ЕВРОПЕЙСКА СМЕТНА ПАЛАТА

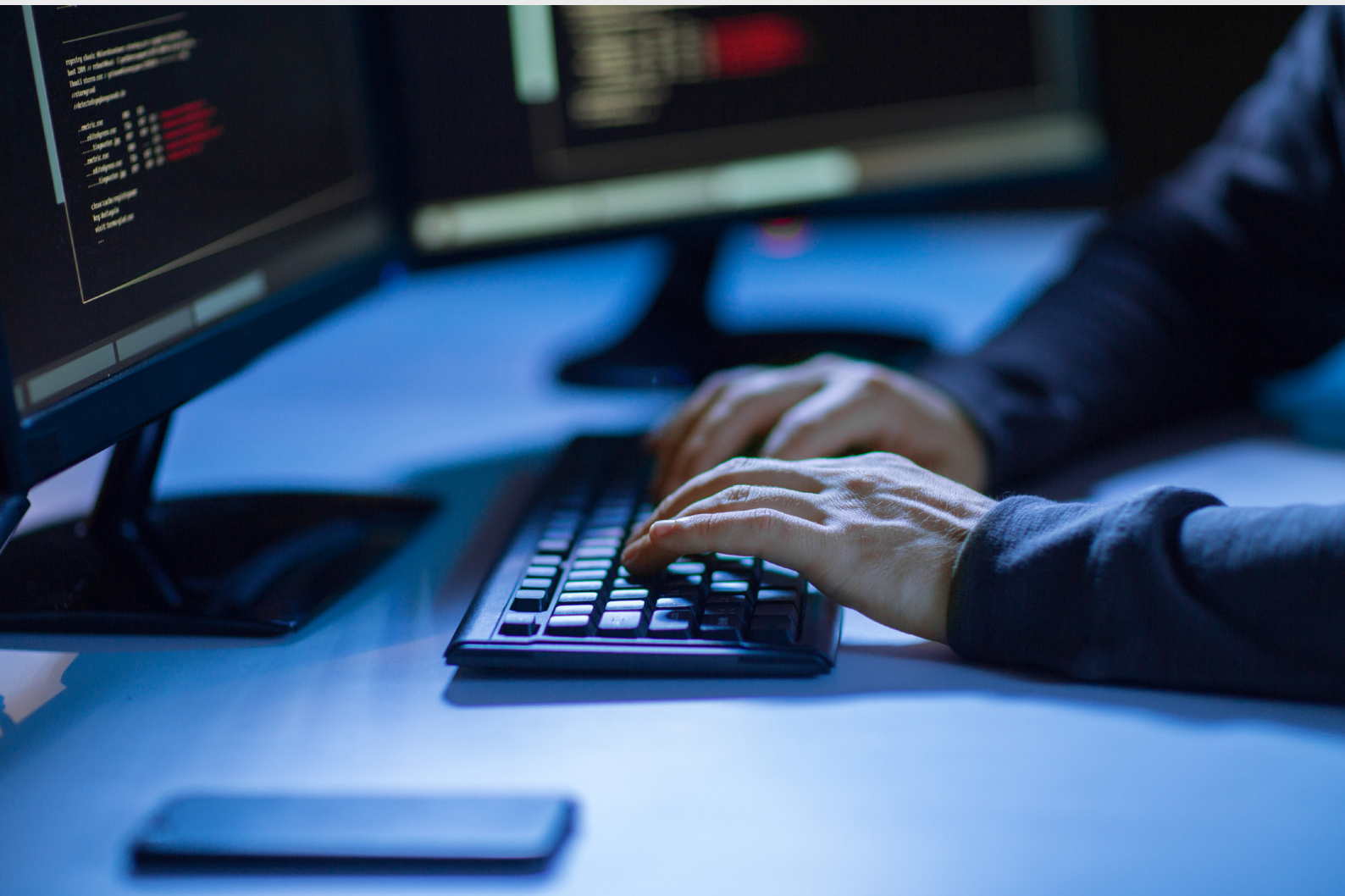
BG

2019

Предизвикателства пред ефективното прилагане на политиката за киберсигурност на ЕС

Информационно-аналитичен документ

Март 2019 г.



Относно документа:

Целта на настоящия информационно-аналитичен документ, който не е одитен доклад, е да представи сложният контекст на политиката за киберсигурност на ЕС и да идентифицира основните предизвикателства пред ефективното осъществяване на тази политика. В него са обхванати темите за мрежовата и информационна сигурност, кибрепрестъпленията, киберзащитата и дезинформацията. Той ще бъде използван и за бъдеща одитна дейност в тази област.

ЕСП основа анализа си на документна проверка на публично достъпната информация в официални документи, документи за изразяване на позиция и проучвания на трети страни. Работата на терен на ЕСП беше извършена между април и септември 2018 г., и бяха взети предвид и развитията до декември 2018 г. ЕСП допълни дейността си с проучване сред националните одитни институции на държавите членки и чрез събеседвания с основни заинтересовани страни от институциите на ЕС и с представители от частния сектор.

Установените предизвикателства са групирани в четири широки групи: i) рамка на политиката; ii) финансиране и разходи; iii) изграждане на устойчивост на киберпространството; iv) ефективно реагиране на киберинциденти. Постигането на по-високо равнище на киберсигурност в ЕС остава неотложно изпитание. Предвид това всяка глава завършва с редица идеи за по-нататъшен размисъл от страна на лицата, изготвящи политиките, законодателите и практиците.

ЕСП би желала да изкаже благодарност за конструктивната обратна информация, която получи от службите на Комисията, Европейската служба за външна дейност, Съвета на Европейския съюз, ENISA, Европол, Европейската организация по киберсигурност и националните одитни институции на държавите членки.

Съдържание

Кратко изложение

I Технологиите създават безброй нови възможности, а новите продукти и услуги стават неразделна част от нашето ежедневие. От своя страна рискът да станем жертва на киберпрестъпление или на кибератака расте, а общественото и икономическото въздействие от това продължава да се увеличава. Предвид това стремежът на Европейския съюз в последните години да ускори усилията за укрепване на киберсигурността и своята цифрова автономност е много навременен.

II Настоящият информационно-аналитичен документ, който не е одитен доклад и се основава на публично достъпна информация, има за цел да направи общ преглед на сложния и разнороден контекст на политиката и да идентифицира основните предизвикателства пред ефективното осъществяване на тази политика. Обхватът на документа на ЕСП включва политиката на ЕС за киберсигурността, както и за киберпрестъпността и киберотбраната, като обхваща и усилията за борба с дезинформацията. Установените от нас предизвикателства са групирани в четири широки групи: i) рамка на политика и законодателство; ii) финансиране и разходи; iii) изграждане на киберустойчивост; и iv) ефективна реакция при кибер инциденти. Всяка глава включва няколко елемента за размисъл по представените предизвикателства.

Рамка на политиката и законодателна рамка

III Разработването на действия, съгласувани с общите цели на стратегията на ЕС за киберсигурност за превръщане на ЕС в най-безопасната цифрова среда в света, е предизвикателство поради липсата на измерими цели и достатъчно надеждни данни. Резултатите рядко се измерват и много малък брой области на политиката са оценени. Ето защо ключово предизвикателство е **да се гарантира значима отчетност и оценка** чрез преминаване към култура на изпълнение с интегрирани практики за оценяване.

IV Законодателната рамка остава непълна. **Пропуските в правото на ЕС и неговото непоследователно транспониране** може да затруднят достигането на пълния потенциал на законодателството.

Финансиране и разходи

V **Съгласуването на равнищата на инвестициите с целите** не е лесно: това изисква да се увеличат не само общите инвестиции в киберсигурността – които

в ЕС са малки и фрагментирани – но също така и въздействието, по-специално чрез по-добро използване на резултатите от разходите за научни изследвания и гарантиране на ефективното насочване и финансиране на стартиращи предприятия.

VI **Наличието на ясна представа за разходите на ЕС** е от съществено значение, за да могат ЕС и неговите държави членки да преценят кои пропуски да отстранят, така че да изпълнят своите заявени цели. Тъй като няма специален бюджет на ЕС за финансиране на стратегията за киберсигурността, липсва и яснота какви средства се изразходват за това.

VII В период на засилени политически приоритети в областта на сигурността **ограниченията при предоставянето на достатъчно ресурси на свързаните с киберсигурността агенции на ЕС** може да възпрепятстват осъществяването на амбициите на ЕС. Преодоляването на това предизвикателство е свързано с намирането на начини за привличане и задържане на таланти.

Изграждане на киберустойчивост

VIII В публичния и частния сектор на ЕС, както и на международно равнище, съществуват множество слабости при управлението на киберсигурността. Това намалява способността на световната общност за реагиране и ограничаване на кибератаките и възпрепятства прилагането на последователен подход в целия ЕС. Следователно предизвикателството е да **се укрепи управлението на киберсигурността**.

IX **Повишаването на уменията и осведомеността** във всички сектори и на всички равнища на обществото е от съществено значение с оглед на нарастващия недостиг на умения в сферата на киберсигурността в световен мащаб. Понастоящем съществуват ограничени стандарти за целия ЕС по отношение на обучението, сертифицирането или оценката на риска за киберсигурността.

X Изграждането на основа за доверие е от първостепенно значение за укрепването на цялостната киберустойчивост. По оценки на самата Комисия координацията като цяло все още е недостатъчна. **Подобряването на обмена на информация и координацията** между публичния и частния сектор остава предизвикателство.

Ефективно реагиране на киберинциденти

XI Цифровите системи станаха толкова сложни, че е невъзможно да се предотвратят всички атаки. Отговорът на това предизвикателство е **бързото откриване и реакция**. Киберсигурността обаче все още не е напълно интегрирана в съществуващите механизми за координация в отговор на кризи на равнището на ЕС, което потенциално ограничава способността на ЕС да реагира при широкомащабни трансгранични киберинциденти.

XII **Защитата на критичната инфраструктура и обществените функции** е от основно значение. Потенциалната намеса в изборните процеси и дезинформационните кампании са основно предизвикателство.

XIII Настоящите предизвикателства, които киберзаплахите поставят пред ЕС и по-широката глобална среда, изискват траен ангажимент и продължаващо неотклонно спазване на основните ценности на ЕС.

Въведение

01 Технологиите създават безброй нови възможности. С появата на нови продукти и услуги те стават неразделна част от нашето ежедневие. С всяка нова разработка обаче нашата технологична зависимост се повишава, както и значението на киберсигурността. Колкото повече лични данни предоставяме онлайн и колкото по-свързани ставаме, толкова по-вероятно е да станем жертва на някаква форма на киберпрестъпление или кибератака.

Какво представлява киберсигурността?

02 Не съществува стандартно, общоприето определение за киберсигурност[1]. Най-общо казано това са всички приети предпазни мерки за защита на информационните системи и техните ползватели от неразрешен достъп, атаки и вреди, за да се гарантира поверителността, целостта и наличността на данните.

03 Киберсигурността включва предотвратяване, откриване, реагиране и възстановяване от киберинциденти. Инцидентите могат да бъдат преднамерени или не и да варират например от случайно оповестяване на информация до атаки на предприятия и критична инфраструктура, кражба на лични данни и дори намеса в демократичните процеси. Всички те могат да имат широкообхватни неблагоприятни последици за отделните хора, организациите и общностите.

04 Като термин, използван в политическите кръгове на ЕС, киберсигурността не се ограничава до мрежовата и информационната сигурност. Тя обхваща всяка незаконна дейност, свързана с използването на цифрови технологии в киберпространството. Следователно това може да включва киберпрестъпления като стартиране на атаки с компютърни вируси и измами с непарични платежни средства, като това може да премине границата между системите и съдържанието, както при онлайн разпространението на материали, съдържащи сексуално насилие над деца. Киберсигурността може да обхваща и дезинформационни кампании за оказване на влияние върху онлайн дебати и подозирана намеса в избори. Освен това Европол счита, че има сближаване между киберпрестъпността и тероризма[2].

05 Различни субекти – включително държави, престъпни групи и хактивисти – предизвикват киберинциденти, водени от различни мотиви. Последиците от тези

инциденти се усещат на национално, европейско и дори на световно равнище. Нематериалният и до голяма степен транснационален характер на интернет и използваните инструменти и тактики обаче често затрудняват установяването на извършителя на атаката (така наречения „проблем с определянето на отговорност“).

06 Многобройните видове заплахи за киберсигурността могат да бъдат класифицирани според това, което правят с данните – разкриване, изменение, унищожаване или нерегламентиран достъп – или с основните принципи на информационна сигурност, които нарушават, както е показано на ***фигура 1*** по-долу. В ***каре 1*** са описани някои примери за атаки. Тъй като атаките срещу информационните системи стават все по-сложни, нашите механизми за защита губят своята ефективност[3].

Фигура 1 – Видове заплахи и принципите на сигурност, които те излагат на риск

Източник: ЕСП, въз основа на изменено проучване на Европейския парламент[4]. Катинар = няма отражение върху сигурността; удивителен знак = риск за сигурността

Каре 1

Видове кибератаки

Всеки път, когато ново устройство бъде регистрирано в интернет или се свърже с други устройства, така наречената „изложена на атака повърхност“ на киберсигурността се увеличава. Експоненциалният растеж на „интернет на нещата“, изчислителните облаци, големите данни и цифровизацията на промишлеността са съпътствани от по-голямо излагане на уязвимости, което позволява на злонамерените лица да засегнат още повече потърпевши. Много трудно е да се поддържа необходимото темпо на развитие предвид разнообразието на видовете атаки и тяхната нарастваща сложност[5].

Малуерът (зловредният софтуер) е предназначен да причинява вреди на устройства или мрежи. Той може да включва вируси, „троянски коне“, софтуер за изнудване, компютърни червеи, адуер и шпионски софтуер. **Софтуерът за изнудване** криптира данните и предотвратява достъпа на потребителите до техните файлове, докато не бъде платен откуп, обикновено в криптовалута, или не бъде извършено определено действие. Според Европол атаките със софтуер за изнудване преобладават като цяло, а броят на видовете софтуер за изнудване рязко се е увеличил през последните няколко години. **Атаките от типа „отказ от обслужване** (DDoS), които правят услугите или ресурсите недостъпни чрез заливането им с повече заявления, отколкото те да могат да изпълняват, също бележат ръст, като през 2017 г. една трета от организациите са били изправени пред този вид атаки[6].

Потребителите могат да бъдат манипулирани неволно да извършат някакво действие или да разкрият поверителна информация. Тази измама може да се използва за кражба на данни или кибершпионаж и е известна като **социално инженерство**. Има различни начини да се постигне това, но широко разпространен метод е **фишингът**, при който електронни писма, които изглеждат изпратени от достоверни източници, подвеждат потребителите да разкрият информация или да щракнат върху връзки, които ще заразят устройствата им с изтеглен малуер. Повече от половината държави членки докладват за разследвания на атаки в мрежата[7].

Може би най-злонамерени сред видовете заплахи са **комплексните устойчиви заплахи** (КУЗ). Това са комплексни нарушители, които извършват дългосрочен мониторинг и кражба на данни, а понякога имат и деструктивни цели. Целта им е да останат незабелязани и да не бъдат разкрити възможно най-дълго време. КУЗ често са свързани с държавата като цяло и са насочени към особено чувствителни сектори като технологии, отбрана и критична инфраструктура. Счита се, че най-малко една четвърт от всички киберинциденти и по-голямата част от разходите са свързани с кибершпионаж[8].

Колко сериозен е проблемът?

07 Въздействието на недостатъчната подготвеност за кибератаки е трудно за отчитане поради липсата на надеждни данни. Икономическото въздействие на киберпрестъпността е нараснало петкратно в периода 2013—2017 г.[9] и е засегнало правителства и предприятия, както големи, така и малки. Прогнозираният ръст на премиите по киберзастраховките от 3 млрд. евро през 2018 г. на 8,9 млрд. евро през 2020 г. е отражение на тази тенденция.

08 Въпреки че финансовото отражение на кибератаките продължава да нараства, наблюдава се тревожно несъответствие между разходите за стартиране на атака и разходите за предотвратяване, разследване и възстановяване. Например извършването на DDoS атака може да струва едва 15 евро на месец, докато загубите, понесени от предприятието, към което е насочена, в т.ч. вредите за неговата репутация, са значително по-големи[10].

09 Въпреки че през 2016 г. 80 % от предприятията в ЕС са претърпели най-малко един киберинцидент[11], признаването на рисковете продължава да бъде на тревожно ниско ниво. Сред дружествата в ЕС 69 % нямат никаква информация или имат само основна информация за своята уязвимост към киберзаплахи[12], а 60 % никога не са правили оценка на потенциалните финансови загуби[13]. Освен това, според проведено глобално проучване една трета от организациите биха предпочели да платят откуп на хакера, вместо да инвестират в информационна сигурност[14].

10 През 2017 г. глобалните атаки на *Wannacry* с искане на откуп и на зловредния софтуер за изтриване на дискове *NotPetya* взети заедно са засегнали над 320 000 жертви в около 150 страни[15]. Тези инциденти доведоха до нещо като световно пробуждане за заплахата, която представляват кибератаките, и дадоха нов тласък за включване на киберсигурността в основното планиране на политиките. Освен това 86 % от гражданите на ЕС понастоящем смятат, че рискът да станат жертва на киберпрестъпление расте[16].

Действия на ЕС в областта на киберсигурността

11 През 2001 г. ЕС стана наблюдаваща организация към Комитета по Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство[17] (Конвенцията от Будапеща). Оттогава насам ЕС работи за подобряване на устойчивостта на киберпространството чрез своята политика,

законодателство и разходи. На фона на нарастващия брой мащабни кибератаки и инциденти дейността се ускори от 2013 г. насам, както е показано на ***фигура 2***. Успоредно с това държавите членки приеха (а в някои случаи вече и актуализираха) първите си национални стратегии за киберсигурност.

12 В ***каре 2*** и ***приложение I*** са представени основните участници от ЕС, които имат отговорности по отношение на киберсигурността.

Каре 2

Кой участва?

Европейската комисия има за цел да повиши капацитета и сътрудничеството в областта на киберсигурността, да укрепи ЕС като участник в сферата на киберсигурността и да я включи в другите политики на ЕС. Основните генерални дирекции (ГД), отговорни за политиката за киберсигурност, са ГД **„Съобщителни мрежи, съдържание и технологии“** (киберсигурност) и ГД **„Миграция и вътрешни работи“** (киберпрестъпност), които отговарят съответно за цифровия единен пазар и за Съюза на сигурност. ГД **„Информатика“** отговаря за информационната сигурност на собствените системи на Комисията.

Комисията се подпомага от множество агенции на ЕС, по-специално **ENISA** (Агенция на Европейския съюз за мрежова и информационна сигурност), агенцията на ЕС за киберсигурност – предимно консултативен орган, който подпомага разработването на политиката, изграждането на капацитет и повишаването на осведомеността. Европейският център за борба с киберпрестъпността на Европол (**EC3**) е създаден, за да засили ответните действия на правоприлагащите органи на ЕС във връзка с киберпрестъпността. Комисията организира екип за незабавно реагиране при компютърни инциденти (**CERT-EU**), който подпомага всички институции, органи и агенции на Съюза.

