ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 9.12.2020 г.
COM(2020) 797 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Първи доклад за напредъка по стратегията на ЕС за Съюза на сигурност

I ВЪВЕДЕНИЕ

Сигурността е една от основните грижи на гражданите, а неотдавнашната поредица от терористични атаки на европейска земя доказа в още по-голяма степен необходимостта от действия от страна на ЕС. На 24 юли 2020 г. Комисията прие **Стратегия на ЕС за Съюза на сигурност за периода 2020—2025 г.**[1], насочена към действия в приоритетни области, в които ЕС може да осигури добавена стойност към усилията на национално ниво. Тя се основава на напредъка, постигнат по-рано в рамките на Европейската програма за сигурност за периода 2015—2020 г.[2], и дава нова перспектива, за да се гарантира, че политиката на ЕС за сигурност отразява променящия се контекст на заплахите; че изгражда дългосрочна устойчивост; че ангажира институциите и агенциите на ЕС, правителствата, частния сектор и отделните лица в общ подход за цялото общество; и че обединява многобройните области на политиката, които имат пряко въздействие върху сигурността. Пълното зачитане на основните права е в основата на тази работа, тъй като сигурността на Съюза може да се гарантира единствено когато всеки е уверен, че основните му права се зачитат напълно.

Заплахата от транснационални терористични мрежи ясно напомня, че е особено важно действията на ЕС да бъдат координирани, за да бъдат ефективни действията за защита на европейците, утвърждаването на общите ни ценности и европейския ни начин на живот. Това е показателно за начина, по който възникващите все по-сложни трансгранични и междусекторни заплахи за сигурността придават на по-тясното сътрудничество в областта на сигурността на всички нива още по-голяма значимост. Горното се отнася за организираната престъпност или търговията с наркотици — отнася се и за света на цифровите технологии, като кибератаките и киберпрестъпността продължават да се увеличават. Всички тези предизвикателства са валидни и отвъд нашите граници и е налице ясна взаимовръзка между вътрешната и външната сигурност. Кризата с COVID-19 изостри вниманието към европейската сигурност, като постави на изпитание устойчивостта на европейската критична инфраструктура, готовността за действия при криза, стратегическите вериги за създаване на стойност и системите за управление на кризи, както и устойчивостта на нашите общества спрямо манипулативна намеса и дезинформация.

Стратегията за Съюза на сигурност включва четири стратегически приоритета за действията на равнището на ЕС: среда на сигурност, която е подготвена за бъдещето, справяне с променящите се заплахи, защита на Европа от тероризма и организираната престъпност и силна европейска екосистема на сигурността. От основно значение за стратегията е изпълнението и това е основната тема на настоящия доклад: изпълнение, което налага пълното ангажиране на националните органи на предната линия на сигурността в ЕС. Настоящият доклад е първият доклад за изпълнението по стратегията в изпълнение на поетия от Комисията ангажимент редовно да докладва за постигнатия напредък[3]. Той обхваща периода от 31 октомври

[1] COM (2020) 605.
[2] COM(2016)230.
[3] По време на изслушването на заместник-председателя Шинас пред Европейския парламент на 3.10.2019 г.

2019 г., когато бе публикуван последният доклад за напредъка на Съюза за сигурност съгласно мандата на предишната Комисия[4].

II СРЕДА НА СИГУРНОСТ, КОЯТО Е ПОДГОТВЕНА ЗА БЪДЕЩЕТО

1. *Защита и устойчивост на критичната инфраструктура*

В ежедневието си гражданите разчитат на все по-силно взаимосвързана и взаимозависима физическа и цифрова инфраструктура. Тази инфраструктура е жизненоважна за функционирането на икономиката и на обществото. Сегашният ни начин на живот не би бил възможен без надеждни доставки на енергия, предвидим транспорт, всеобхватни здравни системи или цифрово управлявана финансова мрежа. Пандемията от COVID-19 беше още по-ясно доказателство, колко е важно да бъде **осигурена устойчивост на критичните сектори и оператори**. ЕС призна общия интерес за защита на критичната инфраструктура от заплахи, независимо дали природни или предизвикани от човека бедствия, или терористични атаки. Настоящата картина на заплахите, пред които са изправени критичните инфраструктури, има широк обхват. Той включва: тероризъм, хибридни действия, кибератаки, вътрешни инциденти; заплахи, свързани с нови и нововъзникващи технологии (като безпилотни летателни апарати, 5G, изкуствен интелект); предизвикателства, свързани с изменението на климата; нарушаване на веригите за доставки; както и намеса в изборните процеси. Сега действащите правила се нуждаят от модернизиране и разширяване[5]. Те трябва да изместят фокуса от защитата към устойчивостта, като внесат повече последователност и съгласуваност в обхванатите сектори и бъдат съсредоточени върху критични субекти, предоставящи основни услуги.

Това ще бъде целта на предстоящите предложения за насърчаване на устойчивостта на **физическите и цифровите инфраструктури**. Общата цел е чрез създаване на стабилен капацитет за предотвратяване, откриване, реагиране и смекчаване на заплахи, както и за готовност за действие в криза да се повиши готовността на национално равнище и на равнището на ЕС. Чрез съществуващото законодателство беше засилено и подобрено управлението на риска в критични сектори; действията в тази насока трябва да бъдат засилени. Основна цел на преразгледаната директива за критичната инфраструктура ще бъде да се насърчи високо общо ниво на устойчивост в достатъчен набор от ключови сектори. По подобен начин актуализирането на Директивата за мрежова и информационна сигурност (директивата за МИС) ще има за цел да се постигне по-голяма съгласуваност при идентифицирането от страна на държавите членки на „операторите на основни услуги“[6]. В по-общ план, макар да е постигнат значителен напредък, възможностите за постигане на киберсигурност в държавите членки продължават да бъдат различни, поради което при преразглеждането целта ще бъде да се насърчи киберсигурността като цяло[7]. Резултатът ще бъде по-обширен и последователен подход към устойчивостта на физическата и цифровата инфраструктура.

---

[4] COM(2019)552.

[5] Директива 2008/114/ЕО и Директива (ЕС) 2016/1148.

[6] COM(2019)546. Комисията проведе също така обществена консултация (7 юли—2 октомври 2020 г.) и посещения във всички държави членки с цел проверка на съответствието при прилагането на директивата посредством срещи с оператори и национални органи.

[7] COM(2019)546.

С напредването на действията към тази по-съгласувана рамка, те се допълват от **секторните инициативи** и се насочват към специфичните уязвимости. Конкретните предизвикателства пред киберсигурността в енергийния сектор сега се посрещат въз основа на препоръката на Комисията от 2019 г.[8], като се вземат предвид специфичните характеристики на сектора като изискванията за работа в реално време, риска от каскадни ефекти и съчетаването на заварени системи с нови технологии. Продължава работата по специален мрежов код за киберсигурност на трансграничните потоци на електроенергия, както и за устойчивост и киберсигурност на критична енергийна инфраструктура. Отново беше стартирана Тематичната мрежа за защита на критичната енергийна инфраструктура, с нов фокус и цели, като първата среща в рамките на тази мрежа бе проведена през юни 2020 г. с над 100 участници онлайн. Тази мрежа осигурява платформа за насърчаване на трансграничното сътрудничество между оператори и собственици на критична енергийна инфраструктура в енергийния сектор.

За да осигури обща отправна точка за сътрудничеството между държавите членки по отношение на **готовността за справяне с рискове в електроенергийния сектор**, през септември 2020 г. Европейската мрежа на операторите на преносни системи за електроенергия представи най-подходящия сценарий при регионална криза в електроснабдяването, както е предвидено в регламента за готовност за справяне с рискове[9]. Това включва кибератаки, както и пандемия и екстремни метеорологични събития. Държавите членки ще изготвят национални сценарии за действие при криза и планове за готовност за справяне с рисковете, за да предотвратят и смекчат кризите в електроснабдяването (първите проекти трябва да бъдат представени през април 2021 г.). За да допринесат за този процес, през юни 2020 г.[10] бяха издадени набор от добри практики, базирани на внимателното наблюдение на въздействието на COVID-19 върху енергийния сектор чрез Групата за координация в областта на електроенергетиката, Координационната група по природния газ и Групата за координация в областта на нефта, както и Групата на европейските регулатори в областта на ядрената безопасност и Групата на компетентните органи на ЕС по въпросите на добива на нефт и газ в морските райони.

Нарастващата и по-сложна зависимост от цифровите процеси при предоставянето на финансови услуги изисква също така повишаване на нивото на киберсигурност във **финансовия сектор**. Въпреки че сигурността на системите за информационни и комуникационни технологии (ИКТ системите) се признава като неразделна част от управлението на риска за финансовите субекти, това все още не е изцяло отразено в регулаторната среда на ЕС за финансовите услуги. На 24 септември 2020 г. Комисията прие своя пакет от стратегии за цифровизиране на финансовите услуги в ЕС[11] с ясната цел да се справи с предизвикателствата и рисковете, свързани с цифровата трансформация, да насърчи устойчивостта, защитата на данните и подходящия пруденциален надзор. Това включва законодателно предложение относно цифровата оперативна устойчивост[12], за да се гарантира, че са налице предпазни

[8] C(2019) 2400.
[9] ОВ L 158, 14.6.2019 г, стр. 1—21.
[10] Енергийна сигурност: добри практики за справяне с рисковете от пандемия (SWD(2020) 104).
[11] https://ec.europa.eu/info/publications/200924-digital-finance-proposals_bg.
[12] COM(2020)595.

мерки за смекчаване на кибератаките и други рискове[13]. Тази инициатива допринася за един силен и жизнеспособен европейски сектор на цифровите финансови услуги и по този начин се укрепва способността на Европа да засили отворената си стратегическа независимост в областта на финансовите услуги и — чрез разширяване — капацитета си за регулиране и надзор на финансовата система, така че да защити финансовата си стабилност.

По време на мащабни извънредни ситуации високата степен на взаимозависимост между секторите и държавите изисква координирани действия за осигуряване на бърза и ефективна реакция, както и по-добри превантивни действия и готовност за подобни ситуации в бъдеще. При преразглеждането на Решението относно Механизма за гражданска защита на Съюза[14] Комисията предложи[15] разработването на **цели за устойчивост при бедствия** и **планиране на устойчивост**, като се обърне специално внимание на изграждането на дългосрочна междусекторна устойчивост на трансгранични бедствия. Предложеният нов подход за изграждане на устойчивост допълва работата по управление на риска от бедствия на национално равнище. На 26 ноември Съветът постигна споразумение за мандат за преговори за засилване на действията за предотвратяване на бедствия, готовността и реакцията въз основа на предложението на Комисията от 2 юни 2020 г.[16].

Пандемията от COVID-19 е свидетелство за въздействието на здравната криза върху сигурността на ниво на ЕС и в световен мащаб и за необходимостта от засилване на планирането за готовност и реагиране при епидемии и други сериозни трансгранични заплахи за здравето. В пакета на Комисията от 11 ноември 2020 г., озаглавен „**Изграждане на Европейски здравен съюз**: подсилване на издръжливостта на ЕС“, се определят следващите стъпки за справяне с трансграничните заплахи за здравето. Той ще осигури засилена рамка за трансгранично сътрудничество срещу всички заплахи за здравето и ще включва три законодателни предложения: да се надгради законодателството относно сериозните трансгранични заплахи за здравето и да се укрепят Европейският център за профилактика и контрол върху заболяванията (ECDC) и Европейската агенция по лекарствата (EMA). Взети заедно тези предложения ще създадат стабилна и разходно ефективна рамка, за да се поставят ЕС и държавите членки на по-сигурна основа, когато реагират на бъдещи здравни кризи.

Важен елемент за защита на ключовите европейски и национални цифрови активи е да се предложи канал за **сигурни комуникации** за критичната инфраструктура. Това се подпомага чрез създаването на мрежова инфраструктура за сигурни и устойчиви правителствени сателитни комуникации като компонент на космическата програма на ЕС.

---

[13] В предложението се определя съгласувана изходна база за изискванията за управление на риска в областта на ИКТ, докладване на инциденти в областта на ИКТ пред финансовите надзорници, цифрово тестване и споделяне на информация. Освен това в него се определя надзорна рамка в европейски мащаб за доставчици трети страни на критични ИКТ услуги.

[14] Решение № 1313/2013/ЕС от 17 декември 2013 г. относно Механизъм за гражданска защита на Съюза.

[15] COM(2020)220.

[16] Предложение за изменение на Решение № 1313/2013/ЕС относно Механизъм за гражданска защита на Съюза — Мандат за преговори с Европейския парламент.

2. ***Киберсигурност***

Ползите от цифровата трансформация са ясни, но е факт, че тя неизбежно е съпровождана с увеличаване на потенциалните уязвимости[17]. Критичната инфраструктура често е обект на все по-сложни кибератаки[18]. Поради това за **киберсигурността** трябва да бъдат загрижени не само политиците, но и всеки, който работи или комуникира онлайн.

За да се увеличат доверието в цифровите продукти, процеси и услуги и тяхната сигурност, с Акта за киберсигурността от юни 2019 г. беше създадена **рамка на ЕС за сертифициране на киберсигурността**. Комисията поиска от ENISA, Агенцията на Европейския съюз за киберсигурност, да изготви две схеми за сертифициране на киберсигурността и подготовката им е в ход. Тази работа включва също така националните органи за сертифициране на киберсигурността, сектора, потребителите, органите по акредитация, стандартизация и сертифициране, както и Европейския комитет по защита на данните.

Една от тези схеми е схемата за **облачни услуги** в подкрепа на сигурен и надежден пазар на облачни услуги. Тя е ключов елемент в **Стратегията на ЕС за данните**, приета през февруари 2020 г.[19]. Това би създало обща база за сигурност за облачните услуги в различните сектори въз основа на най-високия общ знаменател на съществуващите (европейски и международни) стандарти, схеми и практики. Това ще бъде ключов елемент в свободния поток от данни в ЕС[20]. Чрез схемата ще бъде насърчено и въвеждането на облачни технологии, като на потребителите, по-специално на малките и средните предприятия и публичната администрация, се предостави разумно уверение за нивото на сигурност, когато използват облака.

Както беше подчертано в стратегията за Съюза на сигурност, предвид въвеждането в момента на територията на ЕС на инфраструктурата за 5G и потенциалната

[17] Агенция на Европейския съюз за киберсигурност (ENISA) Картина на заплахите 2020 г.: Кибератаките стават все по-сложни, целенасочени, широко разпространени и неоткрити.

[18] След избухването на пандемията агенциите на ЕС и държавите членки установяват значителен ръст на кибератаките, включително срещу сектора на здравеопазването.

[19] COM(2020)66.

[20] Регламент (ЕС) 2018/1807.

зависимост на много от критичните услуги от 5G мрежите, последиците от системни и широкообхватни прекъсвания на услугите могат да бъдат особено сериозни. Резултатът беше следствие от общите усилия на държавите членки да разработят и въведат адекватни мерки за сигурност. След Препоръката на Комисията от март 2019 г. относно **киберсигурността на 5G мрежите**[21] държавите членки завършиха националните оценки на риска, които бяха отразени в координиран доклад на ЕС за оценка на риска[22], в който се посочват предизвикателствата пред сигурността на 5G мрежите. На тази основа на 29 януари 2020 г. групата за сътрудничество по въпросите на мрежовата и информационна сигурност (МИС)[23] публикува **Инструментариум на ЕС за сигурността**[24], в който се посочват необходимите стратегически и технически мерки. Инструментариумът включва мерки за засилване на изискванията за сигурност за операторите на мобилни мрежи (ОММ), осигуряване на многобройни доставчици за отделни ОММ, оценка на рисковия профил на доставчиците и прилагане на ограничения за считаните за високорискови доставчици. Комисията ще подкрепи прилагането на инструментариума, като изцяло използва компетенциите и средствата, с които разполага[25], включително телекомуникациите и правилата за киберсигурност; координацията в областта на стандартизацията, както и сертифицирането на равнището на ЕС; и рамката на ЕС за преки чуждестранни инвестиции[26].

Групата за сътрудничество по въпросите на МИС публикува доклад за напредъка по прилагането на мерките от инструментариума през юли 2020 г.[27]. В него се отбелязва, че по-голямата част от държавите членки вече са приели или са в процес на прилагане на мерките, препоръчани в инструментариума. Мерките, при които изпълнението е с по-малък напредък, включват намаляване на риска от зависимост от високорискови доставчици и разработване на стратегии за използване на различни доставчици както на равнището на дружествата, така и на национално ниво.

През последните няколко месеца институциите на ЕС и държавите членки реагираха на повишеното ниво на риска за киберсигурността, породено от **кризата с COVID-19**, като засилиха обмена на информация и повишиха степента на готовност за потенциална киберкриза. Сътрудничеството с ЕС беше засилено в ключови форуми (Групата за сътрудничество по въпросите на МИС и мрежата на екипите за реагиране при инциденти с компютърната сигурност (CSIRT), както и чрез нови форми на координация и инструменти за обмен на информация[28]. През септември

---

21 COM(2019)2335.

22 Доклад относно координираната оценка на ЕС на риска за киберсигурността при мрежите от пето поколение (5G).

