ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 15.5.2024 г.
COM(2024) 198 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

относно седмия доклад за напредъка по прилагането на Стратегията на ЕС за Съюза на сигурност

I ВЪВЕДЕНИЕ

През юли 2020 г. ЕС прие Стратегията за Съюза на сигурност за периода 2020—2025 г.[1] Създадена в разгара на пандемията от COVID-19, тази стратегия се появява на фона на усложняваща се обстановка по отношение на сигурността, с хибридни и терористични заплахи, насочени към сигурността на европейските граждани и предприятия както във физическото пространство, така и в киберпространството. Действията на ЕС в отговор на тези предизвикателства се основаваха на цялостен подход към сигурността, обхващащ цялото общество, с цел премахване на разделението между различните политики в областта на сигурността и свързване на точките в цялата европейска екосистема на сигурността.

Четири години по-късно геополитическият и икономическият контекст и обстановката по отношение на сигурността в рамките на ЕС и в съседните му държави се промениха коренно и трайно. Рисковете, пред които сме изправени понастоящем, се различават значително от рисковете, които са имали доминираща роля при първоначалното оформяне на идеята за Стратегията за Съюза на сигурност. Пандемията от COVID-19 насочи вниманието към зависимостта на нашите общества и икономики от информационните и комуникационните мрежи, както и от свързаните с тях продукти, и към необходимостта да се гарантира тяхната киберсигурност в условията на бързо развиваща се и изключително адаптивна киберпрестъпност.

Равнището на терористичната заплаха на европейска територия се запазва и редица държави членки наскоро повишиха оценката на заплахата на своя територия до най-високото ниво. Заплахата за стабилността от организираната престъпност продължава да се засилва, като провеждането онлайн на голяма част от търговията и на взаимодействието между хората отваря нови възможности за престъпна дейност. Тъй като милиони хора станаха по-уязвими поради липсата на стабилност в съседните на ЕС държави, контрабандата на мигранти и трафикът на хора се превърнаха в основна цел за лицата, които извличат печалби от престъпна дейност, като експлоатират други хора. Инструментализирането на мигрантите по външните ни граници извади на преден план нови, хибридни форми на заплахи, които в съчетание с кампаниите за дезинформация имат за цел да породят разделение и недоверие в европейските общества. И накрая, потенциалното използване от злонамерени субекти на нови технологии, като например изкуствения интелект, за целите на киберпрестъпността или за манипулиране на информация, поставя нови предизвикателства пред сигурността на нашите демокрации, особено в годината, когато в цяла Европа се провеждат важни избори.

Вътрешната и външната сигурност са взаимно свързани. Руската агресивна война срещу Украйна доведе до увеличаване на кибератаките[2] и разкри потенциалната уязвимост на част от критичната инфраструктура на ЕС. Настоящата ситуация в Близкия изток и безпрецедентният мащаб на насилието в региона засилиха предизвикателствата пред поддържането на вътрешната сигурност на ЕС, с повишен риск от терористични атаки, както от извършители, които действат сами, така и от организирани групи, подпомагани от опити за разпространение на терористично съдържание чрез онлайн платформи и мрежи.

---

1 COM(2020) 605.

2 Доклад относно картината на заплахите на ENISA за 2023 г., стр. 10—11.

В тази променяща се картина на заплахите визията, изложена в Стратегията за Съюза на сигурност, се оказа от особено значение. Не всички рискове могат да бъдат отстранени, но уязвимостта може да бъде преодоляна, а Стратегията на ЕС за Съюза на сигурност осигури стабилна рамка за изграждане на капацитет на ЕС да се противопостави на съществуващите и нововъзникващите заплахи с единна цел и с подобрени колективни механизми за действие. Настоящият седми доклад за напредъка на Съюза на сигурност има за цел да представи преглед на изпълнението на стратегията от нейното приемане през 2020 г. насам. Комисията разгледа всички точки, които първоначално бяха изтъкнати в Стратегията на Съюза за сигурност, но бяха включени и нови инициативи в отговор на променящите се предизвикателства пред сигурността. От решаващо значение за ефективната защита на гражданите на ЕС срещу заплахите за сигурността сега е приключването на оставащите досиета, които все още не са одобрени от Парламента и Съвета, както и прилагането и изпълнението на договореното законодателство от държавите членки.

II ПО-ДОБРЕ ЗАЩИТЕНА И ПО-УСТОЙЧИВА ФИЗИЧЕСКА И ЦИФРОВА ИНФРАСТРУКТУРА

II.1. Критична инфраструктура

Гражданите, предприятията и органите в ЕС разчитат на критичната инфраструктура, която е в основата на услуги със съществено значение, като например енергоснабдяване, водоснабдяване и снабдяване с храни, транспорт и телекомуникации. Ежедневният живот на гражданите и дългосрочното здраве на икономиката зависят от предоставянето на тези услуги. Геополитическият контекст обаче, в който функционира критичната инфраструктура в ЕС, е в голяма степен нестабилен. Той беше влошен от агресивната война на Русия срещу Украйна, както показаха зачестилите хибридни атаки, както и саботажът на газопровода „Северен поток“ и повредите по газопровода на Балтийската връзка.