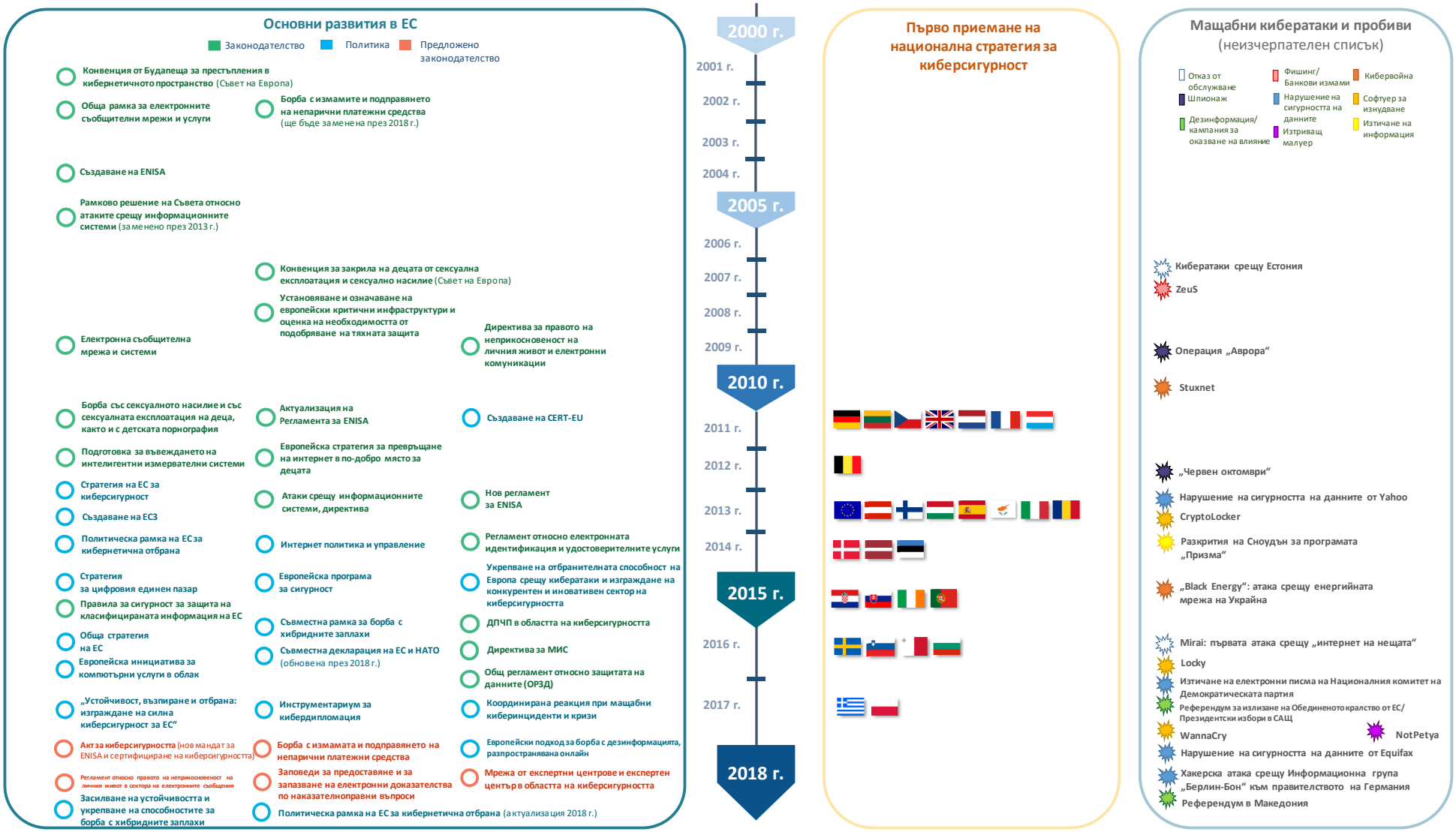
Европейската служба за външна дейност (ЕСВД) ръководи киберотбраната, кибердипломацията и стратегическата комуникация и една от нейните структури е центърът за анализ на информация. **Европейската агенция по отбрана** (EDA) има за цел да разработи способности за киберотбрана.

Държавите членки носят основната отговорност за собствената си киберсигурност, като на равнището на ЕС действат чрез **Съвета**, който има редица органи за координация и обмен на информация (сред които Хоризонталната работна група по въпроси на кибернетичното пространство). **Европейският парламент** действа като съзаконодател.

Организациите от частния сектор, включително промишлеността, органите за управление на интернет и академичните среди са партньори и участници

в разработването и прилагането на политиките – включително чрез договорно публично-частно партньорство (**ДПЧП**).

Фигура 2 – Ускоряване на разработването на политиката и законодателството (към 31 декември 2018 г.)



Източник: ЕСП.

Политика

13 Кибернетичната екосистема на ЕС е сложна и многопластова и обхваща редица области на вътрешната политика като правосъдие и вътрешни работи, цифровия единен пазар и изследователските политики. Във външната политика киберсигурността е включена в дипломацията и става част от нововъзникващата политика на ЕС за отбрана във все по-голяма степен.

14 Крайъгълният камък на политиката на ЕС е **Стратегията за киберсигурност от 2013 г.**[18]. Тази стратегия има за цел цифровата среда в ЕС да се превърне в най-безопасната среда в света, като същевременно защитава основните ценности и свободи. Тя има пет основни цели: i) повишаване на устойчивостта на киберпространството; ii) намаляване на киберпрестъпността; iii) разработване на политика за кибернетична отбрана и изграждане на капацитет; iv) разработване на промишлени и технологични ресурси за киберсигурността; и v) изграждане на международна политика относно киберпространството в съответствие с основните ценности на ЕС.

15 Стратегията за киберсигурност е взаимосвързана с три стратегии, приети впоследствие:

— **Европейската програма за сигурност** (2015 г.) има за цел подобряване на правоприлагането и съдебния отговор спрямо киберпрестъпността, главно чрез възобновяване на актуализирането на съществуващите политики и законодателство[19]. Тя също така си поставя за цел да установи пречките пред наказателните разследвания на престъпленията в кибернетичното пространство и да засили изграждането на киберкапацитет.

— **Стратегията за цифров единен пазар**[20] (2015 г.) има за цел създаване на по-добър достъп до цифровите блага и услуги чрез въвеждането на необходимите условия за максимизиране на потенциала за растеж на цифровата икономика. Укрепването на онлайн сигурността, доверието и приобщаването е от съществено значение за тази цел.

— **Глобалната стратегия**[21] от 2016 г. има за цел засилване на ролята на ЕС в света. Киберсигурността представлява основен стълб чрез подновен ангажимент към въпросите на кибернетичното пространство, сътрудничество с ключови партньори и решителност за справяне с проблемите на киберпространството във всички области на политиката, включително опровергаване на дезинформацията чрез стратегическа комуникация.

16 През последните години, тъй като киберпространството се превръща все повече в оръжие[22] и милитаризирано[23] пространство, то вече се разглежда като петата област на военни действия[24]. Киберотбраната предпазва системите, мрежите и критичната инфраструктура в киберпространството от атаки с военни и други средства. През 2014 г. е приета **Политическа рамка за кибернетична отбрана**, която е актуализирана през 2018 г.[25]. В актуализацията от 2018 г. са определени шест приоритета, включително разработването на способности за киберотбрана, както и защитата на комуникационните и информационните мрежи на общата политика на ЕС за сигурност и отбрана (ОПСО). Киберотбраната е част и от рамката за постоянно структурирано сътрудничество (ПСС) и от сътрудничеството между ЕС и НАТО.

17 **Съвместната рамка на ЕС за борба с хибридните заплахи** (2016 г.) разглежда киберзаплахите както за критичната инфраструктура, така и за частните потребители, като изтъква, че кибератаки могат да се извършват чрез дезинформационни кампании в социалните медии[26]. В нея се отбелязва и необходимостта от повишаване на осведомеността и засилване на сътрудничеството между ЕС и НАТО, което беше материализирано в съвместните декларации на ЕС и НАТО от 2016 г. и 2018 г.[27].

18 През 2017 г. Комисията представи нов пакет за киберсигурността, който отразява нарастващата неотложна необходимост от цифрова защита. Той включваше ново съобщение на Комисията за актуализиране на Стратегията за киберсигурност от 2013 г.[28], план за бърза и координирана реакция при мащабна атака и за бързо прилагане на Директивата за мрежова и информационна сигурност (Директива за МИС)[29]. Освен това пакетът документи включваше редица законодателни предложения (вж. точка ***22***).

Законодателство

19 От 2002 г. насам беше прието законодателство с различна степен на значимост за киберсигурността.

20 Като основен стълб на Стратегията за киберсигурност от 2013 г. в центъра на законодателството е **Директивата за мрежова и информационна сигурност (МИС)**[30] от 2016 г. – първото законодателство за целия ЕС в областта на киберсигурността. Тази директива, която трябваше да бъде транспонирана до май 2018 г., има за цел постигането на минимално равнище на хармонизирани

способности, като се задължат държавите членки да приемат национални стратегии относно МИС и да създадат единни звена за контакт и екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС)[31]. В нея се определят и изисквания за сигурност и уведомяване за операторите на основни услуги в критични сектори и за доставчиците на цифрови услуги.

21 Успоредно с това през 2016 г. влезе в сила **Общият регламент относно защитата на данните**[32](ОРЗД), който се прилага от май 2018 г. Неговата цел е да бъдат защитени личните данни на европейските граждани чрез определяне на правила за тяхното обработване и разпространение. Той предоставя определени права на субектите на данни и налага задължения на администраторите на лични данни (доставчиците на цифрови услуги) по отношение на използването и предаването на информация. С него се налагат и изисквания за уведомяване в случай на нарушение, а в някои случаи може да бъдат наложени глоби. На ***фигура 3*** е показано как Директивата за МИС и ОРЗД се допълват взаимно в своите цели за укрепване на киберсигурността и гарантиране на защитата на данните.

22 Проектът на законодателство, който се обсъжда в момента, включва предложения Акт за киберсигурността за укрепване на ENISA и създаване на приложим на територията на целия ЕС механизъм за сертифициране[33], предложения регламент относно европейските заповеди за предоставяне и за запазване на електронни доказателства[34] и предложената директива за електронните доказателства[35]. Предложението от 2018 г. за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове (наричани по-нататък „мрежа от центрове за експертни познания в областта на киберсигурността и център за изследователски експертни познания) съставлява част от пакета документи относно киберсигурността от 2017 г.[36].

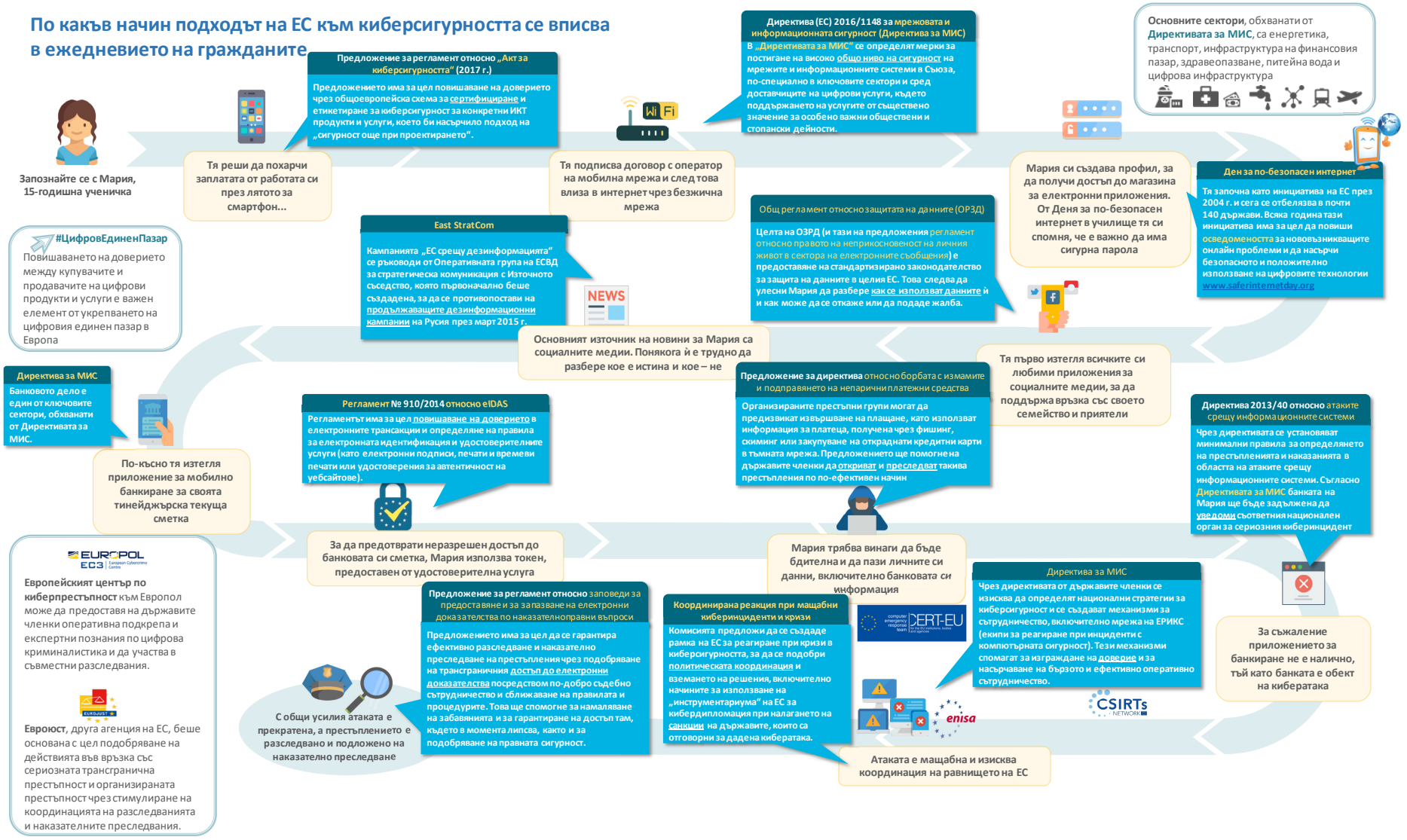
23 Понякога е трудно да се придобие представа за обхвата на политиката и на законодателната рамка, които засягат киберсигурността, и как това се отразява върху нашето ежедневие.

24 Във ***фигура 4*** е направен опит да се очертае пресечната точка на различните законодателни атове и другите дейности с живота на фиктивен европейски гражданин.

Фигура 3 – Как ОРЗД и Директивата за МИС се допълват взаимно

Източник: ЕСП.

Фигура 4 – По какъв начин подходът на ЕС към киберсигурността се вписва в ежедневието на гражданите



Източник: ЕСП.

Изграждане на политика и законодателна рамка

25 Кибернетичната екосистема на ЕС е сложна и многопластова и включва множество заинтересовани страни (вж. ***приложение I***). Обединяването на всичките ѝ коренно различни части е значително предизвикателство. От 2013 г. има целенасочено желание да се внесе последователност в областта на киберсигурността в ЕС[37].

Предизвикателство 1: Необходимост от оценка и отчетност

26 Трудно е да се създаде причинно-следствена връзка между стратегията от 2013 г. и всички наблюдавани промени, както отбеляза Комисията. Целите на стратегията от 2013 г. са много общо формулирани и по-скоро изразяват визия, отколкото измерима цел[38]. Разработването на действия, съгласувани с тези широки цели, е предизвикателство при липсата на измерими цели. Актуализираната рамка за политиката на ЕС за кибернетична отбрана (2018 г.) ще се стреми към разработването на цели, определящи минималното равнище на киберсигурност и доверие, което следва да се постигне. Това обаче ще бъде ограничено до киберотбраната; не са определени цели, определящи желаното равнище на устойчивост за Съюза като цяло.

27 Рядко се измерват резултати и много малък брой области на политика се оценяват[39]. Това отчасти се дължи на скорошното прилагане на много от мерките – законодателни или други – което възпрепятства извършването на цялостна оценка на тяхното въздействие. Предизвикателството е да се определят значими критерии за оценка, които могат да допринесат за измерване на въздействието. Освен това щателната оценка все още не се е превърнала в правило за киберсигурността като цяло. Ето защо е необходимо да се премине към култура на изпълнение с интегрирани практики за оценяване и стандартизирано докладване. Настоящият мандат на ENISA не обхваща оценката и мониторинга на състоянието на киберсигурността и готовността на ЕС.

28 Основаното на факти създаване на политики зависи от наличието на достатъчно надеждни данни и статистически данни, които да подпомагат наблюдението и анализирането на тенденциите и нуждите. Поради липсата на задължителна и обща система за мониторинг няма много надеждни данни. Често липсват показатели или те трудно могат да бъдат определени[40]. В някои области

обаче – като например цикъла на политиката на ЕС – са разработени специфични количествени показатели, които се използват за борба с тежката и организираната престъпност.

29 Много малко държави членки събират редовно официални данни по въпроси, свързани с киберпространството, което затруднява съпоставимостта. До момента ЕС е дал много малко указания относно необходимостта от консолидиране на статистическите данни на европейско равнище[41]. Съществуват и много малко независими анализи за целия ЕС, които обхващат ключови теми като[42]: икономика на киберсигурността, включително поведенчески аспекти (разминаване на стимулите, информационна асиметрия); разбиране на въздействието на киберсривовете и киберпрестъпността; макростастистика за тенденциите в киберсигурността и очакваните предизвикателства; и най-добрите решения за преодоляване на заплахите.

30 На фона на липсата на конкретни цели и недостига на надеждни данни и добре определени показатели до момента оценката на постиженията на стратегията е до голяма степен качествена. В докладите за напредъка често се описват извършените дейности или постигнатите етапни цели без задълбочено измерване на резултатите. Освен това все още не са определени базови стойности за оценка на устойчивостта на системите. В допълнение към това, поради липсата на систематизирано определение за киберпрестъпност е почти невъзможно да се установят подходящи европейски показатели, които биха подпомогнали мониторинга и оценката.

31 Независимият надзор на прилагането на политиката за киберсигурност се различава между отделните държави членки. ЕСП анкетира националните одитни институции във връзка с опита им в одитирането на тази област. Половината от отговорилите[43] никога не са извършвали одит на тази област. А тези от тях, които го бяха правили, бяха фокусирали одитите си главно върху управление на информацията; защита на критичната инфраструктура; обмен на информация и координация между основните заинтересовани страни; подготвеност за инциденти; уведомяване и реакция. Сред по-слабо застъпените теми бяха мерките за повишаване на осведомеността и недостигът на цифрови умения. Резултатите от тези одити или оценки невинаги се оповестяват поради съображения, свързани с националната сигурност. В ***приложение III*** е включен списък на публикуваните одитни доклади от националните одитни институции.

32 Ограниченията в кибернетичните умения (вж. също точки ***82–90***) и трудностите при оценяването на напредъка в областта на киберсигурността се

считат за основни предизвикателства пред одитирането на правителствените мерки в тази област.

Предизвикателство 2: Преодоляване на пропуските в правото на ЕС и неговото нееднакво транспониране

33 Скоростта, с която възникват новите технологии и заплахите, далеч изпреварва разработването и прилагането на законодателството на ЕС. Процедурите на Съюза не са планирани така, че да вземат предвид цифровата ера: разработването на иновативни и гъвкави процедури за гарантиране на подходяща рамка на политиката и законодателна рамка[44] за по-добро предвиждане и насочване на бъдещето е важен приоритет[45].

34 Въпреки желанието за по-голяма съгласуваност законодателната рамка за киберсигурността остава непълна (вж. ***таблица*** 1 за някои примери). Фрагментираността и пропуските възпрепятстват постигането на общите цели на политиката и водят до неефикасност. Установените от Комисията пропуски при оценката на стратегията включват „интернет на нещата“, баланса на отговорностите между потребителите и доставчиците на цифрови продукти и някои аспекти, които не са разгледани в Директивата за МИС. С предложения Акт за киберсигурността се прави опит за частично справяне с това чрез насърчаване на сигурност още при проектирането посредством схема за сертифициране за целия ЕС. Според някои заинтересовани страни все още осезаемо липсват ясно определена политика за цифровия сектор и общ подход към кибершпионажа[46].

Таблица 1 – Пропуски и нееднакво транспониране в законодателната рамка (неизчерпателна)

Област на политика	Примери
Цифров единен пазар	o Настоящата Директива за продажбата на потребителски стоки не обхваща киберсигурността. Предложените директиви относно цифровото съдържание[47] и онлайн продажбите[48] имат за цел да се отстрани този пропуск. o В държавите членки на ЕС, има ограничени и разнообразни правни рамки за задълженията за

	полагане на грижа, което поражда правна несигурност и затруднява прилагането на правни средства за защита[49]. o Политиките относно оповестяването на уязвимостта на софтуера се разработват с различни темпове в отделните държави членки без обща правна рамка на равнището на ЕС, която да позволява координиран подход[50].
Укрепване на мрежовата и информационната сигурност	o Държавите членки са свободни да включат сектори, които не фигурират в Директивата за МИС[51]. Секторите за туристическо настаняване, които не са обхванати, могат да бъдат портал за други престъпления, включително трафик на хора и наркотици и незаконна имиграция[52].
Борба с киберпрестъпността	o Много държави членки не са дали определение за електронни доказателства в националните си законодателства[53] (вж. също точка ***22***). o В настоящото рамково решение относно измамите с непарични платежни средства не са включени изрично инструментите за нефизически плащания като виртуалните валути, електронните пари и мобилните пари и не са обхванати действия като фишинг, скиминг и притежаване и споделяне на информация за платеца[54]. o В Директивата относно атаките срещу информационните системи не се разглежда пряко незаконното придобиване на данни отвътре (например кибершпионаж), което води до предизвикателства за правоприлагането[55]. o След решението на Съда на Европейския съюз относно запазването на данни[56] разликите в прилагането на правната рамка между държавите членки затрудниха правоприлагането, което може да доведе до загуба на насочваща информация във връзка с разследвания и да засегне ефективното наказателно преследване на престъпните дейности онлайн[57].

Източник: ЕСП.

35 Прилагането на някои аспекти на законодателството остава доброволно както за националните органи, така и за частните оператори. Например в рамките на групата за сътрудничество оценката на националните стратегии относно сигурността на мрежите и информационните системи и на ефективността на ЕРИКС се извършва на доброволна основа. Съгласно предложената схема за

сертифициране в Акта за киберсигурността прилагането на сертифициране за продукти и услуги на ИКТ също ще бъде на доброволен принцип.