23 Групата за сътрудничество по въпросите на МИС е създадена, за да осигури стратегическо сътрудничество и обмен на информация между държавите — членки на ЕС, в областта на киберсигурността.

24 https://ec.europa.eu/digital-single-market/en/news/cybersecurity-5g-networks-eu-toolbox-risk-mitigating-measures.

25 COM(2020)50.

26 Регламент (ЕС) 2019/452. В него се съдържат също изрични препратки към „критична инфраструктура“ (както и „критични технологии“) в по-широк смисъл като „фактори, които могат да бъдат взети под внимание от държавите членки или от Комисията“ при оценяването на потенциалното въздействие на дадена инвестиция.

27 Доклад относно напредъка на държавите членки в прилагането на инструментариума на ЕС за киберсигурност на 5G мрежите.

28 Институциите и органите на ЕС проведоха среща в работната група за киберсигурност, свързана с COVID-19, и стартираха изготвянето на седмичен доклад за ситуационна осведоменост и анализ

2020 г. имаше второ симулационното учение Blueprint на оперативно ниво (Blue OLEx)[29], при което беше стартирана и инициативата „Cyber Crisis Liaison Organisation Network“ (CyCLONe) („Мрежа на организациите за връзка при киберкризи“ (CyCLONe) на държавите членки, която е допълнителна мярка за пилагане на плана за бързо реагиране при извънредни ситуации за мащабни, трансгранични киберинциденти или кризи[30].

В глобалното киберпространство кибератаките и заплахите често са с произход извън ЕС. За да се справят ефективно с тези предизвикателства, ЕС и държавите членки си сътрудничат за подобряване на международната сигурност и стабилност в киберпространството, насърчаване на отговорно поведение на държавите, повишаване на устойчивостта в световен мащаб и подобряване на осведомеността относно киберзаплахите и злонамерените кибердейности, включително с международни партньори[31]. На 30 април 2020 г. върховният представител публикува декларация от името на ЕС, в която осъжда злонамереното поведение в киберпространството и изразява солидарност с жертвите[32].

На 30 юли 2020 г. Съветът прие **първите в историята на ЕС киберсанкции** спрямо шест физически лица и три образувания, отговорни за кибератаки или участващи в тях. Те включват опита за кибератака срещу ОЗХО (Организация за забрана на химическото оръжие) и атаките, публично известни като „WannaCry“, „NotPetya“ и „Operation Cloud Hopper“. На 22 октомври 2020 г. Съветът наложи санкции срещу други две лица и едно образувание, които са били отговорни или са участвали в кибератаката срещу германския федерален парламент. Тези решения бяха взети вследствие на непрекъснатите сигнали от страна на ЕС и държавите членки за необходимостта от предотвратяване, обезсърчаване, възпиране и реагиране на злонамерени кибердейности, включително чрез използване на неговия режим на киберсанкции като част от инструментариума за кибердипломация от 2017 г.[33].

Продължава напредъкът по преговорите между съзаконодателните органи относно новите правила за износ, които ограничават продажбата на стоки за

по сектори. ENISA и Европол стартираха кампании за това как да запазим киберситурността по време на пандемията от COVID-19. Екипът за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU) издаде насоки за това как да бъдат създадени защитени частни виртуални мрежи. През лятото на 2019 г. групата за сътрудничество създаде нов работен поток, посветен на киберсигурността в областта на здравеопазването, и Комисията и ENISA стартираха Център на ЕС за споделяне и анализ на здравна информация.

29 https://www.enisa.europa.eu/news/enisa-news/blue-olex-2020-the-european-union-member-states-launch-the-cyber-crisis-liaison-organisation-network-cyclone.

30 C(2017) 6100.

31 ЕС насърчава стратегическата рамка за предотвратяване на конфликти, стабилност и сътрудничество в киберпространството, включително чрез участие на ЕС в дискусиите на ООН относно киберпространството. Два важни форума са отворената група за развитието в областта на информацията и телекомуникациите в контекста на международната сигурност и групата от правителствени експерти (ГПЕ) за насърчаване на отговорно поведение на държавите в киберпространството. Въпросите включват въздействието на международното право, прилагането на договорени необвързващи доброволни норми за отговорно поведение на държавите и мерки за изграждане на доверие, както и прилагането чрез целенасочено изграждане на капацитет.

32 https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/.

33 Решения на Съвета (ОВППС) 2020/1127, 2020/1537 и 2020/651 като част от 9916/17.

кибернаблюдение на режимите, в които се погазват правата на човека, в цял свят[34]. След като бъдат приети, тези правила ще доведат до по-отговорна, конкурентоспособна и прозрачна търговия с изделия с двойна употреба[35]. Предложените изменения, необходими в резултат на технологичното развитие и нарастващите рискове за сигурността, включват нови критерии за предоставяне или отхвърляне на разрешения за износ за определени артикули.

3. Защита на обществените пространства

Както е признато в програмата на ЕС за борба с тероризма[36], защитата на обществените пространства чрез изграждане на устойчивост срещу заплахи за сигурността остава ключов компонент в работата за постигане на ефективен и истински Съюз за сигурност. Комисията работи с широк кръг публични и частни заинтересовани страни за изготвянето на насоки и предоставянето на практическа подкрепа и финансиране[37] в съответствие с **Плана за действие за 2017 г. за подкрепа на защитата на обществените пространства**[38] и набора от добри практики за 2019 г. за подкрепа на защитата на обществените пространства[39]. Както е посочено в програмата на ЕС за борба с тероризма, Комисията ще засили подкрепата си за местните и регионалните органи, които играят ключова роля в защитата на обществените пространства и предотвратяването на радикализацията. Това ще включва изготвяне на протокол на ЕС за градската сигурност и устойчивостта за градовете, в който ще бъдат определени основните принципи и целите за местните органи в тези области.

Тъй като терористичните атаки стават все по-насочени към **местата за поклонение**, специален акцент се поставя върху сътрудничеството между публичните органи и религиозните лидери и конгрегации, с цел подобряване на нивото на осведоменост относно сигурността и подпомагане на прилагането на добри практики и обучение в местата за поклонение. Прилагането на най-обикновени мерки може да стане разделителна линия между живота и смъртта. През октомври 2019 г. синагога в Хале беше обект на терористична атака. Наличието на блиндирана врата, паник бутон и охранителни камери помогнаха за спасяването на човешки живот.

За допълнителна подкрепа на засилените мерки за сигурност в обществените пространства, по-конкретно на местата за поклонение, през 2020 г. Комисията предостави 20 милиона евро на ръководени от заинтересованите страни проекти.

Комисията също така работи за реагиране на **възникващите рискове за обществените пространства**, включително **безпилотните летателни системи**

---

[34] COM(2016)616. Предложението на Комисията има за цел да бъде изменен и преработен Регламент 428/2009, с който се въвежда режим на Общността за контрол на износа, трансфера, брокерската дейност и транзита на изделия и технологии с двойна употреба.

[35] Това са широка гама стоки, материали, софтуер и технологии, които могат да се използват както за граждански, така и за военни цели.

[36] COM (2020) 795.

[37] Поканата за представяне на предложения на фонд „Вътрешна сигурност“ за 2019 г. включва „Secu4All“ — за разработване на цялостен цикъл за обучение за местните органи, за да се осигури на гражданите безопасна градска среда, и „DroneWISE“ — за засилване на готовността на службите за първоначално реагиране за противодействие на враждебни безпилотни летателни апарати. През 2020 г. ще се проведе нова покана, в размер на 12 милиона евро, за набиране на предложения за защита на обществените пространства.

[38] COM(2017)612.

[39] SWD(2019) 140.

(БЛС). Макар че безпилотните летателни апарати осигуряват значителни икономически възможности и възможности за заетост, те представляват и значителен риск за обществените пространства, критичната инфраструктура и други чувствителни обекти, като например затворите. Приетите неотдавна правила[40] на ЕС в тази област намаляват този риск, като повишават сигурността на операциите с безпилотни летателни апарати. От януари 2021 г. операторите на безпилотни летателни апарати също ще трябва да се регистрират при националните органи. Този режим може да бъде допълнен от **регулаторна рамка за системата „U-space“**, европейската автоматична система за управление на движението[41], за да се осигурят по-безопасни и по-сигурни операции с безпилотни летателни апарати. Чрез комбинирането на тези стъпки ще се попречи на хората да управляват безпилотни летателни апарати в ограничени зони и ще се помогне при идентифицирането и преследването на нарушителите.

Комисията работи също така, за да окаже подкрепа на правоприлагащите органи, операторите на критична инфраструктура, организаторите на масови събития и други заинтересовани страни при противопоставянето на употреба на безпилотни летателни апарати, при която липсва съдействие, например като сътрудничи с Европейската агенция за авиационна безопасност за разработване на **добри практики, чрез които да се помогне на заинтересованите страни на летищата** да реагират на инциденти с безпилотни летателни апарати, за които липсва разрешение, улеснява по-хармонизираните **усилия за тестване на контрамерки** в целия ЕС и разработва практически наръчник за заинтересованите страни, насочен към градския контекст.

В **Европейското цифрово есенно училище за защита на обществените пространства**, организирано от Съвместния изследователски център на Комисията през месец октомври 2020 г., участваха над 200 специалисти по градоустройство и публични и частни оператори на обществените пространства. По време на сесиите бяха разгледани разнообразни теми, като например как да се осигури защита срещу взривове и нападения с превозни средства, да се смекчат заплахите, породени от враждебни безпилотни летателни апарати в градски условия, и да се използват технологии за наблюдение и откриване.

Комисията също продължи да подкрепя активно **Партньорството за сигурност на обществените пространства**, стартирано през януари 2019 г. в рамките на Програмата на ЕС за градовете, което публикува своя нов план за действие[42] за осигуряване на сигурност в градски условия на различни нива на управление. Действията включват създаването на рамка за инструмент за самооценка, препоръки за изготвяне на политики, многостепенно управление и финансиране, иновации чрез интелигентни решения и технологии, в това число концепцията за сигурност при проектирането, предотвратяването на заплахи за сигурността и социалното приобщаване. Партньорството вече ще навлезе в етапа на изпълнение.

Чрез четвъртата покана за иновативни дейности за градско развитие беше предоставена и подкрепа за подобряване на сигурността на обществените

[40] Регламент за изпълнение (ЕС) 2019/947 на Комисията.

[41] В този смисъл Комисията може да внесе регламент за изпълнение, който ще бъде приет в рамките на процедура за проверка, включваща комитета за безопасност на въздухоплаването.

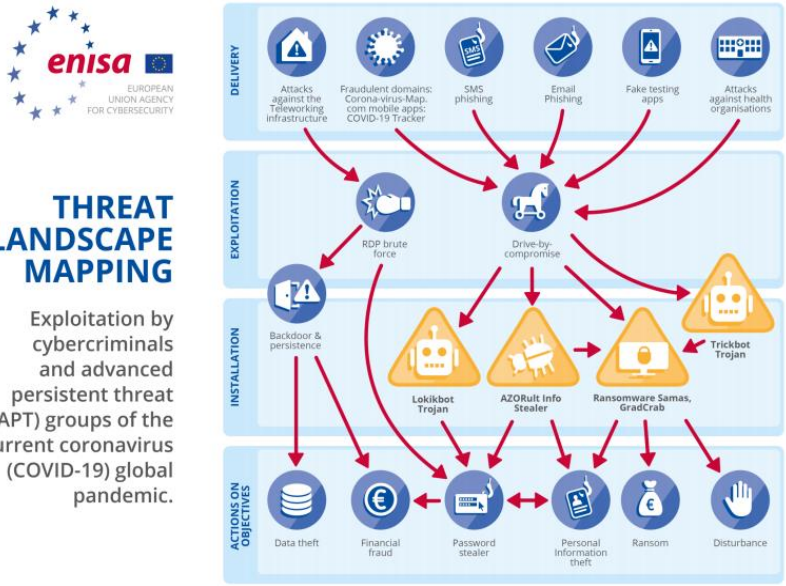
[42] Планът за действие е приет и е достъпен на Futurium: https://ec.europa.eu/futurium/en/security-public-spaces/security-public-spaces-partnership-final-action-plan-0.

пространства на местно ниво. Избрани бяха три града, които чрез финансиране от Европейския фонд за регионално развитие тестват нови решения по въпросите на сигурността в градски условия (Пирея в Гърция, Тампере във Финландия и Торино в Италия).

Що се отнася до реагирането, Комисията също така разработи европейска рамка за подобряване на готовността и реагирането при масови инциденти с масови поражения от изгаряне, като се използва цялостният европейски капацитет за грижи при изгаряне за лечение на пациенти чрез сътрудничество на равнището на ЕС. Механизмът за гражданска защита на Съюза може да се използва за подпомагане на голям брой пациенти със сериозни увреждания от изгаряне, като се осигурява достъп до легла за пациенти с изгаряния в специализирани лечебни центрове, експерти за оценка на изгарянията и капацитет за медицинска евакуация.

III СПРАВЯНЕ С ПРОМЕНЯЩИТЕ СЕ ЗАПЛАХИ

1. *Киберпрестъпност*



Недостатъците на киберсигурността често се използват от престъпниците. Това стана по-ясно от всякога по време на кризата с COVID-19. Ръст бележи „класическата“ киберпрестъпност, при която се използват злонамерения софтуер и софтуера за изнудване (т.е. за кражба на лични данни и данни за плащания или за изнудване на жертви), както и разпространението на нови уебсайтове, които примамват потребителите да инсталират злонамерен софтуер. Извършени бяха кибератаки срещу здравна и научноизследователска инфраструктура, при които бяха блокирани ИКТ системи, които могат да бъдат отключени само срещу заплащане на откуп или с достъп до информация за разработването на ваксини[43]. Наблюдава се и значителен ръст на сексуалното насилие над деца и материалите за сексуално насилие над деца[44].

Реагирането по ефективен начин срещу киберпрестъпността изисква наличието на стабилна рамка за наказателни разследвания и съдебно преследване, като ключова първа стъпка е пълното транспониране и прилагането на директивата относно **атаките срещу информационните системи**[45]. Комисията наблюдава действията на България, Италия, Португалия и Словения след откриването на производства за

[43] Оценка на заплахите от организирана престъпност, ползваща се от интернет (IOCTA) 2020 г., октомври 2020 г.

[44] Доклад на тема: Експлоатация на изолацията: Извършители и жертви на сексуално насилие над деца в интернет по време на пандемията от COVID-19, Европол, 19.6.2020 г.

[45] Директива 2013/40/ЕС.

установяване на неизпълнение на задължения през 2019 г. Необходим е напредък и по прилагането на **Директивата от 2011 г. относно борбата със сексуалното насилие и със сексуалната експлоатация на деца**[46]. Областите, в които все още са необходими усилия, включват превенцията, материалното наказателно право, мерките за помощ, подкрепа и защита на децата жертви. От 2018 г. насам Комисията е открила производства за установяване на неизпълнение на задължения срещу 25 държави членки[47].

На 24 юли 2020 г. Европейската комисия прие **стратегия на ЕС за по-ефективна борба срещу сексуалното насилие над деца**[48], която има за цел да се реагира по ефективен начин от страна на ЕС срещу престъплението сексуално насилие над деца. Възникна и едно специфично предизвикателство, тъй като от 21 декември 2020 г. някои онлайн комуникационни услуги, като например уеб поща или услуги за съобщения, ще попаднат в обхвата на Директивата за правото на неприкосновеност на личния живот и електронни комуникации и са обхванати от преработените определения в Европейския кодекс за електронните съобщения. В резултат на това съществува явен риск доставчиците на тези услуги, които предприемат някои важни доброволни дейности с цел откриване, справяне и докладване на сексуално насилие над деца онлайн, сега да трябва да спрат да го правят. Поради това Комисията предложи **регламент**[49], с който да се допуска тези доброволни дейности да бъдат продължени при определени условия, докато бъде прието дългосрочно законодателно решение. Комисията работи по предложение за такова решение, което е планирано да бъде прието през 2021 г.

Европейската мрежа на центровете за киберсигурност и компетентният център за иновации и операции създадоха **Алианс за кибернетична отбрана, свързана с COVID-19**, с цел разработване на иновативни подходи за противодействие на престъпления, свързани с COVID-19. През април 2020 г. беше създадена специална платформа EIC COVID[50], която да свързва гражданското общество, иноваторите, партньорите и инвеститорите в цяла Европа за целите на разработването на иновативни решения.

С цел да се осигури по-ефективно преследване на престъпленията и с оглед на важността на електронната информация и доказателствата в наказателните разследвания, правоприлагащите и съдебните органи следва бързо да получават достъп до такава информация и доказателства за своите криминални разследвания. Това беше признато в Съвместното изявление на министрите на вътрешните работи от ЕС от 13 ноември 2020 г.[51]. Европол, Евроюст и Европейската съдебна мрежа публикуваха на 1 декември 2020 г. втория си „Доклад по проект SIRIUS относно ситуацията с цифровите доказателства в ЕС“. В доклада се подчертава повишената

---

[46] Директива 2011/93/ЕС.

