрудничество с други заинтересовани страни, отговарящи за кибернетичната сигурност. По линия на Инструмента за стабилност ЕС предприема действия във връзка с бързо променящите се транснационални заплахи, свързани с киберпрестъпността в развиващите се държави и в държави в период на преход, където често липсват нужният капацитет за борба с този вид организирана престъпност.

В отговор на тези предизвикателства Комисията обяви намерението си да създаде Европейски център по киберпрестъпност като приоритет, залегнал в Стратегията за вътрешна сигурност[10]. След като проведе проучване за осъществимостта на подобен център[11] по искане на Съвета[12], Комисията предложи да се създаде Европейски център по киберпрестъпност, който ще бъде част от Европол и ще действа като централно звено в борбата срещу киберпрестъпността в ЕС. В това съобщение, изготвено въз основа на проучването за осъществимостта, се очертават основните функции на Европейския център по киберпрестъпност и се обяснява защо той трябва да бъде в рамките на Европол и как може да бъде създаден. Отражението върху ресурсите ще трябва да бъде оценено допълнително и представено на Комисията, преди центърът да започне да функционира напълно. Създаването на центъра ще бъде отразено, както следва, в предстоящото преразглеждане на правното основание за Европол.

2. ПРЕДЛОЖЕНИЕ ЗА СЪЗДАВАНЕТО НА ЕВРОПЕЙСКИ ЦЕНТЪР ПО КИБЕРПРЕСТЪПНОСТ

За да може Европейският център по киберпрестъпност да има добавена стойност, като едновременно с това се зачита принципът на субсидиарност, се предлага той да се съсредоточи върху следните основни видове киберпрестъпления:

i) Престъпления в кибернетичното пространство, извършени от организирани престъпни групи, по-специално такива, при които се трупат големи печалби, като онлайн измами;

ii) Престъпления в кибернетичното пространство, които причиняват тежки щети на жертвите, като сексуалната експлоатация на деца онлайн; както и

iii) Престъпления в кибернетичното пространство (включително кибератаки), които засягат ключова инфраструктура и информационни системи в Съюза[13].

Като се има предвид постоянно променящият се характер на киберпрестъпността, трябва да има възможност за реакция както в отговор на изискванията на държавите членки, така и при появата на нови заплахи за Съюза, произтичащи от киберпрестъпността.

---

10 „До 2013 г. ЕС ще създаде…център по киберпрестъпност, чрез който държавите членки и институциите на ЕС ще могат да изградят оперативен и аналитичен капацитет за разследвания и сътрудничество с международните партньори“, Стратегия за вътрешна сигурност на ЕС в действие: пет стъпки към една по-сигурна Европа, COM(2010) 673 окончателен, 22 ноември 2010 г.

11 Feasibility study for a European Cybercrime Centre, Final Report, February 2012.

12 Заключения на Съвета относно план за действие за изпълнение на съгласуваната стратегия за борба с престъпността, Съвет по общи въпроси, Люксембург, 26 април 2010 г.

13 Както е посочено в Директива 2008/114/ЕО на Съвета от 8 декември 2008 г. Тази директива в момента се преразглежда, центърът ще вземе предвид бъдещите изменения.

2.1. Основни функции и очаквания от Европейския център по киберпрестъпност

Европейският център по киберпрестъпност трябва да има четири основни функции:

а) Да служи като централно информационно звено на европейско ниво по въпросите на киберпрестъпността

Функцията „обединяване на информация“ ще даде възможност за събиране на информация за престъпленията в кибернетичното пространство от възможно най-широк кръг публични, частни и отворени източници, което ще обогати наличната база данни на полицията. Това би трябвало да доведе до постепенното запълване на съществуващите пропуски в данните на службите, отговарящи за кибернетичната сигурност и за борбата с престъпленията в кибернетичното пространство. Събраната информация ще се отнася до дейностите, свързани с престъпления в кибернетичното пространство, методите и заподозрените. Тя ще послужи както за задълбочаване на знанията за престъпленията в кибернетичното пространство, така и за тяхната превенция, разкриване и наказателно преследване и за насърчаването на подходящи връзки между правоприлагащите органи, екипа за незабавно реагиране при компютърни инциденти (CERT) на общността и специалисти по сигурността от частния сектор в областта на информационните и комуникационни технологии (ИКТ). Обменът на информация трябва да се извършва в съответствие със споразумения за поверителност и правила между различните страни.

Функцията „обединяване на информация“ ще бъде полезна и за подобряване на сигнализирането за престъпления в кибернетичното пространство и обмена на информация. Комисията би искала държавите членки да изискват тежките нарушения в кибернетичното пространство да бъдат докладвани на националните правоприлагащи органи[14]. Това ще даде възможност на националните полицейски служби да предоставят информация за тежки престъпления в кибернетичното пространство по-последователно на Европейския център по киберпрестъпност, който от своя страна ще препредава тази информация, така че колеги в други държави членки да бъдат информирани, ако са си набелязали същата цел, и да могат да се възползват от информацията, с която другите разполагат, при своите разследвания.

