ЕВРОПЕЙСКА
КОМИСИЯ

ВЪРХОВЕН ПРЕДСТАВИТЕЛ
НА СЪЮЗА ПО ВЪПРОСИТЕ
НА ВЪНШНИТЕ РАБОТИ И
ПОЛИТИКАТА НА СИГУРНОСТ

Брюксел, 13.9.2017 г.
JOIN(2017) 450 final

**СЪВМЕСТНО СЪОБЩЕНИЕ ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА**

# Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС

## 1. ВЪВЕДЕНИЕ

Киберсигурността е от критично значение както за нашето благополучие, така и за сигурността ни. Нашето ежедневие и икономиките ни стават все по-зависими от цифровите технологии, а с това ние ставаме все по-уязвими. Инцидентите, свързани с киберсигурността, стават все по-разнообразни по отношение на това кой ги извършва и какво се стреми да постигне. Злонамерените дейности в киберпространството застрашават не само нашите икономики и усилията за цифров единен пазар, но и самото функциониране на нашите демокрации, свободи и ценности. Бъдещата ни сигурност зависи от реформирането на способността ни да защитим ЕС от киберзаплахи: както гражданската инфраструктура, така и военният капацитет разчитат на надеждни цифрови системи. Това бе признато от Европейския съвет през юни 2017 г.[1] и в Глобалната стратегия за външната политика и политика на сигурност на Европейския съюз[2].

Рисковете нарастват експоненциално. Проучванията показват, че между 2013 г. и 2017 г. икономическото въздействие на киберпрестъпността е нараснало петкратно, а до 2019 г. може да се увеличи още четири пъти[3]. Особено голям ръст се наблюдава при софтуера за изнудване[4], като последните атаки[5] отразяват рязкото нарастване на престъпната дейност в киберпространството. Обаче софтуерът за изнудване далеч не е единствената заплаха.

Киберзаплахите произхождат както от недържавни, така и от държавни участници: често са криминални и имат за цел печалба, но могат да бъдат и политически и стратегически. Опасността от престъпления се засилва поради размиването на границата между киберпрестъпността и обичайната престъпност, тъй като престъпниците използват интернет едновременно за увеличаване на мащаба на действията си и като източник за изнамиране на нови методи и средства за извършване на престъпление[6]. Въпреки това в повечето случаи шансовете за издирване на престъпника са минимални, а за съдебното му преследване — още по-малки.

Същевременно държавните участници все по-често постигат своите геополитически цели не само с традиционни средства като военна сила, а също и чрез по-дискретни киберинструменти, включително намеса във вътрешните демократични процеси. Сега широко се признава, че киберпространството се използва като бойно поле — самостоятелно или като част от хибриден подход. Все по-често се срещат кампании за дезинформация, фалшиви новини и кибероперации, насочени към критичната инфраструктура, и те изискват съответен отговор. По тази причина в своя документ за

---

1 http://www.consilium.europa.eu/en/press/press-releases/2017/06/23-euco-conclusions/.

2 http://europa.eu/globalstrategy/.

3 Виж например изследването на компанията McAfee и Центъра за стратегически и международни изследвания (Center for Strategic and International Studies) „Нетни загуби: Оценка на общата стойност на загубите, причинени от киберпрестъпността“, 2014 г.

4 Софтуерът за изнудване е вид зловреден софтуер, който спира или ограничава достъпа на потребителите до тяхната система, като заключва екрана на системата или криптира файловете на потребителите докато не бъде платен откуп.

5 През май 2017 г. атаката със софтуера за изнудване WannaCry порази над 400 000 компютъра в повече от 150 държави. Месец по-късно атаката „Petya“ засегна Украйна и няколко предприятия в целия свят.

6 Европол, „Serious and Organised Crime Threat Assessment 2017“ („Оценка на заплахите от тежката и организираната престъпност за 2017 г.“).

размисъл относно бъдещето на европейската отбрана[7] Комисията подчертава значението на сътрудничеството в киберотбраната.

Ако не подобрим съществено нашата киберсигурност, рискът ще нараства успоредно с цифровизацията. До 2020 г. се очаква към интернет да бъдат свързани десетки милиарди устройства от „интернет на нещата“, но киберсигурността все още не е приоритет при тяхното проектиране[8]. Ако не успеем да защитим устройствата, които ще управляват нашите електропреносни мрежи, автомобили и транспортни мрежи, заводи, финанси, болници и домове, това може да има разрушителни последици и силно да разклати доверието на потребителите в нововъзникващите технологии. Рискът от политически мотивирани атаки към граждански цели и от слабости във военната киберотбрана още повече засилва тази опасност.

Подходът, изложен в настоящото съвместно съобщение, ще постави ЕС в по-добра позиция за справяне с тези заплахи. Чрез този подход ще се създаде по-голяма устойчивост и стратегическа автономност, като се увеличат възможностите по отношение на технологии и умения и се подпомогне изграждането на силен единен пазар. Това изисква да се създадат подходящите структури за изграждане на силна киберсигурност и за реагиране при нужда, с участие в най-висока степен на всички ключови действащи лица. Освен това този подход ще има по-добро възпиращо действие за кибератаките чрез по-успешна работа за откриване, проследяване и търсене на отговорност на съответните лица. Също така той ще отчита световното измерение чрез развиване на международно сътрудничество като платформа за водещата роля на ЕС в областта на киберсигурността. Тези стъпки се основават на подходите на цифровия единен пазар, Глобалната стратегия, Европейската програма за сигурност[9], Съвместна рамка за борба с хибридните заплахи[10] и Съобщението относно начало на дейността на Европейския фонд за отбрана[11][12].

ЕС вече работи по много от тези въпроси: сега е време да се обединят различните работни направления. През 2013 г. ЕС прие Стратегия за киберсигурност, поставяйки началото на ключови работни направления за повишаване на устойчивостта на киберпространството[13]. Главните цели и принципи на тази стратегия за насърчаване на надеждна, безопасна и отворена кибернетична екосистема остават валидни. Постоянно развиващият се и задълбочаващ се контекст на киберзаплахите обаче изисква допълнителни действия за устояване на атаките и предотвратяване на такива атаки в бъдеще[14].

ЕС е добре подготвен за обезпечаване на киберсигурност предвид обхвата на неговите политики и инструментите, структурите и способностите, с които разполага. Макар

---

7 https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf.

8 IDC и TXT Solutions (2014 г.), SMART 2013/0037 Съчетаване на услуги в облак и интернет на нещата (IoT), изследване за Европейската комисия.

9 COM(2015) 185 final.

10 JOIN(2016) 18 final.

11 COM(2017) 295.

12 Този подход се подкрепя и от независимото научно становище на Групата на високо равнище на научните съветници към Механизма за научни становища на Европейската комисия (вж. позоваванията по-долу).

13 JOIN(2013) 1 final. Оценка на тази стратегия е дадена в SWD (2017) 295.

14 Ако не е посочено друго, предложенията в настоящото съобщение са неутрални за бюджета. Всяка инициатива, която има последици за бюджета, ще следва надлежно годишните бюджетни процедури и не може да предопределя следващата многогодишна финансова рамка за периода след 2020 г.

държавите членки да продължават да носят отговорността за националната сигурност, мащабът и трансграничният характер на заплахата показват необходимостта от действия на Съюза, които да насърчават и подпомагат държавите членки да развиват и поддържат повече и по-добри национални възможности за киберсигурност, като същевременно се изгражда такъв капацитет на равнище ЕС. Този подход има за цел да стимулира всички участници — ЕС, държавите членки, предприятията от сектора и отделните лица — да издигнат киберсигурността в приоритет, което е нужно, за да се изгради устойчивост и да се осигури по-добра реакция на ЕС на кибератаки. Подходът ще осигури конкретни стъпки, за да се подпомогне откриването и разследването на всички видове киберинциденти, насочени срещу ЕС и срещу неговите държави членки, и за да се реагира по подходящ начин, включително чрез съдебно преследване на престъпниците. Той ще даде възможност външната дейност на ЕС ефективно да повиши киберсигурността в световен мащаб. В резултат на това ЕС ще промени подхода си от реактивен на проактивен, за да защити европейското благополучие, общество и европейските ценности, както и основните права и свободи, като реагира както на съществуващите, така и на бъдещи заплахи.

## 2. ИЗГРАЖДАНЕ НА УСТОЙЧИВОСТ НА ЕС СРЕЩУ КИБЕРАТАКИ

За силна устойчивост на киберпространството е необходим колективен и широкообхватен подход. Това налага наличието на по-силни и ефективни структури в помощ на киберсигурността и за реагиране на кибератаки в държавите членки, но също така и в собствените институции, агенции и органи на ЕС. Необходим е и по-цялостен подход, съчетаващ различни политики, за изграждане на по-силна устойчивост на киберпространството и стратегическа автономност, със силен единен пазар, силен напредък в технологичните възможности на ЕС и по-голям брой опитни експерти. В основата на това стои по-широкото разбиране, че киберсигурността е предизвикателство пред цялото общество, така че следва да бъдат ангажирани много и различни слоеве на държавата, икономиката и обществото.

### 2.1 Укрепване на Агенцията на Европейския съюз за мрежова и информационна сигурност

**Агенцията на Европейския съюз за мрежова и информационна сигурност (**ENISA) трябва да играе ключова роля за укрепването на устойчивостта на ЕС и за реагирането на кибератаки, но тя е ограничена от сегашния си мандат. Затова Комисията представя предложение за амбициозни реформи, включително **постоянен мандат за агенцията**[15]. Това ще гарантира, че ENISA може да подпомага държавите членки, европейските институции и предприятия в ключови области, включително при прилагането на Директивата за мрежова и информационна сигурност[16] („директивата за МИС“) и на предложената рамка за сертифициране за киберсигурност.