[47] Австрия, Белгия, България, Германия, Гърция, Естония, Ирландия, Испания, Италия, Латвия, Литва, Люксембург, Малта, Нидерландия, Полша, Португалия, Румъния, Словакия, Словения, Унгария, Финландия, Франция, Хърватия, Чешката република, Швеция.

[48] COM(2020)607.

[49] COM(2020)568.

[50] Комисията, заедно с Европейския съвет за иновации и държавите членки, беше домакин на паневропейския хакатон + мачатон „ЕС срещу вируса“ (Hackathon + Matchathon EUvsVirus) https://covid-eic.easme-web.eu/.

[51] Съвместна декларация на министрите на вътрешните работи на ЕС относно неотдавнашните терористични атаки в Европа, 13.11.2020 г., 12634/20.

значимост на електронните доказателства при наказателните разследвания[52]. Европейският парламент все още не е установил своята позиция по предложенията на Комисията относно **трансграничния достъп до електронни доказателства**[53] от април 2018 г., поради което преговорите между съзаконодателните органи тепърва предстои да започнат. Забавянето на приемането на тези предложения задържа работата на правоприлагащите и съдебните органи и усложнява текущите усилия за установяване на съвместими правила за трансграничен достъп до електронни доказателства чрез международни договорености[54].

На международно ниво Комисията участва от името на ЕС в продължаващите преговори по втория допълнителен протокол към Конвенцията на Съвета на Европа **от Будапеща за престъпленията в кибернетичното пространство**. С този протокол на компетентните правоприлагащи органи ще бъдат осигурени засилени, широкообхватни инструменти за трансгранично сътрудничество за разследване и преследване на киберпрестъпления и други тежки форми на престъпления, включително за пряко сътрудничество с доставчиците на услуги. Тъй като при повечето от тези разширени и засилени начини за сътрудничество ще се разчита на обмена на лични данни, от съществено значение е в бъдещия протокол да бъдат предвидени подходящи предпазни мерки за защита на данните не само от гледна точка на основните права, но и за да се гарантират правната сигурност, взаимното доверие и ефективността на оперативното сътрудничество в областта на правоприлагането.

Преговорите следва да приключат през 2021 г. Успоредно с това, в допълнение към мандата, получен от Съвета по правосъдие и вътрешни работи през миналата година, Комисията преговаря за **споразумение между ЕС и САЩ за трансграничен достъп до електронни доказателства**. То би допълнило предложените вътрешни правила на ЕС за пряко трансгранично сътрудничество с доставчиците на услуги чрез премахване на конфликтите на правото и осигуряване на общи правила и предпазни мерки. Официалните преговори започнаха на 25 септември 2019 г., като вече са проведени няколко кръга преговори. Резултатът от преговорите обаче зависи до голяма степен от постигнатия напредък по отношение на вътрешните правила за електронни доказателства.

Що се отнася до **задържането и използването на данни за целите на правоприлагането**, Комисията предприе стъпки въз основа на предходното

[52] Според доклада обемът на трансграничните искания, дадени от органите на ЕС на доставчици на онлайн услуги, се е увеличил значително през 2019 г., като по-голямата част от тях са издадени от Германия (37,7 % от исканията), Франция (17,9 %) и Обединеното кралство (16,4 %). Броят на исканията за достъп до електронни данни се е удвоил в Полша и почти се е утроил във Финландия. Освен това исканията за разкриване при извънредни ситуации са се увеличили с близо 50 % за една година.

[53] COM/2018/226 и COM/2018/225.

[54] Например на 27 декември 2019 г. Общото събрание на ООН (ОС на ООН) прие Резолюция 74/247 относно „Противодействие на използването на информационни и комуникационни технологии за престъпни цели“, с която се създава отворена *ad hoc* междуправителствена комисия от експерти, натоварена да разработи цялостна международна конвенция за киберпрестъпността. ЕС не подкрепя създаването на нов международен правен инструмент за киберпрестъпността, тъй като в Конвенцията от Будапеща за престъпленията в кибернетичното пространство вече е осигурена всеобхватна и многостранна правна рамка. През юли 2020 г. държавите — членки на ООН, се съгласиха да отложат първите стъпки: ЕС допринесе за този процес посредством обща позиция (док. 7677/2/20).

решение по делото *Tele2/Watson*[55] от 2016 г., като проведе експертни консултации със съответните доставчици на услуги, полицията и съдебните органи, гражданското общество, органите за защита на данните, академичните среди и агенциите на ЕС. Анализите се базираха и на проучване на практиките за задържане на данни от доставчиците на електронни съобщителни услуги и нуждите и практиките на правоприлагащите органи за достъп до данни, идентифициране на съответните технологични предизвикателства и прегледа на националните правни рамки[56]. При тази работа стана явна необходимостта правоприлагащите органи да получават достъп до данни, за да изпълняват по-ефективно своите задачи.

На 6 октомври 2020 г. Съдът на Европейските общности постанови решения[57] по отношение на националното законодателство на Белгия, Франция и Обединеното кралство относно запазването, предаването и достъпа до комуникационни данни без съдържание за целите на правоприлагането и националната сигурност. Комисията ще направи оценка на наличните варианти, за да се гарантира, че терористите и други престъпници могат да бъдат идентифицирани и проследявани, като същевременно зачита правото на ЕС, както се тълкува от Съда на ЕС, като вземе предвид и други висящи пред Съда дела по този въпрос.

Друг важен елемент в борбата с киберпрестъпността е работата за осигуряване на наличността и точността на данните за регистрация на имена в интернет („**информация WHOIS**“) в съответствие с усилията на Интернет корпорацията за присвоени имена и адреси (ICANN). Целта на проведените обсъждания е да се гарантира, че онези, които търсят легитимен достъп, включително правоприлагащите органи и операторите по киберсигурността, получават ефективен достъп до общите данни за регистрация на домейни от първо ниво при пълно зачитане на приложимите правила за защита на данните. Окончателните препоръки за нова политика за WHOIS бяха публикувани на 10 август 2020 г. и в момента са в процес на преглед, преди да бъде взето решение от Съвета на ICANN. Комисията ще проучи заключенията от прегледа и ще разгледа дали отразяват в достатъчна степен защитата на данните и съображенията от обществен интерес за предоставяне на ефективен достъп на правоприлагащите органи и операторите по киберсигурност.

2. Съвременно правоприлагане

Тъй като технологиите продължават да променят почти всеки сектор на обществото, включително сигурността, правоприлагащите органи и съдебната система трябва да бъдат запознати с нововъведенията. Интегрирането на изкуствен интелект, големите информационни масиви и високопроизводителните изчислителни технологии в политиката за сигурност, като същевременно не се отслабва ефективната защита на основните права, е от съществено значение за повишаването на безопасността и сигурността.

Комисията работи по редица ключови работни направления[58]. На 25 ноември 2020 г. Комисията предложи[59] Акт за управление на данните — рамка за улеснено

---

[55] Решение на Съда от 21 декември 2016 г. по съединени дела *Tele2 Sverige AB и Watson и други,* C-203/15 и C-698/15.

[56] https://data.europa.eu/doi10.2837/26288

[57] Решения на Съда по дело C-623/17, Privacy International, и по съединени дела C-511/18, La Quadrature du Net и други, C-512/18, French Data Network и други, и C-520/18, Ordre des barreaux francophones et germanophone и други.

[58] Включително Стратегията на ЕС за данните (вж. по-горе).

споделяне и повторно използване на лични и нелични данни за целите на иновациите и развитието. Така ще бъдат обхванати промишлеността и публичните органи чрез виртуални или физически пространства с данни по сектори. По този начин националните правоприлагащи органи ще получат достъп до данни, съхранявани в други пространства с данни за техните собствени иновационни цели. В същото време няма да бъде разрешен достъпът до данни, съхранявани от националните органи за правоприлагане и сигурност, освен ако такъв достъп не е разрешен в европейското или националното право. Националните органи за правоприлагане и сигурност също могат да се възползват, ако отделни субекти на данни доброволно предоставят свои данни за благото на обществото и единствено за целите на научните изследвания.

Работи се също така по изготвянето на нова инициатива за **изкуствения интелект (ИИ)** след публикуването на Бялата книга за ИИ[60]. Освен че се признават възможностите, които технологията на ИИ предлага за повишаване на сигурността и благосъстоянието на гражданите и обществото като цяло, в Бялата книга също така се идентифицират редица рискове — като киберзаплахите, рисковете за личната сигурност или загубата на свързаност. В обществената консултация основните опасения, посочени от участниците, са свързани с възможността ИИ да нарушава основните права и риска да доведе до дискриминация[61]. В съобщението „Изграждане на доверие в ориентирания към човека изкуствен интелект“[62] Комисията подчертава необходимостта системите за ИИ да бъдат устойчиви както на явни атаки, така и на прикрити опити за манипулиране на данни или алгоритми, както и да се предприемат стъпки за намаляване на този риск.

Криптирането играе фундаментална роля за осигуряването на силна киберсигурност и ефективна защита на основни права като неприкосновеността на личния живот, включително поверителността на съобщенията и защитата на личните данни, както и за осигуряване на доверие в услуги и продукти, базирани на технологии за криптиране, като например решенията за цифрова самоличност. В същото време криптирането може да се използва и за скриване на престъпления от правоприлагащите и съдебните органи, което затруднява разследването, разкриването и наказателното преследване. Държавите членки в Съвета призоваха за решения, които позволяват на правоприлагащите и съдебните органи да получават законен достъп до цифрови доказателства при пълно зачитане на поверителността, защитата на данните и гаранциите за справедлив съдебен процес[63]. Комисията ще работи с държавите членки, за да набележи правни, оперативни и технически решения за законен достъп до електронна информация в криптирана среда, чрез която се поддържа сигурността на съобщенията.

Практическите стъпки, които се прилагат, включват **платформа за декриптиране** в Европол, за да се помогне на правоприлагащите органи да получават законен достъп до криптирана информация на устройства, иззети в хода на криминални

---

59 COM(2020)767.
60 COM(2020)65.
61 Съответно 90 % и 87 % от респондентите считат тези опасения за важни или много важни.
62 COM(2019)168.
63 ST 13084 2020 — Резолюция на Съвета относно криптирането — Сигурност чрез криптиране и въпреки него.

разследвания[64]. Европейската група за обучение и образование в областта на киберпрестъпността разработи пилотни модули за обучение, които ще бъдат включени в работата на Агенцията на Европейския съюз за обучение в областта на правоприлагането (CEPOL). Създадена е мрежа от звена на държавите членки с експертни познания в областта на криптирането, чрез които да се споделят най-добри практики и опит и да се подпомогне развитието на набор от технически и практически инструменти.

Системата за цифров обмен на електронни доказателства (eEDES) ще включва инструмент за сигурен, бърз и ефективен трансграничен обмен на европейски заповеди за разследване, искания за взаимопомощ и доказателства в цифров формат. Тя следва постепенно да се обогатява и разширява и към други инструменти за съдебно сътрудничество по наказателноправни въпроси, а бъдещият ѝ обхват ще бъде определен в законодателно предложение за цифровизация на процедурите за съдебно сътрудничество, планирано за 2021 г.[65].

3. Борба с незаконното съдържание онлайн

Радикализацията, водеща до насилнически екстремизъм и тероризъм, е многоизмерно и трансгранично явление, което беше повлияно положително от бързия растеж на интернет. Интернет продължава да се използва за радикализиране и набиране на уязвими лица. През юли звеното на Европол за сигнализиране за незаконно съдържание в интернет премахна 2000 връзки към терористично съдържание — включително ръководства и уроци за това как да се извърши атака. Доказателствата за ролята на интернет за радикализирането и рекламирането на престъпленията на участващите в нападенията във Франция и в Австрия изведоха на още по-преден план необходимостта от ясна законодателна рамка за предотвратяване на разпространението на терористично съдържание онлайн, като същевременно се поддържат ефективни предпазни мерки за защита на основните права. През последните седмици се засилиха преговорите между Европейския парламент и Съвета относно предложения **регламент за предотвратяване на разпространението на терористично съдържание онлайн**[66]. Завършването на тези преговори, по-специално със създаването на новия и ефективен оперативен инструмент за заповеди за премахване за трансгранично елиминиране на терористично съдържание в рамките на един час или по-малко от получаването на тези заповеди, е от решаващо значение за справянето с терористичното съдържание, включително съдържанието, което допринася за радикализация.

Междувременно **интернет форумът на ЕС** продължава да действа като катализатор за действие, като осигурява една основна платформа, която обединява държавите членки и промишлеността, за да се предотврати разпространението на терористично съдържание онлайн и да се противодейства на радикализиращите послания. Форумът работи по разработването на референтен списък със забранени символи и групи в държавите членки, които биха могли да допринесат за политиките за модериране на съдържанието на платформата.

---

[64] Този проект на стойност 6 милиона евро се подкрепя и от Съвместния изследователски център на Комисията.

[65] Съобщение относно цифровизацията на правосъдието в ЕС, COM (2020) 710, 2 декември 2020 г.

[66] COM(2018)640.

Обхватът на дейността на интернет форума на ЕС бе разширен, за да обхване и **сексуалното насилие над деца онлайн**. Форумът ще осигури общо пространство за споделяне на най-добри практики и идентифициране на пречките, пред които са изправени както частните, така и публичните участници, за да се увеличи взаимното разбирателство и да се намерят решения заедно. Той дава възможност също така за политическа координация на високо равнище, за да се постигне максимално увеличаване на ефективността и ефикасността на действията. В рамките на интернет форума на ЕС беше създадена техническа експертна процедура, в която участват академичните среди, промишлеността, публичните органи и организациите на гражданското общество, за да се картографират и да бъде направена предварителна оценка на възможните технически решения за откриване и докладване на сексуално насилие над деца в електронни комуникации, криптирани от край до край. Такива технически решения не следва да отслабват криптирането. Този подход допълва други елементи на борбата срещу сексуалното насилие над деца, както онлайн, така и офлайн, както е описано по-горе.

Комисията също така продължи да споделя знания и опит на ЕС като част от независимия консултативен съвет на новосъздадения **глобален интернет форум за борба с тероризма** и като съвместен ръководител, заедно с Microsoft, на работната група за реагиране при кризи. Съвместно с Европол Комисията продължи да подкрепя държавите членки в прилагането на **Протокола на ЕС за действие при кризи**. На 23 ноември 2020 г. звеното на ЕС за сигнализиране за незаконно съдържание в интернет беше домакин на второ симулационно учение за изготвянето на насоки за подобряване на оперативното реагиране и координацията в реално време между държавите членки и доставчиците на онлайн услуги.

През юни 2020 г. Комисията публикува резултатите от последното наблюдение на прилагането на **Кодекса на поведение във връзка с незаконните изказвания онлайн, пораждащи омраза**[67]. Това показа, че в рамките на 24 часа ИТ дружествата анализират средно 90 % от съдържанието, за което е подаден сигнал, и премахват 71 % от съдържанието, за което бъде счетено, че представлява незаконни изказвания, пораждащи омраза. Установени бяха обаче и недостатъци в прозрачността и обратната връзка с потребителите. Прилагането на Кодекса на поведение през последните четири години също беше включено в размисли за това какви мерки да бъдат предприети спрямо незаконното съдържание онлайн, като същевременно бъде защитена свободата на изразяване в предстоящото предложение за законодателен акт за цифровите услуги. В обръщението си за състоянието на съюза през 2020 г. президентът Фон дер Лайен съобщи също, че до края на 2021 г. Комисията ще предложи да разшири списъка с престъпления на равнище ЕС съгласно член 83, параграф 1 от ДФЕС, за да бъдат включени и престъпления от омраза и реч на омразата[68].

4. *Хибридни заплахи*

Признавайки променящия се характер на хибридните заплахи, през юли 2019 г. Съветът създаде **хоризонтална работна група за повишаване на устойчивостта и борба с хибридните заплахи**. Основната ѝ цел е да подкрепи стратегическата и

[67] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en.

[68] По-подробно е изложено в Стратегията за равнопоставеност на ЛГБТИК за 2020—2025 (COM (2020) 698).

хоризонталната координация между държавите членки в областта на устойчивостта на държавите и обществата, подобряването на стратегическата комуникация и противодействието на дезинформацията. Работата включва проследяване на проучванията на хибридните рискове[69], както отделяне на специално внимание на хибридни заплахи и дезинформация в съседните държави партньори. Дейностите на хоризонталната работна група са представени в годишен доклад, приет на 14 септември 2020 г.