Целта е да се изгради по-мащабна представа за киберпрестъпността в Европа с течение на времето, така че да се изготвят висококачествени стратегически доклади за тенденциите и заплахите, да има по-голяма информираност въз основа на изчерпателни данни за престъпността и да се подобри оперативното разузнаване от информационна база, черпеща данни от различни източници.

б) Да обедини европейските експертни знания по киберпрестъпността, за да помогне на държавите членки при изграждането на техен собствен капацитет

Европейският център по киберпрестъпност ще помага на държавите членки с експертни знания и обучения за борба срещу киберпрестъпността. Основният фокус е върху правоприлагащите органи, но обучения ще бъдат предлагани и на съдебната власт.

---

[14] Като тези, посочени в членове 3—7 в представеното Предложение за директива относно атаките срещу информационните системи, COM(2010) 517 окончателен, 30 септември 2010 г.

Съществуващите инициативи на Европол, CEPOL и държавите членки ще бъдат рационализирани след обстоен анализ на нуждите, така че да се осигури по-добра координация и допълване. Това обучение ще варира от предоставянето на задълбочени технически знания до по-широки знания за изграждането на капацитет, предназначени за полицаи, прокурори и съдии за работа с престъпления в кибернетичното пространство.

Ще бъде създадено бюро по киберпрестъпност с цел обмен на най-добри практики и знания, както и насърчаване на сътрудничеството и отговаряне на запитвания от страна на държавите членки и правоприлагащите органи, съдебната система, частния сектор и организации на гражданското общество, като например при случаи на атаки в кибернетичното пространство или нов вид онлайн измами.

Бюрото по киберпрестъпност ще оказва подкрепа и ще съветва експертни групи по киберпрестъпност, включително Работната група на Европейския съюз по киберпрестъпността и експерти в борбата срещу сексуалната експлоатация на деца онлайн. То ще установи сътрудничество с развиващата се мрежа от центрове за високи постижения в областта на киберпрестъпността, какъвто е 2Centre, както и с изследователската общност.

Европейският център по киберпрестъпност ще подпомага също така държавите членки в усилията им да разработят и внедрят онлайн приложение, основаващо се на утвърдени стандарти, което да сигнализира за престъпления в кибернетичното пространство, да свърже каналите за докладване от различни участници (компании, национални/правителствени CERT групи, граждани и т.н.) към националните правоприлагащи органи, както и от националните правоприлагащи органи към центъра.

Европейският център по киберпрестъпност ще установи контакти и ще улесни обмена на най-добри практики в областта на наказателното правораздаване и правоприлагането. Ефективното участие на съдебната система в борбата срещу киберпрестъпността е от първостепенно значение за подобряване на наказателното преследване на извършителите на тежки престъпления в кибернетичното пространство в държавите членки.

в) Да предостави подкрепа на държавите членки при разследването на престъпления в кибернетичното пространство

Европейският център по киберпрестъпност ще осигурява оперативна подкрепа за разследванията на престъпления в кибернетичното пространство, като например насърчава създаването на съвместни екипи за разследването на престъпления в кибернетичното пространство и обмена на оперативна информация по отношение на провеждащите се разследвания.

Той ще оказва също така техническа помощ на високо равнище (съоръжения, складиране, инструменти) и експертни знания за кодиране при разследването на престъпления в кибернетичното пространство.

г) Да се превърне в колективен глас на европейските следователи в сферата на киберпрестъпността в рамките на правоприлагащите органи и съдебната система

С течение на времето Европейският център по киберпрестъпност може да се превърне в обединяващ пункт за европейските следователи, занимаващи се с престъпления в кибернетичното пространство, като им предостави колективен глас в обсъжданията с ИКТ сектора и други частни компании, както и с изследователската общност, сдружения на потребители и организации на гражданското общество за това как да се подобри превенцията на престъпления в кибернетичното пространство и да се координират целенасочените изследователски дейности.

Европейският център по киберпрестъпност ще се превърне в естествен интерфейс за дейностите на Интерпол, свързани с престъпленията в кибернетичното пространство, и на други международни полицейски части за борба с този вид престъпност. Той може също така да координира приноса към текущите инициативи за управлението на интернет и откритата междуправителствена експертна група на ООН по киберпрестъпността.

Европейският център по киберпрестъпност ще си сътрудничи също така с организации като INSAFE[15] при създаването на информационни кампании за широката общественост, като ги актуализира в съответствие с промените в областта на киберпрестъпността, установени при извършването на анализи от центъра, за да се насърчи разумното и безопасно сърфиране в интернет.