Реформираната ENISA ще има силна консултативна роля при разработването и прилагането на политики, включително чрез съдействие за съгласуваност между секторните инициативи и директивата за МИС и за създаване на центрове за обмен и анализ на информация в критичните сектори. ENISA ще повиши стандартите за качество и ще засили готовността в Европа, като организира ежегодни общоевропейски учения за киберсигурност, съчетаващи реагиране на различни равнища. Освен това тя

[15] COM(2017) 477.

[16] 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.

ще подпомага разработването на политики на ЕС за сертифициране за киберсигурност на информационните и комуникационните технологии (ИКТ) и ще играе важна роля за подобряване на оперативното сътрудничество и управлението на кризи в целия ЕС. Агенцията ще служи също и като център за информация и знания в общността на специалистите по киберсигурност.

Бързото и споделено научаване за заплахи и инциденти още в процеса на тяхното разгръщане е предпоставка за вземане на решение дали е нужно съвместно действие, подпомагано от ЕС, за смекчаване на последиците или за реагиране. Такъв обмен на информация изисква участието на всички съответни действащи лица — органите и агенциите на ЕС, както и държавите членки — на техническо, оперативно и стратегическо равнище. ENISA, в сътрудничество със съответните органи на равнище държави членки и ЕС — по-специално мрежата от екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС)[17], екипите за незабавно реагиране при компютърни инциденти (CERT-EU) на ЕС, Европол и Центърът на ЕС за анализ на информация (INTCEN) — също ще допринася за събиране на информация на равнище ЕС за текущата ситуация. Тази информация може да се използва за разузнаване във връзка с потенциални заплахи и за разработване на политики в контекста на постоянно наблюдение на ситуацията от гледна точка на заплахите и ефективно оперативно сътрудничество, както и при реагиране на широкомащабни трансгранични инциденти.

## 2.2 Към единен пазар на решения, свързани с киберсигурността

Развитието на пазара на решения, свързани с киберсигурността в ЕС — по отношение на продукти, услуги и процеси — се спъва по няколко начина. Основен аспект е липсата на схеми за сертифициране за киберсигурност, признати в целия ЕС, за вграждане в продуктите на по-високи стандарти за устойчивост и укрепване на доверието към пазара в целия ЕС. Затова Комисията предлага да се създаде **европейска рамка за сертифициране за киберсигурност**[18]. Тази рамка ще определя процедурата за създаване на схеми за сертифициране в целия ЕС, обхващащи продукти, услуги и/или системи, които адаптират равнището на сигурност към съответната употреба (като критична инфраструктура или като потребителски устройства)[19]. Рамката ще донесе определени ползи за бизнеса чрез премахване на необходимостта да се преминава през няколко процедури за сертифициране при търговия зад граница и по този начин ще намали административните и финансовите разходи. Освен това използването на схеми, разработени в тази рамка, ще спомогне за изграждане на доверие у потребителите, като сертификат за съответствие ще уведомява и уверява купувачите и потребителите относно свързаните със сигурността свойства на продуктите и услугите, които те купуват и използват. Това ще направи високите стандарти за киберсигурност източник на конкурентно предимство. В резултат ще се повиши устойчивостта, тъй като изделията и услугите в областта на ИКТ официално ще се оценяват спрямо определени стандарти за киберсигурност, които могат да бъдат разработени в тясна връзка с продължаващата по-широка работа по стандартите в сферата на ИКТ[20].

[17] Предвидени в член 9 от директивата за МИС.

[18] COM(2017) 477.

[19] Равнището на сигурност показва степента на строгост на оценката на сигурността и обикновено е съизмеримо със степента на риск, свързана с областите или функциите на даденото приложение (т.е. по-високо равнище на сигурност се изисква за ИКТ продукти и услуги, използвани във високорискови области на приложение или функции).

[20] COM(2016) 176.

Схемите на рамката ще се прилагат доброволно и няма да налагат непосредствени регулаторни задължения на търговците и доставчиците на услуги. Тези схеми няма да противоречат на никои приложими законови изисквания като например законодателството на ЕС относно защита на данните.

След създаването на рамката Комисията ще прикани съответните заинтересовани страни да обърнат внимание главно на три приоритетни области:

- Сигурност в критични приложения и приложения, свързани с висок риск[21]: системите, от които зависим в нашето ежедневие — от нашите автомобили до машините в заводите, от най-големите системи като например самолети и електроцентрали до най-малките като медицинските апарати — все повече се цифровизират и са все повече взаимно свързани. Затова за основните ИКТ компоненти в такива изделия и системи ще се изисква строга оценка за сигурност.

- Киберсигурност в широко разпространени цифрови продукти, мрежи, системи и услуги, използвани както в държавния, така и в частния сектор за защита срещу атаки и в съответствие със законови изисквания[22] — като например криптиране на електронна поща, защитни стени и виртуални частни мрежи; особено важно е разпространяващата се употреба на такива средства да не води до нови източници на риск или нови уязвими места.

- Използването на методи за „сигурност още при проектирането“ при цифрови, взаимно свързани масови потребителски устройства с ниска себестойност, които съставляват Интернет на нещата: схеми по тази рамка може да се използват за обозначаване, че изделията са изработени чрез използване на най-съвременните сигурни методи за проектиране, че са преминали през подходящи изпитвания за сигурност и че търговците са поели ангажимент да осъвременят софтуера си в случай, че бъдат открити нови уязвими места или заплахи.

Посочените приоритети следва да вземат под внимание по-специално развиващата се ситуация на заплахите за киберсигурността, както и важността на основните услуги като транспорт, енергетика, здравеопазване, банково дело, инфраструктурата на финансовия пазар, инфраструктурата на питейната вода и цифровата инфраструктура[23].

Макар че за никое ИКТ изделие, система или услуга не може да се гарантира, че е 100 % сигурно, има няколко общоизвестни и добре документирани дефекти в устройството на ИКТ продуктите, които може да се използват за атаки. Подходът „сигурност още при проектирането“, възприет от производителите на свързани устройства, ИТ софтуер и оборудване, би осигурил прилагане на мерки за киберсигурност преди новите изделия да се пуснат на пазара. Този подход може да бъде част от принципа на задължителна предпазливост и да се развива допълнително едновременно с промишлеността, което може да намали уязвимостта на продукти/софтуер чрез прилагане на редица методи от проектирането до изпитването и

[21] Изключение би било когато задължителното или доброволното сертифициране се ръководи от други актове на Съюза.

[22] Например Директива (ЕС) 2016/1148, Регламент (ЕС) 2016/679, Директива (ЕС) 2015/2366 и други предложени законови актове като Европейски кодекс за електронните съобщения; всеки от тези документи изисква организациите да въведат подходящи мерки за сигурност за справяне със съответните рискове за киберсигурността.

[23] Секторите, които са в обхвата на 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.

проверката, включително официално одобряване където това е приложимо, дългосрочна поддръжка, и използването на сигурни процеси за развитието на жизнения цикъл, както и разработване на актуализации и пачове за отстраняване на открити уязвими места, и бързо актуализиране и ремонтиране[24]. Също така това ще засили доверието на потребителите към цифровите продукти.

Освен това е нужно да се признае важната роля на изследователите на сигурността, които са трети страни, за откриване на уязвими места в съществуващи продукти и услуги, и във всички държави членки да се създадат условия, позволяващи координирано разкриване на уязвимите места[25], като се стъпва на най-добрите практики[26] и се прилагат съответните стандарти[27].

В същото време **специфичните сектори** са изправени пред специфични проблеми и следва да бъдат насърчавани да разработват свои собствени подходи. Така общите стратегии за киберсигурност ще се допълват от специфични за секторите стратегии за киберсигурност в области като финансови услуги[28], енергетика, транспорт и здравеопазване[29].

Комисията вече подчерта специфичните проблеми във връзка с **отговорността**, породени от новите цифрови технологии[30], и в момента се работи за анализиране на възможните последици; следващите стъпки ще приключат през юни 2018 г. Киберсигурността повдига въпроси във връзка с определянето на щети за бизнеса и за веригата на доставките, и ако тези въпроси не бъдат решени, това ще попречи на развитието на силен единен пазар на продукти и услуги, свързани с киберсигурността.

И накрая, развитието на единния пазар на ЕС зависи също от включването на киберсигурността при формулирането на политиката за търговия и за инвестиции. Ефектът на придобиването от чуждестранни субекти на критични технологии — за което киберсигурността е важен пример — е ключов аспект в рамката за **проверка на преките чуждестранни инвестиции в Европейския съюз**[31], която има за цел да се осигури възможност да се проверяват инвестициите от трети страни на основание сигурност и обществен ред. По подобен начин изискванията за киберсигурност вече създадоха търговски ограничения за стоки и услуги от ЕС във важни сектори в известен брой икономики на трети страни. Рамката на ЕС за сертифициране за киберсигурност

---

[24] Киберсигурност на европейския цифров единен пазар, Група на високо равнище на научните съветници, март 2017 г.

[25] Координираното разкриване на уязвимите места е форма на сътрудничество, която улеснява изследователите на сигурността и им позволява да съобщават на собственика или продавача на дадена информационна система за уязвимите места, давайки възможност на организацията да диагностицира уязвимото място и своевременно да го поправи по подходящ начин преди подробна информация за уязвимостта да бъде разкрита пред трети страни или пред обществото.