36 В ЕС киберсигурността е прерогатив на държавите членки. Въпреки това ЕС играе важна роля при създаването на условия за подобряване на капацитета на неговите държави членки и за тяхната съвместна работа и за създаване на доверие. Въпреки големите различия между държавите членки по отношение на капацитета и ангажираността[58], предоставянето на чувствителна информация (за националната сигурност) ще остане доброволно.

37 Непоследователното транспониране на правото на ЕС между държавите членки може да доведе до правна и оперативна несъгласуваност и възпрепятства достигането на пълния потенциал на законодателството. Например държавите членки имат различни тълкувания на начина, по който следва да се прилага контролът на износа на изделия с двойна употреба[59], в резултат на което някои установени в ЕС дружества могат да изнасят технологии и услуги, които могат да се използват за кибернаблюдение и нарушения на правата на човека чрез цензура или прихващане. Европейският парламент изрази загриженост във връзка с това[60].

38 Освен това за защитата на неприкосновеността на личния живот и свободата на изразяване на мнение е необходим подходящ законодателен отговор, така че да се постигне необходимият баланс между защитата на основните ценности и постигането на неотложните приоритети на ЕС в областта на сигурността. Например как да гарантираме криптиране от край до край, като същевременно намерим най-добрия начин да подпомогнем правоприлагането? Или как можем да постигнем целите на ОРЗД, като същевременно разберем последиците от него за публично достъпната информация по отношение на регистраторите на имена на домейни и притежателите на блокове от IP адреси? И по какъв начин това може да се отрази неблагоприятно върху разследванията на правоприлагащите органи[61]?

39 Само по себе си законодателството не гарантира устойчивост. Въпреки че целта на Директивата за МИС е да се постигне високо ниво на сигурност в ЕС, тя е изрично насочена към постигането на минимална, а не максимална хармонизация[62]. С развитието на киберсредата ще продължат да се появяват пропуски.

Елементи за размисъл – рамка на политиката

- Какви важни стъпки са необходими, за да се предизвика преход от страна на създателите на политиките и законодателите към по-силна култура на изпълнение в областта на киберсигурността, включително определяне на общата устойчивост?

- По какъв начин научните изследвания могат да допринесат по-ефективно за генерирането на необходимите данни и статистика, позволяващи значима оценка?

- По какъв начин законодателните процеси в ЕС могат да бъдат адаптирани, за да станат по-гъвкави и да вземат под внимание в по-голяма степен скоростта на развитие на технологиите и заплахите?

- Как практиката за разработване на количествени показатели (показатели, цели) в цикъла на политиката на ЕС може да бъде адаптирана, подсилена и възпроизведена в областта на киберсигурността като цяло?

- Какво може да научи една национална одитна служба от подходите на другите одитни институции към одитирането на политиките и мерките за киберсигурност?

- Кои несъответствия в транспонирането и прилагането на правната рамка на ЕС възпрепятстват един по-ефективен отговор на пропуските в киберсигурността и киберпрестъпността и как те могат да се коригират най-добре от държавите членки и институциите на ЕС?

- Колко ефективен е контролът на ЕС на износа на кибер стоки и услуги при предотвратяването на нарушения на правата на човека извън ЕС?

Финансиране и разходи

40 ЕС си е поставил за цел да се превърне в най-безопасната онлайн среда в света. За осъществяването на тази амбиция са необходими значителни усилия от всички заинтересовани страни, включително стабилна и добре управлявана финансова основа.

Предизвикателство 3: Постигане на съответствие между равнището на инвестициите и целите

Увеличаване на инвестициите

41 Общият размер на световните разходи за киберсигурност като процент от БВП се оценява на около 0,1 %. В Съединените щати[63] този процент достига до около 0,35 % (включително частния сектор). Като процент от БВП разходите на федералното правителство на САЩ възлизат на около 0,1 % или около 21 млрд. щатски долара, предвидени в бюджета за 2019 г.[64]

42 В сравнение с това разходите в ЕС са ниски, фрагментирани и често не са подкрепени със съгласувани правителствени програми. Въпреки че трудно се намират данни, е изчислено, че публичните разходи на ЕС за киберсигурност варират между един и два милиарда евро годишно[65]. Разходите на някои държави членки като процент от БВП са в размер на една десета от равнищата в САЩ или дори по-ниски[66]. Необходимо е ЕС и неговите държави членки да разберат колко инвестират колективно, за да знаят кои пропуски да отстранят.

43 Трудно е да се придобие цялостна представа при липсата на ясни данни поради комплексния характер на киберсигурността и тъй като често не може да се направи разлика между общите разходи в областта на ИТ и тези за киберсигурност[67]. Анкетата на ЕСП потвърди, че е трудно да се получат надеждни статистически данни за разходите както в публичния, така и в частния сектор. Три четвърти от националните одитни институции съобщиха, че липсва централизиран преглед на свързаните с киберпространството държавни разходи, а нито една държава членка не задължава публичните субекти да докладват разходите за киберсигурност отделно в своите финансови планове.

44 Увеличаването на публичните и частните инвестиции в европейските предприятия в областта на киберсигурността е особено трудно. Често се предоставя публичен капитал за началните етапи, но той е по-малък за етапите на

растеж и разширяване[68]. Въпреки че съществуват многобройни инициативи на ЕС за финансиране, те не се използват главно поради бюрокрация[69]. Като цяло предприятията в областта на киберсигурността в ЕС изостават в сравнение с техните международни партньори: броят им е по-малък, а средният размер на привлеченото от тях финансиране е значително по-нисък[70]. Ето защо гарантирането на ефективно насочване и финансирането на стартиращи предприятия е изключително важно за постигането на целите на цифровата политика на ЕС.

Увеличаване на въздействието

45 Преодоляването на недостига на инвестиции в киберсигурност трябва да даде полезни резултати. Например въпреки силните страни на сектора на ЕС за научни изследвания и иновации, резултатите не са достатъчно патентовани, комерсиализирани или мащабно увеличени, за да спомогнат за укрепване на устойчивостта, конкурентоспособността и цифровата автономност[71]. Това важи в особена степен в сравнение с конкурентите на ЕС в световен мащаб. Недостигът на правилно използвани резултати се дължи на набор от фактори[72], включително:

- липсата на последователна транснационална стратегия за увеличаване на мащаба на подхода, за да се отговори на по-широките цифрови нужди на ЕС за конкурентоспособност и по-голяма автономност;
- продължителността на цикъла на веригата на стойността, което означава, че инструментите скоро престават да бъдат актуални;
- липсата на устойчивост, тъй като обикновено проектите приключват с разпускане на екипа на проекта и прекратяване на подкрепата, включително актуализации и решения за коригиране.

46 Предложението на Комисията за създаване на мрежа от центрове за компетентност в сферата на киберсигурността и център за изследователски експертни познания е опит да се преодолее разпокъсаността на изследванията в областта на киберсигурността и да се стимулират мащабните инвестиции[73]. На територията на ЕС има общо 665 експертни центъра.

Предизвикателство 4: Ясна представа за бюджетните разходи на ЕС

47 Централизираната представа за разходите е важна за прозрачността и по-добрата координация. Без нея създателите на политиките трудно ще разберат как разходите се съгласуват с нуждите за постигане на приоритетните цели.

48 Стратегията за киберсигурност не се финансира от специален бюджет. Вместо това на равнището на ЕС разходите за киберсигурност се покриват от общия бюджет на ЕС и от съфинансиране от държавите членки. Анализът на ЕСП показва сложна структура от най-малко десет различни инструмента в рамките на общия бюджет на ЕС, но без ясна представа за това кои средства къде отиват (вж. ***приложение 2***).

49 Ето защо създаването на ясна представа за разходите за тема, която обхваща много области на политиката, е огромно предизвикателство. Разходните програми се управляват от различни части на Комисията, всяка от които има собствени цели, правила и графици. Ситуацията се усложнява още повече, когато се отчете съфинансирането на държавите членки, например по линия на фонд „Вътрешна сигурност“ (Полиция)[74].

Разходи за киберсигурност, които могат да бъдат установени

50 През периода 2014–2018 г. Комисията е изразходвала най-малко 1,4 млрд. евро за прилагане на стратегията[75], като най-голям дял е разпределен за „Хоризонт 2020“[76] („Х 2020“). Финансирането на „Х 2020“ се насочва главно чрез програма „Обществени предизвикателства – сигурни общества“ и проекти по целта „Водещи позиции при базовите и промишлените технологии“[77]. До септември 2018 г. ЕСП установи 279 договорени проекта във връзка с киберсигурността с общо финансиране от ЕС в размер на 786 млн. евро[78]. На ***фигура 5*** е показана типологията на тези проекти въз основа на този анализ.

Фигура 5 – Договорени проекти в областта на киберсигурността по линия на „Х 2020“ (в млн. евро)

Източник: ЕСП.

51 През 2016 г. е създадено договорно публично-частно партньорство (ДПЧП), за да се стимулира европейският сектор на киберсигурността. Целта му е 450 млн. евро от програмата „Х 2020“ да бъдат насочени към ДПЧП и до 2020 г. да бъдат привлечени още 1,8 млрд. евро от частния сектор. През 18-месечния период до 31 декември 2017 г. 67,5 млн. евро са насочени от „Х 2020“ към ДПЧП, а частният сектор е инвестирал 1 млрд. евро[79].

52 Борбата срещу киберпрестъпността се подпомага и от фонд „Вътрешна сигурност“ – Полиция (ФВС-П). ФВС-П подпомага проучвания, експертни срещи и комуникационни дейности; между 2014 г. и 2017 г. те възлизат на близо 62 млн. евро. Държавите членки също така могат да получават безвъзмездна финансова помощ със споделено управление за оборудване, обучение, научни изследвания и събиране на данни. Деветнадесет държави членки са получили тази безвъзмездна финансова помощ в размер на 42 млн. евро.

53 Средствата за подпомагане на съдебното сътрудничество и функционирането на договорите за правна взаимопомощ със специален акцент върху обмена на електронни данни и финансова информация възлизат на 9 млн. евро по програма „Правосъдие“, управлявана от ГД „Правосъдие и потребители“.

54 В Директивата за МИС изрично е посочено, че ЕРИКС следва да разполагат с достатъчни ресурси, за да изпълняват ефективно задачите си[80]. Между 2016 г. и 2018 г. от Механизма за свързване на Европа годишно са предоставяни 13 млн. евро, за които държавите членки са могли да кандидатстват, за да подпомогнат изпълнението на изискванията на директивата. Няма проучване за определяне на действителния размер на необходимите финансови средства, които ще позволят на мрежата на ЕРИКС и на групата за сътрудничество да окажат въздействие.

55 Оперативните разходи на няколко агенции са били специално насочени към киберсигурността и дейностите на киберпрестъпността. От наличната публична информация обаче е трудно да се получат точни данни.

56 Конвенцията от Будапеща (вж. точка ***12***) е в основата на външните разходи на ЕС в областта на киберсигурността. През периода 2014–2018 г. ЕС е изразходвал около 50 млн. евро за укрепване на киберсигурността извън своите граници. Почти половината от тези средства са предоставени чрез Инструмента, допринасящ за стабилността и мира, като целта на един основен проект – GLACY+ на стойност 13,5 млн. евро – е да се укрепи световният капацитет за разработване и прилагане на законодателство в областта на киберпрестъпността и да се засили международното сътрудничество[81]. На други места акцентът на разходите от другите финансови инструменти на ЕС до голяма степен е бил върху Западните Балкани[82], както и върху съседните на ЕС държави, например проектът Cybercrime@EaP с държавите от Източното партньорство има за цел да се подобри международното сътрудничество в областта на киберпрестъпността и електронните доказателства.

Други разходи за киберсигурност

57 В програмите на ЕС невинаги е възможно да се установят конкретни разходи за киберсигурност:

- чрез съвместното предприятие „Електронни компоненти и системи за водещи позиции на Европа“ (ECSEL) финансирането по „Х 2020“ се насочва и за кибер-физически системи. ЕСП обаче не можа да установи конкретна връзка с киберсигурността измежду 27-те проекта на обща стойност 437 млн. евро от периода 2015—2016 г.

- По линия на европейските структурни и инвестиционни фондове са предоставени до 400 млн. евро за разходи в областта на киберсигурността

и удостоверителните услуги. Това включва инвестиции в сигурност и защита на данните за повишаване на оперативната съвместимост и взаимосвързаността на цифровата инфраструктура, електронна идентификация, неприкосновеност на личния живот и удостоверителни услуги.

58 В своя оперативен план за 2018 г. Европейската инвестиционна банка обяви намерението си за период от три години да увеличи финансирането за технологии с двойна употреба, киберсигурност и гражданска сигурност до 6 млрд. евро[83].

Перспективи

59 Компонентът за киберсигурност в размер на 2 млрд. евро от предложената нова програма „Цифрова Европа“[84] (ПЦЕ) за периода 2021–2027 г. е предназначен да укрепи сектора на киберсигурността в ЕС и цялостната защита на обществото, включително чрез подпомагане на прилагането на Директивата за МИС. Очаква се предложената мрежа от центрове за експертни познания в областта на киберсигурността и център за изследователски експертни познания, които имат за цел да доведат до по-рационален подход, да формират основния механизъм за изпълнение за разходите на ЕС по линия на ПЦЕ.

60 Разходите за отбрана от бюджета на ЕС наскоро бяха увеличени чрез Европейската програма за промишлено развитие в областта на отбраната, като през 2019 г. и 2020 г ще бъдат отпуснати 500 млн. евро[85]. Тя ще бъде насочена към подобряване на координацията и ефикасността на разходите за отбрана на държавите членки чрез стимули за съвместно сътрудничество. Целта ѝ е след 2020 г. чрез Европейския фонд за отбрана да генерира общи инвестиции в отбранителни способности в размер на 13 млрд. евро, част от които обхващат киберотбраната[86].

Предизвикателство 5: Предоставяне на достатъчно ресурси на агенциите на ЕС

61 Трите централни органа, които са в основата на политиката за киберсигурност на ЕС – ENISA, ЕС3 на Европол и CERT-EU (вж. ***каре 2***) – са изправени пред трудности по отношение на ресурсите в период на засилени политически приоритети в областта на сигурността. Настоящото разпределение

на човешките и финансовите ресурси в агенциите на ЕС остава предизвикателство за тях, за да отговорят на очакванията[87].

62 Исканията на агенциите за допълнителни ресурси, за да отговорят на нарастващото търсене, не са били напълно удовлетворени, което може да застраши (навременното) изпълнение на целите на политиката. Например:

- Ограничените ресурси бяха фактор, възпрепятствал пълното постигане на целите на ENISA през 2017 г.[88] В пакета за 2017 г. бяха предложени допълнителни ресурси в съответствие с новия мандат на ENISA.

- Осигуряването на анализатори и инвестиции в ИКТ капацитет в ЕСЗ на Европол изостава от търсенето[89]. Освен това в съвместната работна група на Европол и ЕК за борба с киберпрестъпността (J-CAT) работят служители от държавите членки и експерти от трети държави, за да се подпомогнат разследванията въз основа на разузнавателна информация. Разходите до голяма степен обаче се поемат от изпращащите държави, което възпрепятства изпращането на по-голям брой експерти. Създадено е временно командироване в зависимост от конкретния случай с финансиране от Европол или от цикъла на политиката на ЕС, за да се позволи участието на повече държави.

63 Някои ограничения са предизвикани от самите агенции. Много служители на CERT-EU и ENISA са договорно наети, а процедурите за тяхното наемане обикновено са бавни. Други, като например привличането и задържането на таланти, произтичат от неспособността на агенциите да се конкурират със заплатите в частния сектор или се дължат на незадоволителни перспективи за професионално развитие. Ето защо в периода 2014—2016 г. ENISA е възложила голяма част от своята работа на външни изпълнители[90].

64 Недостигът на персонал и на необходимите инструменти може да породи значителни рискове, особено по отношение на събирането на разузнавателни данни за заплахи. Обемът на данните от открити и закрити източници продължава да расте и има риск да надхвърли способностите на анализаторите да извършват подходящи анализи на заплахите. Без наличието на подходящ капацитет и инструменти за успешно интегриране и взаимно свързване на тези данни, те няма да бъдат ефективно преобразувани в годни за използване разузнавателни данни за заплахи, които може да се обменят и анализират на територията на ЕС[91].

Елементи за размисъл – финансиране и разходи

- По какъв начин Комисията и законодателите могат да оптимизират разходите на ЕС за киберсигурност и по-конкретно да ги съгласуват с ясно определени цели?

- Как може по всеобхватен начин да се преодолее недостигът на ресурси в агенциите на ЕС, като се вземат предвид нуждите и целите на Съюза?

- Какви мерки се определят на равнището на ЕС и на държавите членки за намаляване на пречките пред МСП за използване на инвестиционен капитал с цел увеличаване на мащаба на техните дейности?

- Какви конкретни и устойчиви резултати постигат средствата от „Х 2020“, за да доведат до решения в областта на киберсигурността?

- По какъв начин дейностите на ЕС за изграждане на капацитет укрепват капацитета извън неговите граници в съответствие с ценностите на ЕС?

Изграждане на общество, устойчиво на кибератаки

65 Управлението на киберсигурността е свързано с управлението на заплахите и рисковете, укрепването на капацитета и осведомеността и координацията и обмена на информация въз основа на доверие.

Предизвикателство 6: Укрепване на управлението и стандартите

Управление на информационната сигурност

66 Управлението на информационната сигурност е свързано с въвеждането на структури и политики, които да гарантират поверителността, целостта и наличността на данните. Тъй като това не е само технически въпрос, за него е необходимо ефективно ръководство, надеждни процеси и стратегии, съгласувани с организационните цели[92]. Негова подкатегория е управлението на киберсигурността, което се занимава с всички видове заплахи, свързани с киберпространството, в това число целенасочени сложни атаки, нарушения или инциденти, които трудно могат да бъдат открити или управлявани.

67 Моделите за управление на киберсигурността се различават между отделните държави членки и в тях отговорността за киберсигурността често се поделя между много субекти. Възможно е тези разлики да възпрепятстват сътрудничеството, необходимо за реагиране на мащабни трансгранични инциденти и за обмен на разузнавателни данни за заплахи на национално равнище – и в по-голяма степен — на равнището на ЕС. Анкетата на ЕСП сред националните одитни институции показа, че слабостите в механизмите за управление и в управлението на риска на публичните органи се считат за най-големи рискове.

68 Въпреки че последиците за организациите от частния сектор могат да бъдат сериозни, в управлението на киберсигурността се наблюдават много слабости. Почти девет от десет организации посочват, че функцията им за киберсигурност не отговаря напълно на техните нужди[93], а служителите по киберсигурността често са отдалечени поне на две нива от съвета[94].

69 В директивите на ЕС в областта на дружественото право не са определени специални изисквания за оповестяване на кибернетични рискове. В Съединените щати Комисията по ценните книжа и борсите неотдавна издаде необвързващи насоки, за да подпомогне публичните дружества при изготвянето на оповестяване на рискове и инциденти във връзка с киберсигурността[95]. Съвместният комитет на европейските надзорни органи[96] (ESA) предупреди за увеличаване на кибернетичните рискове, насърчи финансовите институции да подобрят уязвимите ИТ системи и да проучат присъщите рискове за информационната сигурност, свързаността и използването на външни изпълнители[97].

70 Укрепването на управлението на информационната сигурност на МСП е особено трудно, тъй като много често те не са в състояние да приложат подходящите системи. МСП не разполагат с актуални насоки относно прилагането на изискванията за информационна сигурност и неприкосновеност на личния живот и намаляването на технологичните рискове[98]. Ето защо основните предизвикателства са по-доброто разбиране на техните нужди и предоставянето на необходимите стимули и подкрепа.

71 Липсата на съгласувана международна рамка за управление на киберсигурността засяга способността за реакция на международната общност и за ограничаване на кибератаките. Ето защо е важно да се постигне консенсус относно такава рамка за управление, която най-добре да отразява интересите и ценностите на ЕС[99]. Опитите за определяне на международни норми за киберпространството стават все по-сложни, както е видно от липсата на консенсус през 2017 г. в рамките на групата от правителствени експерти към ООН относно начина, по който следва да се прилага международното право спрямо реакциите на инциденти от страна на държавите.

72 С цел да укрепи своята програма за управление на киберпространството, ЕС също така е формализирал шест партньорства в областта на киберсигурността за установяване на редовни политически диалози, насочени към изграждане на доверие и общи области за сътрудничество[100]. Крайните резултати са разнообразни, но като цяло в международната сфера ЕС все още не може да бъде считан за „важен участник в киберсигурността“, въпреки че е укрепил позициите си[101].

Информационна сигурност в институциите на ЕС

73 Всяка институция на ЕС има свои правила за управление на информационната сигурност. В междуинституционално споразумение се предвижда Комисията да предоставя помощ в областта на информационната сигурност на другите институции и агенции. Институциите и органите на ЕС признават необходимостта да развият по съгласуван начин своя капацитет в областта на киберсигурността, както и подходите си към управлението на риска. През 2020 г. Комисията, Съветът и ЕСВД следва да представят доклад пред Хоризонталната работна група по въпроси на кибернетичното пространство относно управлението и постигнатия напредък при изясняването и хармонизирането на управлението на киберсигурността в институциите и агенциите на ЕС[102].