2.2. Местоположение

Както се посочва в проучването за осъществимостта, Европейският център по киберпрестъпност ще бъде част от Европол и ще бъде позициониран в рамките на съществуващите му структури.

Това носи значителни предимства. Държавите членки и други важни участници, включително Интерпол и международните правоприлагащи органи, са признали ролята на Европол, която вече има правомощия и за борба с компютърната престъпност[16]. Основната дейност на Европол се състои в това да помага за изграждането на по-безопасна Европа в полза на всички нейни граждани, като подпомага правоприлагащите органи на ЕС чрез обмен и анализ на разузнавателна информация за престъпления.

2.3. Отражение на Европейския център по киберпрестъпност върху ресурсите

В проучването за осъществимостта бяха разгледани различни видове отражение върху ресурсите. Ще трябва да се направи допълнителна оценка на това отражение[17], особено с оглед на други задачи, които може да бъдат възложени на Европол в бъдеще, както и в по-общия контекст на персонала на агенциите на ЕС. Тази оценка ще бъде направена по-специално в контекста на преразглеждането на правното основание за Европол и текущите обсъждания по предложението на Комисията за създаване на фонд „Вътрешна сигурност“. Вече става ясно, че ще се наложи командироване на персонал от държавите членки.

---

15 Европейска мрежа от информационни центрове, които популяризират безопасното и отговорно използване на интернет и мобилни устройства от страна на младите хора.

16 Решение на Съвета (2009/371/ПВР) от 6 април 2009 г. за създаване на Европейска полицейска служба, чл. 4, параграф 1 във връзка с приложението.

17 Оценката трябва да бъде съгласувана с общите нужди като персонал и бюджетни изисквания за агенциите в бюджет 2013 и следващата многогодишна финансова рамка.

Когато се оценяват прогнозните нужди от ресурси, Комисията ще се води от три съображения: първо — предполага се, че ще има умерено нарастване на общия брой разглеждани случаи на киберпрестъпност за разлика от значителното увеличаване на престъпленията в кибернетичното пространство; второ — държавите членки ще подсилят капацитетите си за борба срещу киберпрестъпността и трето — Европейският център по киберпрестъпност ще се занимава само с определен вид престъпления в кибернетичното пространство.

2.4. Управление

Установяването на Европейския център по киберпрестъпност в рамките на Европол трябва да гарантира участието на други ключови действащи лица в стратегическото управление на центъра. Ето защо Комисията предлага да се създаде програмен съвет на Европейския център по киберпрестъпност в рамките на управленската структура на Европол, който ще бъде председателстван от ръководителя на центъра. Този инструмент ще даде възможност на други действащи лица като Евроюст, CEPOL, държавите членки, представлявани от Работната група на ЕС по киберпрестъпността, ENISA и Комисията, да споделят своето ноу-хау, като се избегне излишна допълнителна административна тежест. Съветът може да изисква отчетност за извършването на дейностите, свързани с киберпрестъпността, от страна на Европейския център по киберпрестъпност и по този начин да гарантира, че те са извършени в партньорство, като се отдаде дължимото на опита и се зачитат правомощията на всички действащи лица.

2.5. Сътрудничество с ключови действащи лица

Европейският център по киберпрестъпност трябва осигури координиран отговор на киберпрестъпността не само като даде възможност за съвместна работа между агенциите на ЕС, но и като служи за единен център за контакт в тази област.

а) Държави членки

Основната цел е да се подпомогнат държавите членки в борбата им срещу киберпрестъпността. Информационното бюро по киберпрестъпността на Европейския център по киберпрестъпност и резултатите от работата на центъра, сред които по-конкретен анализ на заплахите и по-добра оперативна подкрепа от информационна гледна точка, ще бъдат от полза за следователите в Европа, занимаващи се с престъпления в кибернетичното пространство. Работната група на ЕС по киберпрестъпността ще гарантира, че съображенията на държавите членки ще бъдат представени пред програмния съвет на Европейския център по киберпрестъпност. Освен това държавите членки ще трябва да продължат да правят необходимите ивестиции в националните си структури за борба с киберпрестъпността, за да имат подходящия интерфейс за взаимодействие с центъра.

б) Европейски агенции и други действащи лица

Съответните агенции, по-специално Евроюст, CEPOL и ENISA, както и CERT-EU, ще участват пряко в дейностите на Европейския център по киберпрестъпност не само посредством програмния съвет, но и чрез оперативно сътрудничество, където е нужно и вземайки предвид техните респективни правомощия.

в) Международни партньори

В стремежа си да се превърне в Европейски информационен център по киберпрестъпността, Европейският център по киберпрестъпност трябва да бъде ценен събеседник за международните партньори по въпросите на престъпленията в кибернетичното пространство. В сътрудничество с Интерпол и стратегическите ни партньори по света центърът трябва да се стреми да подобри координираните отговори в борбата срещу киберпрестъпността и да направи необходимото, така че съображенията на правоприлагащите органи да бъдат взети предвид при по-нататъшното развитие на кибернетичното пространство.