[26] Например Good Practice Guide on Vulnerability Disclosure. From challenges to recommendations, (Ръководство за добрите практики при разкриване на уязвими места. От предизвикателства към препоръки), ENISA, 2016 г.

[27] ISO/IEC 29147:2014 Информационни технологии — Методи за сигурност — Разкриване на уязвими места.

[28] Предстоящата работа на Комисията във връзка с финансовите технологии ще обхване киберсигурността във финансовия сектор.

[29] В сектора на енергетиката например съчетаване на много стари технологии и най-съвременни информационни технологии, по-специално с изискванията на електропреносната мрежа в реално време.

[30] COM(2017) 228.

[31] COM(2017) 478.

допълнително ще укрепи международните позиции на Европа и следва да се допълва от постоянни усилия за разработване на високи световни стандарти за сигурност и споразумения за взаимно признаване.

### 2.3 Пълно прилагане на Директивата за сигурността на мрежите и информационните системи

След като днес на национално равнище са на разположение основните средства за борба против заплахите за киберсигурността, ЕС признава необходимостта за по-нататъшно развитие на стандартите. Поради все по-глобализирания, разчитащ на цифрови технологии и взаимно свързан характер на ключови сектори като банково дело, енергетика и транспорт широкомащабните инциденти, свързани с киберсигурността, рядко засягат само една държава членка.

Директивата за сигурността на мрежите и информационните системи („директивата за МИС“) е първият закон за киберсигурността, валиден за целия ЕС[32]. Тя има за цел изграждане на устойчивост чрез усъвършенстване на националния капацитет за киберсигурност; насърчаване на по-добро сътрудничество между държавите членки; и изискване от предприятията във важни сектори на икономиката да въведат ефективни практики за управление на риска и да докладват на националните органи за сериозните инциденти. Тези задължения се отнасят и за три вида доставчици на ключови интернет услуги: компютърни услуги „в облак“, онлайн търсачки и онлайн места за търговия. Директивата има за цел прилагане на по-решителен и по-систематичен подход и постигане на по-добър информационен поток.

Пълното прилагане на тази директива от всички държави членки най-късно до месец май 2018 г. е крайно необходимо за постигане на устойчивост на ЕС срещу кибератаки. Процесът се подпомага от колективната работа на държавите членки, в резултат от която до есента на 2017 г. ще бъдат създадени насоки за по-хармонизирано прилагане, по-специално във връзка с операторите на основни услуги. Освен това Комисията публикува Съобщение[33] като част от този пакет за киберсигурност в помощ на техните усилия чрез представяне на най-добри практики от държавите членки, свързани с прилагането на директивата, и указания как би трябвало тази директива да се изпълнява на практика.

Една област, в която ще е необходимо директивата да бъде допълнена, е информационният поток. Например директивата обхваща само най-важните стратегически сектори, но логично е необходим подобен подход от страна на всички заинтересовани, засегнати от кибератаки, за да може да се направи систематична оценка на уязвимите места и входните точки за кибератаки. Освен това съществуват пречки за сътрудничеството и обмена на информация между държавния и частния сектор. Правителствата и държавните органи не са склонни да споделят информация, свързана с киберсигурността, понеже се опасяват да не изложат на риск националната сигурност или конкурентоспособността. Частните предприятия не са склонни да споделят информация относно своите уязвими за кибератаки места и претърпените в резултат загуби, тъй като се опасяват да не изложат на риск чувствителна бизнес информация, с което да застрашат репутацията си и да нарушат правилата за защита на

[32] 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.

[33] COM (2017) 476.

личните данни[34]. Необходимо е укрепване на доверието за публично-частно партньорство в подкрепа на сътрудничеството и обмена на информация между по-голям брой сектори. Ролята на центровете за обмен и анализ на информация е особено важна за изграждане на необходимото доверие за обмен на информация между частния и държавния сектор. Предприети са някои първи стъпки по отношение на специфични критични сектори като въздухоплаването, чрез създаването на Европейски център за кибернетична сигурност във въздухоплаването,[35] както и енергетиката — чрез създаването на центрове за обмен и анализ на информация[36]. Комисията ще съдейства изцяло за този подход с подкрепа от страна на ENISA, като ускорено прилагане е необходимо по-специално в секторите, предоставящи основни услуги, както е посочено в директивата за МИС.

### 2.4 Устойчивост чрез бързо реагиране при извънредни ситуации

Когато се извършва кибератака бързата и ефективна реакция може да смекчи нейните последици. Такава реакция може също да покаже, че публичните органи не са безсилни пред лицето на кибератаките и да допринесе за изграждането на доверие. Що се отнася до реакцията на институциите на ЕС, на първо място аспектите на киберсигурността следва да бъдат включени в съществуващите механизми на ЕС за управление на кризи: интегрираните договорености за реакция на ЕС на политическо равнище в кризисни ситуации, координирани от председателството на Съвета[37], и общите системи на ЕС за бързо предупреждение[38]. Необходимостта да се отговори на особено сериозен киберинцидент или кибератака може да бъде достатъчно основание държава членка да се позове на клаузата на ЕС за солидарност[39].

За бърза и ефективна реакция се разчита също и на механизъм за бърз обмен на информация между всички най-важни участници на национално и европейско равнище, който на свой ред изисква яснота относно съответните техни роли и отговорности. Комисията се консултира с институции и с държави членки относно план за осигуряване на ефективен процес на оперативно реагиране на равнище ЕС и равнище държави членки при широкомащабни киберинциденти. **Планът**, представен в препоръка[40] в този пакет, разяснява как киберсигурността се включва в механизмите на равнище ЕС за управление на кризи и посочва целите и начините за сътрудничество между държавите членки, както и между държави членки и съответните европейски

[34] Киберсигурност на европейския цифров единен пазар, Група на високо равнище на научните съветници, март 2017 г. Налице е специфичен въпрос, свързан с търговската тайна; във връзка с него в съобщението „Укрепване на отбранителната способност на Европа срещу кибератаки“ от юли 2016 г. се отбелязват нежеланието да се съобщава за кибернетични кражби на търговски тайни и важността на доверените канали за съобщаване, осигуряващи поверителност.

[35] https://www.easa.europa.eu/newsroom-and-events/news/implementation-european-centre-cyber-security-aviationeccsa.

[36] Това са организации с нестопанска цел, функциониращи по инициатива на техните членове и формирани от частни и държавни субекти, с цел да обменят информация за кибератаки, рискове, предотвратяване, смекчаване на последиците и реагиране на такива атаки. Вж. напр. европейските центрове за обмен и анализ на информация в енергетиката (http://www.ee-isac.eu).

[37] Те позволяват координиране на реакциите на най-високо политическо равнище при големи кризи, засягащи няколко сектора.

[38] Те дават възможност за международен обмен на информация и международна координация при възникващи кризи, засягащи много сектори, и при предвидими или непосредствени заплахи, които изискват действия на равнище ЕС.

[39] Съгласно член 222 от Договора за функционирането на Европейския съюз.

[40] C(2017) 6100.

институции, служби, агенции и органи[41] за реагиране при широкомащабни инциденти и кризи, свързани с киберсигурността. . Препоръката изисква освен това държавите членки и европейските институции да създадат мрежа за реагиране при кризи в киберсигурността, за да започне работа по този план. Той ще бъде периодично изпитван в учения за управление на кризи в киберсигурността и други кризи[42] и при необходимост ще бъде актуализиран.

При положение, че инцидентите, свързани с киберсигурността, могат значително да повлияят върху функционирането на икономиките и върху ежедневието на хората, може да се проучи възможността за **извънреден фонд за киберсигурност** по примера на други такива механизми за действие при кризи в други области на политиката на ЕС. Такъв фонд би дал възможност държавите членки да поискат помощ на равнище ЕС по време на мащабен инцидент или след такъв инцидент, при условие че преди инцидента дадената държава членка е въвела разумна система за киберсигурност, включително прилагане в пълна степен на директивата за МИС, напълно развити рамки за управление на риска и за надзор на национално равнище. Допълвайки съществуващите механизми на равнище ЕС за управление на кризи, такъв фонд би могъл да разгърне капацитет за бързо реагиране в интерес на солидарността и да финансира специфични действия за реагиране при извънредни ситуации като например подмяна на компрометирано оборудване или прилагане на средства за отговор или за смекчаване на последиците, използвайки националния експертен опит по линия на механизма на ЕС за гражданска защита.

### 2.5 Мрежа за компетентност в сферата на киберсигурността с европейски център за изследвания и компетентност в сферата на киберсигурността

Технологичните средства за киберсигурност са стратегически активи и същевременно ключови технологии за развитие в бъдеще. ЕС има стратегически интерес да осигури запазването и развитието на ключовите способности за защита на своята цифрова икономика, своето общество и демокрация, на критичното оборудване и софтуер, и да предоставя основни услуги в сферата на киберсигурността.

Публично-частното партньорство за киберсигурност[43], създадено през 2016 г., бе важна първа стъпка, осигуряваща инвестиции в размер до 1,8 милиарда евро до 2020 г. Обаче мащабът на инвестициите, които се осъществяват понастоящем в други части на света[44] предполага, че е необходимо ЕС да засили инвестирането и да преодолее фрагментирането на капацитета, разпръснат в ЕС.

