ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 24.7.2020 г.
COM(2020) 605 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, ЕВРОПЕЙСКИЯ СЪВЕТ, СЪВЕТА, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ

относно Стратегията на ЕС за Съюза на сигурност

I. Въведение

В политическите насоки на Комисията ясно се посочва, че не можем да пестим усилия, когато става въпрос за защитата на нашите граждани. Сигурността е не просто фундаментът на личната безопасност, тя също така защитава основните права и осигурява основата на доверието и динамиката в икономиката, обществото и демокрацията ни. Понастоящем европейците са изправени пред постоянно изменяща се обстановка по отношение на сигурността, повлияна от променящите се заплахи, както и от други фактори, включително от изменението на климата, демографските тенденции и политическата нестабилност отвъд нашите граници. Глобализацията, свободното движение и цифровата трансформация продължават да носят просперитет, да улесняват живота ни и да стимулират иновациите и растежа. Но тези ползи са неразривно свързани с рискове и разходи. С тях може да бъде злоупотребено с цел тероризъм, организирана престъпност, търговия с наркотици и трафик на хора — все преки заплахи за гражданите и европейския ни начин на живот. Кибератаките и киберпрестъпността продължават да се увеличават. Заплахите за сигурността стават също по-сложни: те се подхранват от способността за трансгранично действие и взаимната свързаност; възползват се от размиването на границите между физическия и цифровия свят; експлоатират уязвими групи, социални и икономически различия. Атаките могат да настъпят внезапно и да оставят малко или да не оставят никакви следи; както държавни, така и недържавни участници могат да разгръщат разнообразни хибридни заплахи[1]; случващото се извън ЕС пък може да окаже решаващо въздействие върху сигурността в рамките на ЕС.

Кризата, свързана с COVID-19, промени също така възприятието ни за заплахите за безопасността и сигурността и съответните политики. Тя изтъкна необходимостта от гарантиране на сигурността както във физическата, така и в цифровата среда. Подчерта значението на отворената стратегическа автономия за нашите вериги на доставки по отношение на продуктите, услугите, инфраструктурите и технологиите от определящо значение. Засили необходимостта от ангажиране на всеки сектор и на всеки отделен човек в общо усилие за гарантиране на това, че ЕС е изначално по-подготвен и устойчив и че при необходимост разполага с по-добри инструменти за реакция.

Гражданите не могат да бъдат защитавани единствено посредством самостоятелни действия на държавите членки. Уповаването на силните ни страни, за да работим заедно, никога не е било от по-голямо значение и ЕС никога не е разполагал с по-голям потенциал за промяна. Той може да служи за пример, като подобри цялостната си система за управление на кризи и работи както в рамките на своите граници, така и извън тях, за да допринесе за глобалната стабилност. Макар основната отговорност за сигурността да се носи от държавите членки, през последните години все повече се налага разбирането, че от сигурността на една държава членка зависи сигурността на всички. ЕС може да осигури мултидисциплинарен и интегриран отговор, като

[1] Макар определенията за хибридните заплахи да се различават, те имат за цел да обхванат комбинацията от насилнически и подривни дейности, конвенционални и неконвенционални методи (т.е. дипломатически, военни, икономически, технологични), които се използват по координиран начин от държавни или недържавни субекти с цел постигане на конкретни цели (в отсъствие на официално обявена война). Вж. JOIN(2016) 18 (final).

помогне на участниците в областта на сигурността в държавите членки с необходимите им инструменти и информация[2].

ЕС може също така да гарантира, че политиката за сигурност продължава да се основава на общите ни европейски ценности — зачитане и спазване на върховенството на закона, равенството[3] и основните права и гарантирането на прозрачност, отчетност и демократичен контрол — с цел политиките да имат правилната основа за доверие. Той може да изгради ефективен и истински Съюз на сигурност, в който правата и свободите на лицата да са добре защитени. Сигурността и зачитането на основните права не са противоречащи си цели, а са съгласувани и взаимно допълващи се. Нашите ценности и основни права трябва да залегнат в основата на политиките в областта на сигурността, като гарантират принципите на необходимост, пропорционалност и законност, и да бъдат придружени от подходящи гаранции за отчетност и осигуряване на правна защита, като същевременно дават възможност за ефективна реакция с цел защита на лицата, особено на най-уязвимите.

Вече са налице съществени правни и практически инструменти и инструменти за подкрепа, но е нужно те да бъдат едновременно подсилени и по-добре прилагани. Постигнат е значителен напредък по отношение на подобряването на обмена на информация и сътрудничеството с държавите членки в областта на разузнаването и на пресичането на възможностите за действие на терористи и престъпници. Продължава обаче да съществува фрагментиране.

Работата трябва също така да надхвърли границите на ЕС. Защитата на Съюза и неговите граждани вече не се ограничава само до гарантиране на сигурността в рамките на ЕС, а обхваща и външното измерение на сигурността. Подходът на ЕС към външната сигурност в рамките на общата външна политика и политика на сигурност (ОВППС) и общата политика за сигурност и отбрана (ОПСО) ще продължи да бъде основен елемент от усилията на ЕС за повишаване на сигурността в рамките на ЕС. Сътрудничеството с трети държави и на световно равнище за справяне с общите предизвикателства е от основно значение за ефективната и всеобхватна реакция, като стабилността и сигурността в съседните на ЕС държави са от решаващо значение за собствената сигурност на ЕС.

Като се основава на досегашната работа на Европейския парламент[4], на Съвета[5] и на Комисията[6], тази нова стратегия показва, че всеки истински и ефективен Съюз на сигурност трябва да съчетава солидна основа от инструменти и политики за постигане на сигурност на практика, като се признава, че сигурността оказва влияние върху

---

[2] Например чрез услугите, предоставяни от космическата програма на ЕС, като например „Коперник“, която осигурява данни от наблюдението на Земята, и приложенията за наблюдение на границите, морска сигурност, правоприлагане, борба с пиратството, възпиране на контрабандата на наркотици и управление на извънредни ситуации.

[3] Съюз на равенство: Стратегия за равенство между половете (2020 — 2025 г.) (COM(2020) 152).

[4] Пример за това е работата на специалната комисия относно тероризма (TERR) на Европейския парламент, която докладва през ноември 2018 г.

[5] От заключенията на Съвета от юни 2015 г. относно „обновена стратегия за вътрешна сигурност“ до по-скорошните резултати на Съвета от декември 2019 г.

[6] „Изпълнение на Европейската програма за сигурност с цел борба срещу тероризма и подготвяне на условията за ефективен и истински Съюз на сигурност“ (COM(2016) 230 final, 20.4.2016 г.). Вж. скорошната оценка на прилагането на законодателството в областта на вътрешната сигурност: Прилагане на законодателството в областта на вътрешните работи в сферата на вътрешната сигурност — 2017—2020 г. (Implementation of Home Affairs legislation in the field of internal security - 2017-2020) (SWD(2020) 135).

всички части на обществото и върху всички обществени политики. ЕС трябва да гарантира сигурна среда за всички, независимо от расовия или етническия им произход, религията, убежденията, пола, възрастта или сексуалната им ориентация.

В Стратегията е обхванат периодът 2020—2025 г. и е поставен акцент върху изграждането на способности и капацитет за осигуряване на среда на сигурност, която е подготвена за бъдещето. В нея е представен обхващащ цялото общество подход към сигурността, който позволява ефективно да се отговори на бързо променящата се картина на заплахите по съгласуван начин. Определят се стратегическите приоритети и съответните действия за интегрирано справяне с цифровите и физическите рискове в цялата екосистема на Съюза на сигурност, като се акцентира върху областите, в които ЕС може да донесе допълнителна стойност. Целта ѝ е да бъде от полза за сигурността, за да бъдат защитени всички в ЕС.

II. Бързо променяща се европейска картина на заплахите за сигурността

Безопасността, просперитетът и благосъстоянието на гражданите зависят от сигурността им. Заплахите за тази сигурност зависят от степента, в която животът и поминъкът им са уязвими. Колкото по-голяма е уязвимостта, толкова по-голям е рискът някой да се възползва от нея. Както уязвимостта, така и заплахите постоянно се изменят и ЕС трябва да се адаптира.

Ежедневието ни зависи от широк спектър от услуги — енергетика, транспорт и финанси, както и здравеопазване. Те разчитат едновременно на физическа и на цифрова инфраструктура, което допринася за уязвимостта и потенциала за смущения. По време на пандемията от COVID-19 новите технологии позволиха на много предприятия и обществени услуги да продължат да функционират, независимо дали чрез осигуряване на свързаността ни, за да вършим работата си от разстояние, или чрез поддържане на логистиката на веригите на доставки. Това обаче също така откри пътя за изключително нарастване на броя на зловредните атаки, опитващи се да използват за престъпни цели породените от пандемията смущения и преминаването към цифрова работа от дома[7]. Недостигът на стоки създаде нови възможности за организираната престъпност. Последиците можеха да бъдат фатални и да нарушат основните здравни услуги в момент, когато те бяха подложени на по-силен от всякога натиск.

Все по-многобройните начини, по които цифровите технологии улесняват живота ни, също превърнаха **киберсигурността** на технологиите във въпрос от стратегическо значение[8]. Домовете, банките, финансовите услуги и предприятията (особено малките и средните предприятия) биват сериозно засягани от кибератаките. Потенциалните вреди се умножават още повече в резултат на взаимозависимостта на физическите и цифровите системи: всяко физическо въздействие неизбежно засяга цифровите системи, а кибератаките срещу информационните системи и цифровите

[7] Европол: Отвъд пандемията. Как COVID-19 ще оформи картината на тежката и организираната престъпност в ЕС (април 2020 г.) (Europol: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU (April 2020).

[8] Препоръка на Комисията „Киберсигурност на 5G мрежите“ (C(2019) 2335); Съобщение „Сигурно внедряване на 5G в ЕС — прилагане на инструментариума на ЕС“ (COM(2020) 50).

инфраструктури могат да доведат до спиране на основни услуги[9]. Възходът на интернета на нещата и повишеното използване на изкуствения интелект ще донесат нови ползи, както и нов набор от рискове.

Светът ни се уповава на цифрови инфраструктури, технологии и онлайн системи, които ни позволяват да правим бизнес, да потребяваме продукти и да ползваме услуги. Всички те се опират на комуникацията и взаимодействието. Зависимостта от интернет благоприятства вълна от **киберпрестъпност**[10]. „Киберпрестъпността като услуга“ и сивата икономика в областта на киберпрестъпността осигуряват лесен онлайн достъп до продукти и услуги, свързани с киберпрестъпността. Престъпниците бързо се адаптират към използването на новите технологии за свои собствени цели. Подправените и фалшифицираните лекарства например проникнаха в законната мрежа на доставки на фармацевтични продукти[11]. Експоненциалното нарастване на онлайн материали, съдържащи сексуално насилие над деца[12], демонстрира социалните последици от променящите се модели на престъпността. В неотдавнашно проучване се посочва, че мнозинството от хората в ЕС (55 %) се притесняват, че до данните им могат да имат достъп престъпници и измамници[13].

Глобалната среда също допринася за засилването на тези заплахи. Решителните промишлени политики на трети държави, съчетани с продължаващите улеснявани от киберпространството кражби на интелектуална собственост, променят стратегическата парадигма за защита и постигане на напредък по отношение на европейските интереси. Това се подчертава от възхода на приложенията с двойна употреба — превръщането на един силен сектор на гражданските технологии в мощен актив за способностите в областта на отбраната и сигурността. Промишленият шпионаж оказва значително въздействие върху икономиката, заетостта и растежа в ЕС: според приблизителните оценки кибернетичните кражби на търговски тайни струват на ЕС 60 милиарда евро[14]. Това изисква задълбочено осмисляне на начина, по който зависимостите и повишеният риск от киберзаплахи засягат способността на ЕС да защитава и физическите лица, и предприятията.

Кризата, свързана с COVID-19, също така подчерта начина, по който социалните разделения и несигурност създават уязвимост за сигурността. Това увеличава

---

[9] През март 2020 г. Университетската болница в Бърно, Чехия, претърпя кибератака, довела до принудително пренасочване на пациенти и отлагане на хирургически операции (Европол: Спекула по време на пандемия. Как престъпниците използват кризата с COVID-19 (Europol: Pandemic Profiteering. How criminals exploit the COVID-19 crisis). С изкуствения интелект може да се злоупотребява с цел цифрови, политически и физически атаки, както и с цел наблюдение. Свързаното с интернет на нещата събиране на данни може да се използва за наблюдение на физически лица (интелигентни часовници, виртуални асистенти и др.).

[10] Според някои прогнози разходите, свързани с нарушения на сигурността на данните, ще нараснат от 3 трилиона щатски долара през 2015 г. на 5 трилиона щатски долара годишно през 2024 г. (Juniper Research, Бъдещето на киберпрестъпността и сигурността (The Future of Cybercrime & Security).

[11] В проучване от 2016 г. (Legiscript) се изчислява приблизително, че в световен мащаб едва 4 % от интернет аптеките функционират законно, като потребителите от ЕС са сред основните цели на незаконните аптеки, действащи онлайн, чийто брой варира между 30 000 и 35 000.

[12] Стратегия на ЕС за по-ефективна борба със сексуалното насилие над деца (COM(2020) 607).

[13] Агенция на Европейския съюз за основните права (2020 г.), Вашите права са важни: Опасения и опит в областта на сигурността, Проучване за основните права (Your rights matter: Security concerns and experiences, Fundamental Rights Survey), Люксембург, Служба за публикации.

[14] Мащабът и въздействието на промишления шпионаж и кражбата на търговски тайни чрез киберсредства (The scale and impact of industrial espionage and theft of trade secrets through cyber), 2018 г.