От началото на мандата на настоящата Комисия ЕС предприе различни мерки за подобряване на защитата на критичната инфраструктура и устойчивостта на субектите, които я експлоатират, за да се избегне или смекчи въздействието от прекъсванията на основните услуги. С приемането на **Директивата относно устойчивостта на критичните субекти** („Директива за УКС“)[3] и преразгледаната **Директива за сигурност на мрежовата информация** („Директива МИС 2“)[4] ЕС укрепи правната рамка, за да се справи с настоящите и бъдещите онлайн и офлайн рискове — от кибератаките до природните бедствия. След транспонирането на директивите от държавите членки ще се гарантира, че рисковете и уязвимостите, засягащи субектите в редица ключови сектори,[5] се вземат под внимание в по-голяма степен. За да се ускори изпълнението на двете директиви, препоръка на Съвета[6] послужи като основа за провеждане на стрес тестове със субекти, експлоатиращи критична инфраструктура, като

[3] Директива (ЕС) 2022/2557 от 14 декември 2022 г. относно устойчивостта на критичните субекти.

[4] Директива (ЕС) 2022/2555 от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза.

[5] Секторите, обхванати от Директива МИС 2 и Директивата за УКС, включват енергетика, транспорт, банково дело, инфраструктура на финансовите пазари, цифрова инфраструктура, здравеопазване, питейна вода, отпадъчни води, публична администрация, космическо пространство и производство, преработка и разпространение на храни.

[6] Предложението на Комисията COM(2022) 551 беше последвано от препоръка на Съвета 2023/C 20/01.

се започне от енергийния сектор, където резултатите понастоящем се анализират от Комисията.

Неотдавнашните събития показаха необходимостта от спешни действия на равнището на ЕС при възникването на инцидент. Комисията предложи[7] **препоръка на Съвета относно подробен план,** относно координиран отговор на равнището на Съюза на смущения в критичната инфраструктура със значително трансгранично значение. В **законодателния акт за извънредните ситуации и устойчивостта на вътрешния пазар** ще бъдат предвидени средства за осигуряване на непрекъснато функциониране на вътрешния пазар по време на криза.

Комисията също така предприе действия за повишаване на устойчивостта на критичната инфраструктура на **секторно равнище**, като се основава на базата, установена от хоризонталното законодателство. В **енергийния сектор** работата по създаването на мрежов кодекс за специфични за сектора правила относно аспектите на киберсигурността на трансграничните потоци на електроенергия ще спомогне за повишаване на устойчивостта и сигурността на електроенергийната система на ЕС. Комисията също така обяви **Плана за действие в областта на вятърната енергия,** за да засили киберустойчивостта на ветроенергийните паркове. В **транспортния сектор** Комисията продължи работата по системата за проверки на сигурността на въздухоплаването и мореплаването, с над 100 извършени проверки в областта на въздухоплаването и 60 проверка в областта на мореплаването. Ще се отнася до **сигурността на мореплаването**, преразгледаната Стратегия на ЕС за морска сигурност[8] и планът за действие към нея бяха одобрени през октомври 2023 г., за да се осигури по-добра защита на критичната морска инфраструктура и на корабите от физически заплахи и киберзаплахи. Комисията също така разработва **обща среда за обмен на информация**, за да се улесни обменът на информация между морските органи през границите и между отделните сектори. Прегледът на **Регламента относно трансевропейската транспортна мрежа**[9] предвижда нови изисквания за защита от рискове за държавите членки, за да се гарантира, че ключовата транспортна инфраструктура на Съюза е ефективно защитена. След извършване на задълбочена оценка на риска в **сектора на инфраструктурата за свързаност** в ЕС с държавите членки и ENISA, Комисията направи редица препоръки за повишаване на киберсигурността и устойчивостта, като например определяне през февруари 2024 г.[10] на действия за подобряване на сигурността на инфраструктурите на подводните кабели, които са от съществено значение за нашите комуникационни мрежи. В съобщението относно управлението на **климатичните рискове** са определени основните категории действия, включително подобреното използване на наличните спътникови данни и услуги за укрепване на устойчивостта на критичната инфраструктура[11].