При сложността на технологиите за киберсигурност, големия размер на необходимите инвестиции и нуждата от решения, които функционират навсякъде в ЕС, Съюзът може да осигури добавена стойност. Като се използва за основа работата на държавите членки и на публично-частното партньорство, следваща стъпка би било да се укрепва капацитетът на ЕС за киберсигурност чрез **мрежа от центрове за компетентност в**

---

[41] Включително Европол, ENISA, екипите на институциите, органите и агенциите на ЕС за незабавно реагиране при компютърни инциденти (CERT-EU) и Центъра на ЕС за анализ на информация (INTCEN).

[42] Например ръководени от EINSA: https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme.

[43] C(2016) 4400 final.

[44] Само през 2017 г. САЩ ще инвестират в киберсигурността 19 милиарда долара — с 35 % повече в сравнение с 2016 г. Белият дом, офис на прессекретаря: „Информационна справка: Национален план за действие за киберсигурност“, 9 февруари 2016 г.

**сферата на киберсигурността**[45] с **европейски център за изследвания и компетентност в сферата на киберсигурността** в нейната основа. Тази мрежа и този център ще насърчават развитието и внедряването на технологии за киберсигурност и ще допълват действията за изграждане на капацитет в тази област на равнище ЕС и на национално равнище. Комисията ще започне оценка на въздействието, за да проучи съществуващите възможности — включително възможността за създаване на съвместно предприятие — с цел тази структура да бъде създадена през 2018 г.

Като първа стъпка и за осигуряване на информация за обмисляне в бъдеще, Комисията ще предложи да се стартира първа фаза по програмата „Хоризонт 2020“, за да се подпомогне обединяването в мрежа на националните центрове за компетентност и да се даде нов импулс за развитие на компетенциите и технологиите в сферата на киберсигурността. За тази цел Комисията възнамерява да предложи краткосрочно финансиране от 50 милиона евро. Това действие ще допълни продължаващото реализиране на публично-частното партньорство за киберсигурност.

Обединяването и насочването на научноизследователските усилия ще бъде основна задача на мрежата и първоначална цел на центъра. За подпомагане на развитието на промишления капацитет центърът може да изпълнява ролята на ръководител на проекти за развитие на този капацитет и да ръководи многонационални проекти. Това ще даде и допълнителен тласък за иновациите и конкурентоспособността на европейската промишленост на световната сцена в разработването на цифрови технологии от следващо поколение, включително изкуствен интелект, квантови компютърни изследвания, блок-вериги и сигурна цифрова идентичност, както и за осигуряване за базираните в ЕС предприятия на достъп до масови данни; всички това е от ключово значение за киберсигурността в бъдеще. Центърът ще използва и работата на ЕС за разширяване на инфраструктурата от високопроизводителни изчислителни мощности: това е крайно необходимо за анализ на големи количества данни, бързо криптиране и декриптиране на данни, проверка на самоличности, симулация на кибератаки и анализ на видео материали[46].

Би могло мрежата от центрове за компетентност да има и възможности за подпомагане на промишлеността чрез изпитване и симулации в помощ на сертифицирането за киберсигурност, описано в раздел 2.2. Участието на мрежата в целия кръг дейности за киберсигурност в ЕС ще осигури постоянно актуализиране на нейните цели в съответствие с нуждите. Центърът ще има за цел въвеждане на високи стандарти за киберсигурност не само при технологичните системи и системите за сигурност, на също и при усвояването на високоспециализирани умения от специалистите, като ще осигурява решения и модели, които да се използват при национални кампании за придобиване на нови цифрови умения. За тази цел той ще повиши капацитета на равнище ЕС за киберсигурност и ще разчита на синергиите, по-специално с ENISA, CERT-EU, Европол, с евентуалния бъдещ фонд за реагиране при извънредни ситуации, свързани с компютърната сигурност, и националните екипи за реагиране при инциденти с компютърната сигурност.

При работата на мрежата за компетентност трябва да се обърне специално внимание на липсата на европейски капацитет за оценка на **криптирането** на продукти и услуги,

[45] Мрежата ще включва съществуващите и бъдещи центрове за киберсигурност, създадени в държавите членки; като членове на тези центрове обикновено са държавни научноизследователски организации и лаборатории.

[46] COM (2012) 45 final и COM (2016) 178 final.

използвани от гражданите, бизнеса и правителствата в рамките на цифровия единен пазар. Сигурното криптиране е основа на надеждните цифрови системи за идентификация, които играят ключова роля за ефективната киберсигурност[47]; също така то защитава интелектуалната собственост на хората и дава възможност за защита на основни права като свободата на изразяване и защита на личните данни и осигурява безопасна онлайн търговия[48].

Тъй като в ЕС гражданският и военният пазар на решения, свързани с киберсигурността, са изправени пред едни и същи предизвикателства[49], а технологиите с двойна употреба изискват тясно сътрудничество в критични области, втора фаза на мрежата и нейния център може да бъде допълнително развита с аспект за киберотбрана, при стриктно спазване на клаузите на Договора, отнасящи се до общата политика за сигурност и отбрана. В допълнение към технологичния си фокус отбранителният аспект може да допринесе за сътрудничество между държавите членки в областта на киберотбраната, включително обмен на информация, осведоменост за ситуацията, изграждане на експертен опит и координирани реакции и подпомагане на развитието на общ капацитет на държавите членки. Освен това този аспект може да бъде платформа, въз основа на която държавите членки да определят приоритети за киберотбрана на ЕС, да изследват възможните общи решения, да допринасят за разработване на общи стратегии, подпомагайки съвместни обучения, учения и тестове за киберотбрана на европейско равнище и работата за създаване на класификации и стандарти в киберотбраната, като центърът ще има помощна и консултативна роля. За изпълнение на посочените дейности ще необходимо центърът да работи в тясно сътрудничество и в пълно допълване с Европейската агенция по отбрана — в областта на киберотбраната и с ENISA — в областта на устойчивостта на киберпространството. Отбранителният аспект ще вземе под внимание процеса, започнал с документа за размисъл относно бъдещето на европейската отбрана.

Високото равнище на устойчивост, нужно при киберотбраната, изисква специфично насочени научноизследователски и технологични усилия. Проектите и технологиите за киберотбрана, разработени от предприятия, могат да използват финансиране от Европейския фонд за отбрана по отношение на фазата на научни изследвания и разработка[50]. Специфични области като системи за криптиране, основани на квантови технологии; осведоменост за киберситуацията; системи за контрол на достъпа, използващи биометрични данни; разкриване на комплексни устойчиви заплахи или извличане на данни могат да са особено уместни в тази връзка. Върховният представител, Европейската агенция по отбрана и Комисията ще подпомагат държавите членки за определяне на области, в които общи проекти за киберсигурност могат да бъдат взети предвид за финансиране от Европейския фонд за отбрана.

## 2.6 Изграждане на силна основа от умения в областта на кибернетиката в ЕС

[47] Комисията ще обяви в рамките на програмата „Хоризонт 2020“ нова награда Horizon — предизвикателство, като ще бъде присъдена сума от 4 милиона евро за най-доброто новаторско решение за методи за лесно установяване на автентичността онлайн.

[48] Киберсигурност на европейския цифров единен пазар, Група на високо равнище на научните съветници, март 2017 г.

[49] „Study on synergies between the civilian and the defence cybersecurity markets“ („Изследване на синергиите между гражданския пазар и пазара на отбраната на решения, свързани с киберсигурността“) (Optimity; SMART 2014-0059).

[50] И сега Европейската програма за промишлено развитие в областта на отбраната дава предимство на проекти в областта на киберотбраната и киберотбраната ще бъде една от темите в поканата за представяне на предложения през 2018 г.

Киберсигурността има аспект, силно свързан с образованието. Ефективната киберсигурност разчита силно на уменията на ангажираните специалисти. Според прогнозите обаче се очаква през 2022 г. недостигът на специалисти с умения в сферата на киберсигурността, работещи в частния сектор в Европа, да достигне 350 000[51]. Обучението по киберсигурност следва да се развива на всички равнища, като се започне от периодични обучения на персонала в областта на киберсигурността, допълнително обучение по киберсигурност за всички ИКТ специалисти и нови специфични учебни програми за киберсигурност. Необходимо е да се създадат силни академични центрове за компетентност, които да отговорят на нуждите от ускорено образование и обучение и които биха могли да използват насоки от европейския център за изследвания и компетентност в сферата на киберсигурността и от ENISA. Целта следва да бъде проектирането на ИКТ продукти и системи, в които от самото начало се вграждат принципи на сигурност, да стане нещо естествено. Образованието по киберсигурност не следва да се ограничава само до специалистите по информационни технологии, а да се включва в учебните програми в други области като машиностроене, бизнес мениджмънт и право, както и в образователните програми, специфични за различните сектори. И накрая, когато учителите и учениците в основните и в средните училища придобиват цифрови умения в училище, те трябва да бъдат обучени да обръщат внимание на киберсигурността и да я разбират.

ЕС заедно с държавите членки следва също да допринесат към тази дейност, въз основа на работата на Коалицията за умения и работни места в областта на цифровите технологии[52], например като създадат схеми за чиракуване в областта на киберсигурността в малките и средни предприятия.