74 В рамките на Комисията генерална дирекция „Информатика“ (DIGIT) е отговорна за сигурността на ИТ инфраструктурата и услугите (вж. ***каре 3***). Основните цели в областта на информационната сигурност в цифровата стратегия на Комисията са интегриране на информационната сигурност в процесите на управление; осигуряване на (икономически) ефективна инфраструктура и устойчивост; разширяване на възможностите за откриване и реагиране на инциденти; и интегриране на информационните технологии и управлението на сигурността[103]. Съгласно своя договор за доставки Комисията гарантира, че почти целият софтуер се поддържа активно и че се използва само софтуер, поддържан от търговеца[104].

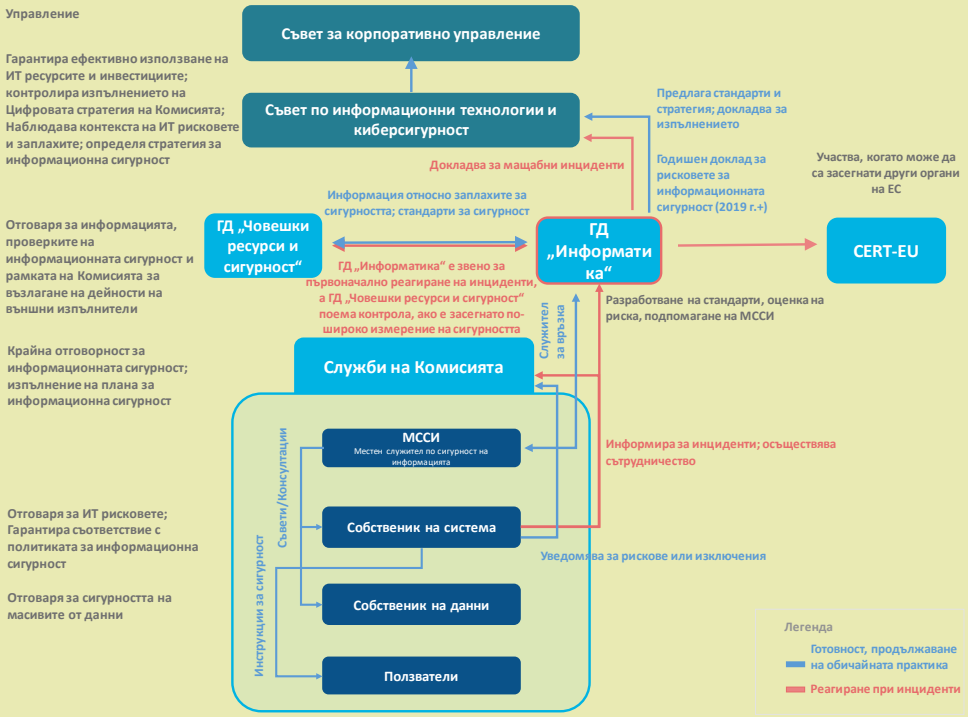
75 Значението на защитата на институциите обхваща и мисиите на ЕС по линия на ОПСО и неговите структури по света. Един от приоритетите на Политическата рамка на ЕС за кибернетична отбрана (актуализация 2018 г.) е да се подобри защитата на комуникационните и информационните системи на ОПСО, използвани от субекти от ЕС. Вече е създаден вътрешен Съвет за управление на киберсигурността към ЕСВД, който заседава за първи път през юни 2017 г.[105]

Каре 3

Защита на информационните системи на Комисията

Приблизително 1 300 системи и 50 000 устройства на Комисията са постоянен обект на кибератаки. Отговорността за ИТ е децентрализирана, както е показано на фигурата по-долу. Информацията и информационната сигурност се базират на общ план за информационна сигурност, определен от ГД „Информатика“. Съветът

по информационни технологии и киберсигурност действа като фактически главен служител по сигурността на информацията и свързва оперативната страна на информационната сигурност с висшето ръководство на Комисията, представлявано от Общия управителен съвет.



Източник: ЕСП въз основа на решения на Комисията[106].

Основната задача на ГД „Човешки ресурси и сигурност“ (HR DS) е да защитава служителите, информацията и активите на Комисията. Тя извършва и разследвания в областта на сигурността във връзка с инциденти, които имат по-широко измерение на сигурността от това на ИТ, като по този начин стават част от нейните дейности за контраразузнаване и борба с тероризма.

ГД „Информатика“ отговаря за информационната сигурност и част от нея е CERT-EU (екип за незабавно реагиране при компютърни инциденти). Създаденият през 2011 г. CERT-EU функционира с годишен бюджет от около 2,5 млн. евро и разполага с около 30 служители. Той е звено за първоначално реагиране при всеки инцидент, свързан информационната сигурност, който засяга няколко институции, но въпреки това не работи денонощно. Той администрира платформа за обмен на информация. През 2018 г. CERT-EU подписа необвързващ меморандум за разбирателство с ENISA, EC3 и Европейската агенция по отбрана за укрепване на сътрудничеството и координацията. Сключил е и техническо споразумение с екипа на НАТО за реагиране при компютърни инциденти (NCIRC).

Оценка на заплахите и рисковете

76 Обоснованите и непрекъснати оценки на заплахите и рисковете са важни инструменти както за публичните, така и за частните организации. Не съществува обаче стандартен подход към класифицирането и картографирането на киберзаплахите или към оценките на риска, поради което съдържанието на оценките се различава съществено и представлява предизвикателство за съгласувания подход към киберсигурността за целия ЕС[107]. Освен това често се използват едни и същи източници или дори други оценки на заплахите, което води до ехокамера, в която отекват повтарящи се констатации[108] с риск да не се обърне достатъчно внимание на други заплахи. Положението се влошава от продължаващото нежелание за обмен на информация и недостатъчното докладване на инциденти.

77 Звеното за синтез на информацията за хибридните заплахи[109], включено в рамките на ЕСВД, беше създадено, за да подобри ситуационната осведоменост и да подпомогне вземането на решения чрез обмен на анализи, но то трябва да разшири експертните си познания, включително в областта на киберсигурността. Успоредно с това CERT-EU предоставя на институциите, органите и агенциите на ЕС доклади и справки относно насочените към тях киберзаплахи.

78 В миналото ENISA отбеляза, че много държави членки имат качествено разбиране за заплахите и че е необходимо по-голямо моделиране на киберзаплахите[110]. Капацитетът за наблюдение за целите на стратегическия анализ ще увеличи цялостното разбиране. За да се гарантира по-цялостна представа обаче, оценките на заплахите биха могли да обхващат не само технологични заплахи, но и социално-политически и икономически заплахи, както и авторите на заплахите и мотивите на участниците.

Стимули

79 Все още съществуват твърде малко правни и икономически стимули, за да бъде възможно организациите да уведомяват и обменят информация за инциденти. Поради опасения, че репутацията им ще пострада, много организации все още предпочитат да се справят дискретно с кибератаките или да плащат на извършителите. Предстои да видим колко ефективно ще се справи Директивата за МИС с повишаването на нивото на уведомленията. Комисията очаква подобренията да настъпят главно на национално равнище, но Актът за киберсигурността ще добави общоевропейска перспектива[111].

80 Чрез включването на определени стандарти в обществените поръчки публичните органи, в ролята си на купувачи на цифрови продукти и услуги, имат значително влияние върху доставчиците чрез обществените поръчки и финансирането на научни изследвания и програми (например като изискват да бъдат приети определени технически стандарти като интернет протокола IPv6, с цел подпомагане на борбата срещу киберпрестъпността). Понастоящем обаче не съществува рамка за съвместни поръчки на инфраструктура за киберсигурност[112]. Комисията може да направи много в това отношение. Предложената ПЦЕ за следващата многогодишна финансова рамка има за цел да се справи с ограничените до този момент инвестиции от публичния сектор за закупуване на най-новите технологии за киберсигурност.

81 Чрез своя регулаторен капацитет Комисията може да гарантира, че се разработват правилните стандарти за широко възприемане с цел повишаване на сигурността. Комисията и Европол работят с органи за управление на интернет като ICANN (вж. точка ***40***) и RIPE-NCC[113], което е от съществено значение за внедряването на подходящата архитектура за борба с киберпрестъпността в помощ на правоприлагащите и съдебните органи.

Предизвикателство 7: Повишаване на уменията и осведомеността

82 ENISA посочва, че потребителите играят важна роля в борбата с кибератаките и че укрепването на уменията, образованието и осведомеността са от решаващо значение за изграждането на общество, устойчиво на кибератаки[114]. Хората на работното място или у дома, които са добре запознати, за да открият предупредителните знаци и разполагат с подходящите техники, могат да забавят или да предотвратят атаките.

83 Особено безпокойство буди нарастващата разлика между необходимото ноу-хау за извършване на киберпрестъпление или стартиране на кибератака и необходимите умения за защита срещу тях. Моделът „престъпление като услуга“ е намалил бариерите за навлизане на пазара на киберпрестъпността: хора без технически познания за тяхното създаване вече могат да наемат ботнети, експлойт китове или пакети от софтуер за изнудване.

Обучение, умения и развитие на капацитет

84 Светът е изправен пред нарастващ недостиг на умения в сферата на киберсигурността; от 2015 г. насам недостигът на работна сила се е увеличил с 20 %[115]. Традиционните канали за наемане на персонал не отговарят на търсенето, включително за управленски и интердисциплинарни длъжности[116]. Почти 90 % от световната работна сила в сферата на киберсигурността е от мъжки пол; трайната липса на разнообразие по отношение на половете допълнително ограничава набора от таланти[117]. Освен това в университетите предметите, свързани с киберпространството, не са достатъчно добре представени в нетехническите програми.

85 Необходимо е всеобхватно обучение и образование сред държавните служители, служителите на правоприлагащите органи, съдебните органи, въоръжените сили и преподавателите. Например съдилищата трябва да могат да се справят с бързо променящите се технически особености на киберпрестъпността и нейните жертви[118]; понастоящем няма стандарти за обучение и сертифициране за целия ЕС[119]. В институциите на ЕС е важно да се овладее подходящата комбинация от умения. Без наличието на подходящи умения институциите няма да могат правилно да определят обхвата, да установят подходящите партньори и нужди в областта на сигурността или няма да имат капацитета да управляват програмите. От своя страна това може да подкопае ефективността на програмите на ЕС или разработването на политиката.

86 Въпреки че държавите членки отговарят за образователните политики на равнището на ЕС, вече се осъществяват множество дейности за обучение (вж. ***таблица 2***) и учения (вж. ***каре 4***). ЕС може да подпомогне включването на стандарти за целия ЕС в учебните планове във всички съответни дисциплини[120]. В областта на цифровата криминалистика например са **необходими** общи стандарти за обучение, за да се *улесни* пътят към допустимостта на доказателствата в държавите членки. Поради трансграничния характер на киберпрестъпността, възможно е да участват множество юрисдикции, което изисква обучение на равнището на ЕС. И все пак CEPOL, Агенцията на ЕС за обучение в областта на правоприлагането, отбелязва, че повече от две трети от държавите членки не предоставят редовно обучение в областта на киберотбраната на служителите на правоприлагащите органи[121]. ЕС също така би могъл да определи начини за постигане на взаимодействие между образованието и обучението в гражданската и военната сфера[122]. В тази връзка ENISA е установила, че въпреки че настоящите възможности за обучение

в секторите от критично значение са големи, те не са насочени в достатъчна степен към устойчивостта на критичната инфраструктура[123].

Таблица 2 – Някои инициативи на ЕС за обучение в сферата на киберсигурността

Проекти на Европейската агенция по отбрана, например подкрепа за учения от частния сектор и проектът Киберполигон	Мрежа на Европейския колеж по сигурност и отбрана (предоставя гражданско-военно обучение), включително киберплатформа за образование, обучение, оценка и учения	Обучения на ENISA, предоставящи програми за обучение, когато търговският пазар не може да ги предостави
Програми за обучение на Europol, CEPOL, ECTEG[124] – включително модел за управление на обучението и рамка за компетентност в областта на обучението (в т.ч. сертифициране)	Мрежа от експертни центрове и център за изследователски експертни познания (предложение)	Мерки в областта на криптирането, предложени в Единадесетия доклад за напредъка по създаването на Съюза на сигурност
Сътрудничество между ЕС и НАТО в областта на обучението и образованието по киберотбрана	Програма „Военен Еразъм“	Европейска мрежа за съдебно обучение

Източник: ЕСП.

87 ЕС е командировал експерти по борба с тероризма и експерти по сигурността в 17 делегации, за да засили връзката между вътрешната и външната сигурност на ЕС[125]. Въпреки ограниченията на ресурсите повече ноу-хау в областта на киберсигурността ще спомогне за осъществяване на подходящите проекти, както и за установяване на полезни взаимодействия с други програми или източници на финансиране[126]. Това би могло също така да повиши популярността на киберсигурността в политическия диалог, въпреки че тя ще трябва да се конкурира с много други приоритети като миграцията, организираната престъпност или завръщането на чуждестранни бойци.

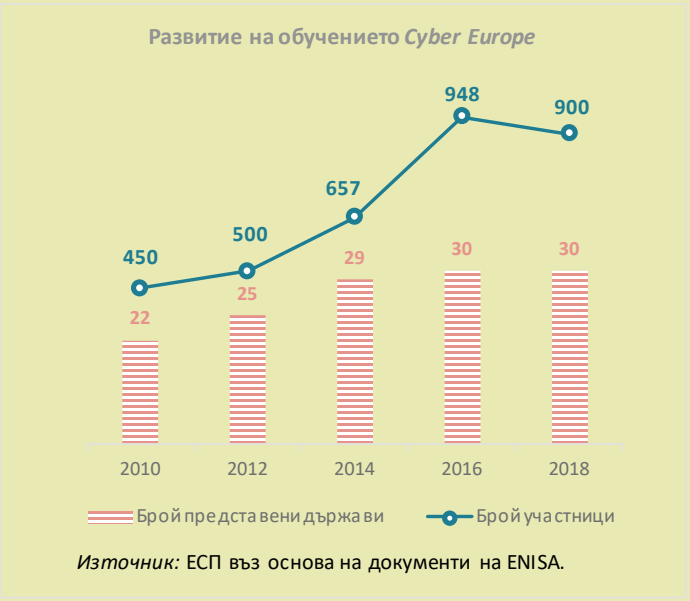
Каре 4

Учения

Ученията са важни елементи от образованието и обучението в областта на киберсигурността и предоставят отлични възможности за повишаване на готовността чрез изпитване на капацитета, реагиране на реални сценарии и изграждане на мрежи от работни отношения. От 2010 г. тяхната честота се е увеличила значително.

Участниците вземат участие на място или от разстояние. След ученията има оценки за установяване на наученото, въпреки че те все още не обхващат изцяло стратегическото/политическото, оперативното и техническото равнище[127].

Водещите учения на ЕС и НАТО – двугодишното „Cyber Europe“ (оперативно) и ежегодното учение „Locked Shields“ (техническо) – събират повече от 1 000 участници от около 30 участващи държави. И двете учения са насочени към защитата и опазването на критичната инфраструктура при симулирани сценарии на атаки. Задълбочеността на ученията се е увеличила значително, като и двете вече включват елементи на медийната, правната и финансовата политика с цел подобряване на ситуационната осведоменост на специалистите. В паралелните и координирани учения PACE (стратегически) се изпитва взаимодействието между ЕС и НАТО при сценарий на хибридна криза.



Източник: ЕСП въз основа на документи на ENISA.

Това не са единствените международни учения. ENISA организира ежегодно киберпредизвикателство, в което екипите се състезават в решаването на предизвикателства, свързани със сигурността, като например уеб и мобилна сигурност, криптографски пъзели, обратен инженеринг, етика и криминалистика. Първото учение на министерско равнище, EU CYBRID, се проведе през септември 2017 г. и беше насочено към стратегическото вземане на решения. През 2018 г. беше стартирано учението на НАТО „Crossed Swords“ с цел да се подобрят офанзивните елементи на учението „Locked Shields“. НАТО организира и ученията „Cyber Coalition“.

Основно предизвикателство е да се осигури активното участие на всички важни заинтересовани страни и координацията на всички учения с цел избягване на дублиране и ефективен обмен на наученото.

Осведоменост

88 Гражданите често са използвани за осъществяване на атаки и разпространение на дезинформация, тъй като има вероятност те неволно да

станат уязвими поради евтини и широко разпространени устройства и софтуер или да станат жертви на социално инженерство. Ето защо повишаването на осведомеността е от съществено значение за изграждането на ефективна киберустойчивост, но това в никакъв случай не е лесна задача, тъй като за неспециалистите е трудно да разберат сложността на киберсигурността и свързаните с нея рискове.

89 Ежегодният Европейски месец на осведомеността за кибернетичната сигурност (ECSM) и Денят за по-безопасен интернет са примери за повишаване на осведомеността. Седем държави извън ЕС вече се включиха в ECSM[128]. Кампанията на Европол *„Кажи не!“* има за цел да намали риска децата да станат жертва на сексуално насилие и изнудване в интернет. Важно е да се намали рискът, тъй като в момента много малко жертви на атаки съобщават за тези престъпления в полицията[129]. Комисията признава, че стратегията за киберсигурност е била само „частично ефективна“ по отношение на повишаването на осведомеността на гражданите и на предприятията[130]. Това се дължи на мащаба на задачата, на ограничените ресурси, на неравномерното участие на държавите членки и на липсата на научни данни за най-добрите начини за повишаване и измерване на осведомеността.

90 Предизвикателството за Комисията и съответните агенции е да се гарантира, че мерките за повишаване на осведомеността: са добре насочени и оповестени; приобщаващи; съобразени с контекста на заплахите; избягват нежелани ефекти като „изтощение от сигурността“[131]; и разработват методи за оценка и количествени показатели за оценка на тяхната ефективност. Това следва да се прилага в еднаква степен в рамките на самите институции на ЕС, където е необходимо да се подобри културата на осведоменост[132].

Предизвикателство 8: Подобряване на обмена на информация и координацията

91 За киберсигурността е необходимо сътрудничество между публичния и частния сектор, главно по отношение на обмена на информация и най-добри практики. Доверието е много важно на всички равнища, за да се създаде подходяща среда за трансграничен обмен на чувствителна информация. Слабата координация води до фрагментираност, дублиране на усилията и пилеене на експертен опит. Ефективната координация може да доведе до осезаеми успехи, като например затварянето на пазарите в тъмната мрежа[133]. Въпреки постигнатия

напредък през последните години, степента на доверие все още е „недостатъчна“[134] на равнището на ЕС и в някои държави членки[135].

Координация между институциите на ЕС и с държавите членки

92 Една от целите на стратегията за киберсигурност и на въведените с Директивата за МИС структури за сътрудничество е засилване на доверието сред заинтересованите страни. В оценката на стратегията беше признато, че е положена основа за стратегическо и оперативно сътрудничество на равнището на ЕС[136]. Въпреки това като цяло координацията е „недостатъчна“[137]. Предизвикателството е да се гарантира, че обменът на информация е не само значим, но също така позволява да се създаде пълна представа за общата картина. Важен фактор в това отношение е да се постигне общо разбиране въз основа на приетата терминология (вж. ***каре 5***).

93 В оценката на ENISA обаче се отбелязва, че подходът на ЕС към киберсигурността не е достатъчно координиран, което води до липса на полезно взаимодействие между дейностите на ENISA и тези на другите заинтересовани страни. Механизмите за сътрудничество все още са относително недоразвити[138]; Актът за киберсигурността има за цел да се справи с това, като засили координиращата роля на ENISA. Желанието за засилване на сътрудничеството е основната причина за подписания през 2018 г. Меморандум за разбирателство между ENISA, EDA, EC3 на Европол и CERT-EU[139]. През следващите години приоритет на Комисията ще бъде да се гарантира подходящо съгласуване между инициативите на политиката, нуждите и инвестиционните програми, за да се преодолее разпокъсаността и да се създадат полезни взаимодействия[140].

94 В обхвата на различните институционални органи са включени координационни функции. Работната група за Съюза на сигурност е създадена, за да играе централна роля в координирането на различните генерални дирекции на Комисията с цел да се подпомогне програмата за Съюз на сигурност[141]. ГД „Съобщителни мрежи, съдържание и технологии“ председателства подработната група по въпросите на киберсигурността към работната група.

95 В Съвета киберсигурността се разглежда от Хоризонталната работна група по въпроси на кибернетичното пространство (HWP), която координира стратегически и хоризонтални въпроси на кибернетичното пространство и подпомага подготовката на учения, като оценява резултатите от тях. Тя работи в тясно сътрудничество с Комитета по политика и сигурност, който има централна роля

при вземането на решения във връзка с всички дипломатически мерки относно киберсигурността (вж. ***каре 6*** в следващата глава). Тъй като киберсигурността е хоризонтална тема, координирането на всички съответни интереси не е еднозначно: не по-малко от 24 работни групи и подготвителни органи наскоро са разглеждали въпроси на кибернетичното пространство[142].