В **космическия сектор космическата стратегия на ЕС за сигурност и отбрана**[12], приета през март 2023 г., включва действия за повишаване на устойчивостта на системите и услугите в космическия сектор и за по-нататъшно разработване на базирани в космоса услуги на ЕС с двойна употреба. По отношение на **водопроводните системи,**

---

7 COM(2023) 526.

8 JOIN (2023) 8.

9 Предварително споразумение от 24 април 2024 г. относно Регламента на Европейския парламент и на Съвета относно насоките на Съюза за развитието на трансевропейската транспортна мрежа.

10 C(2024) 1181.

11 COM (2024) 91.

12 JOIN(2023) 9 final.

в **ръководството към Плана за сигурност на водните ресурси** са обхванати мерките за сигурност за противодействие на враждебни действия срещу физическата и кибернетичната цялост на системите за водоснабдяване и умишленото замърсяване на водата[13]. Във **финансовия сектор** с приемането на **Регламента относно оперативната устойчивост на цифровите технологии (DORA)**[14] се засилва устойчивостта в областта на цифровите технологии на субектите от финансовия сектор на ЕС чрез рационализиране и модернизиране на съществуващите правила. И накрая, в **сектора на здравеопазването,** като част от Европейския здравен съюз[15], **Органът за готовност и реакция при извънредни здравни ситуации (HERA)** подкрепя научноизследователската и развойната дейност, производството и доставката на медицински изделия за противодействие. Освен това модулът за управление на кризи на системата на ЕС за ранно предупреждение и реагиране се разширява, за да подпомогне координирането на сериозните заплахи за здравето и здравните системи и да осигури непрекъсната координация по отношение на заплахите за здравето в рамките на ЕС и на световно равнище. Първите шест европейски референтни лаборатории в областта на общественото здраве бяха номинирани през март 2024 г., а планът на Съюза за предотвратяване, готовност и реакция е в процес на разработване и ще бъде завършен и тестван до края на 2024 г.

II.2. Киберсигурност

Картината на киберзаплахите значително се влоши през последните години, което се доказва от драматичното нарастване на атаките по веригата на доставките и използването на уязвимости в софтуера, операционните системи за мобилни устройства или персонални компютри и виртуалните частни мрежи. Увеличават се кибератаките[16], насочени към тежката промишленост, информационните услуги, правителството и здравеопазването. Софтуерът за изнудване все още е предизвикателство не само по отношение на броя на атаките, но и на нарастващите случаи на тайни споразумения между престъпни групи и държавни участници, водени от интереси, различни от финансовата изгода[17]. В условията на тези увеличаващи се и развиващи се киберзаплахи, ЕС предприе значителни стъпки за подобряване на киберсигурността в държавите членки, укрепване на сигурността на веригите на доставките и продуктите, засилване на солидарността на равнището на ЕС и повишаване на капацитета за откриване, подготовка и реагиране на киберзаплахи и инциденти.

През настоящия мандат беше поставена здрава основа за непрекъснатите усилия на ЕС да защити цифровата си инфраструктура. При **преразглеждането на Директивата МИС** нейният обхват беше значително разширен, за да включва всички средни и големи субекти, работещи в 18 критични сектора, с по-строги изисквания за киберсигурност, задължително докладване на инциденти и европейска структура за координация при киберкризи, предвидена по закон. Сред другите постижения са постигнатото споразумение по **законодателния акт за киберустойчивостта**[18] и приемането на

[13] Хранилище за публикациите на Съвместния изследователски център — Ръководство за прилагане на Плана за сигурност на водните ресурси за системи за питейна вода.

[14] Регламент (ЕС) 2022/2554 на Европейския парламент и на Съвета от 14 декември 2022 г. относно оперативната устойчивост на цифровите технологии във финансовия сектор.

[15] Съобщение относно Европейския здравен съюз.

[16] Доклад относно картината на заплахите на ENISA за 2023 г., стр. 10—11.

[17] Вж. например: https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime

[18] Предварително споразумение бе постигнато на 30 ноември 2023 г. Очаква се то да влезе в сила през 2024 г.

Регламента за европейска цифрова самоличност[19], което значително ще подсили цялостната ни киберсигурност. Със законодателния акт за киберустойчивостта ще бъдат въведени задължителни изисквания за киберсигурност „на етапа на проектирането“ и „по подразбиране“ за хардуера и софтуера, през целия жизнен цикъл на продукта, като се гарантира, че продуктите се доставят на пазара без известни уязвимости. С Регламента за европейска цифрова самоличност ще се улесни развитието на цифровия единен пазар въз основа на удостоверителни услуги и той ще бъде ключов елемент в усилията за справяне с фишинг атаките и подобряване на удостоверяването и управлението на достъпа. Междувременно на 1 август 2025 г. ще влязат в сила новите правила съгласно **Директивата за радиосъоръженията**, определяйки задължения за производителите на безжични устройства да подобрят нивото си на киберсигурност, поверителността и защитата от измами.