### 2.7 Насърчаване на кибернетичната хигиена и осведоменост

Отчита се, че около 95 % от инцидентите са станали възможни поради „някакъв вид човешка грешка, съзнателна или несъзнателна“;[53] това е показателно за силната роля на човешкия фактор. Следователно киберсигурността е отговорност на всеки човек. Това означава, че личното поведение, поведението в корпоративен план и това на публичната администрация трябва да се променят, за да се гарантира, че всеки човек разбира опасността и разполага с необходимите средства и умения бързо да открива атаки и активно да се защити от тях. Нужно е хората да си създадат навици за кибернетична хигиена, а бизнесът и организациите трябва да приемат подходящи програми за киберсигурност, основани на рисковете, и периодично да ги актуализират, за да отразяват развиващата се ситуация на рискове.

Директивата за МИС определя отговорностите на държавите членки не само за обмен на информация за кибератаки на равнище ЕС, но и за въвеждане на комплексни национални стратегии и рамки за сигурност на мрежата и информационните системи. Публичните администрации на европейско и на национално равнище трябва да изпълняват по-нататъшна водеща роля за напредък на тези действия.

---

[51] Световно проучване за работната сила в информационната сигурност, 2017 г. Недостигът в световен мащаб е 1,8 милиона специалисти.

[52] https://ec.europa.eu/digital-single-market/en/digital-skills-jobs-coalition.

[53] IBM „Индекс на сведенията в областта на киберсигурността“ 2014 г., цитиран в Securitymagazine.com, 19 юни 2014 г.

На първо място държавите членки следва да осигурят инструменти за киберсигурност, които да са на разположение на предприятията и хората в максимална степен. По-специално следва да се направи повече за предотвратяване на киберпрестъпленията и смекчаване на тяхното въздействие върху крайните потребители. Вече има пример в работата на Европол с кампанията „NoMoreRansom“ [54], осъществена чрез тясно сътрудничество между правоприлагащи органи и компании за киберсигурност, за да помогне на потребителите да предотвратят заразяване със софтуер за изнудване и да декриптират данни в случай, че са станали жертва на атака. Такива схеми следва да се въведат и за други видове зловреден софтуер, в други сфери, а ЕС да разработи **един портал, обединяващ всички такива инструменти на едно място**, който да предлага за потребителите съвети относно предотвратяването и откриването на зловреден софтуер, както и линкове към механизми за съобщаване за такъв софтуер.

На второ място държавите членки следва да ускорят **използването на по-сигурни инструменти при разработване на електронното управление** и също максимално да се възползват от мрежата за компетентност. Следва да се насърчава въвеждането на сигурни средства за идентификация, като се използва за основа рамката на ЕС за електронна идентификация и удостоверителни услуги при електронни трансакции на вътрешния пазар, която е в сила от 2016 г. и осигурява предсказуема регулаторна среда, позволяваща надеждно и безпроблемно взаимодействие между предприятия, лица и държавни органи[55]. Освен това държавните институции — особено онези, които предоставят основни услуги — следва да осигурят за своите служители обучение в области, свързани с киберсигурността.

На трето място държавите членки следва да направят осведомеността по въпросите на киберсигурността приоритет **в кампаниите за повишаване на осведомеността**, включително онези, насочени към училища, университети, бизнес общността и научноизследователските организации. Ще се разшири мащабът на месеца на киберсигурността, който се провежда всяка година през октомври и се координира от ENISA, за да постигне той по-голям обхват като една обща комуникационна кампания на равнище ЕС и на национално равнище. Също толкова важно е повишаването на осведомеността относно онлайн **кампании за дезинформация и фалшиви новини** в социалните медии, конкретно целящи подкопаване на демократичните процеси и европейските ценности. Макар главната отговорност да остава на национално равнище, включително за изборите за Европейски парламент, обединяването на експертните знания и обменът на опит на европейско равнище определено добавят стойност при осигуряване на фокус за действие[56].

На **сектора** като цяло също е отредена силна роля, но със специално внимание към доставчиците и производителите на цифрови услуги. Необходимо е тя да подпомага потребителите (лица, предприятия и публични администрации) с инструменти, които

---

54 https://www.nomoreransom.org/.

55 Регламент (ЕС) № 910/2014 относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар, приет на 23 юли 2014 г. Също така чрез Механизма за свързване на Европа Комисията осигурява основни градивни елементи и средства за оперативна съвместимост на електронната идентификация и електронния подпис (например доверителни списъци на браузъри).

56 Пример за това е Оперативната група за стратегическа комуникация с Източното съседство (East StratCom) създадена през 2015 г. от държави членки и Върховния представител за противодействие на кампаниите на Русия за дезинформация. Екипът разработва комуникационни продукти и кампании, които имат за главна цел разясняване на политиките на ЕС в региона на Източното партньорство.

да им позволяват да поемат отговорност за собствените си действия онлайн, като им посочва ясно, че поддържането на кибернетична хигиена е неделима част от офертата към потребителите[57]. За откриване и отстраняване на уязвимите места секторът трябва да се стреми да въвежда вътрешни процеси за разследване, групиране и коригиране на тези места, независимо дали източникът на потенциална уязвимост е бил външен или вътре в дадената компания.

**Ключови действия**

- Пълно прилагане на Директивата за сигурността на мрежите и информационните системи;
- Бързо приемане от Европейския парламент и от Съвета на регламента, определящ нов мандат за ENISA и европейска рамка за сертифициране[58];
- Съвместна инициатива на Комисията и промишлеността за дефиниране на принципа за задължителна предпазливост за намаляване на уязвимостта на продукти/софтуер и насърчаване на сигурността още при проектирането;
- Бързо прилагане на плана за реагиране при големи трансгранични инциденти;
- Започване на оценка на въздействието за проучване на възможността за предложение на Комисията през 2018 г. да се създаде мрежа от центрове за компетентност в сферата на киберсигурността и европейски център за изследвания и компетентност в сферата на киберсигурността, като се използва за основа непосредствена пилотна фаза;
- Подпомагане на държавите членки при определяне на области, в които общи проекти за киберсигурност могат да бъдат взети предвид за финансиране от Европейския фонд за отбрана;
- Единен портал за целия ЕС в помощ на пострадалите от кибератаки, предоставящ информация за най-новите заплахи и обединяващ практически съвети и инструменти за киберсигурност;
- Действия от страна на държавите членки за включване на киберсигурността в програмите за придобиване на умения, в електронното управление и в кампаниите за осведомяване;
- Действия от страна на промишлеността за усъвършенстване на обучението на персонала на предприятията във връзка с киберсигурността и за приемане на подхода „сигурност още при проектирането“ по отношение на техните продукти, услуги и процеси.

## 3. СЪЗДАВАНЕ НА ЕФЕКТИВНА СИСТЕМА НА ЕС ЗА КИБЕРВЪЗПИРАНЕ

Ефективно възпиране означава да се въведе кръг от мерки, които са надеждни и същевременно разубеждаващи евентуалните киберпрестъпници и извършители на кибератаки. Докато такива извършители — както недържавни, така и държавни — няма от какво друго да се боят освен от неуспех, те няма да имат много причини да се откажат. Един по-ефективен отговор за прилагане на закона, насочен към откриване, проследяване и съдебно преследване на киберпрестъпниците, има най-голямо значение за ефективно възпиране. Към това се добавя необходимостта ЕС да подпомага държавите членки за развиване на капацитет за киберотбрана с двойна употреба. Ще

[57] Някои производители вече са свикнали с тази концепция, тъй като някои европейски разпоредби относно продукти (като например Директива 2006/42/ЕО относно машините) предписват принципи за „безопасност още при проектирането“.

[58] COM (2017) 477.

започнем да обръщаме тенденцията на кибератаките само когато увеличим шансовете извършителите на такива атаки да бъдат залавяни и съдени. Кибератаките следва незабавно да се разследват и извършителите да бъдат подведени под съдебна отговорност, или да се предприемат действия за подходяща политическа или дипломатическа реакция. При сериозна криза с важно международно измерение и значение за отбраната Върховният представител може да представи пред Съвета варианти за подходящ отговор.

Една стъпка за усъвършенстване на реакцията на наказателното право спрямо кибератаки вече бе направена с приемането през 2013 г. на директивата относно атаките срещу информационните системи[59]. С нея се въвеждат минимални правила относно определението на престъпленията и определянето на наказанията за атаки срещу информационните системи и се вземат оперативни мерки за по-добро сътрудничество между органите. Директивата доведе до съществен напредък при криминализирането на кибератаките на сравнимо равнище във всички държави членки, което улеснява трансграничното сътрудничество между правоприлагащите органи, разследващи тези видове престъпления. Въпреки това все още има какво да се направи за реализиране на пълния потенциал на директивата, ако държавите членки приложат изцяло всичките ѝ разпоредби[60]. Комисията ще продължи да подпомага държавите членки при прилагането на директивата от тях и понастоящем не вижда необходимост да предлага изменения в нея.

### 3.1 Установяване на лицата, действащи злонамерено

За да увеличим нашите шансове да изправяме извършителите пред съд, е необходимо спешно да усъвършенстваме способността си да установяваме отговорните за кибератаките. Намирането на информация, полезна за разследванията на киберпрестъпления, най-вече във вид на цифрови следи, е главно предизвикателство за правоприлагащите органи. Затова е необходимо да увеличим нашите технологични възможности за ефективно разследване, включително чрез подсилване на звеното на Европол за киберпрестъпления с експерти в тази област. Европол се превърна в главно действащо лице за подпомагане на разследванията на държави членки в повече от една юрисдикция. Той следва да стане център за експертни познания и опит за онлайн разследвания и киберкриминалистика в помощ на правоприлагането от страна на държавите членки.