През декември 2019 г. Съветът прие „Заключения относно допълнителните усилия за укрепване на устойчивостта на хибридни заплахи и за борба с тях“[70], като призовава за цялостен подход към сигурността и борбата с хибридните заплахи, който функционира във всички съответни сектори на политиката по стратегически, координиран и последователен начин. Две ключови последващи стъпки бяха предприети през юли 2020 г. Първо, службите на Комисията и Европейската служба за външна дейност (ЕСВД) подготвиха **карта на мерките и документите, свързани с действията на ЕС в отговор на хибридни заплахи**[71]. С изготвянето на такава карта се прави цялостен опис на мерките за борба с хибридните заплахи на равнище ЕС и на съответните политически документи. Тя служи като отправна точка за създаване на онлайн платформа с ограничен достъп от типа „обслужване на едно гише“ за всички мерки, свързани с хибридни заплахи, политическите и законодателните документи, както и съответните проучвания. Второ, в последния годишен **доклад относно борбата с хибридните заплахи**[72] се разглежда изпълнението, обхващащо осведомеността за състоянието, изграждането на устойчивост, готовността и реагирането при кризи, както и международното сътрудничество, и по-специално сътрудничеството между ЕС и НАТО в борбата с хибридните заплахи. Въпреки че в доклада се отбелязва известен напредък по отношение на координацията на равнище ЕС, поради безпрецедентния мащаб и разнообразието от хибридни заплахи днес са необходими допълнителни стъпки на подхода на равнище ЕС за интегриране на външното и вътрешното измерение в съгласуван поток и подкрепа на усилията на държавите членки за борба с хибридните заплахи, както и за укрепване на тяхната устойчивост.

Успоредно с това се работи по прилагането на мерките, заложени в новата стратегия за сигурност, за да бъдат интегрирани съображенията за хибридните заплахи в процеса на разработване на политики, да се разработи онлайн платформа с ограничен достъп, да се създадат изходни критерии за устойчивост на ЕС по сектори, както и да се рационализират информационните потоци за по-нататъшно подобряване на осведомеността за състоянието[73]. Това надгражда дейността на **звеното на ЕС за синтез на информацията за хибридните заплахи** (HFC), създадено в рамките на Центъра на ЕС за анализ на информация (EU INTCEN),

---

[69] Действие 1 от съвместната рамка от 2016 г. за борба с хибридните заплахи, вж. JOIN/2016/018.

[70] Заключения на Съвета 14972/19.

[71] SWD(2020) 152, Съвместен работен документ на службите, Картографиране на мерките, свързани с повишаване на устойчивостта и противодействие на хибридните заплахи.

[72] SWD(2020) 153, Съвместен работен документ на службите, 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.

[73] Например на 26 ноември 2020 г. Съвместният изследователски център предложи нова рамка за повишаване на осведомеността относно заплахите: https://ec.europa.eu/jrc/en/news/jrc-framework-against-hybrid-threats

който остава основният център на ЕС за оценка на хибридните заплахи. До днес то е изготвило над 180 писмени доклада за хибридни и киберзаплахи. Един от проектите на HFC е **„анализът на тенденциите при хибридните заплахи“**[74], в който се предоставят данни по теми като: периодичен анализ на хибридните дейности на новопоявилите се действащи лица; дейности по външно разузнаване срещу държави — членки на ЕС, институции, партньори и интереси; и хибридни държавни и недържавни участници, които се възползват от пандемията от COVID-19.

Сътрудничеството между ЕС и НАТО (в рамките на всеобхватната рамка, предвидена в съвместните декларации от Варшава и Брюксел от 2016 и 2018 г.) се засили допълнително, както беше подчертано в петия доклад за напредъка от юни 2020 г. чрез взаимодействието между персонала и постигането на конкретни резултати в областта на хибридните заплахи, киберзащитата и изграждането на капацитет[75]. Изключително важно е да се разработи единна методология за различните сектори за работата по изходните параметри на устойчивостта спрямо хибридни заплахи, за да се отговори на риска от фрагментиране и дублиране на политики, инструменти и действия. Европейският център за високи постижения в борбата с хибридните заплахи в Хелзинки също участва в това сътрудничество. Сътрудничеството с НАТО беше засилено по време на кризата с COVID-19, включително по отношение на дезинформацията, свързана с пандемията, и справянето с враждебни информационни дейности.

Като цяло в резултат на пандемията от COVID-19 бяха откроени бързо развиващи се рискове от **дезинформация** и реален риск за живота на хората[76]. На 10 юни 2020 г. Комисията и върховният представител приеха **съвместно съобщение относно COVID-19 и дезинформацията**[77], за да отбележат специфичните рискове от дезинформацията относно COVID-19 и действията, които следва да бъдат предприети. Това включва действия на големи онлайн платформи за разработване на политики за справяне със заплахата и засилено наблюдение на действията на платформите, както и специално сътрудничество чрез системата за бързо предупреждение, управлявана от ЕСВД. Пандемията предизвика повече усилия за справяне с дезинформацията и по-добра обществена осведоменост. През първата половина на 2020 г. в публичната база данни **EUvsDisinfo** на случаи на дезинформация бяха добавени 1963 нови случая на прокремълска дезинформация, от които близо една трета имат връзка с инфодемията, свързана с COVID-19. От средата на март до края на април 2020 г. над 10 000 души посещават уебсайта на ден, а общият брой на посетителите е нараснал с 400 % в сравнение със същия период на

[74] Анализът на тенденциите при хибридните заплахи е инструмент, който ще се използва заедно с националните системи за наблюдение на мащаба и интензивността на хибридните заплахи в политическата/дипломатическата, военната, икономическата, информационната, разузнавателната, кибер сферата, социалната, енергийната и инфраструктурната сфера.

[75] Сътрудничеството между служителите в областта на киберсигурността и отбраната се засили допълнително чрез работата по съгласувани концепции и доктрини, учения, обмен на информация и кръстосани брифинги.

[76] Последствията за реалния свят включват палеж на телекомуникационна инфраструктура и подвеждаща здравна информация с преки последици.

[77] JOIN(2020) 8, Съвместно съобщение, Борба с дезинформацията за COVID-19: боравене с точни факти.

2019 г. Реакцията на ЕС включваше целенасочени комуникационни кампании[78] и предоставяне на фактическа информация за пандемията.

Направените изводи са включени в разработването на **европейския план за действие за демокрация**, приет на 2 декември 2020 г.[79]. Това определя ключовите стъпки за укрепване на устойчивостта на демократичната структура на ЕС чрез насърчаване на свободни и честни избори, справяне с пречките пред свободните и независими медии и борба с дезинформацията. Този последен аспект ще се основава на Плана за действие за 2018 г. срещу дезинформацията[80] като основа за по-решителни действия на ЕС за справяне с дезинформацията и за това как да се ангажират ключови заинтересовани страни в гражданското общество и частния сектор. С нетърпение се очаква също така следващата стъпка с **Практическия кодекс относно дезинформацията** след оценка на ефективността на Кодекса от септември 2020 г.[81]. Кодексът е важна и необходима стъпка към създаването на по-прозрачна и отговорна екосистема на онлайн платформата, но би бил по-ефективен, ако са налице уеднаквени определения, по-съгласувано прилагане и повече действия за справяне със специфични области като микротаргетиране. Друг ключов инструмент, с който ЕС разполага днес, е **Европейската обсерватория за цифрови медии,** която започна да функционира от юни 2020 г. Тя обединява ключови заинтересовани страни, работещи по проблемите с дезинформацията, включително проверителите на факти и изследователските среди в университетите.

IV ЗАЩИТА НА ЕВРОПЕЙЦИТЕ ОТ ТЕРОРИЗМА И ОРГАНИЗИРАНАТА ПРЕСТЪПНОСТ

1. *Тероризъм и радикализация*

Неотдавнашните атаки за пореден път показаха, че терористичната заплаха в ЕС остава висока. Убийството на учител в Conflans-Sainte-Honorine на 16 октомври 2020 г. беше последвано от убийството на трима души в църквата Notre-Dame в Ница на 29 октомври. На 2 ноември при терористична атака във Виена загинаха четирима души, а 23-ма бяха ранени. На 13 ноември Съветът прие съвместна декларация на министрите на вътрешните работи на ЕС относно неотдавнашните терористични атаки във Франция и Австрия[82]. Тези неотдавнашни атаки, вдъхновени от джихадизма, са само последните от нарастващата заплаха от насилствен десен екстремизъм и други форми на тероризъм.

С цел по-нататъшна подкрепа на държавите членки в борбата срещу тероризма и радикализацията днес Комисията приема **Програма на ЕС за борба с тероризма**[83]. Настоящата програма се основава на съществуващите политики и инструменти и ще служи за укрепване на рамката на ЕС за по-нататъшно подобряване на

[78] Стартирана беше например кампанията „Мисли, преди да споделиш“, в която се предоставят съвети как да се ограничи разпространението на дезинформацията сред младежките аудитории и разпространителите на информация в държавите от Източното партньорство на ЕС, като бяха получени над 500 000 мнения в социалните медийни платформи.

[79] COM (2020) 790.

[80] JOIN(2018) 36 Съвместно съобщение, План за действие за борба с дезинформацията.

[81] SWD(2020) 180.

[82] Съвместна декларация на министрите на вътрешните работи на ЕС относно неотдавнашните терористични атаки в Европа, 13.11.2020 г., 12634/20.

[83] COM (2020) 795.

предвиждането на заплахи и рискове, предотвратяване на радикализацията и насилствения екстремизъм, за защита на хората и инфраструктурата, включително чрез сигурност на външните граници, както и за ефективни действия след атаки. В нея се очертава също така начинът, по който да бъдат подобрени правоприлагането и съдебното сътрудничество, както и използването на технологии и споделянето на съответната информация в целия ЕС, включително за онези, които извършват проверки по външните граници. Изпълнението и прилагането на законодателството продължават да бъдат от ключово значение.

Превенцията е ключова за борбата с тероризма. Усилията на ЕС в областта на **предотвратяването на радикализацията** се основават на солидния опит, натрупан до момента в подкрепа на работещите на първа линия и разработчиците на политики. На 24 ноември Комисията прие нов **план за действие за интеграция и приобщаване**[84]. От решаващо значение в борбата срещу радикализацията е да се работи по-усилено за обединяване на общностите. По-сплотеното и приобщаващо общество може да спомогне за предотвратяване на разпространението на екстремистки идеологии, които могат да доведат до тероризъм и насилнически екстремизъм. Подкрепата за **Мрежата за осведоменост по въпросите на радикализацията** включва договор за допълнителни 30 милиона евро, сключен през януари 2020 г., за следващите четири години в помощ на действащите на място лица, както и допълнителна подкрепа за подпомагане на създателите на политики и изследователите. Тези и други инструменти, като например **интернет форумът на ЕС**, ще дадат възможност на Комисията да разгледа приоритетните действия, подчертани в стратегическите насоки до 2021 г. относно координиран подход на ЕС за предотвратяване на радикализацията, разработен с държавите членки. Те се допълват от действия по Програмата за борба с тероризма за противодействие на екстремистките идеологии онлайн, засилване на усилията в затворите и за рехабилитация и реинтеграция, включително на чуждестранни бойци терористи, както и за засилване на подкрепата за местните участници и изграждането на по-устойчиви общности.

Директивата относно борбата с тероризма[85], приета през март 2017 г., е основният инструмент за наказателно правосъдие на равнище ЕС за борба с тероризма. С директивата се определят минимални стандарти за определяне на терористични и свързани с тероризма престъпления, както и за санкции, като същевременно на жертвите на тероризма се предоставят права на защита, подкрепа и помощ. На 30 септември 2020 г. Комисията прие доклад[86] за оценка на мерките, предприети от държавите членки за спазване на директивата. В доклада се прави заключението, че транспонирането в националното законодателство е спомогнало за укрепване на подхода на държавите членки за наказателно правосъдие към тероризма и на правата, предоставени на жертвите на тероризъм, но че същевременно продължават да съществуват пропуски. Например не всички държави членки са криминализирали в националното си право всички изброени в директивата престъпления като терористични престъпления, нито са въвели в националното си право разпоредбите за криминализиране на пътуванията с цел тероризъм и санкционирането на финансирането на тероризма, както и за подпомагане на жертвите. Доклад за оценка на директивата ще бъде приет по-късно през 2021 г.

[84] COM(2020)758.
[85] Директива (ЕС) 2017/541
[86] COM (2020) 619.

ЕС продължава да работи в подкрепа на държавите членки, за да се попречи на терористите да получават средства за атаки и да се подкрепи прилагането на правилата. Регламентът за предлагането на пазара и употребата на **прекурсори на взривни вещества**, приет през юни 2019 г.[87], ще започне да се прилага от 1 февруари 2021 г. За да помогне на националните органи и частния сектор да прилагат регламента, през юни 2020 г. Комисията публикува набор от насоки[88]. Освен това през юни 2020 г.[89] Комисията създаде програма за мониторинг на крайните продукти, резултатите и въздействието на регламента.

През ноември 2019 г. Комисията покани държавите членки да направят оценка на изпълнението на плана за действие за 2017 г. с цел подобряване на готовността за действие срещу **химически, биологични, радиологични и ядрени (ХБРЯ)** рискове[90]. Общото заключение беше, че повечето действия са изпълнени. В началото на 2020 г. Комисията изготви, в сътрудничество с национални експерти, списък на високорисковите химикали, които предизвикват загриженост. Това беше основата за взаимодействие с производителите на оборудване с цел подобряване на възможностите за откриване. Неотдавна Комисията започна проучване относно възможностите за ограничаване на достъпа до някои от тези химикали. Работата продължава и като част от Механизма за гражданска защита на Съюза, а допълнителният капацитет за действие срещу ХБРЯ рискове в областта на обеззаразяването, откриването, наблюдението и мониторинга, както и по отношение на складирането се обсъжда с държавите членки.

На 12 октомври 2020 г. Съветът реши да удължи режима на санкции срещу разпространението и употребата на химическо оръжие с една година[91], като позволи на ЕС да наложи ограничителни мерки на лица и субекти, участващи в разработването и употребата на химическо оръжие. На 14 октомври 2020 г. Съветът прие ограничителни мерки срещу шест лица и едно образувание, участващи в атентата срещу Алексей Навални, който беше отровен с токсично нервнопаралитично вещество от групата „Новичок“ на 20 август 2020 г. в Русия[92].

Финансовата информация също е от решаващо значение за идентифицирането на терористични мрежи, тъй като терористите разчитат на финансиране за пътувания, обучение и оборудване, и усилията за **борба с финансирането на тероризма** са от съществено значение за разследванията в борбата с тероризма. Основните въпроси включват използване на съществуващите инструменти и разузнавателна информация в пълния им потенциал, правилно прилагане на международно съгласувани стандарти и справяне с променящите се предизвикателства, породени от нововъзникващите технологии и платформите на социалните медии[93] (вж. по-долу).

---

87 Регламент (ЕС) 2019/1148.

88 Известие на Комисията — Насоки за прилагането на Регламент (ЕС) 2019/1148 относно предлагането на пазара и използването на прекурсори на взривни вещества, ОВ C 210/1, 24.6.2020 г.

89 SWD(2020) 114 final.

90 COM(2017) 610 final.

91 Решение (ОВППС) 2020/1466 на Съвета от 12 октомври 2020 г. за изменение на Решение (ОВППС) 2018/1544.

92 Решение на Съвета (ОВППС) 2020/1482 от 14 октомври 2020 г. и Регламент за изпълнение (ЕС) 2020/1480 на Съвета.

93 Както беше посочено от ЕС през ноември 2019 г. на конференцията на министрите, насочена към борбата с финансирането на тероризма, под надслов *„Спиране на финансирането на тероризма“*, която беше проведена в Австралия.

Транспортната мрежа е била и продължава да бъде цел за тероризъм. Усилията на ЕС включват основан на оценката на риска подход за защита на сектора на авиацията[94]. Зоните на конфликти представляват сериозен риск за гражданската авиация и споделянето на информация и оценката на риска е от съществено значение за смекчаването на риска[95]. Информационната система за предупреждение относно **оценката на риска в зоните на конфликт** в ЕС е призната за най-добра практика и международните стандарти за обмен на информация са включени в законодателството на ЕС[96]. Въз основа на натрупания опит в областта на гражданската авиация Комисията разшири подхода, основан на оценката на риска, за да бъдат обхванати и други видове транспорт. Изпълнението на **плана за действие** на ЕС в областта на **сигурността на железопътния транспорт**[97] е в ход, като се използва експертният опит на платформата на ЕС за пътниците в железопътния транспорт, специална експертна група, създадена от Комисията. Подходът, основан на оценката на риска, е добре известен в морската област и се прилага, като Комисията работи с държавите членки и заинтересованите страни за засилване на сигурността на пътниците. Това е включено в **Стратегията на ЕС за морска сигурност** и нейния **план за действие**, преработен през 2018 г., като е налице и измерение на сигурността и отбраната. Това е изложено в последния доклад за изпълнението, приет и публикуван на 23 октомври 2020 г.[98].