Законодателният акт за киберсолидарност[20] ще бъде повратен момент в откриването на киберзаплахи, готовността и реагирането при инциденти на равнището на ЕС. В него е предвидено създаването на Европейска система за предупреждение в областта на киберсигурността, която ще се състои от общоевропейска мрежа от киберцентрове, с цел изграждане на координирани способности на ЕС за откриване и обща ситуационна осведоменост. Механизъм за действие при извънредни ситуации в областта на киберсигурността ще засили готовността и капацитета за реагиране и възстановяване на държавите членки. Ще бъде създаден киберрезерв на ЕС с цел подпомагане на реакцията при значителни и широкомащабни инциденти в областта на киберсигурността и първоначалното възстановяване, който ще бъде на разположение на държавите членки, институциите на ЕС и трети държави, асоциирани към програмата „Цифрова Европа“.

Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността следва да стане напълно автономен през тази година и ще повиши капацитета и конкурентоспособността на Европа в областта на киберсигурността, като защитава нейната икономика и общество от кибератаки и укрепва нейния технологичен суверенитет чрез съвместни инвестиции в стратегически проекти в областта на киберсигурността.

Приемането на първата европейска **схема за сертифициране на киберсигурността**[21]**,** с помощта на общи критерии на ЕС, е друга важна стъпка в посока създаването на такава среда на вътрешния пазар, на която предприятията и потребителите могат да се доверят. В работната програма на Съюза относно европейската схема за сертифициране на киберсигурността[22], приета през февруари 2024 г., са определени стратегически приоритети за бъдещите европейски схеми за сертифициране на киберсигурността. Актът за киберсигурността беше изменен, за да се създаде възможност за схеми за сертифициране на киберсигурността за управлявани услуги за сигурност, които Комисията ще поиска от ENISA, след влизането му в сила. Работи се по други схеми, като например европейската схема за сертифициране на киберсигурността за облачни услуги, които ще помогнат на потребителите да вземат информирани решения относно услугите, които купуват. Колкото по-високи са нивата на чувствителност на данните и на търсената гаранция, толкова по-строги следва да бъдат изискванията в тези схеми.

[19] Предварително споразумение бе постигнато на 8 ноември 2023 г.
[20] COM(2023) 209.
[21] C(2024) 560, приета на 31 януари 2024 г.
[22] Работен документ на службите на комисията SWD(2024) 38.

Междувременно ЕС предприе стъпки за укрепване на **киберсигурността на институциите, органите, службите и агенциите на ЕС**, като създаде рамка за управление на риска за киберсигурността, както и за ръководство и контрол в областта на киберсигурността, засили ролята на CERT-EU и установи нов междуинституционален съвет по киберсигурност, който да наблюдава и подпомага нейното прилагане. Въпреки това липсата на напредък в преговорите по паралелното предложение относно информационната сигурност, което е от съществено значение за завършването на солидна законодателна рамка за институциите, агенциите и органите на ЕС и по този начин допринася за сигурна европейска администрация, следва да се разгледа като приоритет.

За да допълни интензивната законодателна работа през последните години, Комисията работи за засилване на **оперативното сътрудничество с държавите членки.** Създаването на първите трансгранични мрежи от центрове за операции по сигурността, както и помощта, предоставена през последните две години на държавите членки чрез действието за подкрепа на ENISA с 35 млн. евро по програмата „Цифрова Европа“, показаха как ЕС може да осигури сигурност на своите граждани чрез обединяването на ресурси за повишаване на капацитета за киберсигурност.

За да гарантира икономическа сигурност и отворена стратегическа автономност, ЕС също така възприе проактивен подход за **справяне с рисковете за киберсигурността в нововъзникващите технологии**. Съгласно стратегията за икономическа сигурност се извършват общи оценки на риска във връзка с технологиите от критично значение като изкуствения интелект, авангардните полупроводникови технологии, биотехнологиите и квантовите технологии[23]. За да защити данните и да осигури конфиденциалността на комуникациите, Комисията издаде препоръка[24], с която призовава държавите членки да разработят и приложат координирана пътна карта за прехода към пост-квантова криптография (PQC) в целия ЕС. В препоръката държавите членки се насърчават да оказват подкрепа за разработването на съответните алгоритми и стандарти за пост-квантова криптография, които да бъдат приложени в целия Съюз.