потенциала за по-сложни и **хибридни атаки** от страна на държавните и недържавните участници, като слабостите се използват посредством смесица от кибератаки, увреждане на критичната инфраструктура[15], кампании за дезинформация и радикализация на политическите послания.[16]

Същевременно продължават да се развиват по-отдавна установени заплахи. През 2019 г. се наблюдава низходяща тенденция при **терористичните нападения** в ЕС. Заплахата за гражданите на ЕС от джихадистки нападения, извършени или подбудени от Даиш и Ал-Кайда и техните последователи, обаче продължава да бъде висока[17]. Успоредно с това нараства и заплахата от насилнически десен екстремизъм[18]. Вдъхновените от расизъм нападения трябва да будят сериозно безпокойство: смъртоносните антисемитски терористични нападения в Хале припомниха необходимостта от засилване на ответните мерки в съответствие с декларацията на Съвета от 2018 г.[19]. Всеки пети човек в ЕС е силно притеснен от извършването на терористично нападение през следващите 12 месеца[20]. Преобладаващата част от неотдавнашните терористични нападения бяха „нискотехнологични“ — самостоятелно действащи терористи, които нападат отделни лица на обществени места, а терористичната онлайн пропаганда доби ново значение с излъчването на живо в интернет на нападенията в Крайстчърч[21]. Остава висока заплахата от радикализирани лица — потенциално усилена от завръщащите се чуждестранни бойци терористи и от освободените от затвора екстремисти[22].

Кризата също така показа как съществуващите заплахи могат да се развиват при наличието на нови обстоятелства. **Организираните престъпни** групи използват недостига на стоки, който им открива възможности за създаване на нови незаконни пазари. Търговията със забранени наркотични вещества продължава да бъде най-големият престъпен пазар в ЕС, с минимална стойност на дребно, оценявана приблизително на 30 милиарда евро годишно в ЕС[23]. Трафикът на хора продължава: приблизителните оценки сочат годишна обща печалба за всички форми на

---

[15] Критичните инфраструктури са от основно значение за жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние, чието прекъсване/унищожаване оказва значително въздействие (Директива 2008/114/ЕО на Съвета).

[16] 97 % от гражданите на ЕС са се сблъсквали с фалшиви новини, при 38 % от тях това се случва ежедневно. Вж. JOIN(2020) 8 final.

[17] 13 държави — членки на ЕС, са докладвали общо 119 извършени, неуспешни и осуетени терористични нападения с десетима убити и 27 ранени (Европол, Доклад относно ситуацията и тенденциите при тероризма в Европейския съюз, 2020 г. (European Union Terrorism Situation and Trend Report, 2020).

[18] През 2019 г. бяха отчетени шест десни терористични нападения (едно извършено, едно неуспешно, четири осуетени: три държави членки) на фона на само едно през 2018 г., като има и други загинали при случаи, които не са квалифицирани като тероризъм (Европол, 2020 г.).

[19] Вж. също Декларацията на Съвета относно борбата с антисемитизма и разработването на общ подход по отношение на сигурността за по-добра защита на еврейските общности и институции в Европа.

[20] Агенция на ЕС за основните права (2020 г.), Вашите права са важни: Опасения и опит в областта на сигурността, (Your rights matter: Security concerns and experiences).

[21] В периода между юли 2015 г. и края на 2019 г. Европол откри терористично съдържание на 361 платформи (Европол, 2020 г.).

[22] Европол: Преглед на най-добрите трансатлантически практики за противодействие на радикализацията в затворите и терористичните рецидиви, 2019 г. (Europol: A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism, 2019).

[23] Доклад на ЕЦМНН и Европол за пазарите на наркотици в ЕС за 2019 г.

експлоатация от почти 30 милиарда евро[24]. Международната търговия с фалшифицирани фармацевтични продукти достигна 38,9 милиарда евро[25]. Същевременно ниският процент на конфискация позволява на престъпниците да продължават да разширяват престъпните си дейности и да проникват в законната икономика[26]. С помощта на онлайн пазара и новите технологии, като например триизмерния печат, престъпниците и терористите по-лесно получават достъп до огнестрелни оръжия[27]. Използването на изкуствен интелект, нови технологии и роботика допълнително ще увеличи риска от това престъпниците да се възползват от предимствата на иновациите за злонамерени цели.[28]

Тези заплахи обхващат множество категории и засягат по разнообразни начини различни части на обществото. Всички те представляват сериозна заплаха за физическите лица и предприятията и изискват цялостен и съгласуван отговор на равнището на ЕС. Когато слабостите по отношение на сигурността могат да дойдат дори от малки взаимосвързани домакински уреди, като например свързани с интернет хладилник или кафе машина, вече не можем да разчитаме единствено на традиционните държавни субекти за гарантирането на сигурността ни. Стопанските субекти трябва да поемат по-голяма отговорност за киберсигурността на продуктите и услугите, които пускат на пазара; същевременно е нужно и отделните лица също да имат поне основно разбиране за киберсигурността, за да могат да се защитават сами.

III. Координирана реакция на равнище ЕС за цялото общество

ЕС вече е показвал как може да постига истинска добавена стойност. От 2015 г. насам Съюзът на сигурността създаде нови връзки в начина, по който политиките в областта на сигурността се третират на равнището на ЕС. Необходимо е обаче да се направи повече, за да се ангажира цялото общество, като се включат управленските структури на всички равнища, предприятията във всички отрасли на икономиката и отделните лица във всички държави членки. Повишаването на осведомеността относно рисковете от зависимост[29] и необходимостта от силна европейска промишлена стратегия[30] насочват към ЕС с критична маса на промишленото и технологичното производство и устойчивост на веригите на доставки. Да бъдем силни означава също и пълно зачитане на основните права и ценностите на ЕС: те са предпоставка за легитимни, ефективни и устойчиви политики в областта на сигурността. В тази

[24] Доклад на Европол от 2015 г. относно финансовия бизнес модел на трафика на хора (Europol's Report on Trafficking in Human Beings, Financial Business Model (2015).

[25] Доклад на Службата на ЕС за интелектуална собственост и на ОИСР относно Търговията с фалшифицирани фармацевтични продукти.

[26] Доклад „Възстановяване и конфискация на активи: да гарантираме, че престъпността „не си струва“ (COM(2020) 217).

[27] През 2017 г. в 41 % от всички терористични нападения са били използвани огнестрелни оръжия (Европол, 2018 г.).

[28] През юли 2020 г. правоприлагащи и съдебни органи от Франция и Нидерландия, заедно с Европол и Евроюст, представиха съвместно разследване за разбиване на EncroChat — криптирана телефонна мрежа, използвана от престъпните мрежи, занимаващи се със съпроводени с насилие нападения, корупция, опити за убийства и транспортиране на наркотици в големи мащаби.

[29] Рисковете от чужда зависимост включват повишена изложеност на потенциални заплахи — от използването на уязвимости на ИТ инфраструктурите, с което могат да се компрометират критични инфраструктури (напр. енергетика, транспорт, банкиране, здравеопазване), или поемане на контрол върху системи за управление на индустриални процеси, до увеличен капацитет за кражби на данни или шпионаж.

[30] Съобщение на Комисията „Нова промишлена стратегия за Европа“ (COM(2020) 102).

стратегия на Съюза на сигурност се определят конкретни работни направления за по-нататъшни действия. Тя се основава на следните общи цели:

- ***Изграждане на способности и капацитет за ранно откриване, предотвратяване и бърза реакция при кризи:*** Нужно е Европа да бъде по-устойчива, за да може да предотвратява бъдещи сътресения, да бъде защитена спрямо тях и да им устоява. Трябва да изградим способности и капацитет за ранно откриване и бърза реакция на свързани със сигурността кризи чрез интегриран и координиран подход както в световен мащаб, така и чрез специфични за съответния сектор инициативи (напр. за финансовия, енергийния, съдебния сектор, секторите на правоприлагането, здравеопазването, морския транспорт, транспорта), да доразвиваме съществуващите инструменти и инициативи[31]. Комисията също така ще представи предложения за широкообхватна система за управление на кризи в рамките на ЕС, която би могла да бъде от значение и за сигурността.

- ***Акцент върху резултатите***: Всяка ориентирана към резултатите стратегия трябва да се основава на внимателна оценка на заплахите и рисковете с цел насочване на усилията ни към постигане на най-добри резултати. Необходимо е в нея да се определят и приложат подходящите правила и правилните инструменти. Тя се нуждае от надеждно стратегическо разузнаване като основа за политиките на ЕС в областта на сигурността. Когато е необходимо приемането на законодателство на ЕС, то трябва да бъде последвано от нужните мерки за цялостното му прилагане, за да се избегнат фрагментирането и оставянето на вратички, които да бъдат използвани. Ефективното изпълнение на тази стратегия ще зависи и от осигуряването на подходящо финансиране през следващия програмен период 2021—2027 г., в това число и за свързаните с нея агенции на ЕС.

- ***Приобщаване на всички участници в публичния и частния сектор за полагането на общи усилия:*** Ключовите участници и от публичния, и от частния сектор не са склонни да споделят информация, свързана със сигурността, независимо дали от страх да не се изложи на риск националната сигурност, или конкурентоспособността.[32] Най-ефективни сме обаче, когато всички се подкрепят взаимно. На първо място това означава по-засилено сътрудничество между държавите членки, с участието на правоприлагащите, съдебните и други публични органи и на институциите и агенциите на ЕС, като целта е изграждането на разбиране и обмен, необходими за намирането на общи решения. Сътрудничеството с частния сектор също е от основно значение, още повече като се има предвид, че промишлеността притежава важна част от цифровата и нецифровата инфраструктура, която е от основно значение за ефективната борба с престъпността и тероризма. Отделните граждани също могат да дадат своя принос, например чрез придобиване на умения и осведоменост, за да противодействат на киберпрестъпността или дезинформацията. И накрая, тези

[31] Като например интегрираните договорености за реакция на политическо равнище при кризи (IPCR), Координационния център за реагиране при извънредни ситуации, препоръката на Комисията относно координирана реакция на мащабни киберинциденти и кризи (C(2017) 6100), оперативния протокол на ЕС за борба с хибридните заплахи („EU Playbook“) (SWD(2016) 227).

[32] Вж. съвместното съобщение „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“ (JOIN(2017) 450).

общи усилия трябва да надхвърлят границите ни, за да изградим по-тесни връзки с партньорите със сходни възгледи.

IV. Защита на всички в ЕС: Стратегически приоритети за Съюза на сигурност

ЕС е в уникална благоприятна позиция да даде отговор на тези нови глобални заплахи и предизвикателства. В направения по-горе анализ на заплахите се посочват четири взаимосвързани стратегически приоритета, по които трябва се постигне напредък на равнището на ЕС, при пълно зачитане на основните права: i) среда на сигурност, която е подготвена за бъдещето, ii) справяне с променящите се заплахи, iii) защита на европейците от тероризма и организираната престъпност, iv) силна европейска екосистема на сигурността.

1. Среда на сигурност, която е подготвена за бъдещето

Защита и устойчивост на критичната инфраструктура

В своето ежедневие лицата разчитат на ключови инфраструктури, за да пътуват, работят, ползват основни обществени услуги като болници, транспорт, енергийни доставки или да упражняват своите демократични права. Ако тези инфраструктури не са достатъчно защитени и устойчиви, атаките могат да предизвикат огромни смущения — както физически, така и цифрови — в отделните държави членки и потенциално в целия ЕС.

Съществуващата рамка на ЕС за защита и устойчивост на критичните инфраструктури[33] не е в синхрон с променящите се рискове. Увеличаването на взаимозависимостта означава, че сътресенията в отделен сектор могат да имат непосредствено въздействие върху дейностите в други сектори: атака срещу производството на електроенергия би могла да спре функционирането на телекомуникации, болници, банки или летища, а атака срещу цифрова инфраструктура би могла да доведе до сътресения в електрическите или финансовите мрежи. Тъй като икономиката и обществото ни все повече се изместват в онлайн пространството, рискове като тези стават все по-осезаеми. Законодателната рамка трябва да отговори на тази нарастваща взаимосвързаност и взаимозависимост със солидни мерки за защита и устойчивост на критичната инфраструктура, както по отношение на киберпространството, така и физически. Основните услуги, включително основаващите се на космическа инфраструктура, трябва да бъдат подходящо защитени от настоящи и очаквани заплахи, но същевременно да бъдат и устойчиви. Това включва способността на дадена система да се подготвя и планира, да поема, да се възстановява и да се адаптира по-успешно към нежелани събития.

Същевременно държавите членки са упражнили правото си на преценка, като са приложили съществуващото законодателство по различни начини. Произтичащата от това разпокъсаност може да подкопае вътрешния пазар и да затрудни трансграничната координация — най-очевидно в граничните региони. Операторите, предоставящи основни услуги в различни държави членки, трябва да спазват различни режими на

[33] Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г.); Директива 2008/114/ЕО на Съвета относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита.

отчитане. Комисията проучва дали **новите рамки за физическите и за цифровите инфраструктури** биха могли да доведат до по-голяма последователност и по-съгласуван подход, за да се гарантира надеждното предоставяне на основни услуги. Тази рамка трябва да бъде придружена от **специфични за сектора инициативи** с цел справяне с определени рискове, пред които са изправени критичните инфраструктури, като например в областта на транспорта, космическото пространство, енергетиката, финансите и здравеопазването[34]. Като се имат предвид силната зависимост на финансовия сектор от ИТ услугите и високата му уязвимост към кибератаки, първата стъпка ще бъде инициатива относно цифровата оперативна устойчивост на финансовите сектори. Поради особената чувствителност и въздействието на енергийната система специална инициатива ще спомогне за укрепването на устойчивостта на критичната енергийна инфраструктура срещу физически, кибернетични и хибридни заплахи, като гарантира еднакви условия на конкуренция за енергийните оператори отвъд националните граници.

Свързаните със сигурността последици от преките чуждестранни инвестиции, които биха могли да засегнат критични инфраструктури или технологии, също ще бъдат предмет на оценките, извършвани от държавите — членки на ЕС, и Комисията в рамките на новата европейска рамка за скрининг на преките чуждестранни инвестиции[35].