96 Двете последни законодателни предложения за укрепване на ENISA (2017 г.) и за създаване на мрежа от експертни центрове в областта на киберсигурността и център за изследователски експертни познания (2018 г.) са специално предназначени да преодолеят разпокъсаността и дублирането на усилия. Движещ фактор за мрежата от експертни центрове в областта на киберсигурността и центъра за изследователски експертни познания е необходимостта от попълване на пропуските, които не се попълват от структурите за сътрудничество на Директивата за МИС, тъй като те нямат за цел да подпомагат разработването на авангардни решения.

Каре 5

Опит да се говори на един и същ кибернетичен език: *технологична съгласуваност*

Терминологичната яснота подобрява ситуационната осведоменост и координацията[143] и помага да се определи точно какво представлява заплахата и рискът.

Съвместният изследователски център (JRC) на Комисията неотдавна разработи ревизирана изследователска таксономия, съставена от различни международни стандарти[144]. Нейните цели са да се превърне в референтна точка, която да се използва като еталон от научноизследователските организации в Европа.

Източник: ЕСП, адаптирано от Европейската комисия.

До неотдавна институциите и агенциите на ЕС нямаха общи определения. Това се променя. В рамките на своя план групата за сътрудничество създаде таксономия на инцидентите HYPERLINK "http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=53646“ с цел да улесни ефективното трансгранично сътрудничество.

Сътрудничество и обмен на информация с частния сектор

97 Координацията между публичните органи и частния сектор е от съществено значение за укрепването на общото равнище на киберсигурност. Въпреки това в своята оценка на стратегията за киберсигурност от 2017 г. Комисията установи, че обменът на информация между заинтересованите страни от частния сектор и между публичния и частния сектор „все още не е оптимален“ поради „липсата на надеждни механизми за докладване и стимули за обмен на информация“[145], което възпрепятства постигането на стратегическите цели. Комисията също така отбеляза липсата на механизъм за ефективно сътрудничество, чрез който държавите членки да работят съвместно с цел стратегическо укрепване на мащабния траен промишлен капацитет[146].

98 Центровете за споделяне и анализ на информация (ISAC) са организации, създадени да предоставят платформи и ресурси за улесняване на обмена на информация между публичния и частния сектор, както и за събиране на информация относно киберзаплахи. Те имат за цел да изградят доверие чрез обмен на опит, знания и анализ, по-специално на първопричините, инцидентите и заплахите. В много държави членки вече съществуват национални и секторни ISAC, но на европейско равнище те все още са относително ограничени[147]. Те обаче са съпътствани от редица предизвикателства (ограничения на ресурсите, трудности при оценяването на успеха им, осигуряване на подходящите структури за ангажиране на публичния и частния сектор, участие на правоприлагащите органи), които ще трябва да се преодолеят, ако се очаква да допринасят за подпомагане на прилагането Директивата за МИС и изграждането на капацитет в областта на сигурността на общоевропейско равнище[148].

99 Тясното сътрудничество с частния сектор е особено важно за борбата със сложните киберпрестъпления, но неговата ефективност е неравномерна в отделните държави членки и зависи от равнището на доверие[149]. Към ЕС3 на Европол обаче са създадени редица консултативни групи с оператори от частния сектор, институциите и агенциите на ЕС и други международни организации с цел подобряване на сътрудничеството чрез изграждане на мрежи, обмен на стратегически разузнавателни данни и сътрудничество. Те работят съгласно планове, съгласувани с целите на цикъла на политиката на ЕС[150]. Престъпната злоупотреба с криптиране е друга област, изпълнена с предизвикателства, които изискват по-голямо сътрудничество с частния сектор. Понастоящем ЕС3 на Европол проучва възможностите за организиране на краткосрочни командировки в J-CAT (вж. точка ***65***) във връзка с конкретни случаи за експерти от частния сектор и академичните среди.

100 Липсата на механизми за ефективно сътрудничество засяга както публичните, така и частните общности в гражданския сектор и сектора, свързан с отбраната. Сред областите, които пораждат общо предизвикателство, са криптографията, сигурните вградени системи, откриването на зловреден софтуер, симулационните техники, защитата на мрежовата и системната комуникация и технологиите за установяване на автентичността. Насърчаването на гражданско-военното сътрудничество и подпомагането на научните изследвания и технологиите (по-специално чрез подпомагане на МСП) са два от приоритетите в актуализираната рамка за политиката на ЕС за кибернетична отбрана (актуализация 2018 г.).

Елементи за размисъл – изграждане на устойчивост

- Как на равнището на ЕС може да се постигне подходящ баланс между необходимостта от оптимизиране на политиката за киберсигурност и гарантиране на ефективна координация между различните участници и разпределяне на отговорностите?
- Колко добре подготвени са институциите и агенциите на ЕС за следващата голяма атака, насочена директно срещу тях?
- Как могат свързаните с киберсигурността агенции да станат по-привлекателни за талантите?
- Какви допълнителни стъпки са необходими за гарантиране на достатъчен капацитет в институциите и агенциите на ЕС, който да даде възможност за съгласувана рамка за оценка на рисковете и заплахите?
- По какъв начин европейските надзорни органи (Европейският банков орган, Европейският орган за ценни книжа и пазари и Европейският орган за застраховане и професионално пенсионно осигуряване) се справят с присъщите за финансовия сектор кибернетични уязвимости и какви поуки може да се извлекат от това за другите сектори?
- С оглед на цялостния недостиг на експертни познания, как може да се използва най-добре техническата помощ на ЕС за публичните органи, така че да се постигне максимално цялостното въздействие за подобряване на киберустойчивостта?
- Как могат ЕС и държавите членки да осигурят своето значимо присъствие в международните дискусии, за да насочват управлението и стандартите в киберпространството и да популяризират ценностите на ЕС?
- Кои мерки за повишаване на осведомеността на равнището на ЕС и на държавите членки (включително усилия за предотвратяване) наистина променят нещо и какво може да направи ЕС, за да ги засили?
- Каква роля може да изиграе ЕС, за да спомогне за постигане на разнообразие по отношение на половете в сферата на киберсигурността?
- Как ЕС и държавите членки могат да увеличат полезното взаимодействие между гражданския сектор и сектора, свързан с отбраната, в съответствие с рамката за политиката на ЕС за кибернетична отбрана (актуализация 2018 г.)?

Ефективно реагиране на киберинциденти

101 Разработването на ефективен отговор на кибератаките е от основно значение, за да бъдат спрени на възможно най-ранен етап. Особено важно е секторите от критично значение, държавите членки и институциите на ЕС да могат да реагират по бърз и координиран начин. Ранното откриване е от съществено значение за това.

Предизвикателство 9: Ефективно откриване и реакция

Откриване и уведомяване

102 Общите инструменти за откриване спомагат за неутрализиране на голяма част от атаките в ежедневието[151]. Въпреки това цифровите системи станаха толкова сложни, че предотвратяването на всяка една атака е невъзможно. Поради своята сложност атаките често не могат да бъдат открити дълго време. Ето защо експертите твърдят, че следва да се постави акцент върху бързото откриване и защитата[152]. При някои инструменти за откриване обаче – като например автоматичност, машинно самообучение и поведенчески анализ, които са насочени към намаляване на рисковете и анализ и извличане на поуки от поведението на системата – се наблюдава ниска степен на възприемане от страна на предприятията[153]. Това се дължи отчасти на генерирането на неверни положителни резултати, поради което незастрашаващи дейности погрешно се определят като зловредни.

103 След като бъде открит и анализиран пробив, е необходимо бързо уведомяване и докладване, за да може другите публични и частни субекти да предприемат превантивни действия, а съответните органи да подпомогнат засегнатите. Много организации не желаят да признават и докладват киберинциденти[154]. Ранното включване на правоприлагащите органи в първоначалната реакция на подозирано киберпрестъпление и активният обмен на информация с ЕРИКС също са от съществено значение.

104 Поради предишната липса на общи изисквания на ЕС относно уведомяването за инциденти съществуваше риск да се забави съобщаването на нарушения и да се възпрепятства реакцията, което Директивата за МИС имаше за

цел да преодолее (вж. точка ***21***). След атаките Wannacry от 2017 г. Комисията заключи, че системата на мрежата ЕРИКС все още не функционира пълноценно[155]. Тъй като прилагането на директивата продължава, остава да се види дали разработените от групата за сътрудничество насоки ще се справят ефективно с нежеланието за докладване на инциденти[156].

105 Съгласно действащите регламенти на ЕС операторите на основни услуги в определени сектори имат многобройни задължения за уведомяване (включително на потребителите), което може да засегне ефективността на процеса. Например операторите във финансовия и банковия сектор са обект на различни критерии, стандарти, прагове и срокове за уведомяване съгласно ОРЗД, Директивата за МИС, Директивата за платежните услуги, ЕЦБ/ЕНМ, Target 2 и Регламента относно eIDAS[157]. Ето защо е важно тези задължения да се рационализират, тъй като освен че представляват ненужна административна тежест, подобна хетерогенност може да доведе до фрагментирано докладване.

Координирана реакция

106 Разработването на европейска рамка за сътрудничество при киберкризи все още не е завършено. Ето защо беше въведен свързаният с нея „план“[158] (вж. точка ***19***), за да се внесе киберперспектива в механизма за интегрирана реакция на ЕС при политическа криза (IPCR), да се подобри ситуационната осведоменост и да се гарантира по-добра интеграция с другите механизми на ЕС за управление на кризи[159]. Планът включва институциите, агенциите и държавите членки на ЕС. Безпроблемното интегриране на всички тези механизми за реакция при кризи не е лесно[160]. Настоящата липса на съвместна защитена комуникационна мрежа в институциите на ЕС също представлява важен недостатък[161].

107 Капацитетът на ЕС за реакция на кибератаки на оперативно и политическо равнище в случай на мащабен трансграничен киберинцидент е определен като „ограничен“, отчасти тъй като киберсигурността все още не е интегрирана в съществуващите координационни механизми на равнището на ЕС за реакция при кризи[162]. Директивата за МИС не е преодоляла този недостатък.

108 Наскоро предложената реформа на ENISA, с която се предвижда по-голяма оперативна роля при справянето с мащабни киберинциденти, не беше подкрепена от държавите членки, които предпочитат ролята на агенцията да бъде подкрепяща и допълваща собствените им оперативни действия[163]. На равнището на държавите членки вече има много CERT/ЕРИКС, но техният

капацитет се различава значително. Това представлява пречка за ефективното трансгранично сътрудничество, необходимо за реакцията на мащабни инциденти[164].

109 ЕСП се опита да очертае различните роли, възложени на определените в плана различни действащи лица, но има пропуски, които ще трябва да се запълнят в хода на изпълнението. Една първоначално недостатъчно добре разгледана област е правоприлагането, въпреки че Протоколът на ЕС за спешно реагиране на правоприлагащите органи влезе в сила през декември 2018 г.[165] От решаващо значение за успеха на плана е да се гарантира, че той е практичен и че всички страни знаят какво да правят; за това ще е необходимо задълбочено изпитване през следващите години.

110 Ефективната реакция не е свързана само с ограничаване на вредите; поемането на отговорност за атаките също е от основно значение. Проследяването и установяването на извършителите най-вече при хибридна атака може да бъде много трудно поради нарастващата злоупотреба с инструменти за анонимизиране, криптовалути и криптиране. Това е известно като „проблем с определянето на отговорност“. Решаването на този проблем не е само технически въпрос – това е и предизвикателство за наказателното правосъдие. Възможно е правните и процедурните различия между държавите да възпрепятстват наказателните разследвания и преследването на заподозрените. За решаването на проблема с определянето на отговорност ще бъде необходим по-формализиран оперативен обмен на информация чрез по-ясни процедури, например с Европол или с Европейската съдебна мрежа на Евроюст по въпросите на киберпрестъпността.

111 На политическо равнище инструментариумът за кибердипломация (вж. ***каре 6***) е разработен, за да подпомогне уреждането с мирни средства на международни спорове в киберпространството. Създаването на екипи за бързо реагиране при кибератаки и на инициатива за взаимопомощ в областта на киберсигурността са два проекта за насърчаване на засиления обмен на информация, които се разработват в рамките на ПСС[166].

Каре 6

Инструментариум за кибердипломация

Рамката за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството[167], или „инструментариумът за кибердипломация“, беше създадена вследствие на заключенията на Съвета от 2015 г. относно кибердипломацията[168]. Целта на кибердипломацията е разработване и прилагане на общ и всеобхватен подход към киберпространството въз основа на ценностите на ЕС, принципите на правовата държава, изграждане на капацитет и партньорства, насърчаване на многостранния модел за управление на интернет, ограничаване на заплахите за киберсигурността и по-голяма стабилност в международните отношения.

Инструментариумът дава възможност на ЕС и неговите държави членки да организират съвместен дипломатически отговор срещу злонамерени действия в киберпространството, като използват пълноценно мерките по линия на общата външна политика и политика на сигурност. Те могат да включват превантивни мерки (например за повишаване на осведомеността, изграждане на капацитет), мерки за сътрудничество, стабилност и ограничителни мерки (например забрани за пътуване, оръжейно ембарго, замразяване на средства) или подкрепа за отговора на държавите членки[169]. Идеята е, че по-нататъшното сътрудничество за ограничаване на заплахите и изпращане на ясен сигнал за вероятните последици от съвместния отговор може да предотврати (потенциално) агресивното поведение.

Съвместният отговор на ЕС срещу злонамерени действия в киберпространството следва да бъде пропорционален на обхвата, мащаба, продължителността, интензитета, сложността, степента на усъвършенстване и въздействието на действията в киберпространството.

Неразделна част от успеха на инструментариума ще бъде това доколко добре е свързан с плана и IPCR (вж. точка *Error! Reference source not found.*), колко добра ситуационна осведоменост се създава чрез бързия и непрекъснат обмен на информация (включително относно елементите на определянето на отговорност)[170] и накрая – ефективното сътрудничество. От решаващо значение за успешното прилагане на инструментариума е и ефективната и координирана комуникация. До този момент инструментариумът е използван два пъти: за започване на диалог със Съединените щати след атаката *Wannacry*[171] и за разработване на заключения на Съвета, осъждащи злонамереното използване на ИКТ[172]. Привеждането в действие на инструментариума продължава; остава да се види колко ефективен ще бъде той при постигането на целите си.

Предизвикателство 10: Защита на критичната инфраструктура и обществените функции

Защита на критичната инфраструктура

112 Голяма част от критичната инфраструктура на ЕС се експлоатира чрез системи за промишлен контрол (ICS)[173]. Много от тях са разработени като самостоятелни системи с ограничена свързаност с външния свят. Тъй като компонентите на ICS са свързани с интернет, те са станали по-уязвими на външна намеса. Въпреки че поддържането и актуализирането на съществуващите системи вече не е възможно, тяхното модернизиране не става бързо или евтино. Ето защо усилията за повишаване на сигурността на критичната инфраструктура трябва да включват модернизиране на ICS.

113 Тъй като промишлеността продължава да се цифровизира (обичайно познато като „Индустрия 4.0“), въздействието на даден мащабен инцидент в един промишлен сектор може да има верижен ефект на други места. ENISA отбеляза, че е важно да се определи въздействието на взаимната зависимост на критичните сектори[174]. Това е от съществено значение, за да се разбере потенциалното разпространение на даден инцидент, и е в основата на добре координираните реакции.

114 Целта на Директивата за МИС е да се подобри подготвеността в ключови сектори, отговорни за критичната инфраструктура. Не всички сектори обаче са обхванати (вж. ***таблица 1***)[175], което „намалява ефективността на стратегията“[176]: особено важно в тази връзка е да се защити демократичната почтеност на изборите от намеса в изборната инфраструктура и от дезинформация (вж. ***каре 7***). Ето защо, освен преразглеждането на действащото законодателство, основно предизвикателство ще бъде включването на тези сектори в ефективни реакции на мащабни инциденти.

115 Уязвимостите на критичната инфраструктура не свършват на границите на Европа. Особено предизвикателство за Комисията е насърчаването на държавите кандидатки да приемат същите стандарти като държавите членки, например в области като законодателството във връзка с киберпространството или защитата на критичната инфраструктура.

Каре 7

Защита на критичните обществени функции: *борба срещу намесата в изборите*

През май 2019 г. около 400 млн. гласоподаватели ще отидат до пунктовете за гласуване в изборите за Европейски парламент – първите, които се провеждат съгласно ОРЗД. Те идват след скандалите около злоупотребата с лични данни за политическо микротаргетиране и безпрецедентни кампании за координирана дезинформация („фалшиви новини“). Комисията предупреди за възможна кибернамеса в тези избори[177]; борбата срещу нея ще изисква подход изцяло на правителствено и обществено равнище.

Изборна инфраструктура

Организирането на избори е сложно, а гарантирането на тяхната защита и почтеност е отговорност на държавите членки. Намесата в изборите и изборната инфраструктура може да има за цел да повлияе на предпочитанията на гласоподавателите, избирателната активност или на самия изборен процес, включително действителното гласуване, преброяването на гласовете и комуникацията. На изборите за Европейски парламент защитата на така наречената „последна миля“ (съобщаването на резултатите от националните столици до Брюксел) е особено важно предизвикателство с оглед на това, че не съществува и не е изпитан общ подход към сигурността за тази цел[178].

Неотдавнашният пакет от мерки на Комисията за изборите включва мерки за засилване на изборната киберсигурност, като например определянето на национални звена за контакт, които да координират и обменят информация при подготовката за изборите. Обменът на най-добри практики и извлечените поуки са от особено значение[179].

Избирателните системи не се считат за част от критичната инфраструктура[180] и не са обхванати от Директивата за МИС. Въпреки това групата за сътрудничество е разработила практически насоки относно сигурността на изборната технология в подкрепа на публичните органи. Очаква се националните звена за контакт да се срещнат в началото на 2019 г.[181] Държавите членки също така се насърчават да извършват оценки на риска от киберзаплахи за техните изборни процеси.

Дезинформация

Дезинформацията е все по-важен елемент от хибридните атаки, който включва кибератаки и хакерски атаки на мрежи. Тя може да се използва за разделяне на обществата, насаждане на недоверие и подкопаване на доверието в демократичните процеси или във връзка с други въпроси (например движението срещу ваксините или изменението на климата). Нейният мащаб, скорост и обхват се разрастват и тя представлява реална заплаха за сигурността на ЕС.

ЕС предприе редица мерки за борба с дезинформацията. От 2015 г. към ЕСВД беше създадена Оперативна група на ЕС за стратегическа комуникация с Източното съседство за противодействие на дезинформационните кампании на Русия[182]. Експертите приветстваха нейната работа за популяризиране на политиките на ЕС, подпомагане на независимите медии в съседните държави и прогнозиране, проследяване и борба с дезинформацията[183]. Въпреки това ресурсите на оперативната група са ограничени спрямо мащаба и сложността на дезинформационните кампании[184]. Необходимо е по-систематично взаимодействие със съществуващите структури на ЕС и по-добро сътрудничество в областта на стратегическата комуникация[185]. През декември 2018 г. Европейският съвет одобри нов план за действие[186].

Неотдавна въз основа на своето съобщение от април 2018 г. относно борбата с дезинформацията, разпространявана онлайн[187], Комисията разработи доброволен кодекс за поведение на принципа на саморегулирането[188], основан на съществуващите инструменти на политиката, към който се присъединиха онлайн платформите и рекламната индустрия[189]. Действията включват помощ за повишаване на надеждността на съдържанието и подпомагане на усилията за увеличаване на медийната и новинарската грамотност. Беше създадена и независима европейска мрежа от проверители.

Комисията посочва, че в случай че кодексът за поведение не се спазва, може да последват допълнителни регулаторни мерки. Определянето на ефективността на мерките ще се окаже решаващо, по-специално определянето на начини за измерване на подобренията в доверието, прозрачността и отговорното отношение.

Друго предизвикателство ще бъде да се намерят начини за подобряване на откриването, анализа и разобличаването на дезинформацията[190]. Необходимо е и активно и стратегическо наблюдение и анализ на източниците на отворени данни[191]. Опитите за по-добро разбиране на контекста на заплахите следва да обхващат и нововъзникващите тенденции като „дълбинните фалшификати“ (фалшиви видеоматериали, направени с помощта на изкуствен интелект и дълбочинно машинно самообучение), както и необходимите инструменти за тяхното откриване.

Повишаване на автономността

116 ЕС е нетен вносител на свързани с киберсигурността продукти и услуги, което увеличава риска от технологична зависимост и уязвимост от оператори извън ЕС[192]. Тази реалност подкопава по-специално сигурността на критичната инфраструктура на ЕС, която се подпомага и от сложни глобални вериги на доставки. Рискът се увеличава допълнително, когато оператори извън ЕС

придобиват европейски предприятия в областта на киберсигурността. Държавите членки отговарят за скрининга на преките чуждестранни инвестиции (ПЧИ), а в момента не съществува механизъм за скрининг за територията на целия ЕС[193].