Европол предоставя подкрепа на държавите членки при разследванията, свързани с тероризма, чрез **Европейския център за борба с тероризма (ЕСТС)**. Исканията на държавите членки за оперативна подкрепа за ЕСТС продължават да се увеличават и в момента ЕСТС е част от почти всяко голямо разследване, свързано с борбата с тероризма. През 2019 г. Европол подкрепи общо 632 различни операции в областта на борбата с тероризма. Разследващите от държавите членки също одобриха тази дейност, като нивото на удовлетвореност се повиши от 8/10 през 2018 г. до 9,1/10 през 2019 г. ЕСТС координира общо 18 дни за действия през 2019 г.[99].

Евроюст също така подкрепи 116 разследвания в областта на тероризма през периода 2019—2020 г. Текущата работа ще доведе до законодателно предложение относно обмена на случаи на трансграничен цифров тероризъм с цел развиване на Съдебния регистър в областта на борбата с тероризма (СРБТ), стартиран през 2019 г.[100], както и до разширяване на работата, свързана с десни и леви екстремистки групировки.

---

[94] Интегрираният процес на оценката на риска за сигурността във въздухоплаването на ЕС подпомага процедурата на вземане на решения в областта на сигурността на въздушните товари, стандартите за сигурност във въздухоплаването и рисковете за гражданското въздухоплаване, произтичащи от зоните на конфликти.

[95] Трагичният инцидент, при който беше свален полет 752 на украинските международни авиолинии на 8 януари 2020 г., също доказа значението на обмена на информация и оценката на рисковете за сигурността на гражданското въздухоплаване.

[96] https://eur-lex.europa.eu/legal-content/BG/TXT/PDF/?uri=CELEX:32019R1583&from=EN

[97] COM 2018 (470) final.

[98] Доклад на службите на Комисията, Европейската служба за външна дейност и Европейската агенция по отбрана относно изпълнението на преразгледания план за действие във връзка със Стратегията на ЕС за морска сигурност, SWD (2020) 252.

[99] Консолидиран годишен доклад за дейността през 2019 г., Европол, 9.6.2020 г.

[100] СРБТ се управлява от Евроюст на 24-часова база и осигурява активна подкрепа на националните съдебни органи. Тази централизирана информация следва да подпомогне прокурорите да предприемат по-активно координиране и да идентифицират заподозрени лица или мрежи, които се разследват в конкретни случаи с потенциални трансгранични последици.

На 30 юли 2020 г. Съветът последно поднови списъка на ЕС на лицата, групировките и образуванията, спрямо които се прилагат ограничителни мерки, насочени към борбата с тероризма. Последният списък съдържа 14 физически лица и 21 образувания. Същия ден Съветът наложи ограничителни мерки на едно лице по насочения срещу дейността на ИДИЛ (Даиш)/Ал Кайда режим за налагане на санкции за борба с тероризма. В момента има пет лица, самостоятелно вписани в списъка по този режим, който беше подновен за една година на 19 октомври 2020 г.[101].

Важен елемент от политиката за борба с тероризма се отнася до заплахите, свързани с **чуждестранните бойци терористи (FTF)** в момента в Сирия и Ирак. При пълно зачитане на основната отговорност на държавите членки по тези въпроси подкрепата и сътрудничеството на равнище ЕС помага на държавите членки да се справят с общите предизвикателства: преследване на извършителите на терористични престъпления, предотвратяване на неразкрито влизане в Шенгенското пространство и реинтеграция и рехабилитация на завърнали се чуждестранни бойци терористи. Комисията например работи в тясно сътрудничество с държавите членки и ключовите държави партньори, за да се гарантира, че доказателствата от бойното поле се споделят и използват ефективно за идентифициране, откриване на границите на ЕС и преследване. Меморандумът от 2020 г за доказателствата, събрани на бойното поле,[102] публикуван от Евроюст, показва, че макар да има много предизвикателства пред получаването на такива данни и гарантирането, че отговарят на критериите за допустими доказателства, те могат да помогнат за подвеждането под наказателна отговорност на лица, заподозрени в тероризъм.

Комисията също така улеснява диалога с държавите членки и участниците в хуманитарните дейности, за да се направи изчерпателен и фактически преглед на ситуацията в лагерите в Североизточна Сирия, където се намират членовете на семействата на чуждестранни бойци терористи от ЕС. Специален акцент е поставен върху положението на децата в сирийските лагери. Комисията също така помага на държавите членки да споделят опит относно националните мерки и механизми за по-добро управление на **рехабилитацията и реинтеграцията** на завръщащите се чуждестранни бойци терористи, както и на децата. Мрежата за осведоменост по въпросите на радикализацията също така провежда учебни посещения и предоставя съобразени с конкретните нужди съвети за по-добро справяне с предизвикателствата пред осъдените завърнали се лица, по-специално след освобождаването им от затвора, както и с ролята на семействата и местните общности в усилията за реинтеграция.

Партньорствата за борба с тероризма и сътрудничеството с трети държави и партньорите от съседните на ЕС държави също са от съществено значение за подобряване на сигурността в ЕС и за по-добро свързване на вътрешните и външните измерения на политиката на ЕС за сигурност. Съветът призова за по-нататъшно укрепване на външния ангажимент на ЕС за борба с тероризма[103], като беше поставен акцент върху Западните Балкани, Северна Африка и Близкия изток, региона Сахел, Африканския рог и Азия. Осъществяването на тази работа продължава, като се използват изцяло инструментите за външна дейност,

[101] Решения на Съвета (ОВППС) 2020/1132, 2020/1126 и 2020/1516.

[102] https://www.eurojust.europa.eu/eurojust-memorandum-battlefield-evidence-0.

[103] Заключения на Съвета (8868/20) относно външните действия на ЕС за предотвратяване и противодействие на тероризма и насилническия екстремизъм (16 юни 2020 г.).

включително диалогът за борба с тероризма на високо ниво и мрежата от 17 **експерти по борбата с тероризма/сигурността**[104], участващи в делегациите на ЕС, чрез което продължава предоставянето на подкрепа, улеснява се сътрудничеството и се насърчава изграждането на капацитет. В момента се обмисля възможността за укрепване и разширяване на тази мрежа.

В Съвместния план за действие за борба с тероризма за **Западните Балкани** за 2018 г. и придружаващите го двустранни споразумения, подписани през 2019 г. с всеки от партньорите[105], се поставя акцент върху регион от ключово значение за общите цели на сигурността и за защитата на хората, живеещи в ЕС. На Министерския форум ЕС — Западни Балкани по въпросите на правосъдието и вътрешните работи, проведен на 22 октомври 2020 г., партньорите от ЕС и Западните Балкани потвърдиха своя ангажимент за изпълнение на целите на съвместния план за действие след 2020 г.[106]. Сътрудничеството със Западните Балкани включва управление на текущото завръщане на чуждестранни бойци терористи и членовете на техните семейства, както и по-нататъшната интеграция в дейности за борба срещу радикализацията. ЕС изпълнява и редовния си ангажимент за борба с тероризма с **Близкия изток, Северна Африка и Централна Азия**[107]. Работата с **Централна Азия** е съсредоточена върху справянето с химически, биологични, радиологични и ядрени заплахи. Съвместният комитет за сътрудничество към **Съвета за сътрудничество на арабските държави от Персийския залив и ЕС** заседава на 25 юни 2020 г., като разгледа различни въпроси, включително борбата срещу радикализацията и справянето с финансирането на тероризма и изпирането на пари, както и киберсигурността и сътрудничеството с Европол. ЕС работи с НАТО по първия по рода си одит на химични, биологични, радиологични и ядрени заплахи в една от държавите от Персийския залив в края на 2019 г. Като цяло в края на 2019 г. бяха заделени около 465 милиона евро за текущи проекти за борба с тероризма и предотвратяване на насилническия екстремизъм извън ЕС, което представлява 15 % увеличение спрямо предходната година.

ЕС също така продължи да задълбочава сътрудничеството с **Организацията на обединените нации** в борбата с тероризма[108], по-специално със Службата на ООН за борба с тероризма и Изпълнителната дирекция за борба с тероризма, включително чрез годишни диалози на високо равнище, а неотдавна и чрез активно участие във виртуалната Седмица на ООН за борба с тероризма през лятото на 2020 г. Комисията също така следи отблизо разискванията относно преразглеждането на определението

---

[104] Алжир, Босна и Херцеговина (регионален за Западните Балкани), Етиопия (връзка с Африканския съюз), Индонезия (регионален за Югоизточна Азия и връзка с Асоциация на народите от Югоизточна Азия (АСЕАН) — регионален форум на АСЕАН), Ирак, Йордания, Кения (регионален за Африканския рог), Киргизстан (регионален за Централна Азия), Либия, Ливан, Мароко, Нигерия, Пакистан, Саудитска Арабия, Тунис, Турция, Чад (регионален за Сахел).

[105] Албания, Босна и Херцеговина, Косово*, Северна Македония, Сърбия, Черна гора.

[106] Съвместно изявление за пресата: https://www.consilium.europa.eu/bg/press/press-releases/2020/10/23/joint-press-statement-eu-western-balkans-ministerial-forum-on-justice-and-home-affairs/pdf.

[107] Действията за борба с тероризма бяха подчертани например в новата стратегия на ЕС за Централна Азия.

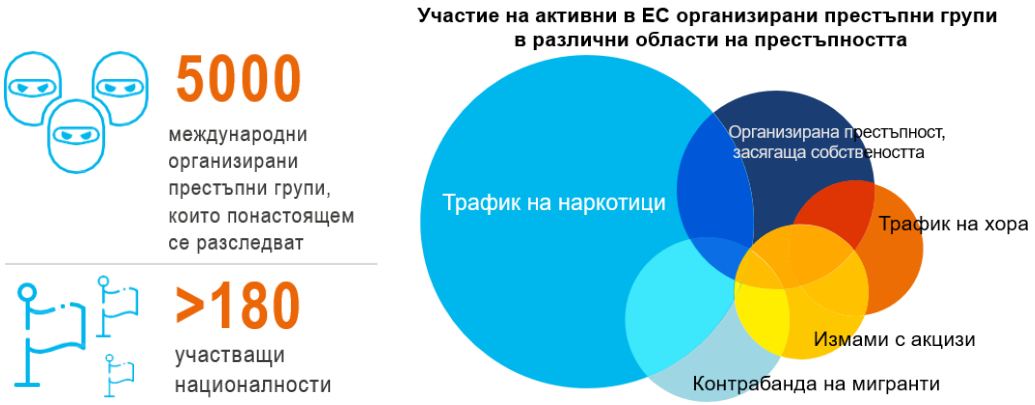
*Това название не засяга позициите по отношение на статута и е съобразено с Резолюция 1244/1999 на Съвета за сигурност на ООН и становището на Международния съд относно обявяването на независимост от страна на Косово.

[108] През 2019 г. беше подписана Рамка за сътрудничество между ЕС и ООН за борба с тероризма https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf.

на терористични престъпления в Конвенцията на **Съвета на Европа** за предотвратяване на тероризма, като насърчава тясното съгласуване с определенията в правото на ЕС. Продължава доброто сътрудничество в областта на борбата с тероризма и химичните, биологичните, радиологичните и ядрените материали между **НАТО** и ЕС, като се обменя информация относно изграждането на капацитет, за да се избегне дублиране и да се осигури взаимно допълване.

2. Борба с организираната престъпност

Организираната престъпност нараства, придобива все по-голямо трансгранично измерение и се премества в онлайн пространството.



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

Действията на Комисията включват борба с наркотиците, незаконното огнестрелно оръжие, финансовите престъпления, незаконния внос на културни ценности, трафика на хора или престъпленията против околната среда, подпомагане на правоприлагащите органи на държавите членки и съдебните органи в държавите членки, както и партньорите в съседните на ЕС държави. Сътрудничеството с трети държави, по-специално в съседството на ЕС като Западните Балкани, както и с международни организации, включително Службата на ООН по наркотиците и престъпността (СНПООН)[109], също имаха ключова роля[110].

През 2019 г. **Центърът на Европол за борба с тежката и организираната престъпност** получи и обработи близо 55 000 вноски за оперативни дейности, което представлява увеличение с 12 % в сравнение с 2018 г. Що се отнася до броя на подкрепените операции, центърът е подпомогнал държави в 726 случая[111]. От решаващо значение е и цялостното транспониране във всички държави членки на законодателната рамка на ЕС за организираната престъпност[112], която има за цел да се хармонизират законите на държавите членки относно криминализирането на престъпления, свързани с участие в престъпна организация, и да се определят санкции за тези престъпления. Комисията стартира проучване, за да анализира

[109] На 8 декември 2020 г. беше проведен диалог на високо равнище между ЕС и СНПООН.
[110] В края на 2019 г. за текущи действия срещу организираната престъпност извън ЕС бяха предвидени около 830 милиона евро.
[111] Консолидиран годишен доклад за 2019 г., Европол, юни 2020 г.
[112] Рамково решение 2008/841.

начините за подобряване на това законодателство. По-нататъшни стъпки за засилване на борбата с организираната престъпност в ЕС ще бъдат заложени в Програмата на ЕС за борба с организираната престъпност, която ще бъде приета през първото тримесечие на 2021 г.

Обезпечаването и конфискацията на облаги от престъпна дейност са сред най-ефективните средства за борба с организираната престъпност. Новият **Европейски център за борба с финансовата и икономическата престъпност** (EFECC), създаден през юни 2020 г. към Европол, ще подобри оперативната подкрепа, предоставяна на държавите членки и органите на ЕС в областта на финансовите и икономическите престъпления, и ще насърчава систематичното използване на финансови разследвания. В подкрепа на усилията на ЕС за по-ефективно идентифициране, обезпечаване и конфискация на активи от престъпна дейност Съветът прие заключения през юни 2020 г. за засилване на финансовите разследвания за борба с тежката и организираната престъпност.[113] През 2021 г. Комисията ще преразгледа законодателството относно обезпечаването и конфискацията на облаги от престъпна дейност[114] и относно Службите за възстановяване на активи[115].

За борбата с организираната престъпност са необходими предпазни мерки, за да се гарантира, че работата на правоприлагащите органи може да се осъществява ефективно в основни граници, като например защитата на личните данни. С Директивата относно правоприлагането в областта на защитата на данните от 2016 г., в частта относно защитата на физическите лица по отношение на обработването на лични данни, свързани с престъпления[116], се защитава основното право на защита на данните, когато личните данни се използват от органите за наказателното правоприлагане за целите на правоприлагането. С нея се гарантира, че личните данни на жертвите, свидетелите и заподозрените в престъпление са надлежно защитени и улесняват трансграничното сътрудничество в борбата с престъпността и тероризма. Крайният срок за транспонирането на Директивата относно правоприлагането в областта на защитата на данните изтече на 6 май 2018 г. Към днешна дата повечето държави членки са приели законодателство, с което директивата се транспонира. Някои производства за установяване на неизпълнение на задължения обаче все още са в ход[117]. В момента Комисията оценява съответствието на националните закони за транспониране с директивата.

Борба срещу незаконните наркотици

През юли 2020 г. Комисията прие нова **програма и план за действие на ЕС по отношение на наркотиците за периода 2021—2025 г.,**[118] като продължение на

[113] Заключения на Съвета 8927/20.
[114] Директива 2014/42/ЕС.
[115] Решение 2007/845/ПВР на Съвета.
[116] Директива (ЕС) 2016/680 относно защитата на физическите лица във връзка с обработването на лични данни, свързани с престъпления.
[117] Три държави членки (Германия, Испания, Словения) все още не са уведомили за пълното транспониране въпреки производствата за установяване на неизпълнение на задължения. Комисията заведе едно дело за липса на транспониране пред Съда и през май 2020 г. предаде допълнителни мотивирани становища на другите две държави членки за това, че не са транспонирали изцяло директивата.
[118] COM(2020)606.

текущите стратегии на ЕС по отношение на наркотиците[119]**.** С това се определят политическата рамка и приоритетите за действие през следващите пет години. Основният акцент на програмата е: 1) мерки за засилване на сигурността срещу незаконния трафик на наркотици — от организираните престъпни групи до управлението на външните граници и незаконното разпространение и производство; 2) по-голяма превенция, включително повишаване на осведомеността за вредите от наркотиците, по-специално връзката между използването на наркотици, насилието и друга престъпна дейност; както и 3) справяне с вредите, свързани с употребата на наркотици, чрез достъп до лечение, намаляване на риска и вредите и балансиран подход към темата за наркотиците в затворите. На 30 ноември 2020 г. Комисията прие оценка на политиката на ЕС за прекурсорите на наркотични вещества, в която се прави заключението, че са необходими допълнителни действия за предотвратяване на достъпа на организираните престъпни групи в ЕС до химикалите, използвани за производството на незаконни синтетични наркотици[120].

ЕС също така финансира конкретни проекти за засилване на борбата срещу наркотиците, като например Форума на гражданското общество по въпросите на наркотиците. В Европейския доклад за наркотиците за 2020 г. на Европейския център за мониторинг на наркотици и наркомании, публикуван на 22 септември 2020 г.[121], са посочени текущите употреби на наркотици и пазарните тенденции в ЕС, Турция и Норвегия. От доклада е видно, че има увеличаване на количеството иззет кокаин, достигащо рекордно висок размер от 181 тона, че количеството на иззетия хероин е почти удвоено и възлиза на 9,7 тона, както и че в ЕС има голямо количество наркотици с висока чистота. В доклада също така се изследва появата на нови синтетични опиоиди, които предизвикват опасения за здравето, и се търсят решения на предизвикателствата, породени от пандемията от COVID-19.