ЕС може също така да създаде нови инструменти за подпомагане на устойчивостта на критичните инфраструктури. Засега световният интернет показва висока степен на устойчивост, по-специално по отношение на способността да поддържа увеличен обем на трафика. Необходимо е обаче да бъдем подготвени за евентуални бъдещи кризи, застрашаващи сигурността, стабилността и устойчивостта на интернет. Осигуряването на функционирането на интернет означава предприемането на убедителни мерки срещу киберинциденти и злонамерени онлайн дейности, както и ограничаването на зависимостта от инфраструктура и услуги, намиращи се извън Европа. Това ще изисква комбинация от законодателни мерки и преглед на съществуващите правила, за да се гарантира високо общо ниво на сигурност на мрежовите и информационните системи в ЕС; повишаване на инвестициите в научни изследвания и иновации; и търсене на начини за внедряване или укрепване на основни интернет инфраструктури и ресурси, по-специално системата за имена на домейни[36].

Важен елемент за защита на ключовите европейски и национални цифрови активи е да може да се предложи канал за сигурни комуникации за критичната

[34] Като се има предвид, че секторът на здравеопазването беше подложен на натиск, особено по време на кризата, свързана с COVID-19, Комисията ще обмисля също така инициативи за укрепване на рамката на ЕС в областта на здравната сигурност и на отговорните агенции на ЕС, за да се реагира на сериозните трансгранични заплахи за здравето.

[35] С пълното си влизане в сила на 11 октомври 2020 г. Регламент (ЕС) 2019/452 на Европейския парламент и на Съвета от 19 март 2019 г. за създаване на рамка за скрининг на преки чуждестранни инвестиции в Съюза ще предостави на ЕС нов механизъм за сътрудничество в областта на преките инвестиции от държави извън ЕС, за които инвестиции има вероятност да засегнат сигурността или обществения ред. Съгласно Регламента държавите членки и Комисията ще правят оценка на потенциалните рискове, свързани с такива ПЧИ, и когато е целесъобразно и от значение за повече от една държава членка, ще предлагат подходящи средства за смекчаване на такива рискове.

[36] Система за имена на домейни (DNS) представлява йерархична и децентрализирана система за именуване на компютри, услуги или други ресурси, свързани към интернет или частни мрежи. Тя преобразува имена на домейни в IP адреси, необходими за локализиране и идентифициране на компютърни услуги и устройства.

инфраструктура. Комисията работи с държавите членки за въвеждането на сертифицирана напълно защитена откраи докрай основана на квантовите технологии инфраструктура, наземна и базирана в космоса, в съчетание със сигурната правителствена сателитна система за комуникация, определена в Регламента за космическата програма[37].

Киберсигурност

Броят на кибератаките продължава да расте[38]. Тези атаки са по-сложни от всякога, произлизат от широк кръг източници в ЕС и извън него и са насочени към области с максимална уязвимост. Често се включват държавни или подкрепяни от държавата участници, които атакуват ключови цифрови инфраструктури, като например основните доставчици на услуги „в облак“[39]. Кибернетичните рискове също се превръщат в сериозна заплаха за финансовата система. Международният валутен фонд оценява годишните загуби, дължащи се на кибератаки, на 9 % от нетните приходи на банките в световен мащаб, или на около 100 милиарда щатски долара.[40] Преминаването към свързани устройства ще донесе големи ползи за потребителите: но с по-малко данни, съхранявани и обработвани в центрове за обработка на данни, и повече данни, обработвани по-близо до потребителите, „в периферията“[41], съсредоточаването на киберсигурността върху защитата на централните звена вече няма да е възможно[42].

През 2017 г. ЕС предложи подход към киберсигурността, в чиято основа стои изграждането на устойчивост, бързото реагиране и ефективното възпиране[43]. Сега ЕС трябва да гарантира, че неговите способности в областта на киберсигурността отговарят на предизвикателствата на действителността, за да се постигне както устойчивост, така и реакция в тази област. Това изисква подход, който действително обхваща цялото общество и при който институциите, агенциите и органите на ЕС, държавите членки, промишлеността, академичните среди и физическите лица отдават на киберсигурността дължимия приоритет[44]. Този хоризонтален подход трябва да бъде допълнен от специфични за сектора подходи за киберсигурност в области като енергетика, финансови услуги, транспорт или здравеопазване. Следващата фаза на работата на ЕС следва да бъде очертана в една преразгледана Европейска стратегия за киберсигурност.

---

37 Предложение за регламент за създаване на космическа програма на Съюза и на Агенция на Европейския съюз за космическата програма COM(2018) 447.

38 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

39 Разпределените атаки тип „отказ от обслужване“ (DDoS атаки) продължават да бъдат постоянна заплаха: през февруари 2020 г. основните доставчици трябваше да се справят с масови DDoS атаки, като например атака срещу уеб услугите на Amazon.

40 https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

41 Периферните изчисления (edge computing) са разпределена, отворена ИТ архитектура, която се характеризира с децентрализирана изчислителна мощност, която захранва мобилните компютърни технологии и технологиите за „интернет на нещата“ (IoT). В рамките на периферните изчисления данните се обработват от самото устройство или от местен компютър или сървър, а не се предават в център за данни.

42 Съобщение относно европейска стратегия за данните, COM(2020) 66 final.

43 Съвместно съобщение „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“, JOIN (2017) 450.

44 В доклада „Cybersecurity — our digital Anchor“ на Съвместния изследователски център се представя многостранен поглед върху растежа на киберсигурността през последните 40 години.

Разглеждането на нови и подобрени форми на сътрудничество между разузнавателните служби, INTCEN и други организации, работещи в областта на сигурността, следва да бъде част от усилията за укрепване на киберсигурността, както и за борба с тероризма, екстремизма, радикализма и хибридните заплахи.

Предвид въвеждането в момента на територията на ЕС на **инфраструктурата за 5G** и потенциалната зависимост на много от критичните услуги от 5G мрежите, последиците от системни и широкообхватни прекъсвания на услугите биха били особено сериозни. Процесът, въведен с Препоръката на Комисията от 2019 г. относно киберсигурността на 5G мрежите[45], вече доведе до конкретни действия от страна на държавите членки по отношение на ключовите мерки, изложени в набора от инструменти за 5G[46].

Една от най-важните дългосрочни нужди е разработването на култура на **киберсигурност още при проектирането,** в която сигурността е вградена в продуктите и услугите от самото начало. Важен принос за това ще бъде новата рамка за сертифициране на киберсигурността съгласно Акта за киберсигурността[47]. Рамката вече е в ход, с две схеми за сертифициране, които вече са в процес на изготвяне, а приоритетите за следващи схеми ще бъдат определени по-късно тази година. Сътрудничеството между Агенцията на ЕС за киберсигурност (ENISA), органите за защита на данните и Европейския комитет по защита на данните[48] е от ключово значение в тази област.

Комисията вече установи, че е необходимо **съвместно киберзвено,** което да предоставя структурирано и координирано сътрудничество. Това би могло да включва механизъм за взаимопомощ по време на криза на равнище ЕС. Въз основа на изпълнението на Препоръката относно концепцията[49] съвместното киберзвено би могло да изгради доверие между различните участници в европейската екосистема на киберсигурността и да предложи ключова услуга на държавите членки. Комисията ще започне обсъждания със съответните заинтересовани страни (като се започне с държавите членки) и ще определи ясен процес, етапи и график до края на 2020 г.

Важни са също така общите правила относно сигурността на информацията и киберсигурността за всички институции, органи и агенции на ЕС. Целта следва да бъде създаването на задължителни и високи общи стандарти за сигурен обмен на информация и сигурност на цифровите инфраструктури и системи във всички институции, органи и агенции на ЕС. Тази нова рамка следва да бъде в основата на силно и ефикасно оперативно сътрудничество в областта на киберсигурността в институциите, органите и агенциите на ЕС, с акцент върху ролята на екипа за незабавно реагиране при компютърни инциденти (CERT-EU) за институциите, органите и агенциите на ЕС.

---

[45] Препоръка на Комисията относно киберсигурността на 5G мрежите, COM(2019) 2335 final. В препоръката се предвижда нейното преразглеждане през последното тримесечие на 2020 г.

[46] Вж. доклада от 24 юли 2020 г. на групата за сътрудничество по въпросите на МИС относно изпълнението на набора от инструменти.

[47] Регламент (ЕС) 2019/881 относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“).

[48] Съобщение относно защитата на данните като стълб на оправомощаването на гражданите и на подхода на ЕС по отношение на цифровия преход — две години от прилагането на Общия регламент относно защитата на данните, COM(2020) 264.

[49] Препоръка 2017/1584 на Комисията относно координирана реакция на мащабни киберинциденти и кризи.

Предвид глобалния си характер, изграждането и поддържането на солидни **международни партньорства** е от основно значение за по-нататъшно предотвратяване, възпиране и реагиране на кибератаки. Рамката за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството („инструментариум за кибердипломация“)[50] определя мерки в рамките на общата външна политика и политика на сигурност, включително ограничителни мерки (санкции), които могат да бъдат използвани срещу дейности, които вредят на неговите политически и икономически интереси, както и интереси в областта на сигурността. ЕС следва също така да задълбочи работата си чрез фондовете за развитие и сътрудничество, за да се осигури изграждането на капацитет в подкрепа на държавите партньори за укрепване на техните цифрови екосистеми, за приемане на национални законодателни реформи и спазване на международните стандарти. Това повишава устойчивостта на цялата общност и нейната способност за противодействие и ефективно реагиране на киберзаплахи. Това включва специална работа за повишаване на осведомеността относно стандартите на ЕС и съответното законодателство за повишаване на киберсигурността в съседните на Съюза държави партньори[51].

Защита на обществените пространства

Неотдавнашните терористични нападения бяха насочени към **обществени пространства**, включително места за богослужение и транспортни центрове, като бе използван техният отворен и достъпен характер. Възходът на тероризма, предизвикан от политически или идеологически мотивиран екстремизъм, направи тази заплаха още по-остра. Това налага както по-строга физическа защита на такива места, така и подходящи системи за откриване, без да се накърняват свободите на гражданите[52]. Комисията ще засили публично-частното сътрудничество за защита на обществените пространства, с финансиране, обмен на опит и добри практики, конкретни насоки[53] и препоръки.[54] Част от подхода ще бъдат също повишаването на осведомеността, изискванията за ефективност и изпитването на оборудването за откриване, както и засилването на проверките на работното място с цел справяне с вътрешните заплахи. Важен аспект, който трябва да бъде взет предвид, е фактът, че малцинствата и уязвимите лица могат да бъдат непропорционално засегнати, включително лицата, които представляват цели, поради тяхната религия или пол, и поради това се нуждаят от специално внимание. Регионалните и местните публични органи играят важна роля за подобряване на сигурността на обществените пространства. Комисията също така помага за насърчаване на иновациите на градовете в областта на сигурността на обществените пространства[55]. Стартирането през ноември 2018 г. на ново

[50] http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/bg/pdf

[51] Вж. Насоките за изграждане на външен киберкапацитет на ЕС, приети в заключенията на Съвета от 26 юни 2018 г.

[52] Системите за биометрична идентификация от разстояние заслужават специално внимание. Първоначалните възгледи на Комисията са изложени в Бялата книга на Комисията от 19 февруари 2020 г. относно изкуствения интелект, COM (2020) 65.

[53] Например Насоките за избор на подходящи обезопасяващи бариери за защита на общественото пространство (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] Насоки за добри практики са дадени в SWD (2019) 140, включително раздел относно публично-частното сътрудничество. Финансирането по линия на фонд „Вътрешна сигурност“ (ФВС — Полиция) отделя специално внимание на засилването на публично-частното сътрудничество.

[55] Три града (Пирея в Гърция, Тампере във Финландия и Торино в Италия) ще изпробват нови решения като част от иновативните дейности за градско развитие, съфинансирани от Европейския фонд за регионално развитие (ЕФРР).

партньорство за Програма за градовете[56] в областта на „сигурността в обществените пространства“ отразява силния ангажимент на държавите членки, Комисията и градовете за по-добро справяне със заплахите за сигурността в градското пространство.

Пазарът на **дронове** продължава да се разраства, като тези устройства разполагат с много на брой ценни и законни начини на употреба. Те обаче имат и потенциал да бъдат използвани неправомерно от престъпници и терористи, като обществените пространства са особено застрашени от подобна употреба. Целите могат да включват отделни индивиди, събирания на хора, критична инфраструктура, правоприлагащи органи, граници или обществени пространства. Познанията относно употребата на дронове в ситуации на конфликт могат да се върнат обратно в Европа или директно (чрез връщане на чуждестранни бойци терористи), или онлайн. Правилата, които вече са разработени от Европейската агенция за авиационна безопасност, са важна първа стъпка в области като регистрацията на оператори на дронове и задължителното дистанционно идентифициране на дронове. Тъй като дроновете стават все по-широко достъпни, по-евтини и по-способни, се наблюдава необходимост от допълнителни действия. Те могат да включват обмен на информация, насоки и добри практики, които да се използват от всички участници, включително органите за правоприлагане, както и повече изпитвания на мерки за противодействие на дронове.[57] Освен това следва допълнително да се анализират и разгледат последиците за неприкосновеността на личния живот и защитата на данните при използването на дронове на обществени места.

Ключови действия
• Законодателство относно защитата и устойчивостта на критичната инфраструктура • Преразглеждане на Директивата за сигурност на мрежите и информационните системи • Инициатива за оперативната устойчивост на финансовия сектор • Защита и киберсигурност на критичната енергийна инфраструктура и мрежов кодекс за киберсигурност за трансграничния пренос на електроенергия • Европейска стратегия за киберсигурност • Следващи стъпки към създаването на съвместно киберзвено • Общи правила относно сигурността на информацията и киберсигурността за институциите, органите и агенциите на ЕС. • Засилване на сътрудничеството в областта на защитата на обществените пространства, включително на местата за богослужение • Обмен на най-добри практики във връзка със злоупотребата с дронове

[56] Програмата на ЕС за градовете представлява нов многостепенен работен метод, който насърчава сътрудничеството между държавите членки, градовете, Европейската комисия и други заинтересовани страни с цел стимулиране на растежа, качеството на живот и иновациите в европейските градове, както и идентифициране и успешно справяне със социалните предизвикателства.