117 По-голямата стратегическа автономност е цел на Глобалната стратегия на ЕС и на съобщението от 2017 г. „*Устойчивост, възпиране и отбрана*“[194]. Преодоляването на многобройните предизвикателства, представени в настоящия доклад, ще спомогне за повишаване на тази желана автономност. Нито една отделна мярка няма да постигне това самостоятелно.

Елементи за размисъл – ефективна реакция

- По какъв начин Директивата за МИС е подобрила уведомяването за киберинциденти в критичните сектори и извън тях?
- Колко добре институциите на ЕС интернализират координацията на реакцията при кризи за мащабен киберинцидент?
- Как кибердипломацията може да играе по-важна роля във външните дейности на ЕС?
- Пропорционални ли си на мащаба и сложността на проблема настоящите структури и действия на ЕС за борба с дезинформацията?

Заключителни бележки

118 През последните години Съюзът и неговите държави членки поставиха киберсигурността на предна позиция в дневния ред с цел подобряване на цялостната киберустойчивост. Въпреки това постигането на по-голямо равнище на киберсигурност в Съюза остава мащабно начинание. В настоящия информационно-аналитичен документ ЕСП си постави за цел да открои някои от основните предизвикателства пред амбицията на ЕС да се превърне в най-безопасната цифрова среда в света.

119 Прегледът на ЕСП показва, че е необходимо да се премине към култура на постигането на резултати, за да се гарантира необходимата **отчетност и оценка**. **Остават** някои **пропуски в законодателството, а действащото законодателство не е транспонирано последователно от държавите членки.** Това може да затрудни достигането на пълния потенциал на законодателството. Друго установено предизвикателство е свързано със **съгласуването на равнищата на инвестициите със стратегическите цели**, което изисква увеличаване на инвестициите и тяхното въздействие. Това е по-трудно, когато ЕС и неговите държави членки нямат **ясна представа за разходите на ЕС** за киберсигурност. Съобщава се и за **ограничения при предоставянето на достатъчно ресурси на свързаните с киберсигурността агенции на ЕС**, включително за трудности при привличането и задържането на таланти.

120 В наличните проучвания се стига до заключението, че **управлението на киберсигурността може да бъде укрепено**, за да се повиши способността на световната общност за реагиране на кибератаки и инциденти. Същевременно е невъзможно да се предотвратят всички атаки. Ето защо **бързото откриване и реакция** и **защитата на критичната инфраструктура и обществените функции**, заедно с по-добрия **обмен на информация и координацията** между публичния и частния сектор са основни предизвикателствата, които следва да се преодолеят. И накрая, нарастващият недостиг на умения по киберсигурност в световен мащаб означава, че **повишаването на уменията и осведомеността** във всички сектори и на всички равнища на обществото също представлява съществено предизвикателство.

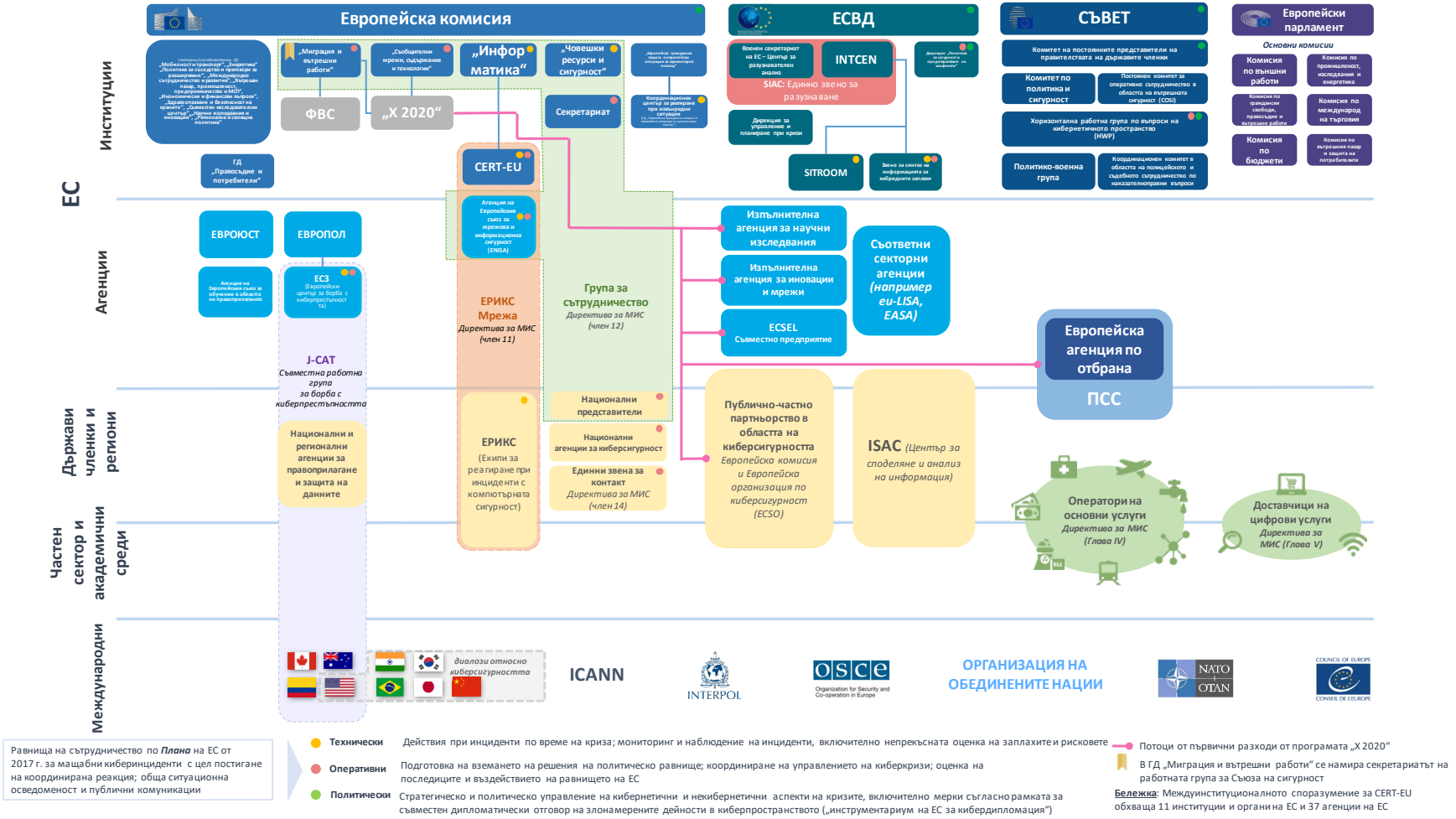
121 Тези предизвикателства, които киберзаплахите поставят пред ЕС и по-широката глобална среда, изискват траен ангажимент и продължаващо неотклонно спазване на основните ценности на ЕС.

Настоящият информационно-аналитичен документ беше приет от Одитен състав III на заседанието му от 14 февруари 2019 г.

За Сметната палата

Klaus-Heiner Lehne
Председател

Приложение I — Сложна, многопластова среда с много участници



Равница на сътрудничество по *Плана* на ЕС от 2017 г. за мащабни киберинциденти с цел постигане на координирана реакция; обща ситуационна осведоменост и публични комуникации

- **Технически** Действия при инциденти по време на криза; мониторинг и наблюдение на инциденти, включително непрекъсната оценка на заплахите и рисковете
- **Оперативни** Подготовка на вземането на решения на политическо равнище; координиране на управлението на киберкризи; оценка на последиците и въздействието на равнището на ЕС
- **Политически** Стратегическо и политическо управление на кибернетични и некибернетични аспекти на кризите, включително мерки съгласно рамката за съвместен дипломатически отговор на злонамерените дейности в киберпространството („инструментариум на ЕС за кибердипломация“)

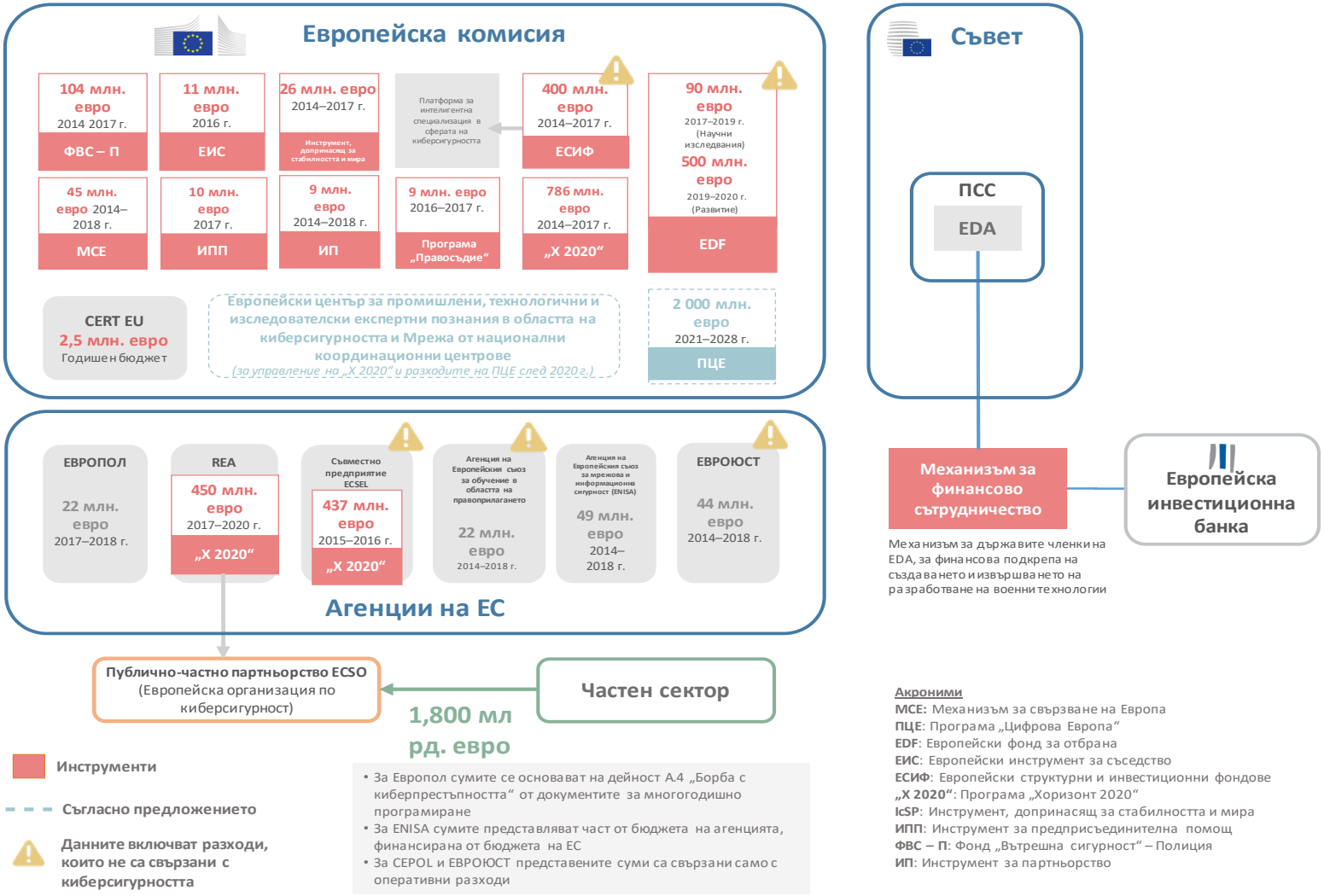
Потоци от първични разходи от програмата „Х 2020“

В ГД „Миграция и вътрешни работи“ се намира секретариатът на работната група за Съюза на сигурност

Бележка: Междуинституционалното споразумение за CERT-EU обхваща 11 институции и органи на ЕС и 37 агенции на ЕС

Източник: ЕСП.

Приложение II — Разходи на ЕС за киберсигурност от 2014 г.



Източник: ЕСП въз основа на документи на Европейската комисия и на агенциите на ЕС.

Приложение III — Доклади на одитните служби на държавите членки

Вид	Заглавие (с хипервръзка)	Година	ДЧ
Одити на съответствието	Докладна записка от оценката на вътрешния контрол	2014 г.	FR
	Доклад относно сертифицирането на отчетите на общата схема за социална сигурност (отбрана, външни работи)	2016 г.	FR
	Сертифициране на държавните отчети	2016 г.	FR
	Гарантиране на сигурността и защитата на националните бази данни от критично значение в Естония	Фин. 2018 година/все още не е публикуван	EE
	Ефективност на вътрешния контрол при защитата на личните данни в националните бази данни	2008 г.	EE
Одити на изпълнението/на икономическата ефективност	Доклад относно ограничаването на кибератаките	2013 г.	DK
	RiR 2014:23 Информационна сигурност в гражданската публична администрация	2014 г.	SE
	Доклад относно обработването от правителството на поверителни данни за лицата и дружествата	2014 г.	DK
	Национална програма за киберсигурност	2014 г.	UK
	Доклад до комисията по бюджета на парламента на Федерална република Германия в съответствие с раздел 88, параграф 2 от Наредбата за федералния бюджет (BHO) – Консолидация на ИТ, федерално правителство	2015 г.	DE
	Доклад относно достъпа до ИТ системи, които подпомагат предоставянето на основни услуги на датското общество	2015 г.	DK
	Публичен орган за планиране Plaine de France	2015 г.	FR
	„Контекст на киберсигурността в Литва“ Версия на литовски език резюме, преведено на английски език	2015 г.	LT
	Изпълнение на задачи в областта на киберсигурността от публичните органи в Полша (на полски език)	2015 г.	PL
	RiR 2015:21 Киберпрестъпност – полицията и прокурорите може да бъдат по-ефективни	2015 г.	SE
	Недостиг на цифрови умения в управлението (проучване)	2015 г.	UK
	Доклад до федералния парламент: Федерални финанси: събиране на данък върху наследствата	2016 г.	BE
	Доклад относно управлението на информационната сигурност в системите, възлагани на външни доставчици	2016 г.	DK
	Одитен доклад относно дейността по кредитиране на Официалния кредитен институт 2016 г.	2016 г.	ES
	Управление на държавната мрежа за сигурност	2016 г.	FI
	Гарантиране на сигурността на ИТ системите, използвани за публични задачи	2016 г.	PL
	Превенция и борба с тормоза в киберпространството сред децата и младите хора	2016 г.	PL

Вид	Заглавие (с хипервръзка)	Година	ДЧ
	Дейност в областта на информационната сигурност в девет агенции – Още един одит на информационната сигурност в държавата. RiR 2016:8	2016 г.	SE
	Защита на информацията в правителството	2016 г.	UK
	Доклад относно защитата на ИТ системите и здравните данни в три региона на Дания	2017 г.	DK
	Докладна записка за резултатите от международния паралелен одит „Ефективност на вътрешния контрол при защитата на личните данни в националните бази данни“.	2017 г.	EE
	Механизми за киберазщита	2017 г.	FI
	Управление на операционната надеждност на електронните услуги	2017 г.	FI
	Мрежа на селскостопанските камари (обобщение)	2017 г.	FR
	Търговско-промишлена камара на Воклюз (от регионалния одитен състав PACA)	2017 г.	FR
	Гарантиране на сигурността и защитата на националните бази данни от критично значение в Естония	Фин. 2018 година/все още не е публикуван	EE
	„Развитие на държавна инфраструктура за електронни комуникации“ Версия на литовски език резюме (преведено на английски език)	2017 г.	LT
	Одит на информационните технологии:Киберсигурност в държавните ведомства	2017 г.	MT
	Система на националните регистри: сигурност, ефективност и използваемост	2017 г.	PL
	Инцидентът WannaCry	2017 г.	UK
	Онлайн измами	2017 г.	UK
	Доклад относно защитата от атаки със софтуер за изнудване	2018 г.	DK
	Болница Арпажон (от регионалната камара на Ил дьо Франс)	2018 г.	FR
	„Управление на критичните държавни информационни ресурси“	2018 г.	LT
	„Електронни престъпления“	2019 г.	LT
	Информационната сигурност в Полша	2019 г.	PL
Други	База данни на публичните органи	Няма данни	BE
	Въпросник относно сигурността и политиката за анализ на риска (в процес на попълване)	Няма данни	BE

Акроними и съкращения

CERT: – EU: Екип за незабавно реагиране при компютърни инциденти

DDoS: Разпределени атаки тип „отказ от обслужване“

DIGIT: Генерална дирекция „Информатика“

EC3: Европейски център за борба с киберпрестъпността към Европол

ECSEL: Електронни компоненти и системи за водещи позиции на Европа

ECSM: Европейски месец на осведомеността за кибернетичната сигурност

ECSO: Европейска организация по киберсигурност

EDA: Европейска агенция по отбрана

ENISA: Агенция на Европейския за мрежова и информационна сигурност

HWPCI: Хоризонтална работна група по въпроси на кибернетичното пространство

ICS: Системи за промишлен контрол

JRC: Съвместен изследователски център

NCIRC: Център на НАТО за реагиране при инциденти с компютърната сигурност

ГД CONNECT: „Съобщителни мрежи, съдържание и технологии“

ГД HOME: Генерална дирекция „Миграция и вътрешни работи“

ГД JUST: Генерална дирекция „Правосъдие и потребители“

Директива за МИС: Директива за мрежовата и информационната сигурност

ДПЧП: Договорно публично-частно партньорство

ЕНО: Европейски надзорен орган

ЕРИКС: Екип за реагиране при инциденти с компютърната сигурност

ЕС: Европейски съюз

ЕСВД: Европейска служба за външна дейност

ЕСИФ: Европейски структурни и инвестиционни фондове

ЕСП: Европейска сметна палата

МСП: Малки и средни предприятия

МССИ: Местен служител по сигурност на информацията

НОС: Национална одитна служба

ОПСО: Обща политика за сигурност и отбрана

ОРЗД: Общ регламент относно защитата на данните

ПСС: Рамка за постоянно структурирано сътрудничество

ПЦЕ: Програма „Цифрова Европа“

ПЧИ: Преки чуждестранни инвестиции

УСИС: Управителен съвет по сигурност на информационните системи

ФВС – П: Фонд „Вътрешна сигурност“ – Полиция

Речник на термините

Адуер: Зловреден софтуер, показващ рекламни банери или изскачащи прозорци, които съдържат код за проследяване на онлайн поведението на жертвите.

Ботнет: Мрежа от компютри, заразени със зловреден софтуер и контролирани от разстояние, без знанието на потребителите, с цел изпращане на нежелани електронни съобщения, кражба на информация или стартиране на координирани кибератаки.

Векторизиране на текст: Процес на преобразуване на думи, изречения или цели документи в цифрови вектори, за да могат да бъдат използвани от алгоритми за машинно самообучение.

Данни за достъпа: Информация за дейностите по вписване и отписване на потребителя за достъп до дадена услуга, като например час, дата и IP адрес.

Дезинформация: Доказуемо невярна или подвеждаща информация, която се създава, представя и разпространява с цел да се извлече икономическа изгода или съзнателно да се въведе в заблуждение обществеността, като последиците от това могат да бъдат в ущърб на обществения интерес.

Достъпност: Осигуряване на навременен и надежден достъп до информация и нейното използване.

Екосистема на киберсигурност: Сложна общност от взаимодействащи си устройства, данни, мрежи, хора, процеси и организации и средата от процеси и технологии, които оказват влияние върху тези взаимодействия и ги подпомагат.

Експлойт кит: Вид инструментариум, който киберпрестъпниците използват, за да атакуват слабите места в мрежовите и информационните системи, така че да могат да разпространяват зловреден софтуер или да извършват други злонамерени дейности.

Заварена система: Излязла от употреба или остаряла компютърна система, приложение или език за програмиране, които все още се използват, но за които може да не са налични актуализации и поддръжка от търговеца, включително поддръжка на сигурността.

Изборна инфраструктура: Включва ИТ системи и бази данни за изборни кампании, чувствителна информация за кандидатите, регистрацията на гласоподаватели и системи за управление.

Изтриващ малуер: Клас малуер, чиято цел е да изтрие твърдия диск на заразения от него компютър.

Интернет на нещата: Мрежата от ежедневни предмети, оборудвани с електроника, софтуер и сензори, за да може да комуникират и да обменят данни по интернет.

Информационна сигурност: Набор от процеси и инструменти за защита на физически и цифрови данни от неразрешен достъп, използване, нарушаване, разкриване, изменение, запис или унищожаване.

Кибератака: Опит за подкопаване или унищожаване на поверителността, целостта и наличието на данни или на компютърна система чрез киберпространството.

Киберинцидент: Събитие, което пряко или непряко вреди на или заплашва устойчивостта и сигурността на дадена ИТ система и данните, които тя обработва, съхранява или предава.

Киберотбрана: Подкатегория на киберсигурността, насочена към защита на киберпространството с военни и други подходящи средства с цел постигане на стратегически военни цели.