Работата срещу наркотиците продължава на няколко различни равнища. **Законодателният пакет за новите психоактивни вещества** (НПВ) беше приет през есента на 2017 г.[122] и започна изцяло да се прилага през ноември 2018 г. Пет държави членки все още са в производство за установяване на неизпълнение на задължения[123]. Вече е приет първият делегиран акт, с който ново психоактивно вещество (изотонитазен) се определя като наркотик[124].

На **международната сцена** ЕС участва активно в работата на Комисията на ООН по упойващите вещества[125], по-специално с цел актуализиране по отношение на включването в списъците на нови психоактивни вещества[126], както и за преместване на канабиса и свързаните с него вещества в друг списък[127]. Съветът[128] одобри два

[119] Стратегия на ЕС за наркотиците за периода 2013—2020 г. и План за действие на ЕС за наркотиците за периода 2017—-2020 г.

[120] COM(2020) 768, 30 ноември 2020 г.

[121] Европейски доклад за наркотиците за 2020 г.: Тенденции и развитие, Европейски център за мониторинг на наркотици и наркомании (ЕЦМНН), 22.09.2020 г.

[122] Регламент (ЕС) 2017/2010 и Директива (ЕС) 2017/2010.

[123] Австрия, Ирландия, Португалия, Словения и Финландия.

[124] C/2020/5897; ОВ L 379, 13.11.2020 г., стр. 55.

[125] Управляващ орган в Службата на ООН по наркотиците и престъпността (СНПООН).

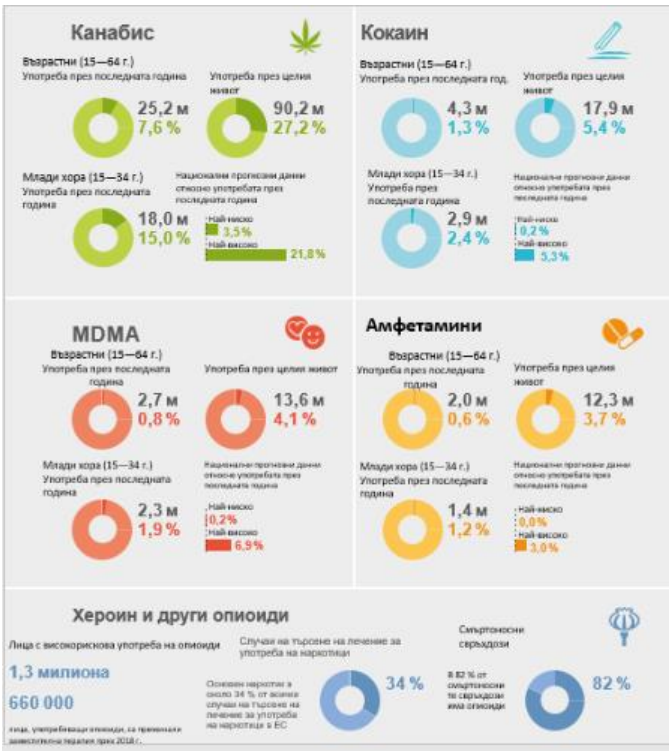
[126] COM(2019)631.

[127] COM(2019) 624 и COM(2020) 659.

[128] Срещата на високо равнище между ЕС и Китай на 16—17 юли 2018 г. в Пекин доведе до сключване на споразумение за започване на годишен диалог между ЕС и Китай относно наркотиците. Условията на бъдещия диалог бяха потвърдени от Комитета на постоянните

нови диалога относно наркотиците с Китай и Иран, а Европейският център за мониторинг на наркотици и наркомании отбеляза напредък по договореностите за работа с трети държави[129].

Борба с финансовата престъпност



Прието е ново законодателство за засилване на борбата с финансовата престъпност, както и изпирането на пари. Директивата, с която се улеснява използването на финансова и друга информация за предотвратяване, разкриване, разследване или наказателно преследване на някои престъпления, беше приета през 2019 г., като чрез нея правоприлагащите органи и службите за отнемане на активи получават достъп до национални централизирани регистри на банкови сметки за целите на борбата с тежките престъпления. Директивата има за цел също така да се подобри сътрудничеството между правоприлагащите органи и звената за финансово разузнаване (ЗФР), както и да се улесни обменът на информация между ЗФР. През юни 2020 г. Комисията публикува доклада „Възстановяване и конфискация на активи: да гарантираме, че престъпността „не си струва“[130]. В него беше отбелязан потенциалът за по-голяма хармонизация в режимите[131] за отнемане на активи с цел модернизиране на законодателството на ЕС относно отнемането на активи и укрепването на капацитета на националните органи в борбата с организираната престъпност. Беше започнат допълнителен анализ на отнемането на активи чрез външно проучване. Регламентът за взаимното признаване на заповедите за изземване и конфискация[132] ще се прилага от 19 декември 2020 г. и значително ще подобри сътрудничеството между държавите членки.

През май 2020 г. Комисията прие **план за действие за цялостна политика на Съюза за предотвратяване на изпирането на пари и финансирането на тероризма,**[133] за да бъде засилена рамката на ЕС. На 5 ноември Съветът прие заключения относно борбата с изпирането на пари и финансирането на тероризма[134], като по-специално поиска от Комисията да работи за приемането на единен

представители (Корепер) на 30 октомври 2019 г. Съветът одобри стартирането на нов диалог между ЕС и Иран относно наркотиците на 5 март 2020 г.

[129] Становище на Комисията относно проекта на работно споразумение с Косово, приет на 14 април 2020 г., и относно проекта на работно споразумение със Сърбия, приет на 16 декември 2019 г.

[130] COM (2020) 2017 г.

[131] Включително оценката на Директива 2014/42/ЕС и Решение 2007/845/ПВР на Съвета.

[132] Регламент (ЕС) 2018/1805.

[133] C(2020) 2800 final.

[134] Заключения на Съвета 12608/20.

правилник, създаването на независим надзорен орган и координацията на звената за финансово разузнаване. В съответствие със заключенията на Съвета за засилване на финансовите разследвания[135] Комисията оценява също необходимостта от взаимно свързване на централизираните регистри на банкови сметки, което значително би ускорило достъпа на звената за финансово разузнаване и правоприлагащите органи до информация за банкови сметки. Успоредно с това продължават усилията да се гарантира, че най-новите стандарти на ЕС се прилагат ефективно от държавите членки. Правилата съгласно петата директива относно борбата с изпирането на пари имат за цел да се повиши степента на прозрачност на структурите на корпоративна собственост. Крайният срок за транспониране изтече на 1 януари 2020 г. и Комисията започна производства за неизпълнение на задължения срещу 16 държави членки[136]. Друга важна мярка е новият Регламент относно контрола на паричните средства[137], който беше приет през октомври 2018 г. и става приложим от 3 юни 2021 г. С него ще бъде подобрена съществуващата система за контрол на паричните средства, които влизат в ЕС и излизат от него, като разпоредбите за прилагане са в процес на подготовка.

На външния фронт продължават усилията за подкрепа на държавите партньори в борбата с изпирането на пари и финансирането на тероризма. В този контекст ЕСВД и делегациите на ЕС играят ключова роля за насърчаването и подпомагането на политическия ангажимент по отношение на трети държави и международни организации, като Специалната група за финансови действия (FATF).

В допълнение към тази работа Комисията стартира глобален механизъм за предоставяне на подкрепа на партньорските държави извън ЕС с цел въвеждане на ефективни рамки за борба с изпирането на пари/борбата с тероризма в съответствие с международните стандарти. Действието на стойност 20 милиона евро има за цел също така да насърчи сътрудничеството между участниците от финансовата сфера и правосъдието на национално, регионално и международно равнище.

Борба с корупцията

Корупцията сама по себе си е престъпление и ключов фактор за организираната престъпност. Предотвратяването и борбата с корупцията ще бъдат обект на редовно проследяване и оценка на нормативната уредба на държавите членки в рамките на новоустановения **механизъм за върховенството на закона[138]**. Първият доклад за целия ЕС относно върховенството на закона беше приет на 30 септември 2020 г.[139]. От него е видно, че много държави членки имат високи стандарти за върховенство на закона, но продължават да съществуват важни предизвикателства. Докладът обхваща всички държави членки с обективни и фактически годишни оценки, като целта е да повишат осведомеността и разбирането за развитието в отделните държави членки, за да могат да бъдат идентифицирани рисковете, да се разработят

[135] Заключения на Съвета 8927/20.

[136] Австрия, Белгия, Гърция, Естония, Ирландия, Испания, Кипър, Люксембург, Нидерландия, Обединеното кралство, Полша, Португалия, Румъния, Словакия, Словения, Унгария, Чешката република

[137] Регламент (ЕС) 2018/1672.

[138] Чрез европейския механизъм за върховенството на закона се осъществява процес на диалог между Комисията и държавите членки, както и Съвета и Европейския парламент, и националните парламенти, гражданското общество и други заинтересовани страни относно върховенството на закона. Докладите за върховенството на закона са в основата на този нов процес.

[139] COM(2020)580.

възможни решения и подкрепата да бъде насочена на ранен етап. На този етап **Европейската прокуратура** (ЕРРО) ще се бори с престъпленията против бюджета на ЕС в участващите 22 държави от ЕС. Тя ще има правомощието за разследване, наказателно преследване и предаване на съд на отговорните за престъпления срещу бюджета на ЕС като измама, корупция или сериозни трансгранични измами с ДДС. ЕРРО следва да започне да функционира през първото тримесечие на 2021 г.[140].

Понастоящем Комисията извършва оценка на транспонирането в националното право на правилата, установени в **Директивата относно борбата с измамите, засягащи финансовите интереси на Съюза**, по наказателноправен ред[141] и е образувала производства за установяване на неизпълнение на задължения срещу държавите членки, които не са уведомили за пълно транспониране[142]. Праз 2021 г. Комисията ще приеме доклад за оценка на степента, в която държавите членки са взели необходимите мерки, за да се съобразят с директивата.

Борба с трафика на културни ценности

Основната цел на **Регламента за въвеждането и вноса на движими културни ценности**[143], приет през юни 2019 г., е да бъде спрян вносът в Съюза на културни ценности, които са незаконно изнасяни от държавата им на произход. За да осигури правилното му прилагане, в момента Комисията подготвя приемането на разпоредби за прилагане, включително за централизирана електронна система за внос на културни ценности, чрез която ще може да се съхранява и обменя информация между държавите членки, както и да се извършват необходимите формалности при вноса[144]. До края на 2020 г. ще влезе в сила правило за обща забрана, което ще осигури на митниците на държавите членки законни средства за контрол и действие по отношение на пратки, които могат да съдържат културни ценности, незаконно изнесени от държавата им на произход.

Борба с незаконния трафик на огнестрелни оръжия

На 24 юли 2020 г. Комисията публикува нов **план за действие на ЕС относно трафика на огнестрелни оръжия за периода 2020—2025 г.**[145]**.** На конференцията на високо равнище на министрите от министерствата на външните работи и вътрешните работи на ЕС и Западните Балкани на 31 януари 2020 г. беше подчертана необходимостта от повече действия в борбата с незаконния трафик на огнестрелни оръжия. Планът за действие включва конкретни действия за подобряване на правния контрол върху огнестрелните оръжия, познаването на заплахата, свързана с огнестрелните оръжия, сътрудничеството на правоприлагащите органи и

[140] Решението за изпълнение на Съвета за назначаване на европейските прокурори влезе в сила на 29 юли 2020 г. Европейските прокурори от колегиума проведоха първото си заседание на 28 септември 2020 г. ЕРРО скоро ще сключи работни договорености с Европол, Евроюст и OLAF.

[141] Директива (ЕС) 2017/1371

[142] Понастоящем остават открити производствата за установяване на неизпълнение на задължения срещу Австрия, Ирландия и Румъния.

[143] Регламент (ЕС) 2019/880.

[144] Системата за внос на културни ценности трябва да бъде създадена най-късно до 28 юни 2025 г. Комисията прие първия доклад за напредъка в разработването на системата за внос на културни ценности. [COM(2020) 342].

[145] COM(2020)608: този нов план за действие включва френско-германската инициатива за Западните Балкани „Пътна карта за постигане на устойчиво решение за незаконното притежание, злоупотребата със и трафика на МОЛВ/огнестрелни оръжия и боеприпаси за тях в Западните Балкани до 2024 г.“.

международното сътрудничество, като се поставя акцент върху Югоизточна Европа. Комисията предприе стъпки, за да се гарантира, че директивата за контрол върху придобиването и притежаването на оръжия, приета през май 2017 г.[146], е изцяло транспонирана от държавите членки. Въпреки това 10 държави членки все още не са уведомили за пълното транспониране на директивата[147], а голяма част от държавите членки не са транспонирали приетото впоследствие законодателство за прилагане. В резултат на това Комисията започна производства за установяване на неизпълнение на задължения от държавите членки[148]. Комисията извършва задълбочена оценка и на съобщените мерки за транспониране и ще докладва за прилагането на директивата през първата половина на 2021 г. Комисията също така започна оценка на възможната модернизация на правната рамка относно мерките за внос, износ и транзит на огнестрелни оръжия[149].

Борба с трафика на хора

В стратегията за Съюза на сигурност се подчертава необходимостта от разработване на нов стратегически подход за изкореняване на трафика на хора в контекста на програмата за борба с организираната престъпност. Освен това, както е посочено в член 20 от Директивата за борба с трафика на хора[150], през октомври 2020 г. Комисията публикува третия си доклад за напредъка в борбата с трафика на хора[151].

Тук е виден напредъкът в транснационалното сътрудничество, трансграничното правоприлагане и съдебните оперативни действия; създаването на национални и транснационални механизми за насочване на жертвите и разработване на база от знания за

[146] Директива (ЕС) 2017/853 Ключови бяха и две директиви за прилагане от 16 януари 2019 г., в които се предвиждат технически спецификации за маркировката и за сигналните и предупредителните оръжия.

[147] Това са: Дания, Испания, Кипър, Люксембург, Полша, Словакия, Словения, Унгария, Чешката република, Швеция.

[148] По отношение на настоящата директива текат 25 производства (Австрия, Белгия, България, Германия, Гърция, Дания, Естония, Ирландия, Испания, Кипър, Латвия, Литва, Люксембург, Малта, Нидерландия, Обединеното кралство, Полша, Португалия, Румъния, Словакия, Словения, Унгария, Финландия, Франция, Чешката република, Швеция) и 34 производства, свързани с директивите за прилагане (Директива 2019/68 — Австрия, Белгия, България, Германия, Гърция, Ирландия, Испания, Италия, Кипър, Люксембург, Обединеното кралство, Полша, Румъния, Словения, Унгария, Финландия, Хърватия, Чешката република, Швеция, и Директива 2019/69 — България, Гърция, Ирландия, Испания, Италия, Кипър, Люксембург, Нидерландия, Обединеното кралство, Полша, Румъния, Словения, Унгария, Финландия, Хърватия, Чешката република, Швеция).

[149] Регулирана от Регламент (ЕС) № 258/2012.

[150] ОВ L -101, 15.4.2011 г., стр. 1.

[151] COM(2020) 661 final, допълнено от проучване относно събирането на данни за трафика на хора в ЕС през периода 2017—2018 г.

трафика. Държавите членки използват все по-често агенциите на ЕС, за да обменят информация, да извършват съвместни действия и да използват съвместни екипи за разследване в борбата с трафика на хора както в рамките на ЕС, така и извън него[152]. Оперативното сътрудничество донесе осезаеми резултати, особено в рамките на Европейската мултидисциплинарна платформа за борба с криминални заплахи: през 2019 г. тази работа е довела до 825 ареста, установяването на 8824 заподозрени и 1307 потенциални жертви, включително 69 деца. Установени или разбити са били 94 организирани престъпни групи, участващи в тези престъпления, и са замразени в банкови сметки над 1,5 милиона евро активи. На Европейския ден за борба с трафика на хора на 18 октомври 2020 г. Комисията публикува проучване за разходите за трафик на хора и друго проучване за националните и транснационалните механизми за насочване[153].

Контрабанда на мигранти

Европейският център за контрабанда на мигранти съобщава за непрекъснато увеличаване на дейностите по **контрабанда на мигранти**, най-вече в Западните Балкани и съседните държави, както и при вторичните движения в целия ЕС. През 2019 г. Европол допринесе за установяването на 14 218 заподозрени, участващи в трафик на мигранти[154]. През май 2020 г. Евроюст създаде целева група за прокурорите, работещи в областта на контрабандата на мигранти, като важен център за осъществяване на редовна връзка между ключови участници от съдебната система на национално равнище в държавите — членки на ЕС, и за подпомагане на съвместната им оперативна реакция[155].