[57] Наскоро беше създадена многогодишна програма за изпитвания с цел подпомагане на държавите членки при разработването на обща методология и платформа за изпитвания в тази област.

2. Справяне с променящите се заплахи

Киберпрестъпност

Технологиите създават нови възможности за обществото. Те също така предлагат нови инструменти за съдебната система и за правоприлагането. Но в същото време технологиите отварят врати за престъпниците. Зловредният софтуер, кражбата на лични или търговски данни чрез хакерски атаки, както и прекъсването на цифровите дейности, причиняващо финансови щети или накърняване на репутацията, се увеличават. Първата линия на отбрана е създаването на устойчива среда, характеризираща се със силна киберсигурност. Правоприлагащите органи трябва да могат да работят в сферата на цифровите разследвания с ясни правила за разследване и наказателно преследване на престъпления и предоставяне на необходимата защита на жертвите. Тази дейност следва да се основава на извършеното от съвместната работна група за действие в областта на киберпрестъпността в Европол и на протокола за реагиране при извънредни ситуации в областта на правоприлагането, създаден с цел координиране на реакцията при широкомащабни кибератаки. Ефективните механизми, позволяващи публично-частни партньорства и сътрудничество, също са от ключово значение.

Успоредно с това борбата с киберпрестъпността следва да се превърне в стратегически комуникационен приоритет в целия ЕС, за да могат европейците да са в течение за рисковете и превантивните мерки, които сами биха могли да предприемат. Това следва да бъде част от един проактивен подход. Важна стъпка е и пълното прилагане на настоящата правна рамка[58]: Комисията ще бъде готова да използва процедури за установяване на неизпълнение на задължения, когато е целесъобразно, както и да преразгледа тази рамка, за да гарантира, че тя продължава да отговаря на поставените цели. Освен това Комисията ще проучи, съвместно с Европол и Агенцията на ЕС за киберсигурност, възможността за създаване на система на ЕС за бързо предупреждение, свързана с киберпрестъпността, която би могла да осигури обмен на информация и бързи реакции при рязко увеличаване на киберпрестъпленията.

Киберпрестъпността е глобално предизвикателство, за което е необходимо ефективно международно сътрудничество. ЕС подкрепя Будапещенската конвенция на Съвета на Европа за престъпления в кибернетичното пространство, която е ефективен и добре установен модел, който позволява на всички държави да определят кои системи и канали за комуникация е необходимо да въведат, за да могат да работят ефективно помежду си.

Почти половината от гражданите на ЕС се тревожат по въпроса за злоупотребата с данни[59], а **кражбата на самоличност** буди сериозно безпокойство[60]. Използването с измамна цел на самоличността с цел получаване на финансова облага е само един от

---

[58] Директива 2013/40/ЕС относно атаките срещу информационните системи.

[59] 46 % (проучване на Евробарометър за отношението на европейците към киберсигурността, януари 2020 г.).

[60] В огромната си част респондентите в проучването на Евробарометър от 2018 г. „ Отношение на европейците към сигурността на интернет“ (95 %) смятат кражбата на самоличност за тежко престъпление, а седем от десет твърдят, че това е много тежко престъпление. В проучването на Евробарометър от януари 2020 г. бяха потвърдени опасенията във връзка с киберпрестъпността, онлайн измамите и кражбата на самоличност: две трети от респондентите са загрижени за банковата измама (67 %) или кражбата на самоличност (66 %).

неговите аспекти, но това престъпление може да има и голямо лично и психологическо въздействие, като например незаконно качени материали в интернет от крадеца на самоличност могат да останат онлайн с години. Комисията ще проучи възможните практически мерки за защита на жертвите срещу всички форми на кражба на самоличност, като вземе предвид предстоящата европейска инициатива за цифрова идентичност[61].

Борба с киберпрестъпността означава да гледаме напред. Така като обществото използва нови технологични разработки за укрепване на икономиката и обществото, престъпниците също могат да се стремят да използват тези инструменти за постигане на отрицателни цели. Например престъпниците могат да използват изкуствен интелект за откриване и идентифициране на пароли или за опростяване на създаването на зловреден софтуер, както и да злоупотребяват с изображения и звук, които след това могат да бъдат използвани за кражба на самоличност или измама.

Съвременно правоприлагане

Правоприлагащите органи и практикуващите юристи трябва да се адаптират към новите технологии. Технологичното развитие и възникващите заплахи изискват правоприлагащите органи да имат достъп до нови инструменти, да придобият нови умения и да разработят алтернативни техники за разследване. За да се допълнят законодателните действия, насочени към подобряване на трансграничния достъп до електронни доказателства за наказателни разследвания, ЕС може да помогне на правоприлагащите органи да развият необходимия капацитет за идентифициране, осигуряване и разчитане на данните, необходими за разследване на престъпления, и за използване на тези данни като доказателство в съда. Комисията ще проучи мерки за **увеличаване на капацитета на правоприлагащите органи в областта на цифровите разследвания**, като ще определи как да се използват по най-добрия начин научните изследвания и разработки, за да се създадат нови инструменти за правоприлагащите органи; и как обучението може да предложи подходящите умения за правоприлагащите органи и съдебната система. Това включва и предоставянето на строги научни оценки и методи за изпитване чрез Съвместния изследователски център на Комисията.

Общите подходи могат също така да гарантират, че **изкуственият интелект, космическите способности, големите информационни масиви** и **високопроизводителните изчислителни технологии са интегрирани** в политиката за сигурност по начин, който е ефективен както в борбата с престъпленията, така и при гарантирането на основните права. Изкуственият интелект би могъл да действа като мощен инструмент за борба с престъпността, създавайки огромни способности за разследване чрез анализ на големи количества информация и разпознаване на модели и аномалии[62]. Той може също така да предостави конкретни инструменти, като например да подпомогне идентифицирането на терористично съдържание онлайн, да разкрие подозрителни трансакции при продажбата на опасни продукти или да предложи помощ на гражданите при извънредни ситуации. Реализирането на този потенциал означава събиране на научните изследвания, иновациите и потребителите на изкуствения интелект с правилното управление и техническа инфраструктура, с активното участие на частния сектор и академичните среди. Това означава също така

[61] Съобщение от 19 февруари 2020 г. относно изграждане на цифровото бъдеще на Европа, COM(2020) 67.

[62] Например при финансови престъпления.

да се гарантират най-високите стандарти за спазване на основните права, като същевременно се гарантира ефективна защита на гражданите. По-специално решенията, които оказват въздействие върху отделни лица, трябва да бъдат подложени на преглед от човек и да са в съответствие с приложимото законодателство на ЕС в тази област[63].

В около 85 % от разследванията на тежки престъпления са необходими електронна информация и доказателства, а 65 % от общия брой на исканията се изпращат до доставчици, намиращи се в друга юрисдикция[64]. Фактът, че традиционните физически следи са се преместили онлайн, разширява допълнително разликата между капацитета на правоприлагащите органи и този на престъпниците. Въвеждането на ясни правила за трансграничен достъп до електронни доказателства за наказателни разследвания е от съществено значение. Ето защо бързото приемане от Европейския парламент и Съвета на предложенията за електронните доказателства е от ключово значение за предоставянето на ефективен инструментариум на практикуващите специалисти. Трансграничният достъп до електронни доказателства чрез многостранни и двустранни международни преговори също е от ключово значение за установяването на съвместими правила на международно равнище[65].

Достъпът до цифрови доказателства зависи и от наличието на информация. Ако данните се заличават твърде бързо, важни доказателства могат да изчезнат, така че вече да не съществува възможност за идентифициране и намиране на местонахождението на заподозрени лица и престъпни мрежи (както и на жертви). От друга страна, схемите за запазване на данни повдигат въпроси относно защитата на неприкосновеността на личния живот. В зависимост от изхода на висящите дела пред Съда на Европейския съюз Комисията ще прецени какви по-нататъшни действия да предприеме във връзка със запазването на данни.

Достъпът до информация за регистрацията на име на домейн онлайн („данни WHOIS“)[66] е важен за наказателните разследвания, киберсигурността и защитата на потребителите. Достъпът до тази информация става все по-труден, докато се чака приемането на нова политика за WHOIS данните от Интернет корпорацията за присвоени имена и адреси (ICANN). Комисията ще продължи да работи с ICANN и с общността от заинтересовани страни, за да се гарантира, че участниците, законно търсещи достъп, включително правоприлагащите органи, могат да получат ефективен достъп до данните WHOIS в съответствие с европейските и международните разпоредби за защита на данните. Това ще включва оценка на възможните решения, включително дали може да е необходимо законодателство за изясняване на правилата за достъп до такава информация.

Правоприлагащите и съдебните органи също трябва да разполагат с необходимото оборудване, за да се сдобиват с необходимите данни и доказателства, след като **5G**

---

[63] Това означава съответствие със съществуващото законодателство, включително с Общия регламент (ЕС) 2016/679 относно защитата на данните, както и с Директива (ЕС) 2016/680 относно правоприлагането в областта на защитата на данните, която регулира обработването на лични данни за целите на откриване, предотвратяване, разследване и наказателно преследване на престъпления или изпълнението на наказания.

[64] COM SWD(2018) 118 final.

[65] По-специално, вторият допълнителен протокол към Конвенцията от Будапеща на Съвета на Европа за престъпления в кибернетичното пространство и споразумение между ЕС и Съединените щати относно трансграничния достъп до електронни доказателства.

[66] Съхранявани в бази данни, поддържани от 2 500 регистрационни оператори, базирани в цял свят.

инфраструктурата за мобилните далекосъобщения се внедри изцяло в ЕС по начин, който зачита поверителността на съобщенията. Комисията ще подкрепи един засилен и координиран подход при изграждането на международни стандарти, определянето на най-добрите практики, процеси и техническата оперативна съвместимост в ключови технологични области като ИИ, „интернет на нещата“ или блокчейн технологиите.

Днес значителна част от разследванията срещу всички форми на престъпност и тероризъм включват **криптирана информация**. Криптирането е от съществено значение за цифровия свят, като гарантира сигурността на цифровите системи и трансакциите и защитава редица основни права, включително свободата на изразяване, неприкосновеността на личния живот и защитата на данните. Въпреки това, ако се използва за престъпни цели, криптирането може също да маскира самоличността на престъпниците и да скрие съдържанието на комуникациите им. Комисията ще проучи и подкрепи балансирани технически, оперативни и правни решения за справяне с предизвикателствата и ще насърчава подход, който запазва ефективността на криптирането за защитата на неприкосновеността на личния живот и на сигурността на комуникациите, като същевременно осигурява ефективен отговор на престъпността и тероризма.

Борба с незаконното съдържание онлайн

Сближаването на онлайн сигурността и тази във физическата среда означава продължаване на действията за **противодействие на незаконното съдържание онлайн**. Все по-често основни заплахи за гражданите, като тероризъм, екстремизъм или сексуално насилие над деца, разчитат на цифровата среда: това изисква конкретни действия и рамка за гарантиране на зачитането на основните права. Важна първа стъпка е бързото приключване на преговорите по предложеното законодателство относно терористичното съдържание онлайн[67] и гарантирането на неговото изпълнение. Засилването на доброволното сътрудничество между правоприлагащите органи и частния сектор в **интернет форума на ЕС** също е от ключово значение за борбата със злоупотребата с интернет от страна на терористи, екстремисти и престъпници. Звеното на ЕС за сигнализиране за незаконно съдържание в интернет в Европол ще продължи да играе ключова роля за наблюдението на дейността на терористичните групи онлайн и за действията, предприети от платформите[68], както и за по-нататъшното разработване на **Протокола на ЕС за действие при кризи**[69]**.** Освен това Комисията ще продължи да работи с международни партньори, включително чрез участие в **Световния интернет форум за борба с тероризма**, за да се справи с тези предизвикателства на световно равнище. Ще продължи работата в подкрепа на разработването на алтернативни и противоположни послания чрез Програмата за овластяване на гражданското общество[70].

За да се предотврати и противодейства на разпространението на незаконните изказвания онлайн, пораждащи омраза, през 2016 г. Комисията стартира „Кодекс на поведение във връзка с незаконните изказвания онлайн, пораждащи омраза“, с

---

[67] Предложение за предотвратяване на разпространението на терористично съдържание онлайн, COM(2018) 640, 12 септември 2018 г.

[68] Европол, ноември 2019 г.

[69] „Европа, която закриля — Протокол на ЕС за действие при кризи: реагиране на терористично съдържание онлайн“ (октомври 2019 г.).

[70] Във връзка с работата на Програмата за осведоменост по въпросите на радикализацията вж. раздел IV.3 по-долу.

доброволен ангажимент от страна на онлайн платформите да премахват съдържание, включващо език на омразата. Според последната оценка в рамките на 24 часа дружествата анализират 90 % от съдържанието, за което е подаден сигнал, и премахват 71 % от съдържанието, което бъде счетено, че представлява изказвания, пораждащи омраза. Платформите обаче трябва да подобрят прозрачността и обратната връзка с потребителите и да гарантират последователна оценка на съдържанието, за което е подаден сигнал[71].