Киберпрестъпност: Различни престъпни дейности, в които компютри и ИТ системи са или основен инструмент, или основна цел. Тези дейности включват: традиционни престъпления (например измами, фалшифициране и кражба на самоличност); престъпления, свързани със съдържанието (например онлайн разпространение на детска порнография или подбуждане към расова омраза); и престъпления, които са възможни само при компютри и информационни системи (например атаки срещу информационни системи, предизвикване на отказ на услуга и зловреден софтуер).

Киберпространство: Нематериалната глобална среда, в която се осъществява онлайн комуникация между хора, софтуер и услуги чрез компютърни мрежи и технологични устройства.

Киберсигурност: Всички приети предпазни мерки за защита на ИТ системите и техните данни от неразрешен достъп, атаки и вреди, за да се гарантира тяхната достъпност, поверителност и цялост.

Киберустойчивост: Способността за предотвратяване, подготовка, устояване и възстановяване от кибератаки и инциденти.

Компютърни услуги в облак: Предоставяне на ИТ ресурси по заявка – като например съхранение, изчислителна мощност или капацитет за обмен на данни – по интернет чрез хостинг на отдалечени сървъри.

Коригиране: Въвеждане на набор от промени в софтуер с цел да бъде актуализиран, поправен или подобрен, включително отстраняване на слаби места в сигурността.

Криптиране: Преобразуването на читаема информация в нечитаем код с цел да бъде защитена. За да прочете информацията, потребителят трябва да има достъп до таен ключ или парола.

Криптовалута: Цифров актив, който се издава и обменя чрез използване на техники за криптиране, независимо от централна банка. Той се приема като платежно средство сред членовете на виртуална общност.

Критична инфраструктура: Физически ресурси, услуги и съоръжения, чието нарушаване или унищожаване би имало сериозни последици за функционирането на икономиката и обществото.

Лични данни: Информация, свързана с лице, чиято самоличност може да бъде установена.

Малуер: Зловреден софтуер. Компютърна програма, предназначена да навреди на даден компютър, сървър или мрежа.

Модел „престъпление като услуга“ (Caas): Престъпен бизнес модел, който е двигател на цифровата сива икономика, предоставяща широк кръг от търговски услуги и инструменти, които позволяват на неквалифицирани, начинаещи киберпрестъпници да извършват киберпрестъпления.

Мрежова сигурност: Подкатегория на киберсигурността за защита на данните, които се изпращат чрез устройства в една и съща мрежа, за да се гарантира, че информацията не се прихваща или променя.

Поверителност: Защита на информация, данни или активи от неразрешен достъп или оповестяване.

Престъпление, извършвано чрез кибернетични средства: Традиционно престъпление, което се извършва в по-голям мащаб чрез използване на ИТ системи.

Разпределена атака тип „отказ от обслужване“ (DDoS): Кибератака, която пречи на легитимните потребители да получат достъп до онлайн услуга или ресурс, като я натоварват с повече заявки, отколкото може да поеме.

Скиминг: Кражба на данни от кредитни или дебитни карти при тяхното въвеждане онлайн.

Софтуер за изнудване: Зловреден софтуер, който не позволява на жертвите достъп до компютърна система или прави файловете нечетими, обикновено чрез криптиране. Обикновено след това извършителят на атаката изнудва жертвата, като отказва да възстанови достъпа, докато не бъде платен откуп.

Социално инженерство: В информационната сигурност, психологическа манипулация с цел да се заблудят хората да извършат действие или да разкрият поверителна информация.

Същинско компютърно престъпление: Престъпление, което може да бъде извършено само с използване на ИТ устройства.

Удостоверителни услуги: Услуги, които повишават правната валидност на дадена електронна трансакция, като например електронни подписи, печати, времеви печати, препоръчана поща и удостоверяване на автентичността на уебсайт.

Управление на уязвимостта: Неразделна част от компютърната и мрежовата сигурност с цел активно ограничаване или предотвратяване на използването на уязвимостите на системата и софтуера чрез тяхното установяване, класифициране и отстраняване.

Фишинг: Практиката да се изпращат електронни съобщения, за които се претендира, че идват от надежден източник, за да се заблудят получателите да щракнат върху зловредни връзки или да споделят лична информация.

Хактивист: Лица или групи, които получават неразрешен достъп до информационни системи или мрежи с цел постигане на социални или политически цели.

Хибридна заплаха: Израз на враждебно намерение, който противниците отправят чрез използване на комбинация от конвенционални и неконвенционални техники за водене на война (т.е. военни, политически, икономически и технологични методи), докато твърдо преследват целите си.

Цифрово съдържание: Всички данни – като например текст, звук, изображения или видео – които се съхраняват в цифров формат.

Цялост: Предпазване от неуместно изменение или унищожаване на информация и гарантиране на нейната автентичност.

[1] В проекта за Акт за киберсигурността на ЕС тя е определена като „всички дейности, необходими за защита от киберзаплахи на мрежите и информационните системи, на техните ползватели и засегнати лица“. Очаква се актът да бъде приет от Европейския парламент и Съвета в началото на 2019 г.

[2] Европол, *Оценка на заплахата от организираната престъпност в интернет, 2017 г.*.

[3] Европейска организация за киберсигурност (ECSO), *European Cybersecurity Industry Proposal for a contractual Public-Private Partnership*, 2016 г.

[4] Европейски парламент, *Киберсигурност в Европейския съюз и извън него —проучване относно заплахите и ответните мерки на политика*, Проучване за Комисията по граждански свободи, правосъдие и вътрешни работи (LIBE), септември 2015 г.

[5] ENISA, *ENISA Threat Landscape Report 2017*, 18 януари 2018 г.

[6] Европол, Оценка на заплахата от организираната престъпност в интернет, 2018 г.

[7] Европол, *, пак там,* 2018 г.

[8] Европейски център за политикономика, *Stealing Thunder:Will cyber espionage be allowed to hold Europe back in the global race industrial competitiveness? (Да откраднеш гръм — ще бъде ли позволено на кибершпионажа да забави Европа в световната надпревара за конкурентоспособност на промишлеността?)*, Извънреден документ № 2/18, февруари 2018 г.

[9] Европейската комисия, Годишна реч на председателя относно състоянието на Съюза за 2017 г., State of the Union 2017.

[10] Европол, *World’s Biggest Marketplace selling internet paralysing DDoS attacks taken down*, съобщение за пресата, 25 април 2018 г.

[11] Европол, *Оценка на заплахата от организираната престъпност в интернет, 2017 г.*.

[12] Европейска комисия, Информационна справка относно киберсигурността, септември 2017 г.

[13] Разходите могат да включват: загуба на приходи; разходи за ремонт на повредени системи; потенциални задължения за откраднати активи или информация; стимули за запазване на клиенти; по-високи застрахователни премии; по-големи разходи за защита (нови системи, служители, обучение); потенциално уреждане на разходи за постигане на съответствие или на съдебни разноски.

[14] NTT Security, *Risk: Value 2018 Report*.

[15] Софтуерът *WannaCry* използва уязвими места в протокола на Microsoft Windows, позволяващи дистанционно “превземане” на който и да е компютър. След като откриха тази уязвимост, от Microsoft пуснаха коригираща програма. Стотици хиляди компютри обаче все още не бяха актуализирани и впоследствие много от тях бяха заразени. Източник: A. Greenberg, *Отговорността за Wannacry е на Северна Корея, но и на Агенцията за национална сигурност*, WIRED, 19 декември 2017 г.

[16] Европейска комисия, *Нагласи на европейците по отношение на киберсигурността (Europeans' attitudes towards cybersecurity*, специално проучване Евробарометър 464a, септември 2017 г. Очаква се в началото на 2019 г. да бъде публикувано последващо проучване.

[17] Конвенцията от Будапеща е обвързващ международен документ с насоки за държави, разработващи законодателство за борба с киберпрестъпността. Тя предоставя рамка за международно сътрудничество между държавите – страни по конвенцията. Понастоящем Комисията, Съветът на Европейския съюз, Европол, ENISA и Евроюст представляват ЕС.

[18] Европейска комисия, *Стратегия на Европейския съюз за киберсигурност: Отворено, безопасно и сигурно киберпространство*, JOIN (2013) 1 окончателен, 7 февруари 2013 г.

[19] Европейска комисия, *Европейска програма за сигурност*, COM(2015) 185 окончателен, 28 април 2015 г.

[20] Европейска комисия, *Стратегия за цифров единен пазар в Европа*, COM(2015) 192 окончателен, 6 май 2015 г.

[21] EEAS *Обща визия, общи действия за по-силна Европа. Глобална стратегия за външната политика и политика на сигурност на Европейския съюз*, юни 2016 г.

[22] Зловредният софтуер, използван при атаката със софтуера WannaCry, която беше приписана на Северна Корея от Съединените щати, Обединеното кралство и Австралия, първоначално е разработен и съхраняван в Агенцията за национална сигурност на САЩ, за да могат да се използват уязвими места в Windows. Източник: A. Greenberg, пак там, WIRED, 19 декември 2017 г. След атаките Microsoft осъди съхраняването на слаби места на софтуер от правителствата и повтори призива си за необходимост от цифрова Женевска конвенция.

[23] Център за европейски политически изследвания (CEPS), *Strengthening the EU's Cyber Defence Capabilities – доклад на оперативна група на CEPS*, ноември 2018 г.

[24] В допълнение към земя, море, въздух и космическо пространство.

[25] Политическа рамка на ЕС за кибернетична отбрана (актуализация през 2018 г.)

[26] Европейска комисия/Европейска служба за външна дейност, *Съвместна рамка за борба с хибридните заплахи — ответни действия на Европейския съюз*, JOIN(2016) 18 окончателен.

[27] Съвместна декларация на председателите на Европейския съвет и Европейската комисия и генералния секретар на Организацията на северноатлантическия договор, 8 юли 2016 г. и 10 юли 2018 г.

[28] Европейска комисия/Европейската служба за външна дейност, *„Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“,* JOIN(2017) 450 окончателен, 13 септември 2017 г.

[29] 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 (ОВ L 194, 19.7.2016 г., стр. 1).

[30] 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.

[31] Те се интегрират в създадени с директивата структури за сътрудничество, мрежата на ЕРИКС (мрежа, която се състои от определените от държавите членки на ЕС ЕРИКС и CERT-EU; ENISA изпълнява ролята на секретариат) и групата за сътрудничество (улеснява и подкрепя стратегическото сътрудничество и обмена на информация между държавите членки, за която ролята на секретариат се изпълнява от Комисията).

[32] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 г. относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

[33] Европейска комисия, *Предложение за Регламент на Европейския парламент и на Съвета относно ENISA — Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“)*, COM(2017) 477 окончателен, 13 септември 2017 г..

[34]Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно европейските заповеди за предоставяне и за запазване на електронни доказателства по наказателноправни въпроси, COM(2018) 225 окончателен, 17 април 2018 г.

[35] Европейска комисия, *Предложение за ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА за установяване на хармонизирани правила относно определянето на юридически представители за целите на събирането на доказателства по наказателни производства*. COM(2018) 226 окончателен, 17 април 2018 г.

[36] Европейска комисия, *Предложение за регламент на Европейския парламент и на Съвета за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове,* COM(2018) 630 окончателен, 12 септември 2018 г.

[37] H. Carrapico и A. Barrinha, *The EU as a Coherent (Cyber)Security Actor?*, Journal of Common Market Studies, том 55, № 6, 2017 г.

[38] Европейска комисия, пак там, SWD(2017) 295 окончателен, 13 септември 2017 г.

[39] Служба на ЕП за парламентарни изследвания, *Трансатлантическа кибернесигурност и киберпрестъпност. Икономическо въздействие и бъдещи перспективи*, ЕП 603.948, декември 2017 г.

[40] ENISA, *Рамка за оценяване на стратегии за киберсигурност*, 27 ноември 2014 г.

[41] Изключение прави член 14 (Мониторинг и статистика) от Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 година относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета.

[42] Европейски икономически и социален комитет, *Cybersecurity: ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks*, март 2018 г. Оперативна група на CEPS-ECRI, Киберсигурност във финансите – достигане до правилния политически микс!, юни 2018 г.

[43] 24 от 28 ВОИ в държавите членки отговориха на нашата анкета.

[44] Т.е. основана на принципи и възможно най-неутрална по отношение на технологиите.

[45] Европейска комисия, Механизъм за научни становища, Научно становище № 2/2017, 24 март 2017 г.

[46] L. Rebuffi, *EU Digital Autonomy:A possible approach*, Digma Zeitschrift für Datenrecht und Informationssicherheit, септември 2018 г. Европейски център за политикономика, пак там, Извънреден документ № 2/18, февруари 2018 г.

[47] Европейска комисия, *Предложение за директива на Европейския парламент и на Съвета относно някои аспекти на договорите за предоставяне на цифрово съдържание*, COM(2015) 634 окончателен, 9 декември 2015 г.

[48] Европейска комисия, *Предложение за директива на Европейския парламент и на Съвета относно някои аспекти на договорите за онлайн продажби и други продажби на стоки от разстояние*, COM(2017) 635 окончателен, 9 декември 2015 г.

[49] Нидерландски съвет по киберсигурност, *Европейска прогнозна среща по въпросите на киберсигурността 2016 г.: Публично-частни академични препоръки към Европейската комисия относно „интернет на нещата“ и хармонизирането на задълженията за полагане на грижа*, 2016 г.

[50] Център за европейски политически изследвания, *Оповестяване на уязвимостта на софтуера в Европа –технологии, политики и правни предизвикателства – доклад на оперативна група на CEPS*, юни 2018 г.

[51] Европейска комисия, *Максимално оползотворяване на МИС — за ефективно прилагане на Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза*, COM(2017) 476 окончателен/2, 4 октомври 2017 г.

[52] Европол, пак там, 2017 г.

[53] Съвет на Европейския съюз, *Окончателен доклад относно седмия кръг на взаимни оценки „Практическо изпълнение и функциониране на европейските политики за превенция на киберпрестъпността и борба с нея“*, 12711/1/17 REV 1, 9 октомври 2017 г.

[54] Европейска комисия, Оценка на въздействието, придружаваща документа Предложение за Директива относно борбата с измамата и подправянето на непарични платежни средства, SWD(2017) 0298 окончателен, 13 септември 2017 г. През декември 2018 г. беше постигнато политическо споразумение относно новото законодателство и се очаква то да бъде прието в началото на 2019 г.

[55] Европол, пак там, 2017 г.

[56] C-362/14: Maximillian Schrems срещу Data Protection Commissioner (Ирландия), 6 октомври 2015 г.

[57] Европол/Евроюст, *Общи предизвикателства в борбата с киберпрестъпността*, 7021/17, 13 март 2017 г.

[58] Европейска комисия, *Оценка на стратегията за киберсигурност на ЕС за 2013 г.*, SWD (2017) 295 окончателен, 13 септември 2017 г.

[59] Служба на ЕП за парламентарни изследвания, *Брифинг:Законодателството на ЕС в развитие – Преглед на контрола на износа на изделия с двойна употреба*, PE589.832.

[60] Резолюция на Европейския парламент, *Правата на човека и технологиите: отражението на охранителните системи и системите за наблюдение върху правата на човека в трети държави*, (2014/2232(INI)), 8 септември 2015 г. Стоките и услугите с двойна употреба, които включват софтуер и технологии, могат да имат гражданско и военно приложение.

[61] Публично достъпната информация се съхранява в базата данни WHOIS, управлявана от ICANN (Интернет корпорация за присвоени имена и адреси). ICANN поддържа системата за имена на домейни. Злоупотребата с имена на домейни улеснява киберпрестъпността.

[62] Член 3, Директива за МИС, пак там.

[63] Атлантически съвет, *Връзка с риска:победени от киберрисковете?Икономически ползи и разходи на алтернативното кибербъдеще*, 10 септември 2015 г.

[64] Белият дом, *Разходи за киберсигурност за данъчната 2019 година*.

[65] Европейска комисия, *Работен документ на службите на Комисията:Оценка на въздействието, придружаваща документа Предложение за регламент на Европейския парламент и на Съвета за създаване на програмата „Цифрова Европа“ за периода 2021–2027 г.*, SWD(2018) 305 окончателен, 6 юни 2018 г.

[66] Център за стратегически изследвания в Хага, *Инвестиции на Нидерландия в ИКТ и киберсигурност: поглед в перспектива*, декември 2016 г.

[67] Европейска комисия, пак там, COM(2018) 630 окончателен, 12 септември 2018 г.

[68] Отдел за научни прогнози към Службата на ЕП за парламентарни изследвания, *Постигане на суверенен и надежден сектор на ИКТ в ЕС*, декември 2017 г.

[69] Европейски алианс на цифровите МСП, *Документ за позиция относно европейската стратегия за киберсигурност – насърчаване на екосистемата на МСП*, 31 юли 2017 г.

[70] Отдел за научни прогнози към Службата на ЕП за парламентарни изследвания, пак там, декември 2017 г.

[71] Пак там.

[72] Европейска комисия, *Оценка на въздействието на предложените център за изследователски експертни познания и Мрежа от национални координационни центрове*, SWD(2018) 403 окончателен (Част 1/4), 12 септември 2018 г.

[73] Европейска комисия, пак там, COM(2018) 630 окончателен, 12 септември 2018 г.

[74] ЕСП, Специален доклад № 13/2018: „Мерки срещу радикализацията, която води до тероризъм“

[75] Посочените в настоящия раздел данни са от публично достъпни документи на Комисията, с изключение на тези за 42 млн. евро в точка ***53***, които Комисията предостави пряко на ЕСП.

[76] „Хоризонт 2020“ е програмата на ЕС за научни изследвания и иновации на стойност 80 млрд. евро, подпомагаща Съюза за иновации, чиято цел е да гарантира глобалната конкурентоспособност на ЕС.

[77] „Хоризонт 2020“, Обществено предизвикателство 7 „Сигурни и иновативни общества – защита на свободата и сигурността на Европа и нейните граждани“.

[78] ЕСП анализира проекти по „Х 2020“ от базата данни CORDIS. ЕСП извърши векторизиране на текста за описанието на всеки проект, като използва таксономията на JRC за киберсигурността (вж. ***каре 5*** в следващата глава), за да установи проектите, за които има вероятност да са свързани с киберсигурността. След това ЕСП извърши ръчна проверка и анализ на резултатите.

[79] Европейска организация по киберсигурност, *Доклад на ECSO за мониторинг на напредъка на ДПЧП за периода 2016–2017 г.*, 29 октомври 2018 г.

[80] Член 9, параграф 2, Директива за МИС, пак там.

[81] GLACY+ (Глобални действия в областта на киберпрестъпността+) е съвместен проект със Съвета на Европа. Той подпомага дванадесет държави от Африка, Азия и Тихоокеанския басейн, Латинска Америка и региона на Карибския басейн, които на свой ред могат да служат като центрове за обмен на опит със съответните им региони.

[82] Европейският център за политическа стратегия (EPSC), аналитичният център на Комисията, коментира риска от поява на „бяло петно в цифровата сфера“, ако разделението между ЕС и неговите съседни държави от Западните Балкани продължи да се разраства. Държави като Китай и Русия инвестират значителни суми в региона, което поражда риск ЕС да бъде игнориран като участник в киберпространството в региона. Източник: EPSC, *Ангажиране със Западните Балкани – инвестиция в сигурността на Европа*, 17 май 2018 г.

[83] Европейска инвестиционна банка, *Оперативна рамка и оперативен план на групата на ЕИБ за 2018 г.*, 12 декември 2017 г. Към момента на изготвяне на документа не беше налична допълнителна информация.

[84] Европейска комисия, *Предложение за регламент на Европейския парламент и на Съвета за създаване на програмата „Цифрова Европа“ за периода 2021–2027 г.*, COM(2018) 434 окончателен, 6 юни 2018 г.

[85] Европейска комисия, *Регламент (ЕС) 2018/1092 на Европейския парламент и на Съвета от 18 юли 2018 г. за създаване на Европейска програма за промишлено развитие в областта на отбраната с цел подкрепа на конкурентоспособността и иновационния капацитет на отбранителната промишленост на Съюза* (ОВ L 200, 7.8.2018 г., стр. 30). Освен това през 2017 г. беше създадено подготвително действие за научни изследвания в областта на отбраната на обща стойност 90 млн. евро за периода 2017–2019 г. и финансирано от „Х 2020“. Не е ясно дали то включва разходи, свързани с киберсигурността.

[86] През 2019 г. се планира да бъде публикуван отделен информационно-аналитичен документ на ЕСП относно отбраната на ЕС.

[87] Работната сила на ЕС3 на Европол, ENISA, ЕСВД, Европейската агенция по отбрана и CERT-EU възлиза общо на 159 души. В този общ брой не са включени свързаните с киберпространството служители в Европейската комисия или в държавите членки. Източник: Център за европейски политически изследвания, пак там, ноември 2018 г.

[88] *Оценка на ENISA*, 2017 г.