Борба с престъпленията срещу околната среда

Престъпленията срещу околната среда представляват действия в нарушение на законодателството в областта на околната среда, които нанасят или могат да нанесат значителни вреди или пораждат значителни рискове за околната среда и човешкото здраве[156]. Сред най-важните области на **престъпленията против околната среда** са незаконните емисии или изхвърлянето на вещества във въздуха, водите или почвата, незаконната търговия с диви животни, незаконната търговия с озоноразрушаващи вещества и незаконно извършваните превоз или изхвърляне на отпадъци. Неотдавнашната оценка на Директивата относно престъпленията срещу околната среда[157] показа, че напредъкът по разработването на европейска рамка не е съпроводен със значително въздействие на място, включително по отношение на по-доброто трансгранично сътрудничество и равнопоставеността по отношение на

[152] Европейският орган по труда например си сътрудничи с Европол в борбата с трафика на хора в ЕС за всички форми на експлоатация, включително сексуална и трудова експлоатация, както и за всички форми на трафик на деца. Това е и признание на Протокола на Международната организация на труда относно премахването на принудителния труд (P29). Този протокол представлява основен трудов стандарт, с който принудителният труд се определя като престъпление, насочен е към превенцията, защитата на жертвите, обезщетенията и международното сътрудничество при настоящите форми на принудителен труд, включително свързаните с трафика на хора.

[153] Проучвания на икономическите, социалните и човешките разходи за трафик на хора и преглед на функционирането на националните и транснационалните механизми за насочване на държавите членки, достъпни на адрес https://ec.europa.eu/anti-trafficking.

[154] Европейски център за борба с контрабандата на мигранти, 4-ти годишен доклад, 15.5.2020 г.

[155] http://www.eurojust.europa.eu/press/PressReleases/Pages/2020/2020-05-29.aspx.

[156] Директива относно защитата на околната среда чрез наказателно право, 2008/99/ЕО.

[157] SWD(2020) 259 final.

санкциите в държавите членки. По-специално това не е довело до повече присъди и налагане на възпиращи в по-голяма степен санкции в държавите членки. Ето защо беше решено директивата да бъде преразгледана до края на 2021 г.

На 29—30 октомври 2019 г. Евроюст, съвместно с Европейската мрежа на прокурорите по въпросите на околната среда (ENPE), проведе конференция на тема „Международно сътрудничество и сътрудничество в борбата с престъпленията срещу околната среда“, за да бъде повишена осведомеността и насърчено трансграничното сътрудничество между прокурорите и други практикуващи юристи във и извън ЕС по отношение на престъпленията срещу околната среда.

В момента се извършва оценка на плана за действие срещу трафика на диви животни, приет през 2016 г. Пример за конкретно действие е проект, който се провежда до януари 2021 г., насочен към трафика на диви животни във и през ЕС, при който се използват интернет и услуги за доставка на колети, с цел предотвратяване и неутрализиране на мрежите за киберпрестъпления срещу дивата природа[158].

V. СИЛНА ЕВРОПЕЙСКА ЕКОСИСТЕМА НА СИГУРНОСТТА

За да има един истински и ефективен Съюз на сигурност, трябва да бъде положено общо усилие от всички обществени слоеве. 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, най-вече у най-уязвимите, жертвите и свидетелите.

1. Сътрудничество и обмен на информация

Един от най-важните приноси, които ЕС може да даде за защитата на гражданите, е да подпомогне лицата, отговарящи за сигурността, да работят добре заедно. Сътрудничеството и обменът на информация са мощни инструменти за борба с престъпността и тероризма, за справяне със заплахи като киберсигурността и за осигуряване на правосъдие. В подкрепа на обмена на информация между правоприлагащите и съдебните органи са въведени редица инструменти.

Днес Комисията приема преразгледания мандат на **Европол**[159] с цел внасяне на редица целенасочени подобрения в работата на тази агенция. Това ще позволи на Европол да се справя по-добре с променящия се характер на престъпленията, извършени чрез интернет, както и с финансовите престъпления. Европол ще засили сътрудничеството с частния сектор и ще приведе разпоредбите за защита на данните в съответствие със съществуващите правила на ЕС.

Европол и други агенции на ЕС, като например Европейската агенция за гранична и брегова охрана (Frontex), CEPOL и Евроюст, продължиха да развиват политическия цикъл на ЕС по отношение на тежката и организираната международна престъпност, „**Европейската мултидисциплинарна платформа за борба с криминални заплахи**“ (EMPACT).[160]. Сътрудничеството по EMPACT

[158] https://wwf.be/fr/wildlife-cybercrime/.
[159] COM (2020) 796.
[160] EMPACT е инструментът на ЕС за полицейско сътрудничество за справяне с най-важните заплахи за сигурността на ЕС чрез засилване на сътрудничеството между съответните служби на държавите членки, институциите на ЕС и агенциите на ЕС, както и трети държави и организации.

продължи да се доказва като ефективен инструмент срещу организираната престъпност в цяла Европа, например по време на „дните на съвместни действия“ през септември, октомври и ноември 2020 г.[161]. Това е ясен знак за стойността на сътрудничеството. Чрез сътрудничеството бяха подкрепени също така цели, които е по-трудно да бъдат количествено измерени: подобрена разузнавателна картина, обучение и изграждане на капацитет, превенция, сътрудничество с партньори извън ЕС и борба с онлайн престъпността[162]. В независимата оценка на политическия цикъл на ЕС за периода 2018—2021 г./EMPACT през 2020 г.[163] се стигна до заключението, че това е все по-актуален и ефективен начин за справяне с най-належащите заплахи, породени от организираните престъпни групи. Добавената стойност се получава чрез осигуряването на платформа за сътрудничество, която позволява на държавите членки да постигнат по-добри резултати срещу тежката и организираната престъпност, отколкото ако сами посрещат тези проблеми. В оценката бяха набелязани възможностите и дадени препоръки за по-нататъшно развитие на този много полезен инструмент за сътрудничество за следващия цикъл през периода 2022—2025 г.

През 2021 г. Комисията ще стартира инициатива за „**Кодекс за полицейско сътрудничество“ на ЕС** с цел рационализиране, разширяване, развиване, модернизиране и улесняване на сътрудничеството в областта на правоприлагането между съответните национални агенции. Това ще представлява голяма подкрепа за държавите членки в борбата им срещу тежката и организираната престъпност и тероризма.

Необходимо е сътрудничество и между **полицията и други ключови правоприлагащи органи**, както и с агенции като митниците. **Митниците** на ЕС играят ключова роля в гарантирането на сигурността на външните граници и веригата на доставки, като по този начин допринасят за вътрешната сигурност на Европейския съюз. Новите и нарастващите заплахи засягат основните взаимовръзки между митническите и правоприлагащите органи, като се подчертава по-специално стойността на „откриването/предотвратяването“ на митническия контрол и водещата роля на митниците по отношение на стоките. Комисията подкрепя и насърчава сътрудничеството между митниците и Европол[164] с пряко въздействие върху

EMPACT свързва различни заинтересовани страни (чрез мултидисциплинарен подход), за да подобрява и укрепва сътрудничеството между държавите членки, институциите на ЕС и агенциите на ЕС, както и с трети държави и организации, включително частния сектор.

[161] Дни на съвместни действия (ДСД) по EMPACT: „операция BOSPHORUS“, иззети са 1776 огнестрелни оръжия (2—11 ноември), „ДСД Mobile 3“: възстановени са повече от 350 откраднати коли и над 1000 откраднати автомобилни части. (12—13 октомври), „ДСД срещу трафика на хора с цел трудова експлоатация“, служителите установиха 715 потенциални жертви на трудова експлоатация (14—20 септември). „ДСД срещу престъпността в югоизточна Европа“, 51 оръжия от различен тип и 47 килограма различни наркотици (септември).

[162] Всички подробни информационни листове за резултатите с данни, според приоритетите на EMPACT по отношение на престъпността в ЕС, могат да бъдат разгледани тук: https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf, Doc 7623/20,5 май 2020 г.

[163] Извършването на независима оценка беше предвидено в заключенията на Съвета от 27 март 2017 г. относно продължаването на политическия цикъл на ЕС по отношение на организираната и тежката международна престъпност за периода 2018—2021 г. (7704/17).

[164] Вж. например плана за действие на работна група „Митническо сътрудничество“ (CCWP). Основните области за 2020—2021 г. включват: засилено присъствие на митнически служители в бюрата за връзка в Европол, пряк достъп на митническите органи до приложението за мрежа за сигурен обмен на информация на Европол (SIENA), по-добро представителство на митническите

действията в области, сред които огнестрелни оръжия, престъпления против околната среда, финансиране на престъпления и киберпрестъпност. Понастоящем митническите органи участват в няколко ръководени от Европол действия срещу тежката и международната организирана престъпност[165], както и в обучения на CEPOL. Тези дейности помагат за насърчаване и развиване на по-нататъшното междуведомствено сътрудничество и за подобряване на взаимодействието между ключовите участници.

Силните и ефективни информационни системи са необходими за по-добрия обмен на информация между съдебните и правоприлагащите органи в целия ЕС. **Шенгенската информационна система (ШИС)** също беше подсилена чрез актуализирани правила, с които се отстраняват евентуалните пропуски чрез установяване на допълнителни категории сигнали, чрез разширяване на списъка на обектите, за които могат да се въвеждат сигнали, както и чрез разрешаване на въвеждането на нови видове данни[166]. Новите правила влязоха в сила на 28 декември 2018 г. и следва да започнат да функционират пълноценно до декември 2021 г.[167].

По подобен начин през 2019 г. **Европейската информационна система за съдимост (ECRIS)** беше допълнена от система, която позволява ефективен обмен на информация за съдимост за граждани на трети държави, осъдени в ЕС (ECRIS за граждани на трети държави). В момента текат работите по техническото разработване и внедряването на тази нова централизирана система, като се очаква да бъде пусната в експлоатация през 2023 г.

На 24 юли 2020 г. Комисията прие Доклада за преглед на директивата за резервационните данни на пътниците (PNR данните)[168], в който бе направен преглед на първите две години от прилагането на тази директива[169]. Това свидетелства, че разработването на общоевропейска система за PNR данни е в ход. Използването на PNR данни е от съществено значение в борбата с тероризма, тежката престъпност и организираните престъпления и вече дава осезаеми резултати. Само една държава членка все още не е уведомила Комисията за пълното транспониране[170]. На 3 декември 2020 г. Комисията изпрати мотивирано становище за липсата на уведомление за пълното транспониране на директивата.

На 9 септември 2020 г. Комисията публикува оценката на **Директивата за предварителна информация за пътниците** от 2004 г.[171]. В оценката се посочват редица недостатъци и несъответствия, които ще бъдат взети предвид при предстоящото преразглеждане на настоящата законодателна рамка. Друг ключов инструмент за по-нататъшно проучване са **решенията „Прюм“**[172], които ще бъдат

служители в националните звена на Европол и участие на полицейски и митнически ръководители в конвенцията на европейските полицейски ръководители.

165 Измами с акцизи/ДДС, трафик на огнестрелни оръжия, престъпления срещу околната среда, средства с престъпен произход, борба срещу сексуалното насилие над деца.

166 Регламент (ЕС) 2018/1860, Регламент (ЕС) 2018/1861, Регламент (ЕС) 2018/1862.

167 ШИС също ще бъде актуализирана в съответствие с предложените изменения на Регламента за Европол (COM(2020) XXX).

168 COM(2020)305.

169 Директива (ЕС) 2016/681.

170 Словения.

171 SWD(2020) 174.

172 Рамката „Прюм“ дава възможност за автоматичен обмен на ДНК, пръстови отпечатъци и данни за регистрацията на превозни средства между правоприлагащите органи. Публикувана е първоначална оценка на въздействието.

разгледани в светлината на оперативното, технологичното развитие и развитието в съдебната област и областта на защитата на данните.

Сътрудничеството трябва да излезе извън границите на ЕС, за да бъдат ангажирани **ключови трети държави в борбата с тероризма и организираната престъпност**. На 13 май 2020 г. Съветът разреши започването на преговори с Нова Зеландия относно обмена на лични данни между Европол и Нова Зеландия. Преговорите с Турция продължават, но не е постигнат напредък по преговорите относно обмена на лични данни за борба с тежката престъпност и тероризма с Алжир, Египет, Израел, Йордания, Ливан, Мароко, Тунис. Освен това на 19 ноември 2020 г. Комисията прие Препоръка за решение на Съвета, с което се разрешава започването на преговори за сключване на споразумение между Европейския съюз и десет трети държави за сътрудничество между Евроюст и тези трети държави по отношение на обмена на лични данни[173].

Що се отнася до **международното сътрудничество при обмена на PNR данни** за целите на борбата с тероризма и тежката престъпност, Съветът разреши започването на преговори с Япония за подписване на споразумение за резервационните данни на пътниците[174]. Междувременно **съвместните оценки на съществуващите споразумения между ЕС и САЩ, както и между ЕС и Австралия** *са в процес на финализиране.* Комисията също така стартира процес за преглед на цялостния си настоящ подход за предаване на PNR данни на трети държави[175].

Комисията работи също така с ООН за увеличаване на капацитета на държавите партньори за предотвратяване, разкриване, разследване и наказателно преследване на терористични престъпления и други тежки престъпления чрез събиране и анализ на данни за пътниците, както и предварителна информация за пътниците (API), така и PNR.

Комисията се ангажира с процеса на улесняване на предаването на PNR данни в съответствие с правните изисквания на ЕС в рамките на новите стандарти[176] за PNR данните, приети от Международната организация за гражданско въздухоплаване (ИКАО)[177]. На 23 юни 2020 г. Съветът на ИКАО прие новите стандарти и препоръчителни практики (СПП) относно PNR данните[178] и неговите договарящи се страни разполагат със срок до 30 януари 2021 г., за да информират ИКАО за евентуални различия между техните национални практики за регулиране и новите СПП за PNR данните.

2. Приносът на силните външни граници

Модерното и ефективно управление на външните граници е от ключово значение за гарантиране на сигурността на гражданите на ЕС. Мобилизирането на всички

[173] Предложените трети държави са следните: Алжир, Армения, Босна и Херцеговина, Египет, Израел, Йордания, Ливан, Мароко, Тунис и Турция, COM (2020) 743 final.

[174] 18 февруари 2020 г.

[175] Пътна карта за външното измерение на политиката на ЕС относно резервационните данни на пътниците, достъпна на адрес: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12531-External-dimension-of-the-EU-policy-on-Passenger-Name-Records-

[176] Решение (ЕС) 2019/2107 на Съвета.

[177] Резолюция 2396 на Съвета за сигурност на ООН (2017 г).

[178] Нарича се изменение 28 от приложение 9 (Улесняване) към Конвенцията за международно гражданско въздухоплаване („Чикагската конвенция“).

действащи лица, имащи отношение към този въпрос, с цел извличане на максимална полза за сигурността по границите и обезпечаването им с адекватни инструменти, може да окаже реално въздействие върху предотвратяването на трансграничната престъпност и тероризма. В новия пакт за миграцията и убежището[179] се подчертава и необходимостта от стабилно и справедливо управление на външните граници, както и от проверки на самоличността, здравето и сигурността. Това е част от всеобхватен подход, който свидетелства как политиката в областта на миграцията, предоставянето на убежище, интеграцията и управлението на границите зависи от напредъка във всички измерения.

В новия пакт се отбелязва, че ефективно функциониращото Шенгенско пространство е изключително важно за политиката за миграцията и също така води до дълбоки последици за сигурността. Това беше обсъдено на първия Шенгенски форум, проведен на 30 ноември 2020 г. Представители на държавите членки и Европейския парламент се договориха, че ефективно функциониращото Шенгенско пространство е важно за гражданите както по отношение на свободното движение, така и по отношение на сигурността. Този процес ще бъде включен в нова стратегия за Шенгенското пространство, която ще бъде представена през 2021 г. Механизмът за оценка и наблюдение на Шенген представлява ключов инструмент за гарантиране на взаимно доверие и за осигуряване на по-добро и последователно прилагане на достиженията на правото от Шенген, включително неговите последици за сигурността. Това беше важна тема от доклада, приет на 25 ноември[180], в който се представя актуалното състояние на прилагането на достиженията на правото от Шенген и се прави преглед на функционирането на механизма за оценка и наблюдение на Шенген.

Регламентите за оперативна съвместимост[181] имат за цел съществуващите и новите или модернизираните информационни системи на ЕС за управление на сигурността, управление на границите и миграцията да работят съвместно по един по-интелигентен и по-ефективен начин. Оперативната съвместимост между информационните системи на ЕС ще подобри ефективността и ефикасността на проверките по външните граници, ще допринесе за предотвратяване на незаконната имиграция и за високо ниво на сигурност. Чрез нея ще бъде осигурен ценен допълнителен инструмент за правоприлагащите и граничните органи[182]. Държавите членки, асоциираните към Шенген държави и съответните агенции на Съюза (eu-LISA, Европейската агенция за гранична и брегова охрана и Европол) трябва да бъдат подготвени, като Комисията наблюдава подготовката и готовността, за да се гарантира, че до края на 2023 г. ще бъде постигнато пълното прилагане.