Интернет форумът на ЕС ще улесни и обмена на информация относно съществуващите и развиващите се технологии с цел преодоляване на предизвикателствата, свързани със сексуалното насилие над деца онлайн. Борбата със сексуалното насилие над деца онлайн е в центъра на новата стратегия за засилване на **борбата срещу сексуалното насилие над деца**[72], чиято цел е да се увеличи максимално използването на инструментите за борба с тези престъпления на равнище ЕС. Дружествата трябва да могат да продължат работата си за откриване и премахване на материали, съдържащи сексуално насилие над деца онлайн, а вредите от такова съдържание изискват създаването на уредба, с която да се определят ясни и постоянни задължения за справяне с проблема. В стратегията ще бъде посочено също така, че Комисията ще започне да подготвя специфично секторно законодателство за по-ефективно справяне със сексуалното насилие над деца, при пълно зачитане на основните права.

В по-общ план, в предстоящия законодателен акт за цифровите услуги ще бъдат изяснени и подобрени правилата за отговорността и безопасността на цифровите услуги и ще се премахнат демотивиращите фактори, които възпират действията за ограничаване на незаконното съдържание, стоки или услуги.

Освен това Комисията ще продължи да работи с международните партньори и с **Глобалния интернет форум за борба с тероризма**, включително чрез независимия консултативен комитет, за да се обсъдят начините за справяне с тези предизвикателства на световно равнище, като същевременно се запазят ценностите и основните права на ЕС. Следва да се обърне внимание и на нови теми, като например алгоритмите или онлайн игрите[73].

Хибридни заплахи

Мащабът и разнообразието на хибридните заплахи днес са безпрецедентни. Кризата с COVID-19 е поредното доказателство за това — някои държавни и недържавни субекти се опитват да се възползват от пандемията, по-специално чрез манипулиране на информационната среда и застрашаване на ключови инфраструктури. Това създава риск от отслабване на социалното сближаване и подкопаване на доверието в институциите на ЕС и правителствата на държавите членки.

Подходът на ЕС към хибридните заплахи е изложен в Съвместната рамка от 2016 г.[74] и в съвместното съобщение от 2018 г. относно укрепването на устойчивостта срещу

[71] https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

[72] Стратегия на ЕС за по-ефективна борба срещу сексуалното насилие над деца, COM(2020) 607.

[73] Терористите все по-често използват системата за обмен на съобщения на платформите за игри за обмен на информация, а младите терористи също така възпроизвеждат насилствени нападения във видеоигрите.

[74] Съвместна рамка за борба с хибридните заплахи — ответни действия на Европейския съюз, JOIN(2016) 18.

хибридните заплахи[75]. Действията на равнище ЕС са подкрепени със значителен набор от инструменти, свързващи вътрешната и външната сигурност, и се основават на подход, който обхваща цялото общество, и на тясното сътрудничество със стратегически партньори, по-специално НАТО и Г-7. Заедно с настоящата стратегия се публикува и доклад за прилагането на подхода на ЕС спрямо хибридните заплахи[76]. Въз основа на картографирането[77], представено успоредно с настоящата стратегия, службите на Комисията и Европейската служба за външна дейност ще създадат **онлайн платформа с ограничен достъп** с информация за държавите членки относно инструментите и мерките на равнище ЕС за противодействие на хибридните заплахи.

Макар отговорността за борбата с хибридните заплахи да се носи основно от държавите членки — поради характерните връзки с националните политики в областта на сигурността и отбраната — някои уязвими точки са общи за всички държави членки, а някои заплахи се простират отвъд националните граници, като например атаките срещу трансгранични мрежи или инфраструктура. Комисията и върховният представител ще определят подход на ЕС спрямо хибридните заплахи, който да хармонизира външното и вътрешното измерение и да обедини националните и общоевропейските съображения. Той трябва да обхваща целия спектър на действие — от ранното откриване, анализа, повишаването на осведомеността, изграждането на устойчивост и превенция до реакцията при кризи и управлението на последиците.

В допълнение към засиленото прилагане, при условия на постоянно развитие на хибридните заплахи, специално внимание ще бъде насочено и към **включването на съображенията във връзка с хибридните заплахи в процеса на разработване на политиките**, за да се върви в крак с динамиката на събитията и да се гарантира, че не се пренебрегва нито една потенциално значима инициатива. Хибридните заплахи ще бъдат вземани под внимание при оценката на въздействието на нови инициативи, включително инициативи в области, които до момента са извън обхвата на рамката за борба с хибридните заплахи, като например образование, технологии и научни изследвания. Този подход ще използва резултатите от извършената работа по отношение на концептуализацията на хибридните заплахи, която предоставя цялостен поглед върху различните инструменти, които може да бъдат използвани от противниците[78]. Целта следва да бъде да се гарантира, че процесът на вземане на решения се основава на редовни, изчерпателни разузнавателни данни за развитието на хибридните заплахи. Това ще зависи в голяма степен от разузнавателните сведения на държавите членки и от допълнителното засилване на сътрудничеството в областта на разузнаването с компетентните служби на държавите членки чрез Центъра на ЕС за анализ на информация (EU INTCEN).

---

[75] Повишаване на устойчивостта и укрепването на способностите за борба с хибридните заплахи, JOIN(2018) 16.

[76] SWD(2020) 153 Доклад относно прилагането на Съвместната рамка от 2016 г. за борба с хибридните заплахи и Съвместното съобщение от 2018 г. относно повишаването на устойчивостта и укрепването на способностите за борба с хибридните заплахи.

[77] SWD(2020) 152 Картографиране на мерките, свързани с повишаване на устойчивостта и противодействие на хибридните заплахи.

[78] Картината на хибридните заплахи: концептуален модел, JRC117280, доклад, разработен съвместно от Съвместния изследователски център и Центъра за високи постижения в борбата с хибридните заплахи.

За да се развие **ситуационната осведоменост**, службите на Комисията и Европейската служба за външна дейност ще проучат възможностите за рационализиране на информационните потоци от различни източници, включително държавите членки, както и агенциите на ЕС, като ENISA, Европол и Frontex. Звеното на ЕС за синтез на информацията за хибридните заплахи ще продължи да бъде координационното звено на ЕС за оценка на хибридните заплахи. **Изграждането на устойчивост** е от основно значение за предотвратяването и защитата от хибридни заплахи. Ето защо е от решаващо значение систематично да се проследява и обективно да се измерва напредъкът в тази област. Първата стъпка ще бъде да се определят изходните параметри на устойчивостта спрямо хибридни заплахи по сектори както за държавите членки, така и за институциите и органите на ЕС. На последно място, с цел повишаване на **готовността за реакция при кризи** следва да бъде преразгледан съществуващият протокол, както е посочено в EU Playbook от 2016 г.[79], като се направи един по-широк преглед и се укрепи системата на ЕС за реакция при кризи, която в момента е в процес на създаване[80]. Целта е да се постигне максимален ефект от действията на ЕС, като се обединят бързо секторните реакции и се осигури безпрепятствено сътрудничество с нашите партньори и на първо място — НАТО.

Ключови действия
• Да се гарантира, че законодателството в областта на киберпрестъпността се прилага и е подходящо за целта • Стратегия на ЕС за по-ефективна борба срещу сексуалното насилие над деца • Предложения за откриване и отстраняване на материали, съдържащи сексуално насилие над деца • Подход на ЕС в борбата с хибридните заплахи • Преглед на оперативния протокол на ЕС за борба с хибридните заплахи (EU Playbook) • Оценка на начините за повишаване на капацитета за правоприлагане при цифровите разследвания

3. Защита на европейците от тероризъм и организирана престъпност

Тероризъм и радикализация

Заплахата от тероризъм в ЕС продължава да е висока. Въпреки намаляването на броя на нападенията като цяло, те все още могат да имат опустошителен ефект. Освен това радикализацията може в по-общ план да поляризира и да дестабилизира социалното сближаване. Държавите членки носят основната отговорност в борбата с тероризма и радикализацията. Въпреки това, постоянно нарастващото трансгранично/междусекторно измерение на заплахата изисква по-нататъшни стъпки в сътрудничеството и координацията в ЕС. Приоритет е ефективното прилагане на законодателството на ЕС за борба с тероризма, включително ограничителните

[79] Оперативен протокол на ЕС за борба с хибридните заплахи (EU Playbook), SWD(2016) 227.

[80] След провеждането на видеоконференцията си от 26 март 2020 г. членовете на Европейския съвет приеха изявление относно действията на ЕС в отговор на разпространението на COVID-19, като приканиха Комисията да направи предложения за по-амбициозна и широкообхватна система за управление на кризи в рамките на ЕС.

мерки[81]. Продължава да е на дневен ред и разширяването на мандата на Европейската прокуратура, за да обхване трансграничните терористични престъпления.

Борбата с тероризма започва със справяне с първопричините. Поляризацията на обществото, реалната или възприеманата дискриминация и други психологически и социологически фактори могат да засилят уязвимостта на хората спрямо радикалната пропаганда. В този контекст борбата с **радикализацията** върви ръка за ръка с насърчаването на социалното сближаване на местно, национално и европейско равнище. През последното десетилетие бяха разработени няколко значими инициативи и политики, по-специално чрез Мрежата за осведоменост по въпросите на радикализацията и чрез инициативата „Градовете в ЕС срещу радикализацията“.[82] Сега е моментът да се обмислят действия за рационализиране на политиките, инициативите и фондовете на ЕС за справяне с радикализацията. Тези действия могат да подпомогнат развитието на способности и умения, да засилят сътрудничеството, да укрепят базата от доказателства и да спомогнат за оценката на напредъка, с участието на всички заинтересовани страни, включително практикуващи специалисти на първа линия, политици и представители на академичните среди[83]. Меките политики, като образованието, културата, младежта и спорта, биха могли да допринесат за предотвратяване на радикализацията, като предоставят възможности за младежите, изложени на риск, и за сближаване в рамките на ЕС[84]. Приоритетните области включват работа по ранно откриване и управление на риска, изграждане на устойчивост и деангажиране, както и реабилитация и реинтеграция в обществото.

Терористите се опитаха да придобият и да използват за направа на оръжия **химически, биологични, радиологични и ядрени** (ХБРЯ)[85] материали, както и да развият необходимите знания и капацитет, за да ги използват[86]. Потенциалът на нападенията с ХБРЯ материали е силно застъпен в терористичната пропаганда. Тъй като потенциалните вреди са твърде значителни, необходимо е да се обърне особено внимание на проблема. Въз основа на подхода, използван за регулиране на достъпа до прекурсори на взривни вещества, Комисията ще разгледа възможността за ограничаване на достъпа до някои опасни химикали, които биха могли да бъдат използвани за извършване на нападения. Укрепването на капацитета на механизма на ЕС за гражданска защита (rescEU) в областта на ХБРЯ материали също ще бъде от ключово значение. Сътрудничеството с трети държави е важно и за укрепване на общата култура на безопасност и сигурност във връзка с ХБРЯ материали, като се използват пълноценно глобалните центрове на ЕС за високи постижения в областта на ХБРЯ материали. Това сътрудничество ще включва национални оценки на пропуските и рисковете, подкрепа за национални и регионални планове за действие в областта на

---

[81] Съветът прие ограничителни мерки по отношение на ИДИЛ (Даиш) и Ал-Кайда, както и специални ограничителни мерки, насочени срещу определени лица и образувания с оглед на борбата с тероризма. Вж. Карта на санкциите на ЕС (https://www.sanctionsmap.eu/#/main) за преглед на всички ограничителни мерки.

[82] Пилотната инициатива „Градовете в ЕС срещу радикализацията“ има двойната цел да насърчава обмена на експертен опит между градовете в ЕС и да събира обратна информация относно най-добрите начини за оказване на подкрепа на местните общности на равнище ЕС.

[83] Например финансиране по линия на Европейския фонд за сигурност и Програмата за гражданството.

[84] Действия на ЕС като виртуален обмен по програмата „Еразъм+“, e-twinning („електронно побратимяване“).

[85] През последните две години например имаше няколко случая в Европа (Франция, Германия, Италия) и другаде (Тунис, Индонезия) с използване на биологични агенти (обикновено растителни токсини).

[86] Съветът прие ограничителни мерки срещу разпространението и употребата на химическо оръжие.

ХБРЯ материали, обмен на добри практики и дейности за изграждане на капацитет в областта на ХБРЯ.

ЕС разработи най-напредничавото законодателство в света за ограничаване на достъпа до **прекурсори на взривни вещества**[87] и за откриване на съмнителни сделки, насочени към създаването на самоделни взривни устройства. Въпреки това заплахата от взривни устройства, създадени в домашни условия, продължава да е висока и се използва в множество атаки в целия ЕС[88]. Като първа стъпка правилата трябва да се прилагат и да се гарантира, че онлайн средата не позволява заобикалянето на контрола.

Ефективното преследване на лицата, извършили терористични престъпления, включително **чуждестранните бойци терористи**, които понастоящем пребивават в Сирия и Ирак, също е важен елемент от политиката за борба с тероризма. Въпреки че тези въпроси са предимно от компетентността на държавите членки, координацията и подкрепата от ЕС могат да помогнат на държавите членки да се справят с общите предизвикателства. Подготвяните мерки за пълно прилагане на законодателството в областта на сигурността на границите[89] и за пълноценно използване на всички съответни бази данни на ЕС за обмен на информация относно известни заподозрени лица ще бъдат важна стъпка напред. Освен идентифицирането на високорисковите лица е необходима и политика за реинтеграция и реабилитация. Междудисциплинарното сътрудничество, включително със служителите в затворите и пробационните служби, ще подобри разбирането в съдебната система на процесите на радикализация към насилнически екстремизъм и подхода на съдебния сектор във връзка с осъждането и използването на алтернативи на задържането.