Прилагането на инструментариума на ЕС за сигурността в областта на 5G[25] е от ключово значение, за да се гарантира, че 5G и пост-5G мрежите и технологиите, свързани с тях, са надеждни и защитени в киберпространството. В съответствие с инструментариума Комисията ще се стреми да избягва излагането на корпоративните си комуникации на въздействието на мобилни мрежи, които използват високорискови доставчици, както и да отразява своята оценка във всички съответни програми и инструменти на ЕС за финансиране[26]. Подходът на ЕС към киберсигурността вече обхваща не само превенцията и защитата на критичната инфраструктура, но и **управлението на кризи,** включително със създаването и официалното утвърждаване на **Европейската мрежа за връзка на организациите при кибернетични кризи (EU-CyCLONe)**. Развитието на екосистема от заинтересовани страни и мрежи за управление на кризи засили готовността на ЕС за колективни действия в случай на сериозен киберинцидент. Добрата координация между различните нива (техническо, оперативно и политическо) и силните полезни взаимодействия между различните общности в областта на киберсигурността изискват редовни упражнения и взаимодействия между

[23] C(2023) 6689.
[24] C(2024) 2393.
[25] Група за сътрудничество за МИС 1/2020, *Киберсигурност на 5G мрежите — инструментариум на ЕС от мерки за смекчаване на риска.*
[26] C(2023) 4049.

отделните сектори, оценки на риска, стрес-тестове и документация, която е ясна, актуална и разбираема за всички участници.

Сигурността и конкурентоспособността на ЕС зависят от наличието на работна сила с професионална квалификация в областта на киберсигурността. Въпреки това Съюзът е изправен пред значителен недостиг на специалисти в областта на киберсигурността, което увеличава рисковете пред ЕС, неговите държави членки, предприятията и гражданите от киберинциденти, които може да не бъдат засечени бързо или да не бъдат посрещнати с адекватна и навременна реакция[27]. Създаването на **Академия за киберумения** ще помогне за справяне с този проблем, като обедини и подобри координацията на съществуващите инициативи за обучение за придобиване на умения в областта на киберсигурността. Нарастващият брой ангажименти към академията показва желанието на отрасъла и на академичната общност да станат основни участници в насърчаването на по-голям брой специалисти, включително млади жени, да станат част от областта на киберсигурността.

В новата **политика на ЕС в областта на киберотбраната** се установяват средствата за подобряване на координацията между цивилните общности в областта на киберсигурността и военната/отбранителната екосистема, като връзките между тези две области вероятно ще се увеличават в бъдеще. Политиката също така дава възможност на ЕС и неговите държави членки да повишат капацитета си да защитават, откриват, отбраняват и възпират, като използват по подходящ начин целия набор от възможности за защита, достъпни за гражданските и военните общности в по-широкия контекст на сигурността и отбраната на ЕС, в съответствие с международното право. В новата политика е подчертана необходимостта от по-силно сътрудничество между публичния и частния сектор и са предложени начини това да се случи.

ЕС в действие

От създаването си насам ENISA е изготвила 70 доклада за ситуационна осведоменост, като са анализирани повече от 4 000 инцидента. Обработила е 22 обаждания за мащабни инциденти. ENISA съвместно е организирала редица учения с реални действия в областта на киберсигурността, най-новото от които, в съвместно домакинство с Комисията, тества готовността на Европейската мрежа за връзка на организациите при кибернетични кризи (EU-CyCLONe), която обединява националните органи на държавите членки, отговарящи за управлението на киберкризи, и Комисията. Такива учения подобряват координацията и по този начин смекчават въздействието на евентуални бъдещи атаки в ЕС.

В рамките на програмата „Цифрова Европа“ Комисията разпределя бюджет от 84 млн. евро за подпомагане на действията в подкрепа на киберсигурността съгласно новото законодателство на ЕС, включително прилагане на изкуствен интелект и други базови технологии за центрове за операции по сигурността, както и прехода на Европа към пост-квантова криптография. Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще помогне да се гарантира, че тези проекти са от полза за бизнеса, МСП и публичните администрации в държавите членки и асоциираните държави.

[27] ENISA, *Прогнозиране на киберзаплахите до 2030 г., актуализиране до 2024 г.*

III БОРБА С ТЕРОРИЗМА И РАДИКАЛИЗАЦИЯТА

III.1. Мерки за борба с тероризма

Заплахата от тероризъм продължава да бъде сериозна и съществува риск да бъде засегната от конфликти извън ЕС. Според Европол[28] през 2022 г. от държавите членки са докладвани 28 извършени, неуспешни или осуетени атаки, което представлява увеличение в сравнение с 2021 г. (18 атаки), но намаление спрямо 2020 г., когато са докладвани 56 атаки. От атаката на Хамас на 7 октомври 2023 г. насам в някои общности в държавите членки се наблюдава повишено напрежение, за което свидетелстват три терористични атаки (Арас във Франция на 13 октомври, Брюксел на 16 октомври и Париж на 2 декември 2023 г.). Успоредно с това някои държави членки са изправени пред значителна заплаха от насилствен крайнодесен екстремизъм. Съобщава се, че от 7 октомври 2023 г. насам са се увеличили възхвалата на тероризма и словото на омразата, по-специално под формата на антисемитизъм и антимюсюлманска омраза[29].