Широкоразпространената практика на повече от един потребител — понякога хиляди — да се дава един и същ IP адрес прави технически много трудно разследването на зловредно онлайн поведение. Също така понякога това изисква — например при сериозни престъпления като сексуално насилие над деца — да се проверяват голям брой потребители, за да бъде идентифицирано едно лице, действало злонамерено. По тази причина ЕС ще насърчи въвеждането на новия протокол (IPv6), тъй като той позволява един IP адрес да се използва само от един потребител, и така ще даде ясни предимства за прилагането на закона и за разследванията във връзка с киберсигурността. Като първа стъпка за насърчаване на това въвеждане Комисията ще включи във всички свои политики изискването за преминаване към IPv6, включително такива изисквания при обществените поръчки, финансирането на проекти и научни изследвания, както и подкрепа за необходимите материали за обучение. Освен това

[59] Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи.

[60] COM(2017) 474.

държавите членки следва да разгледат възможността за сключване на доброволни споразумения с доставчиците на интернет услуги, за да ускорят въвеждането на IPv6.

*Белгия е световен водач[61] по темп на въвеждане на IPv6 също благодарение на публично-частно партньорство: съответните заинтересовани страни възнамеряваха да ограничат използването на един IP адрес до максимум 16 потребители като част от доброволна мярка за саморегулиране, и това поощри преминаването към IPv6[62].*

Казано по-общо, необходимо е допълнително повишаване на отговорността за действията в интернет. Това означава да се предприемат мерки за предотвратяване на злоупотребата с имена на домейни за разпространение на нежелани електронни писма или за атаки с фалшива самоличност (фишинг). За целта Комисията ще работи за усъвършенстване на функционирането на системата за имена на домейни и системата IP WHOIS[63] и на наличието и точността на информацията в тях в съответствие с усилията на Интернет корпорацията за присвоени имена и адреси[64].

### 3.2 Подобряване на ответните мерки по правоприлагане

Ефективното **разследване** и **съдебно преследване** на престъпленията, извършвани чрез кибернетични средства, са най-важната възпираща мярка против кибератаки. Необходимо е обаче съществуващата процедурна рамка по-добре да се приспособи към възрастта на интернет[65]. Скоростта на кибератаките може да затрудни нашите процедури и също така да създаде определени нужди за незабавно трансгранично сътрудничество. С тази цел, както бе оповестено в Европейската програма за сигурност, в началото на 2018 г. Комисията ще представи предложения за **улесняване на достъпа до електронни доказателства в други държави**. Успоредно с това Комисията изпълнява практически мерки за улесняване на трансграничния достъп до електронни доказателства при наказателни разследвания, включително финансиране на обучения по трансгранично сътрудничество, разработване на електронна платформа за обмен на информация в рамките на ЕС и стандартизиране на формите за сътрудничество в съдебната област, използвани между държавите членки.

Друга пречка за ефективното наказателно преследване са различните криминалистични процедури за събиране на електронни доказателства при разследването на киберпрестъпления в различните държави членки. Това може да се коригира, като се работи за създаване на общи криминалистични стандарти. Освен това в подкрепа на проследяването и определянето на отговорност е необходимо да се подсилят свързаните с криминалистиката способности. Една стъпка би било по-нататъшното развитие на свързаните с криминалистиката способности на Европол, като се адаптират наличните бюджетни и човешки ресурси в Европейския център по киберпрестъпност към Европол, за да отговарят на нарастващата нужда от оперативна помощ при трансгранично разследване на киберпрестъпления. Друга стъпка би било да се имитира

---

61 https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption.

62 http://bipt.be/public/files/nl/22027/Raadpleging_ipv6.pdf.

63 Протокол за въпрос и отговор, широко използван за запитвания към бази данни, съхраняващи данни за регистрираните потребители или правоприемници на даден интернет ресурс.

64 Интернет корпорацията за присвоени имена и адреси (ICANN) е организация с нестопанска цел, която отговаря за координирането на поддръжката и процедурите на няколко бази данни, отнасящи се до пространствата на имена (namespaces) в интернет.

65 Само един пример: (виртуалният) централен сървър на бот мрежата (ботнет) Avalanche за командване и контрол променяше физическите сървъри и домейни на всеки пет минути.

изложеният по-горе технологичен фокус за криптиране, като се изследва как злоупотребата с него от страна на престъпниците създава значителни предизвикателства в борбата против сериозните престъпления, включително тероризъм и киберпрестъпления. Комисията ще оповести резултатите от сегашното изследване на **ролята на криптирането при наказателните разследвания**[66] най-късно до октомври 2017 г.[67]

При безграничния характер на интернет рамката за международно сътрудничество, дадена от **Будапещенската конвенция на Съвета на Европа за престъпленията в кибернетичното пространство**[68] предлага възможността група различни страни да използват оптимален правен стандарт за различните национални законодателства за справяне с киберпрестъпността. Понастоящем се проучва възможността за добавяне на протокол[69] към тази конвенция, който също може да осигури полезна възможност за решаване на въпроса за трансграничния достъп до електронни доказателства в международен контекст. Вместо да се създават нови международни правни инструменти по проблемите на киберпрестъпността, ЕС призовава всички държави да въведат подходящо национално законодателство и да си сътрудничат, използвайки тази съществуваща международна рамка.

Широката достъпност на инструменти за анонимност правят лесно престъпниците да се крият. „**Тъмната мрежа**“[70] („Даркнет“) разкри за престъпниците нови възможности за достъп до материали за сексуално насилие над деца, до наркотици и оръжие, често с незначителен риск да бъдат заловени[71]. Сега тази мрежа е основен източник и за средства като зловреден софтуер и хакерски инструменти, използвани при киберпрестъпления. Комисията, съвместно със съответните заинтересовани страни, ще анализира националните подходи с цел да определи нови решения. Европол следва да улеснява и подкрепя разследвания на „тъмната мрежа“, да оценява заплахите, да съдейства за определяне на юрисдикция и да степенува по приоритетност високорисковите случаи, а ЕС може да играе водеща роля при координирането на международните действия[72].

---

66 Председателство на Съвета, „Резултати от заседанието на Съвета по правосъдие и вътрешни работи на 8 и 9 декември 2016 г.“, № 15391/16.

67 Осми доклад за напредъка към постигането на ефективен и истински Съюз на сигурност, 29 юни 2017 г., COM(2017) 354 final.

68 Конвенцията е първият международен договор относно престъпленията, извършвани чрез интернет и други компютърни мрежи, като третира по-специално нарушенията на авторското право, компютърните измами, детската порнография и нарушаването на мрежовата сигурност. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 До 2017 г. 55 правителства са ратифицирали Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство или са се присъединили към нея.

69 Задание за подготовката на проект за Втори допълнителен протокол към Будапещенската конвенция за престъпленията в кибернетичното пространство T-CY (2017)3.

70 „Тъмната мрежа“ се състои от съдържание в насложени една върху друга мрежи, които използват интернет, но изискват специфичен софтуер, специфични конфигурации или разрешение за достъп. „Тъмната мрежа“ представлява малка част от deep web — онази част от интернет, която не се индексира от търсачките.

71 Забележително изключение е неотдавнашното разбиване на две от най-големите престъпни места за търговия в „тъмната мрежа“ (скритият интернет): AlphaBay и Hansa: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

72 Европол вече играе важна роля в тази област. За пример от неотдавна вж.: https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation.

Една разрастваща се област на престъпна дейност в киберпространството е използването на данни от кредитни карти или други електронни средства за разплащане с цел измама. Документите за идентифициране при плащане, до които се достига чрез кибератаки срещу онлайн търговци или други легитимни предприятия, след това се търгуват онлайн и могат да бъдат използвани от престъпници за извършване на измами[73]. Комисията представя предложение за **Директива за борба срещу измамите и фалшифицирането на непарични платежни средства**[74]. Тя има за цел актуализиране на съществуващите правила в тази област и засилване на способността за прилагате на закона за справяне с този вид престъпления.

Нужно е да се подобрят и възможностите на правоприлагащите органи на държавите членки за разследване на киберпрестъпления, както и разбиранията на прокурорите и съдиите относно престъпленията, извършвани чрез кибернетични средства, и възможностите за тяхното разследване. Агенцията на Европейския съюз за сътрудничество в областта на наказателното правосъдие (Евроюст) и Европол допринасят за тази цел и за по-добра координация, в тясно сътрудничество със специализирани консултативни групи в рамките на центъра по киберпрестъпност към Европол и с мрежите от ръководители на звена за борба с киберпрестъпността и прокурори, специализирани в тази област. Комисията ще отпусне финансиране в размер на 10,5 милиона евро за борба с киберпрестъпността, главно от своя **Фонд „Вътрешна сигурност“ — програма „Полиция“**. Обучението е важен елемент и Европейската група за обучение и образование в областта на киберпрестъпността е разработила полезни материали. Сега с помощта на Агенцията на Европейския съюз за обучение в областта на правоприлагането (CEPOL) те следва да се разпространяват широко сред специалистите, прилагащи закона.

### 3.3 Публично-частно сътрудничество срещу киберпрестъпността

Ефективността на традиционните механизми за правоприлагане е подложена на изпитание от особеностите на дигиталния свят, който се състои най-вече от инфраструктура, която е частна собственост, и многобройни различни участници, намиращи се в най-различни юрисдикции. По тази причина сътрудничеството с частния сектор, включително промишлеността и гражданското общество, е от съществено значение за ефективната борба на държавните органи с престъпността. В този контекст финансовият сектор също е от ключово значение и сътрудничеството с него следва да се разшири. Необходимо е например да се засили ролята на звената за финансово разузнаване[75] във връзка с киберпрестъпността.