На 8 декември 2020 г. съзаконодателите постигнаха предварително споразумение по предложението за **актуализиране на Визовата информационна система**[183].

Необходимо е обаче да бъдат приети **някои ключови законодателни актове**. Европейският парламент трябва да постигне договореност за готовността си да

[179] COM (2020) 609.
[180] SWD(2020)327final.
[181] Регламент 2019/817 и Регламент (ЕС) 2019/818.
[182] Съществуващи системи: Шенгенска информационна система (ШИС), Визова информационна система (ВИС), Евродак и бъдещите системи: Система за влизане/излизане, Система на ЕС за информация за пътуванията и разрешаването им (ETIAS), Европейска информационна система за съдимост за граждани на трети държави (ECRIS-TCN) ETIAS, ECRIS-TCN).
[183] COM(2019)12.

взаимодействия със Съвета относно измененията[184] на Системата на ЕС за информация за пътуванията и разрешаването им (ETIAS)[185].

Връзките между съответните информационни системи за анализ на риска за сигурността са от решаващо значение за подобряването на нашата сигурност. Подобряването на **сътрудничеството между митническите и граничните органи** и взаимодействието между техните **информационни системи** при спазване на съответните принципи на взаимозависимост и взаимоограничаване, включително защитата на личните данни и законодателството за неприкосновеност на личния живот, е приоритет на плана за действие за извеждане на Митническия съюз на следващото ниво от 28 септември 2020 г.[186]. В предварителна оценка, проведена от Комисията с полицейски и митнически експерти от държавите членки, по-специално се препоръчва свързване на Шенгенската информационна система (ШИС) и данните на Европол с митническата система за контрол на вноса (ICS2)[187], а предстои да започне и проучване на осъществимостта.

Регламентът за европейската гранична и брегова охрана[188] влезе в сила през декември 2019 г. и представлява основно преразглеждане на възможностите и инструментите на ЕС за укрепване на външните европейски граници. По този начин значително ще се подобри приносът на граничните служби за сигурността. С новия мандат се повишава способността на Frontex да подпомага държавите членки в управлението на външните граници и връщанията и се разширяват възможностите за сътрудничество с трети държави. В момента се работи за подготовка на постоянния корпус на Европейската гранична и брегова охрана за първото му разполагане от 1 януари 2021 г.

През юни 2019 г. ЕС въведе **по-строги стандарти за сигурност на личните карти**, за да се улесни свободното движение на гражданите на ЕС и в същото време да бъдат намалени измамите със самоличност[189]. Държавите членки трябва да започнат да издават лични карти и документи за пребиваване с нови стандарти за сигурност от август 2021 г. Към момента повечето от тях са в процес на привеждане на дизайна на документите си в съответствие с изискванията на регламента.

3. Засилване на научните изследвания и иновациите в областта на сигурността

С изследванията в областта на сигурността и насърчаването на иновациите се подкрепя координираният отговор на ЕС на сложни предизвикателства и става възможно предприемането на конкретни стъпки за намаляване на рисковете. Съюзът за сигурност е една от четирите приоритетни области в рамките на работната програма по **„Хоризонт 2020“**[190] за периода 2018—2020 г., която представлява 50 % от общото публично финансиране за изследвания на сигурността в ЕС. В резултат на

[184] COM(2019) 3 final и COM(2019) 4 final.
[185] Регламент (ЕС) 2018/1240 и Регламент (ЕС) 2018/1241.
[186] COM(2020)581.
[187] Система за предварителна информация за товарите, използвана за ранна оценка на риска за сигурността на всички движения на стоки, преминаващи през външната граница.
[188] Регламент 2019/1896.
[189] Регламент 2019/1157.
[190] ЕС отпусна финансиране в размер на около 91 милиона евро за проекти за подобряване на защитата на инфраструктурите, включително срещу комбинирани кибер и физически заплахи, за по-добро и бързо реагиране при инциденти и за по-добър обмен на информация.

поканата за изследване на сигурността по „Хоризонт 2020“ за 2019 г. бяха избрани 42 проекта, за които ще бъде отпуснато финансиране от ЕС с размер от общо 253 милиона евро. Работата ще включва защита на инфраструктурата, повишаване на устойчивостта при бедствия, борба с престъпността и тероризма и осигуряване на външните граници, както и подобряване на цифровата сигурност. Предвиденият бюджет, предназначен за проектите през 2020 г., възлиза на 265 милиона евро. В тази сума е включена покана за предложения за изкуствен интелект на стойност 20 милиона евро, която ще подпомогне европейските правоприлагащи агенции да увеличат капацитета за използване на изкуствен интелект, да намалят разликата в уменията си в областта на изкуствения интелект и да засилят сътрудничеството. Дейностите за подготовка по новата рамкова програма за научни изследвания „Хоризонт Европа“ ще спомогнат за изпълнението на стратегията на ЕС за Съюза на сигурност, както и управлението на границите и измерението на сигурността съгласно новия пакт за миграцията и убежището, политиките на ЕС за намаляване на риска от бедствия и Стратегията на ЕС за морска сигурност[191].

Изследванията в областта на сигурността, финансирани от ЕС, се оказаха ефективни и при насърчаване на сътрудничеството и подкрепата на специалистите по сигурността по време на пандемията от COVID-19[192]. Подкрепата включва инструменти за съвместна оценка и разследване на рискове от епидемии, престъпления и заплахи.

За да се осигури внедряването на **иновативни проекти**, агенциите на ЕС трябва да бъдат интегрирани в съществуващата среда за изследвания и иновации в областта на сигурността. След срещата на Съвета по правосъдие и вътрешни работи през октомври 2019 г. агенциите на ЕС и Съвместният изследователски център на Комисията понастоящем създават **център за иновации на ЕС за вътрешна сигурност,** въз основа на действащите правни мандати, който да служи като мрежа за сътрудничество на техните лаборатории за иновации. Центърът ще функционира като механизъм за координация в подкрепа на образуванията, участващи в обмена на информация и знания, създаването на съвместни проекти и разпространението на резултати и разработени технологични решения, които са от значение за вътрешната сигурност[193].

Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежата от национални координационни центрове са отговорът на Европа в подкрепа на иновациите и политиката за киберсигурност в промишлеността. Те имат за цел да се укрепи европейският капацитет за киберсигурност, да се защитят нашата икономика и обществото от кибератаки, да се поддържат високи научни постижения и да се засили конкурентоспособността на ЕС. Понастоящем се провеждат тристранни срещи.

---

[191] В рамките на „Хоризонт Европа“ с клъстер 3 ще бъде подкрепен по-специално приоритетът на политиката на Комисията „Утвърждаване на нашия европейски начин на живот“, както и приоритетите „Европейски зелен пакт“ и „Европа, подготвена за цифровата ера“.

[192] Действия по „Хоризонт 2020“ в подкрепа на реагирането при пандемии могат да бъдат намерени на следния адрес: https://www.researchgate.net/publication/341287556.

[193] На 21 февруари 2020 г. постоянният комитет за оперативно сътрудничество в областта на вътрешната сигурност потвърди в изявлението на мисията основните характеристики, задачите и управлението на центъра за иновации на ЕС за вътрешна сигурност.

4. 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. Друг важен елемент е достъпът на жертвите до упражняване на техните права.

Специалисти по правоприлагане и правосъдие

Ограниченията, свързани с COVID-19, силно засегнаха CEPOL, която беше задължена да отмени всички планирани присъствени дейности от март 2020 г. Тези специални обстоятелства предизвикаха и нарастващо търсене на онлайн услуги; през първите четири месеца на годината Агенцията отбеляза 30 % увеличение на виртуалните дейности и 100 % увеличение на онлайн потребителите. Сред приоритетните области за обучение за 2019—2021 г.[194] са борбата срещу нелегалната имиграция, борбата с тероризма, трафикът на хора и киберпрестъпността и сексуалното насилие над деца. В момента Комисията подготвя оценката на CEPOL, която трябва да приключи до юли 2021 г.

Широката общественост

Кампанията #SaferInternet4EU стартира на Деня за безопасен интернет през 2018 г. Дейностите обхванаха близо 63 милиона души в ЕС през последните 2 години и включват награди, подкрепа за учители и киберхигиена. Мрежата от центрове за безопасен интернет предостави над 1800 нови ресурса по теми като фалшиви новини, кибертормоз, съображения за неприкосновеността на личния живот, поддържане и киберхигиена.

През октомври 2020 г. за осми път беше отбелязан Европейският **месец на киберсигурността** в ЕС, в който се насърчава онлайн сигурността в ЕС. Тази година акцентът на кампанията на европейския месец на киберсигурността се поставя върху проблемите на сигурността, обострени от все по-цифровото ни ежедневие, особено в условията на пандемията от COVID-19. С призива за внимателно използване на интернет (Think Before U Click — „помисли, преди да щракнеш“) вниманието в кампанията се насочва към различни теми, свързани с киберсигурността, така че да се помогне на потребителите да разпознават киберзаплахите и да се подготвят за тях. Тече подготовка за европейското състезание по киберсигурност, което ще се проведе през 2021 г. в Прага.

Ключов инструмент за подпомагане на жертвите на киберпрестъпления е No More Ransom[195], безплатно хранилище на инструменти за дешифриране, което помага на жертвите да се борят, без да плащат на хакерите. С подкрепата на Европейския център за борба с киберпрестъпността на Европол през юли 2020 г. беше отбелязана четвъртата годишнина от неговото създаване, а от пускането му на пазара е използван от над 4,2 милиона посетители от 188 държави, като благодарение на него е предотвратено плащането на искания за откуп на стойност около 632 милиона долара, които щяха да попаднат в ръцете на престъпниците.

[194] Оценка на стратегическите нужди от обучение на Европейския съюз (EU-STNA) за периода 2018—2021 г., доклад за EU-STNA, CEPOL.

[195] https://www.nomoreransom.org/.

На 2 юли 2020 г. Комисията представи **Европейската програма за умения**[196] за постигане на устойчива конкурентоспособност, социална справедливост и устойчивост. В нея са заложени амбициозни количествени цели за подобряване на съществуващите умения и обучение в нови умения, които трябва да бъдат постигнати през следващите 5 години. 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. На 10 ноември 2020 г. Комисията стартира Пакт за умения по време на петото издание на Европейската седмица на професионалните умения през 2020 г. С него се насърчават съвместните действия за увеличаване на въздействието на инвестициите в подобряване на съществуващите умения и обучението в нови умения. Едновременно с пакта бяха обявени първите европейски партньорства за овладяване на умения в три области: автомобилостроенето, микроелектрониката и космическата и отбранителната промишленост.

На 30 септември 2020 г. Комисията прие набор от политически стратегии, които ще имат важно въздействие върху развитието на възможностите на ЕС за сигурност в дългосрочен план. **Планът за действие в областта на цифровото образование за периода 2021—2027 г.**[197] ще стимулира развитието на високоефективна екосистема за цифрово образование с по-добри умения за целите на цифровата трансформация[198]. На същия ден беше прието съобщение относно **европейското пространство за образование** до 2025 г.[199], като ключови акценти бяха основните и цифровите умения. В съобщението относно ново **европейско научноизследователско пространство за научни изследвания и иновации**[200] се определя пътят за подобряване на европейската среда за научни изследвания и иновации и за ускоряване на прехода на ЕС към водеща позиция в областта на цифровизацията, както и борбата с насилието, основано на пола, във всичките му форми, в организациите за научни изследвания и иновации.

Програмата „Еразъм+“ също допринася за борбата с радикализацията чрез проекти за борба с радикализацията, насилническия екстремизъм, социалното изключване, дезинформацията и фалшивите новини[201]. Пример за това е Проектът за превенция на радикализацията в затворите, който има за цел да се повишат компетенциите на персонала на първа линия да идентифицира, докладва и интерпретира сигнали за радикализация и да реагира по подходящ начин[202]. Проектът No Hate BootCamp помогна на младите работници да станат „посланици без реч на омразата“ в своите местни общности.

Самата Комисия се стреми да ангажира обществеността в обсъждания относно политиката на ЕС за сигурност. Действията на равнище ЕС станаха по-видими и

---

[196] COM(2020)274.
[197] COM(2020)624.
[198] https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-communication-sept2020_en.pdf.
[199] COM(2020)625.
[200] COM(2020)628.
[201] До момента са финансирани около 80 проекта, в които са обхванати въпроси, свързани с радикализацията; повече от сто проекта с начини за предотвратяване и борба с кибертормоза и повече от сто проекта, свързани с образование за критично и етично използване на интернет с оглед справяне с онлайн дезинформацията.
[202] http://www.r2pris.org/.

достъпни за гражданите чрез новия **уебсайт за Стратегията за сигурност на ЕС**[203]. Започнаха няколко **обществени консултации**, които дават възможност на гражданите да влияят пряко върху формирането на политиката.

Всички жертви на престъпления имат право на подкрепа и защита, но жертвите на най-тежките престъпления като тероризъм или сексуална експлоатация на деца се нуждаят от специално внимание. На 24 юни 2020 г. Комисията прие първата по рода си **стратегия на ЕС за правата на жертвите (2020—2025 г.)**[204]. Тя се отнася за жертвите на всички престъпления, но в нея се обръща специално внимание на най-уязвимите, включително жертвите на тероризъм, децата, станали жертва на сексуална експлоатация, и жертвите на трафик на хора. На 22 септември 2020 г. Комисията организира Конференция на високо равнище за правата на жертвите, по време на която откри **платформата за правата на жертвите**, за да насърчи по-хоризонтален подход към правата на жертвите[205]. Комисията също така назначи своя първи по рода си **координатор за правата на жертвите**, за да подкрепи съгласуваността и ефективността в политиката за правата на жертвите.

По отношение на **жертвите на тероризъм** през януари 2020 г. беше създаден Център на ЕС за експертен опит за жертвите на тероризъм, за да бъдат предложени експертен опит, насоки и подкрепа за националните органи и организациите за подкрепа на жертвите. Той насърчава трансграничния обмен на най-добри практики и споделянето на експертен опит между работещите в тази сфера и специалистите. Той няма за цел да се предлага пряка помощ на определени жертви на тероризъм, а да бъдат подкрепени националните структури при предоставянето на професионална помощ и подкрепа, както и насоки, които да бъдат публикувани през 2020 г. Центърът на ЕС е пилотен проект, който ще продължи две години. Председателството на Съвета полага усилия да подкрепи тази инициатива с мрежа от единни национални точки за контакт за жертвите на тероризъм.

VI ЗАКЛЮЧЕНИЕ

Стратегията за Съюза на сигурност беше създадена с цел осигуряване на цялостен и динамичен подход. Неотдавнашните терористични атаки отново показаха как трябва да може да реагира ЕС, укрепвайки нашата устойчивост и способност за отговор чрез модернизация и ефективно разгръщане на ключовите инструменти, с които разполагаме. Те показват и необходимостта всички участници да бъдат изцяло включени в общ подход, така че държавите членки, институциите на ЕС, частният сектор, неправителствените организации (НПО) и самите граждани да могат да играят роля в изграждането на достатъчно силна и гъвкава система за сигурност, която да функционира ефективно. Този съгласуван и последователен подход е и най-

[203] https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union-strategy_en.

[204] COM(2020) 258.

[205] Платформата ще обедини за първи път всички съответни участници на равнище ЕС в областта на правата на жертвите. Тя ще включва Комисията и ключови заинтересовани страни, като например Европейската мрежа за правата на жертвите, европейската мрежа от национални точки за контакт относно обезщетението, координатора на ЕС за борбата с тероризма, съответните агенции като Евроюст, Агенцията за основните права, Агенцията на Европейския съюз за обучение в областта на правоприлагането, Европейския институт за равенство между половете и гражданското общество.

добрият начин да бъдем уверени, че нашите основни права са защитени като част от утвърждаването на европейския ни начин на живот.

В настоящия доклад са цитирани многобройните работни направления, по които се работи в момента. В него се посочва също така как трябва да бъде запазена набраната скорост. Целта на представената днес Програма на ЕС за борба с тероризма е да се укрепи европейската рамка за противодействие на тероризма, като бъдат очертани следващите необходими стъпки: да се предвижда и предотвратява тероризмът, да бъдат защитени гражданите и инфраструктурата и да има готовност за реагиране, като се има предвид връзката между вътрешната и външната сигурност. Вече сме повишили степента на сътрудничество, полагат се повече усилия за справяне с радикализацията, налице са повече инструменти за лишаване на терористите от средства за атака. Сега трябва да се направи следващата крачка напред. Най-важното е да се осигури приемането на нови правила за справяне с терористичното съдържание онлайн, като основен приоритет тази година е постигането на споразумението в тази насока. Комисията също така настоятелно призовава държавите членки да ускорят прилагането на всички договорени законодателни актове. Обезпечаването на сигурността на гражданите на ЕС е обща отговорност и предприемането на общи действия трябва да бъде колективна амбиция за по-сигурна Европа.