г) Частен сектор, изследователски среди и организации на гражданското общество

Изграждането на доверие между частния сектор и правоприлагащите органи е от първостепенно значение в борбата срещу киберпрестъпността. Консолидирайки работата на Европол със съществуващите и с нови партньори, Европейският център по киберпрестъпност трябва да изгради надеждни мрежи и платформи за обмен на информация с индустрията и други действащи лица като изследователската общност и организациите на гражданското общество. Това трябва да улесни междуобщностния обмен на информация по редица въпроси, включително ранното предупреждение за киберзаплахи и координирани отговори под формата на работни групи на кибератаки и други видове престъпления в кибернетичното пространство.

Европейският център по киберпрестъпност трябва също така да допринесе за по-мащабните усилия на компаниите от частния сектор, които разполагат със значителни цифрови данни, като банки и търговци на дребно онлайн, да се борят и да се защитават по-добре от киберпрестъпления и да намалят уязвимостта при разработването на технологии.

От взаимен интерес за правоприлагащите органи и за частния сектор е да се създаде по-ясна картина на кибернетичното пространство в реално време, както и да се работи за по-ефективното разбиване на мрежи от киберпрестъпници чрез по-ефективното разкриване на новите начини на действие и бързото арестуване на киберпрестъпници.

3. ПЪТНА КАРТА ЗА СЪЗДАВАНЕТО НА ЕВРОПЕЙСКИЯ ЦЕНТЪР ПО КИБЕРПРЕСТЪПНОСТ

3.1. Дейности до края на 2013 г.

За да се постигне първоначалният оперативен капацитет, Комисията ще проучи в тясно сътрудничество с Европол какво ще бъде необходимо като човешки и финансови ресурси за създаването на екип за Европейския център по киберпрестъпност до края на настоящата финансова рамка на ЕС. Екипът ще има задачи като например изготвянето на мандата и организационната структура на центъра, както и разработването на критерии за оценка на постигнатите резултати. Ролята и функционирането на програмния съвет ще бъдат определени допълнително въз основа на споразумение между участниците.

С оглед на създаването на функцията „обединяване на информация“ екипът трябва да създаде връзки с експерименталния екип на CERT-EU, както и с ENISA, когато е необходимо (като се вземат предвид техните ограничени ресурси). За да се подобри сигнализирането за престъпления в кибернетичното пространство, ще се извърши

картографиране, за да се създаде карта за оперативната съвместимост на съществуващите системи за сигнализиране на престъпления в кибернетичното пространство в държавите членки.

Ще бъде създадено бюро по киберпрестъпност. Това бюро може да бъде подпомагано от специално създадена, сигурна онлайн платформа на общността. Настоящите обучителни дейности на Европол, CEPOL и на Европейската група за обучение и образование в областта на киберпрестъпността могат да бъдат подложени на оценка и да бъдат рационализирани под координацията на Европейския център по киберпрестъпност и неговия програмен съвет. Трябва да се направи анализ на нуждите от обучение, при който се отчитат и изискванията на съдиите и прокурорите. На базата на този анализ може да се проведе основен обучителен курс за борба срещу киберпрестъпността за представителите на системата на наказателното правосъдие.

Освен това ще трябва да се направи и представи по-точна оценка на нужните човешки и финансови ресурси с оглед на решенията по следващата многогодишна финансова рамка. Тази оценка трябва да предостави информация и за възможното по-нататъшно развитие на Европейския център по киберпрестъпност.

4. ЗАКЛЮЧЕНИЕ

Тъй като организираната престъпност разширява обхвата на дейността си в кибернетичното пространство, правоприлагащите органи трябва да следват тази тенденция. ЕС може да предостави на държавите членки и на индустрията необходимите инструменти за борба срещу съвременната и постоянно променяща се заплаха от киберпрестъпността, която по дефиниция не познава граници. Ако могат да бъдат осигурени нужните човешки и финансови ресурси, Европейски център по киберпрестъпност ще действа като централно звено в борбата на Европа срещу киберпрестъпността чрез обединяване на опит, оказване на помощ за наказателните разследвания и насърчаване на намирането на решения на общоевропейско ниво, като същевременно се повишава информираността на обществото по въпросите на киберпрестъпността в Съюза. По този начин центърът ще допринесе за запазването на достъпен интернет и легитимна цифрова икономика и за защитата на гражданите и бизнеса в Европа при използването на онлайн услуги.

Съветът се приканва да подкрепи това предложение, а Европейският парламент, както и други ключови действащи лица, се насърчават да допринесат за развитието на центъра.