Предизвикателството във връзка с чуждестранните бойци терористи е илюстрация на връзката между вътрешната и **външната сигурност.** Сътрудничеството в областта на борбата с тероризма, предотвратяването и борбата с радикализацията и насилническия екстремизъм е от основно значение за сигурността в ЕС[90]. Необходими са допълнителни стъпки за развитие на партньорства за борба с тероризма и сътрудничество със съседните и други държави въз основа на експертния опит на мрежата от експерти на ЕС в областта на борбата с тероризма/сигурността. Съвместният план за действие в областта на борбата с тероризма за Западните Балкани е добър пример за такова целенасочено сътрудничество. По-специално следва да се положат усилия за подпомагане на капацитета на държавите партньори за идентифициране и установяване на местонахождението на чуждестранни бойци терористи. Освен това ЕС ще продължи да насърчава многостранното сътрудничество, като работи съвместно с водещите световни организации в тази област, като Организацията на обединените нации, НАТО, Съвета на Европа, Интерпол и ОССЕ. Той ще се ангажира също така с Глобалния форум за борба с

[87] Химикали, които биха могли да бъдат използвани за производството на самоделни взривни устройства. Те са уредени в Регламент (ЕС) 2019/1148 за предлагането на пазара и употребата на прекурсори на взривни вещества.

[88] Примери за такива опустошителни нападения са атаките в Осло (2011 г.), Париж (2015 г.), Брюксел (2016 г.) и Манчестър (2017 г.). При нападение със самоделно взривно устройство в Лион (2019 г.) пострадаха 13 души.

[89] Включително новия мандат на Европейската агенция за гранична и брегова охрана (Frontex).

[90] В заключенията си от 16 юни 2020 г. Съветът подчерта необходимостта от защита на гражданите на ЕС от тероризъм и насилнически екстремизъм, във всичките им форми и независимо от техния произход, както и от по-нататъшно укрепване на външния ангажимент на ЕС за борба с тероризма в определени приоритетни географски райони и тематични области.

тероризма и Световната коалиция срещу Даиш, както и със съответните представители на гражданското общество. Инструментите на външната политика на Съюза, включително развитието и сътрудничеството, също играят важна роля при работата с трети държави за предотвратяване на тероризма и пиратството. Международното сътрудничество е от съществено значение и за премахването на всички източници на **финансиране на тероризма**, например чрез Специалната група за финансови действия.

Организирана престъпност

Организираната престъпност нанася огромни щети на икономиката и на хората. Икономическите загуби, дължащи се на организираната престъпност и корупцията, се оценяват на сума между 218 и 282 милиарда евро годишно[91]. През 2017 г. в Европа бяха разследвани повече от 5 000 организирани престъпни групи — увеличение с 50 % в сравнение с 2013 г[92]. Организираната престъпност работи все повече на трансгранично равнище, включително от непосредственото съседство на ЕС, което изисква засилено оперативно сътрудничество и обмен на информация с партньорите в съседните държави.

Появяват се нови предизвикателства и онлайн престъпленията се увеличават: пандемията от COVID-19 доведе до огромно нарастване на онлайн измамите сред уязвимите групи, както и до кражби и грабежи на здравни и санитарни продукти.[93] ЕС трябва да засили работата си срещу организираната престъпност, включително на международно равнище, с повече инструменти за разбиване на бизнес модела на организираната престъпност. Борбата с организираната престъпност изисква и тясно сътрудничество с местните и регионалните администрации, както и с гражданското общество, които са ключови партньори в областта на предотвратяването на престъпността и оказването на помощ и подкрепа на жертвите, като необходимостта е особено голяма в администрациите в граничните региони. Тази работа ще бъде обединена в **Програма за борба с организирана престъпност**.

Повече от една трета от организираните престъпни групи, действащи в ЕС, участват в производството, трафика или разпространението на наркотици. Зависимостта от наркотици доведе до над осем хиляди смъртни случая в резултат на свръхдоза в ЕС през 2019 г. Основната част от **трафика на наркотици** се осъществява през граница и много от печалбите проникват в законната икономика.[94] Новата програма на ЕС за борба с наркотиците[95] ще засили усилията на ЕС и на държавите членки за намаляване на търсенето и предлагането на наркотици, като определи съвместни действия за решаване на общ проблем и засили диалога и сътрудничеството между ЕС и външните партньори по въпросите на наркотиците. След оценка на Европейския център за мониторинг на наркотиците и наркоманиите Комисията ще прецени дали неговият мандат се нуждае от актуализиране, за да се отговори на новите предизвикателства.

---

[91] По отношение на брутния вътрешен продукт (БВП); Доклад на Европол: „Още ли се отплаща престъпността?“ — отнемане на незаконно придобито имущество в ЕС, 2016 г.

[92] Европол, Оценка на заплахата от тежката и организираната престъпност, 2013 и 2017 г.

[93] Европол, 2020 г.

[94] Европейски център за мониторинг на наркотиците и наркоманиите и Европол, Доклад за пазарите на наркотични вещества в ЕС, 2019 г. (ноември 2019 г.).

[95] Програма на ЕС за борба с наркотиците и План за действие за периода 2021—2025 г., COM(2020) 606.

Организираните престъпни групи и терористите са основни участници и в търговията с **незаконни огнестрелни оръжия**. Между 2009 г. и 2018 г. в Европа бяха извършени 23 масови стрелби, при които бяха убити над 340 души[96]. Огнестрелните оръжия често се внасят нелегално в ЕС чрез неговите непосредствени съседи[97]. Това показва необходимостта от засилване на координацията и сътрудничеството както в рамките на ЕС, така и с международните партньори, и по-специално с Интерпол, с цел да се хармонизира събирането на информация и докладването относно конфискациите на огнестрелно оръжие. От ключово значение е също така да се подобри проследимостта на оръжията, включително в интернет, и да се осигури обмен на информация между органите по лицензирането и правоприлагането. Комисията предлага нов **План за действие на ЕС срещу трафика на огнестрелни оръжия**[98] и ще оцени също така дали правилата относно разрешенията за износ и мерките за внос и транзит на огнестрелни оръжия продължават да са подходящи за целите, чието постигане се търси[99].

Престъпните организации третират мигрантите и лицата, нуждаещи се от международна закрила, като стока. 90 % от незаконните мигранти, пристигащи в ЕС, са подпомагани от престъпна мрежа[100]. Контрабандата на мигранти често е свързана и с други форми на организирана престъпност, по-специално с трафика на хора[101]. Освен огромната човешка цена на трафика на хора, по оценка на Европол годишната печалба от всички форми на експлоатация във връзка с трафика на хора в световен мащаб възлиза на 29,4 милиарда евро. Това е транснационална престъпност, която се подхранва от незаконно търсене във и извън ЕС и засяга всички държави — членки на ЕС. Лошите резултати по отношение на разкриването, преследването и осъждането на тези престъпления изискват нов подход за засилване на действията. Нов **всеобхватен подход към трафика на хора** ще доведе до по-добра съгласуваност на действията. В допълнение, Комисията ще представи **нов план за действие на ЕС срещу контрабандата на мигранти** за периода 2021—2025 г. Двете направления ще се съсредоточат върху борбата с престъпните мрежи, ще засилят сътрудничеството и ще подкрепят работата на правоприлагащите органи.

Организираните престъпни групи, както и терористите, търсят възможности и в други области, особено тези, които генерират големи печалби при нисък риск от разкриване, като например **престъпленията против околната среда**. Незаконният лов и търговия с екземпляри от дивата флора и фауна, незаконната минна дейност, дърводобивът и незаконното депониране и превози на отпадъци са се превърнали в четвъртата по големина престъпна дейност в света[102]. Налице е и престъпно използване на схемите за търговия с емисии и системите за енергийни сертификати, както и злоупотреба с

[96] Фламандски институт за мир, „Въоръжени, за да убиват“ (Flemish Peace Institute, Armed to kill) (октомври 2019 г.).

[97] ЕС финансира борбата срещу разпространението и трафика на малки оръжия и леки въоръжения в региона от 2002 г.; той предоставя финансиране по-специално на мрежата от експерти в областта на огнестрелните оръжия в Югоизточна Европа (SEEFEN). От 2019 г. насам партньорите от Западните Балкани участват пълноценно в приоритета за огнестрелните оръжия на Европейската мултидисциплинарна платформа за борба с криминални заплахи (EMPACT).

[98] COM(2020) 608.

[99] Регламент (ЕС) № 258/2012 за прилагане на член 10 от протокола на Организацията на обединените нации срещу незаконното производство и трафик с огнестрелни оръжия.

[100] Източник: Европол.

[101] Европол, Европейски център за борба с контрабандата на мигранти (EMSC), 4-ти годишен доклад.

[102] Оценка за бързо реагиране на UNEP—Интерпол: „Ръстът на престъпленията срещу околната среда“, юни 2016 г.

финансиране, определено за екологична устойчивост и устойчиво развитие. Докато насърчава действията на ЕС, държавите членки и международната общност за засилване на усилията за борба с престъпленията спрямо околната среда[103], Комисията извършва оценка на това дали Директивата относно престъпленията срещу околната среда[104] продължава да е подходяща за определените в нея цели. **Трафикът на културни ценности** също се превърна в една от най-доходоносните престъпни дейности, източник на финансиране за терористите и за организираната престъпност, и продължава да расте. Следва да се проучат стъпки за подобряване на проследимостта на културните ценности онлайн и офлайн на вътрешния пазар, както и за сътрудничеството с трети държави, в които културните ценности са плячкосвани, и за предоставяне на активна подкрепа за правоприлагащите и академичните общности.

Икономическите и финансовите престъпления са изключително сложни, но всяка година засягат милиони граждани и хиляди предприятия в ЕС. Борбата с измамите е от решаващо значение и изисква действия на равнище ЕС. Европол, заедно с Евроюст, Европейската прокуратура и Европейската служба за борба с измамите подкрепят държавите членки и ЕС за защитата на икономическите и финансовите пазари и на парите на данъкоплатците в ЕС. Европейската прокуратура ще започне да функционира пълноценно в края на 2020 г. и ще разследва, преследва и предава на съд престъпленията против бюджета на ЕС, като например измами, корупция и изпиране на пари. Освен това тя ще се бори с трансграничните измами с ДДС, които струват на данъкоплатците най-малко 50 милиарда евро годишно.

Комисията също така ще подкрепи развиването на експертен капацитет и разработването на законодателна рамка в областта на нововъзникващите рискове, като например криптоактивите и новите системи за плащане. Комисията по-специално ще проучи действията в отговор на появата на криптовалути, като например биткойн, и въздействието, което тези нови технологии ще имат върху начина на емитиране, обмен, споделяне и достъп до финансови активи.

В рамките на Европейския съюз следва да има нулева толерантност към незаконните пари. В продължение на повече от тридесет години ЕС разработи стабилна регулаторна уредба за предотвратяване и борба с **изпирането на пари** и финансирането на тероризма, при пълно зачитане на необходимостта от защита на личните данни. Въпреки това е налице все по-голям консенсус, че прилагането на настоящата правна уредба трябва да бъде значително подобрено. Необходимо е да се обърне внимание на големите различия в начина, по който се прилага уредбата, и на сериозните слабости в налагането на правилата. Както се посочва в плана за действие от май 2020 г.[105], в момента се извършва оценка на възможностите за укрепване на правната уредба на ЕС за борба с изпирането на пари и финансирането на тероризма. Сред областите, които трябва да се проучат, е свързването на националните централизирани регистри на банковите сметки, което би могло значително да ускори достъпа до финансовата информация на звената за финансово разузнаване и компетентните органи.

[103] Вж. „Европейски зелен пакт“, COM(2019) 640 final.
[104] Директива 2008/99/ЕО относно защитата на околната среда чрез наказателно право.
[105] План за действие за предотвратяване на изпирането на пари и финансирането на тероризма, COM(2020) 2800.

В ЕС **печалбите на организираните престъпни групи** се оценяват на 110 милиарда евро годишно. Настоящият отговор включва хармонизирано законодателство относно конфискацията и отнемането на активи,[106] подобряване на обезпечаването и конфискацията на незаконно придобито имущество в ЕС и създаване на условия за взаимно доверие и ефективно трансгранично сътрудничество между държавите членки. Само около 1 % от тези печалби обаче се конфискуват[107], което позволява на организираните престъпни групи да инвестират в разширяване на престъпните си дейности и да проникват в законната икономика, като по-специално малките и средните предприятия, които имат затруднения при достъпа до кредити, са ключова цел за изпирането на пари. Комисията ще анализира прилагането на законодателството[108] и евентуалната необходимост от допълнителни общи правила, включително относно неоснованата на присъда конфискация. Службите за отнемане на активи[109], ключови участници в процеса на отнемане на незаконно придобито имущество, също биха могли да бъдат снабдени с по-добри инструменти за по-бързо идентифициране и проследяване на активи в целия ЕС, за да се увеличат процентите на конфискация.

Организираната престъпност и **корупцията** са тясно свързани. По груби оценки само корупцията коства 120 милиарда евро годишно на икономиката на ЕС[110]. Предотвратяването и борбата с корупцията ще продължат да бъдат подлагани на редовен мониторинг чрез механизма за върховенството на закона и европейския семестър. В рамките на европейския семестър бе извършена оценка на предизвикателствата при борбата с корупцията, например във връзка с обществените поръчки, публичната администрация, бизнес средата или здравеопазването. Новият годишен доклад на Комисията относно върховенството на закона ще обхване борбата с корупцията и ще даде възможност за провеждане на превантивен диалог с националните органи и заинтересованите страни на равнище ЕС и на национално равнище. Организациите на гражданското общество също могат да играят ключова роля за насърчаване на действията на публичните органи за предотвратяване и борба с организираната престъпност и корупцията, като тези групи биха могли да бъдат обединени ползотворно в общ форум. Поради трансграничното естество на проблема друг ключов аспект представляват сътрудничеството и взаимопомощта със съседните на ЕС региони в борбата с организираната престъпност и корупцията.

Ключови действия
• Програма на ЕС за борба с тероризма, включваща обновени действия за борба с радикализацията в ЕС • Ново сътрудничество с ключови трети държави и международни организации в борбата с тероризма

[106] Законодателството на ЕС изисква създаването на служби за отнемането на активи във всички държави членки.

[107] Доклад, озаглавен „Възстановяване и конфискация на активи: да гарантираме, че престъпността „не си струва“, COM(2020) 217 final.