*Някои държави членки вече предприеха важни стъпки. В Нидерландия финансовите институции и правоприлагащите органи работят рамо до рамо в Оперативната група по електронни престъпления за борба против измамите в интернет и киберпрестъпността. Германският център за компетентност против киберпрестъпността осигурява за своите членове оперативен център за обмен на информация в тясно сътрудничество с Германската федерална полиция и за*

[73] Приходите от измами са важен източник на доходи за организираната престъпност и затова правят възможни други престъпни дейности като тероризъм, трафик на наркотици и на хора.

[74] COM(2017) 489.

[75] Звената за финансово разузнаване служат за национални центрове за приемане и анализ на съобщения за подозрителни трансакции и на друга информация във връзка с пране на пари, свързани с това предполагаеми престъпления и финансиране на тероризма, и за разпространение на резултатите от този анализ.

*разработване на мерки, осигуряващи защита срещу киберпрестъпления. Шестнадесет държави членки[76] създадоха центрове за високи постижения в борбата с киберпрестъпността, за да улеснят сътрудничеството между правоприлагащите органи, академичните институции и частните партньори за създаване и обмен на най-добри практики, за обучение и изграждане на капацитет.*
*Комисията подкрепя създаването на публично-частни партньорства и механизми за сътрудничество чрез конкретни проекти като например Мрежата от експерти по киберпрестъпност и център за борба против измамите в интернет[77], прилагащи модел и стандарт за обмен на информация с цел анализиране на рисковете от електронни престъпления и онлайн измами и смекчаване на последиците от такива престъпления и измами.*

В контекста на киберпрестъпността е необходимо частните предприятия да могат да обменят с правоприлагащите органи информация относно конкретни инциденти, включително лични данни, при стриктно спазване на правилата за защита на данните. Реформата на ЕС в областта на защитата на данните, която ще се прилага от месец май 2018 г., дава кръг от правила, определящи условията, при които правоприлагащи органи и частни субекти може да си сътрудничат. Европейската комисия ще работи с Европейския комитет по защита на данните и със съответните заинтересовани страни за определяне на най-добри практики в тази област и за предоставяне на насоки, където това е уместно.

### 3.4 Засилване на политическия отговор

Приетата неотдавна **рамка за съвместен дипломатически отговор на ЕС на злонамерените дейности в киберпространството**[78] („Инструментариум за кибердипломация“) определя мерките съгласно общата външната политика и политика на сигурност, включително ограничителни мерки, които могат да се използват за засилване на реакцията на ЕС на действия, които вредят на политическите и икономическите интереси на Съюза и на неговите интереси в областта на сигурността. Тази рамка представлява важна стъпка в развитието на капацитет за сигнализиране и реагиране на равнище ЕС и на равнище държави членки. Тя ще увеличи нашите възможности за определяне на източниците на злонамерени действия в киберпространството, за да се повлияе върху поведението на потенциални агресори, като същевременно се отчита необходимостта от осигуряване на пропорционален отговор. Определянето дали дадено действие произхожда от държавно или от недържавно действащо лице остава независимо политическо решение, основано на сведения от всички възможни източници. Работата с държавите членки за прилагане на рамката понастоящем продължава и ще напредва при тясно съгласуване с плана за реагиране при широкомащабни киберинциденти[79]. Сведенията относно ситуацията, необходими за прилагането на мерки в кръга на тази рамка, следва да се обобщават,

[76] Австрия, Белгия, България, Великобритания, Германия, Гърция, Естония, Ирландия, Испания, Кипър, Литва, Полша, Румъния, Словения, Франция и Чешка република.

[77] Инициативата EU-OF2CEN има за цел да направи възможен обмена на информация, свързана с измами в интернет, между банки и правоприлагащи служби в целия ЕС, за да се предотвратят плащания към измамници и „мулета“ за изпирането на пари и да се разследват и дават под съд извършителите. Тя се съфинансира от ЕС (Фонд „Вътрешна сигурност“ — програма „Полиция).

[78] http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-cyber-diplomacy-toolbox/.

[79] C(2017) 6100.

анализират и споделят от INTCEN[80], работещ в тясно сътрудничество с държавите членки и институциите на ЕС.

### 3.5 Изграждане на възможности за възпиране за киберсигурност чрез отбранителния капацитет на държавите членки

Държавите членки вече разработват мерки за киберотбрана. Освен това при размиването на границите между киберотбрана и киберсигурност, възможната двойна употреба на киберинструменти и технологии, както и при големите различия в подходите на различните държави членки, ЕС има възможност да съдейства за насърчаване на синергия между военните и гражданските усилия[81].

Онези държави членки, които разполагат с по-силни възможности в сферата на киберсигурността и желаят да ги обединят, може да разгледат — със съдействие от страна на Върховния представител, Комисията и Европейската агенция по отбрана — възможността за включване на киберотбраната в рамката на постоянното структурирано сътрудничество (ПСС). Това може да бъде подкрепено от описаната по-горе работа за насърчаване на промишления капацитет и стратегическата автономност на ЕС. Съюзът може също така да съдейства за оперативна съвместимост, включително чрез подпомагане на усилията за развитие на капацитета, координиране на обучението и образованието и стандартизация на изделията с двойна употреба.

Следва да се използва в максимална степен съвместната рамка за борба с хибридни заплахи, които често включват кибератаки, по-специално чрез звеното на ЕС за синтез на информацията за хибридните заплахи, и неотдавна създаденият Европейски център за борба с хибридните заплахи, разположен в Хелзинки, чиято мисия е да насърчава стратегическия диалог и да извършва научни изследвания и анализи.

Съюзът ще наблегне отново на политическата рамка на ЕС за кибернетична отбрана от 2014 г.[82] като инструмент за по-нататъшно интегриране на киберсигурността и отбраната в общата политика за сигурност и отбрана (ОПСО). От съществено значение е устойчивостта на самите мисии и операции по ОПСО срещу кибератаки: ще бъдат разработени стандартни процедури и технически възможности, които могат да са в помощ на разгърнати мисии и операции — както граждански, така и военни, и също на съответните структури „Способности за планиране и провеждане на операции“ и на доставчиците на ИТ услуги на Европейската служба за външна дейност (ЕСВД). За засилване на сътрудничеството между държавите членки и по-добро насочване на усилията на Съюза в тази област Европейската агенция по отбрана и ЕСВД, в сътрудничество със службите на Комисията, ще съдействат за ангажиране на стратегическо равнище на определящите политиката в областта на отбраната на държавите членки. ЕС ще подпомага също и разработването на решения за сигурност на европейското киберпространство като част от усилията в подкрепа на европейската отбранителна технологична и индустриална база. Това включва и подпомагане на регионални клъстери за високи постижения в сектора на киберсигурността и отбраната.

Като работят в тясно сътрудничество с ЕСВД, с държавите членки и с други подходящи органи на ЕС, до 2018 г. службите на Комисията ще пуснат в действие **платформа за образование и обучение в областта на киберотбраната** за справяне със сегашния

[80] JOIN(2016) 018 final.

[81] ЕС разбира, че също както земята, въздуха и морето, киберпространството е поле за действие. Действията за киберотбрана включват и защитата и устойчивостта на космическите активи и съответната наземна инфраструктура.

[82] www.consilium.europa.eu/en/workarea/downloadasset.aspx?id=40802190515.

недостиг на умения по киберотбрана. Платформата ще допълва работата на Европейската агенция по отбрана в тази област, като спомага за решаване на проблема с недостатъчните умения в областта на киберсигурността и киберотбраната.

**Ключови действия**

- Инициатива на Комисията за трансграничен достъп до електронни доказателства (началото на 2018 г.);
- Бързо приемане от Европейския парламент и от Съвета на предложената Директива за борба срещу измамите и фалшифицирането на непарични платежни средства;
- Въвеждане на изисквания за IPv6 при обществените поръчки, научните изследвания и финансирането на проекти в ЕС; доброволни споразумения между държавите членки и доставчиците на интернет услуги за ускоряване на въвеждането на IPv6;
- Подновено/разширено внимание в Европол към киберкриминалистиката и наблюдение на „тъмната мрежа“ (скрития интернет);
- Прилагане на рамката за общ дипломатически отговор на ЕС на зловредните действия в киберпространството;
- Допълнителна финансова подкрепа за национални и международни проекти за по-добро наказателно правосъдие в киберпространството.
- Стартиране през 2018 г. на образователна платформа по въпросите на киберсигурността за справяне със сегашния недостиг на умения във връзка с киберсигурност и киберотбрана.

## 4. УКРЕПВАНЕ НА МЕЖДУНАРОДНОТО СЪТРУДНИЧЕСТВО В СФЕРАТА НА КИБЕРСИГУРНОСТТА

Ръководена от основните ценности и права като свобода на изразяване, право на неприкосновеност на личния живот и защита на личните данни, и утвърждаването на открито, свободно и сигурно киберпространството, политиката на ЕС за международна киберсигурност има за цел да отговори на постоянно развиващото се предизвикателство да се поддържа стабилност на световното киберпространство и да допринесе за стратегическата независимост на Европа в киберпространството.