Съгласно Стратегията за Съюза на сигурност бяха приети набор от мерки и инструменти за подпомагане на държавите членки в борбата срещу тероризма. След като бе приета през декември 2020 г., **Програмата на ЕС за борба с тероризма**[30] даде възможност на ЕС по-добре да предвижда, предотвратява, защитава и реагира на терористични заплахи. Директивата за борба с тероризма,[31] приета през 2017 г., понастоящем се прилага от всички държави членки, като обучението и пътуването с цел тероризъм, както и финансирането на тероризма са криминализирани. В редица държави членки за недостатъците по отношение на транспонирането на директивата се търси решение посредством производства за установяване на нарушения и бяха организирани няколко семинара, за да се гарантира, че законодателството постига пълното си въздействие при прилагането.

Някои **чуждестранни бойци терористи** се завърнаха в ЕС, но значителен брой продължават да бъдат в лагери и затвори в Североизточна Сирия. Макар че основната отговорност е на държавите членки, сътрудничеството на равнището на ЕС им помага да се справят с предизвикателства като наказателното преследване на извършителите на терористични престъпления, предотвратяването на неоткритото влизане в Шенгенското пространство със системни проверки в Шенгенската информационна система, като се използват пълноценно нейните функции, и реинтеграцията и реабилитацията на завърналите се чуждестранни бойци терористи. Както Европол, така и Евроюст изиграха ключова роля в координирането на тези разследвания и наказателни преследвания.

Лишаването на терористите от средствата за извършване на атака е от ключово значение в борбата срещу тероризма. Новото **законодателство относно огнестрелните оръжия** ще повлияе върху възможността на терористите да имат достъп до оръжия в ЕС. Новото законодателство, предназначено да ограничи достъпността на **прекурсорите на взривни вещества,** които терористите биха могли да използват за производство на бомби, влезе в сила през февруари 2021 г.[32] Въз основа на подхода, използван за

[28] Европол 2023 г., Доклад за 2023 г. относно обстановката и тенденциите в Европейския съюз, свързани с тероризма.

[29] Вж.: isdglobal.org, 31 октомври 2023 г.; isdglobal.org, 2 ноември 2023 г.

[30] COM(2020) 795.

[31] Директива (ЕС) 2017/541 от 15 март 2017 г. относно борбата с тероризма.

[32] Регламент (ЕС) 2019/1148 от 20 юни 2019 г. за предлагането на пазара и употребата на прекурсори на взривни вещества.

регулиране на достъпа до прекурсори на взривни вещества, Комисията извърши оценка на въздействието на регулирането на достъпа до **високорискови химикали.** Освен това бързият напредък в областта на изкуствения интелект и биотехнологиите води до намаляване на пречките пред достъпа до опасни химикали и патогени, което увеличава риска от химични и биологични аварии.

За да **повиши готовността**, Комисията изгражда европейски стратегически резерви от капацитет чрез rescEU и HERA за реакция при химически, биологични, радиологични и ядрени заплахи. Тези стратегически резерви гарантират, че мерките за противодействие, включително оборудването, са на разположение за защита срещу последиците от инциденти. ЕС продължи да укрепва рамката на ЕС за **предотвратяване и борба с изпирането на пари и финансирането на тероризма** и следи отблизо изпълнението, за да гарантира, че законодателството има принос за по-ефективното разкриване на средства, предназначени за финансирането на терористични организации. В подкрепа на разследванията, свързани с финансирането на тероризма, през 2021 г. Комисията също така установи **мрежа от финансови следователи за борба с тероризма**. Мрежата, председателствана от Комисията, подпомага обмена между следователите на държавите членки на техники и опит в борбата с финансирането на тероризма.

Защитата на хората и обществените пространства е приоритет на Програмата за борба с тероризма. Чрез програмата на ЕС за консултанти по въпросите на защитата и сигурността повече от 100 специално обучени национални експерти и експерти от Комисията са на разположение да провеждат, по искане на орган на държава членка и финансирани от Комисията, мисии за оценка на уязвимостта, за да помагат за опазването от терористични заплахи на обществените пространства, високорисковите събития и критичната инфраструктура в ЕС. Както е отразено в съвместното съобщение на Комисията и на върховния представител от 6 декември 2023 г.[33], озаглавено „Няма място за омраза: Европа, обединена срещу омразата“, увеличено е финансирането за защитата на обществените пространства и местата за богослужение на всички вероизповедания. От 2020 г. насам чрез **фонд „Вътрешна сигурност“** е осигурен бюджет от 30 млн. евро за програмата „PROTECT“, в която е обърнато специално внимание на опазването на местата за богослужение, включително синагоги и джамии: допълнителни 5 млн. евро помагат за справяне с конкретни заплахи от нарастващия антисемитизъм. Комисията работи с гражданското общество в борбата със словото на омразата, например чрез Европейския граждански панел за борба с омразата в обществото.