[89] В своя многогодишен план за периода 2018–2020 г. Европол е поискала годишно увеличение на персонала със 70 временно наети лица, но за 2018 г. е одобрено увеличение от едва 26 служители. В следващия проект на многогодишен план за периода 2019–2021 г. Европол е включила умерено увеличение тъй като се предполага, че искане за повече ресурси няма да бъде изпълнено. Източник: Консултация относно многогодишното програмиране за периода 2019–2021 г., представена пред Съвместната група за парламентарен контрол, A 000834, 1 февруари 2018 г.

[90] *Оценка на ENISA*, 2017 г. В периода 2014—2016 г. около 80 % от оперативния бюджет на ENISA са използвани за възлагане на проучвания.

[91] ENISA, *Проучване на възможностите и ограниченията на настоящите платформи за разузнавателни данни за заплахи*, декември 2017 г.

[92] ISACA (известна по-рано като Асоциация за одит и контрол на информационни системи), *Управление на информационната сигурност – насоки за съветите на директорите и изпълнителните управителни органи*, второ издание, 2006 г.

[93] EY, *Да си върнем киберсигурността: подготовка за справяне с кибератаки.20-то глобално проучване на информационната сигурност от 2017 г.*, стр. 16.

[94] McKinsey (J. Choi, J. Kaplan, C. Krishnamurthy и H. Lung), *Мит или реалност? Информация за действителните разходи и въздействието на програмите за киберсигурност*, юли 2017 г.

[95] Комисия по ценните книжа и борсите, *Коментари и тълкувателни насоки относно оповестяването на рискове за киберсигурността от публични дружества*, 21 февруари 2018 г.

[96] Форум за сътрудничество между Европейския банков орган, Европейския орган за ценни книжа и пазари и Европейския орган за застраховане и професионално пенсионно осигуряване.

[97] Европейски орган за ценни книжа и пазари, *Доклад на Съвместния комитет относно рисковете и уязвимостите във финансовата система на ЕС*, април 2018 г.

[98] ENISA, *Информационна сигурност и стандарти за неприкосновеност на личния живот за МСП: препоръки за подобряване на приемането на стандарти за информационна сигурност и неприкосновеност на личния живот в МСП*, декември 2015 г.

[99] По отношение на държавите членки Механизмът за научни становища на Комисията отбеляза значителната и уникална степен на съгласие относно основните принципи и ценности, както и общия стратегически интерес, които могат да залегнат в основата на ефективното управление на киберсигурността в ЕС. Източник: Научно становище 2/2017, 24 март 2017 г.

[100] Съединените щати, Китай, Япония, Южна Корея, Индия и Бразилия.

[101] Европейски колеж по сигурност и отбрана (T. Renard и A. Barrinha), *Наръчник по киберсигурност, глава 3.4 ЕС като партньор в кибердипломацията и отбраната*, 23 ноември 2018 г.

[102] Съвет на Европейския съюз, *План за действие за изпълнение на заключенията на Съвета относно Съвместното съобщение до Европейския парламент и Съвета: „Устойчивост, възпиране и отбрана:изграждане на силна киберсигурност за ЕС“*, 15748/17, 12 декември 2017 г.

[103] Европейска комисия, *Цифрова стратегия на Европейската комисия: Цифрово преобразувана, насочена към потребителите и основана на данни Комисия*, C(2018) 7118 окончателен, 21 ноември 2018 г.

[104] Отговор на члена на Комисията Габриел на въпрос с искане за писмен отговор (E-004294-17), 28 юни 2017 г.

[105] Съвет на Европейския съюз, *Годишен доклад за прилагането на Политическата рамка за кибернетична отбрана*, 15870/17, 19 декември 2017 г.

[106] Решения 2015/443, 2015/444 и 2017/46 уреждат сигурността на комуникационните и информационните системи на Комисията. С Решение C(2018) 7706 на Комисията от 21 ноември 2018 г. се създава Съвет по информационни технологии и киберсигурност, в който се сливат предишният Съвет по информационни технологии и Управителният съвет по сигурност на информационните системи.

[107] Европейски икономически и социален комитет, пак там, 2018 г.

[108] Европейски парламент, пак там, септември 2015 г.

[109] Звеното за синтез на информацията за хибридните заплахи е създадено през 2016 г. в рамките на Центъра на ЕС за анализ на информация към ЕСВД. То получава и анализира класифицирана информация и информация от открити източници, предоставяна от различни заинтересовани страни във връзка с хибридни заплахи.

[110] ENISA, *Оценки на риска на национално равнище: доклад за анализ*, ноември 2013 г.

[111] Европейска комисия, *Оценка на въздействието на Агенцията на ЕС за киберсигурност и Акта за киберсигурността*, SWD(2017) 500 окончателен (Част 1/6), 13 септември 2017 г.

[112] Европейска комисия, пак там,SWD(2018) 403 окончателен, 12 септември 2018 г.

[113] Мрежов координационен център на европейската IP мрежа, регионалният интернет регистър за Европа, който контролира разпределянето и регистрацията на ресурси за интернет номера.

[114] ENISA, *Широкомащабна пилотна съвместна кампания на EISAS за повишаване на осведомеността на гражданите и МСП в ЕС*, ноември 2012 г.

[115] Център за кибербезопасност и образование, в партньорство с Booz Allen Hamilton, Alta Associates и Frost & Sullivan, *Проучване на световната работна сила в областта на информационната сигурност за 2017 г. – сравнителен анализ на капацитета на работната сила и реакцията на киберрискове*.

[116] Европейски икономически и социален комитет, пак там, 2018 г.

[117] Камара на лордовете, *Съвместна комисия в Камарата на общините по Стратегията за национална сигурност, умения в сферата на киберсигурността и критичната национална инфраструктура на Обединеното кралство, втори доклад за сесия 2017–2019 г.*, 16 юли 2018 г.

[118] Европол/Евроюст, *Общи предизвикателства в борбата с киберпрестъпността*, 7021/17, 13 март 2017 г.

[119] Европол/Евроюст, пак там, 7021/17, 13 март 2017 г.

[120] Европейска комисия, пак там,SWD(2018) 403 окончателен, 12 септември 2018 г.

[121] CEPOL, *Решение на Управителния съвет 33/2018/МВ относно единния програмен документ на CEPOL за периода 2020–2022 г.*, 20 ноември 2018 г.

[122] Например сътрудничество между ЕСВД, държавите членки, агенции и органи като CEPOL, ECTEG или EDSC.

[123] ENISA, *Анализ на нуждите от обучение по информационна сигурност в секторите от критично значение*, декември 2017 г.

[124] Европейска група за обучение и образование в областта на борбата с киберпрестъпността.

[125] Европейска комисия, Тринадесети доклад за напредъка в създаването на ефективен и истински Съюз на сигурност (COM(2018) 46 окончателен, 24 януари 2018 г.

[126] Въз основа на констатациите и оценките в Специален доклад № 14/2018, пак там.

[127] Резолюция на Европейския парламент от 13 юни 2018 г. относно киберотбраната (2018/2004(INI)). Съвет на Европейския съюз, пак там, 15870/17, 19 декември 2017 г.

[128] Швейцария, бивша югославска република Македония, Украйна, Босна и Херцеговина, Косово (това название не засяга позициите по отношение на статута и е съобразено с Резолюция 1244/1999 на Съвета за сигурност на ООН и становището на Международния съд относно обявяването на независимост от страна на Косово), Турция и Съединените щати.

[129] Европол, *Оценка на заплахата от организираната престъпност за ЕС за 2018 г.*

[130] Европейска комисия, пак там, SWD(2017) 295 окончателен, 13 септември 2017 г.

[131] B. Stanton, M. F. Theofanos, S. S. Prettyman и S. Furman, *Security Fatigue*, списание „IT Professional“, том 18, брой 5, 2016 г., стр. 26–32. Вж. също NIST.

[132] Европейска комисия/Европейска служба за външна дейност, *Повишаване на устойчивостта и укрепване на способностите за борба с хибридните заплахи*, JOIN(2018) 16 окончателен, 13 юни 2018 г.

[133] Например затварянето на AlphaBay и Hansa при съвместни операции, ръководени от ФБР и нидерландската национална полиция с подкрепата на Европол. Това бяха два от най-големите пазари за търговия с незаконни стоки като наркотици, огнестрелни оръжия и инструменти за извършване на киберпрестъпления, като например зловреден софтуер. Източник: Европол, *Престъпност в тъмната мрежа: координираното правоприлагане е единственото средство за справяне с нея*, Съобщение за пресата, 29 май 2018 г.

[134] Европейска комисия, пак там, SWD(2018) 403 окончателен, 12 септември 2018 г.

[135] Съвет на Европейския съюз, пак там, 12711/1/17 REV 1, 9 октомври 2017 г.

[136] Европейска комисия, пак там, SWD(2017) 295 окончателен, 13 септември 2017 г.

[137] Европейска комисия/Европейска служба за външна дейност, пак там, JOIN(2018) 16, 13 юни 2018 г.

[138] Европейска комисия, SWD(2017) 500 окончателен, 13 септември 2017 г.

[139] *Меморандум за разбирателство – ENISA, EDA,EC3 на Европол и CERT-EU*, 23 май 2018 г.

[140] Европейска комисия, Покана за представяне на предложения: *Създаване и експлоатация на пилотен проект за Мрежа за компетентност в сферата на киберсигурността с цел да се разработи обща пътна карта за научни изследвания и иновации в областта на киберсигурността*, 27 октомври 2017 г.

[141] Жан-Клод Юнкер, Възложително писмо до члена на Европейската комисия, отговарящ за Съюза на сигурност, 2 август 2016 г. Отбраната не попада в компетентността на работната група.

[142] Съвет на Европейския съюз, *Пътна карта на ЕС за киберсигурността*, 8901/17, 11 май 2017 г.

[143] Friends of Europe („Приятели на Европа“), *Дебат за сигурността плюс:краудсорсинг на решения за световните проблеми в областта на сигурността* 5-то издание, ноември 2017 г.

[144] Технически доклади на JRC, Карта на европейските експертни центрове по въпросите на киберсигурността: *определения и таксономия.* Оценка на въздействието на предложените център за изследователски експертни познания и Мрежа от национални координационни центрове, SWD(2018) 403 окончателен, 12 септември 2018 г.

[145] Европейска комисия, пак там,SWD(2017) 295 окончателен, 13 септември 2017 г.

[146] Европейска комисия, пак там,SWD(2018) 403 окончателен, 12 септември 2018 г.

[147] Например ISAC към европейските финансови институции включва представители на финансовия сектор, националните CERT, правоприлагащи агенции, ENISA, Европол, Европейската централна банка, Европейският платежен съвет и Европейската комисия.

[148] ENISA, *Модели на сътрудничество на Центровете за споделяне и анализ на информация (ISAC)*, 14 февруари 2018 г.

[149] Съвет на Европейския съюз, пак там, 12711/1/17 REV 1, 9 октомври 2017 г.

[150] https://www.europol.europa.eu/empact.

[151] В проучване на Accenture от 2018 г. в 15 държави беше установено, че се предотвратяват 87 % от целенасочените кибератаки: *Състояние на киберустойчивостта 2018 г.*, 10 април 2018 г.

[152] P. Timmers, *Киберсигурността налага преосмисляне на стратегическата автономност*, Политически блог на Oxford University, 14 септември 2018 г.

[153] Caroline Preece, *Три причини, поради които откриването на киберзаплахи все още е неефективно*, IT Pro, 14 юли 2017 г.

[154] Европейски икономически и социален комитет, *пак там*, март 2018 г.

[155] Европейска комисия, *Осми доклад за напредъка по създаването на ефективен и истински Съюз на сигурност*, COM(2017) 354 окончателен, 29 юни 2017 г.

[156] Вж. различните публикации на групата за сътрудничество във връзка с МИС.

[157] ДПУ 2: Директива за платежните услуги 2; ЕЦБ/ЕНМ: Европейска централна банка/Единен надзорен механизъм; Target 2: Трансевропейска автоматизирана система за брутен сетълмент на експресни преводи в реално време (второ поколение), Регламент (ЕС) № 910/2014 относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар. Източник: Оперативна група на CEPS-ECRI, пак там, юни 2018 г.

[158] Европейска комисия, *Препоръка относно координирана реакция на мащабни киберинциденти и кризи*, C(2017) 6100 окончателен, 13 септември 2017 г.

[159] Европейска комисия, пак там,SWD(2017) 295 окончателен, 13 септември 2017 г. Съществуват няколко механизма за управление на кризи, включително механизмът за интегрирана реакция на ЕС при политическа криза, Argus (механизмът на Комисията за реакция при кризи), механизмът на ЕСВД за реакция при кризи, Механизмът за гражданска защита на Съюза и Протоколът за реагиране при извънредни ситуации на правоприлагащите органи в ЕС.

[160] Освен това то може да предизвика позоваване на член 42, параграф 7 от Договора за Европейския съюз (клаузата за взаимна помощ) или член 222 от Договора за функционирането на Европейския съюз (клаузата за солидарност).

[161] Европейска комисия/Европейска служба за външна дейност, пак там, JOIN(2018) 16, 13 юни 2018 г. През декември 2018 г. в медиите беше съобщено за предполагаеми хакерски атаки на мрежата на ЕСВД за дипломатическа комуникация COREU (източник: *New York Times, Разбити от хакери европейски каблограми показват силно безпокойство във връзка с Тръмп, Русия и Иран*; 18 декември 2018 г.). В момента въпросът се разследва.

[162] Сътрудничеството в областта на ранното предупреждение и взаимопомощта също трябва да се доразвие: *Заключения на Съвета относно координираната реакция на ЕС при мащабни инциденти и кризи в областта на киберсигурността*, 10085/18, 26 юни 2018 г.

[163] Служба на ЕП за парламентарни изследвания, *Брифинг Законодателството на ЕС в развитие: ENISA и нов акт за киберсигурността*, PE 614.643, септември 2018 г.

[164] Европейски икономически и социален комитет, пак там, 2018 г.

[165] Съвет на Европейския съюз, *Протокол на ЕС за спешно реагиране на правоприлагащите органи (LE ERP) за мащабни трансгранични кибератаки*, 14893/18, декември 2018 г.

[166] Екипи за бързо реагиране при кибератаки и екипи за взаимопомощ в областта на киберсигурността; Платформа за обмен на информация относно киберзаплахи и реагиране при инциденти. Източник: Съвет на Европейския съюз, *Актуализиран списък на проекти в рамките на постоянното структурирано сътрудничество (ПСС) – общ преглед*, 19 ноември 2018 г.

[167] Съвет на Европейския съюз, Заключения относно разработването на рамка за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството, 9916/17, 7 юни 2017 г.

[168] Съвет на Европейския съюз, *Заключения на Съвета относно кибердипломацията*, 6122/55, 11 февруари 2015 г.

[169] Съвет на Европейския съюз, *Проект на насоки за изпълнение за рамката за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството*, 13007/17.

[170] Определянето на отговорност за даден инцидент остава суверенно политическо решение на държавите членки, а не всички мерки на инструментариума изискват такова определяне.

[171] Инструментариумът не доведе до съвместни действия; отделните държави членки приеха позицията на САЩ.

[172] Съвет на Европейския съюз, *Заключения на Съвета относно злонамерени действия в киберпространството*, 7925/18, 16 април 2018 г.

[173] Някога компютърните системи контролираха процесите в различни сектори, като например комунални услуги, химическо и промишлено производство, хранително-вкусова промишленост, транспортни системи и центрове и логистични услуги.

[174] ENISA, пак там, декември 2017 г.

[175] Например публичната администрация, химическата и ядрената промишленост, производството, хранително-вкусовата промишленост, туризмът, логистиката и гражданската защита.

[176] Европейска комисия, пак там,SWD(2017) 295 окончателен, 13 септември 2017 г.

[177] Изказване на члена на Комисията Йоурова на пленарната сесия на Европейския парламент относно *Повишаване на устойчивостта на ЕС срещу влиянието на чуждестранни участници върху предстоящата предизборна кампания за ЕП*, 14 ноември 2018 г.

[178] Фондация „Карнеги“ за международен мир, *Руска намеса в изборите: борбата на Европа срещу фалшивите новини и кибератаките*, 23 май 2018 г.

[179] Европейски център за политическа стратегия (L. Past), Киберсигурност на изборната технология: неизбежни атаки и разнообразни реакции, в: „Изборна намеса в цифровата ера – изграждане на устойчивост на киберзаплахи: сборник от аналитични статии на 35 водещи специалисти и експерти“, 2018 г.

[180] Съгласно Директива 2008/114/ЕО на Съвета относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита.

[181] Европейска комисия, Препоръка относно мрежите за изборно сътрудничество, онлайн прозрачността, защитата срещу кибернетични инциденти и борбата срещу кампаниите за дезинформация в контекста на изборите за Европейски парламент, C(2018) 5949 окончателен, 12 септември 2018 г.

[182] Заключения на Европейския съвет, EUCO 11/15, 20 март 2015 г. Оттогава насам бяха добавени две допълнителни оперативни групи – за Западните Балкани и Южното съседство.

[183] В доклад на Атлантическия съвет ЕС беше призован да изиска от всички държави членки да изпратят национални експерти в оперативната група. Вж.: D. Fried и A. Polyakova, *Демократична защита срещу дезинформацията*, 5 март 2018 г.

[184] Първоначално без собствен бюджет, през 2018 г. от Европейския парламент ѝ бяха отпуснати 1,1 млн. евро за подготвително действие „StratCom Plus“.

[185] Фондация „Карнеги“ за международен мир, (E. Brattberg, T. Maurer), пак там, 23 май 2018 г.

[186] Европейска комисия, Върховен представител на Съюза по въпросите на външните работи и политиката на сигурност, *План за действие за борба с дезинформацията*, JOIN(2018) 36 окончателен. Планът е съсредоточен върху: подобряване на способността на институциите на ЕС за откриване, анализиране и разкриване на дезинформация; засилване на координираната и съвместна реакция; мобилизиране на частния сектор; и засилване на осведомеността и устойчивостта на обществото.

[187] Европейска комисия, *Европейски подход за борба с дезинформацията, разпространявана онлайн*, COM(2018) 236 окончателен, 26 април 2018 г.

[188] Да не се бърка с кодекса на поведение за противодействие на незаконната реч на омразата онлайн.

[189] JRC, *Цифровата трансформация на новинарските медии и подемът на дезинформацията и фалшивите новини*, Технически доклади на JRC, JRC Digital Economy Working Paper 2018-02, април 2018 г.

[190] ENISA, *Засилване на мрежовата и информационната сигурност и защита срещу дезинформацията, разпространявана онлайн („фалшивите новини“)*, април 2018 г.

[191] Европейски център за политическа стратегия (C. Frutos López), *Отговорност за подпомагане на организацията на изборите при предвиждането и противодействието на киберзаплахите*, в: пак там, 2018 г.

[192] Европейска комисия, пак там, SWD(2018) 403 окончателен, 12 септември 2018 г.

[193] Предложеният регламент (COM(2017) 487 окончателен, 13 септември 2018 г.) за скрининг на ПЧИ, представен през септември 2017 г., в момента преминава през законодателния процес. Той обхваща по-специално критичните технологии, които включват изкуствен интелект, киберсигурност и приложения с двойна употреба.

[194] Европейска комисия/Европейска служба за външна дейност, пак там, JOIN(2017) 450 окончателен, 13 септември 2017 г.

Екип на ЕСП

Настоящият информационно-аналитичен документ – „Предизвикателства пред ефективното прилагане на политиката за киберсигурност на ЕС“ беше приет от Одитен състав III „Външни дейности/Сигурност и правосъдие“, с ръководител Bettina Jakobsen – член на ЕСП. Одитът беше ръководен от члена на ЕСП Baudilio Tomé Muguruza, със съдействието на Daniel Costa de Magalhaes – ръководител на неговия кабинет, и Ignacio Garcia de Parada – аташе в кабинета; Alejandro Ballester-Gallardo — главен ръководител; Michiel Sweerts – ръководител на задача; Simon Dennett, Aurelia Petliza, Mirko Iaconisi, Michele Scardone, Silvia Monteiro Da Cunha – одитори, и Johannes Bolkart – стажант. Hannah Critoph предостави езикова подкрепа.

От ляво надясно: Ignacio Garcia de Parada, Silvia Monteiro Da Cunha, Michele Scardone, Michiel Sweerts, Mirko Iaconisi, Baudilio Tomé Muguruza, Simon Dennett, Hannah Critoph, Daniel Costa de Magalhaes.

ЕВРОПЕЙСКА
СМЕТНА
ПАЛАТА

Служба за публикации

ЕВРОПЕЙСКА СМЕТНА ПАЛАТА
12, rue Alcide De Gasperi
1615 Luxembourg
LUXEMBOURG

Тел. +352 4398-1

За запитвания: eca.europa.eu/bg/Pages/ContactForm.aspx
Уебсайт: eca.europa.eu
Туитър: @EUAuditors