[108] Директива 2014/42/ЕС за обезпечаване и конфискация на средства и облаги от престъпна дейност.

[109] Решение 2007/845/ПВР на Съвета относно сътрудничеството между Службите за възстановяване на активи на държавите членки при проследяване и установяване на облаги или друго имущество, свързани с престъпления.

[110] Общият размер на разходите за икономиката, свързани с корупцията, трудно може да бъде изчислен, макар че редица образувания, включително Международната търговска камара, „Трансперънси интернешънъл“, Глобалният договор на ООН и Световният икономически форум, положиха усилия в тази насока, посочвайки, че корупцията възлиза на 5% от световния БВП.

- Програма за борба с организираната престъпност, включително трафика на хора
- Програма на ЕС относно наркотиците и План за действие за периода 2021—2025 г.
- Оценка на Европейския център за мониторинг на наркотици и наркомании
- План за действие на ЕС относно трафика на огнестрелни оръжия за периода 2020—2025 г.
- Преглед на законодателството относно обезпечаването и конфискацията и относно службите за възстановяване на активи
- Оценка на Директивата относно престъпленията срещу околната среда
- План за действие на ЕС срещу контрабандата на мигранти за периода 2021—2025 г.

4. Силна европейска екосистема на сигурността

За да има един истински и ефективен Съюз на сигурност, трябва да бъде положено общо усилие от всички части на обществото. Правителствата, правоприлагащите органи, частният сектор, образователните системи и самите граждани трябва да бъдат ангажирани, оборудвани и правилно свързани, за да се изградят готовност и устойчивост у всички, и особено у най-уязвимите, жертвите и свидетелите.

Всички политики се нуждаят от аспект, свързан със сигурността, и ЕС може да допринесе на всички равнища. У дома домашното насилие е един от най-сериозните рискове за сигурността. 22 % от жените в ЕС са преживели насилие от интимен партньор[111]. Присъединяването на ЕС към Конвенцията от Истанбул за превенция и борба с насилието над жени и домашното насилие продължава да бъде основен приоритет. Ако преговорите продължат да бъдат блокирани, Комисията ще предприеме други мерки за постигане на същите цели, като тези на Конвенцията, включително като предложи добавяне на насилието над жени към списъка на приоритетните за ЕС престъпления, посочени в Договора.

Сътрудничество и обмен на информация

Един от най-важните приноси, които ЕС може да даде за защитата на гражданите, е да помогне на лицата, отговарящи за сигурността, да работят добре заедно. Сътрудничеството и обменът на информация са най-мощните инструменти за борба с престъпността и тероризма и за осигуряването на правосъдие. За да бъдат ефикасни, те трябва да бъдат целенасочени и да се осъществяват своевременно. За да бъдат надеждни, те трябва да се придружават от общи гаранции и механизми за контрол.

С цел постигане на по-нататъшно развитие на **оперативното сътрудничество между държавите членки в областта на правоприлагането**, бяха създадени редица инструменти на ЕС и специални секторни стратегии[112]. Един от основните инструменти на ЕС в подкрепа на сътрудничеството между правоприлагащите органи на държавите членки е Шенгенската информационна система, която се използва за обмен на данни относно издирвани и изчезнали лица и вещи в реално време. Резултатите от прилагането ѝ бяха усетени при задържането на престъпници, изземването на наркотици и спасяването на потенциални жертви[113]. Степента на сътрудничеството може обаче да бъде подобрена още повече чрез рационализиране и

[111] Съюз на равенство: Стратегия за равенство между половете (2020 — 2025 г.), COM(2020) 152.

[112] Например планът за действие във връзка със Стратегията на ЕС за морска сигурност, който доведе до значими постижения при сътрудничеството между съответните агенции на ЕС във връзка с функциите, свързани с бреговата охрана.

[113] Борбата на ЕС срещу организираната престъпност през 2019 г. (Съвет, 2020 г.).

модернизиране на наличните инструменти. По-голямата част от правната уредба на ЕС, залегнала в основата на оперативното сътрудничество в областта на правоприлагането, беше създадена преди 30 години. Сложната мрежа от двустранни споразумения между държавите членки, много от които са остарели или не се използват достатъчно, поражда риск от фрагментиране. В по-малките държави или в държави без излаз на море служителите на правоприлагащите органи, които извършват трансгранична дейност, се налага да извършват оперативни действия, следвайки понякога до седем различни набора от правила; в резултат на това някои операции, като например преследването по гореща следа на заподозрени с пресичане на вътрешните граници, просто не се провеждат. Оперативното сътрудничество чрез използване на нови технологии, например дронове, също не е обхванато от действащата рамка на ЕС.

Оперативната ефективност може да се подпомага чрез специално сътрудничество в областта на правоприлагането, което може да спомогне и за предоставянето на ключова подкрепа за други цели на политиката — например предоставяне на информация за сигурността за целите на новата оценка на преките чуждестранни инвестиции. Комисията ще обмисли по какъв начин наличието на кодекс за полицейско сътрудничество би могло да спомогне за това. Правоприлагащите органи на държавите членки все по-често използват подкрепа и експертен опит на равнище ЕС, а Центърът на ЕС за анализ на информация (INTCEN) изигра ключова роля за насърчаване на обмена на стратегически разузнавателни данни между службите за разузнаване и сигурност на държавите членки, осигурявайки ситуационна осведоменост, основана на разузнавателни данни, в полза на институциите на ЕС[114]. **Европол** също може да играе ключова роля като разшири сътрудничеството си с трети държави с цел противодействие на престъпността и тероризма в съответствие с други външни политики и инструменти на ЕС. Понастоящем обаче Европол е изправена пред редица сериозни ограничения — по-специално във връзка с прекия обмен на лични данни с частноправни субекти — които пречат на тази агенция да оказва на държавите членки ефективна подкрепа в борбата с тероризма и престъпността. Мандатът на Европол е в процес на оценяване, за да се види как следва да бъде подобрен, така че да се гарантира, че Агенцията ще може да изпълнява пълноценно своите задачи. В този контекст съответните органи на равнище ЕС (например OLAF, Европол, Евроюст и Европейската прокуратура) също следва да работят в по-тясно сътрудничество и да подобряват обмена на информация.

Друга ключова връзка се отнася до по-нататъшното развитие на **Евроюст** с цел постигане на максимална синергия между сътрудничеството в областта на правоприлагането и съдебното сътрудничество. ЕС би извлякъл ползи и от по-стратегическа съгласуваност: **EMPACT**[115] — политическият цикъл на ЕС за борба с тежката и международната организирана престъпност, предоставя на органите методология, основана на разузнавателни данни в наказателната област, за да им даде възможност да действат съвместно с цел справяне с най-важните заплахи от престъпления, засягащи ЕС. Това доведе до постигане на важни оперативни резултати[116] през последното десетилетие. Въз основа на опита на практикуващите

[114] INTCEN служи като единствен портал на службите за разузнаване и сигурност на държавите членки за осигуряване на ЕС на ситуационна осведоменост, основана на разузнавателни данни.

[115] EMPACT е абревиатура за Европейска мултидисциплинарна платформа за борба с криминални заплахи.

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

специалисти съществуващият механизъм следва да бъде рационализиран и опростен, за да се реагира по-добре на най-неотложните и променящи се заплахи от престъпления в рамките на нов цикъл на политиката за периода 2022—2025 г.

Наличието на своевременна и относима **информация** е от ключово значение за ежедневната работа по преследването на престъпността. Въпреки че на равнище ЕС са разработени нови бази данни в областта на сигурността и управлението на границите, голяма част от информацията все още се намира в националните бази данни или се обменя извън тези инструменти. Това води до значително допълнително работно натоварване, закъснения и по-голям риск от пропускане на ключова информация. Прилагането на подобрени, по-бързи и опростени процедури с участието на цялата общност, работеща в областта на сигурността, би довело до по-добри резултати. Наличието на подходящи инструменти е от основно значение, ако искаме обменът на информация да достигне до възможния си потенциал при действителното преследване на престъпността, като се предвидят необходимите гаранции, така че при обмена на данни да се спазват законодателството в областта на защитата на данните и основните права. С оглед на развитието в областта на технологиите, криминалистиката и защитата на данните и променените оперативни нужди, ЕС би могъл да обмисли дали е необходимо да се модернизират инструменти, като **решенията „Прюм“ от 2008 г.**, с които е въведен автоматизиран обмен на данни за ДНК, за дактилоскопични отпечатъци и за регистрацията на превозни средства, така че да се създаде възможност за автоматизиран обмен на допълнителни категории данни, които вече са на разположение в криминални или други бази данни на държавите членки, за целите на наказателните разследвания. Наред с това Комисията ще разгледа възможността за обмен на полицейски досиета, за да се спомогне за установяване дали в други държави членки има полицейски досиета за дадено лице и да се улесни достъпът до тези досиета, след като наличието им бъде установено, с всички необходими гаранции.

Информацията за пътниците спомогна за подобряването на граничния контрол, намаляването на незаконната миграция и идентифицирането на лицата, които представляват риск за сигурността. Предварителната информация за пътниците се състои от биографичните данни за всеки пътник, събирани от въздушните превозвачи по време на регистрацията и изпращани предварително на органите за граничен контрол на местоназначението. Преразглеждането на правната уредба[117] би дало възможност за по-ефективно използване на информацията, като същевременно ще се гарантира спазване на законодателството за защита на данните и ще се улесни потокът от пътници. Резервационните данни на пътниците (PNR данни) са данните, предоставяни от пътниците при резервиране на полети. Прилагането на Директивата за резервационните данни на пътниците[118] е от ключово значение и Комисията ще продължи да подкрепя и да осигурява спазването ѝ. Освен това, като средносрочно действие Комисията ще започне преглед на настоящия подход относно **предаването на PNR данни на трети държави**.

Съдебното сътрудничество е необходимо допълнение към усилията на полицията за борба с трансграничната престъпност. То премина през по-дълбоки промени през

[117] Директива 2004/82/ЕО на Съвета относно задължението на превозвачите да съобщават данни на пътниците.

[118] Директива (ЕС) 2016/681 относно използването на резервационни данни на пътниците с цел предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и тежки престъпления.

последните 20 години. Органи като **Европейската прокуратура** и **Евроюст** трябва да разполагат с необходимите средства, за да могат да работят пълноценно или трябва да бъдат укрепени. Сътрудничеството между работещите в сферата на правосъдието също би могло да се засили чрез по-нататъшни действия във връзка с взаимното признаване на съдебни решения, съдебното обучение и обмена на информация. Целта следва да бъде да се повиши взаимното доверие между съдиите и прокурорите, което е от основно значение за гладкото протичане на трансграничните производства. Използването на **цифрови технологии** също може да повиши ефикасността на нашите правосъдни системи. Създава се нова цифрова система за обмен, чрез която да се предават европейски заповеди за разследване, искания за правна взаимопомощ и свързани съобщения между държавите членки, като Евроюст оказва помощ в тази насока. Комисията ще работи с държавите членки за ускоряване на въвеждането на необходимите информационни системи на национално равнище.

Международното сътрудничество също е от ключово значение за ефективното правоприлагане и съдебното сътрудничество. Двустранните споразумения с ключови партньори играят ключова роля за осигуряване на информация и доказателства от държави извън ЕС. **Интерпол**, една от най-големите междуправителствени организации на криминалната полиция, има важна роля. Комисията ще разгледа възможните начини за засилване на сътрудничеството с Интерпол, включително за евентуален достъп до базите данни на Интерпол и за укрепване на оперативното и стратегическото сътрудничество. Правоприлагащите органи в ЕС разчитат също така на ключови държави партньори за откриването и разследването на престъпници и терористи. **Партньорствата в областта на сигурността между ЕС и трети държави** биха могли да бъдат засилени с цел по-голямо сътрудничество за противодействие на общите заплахи, като тероризма, организираната престъпност, киберпрестъпността, сексуалното насилие над деца и трафика на хора. Този подход ще се основава на общите интереси в областта на сигурността и ще се опира на провеждания диалог във връзка със сътрудничеството и сигурността.

Наред с обмена на информация, обменът на експертен опит може да бъде от особено значение за повишаване на готовността на правоприлагащите органи за реакция при **нетрадиционни заплахи**. Комисията не само ще насърчава обмена на най-добри практики, но и ще проучи възможността за създаване на **механизъм на равнище ЕС за координация за полицейските сили** в случай на форсмажорни обстоятелства, като пандемии. Пандемията също така показа, че полицейските дейности във връзка с цифровата общност, придружени от правни уредби за улесняване на полицейската дейност в интернет, ще бъдат от основно значение за борбата с престъпността и тероризма. Партньорствата между полицията и общностите, както офлайн, така и онлайн, могат да предотвратят извършването на престъпления и да смекчат въздействието на организираната престъпност, радикализацията и терористичните дейности. Свързването на решенията на местно, регионално, национално и европейско равнище в сферата на полицията е ключов фактор за успеха на Съюза на сигурност на ЕС като цяло.

Приносът на силните външни граници

Модерното и ефикасно управление на външните граници води до двойна полза, тъй като поддържа целостта на Шенгенското пространство и осигурява сигурност за нашите граждани. Мобилизирането на всички действащи лица, имащи отношение към този въпрос, с цел извличане на максимална полза за сигурността по границите може да окаже реално въздействие върху предотвратяването на трансграничната престъпност и тероризма. Съвместните оперативни дейности на наскоро подсилената

европейска гранична и брегова охрана[119] допринасят за предотвратяването и разкриването на трансгранични престъпления по **външните граници** и извън ЕС. Митническите дейности за откриване на рискове за безопасността и сигурността у всички стоки, преди те да пристигнат в ЕС, както и за контрол на стоките при пристигането им са от решаващо значение за борбата срещу трансграничната престъпност и тероризма. В бъдещия План за действие за митническия съюз ще бъдат обявени също така действия за укрепване на управлението на риска и за усилване на вътрешната сигурност, включително по-специално като се прецени възможността за изграждане на връзка между съответните информационни системи за анализ на рисковете за сигурността.