### 4.1 Киберсигурност във външните отношения

Фактите сочат, че хората във всички части на света определят кибератаките от други държави за една от най-важните заплахи за националната сигурност[83]. При глобалния характер на заплахите изграждането и поддържането на здрави съюзи и партньорства с трети държави има основно значение за предотвратяването и възпирането на кибератаки, които влияят все повече върху международната стабилност и сигурност. ЕС ще счита създаването на стратегическа рамка за предотвратяване на конфликти и за стабилност в киберпространството за приоритет в своите двустранни, регионални, многостранни ангажименти и в ангажиментите си с много на брой заинтересовани страни.

ЕС силно подкрепя становището, че международното право и по-специално Хартата на ООН, е в сила в киберпространството. Като допълнение към задължителните международни правни норми ЕС подкрепя доброволните незадължителни норми,

[83] Пролет 2017 г., Проучване на световните нагласи, Център за изследвания „Пю“ (Pew Research Centre).

правила и принципи за отговорно държавно поведение, формулирани от групата правителствени експерти към ООН[84]; освен това Съюзът насърчава разработването и прилагането на регионални мерки за изграждане на доверие, както в рамките на Организацията за сигурност и сътрудничество в Европа, така и в други региони.

На двустранно равнище диалогът относно киберсигурността[85] ще бъде допълнително развит и допълнен от усилия за улесняване на сътрудничеството с трети държави за укрепване на принципите на надлежни проверки и държавна отговорност в киберпространството. ЕС ще счита въпросите на международната сигурност в киберпространството за приоритет в своите международни ангажименти, същевременно обръщайки внимание киберсигурността да не се превръща в претекст за протекция на пазари и ограничаване на основни права и свободи, включително свобода на изразяване и достъп до информация. Комплексният подход към киберсигурността изисква зачитане на правата на човека и ЕС ще продължи да подкрепя основните ценности на Съюза в световен мащаб, доразвивайки своите насоки относно правата на човека за свободата в интернет[86]. В това отношение Съюзът подчертава значението на участието на всички заинтересовани страни в управлението на интернет.

Освен това Комисията представи предложение[87] за модернизиране на контрола на ЕС върху износа, включително въвеждане на контрол върху износа на критични технологии за кибернаблюдение, които могат да причинят нарушения на човешките права или с тях да се злоупотреби срещу собствената сигурност на ЕС, и ще развива диалога с трети държави за насърчаване на глобално сближаване и отговорно поведение в тази област.

### 4.2 Изграждане на капацитет за киберсигурност

Глобалната стабилност в киберпространството разчита на местната и националната способност на всички държави да предотвратяват и да реагират на киберинциденти, и да разследват и съдебно да преследват случаите на киберпрестъпления. Подпомагането на усилията за изграждане на устойчивост в трети държави ще увеличи равнището на киберсигурността в глобален мащаб, а това ще има положителни последици за ЕС. Противодействието на бързо развиващите се киберзаплахи е свързано с необходимост от действия за обучение, за разработване на политики и законодателство, както и от ефективно функциониращи екипи за незабавно реагиране при компютърни инциденти и звена за борба с киберпрестъпленията във всички държави в света.

От 2013 г. ЕС е лидер в изграждането на международен капацитет за киберсигурност и систематично свързва тези усилия със сътрудничеството за развитие. ЕС ще продължи да насърчава модел на изграждане на капацитет, основан на правата, в съответствие с подхода Digital4Development (цифрови технологии за развитие)[88]. Приоритетите за изграждане на капацитет ще са съседните на ЕС държави и развиващите се държави, в които свързаността нараства бързо и заплахите се развиват с висока скорост. Усилията на Съюза ще допълват програмата на ЕС за развитие в светлината на Програмата за устойчиво развитие до 2030 г. и цялостните действия за изграждане на институционален капацитет.

---

[84] A/68/98 и A/70/174.

[85] През септември 2017 г. ЕС проведе разговори относно киберпространството със САЩ, Китай, Япония, Република Корея и Индия.

[86] Насоки на ЕС за правата на човека относно свободата на изразяване онлайн и офлайн.

[87] COM(2016) 616.

[88] SWD(2017) 157.

За подобряване на способността на ЕС да мобилизира своите колективни експертни знания и опит в помощ на изграждането на такъв капацитет следва да се създаде специална мрежа на ЕС за изграждане на киберкапацитет, обединяваща ЕСВД, органите на държавите членки, отговарящи за киберпространството, агенции на ЕС, службите на Комисията, академичните институции и гражданското общество. Ще бъдат разработени насоки на ЕС за изграждане на киберкапацитет, които ще спомогнат за по-добро политическо ръководство и определяне на приоритети на действията на ЕС за подпомагане на трети държави.

Също така ЕС ще работи съвместно с други донори в тази област, за да се избегне дублирането на усилията и да се съдейства за по-целенасочено изграждане на капацитет в различните региони.

### 4.3 Сътрудничество между ЕС и НАТО

Надграждайки съществения напредък, който вече е постигнат, ЕС ще задълбочава сътрудничеството с НАТО в областта на киберсигурността, хибридните заплахи и отбраната, както предвижда съвместната декларация от 8 юли 2016 г.[89] Приоритетите включват насърчаване на оперативната съвместимост чрез ясни изисквания и стандарти, засилване на сътрудничеството при обучение и учения, хармонизиране на изискванията за обучение.

ЕС и НАТО ще подпомагат също и сътрудничеството в научните изследвания и иновации за киберотбраната и ще развиват съществуващото техническо споразумение за обмен на информация относно киберсигурността между техните съответни органи по киберсигурност[90]. Неотдавнашните съвместни постижения за противодействие на хибридните заплахи, по-специално сътрудничеството между Звеното на ЕС за синтез на информацията за хибридните заплахи и клона, създаден в рамките на НАТО за анализ на хибридните заплахи, следва да се развиват допълнително за засилване на устойчивостта и по-успешно реагиране при киберкризи. По-нататъшното сътрудничество между ЕС и НАТО ще се подпомага чрез учения за киберотбрана с участието на ЕСВД и други органи на ЕС и съответните органи на НАТО, включително Съвместният експертен център на НАТО за кибернетична защита, разположен в Талин. За пръв път НАТО и ЕС ще проведат успоредни и координирани учения за реагиране на сценарий за хибридна заплаха, като НАТО ще води ученията през 2017 г., а през 2018 г. ЕС на свой ред ще поеме водеща роля. Следващият доклад относно сътрудничеството между ЕС и НАТО, който ще бъде представен на съответните Съвети през 2017 г., ще предложи да се разгледат възможностите за по-нататъшно разширяване на сътрудничеството, по-специално чрез осигуряване на общи, сигурни и надеждни начини за комуникация между всички участващи съответни институции, включително ENISA.

**Ключови действия**

- Осъществяване на напредък по стратегическата рамка за предотвратяване на конфликти и за стабилност в киберпространството;
- Създаване на нова мрежа за изграждане на капацитет за подпомагане на способността на трети държави да се справят с киберзаплахи, и разработване на насоки на ЕС за изграждане на киберкапацитет, за да се определят по-успешно приоритетите в усилията на Съюза;

[89] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/.

[90] CERT-EU и центърът на НАТО за реагиране при инциденти с компютърната сигурност (NCIRC).

- По-нататъшно сътрудничество между ЕС и НАТО, включително участие в успоредни и координирани учения и по-добра оперативна съвместимост на стандартите за киберсигурност.

## 5. ЗАКЛЮЧЕНИЕ

Готовността за справяне с киберзаплахи е от основно значение както за цифровия единен пазар, така и за нашия Съюз за сигурност и отбрана. Укрепването на европейската киберсигурност и справянето със заплахите към граждански и военни цели са задължителни.

Предстоящата среща на върха на 29 септември 2017 по въпросите на цифровите технологии, организирана от председателството на Естония, предоставя възможност да се покаже обща решимост киберсигурността да бъде поставена в центъра на ЕС като цифрово общество. Комисията призовава държавите членки като част от тази обща отговорност да поемат ангажимент за начина, по който възнамеряват да действат в областите, в които носят главната отговорност. Това следва да включва укрепване на киберсигурността чрез:

- Осигуряване на пълно и ефективно прилагане на директивата за МИС най-късно до 9 май 2018 г., както и необходимите ресурси, за да могат държавните органи, отговарящи за киберсигурността, да изпълняват ефективно своите задачи;
- Прилагане на същите правила към публичните администрации поради ролята, която имат в обществото и в икономиката като цяло;
- Осигуряване на обучение по въпроси на киберсигурността в публичната администрация;
- Определяне на осведомеността в кибернетичната област за приоритет в информационните кампании и включване на киберсигурността в академичните и професионалните учебни програми;
- Използване на инициативи на Постоянното структурирано сътрудничество (ПСС) и Европейския фонд за отбрана за подпомагане на разработването на проекти в сферата на киберотбраната.

Настоящото съвместно съобщение определя мащаба на предизвикателството и кръга от мерки, които ЕС може да вземе. Нужна ни е Европа, която е устойчива, която може ефективно да защити своите граждани чрез предвиждане на възможни инциденти в сферата на киберсигурността, чрез изграждане на силна защита в своите структури и поведение, чрез бързо възстановяване от евентуални кибератаки и чрез възпиране на отговорните за такива атаки. Това съобщение предлага целенасочени мерки, които допълнително ще укрепят структурите и капацитета на ЕС за киберсигурност по един координиран начин, с пълното съдействие на държавите членки и различните засегнати структури на ЕС и при зачитане на техните компетенции и отговорности. Неговото изпълнение ще покаже ясно, че ЕС и държавите членки ще работят съвместно за въвеждане на стандарт за киберсигурност, съответстващ на постоянно нарастващите предизвикателства, пред които днес Европа е изправена.