Безпилотните летателни апарати стават все по-разпространен и достъпен инструмент, който може да се използва за легитимни, но също така и за злонамерени цели, включително атаки на обществени пространства и срещу лица и критична инфраструктура. През октомври 2023 г. Комисията прие съобщение относно противодействие на заплахите, произтичащи от предназначени за гражданска употреба безпилотни летателни апарати, които не оказват съдействие[34]. Сред вече изпълнените ключови действия са създаването на експертна група за противодействие на безпилотните летателни апарати, която ще консултира на равнище политики и на оперативно равнище, както и извършването на специална оценка на риска относно заплахата, представлявана от безпилотни летателни апарати, които не оказват съдействие, за гражданската авиация и летищните съоръжения. Комисията също така извърши **цялостно картографиране на рисковете за сигурността на**

[33] JOIN(2023) 51.
[34] COM/2023/659.

въздухоплаването, за да направи преглед на съществуващите и променящите се заплахи и уязвимости с оглед актуализиране на базовото ниво на режима на сигурност на въздухоплаването на летищата в ЕС[35].

III.2. Предотвратяване на радикализацията и борба с нея

Предотвратяването на радикализацията е първата стъпка към предотвратяването на терористични атаки. Комисията засили подкрепата си за държавите членки, за да помогне за предотвратяването на излагането на гражданите на вредно екстремистко и терористично съдържание онлайн и офлайн, включително в затворите. Чрез Мрежата за осведоменост по въпросите на радикализацията Комисията обединява 6500 практикуващи специалисти (създатели на политики, правоприлагащи органи, изследователи) от цяла Европа, за да разработят най-добри практики за справяне с насилническия екстремизъм. От юни 2024 г. Мрежата за осведоменост по въпросите на радикализацията ще бъде интегрирана в Центъра на знанията на ЕС за предотвратяване на радикализацията. С **Центъра на знанията на ЕС**, ЕС има за цел да премахне разделението между съответните създатели на политики, практикуващи специалисти и изследователи, като предоставя задълбочени проучвания, прогнозни сценарии, подкрепа за действия в отговор на геополитически промени, обучения по стратегическа комуникация, както и инструменти за разработване на политики и практики за противодействие на радикализацията. Комисията също така прие Препоръка относно процесуалните права на заподозрените и обвиняемите, които са обект на предварително задържане, и относно материалните условия на задържане[36], която включва мерки за справяне с проблема с радикализацията в затворите.

ЕС също така работи за предотвратяване на чужди влияния и финансиране за насърчаване на радикални/екстремистки възгледи в държавите членки. Комисията продължава да бъде бдителна, за да предотвратява използването на средства от ЕС за финансирането на проекти, несъвместими с европейските ценности, или преследването на незаконни цели. В преразгледания Финансов регламент[37] въпросът за убеждението за „подбуждане към омраза“ вече е добавен като основание за изключване от финансиране от ЕС. През януари 2024 г. Комисията издаде нови насоки за ръководителите на финансови програми относно последиците от нарушаването на ценностите на ЕС.

Дезинформация, предназначена да подбужда омраза, и терористично съдържание, включително генерирани от изкуствен интелект изображения, циркулират онлайн и може да вдъхновят актове на насилнически екстремизъм. Ключов инструмент за предотвратяване на разпространението на терористично съдържание онлайн е **Регламентът относно справянето с разпространението на терористично съдържание онлайн**[38], който задължава доставчиците на хостинг услуги да премахват терористично съдържание или да блокират достъпа към него в срок от един час от получаването на заповед за премахване от органите на държавите членки. В своя доклад за оценка, приет през февруари 2024 г., Комисията съобщи, че регламентът е ефективен в предотвратяването на разпространението на терористично съдържание онлайн. Досега 23 държави членки са определили компетентните органи, които трябва да издават заповедите за премахване, и в периода от юни 2022 г. до април 2024 г. са издадени около 500 заповеди за премахване. Успоредно с това в редица държави членки за недостатъците по

[35] Работен документ на службите на Комисията SWD (2023) 37 final.

[36] Препоръка (ЕС) 2023/681 на Комисията от 8 декември 2022 г.

[37] Временно политическо споразумение беше постигнато на 7 декември 2023 г.

[38] Регламент (ЕС) 2021/784 от 29 април 2021 г. относно справянето с разпространението на терористично съдържание онлайн.

отношение на транспонирането на регламента се търси решение чрез производства за установяване на нарушения.