Рамката за **оперативна съвместимост между информационните системи на ЕС** в областта на правосъдието и вътрешните работи беше приета през май 2019 г. Тази нова структура има за цел да подобри ефикасността и ефективността на новите или модернизираните информационни системи[120]. Тя ще доведе до по-бързо предоставяне на по-систематизирана информация на служителите на правоприлагащите органи, граничните служители и служителите в областта на миграцията. Тя ще спомогне за правилното установяване на самоличността на лицата и ще допринесе за борбата с измамите със самоличност. За да може това действително да се случва, е необходимо прилагането на оперативната съвместимост да бъде приоритет както на политическо, така и на техническо равнище. Тясното сътрудничество между агенциите на ЕС и всички държави членки ще бъде от първостепенно значение за постигането на целта за пълна оперативна съвместимост до 2023 г.

Измамите с документи за пътуване се считат за едно от най-често извършваните престъпления. Този вид измама улеснява нелегалното движение на престъпници и терористи и играе ключова роля при трафика на хора и търговията с наркотици[121]. Комисията ще обмисли по какъв начин да разшири настоящата работа по стандартите за сигурност на документите за пребиваване и пътуване в ЕС, включително чрез цифровизация. От август 2021 г. държавите членки ще започнат да издават лични карти и документи за пребиваване съгласно хармонизирани стандарти за сигурност, включително чип, съдържащ биометрични идентификатори, които могат да бъдат проверявани от всички гранични органи в ЕС. Комисията ще наблюдава прилагането на тези нови правила, включително постепенната замяна на документите, които са в обращение понастоящем.

Засилване на научните изследвания и иновациите в областта на сигурността

Работата, насочена към гарантиране на киберсигурността и към борбата с организираната престъпност, киберпрестъпността и тероризма, зависи в много голяма степен от разработването на инструменти за бъдещето, които да спомогнат за създаването на по-безопасни и по-сигурни нови технологии, за справяне с предизвикателствата, пораждани от технологиите, и да подпомагат работата на

[119] Състояща се от Европейската агенция за гранична и брегова охрана (Frontex) и органите за гранична охрана и за брегова охрана на държавите членки.

[120] Системата за влизане/излизане (СВИ), Системата на ЕС за информация за пътуванията и разрешаването им (ETIAS), разширената Европейска информационна система за съдимост (ECRIS-TCN), Шенгенската информационна система, Визовата информационна система и бъдещата актуализирана система Евродак.

[121] Връзката между документните измами и трафика на хора е описана във Втория доклад относно напредъка в борбата с трафика на хора (COM(2018) 777) и придружаващия го документ SWD(2018) 473, както и в документа на Европол „Доклад за състоянието — трафикът на хора в ЕС“ от 2016 г.

правоприлагащите органи. За тази цел обаче е нужно участие от страна на частни партньори и промишлеността.

Иновациите следва да се разглеждат като стратегически инструмент за противодействие на настоящите заплахи и за предвиждане на бъдещите рискове и възможности. Иновативните технологии могат да предложат нови инструменти за подпомагане на правоприлагащите органи и другите участници в областта на сигурността. Изкуственият интелект и анализът на големи информационни масиви биха могли да използват високопроизводителните изчислителни технологии, за да предложат по-добра разкриваемост и бърз и цялостен анализ[122]. Ключова предпоставка за разработването на надеждни технологии е наличието на висококачествени набори от данни, които да са на разположение на компетентните органи за обучение, изпитване и валидиране на алгоритми[123]. В по-общ план, рискът от технологична зависимост понастоящем е висок — така например, ЕС е нетен вносител на продукти и услуги в областта на киберсигурността, с всичко, което това влече след себе си за икономиката и критичните инфраструктури. За да овладее технологиите и да гарантира непрекъснатост на доставките, включително в случай на нежелани събития и кризи, Европа трябва да осигури присъствие и капацитет в критичните части на съответните вериги за създаване на стойност.

Научните изследвания, иновациите и технологичното развитие в ЕС предоставят възможност аспектът, отнасящ се до сигурността, да бъде взет под внимание още при разработването на тези технологии и тяхното прилагане. Следващото поколение предложения за финансиране от ЕС може да бъде използвано като основен стимул[124]. При инициативите за европейските пространства на данни и за инфраструктури за компютърни услуги в облак сигурността е взета под внимание от самото начало. Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежата от национални координационни центрове[125] имат за цел да изградят ефективна и ефикасна структура за обединяване и споделяне на капацитета и резултатите от научните изследвания в областта на киберсигурността. Космическата програма на ЕС предоставя услуги в подкрепа на сигурността на ЕС, неговите държави членки и отделни физически лица[126].

С над 600 проекта, започнати от 2007 г. насам, на обща стойност от близо 3 милиарда евро, финансираните от ЕС научни изследвания в областта на сигурността са ключов инструмент за насочване на технологиите и знанията към подпомагане на намирането на решения, свързани със сигурността. В рамките на преразглеждането на мандата на

[122] Тази дейност може да се основава на Стратегията на Комисията за изкуствения интелект.

[123] Европейска стратегия за данните (COM(2020) 66 final).

[124] Предложенията на Комисията за „Хоризонт Европа“, фонд „Вътрешна сигурност“, Фонда за интегрирано управление на границите, програма EUInvest, Европейския фонд за регионално развитие и програма „Цифрова Европа“ ще спомогнат за разработването и внедряването на новаторски технологии и решения за сигурност по веригата за създаване на стойност в областта на сигурността.

[125] Предложение от 12 септември 2018 г. за Регламент 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).

[126] Например програма „Коперник“ предоставя услуги, които позволяват наблюдение на външните граници на ЕС и морско наблюдение, с което се подпомагат действията срещу пиратството и контрабандата, а така също се оказва подкрепа за критични инфраструктури. След като започне да функционира пълноценно, тази програма ще бъде от ключово значение за гражданските и военните мисии и операции.

Европол Комисията ще обмисли създаването на **Европейски център за иновации в областта на вътрешната сигурност**[127], който ще се стреми да намира общи решения за общите предизвикателства в областта на сигурността, както и възможности в тази област, които държавите членки не биха могли да използват самостоятелно. Сътрудничеството е от основно значение за насочването на инвестициите към постигане на най-добри резултати и за разработването на иновативни технологии, съчетаващи сигурност и икономическа полза.

Повишаване на уменията и на осведомеността

Осведомеността за проблемите, свързани със сигурността, и придобиването на необходимите умения за справяне с потенциални заплахи са от съществено значение за изграждането на по-устойчиво общество, в което предприятията, администрациите и физическите лица са по-добре подготвени. Предизвикателствата пред ИТ инфраструктурата и електронните системи разкриха необходимостта от подобряване на нашия човешки капацитет за подготвеност и реагиране в областта на киберсигурността. Наред с това пандемията подчерта значението на цифровизацията във всички области на икономиката и обществото на ЕС.

Дори **елементарното познаване на заплахите за сигурността** и начините за борба с тях може да окаже реално въздействие върху устойчивостта на обществото. Осъзнаването на рисковете от киберпрестъпността и необходимостта от самозащита от нея могат да се съчетаят със защитата за противодействие на кибератаките, осигурявана от доставчиците на услуги. Информацията относно опасностите и рисковете, свързани с трафика на наркотици, може да затрудни престъпниците да постигат целите си. ЕС може да стимулира разпространяването на най-добри практики, например чрез мрежата от центрове за безопасен интернет[128], и да гарантира, че в собствените му програми се включват такива цели.

Бъдещият план за действие в областта на цифровото образование следва да включва целенасочени мерки за изграждане на ИТ умения в областта на сигурността у цялото население. Приетата наскоро Програма за умения[129] подпомага изграждането на умения през целия живот. Тя включва специално предвидени действия за увеличаване на броя на завършилите образование в областта на науката, технологиите, инженерството, изкуствата и математиката, необходими в авангардни области като киберсигурността. Допълнителни действия, финансирани по линия на програма „Цифрова Европа“, ще позволят на специалистите да бъдат в крак с промените в областта на заплахите за сигурността и същевременно ще запълнят недостига на работна ръка в тази област на пазара на труда в Европа. Общото въздействие ще се изразява в предоставяне на възможности на лицата да придобият умения, за да се справят със заплахите за сигурността, както и на възможности на предприятията да намерят специалистите в тази област, от които се нуждаят. Бъдещите европейско научноизследователско пространство и европейско пространство за образование също ще насърчават развиването на кариера в областта на науката, технологиите, инженерството, изкуствата и математиката.

---

[127] Той ще работи и с Европейската агенция за гранична и брегова охрана — Frontex, CEPOL, eu-LISA и Съвместния изследователски център (JRC).

[128] Вж. www.betterinternetforkids.eu: понастоящем централният портал и националните центрове за безопасен интернет се финансират от Механизма за свързване на Европа (МСЕ), а бъдещото финансиране е предложено по линия програма „Цифрова Европа“.

[129] Европейска програма за умения за постигане на устойчива конкурентоспособност, социална справедливост и издръжливост (COM(2020) 274 final).

Друг важен елемент е достъпът на **жертвите** до упражняване на техните права — те трябва да получават необходимата помощ и подкрепата, от която се нуждаят с оглед на специфичните си обстоятелства. Когато става въпрос за малцинствата и за най-уязвимите жертви, като деца или жени, жертви на трафик с цел сексуална експлоатация или изложени на домашно насилие, се изискват специални усилия[130].

Повишаването на **уменията в областта на правоприлагането** играе особена роля. Съществуващите и новите технологични заплахи изискват повече инвестиции в повишаването на уменията на служителите на правоприлагащите органи на най-ранен етап, но също и през цялата им кариера. Агенцията на ЕС за обучение в областта на правоприлагането (CEPOL) е основен партньор, който подпомага държавите членки при изпълнението на тази задача. Обучението на правоприлагащите органи във връзка с расизма и ксенофобията, както и с правата на гражданите в по-общ план, трябва да бъде основен елемент от културата на ЕС в сферата на сигурността. Националните правосъдни системи и работещите в сферата на правосъдието трябва също така да бъдат подготвени да се адаптират и да реагират при безпрецедентни обстоятелства. Обучението е от основно значение, за да може органите по места да използват инструментите в оперативна обстановка. Наред с това следва да се положат всички усилия за засилване на интегрирането на принципа на равенство между половете и за по-голямо участие на жените в правоприлагането.

Ключови действия
• Подсилване на мандата на Европол • Обмисляне на изготвянето на „Кодекс за полицейско сътрудничество“ на ЕС и координация на полицията по време на криза • Укрепване на Евроюст с цел установяване на връзки между съдебните и правоприлагащите органи • Преразглеждане на Директивата за предварителната информация за пътниците • Съобщение относно външното измерение на резервационните данни на пътниците • Засилване на сътрудничеството между ЕС и Интерпол • Рамка за преговори с ключови трети държави относно обмена на информация • Подобряване на стандартите за сигурност за документите за пътуване • Обмисляне на създаването на Европейски център за иновации в областта на вътрешната сигурност

V. Заключения

В съвременния все по-неспокоен свят Европейският съюз все още се счита от много хора за едно от най-безопасните и сигурни места. Това обаче не е нещо, което може да се приема за даденост.

Новата стратегия за Съюза на сигурност поставя основите на екосистема на сигурността, която обхваща европейското общество в неговата цялост. Тя се основава на съзнанието, че сигурността представлява споделена отговорност. Сигурността е въпрос, който засяга всички. Всички държавни органи, предприятия, социални организации, институции и граждани трябва да изпълняват отговорностите си, за да направят обществата ни по-сигурни.

[130] Вж. Стратегия за равенство между половете (COM(2020) 152); Стратегия за правата на жертвите (COM(2020) 258) и Европейска стратегия за по-добър интернет за децата (COM(2012) 196).

В днешно време въпросите, свързани със сигурността, трябва да се разглеждат в много по-широка перспектива, отколкото в миналото. Погрешното разграничаване на физическата и цифровата среда трябва да бъде преодоляно. Стратегията на ЕС за Съюза на сигурност обединява пълния набор от нужди, свързани със сигурността, и се съсредоточава върху областите, които ще бъдат от най-голямо значение за сигурността на ЕС през идните години. В нея също така се признава, че заплахите за сигурността не зачитат географски граници, както и че има все по-голяма взаимосвързаност между вътрешната и външната сигурност[131]. В този контекст за ЕС ще бъде важно да си сътрудничи с международните партньори, за да осигурява защита на всички граждани на ЕС и да поддържа тясна координация с външните действия на ЕС при изпълнението на тази стратегия.

Нашата сигурност е свързана с основните ни ценности. Всички действия и инициативи, предложени в тази стратегия, ще зачитат в пълна степен основните права и нашите европейски ценности. Това са основите на нашия европейски начин на живот и те трябва да продължат да заемат централно място в цялата ни работа.

Накрая, Комисията е напълно наясно с факта, че стойността на всяка политика или действие зависи от тяхното изпълнение. Ето защо трябва да се набляга неуморно върху правилното изпълнение и прилагане на действащото и бъдещото законодателство. За тази цел ще бъде извършван мониторинг чрез редовни доклади за Съюза на сигурност и Комисията ще предоставя пълна информация на Европейския парламент, Съвета и заинтересованите страни и ще им осигурява възможност да участват във всички съответни действия. Наред с това Комисията е готова да участва и да организира съвместни дебати с институциите относно Стратегията за Съюза на сигурност, така че те заедно да направят равносметка за постигнатия напредък и същевременно да помислят съвместно по бъдещите предизвикателства.

Комисията приканва Европейския парламент и Съвета да подкрепят настоящата Стратегия за Съюза на сигурност като основа за сътрудничеството и съвместните действия в областта на сигурността през следващите пет години.

[131] Вж. Глобалната стратегия на ЕС.