Комисията също така публикува набор от насоки за учителите и преподавателите за справяне с дезинформацията и насърчаване на цифровата грамотност чрез образование и обучение.

Това, което се счита за незаконно офлайн, трябва да бъде обявено за незаконно и онлайн. Прилагането на **Акта за цифровите услуги**[39] от 17 февруари 2024 г. е решителна стъпка в тази посока, със задължения за всички онлайн платформи за противодействие на незаконното съдържание. Друг елемент от инструментариума на ЕС за борба с тероризма е **звеното на ЕС за сигнализиране за незаконно съдържание в интернет**, което сигнализира за терористично съдържание на над 300 платформи и повишава осведомеността относно действията срещу терористичната пропаганда. **Интернет форумът на ЕС** също подкрепя технологичния отрасъл при модерирането на екстремистко съдържание и в момента се занимава с риска от терористична експлоатация на генеративния изкуствен интелект, като допълва законодателните промени, по-специално Законодателния акт за изкуствения интелект[40]. След нападението през март 2019 г. в Крайстчърч Интернет форумът на ЕС одобри Протокола на ЕС за действие при кризи, за да осигури сътрудничество между правоприлагащите органи и отрасъла след криза.

III.3. Подкрепа на жертвите на тероризъм

През януари 2020 г. Комисията създаде Център на ЕС за експертен опит за **жертвите на тероризъм**, за да предложи експертен опит, насоки и подкрепа за националните органи и организациите за подкрепа на жертвите. Центърът на ЕС помага да се гарантира, че правилата на ЕС относно жертвите на тероризъм се прилагат правилно, като насърчава обмена на най-добри практики и споделянето на опит.

ЕС в действие

28 терористични атаки са извършени, неуспешни или осуетени през 2022 г. През 2022 г. в държавите членки са арестувани 380 лица за престъпления, свързани с тероризъм. 14 от тях се отнасят до финансирането на тероризма, като всички те са свързани с джихадисткия тероризъм**. Евроюст** подкрепи действия по 203 случая, включително работата на 8 съвместни екипа за разследване. От юни 2022 г. насам са изпълнени 350 заповеди за премахване съгласно Регламента относно предотвратяването на разпространението на терористично съдържание онлайн.

С подкрепата на Комисията държавите членки въведоха инструменти за оценка на риска, специални режими на задържане, програми за реабилитиране и реинтеграция, обучение на персонала на затворите и пробационния персонал, структури за обмен на информация и мултидисциплинарно сътрудничество за контрол на бивши правонарушители след освобождаване.

Регламент относно справянето с разпространението на терористично съдържание онлайн доказа своята ценност, например като осигури възможност за бързото премахване на терористично съдържание след нападението, извършено на 7 октомври 2023 г. от Хамас срещу Израел.

[39] Регламент (ЕС) 2022/2065 от 19 октомври 2022 г. относно единния пазар на цифрови услуги (Акт за цифровите услуги).

[40] Временно политическо споразумение беше постигнато на 8 декември 2023 г.

IV. БОРБА С ОРГАНИЗИРАНАТА ПРЕСТЪПНОСТ

Организираната престъпност представлява заплаха за европейските граждани, предприятията, държавните институции, както и за икономиката като цяло. Престъпните мрежи участват в различни престъпни дейности, включително трафик на наркотици, организирани престъпления срещу собствеността, престъпления против околната среда, измами, контрабанда на мигранти и трафик на хора. Киберпрестъпността и основаното на пола кибернасилие бяха допълнително стимулирани от засиленото използване на интернет и онлайн услуги. В допълнение смущенията, причинени от военната агресия на Русия срещу Украйна, създадоха нови ниши, които бързо бяха поети от организираните престъпни групи. Престъпниците лесно извършват операции онлайн и през границите, което създава необходимост от последователни транснационални действия и действия на европейско равнище. **Стратегията на ЕС за борба с организираната престъпност за периода 2021—2025 г.**[41], приета от Комисията през април 2021 г., подчертава значението на разбиването на структурите на организираната престъпност, насочено към лицата на върха на престъпните организации, по-специално онези групи, които представляват най-голям риск за сигурността на Европа.

IV.1. Киберпрестъпност

Въпреки че технологичното развитие води до важни и бързи подобрения в нашето общество, то също така осигурява възможност на киберпрестъпниците да се възползват от факта, че цифровият свят няма граници. Между май 2021 г. и юни 2022 г. е сигнализирано за 3 640 атаки със софтуер за изнудване срещу предприятия и институции в ЕС, а през 2023 г. общата стойност на плащанията във връзка със софтуера за изнудване за първи път са надхвърлили 1 млрд. евро[42]. Престъпленията, вариращи от широкомащабни кибератаки до дейности, използващи зловреден софтуер, шпионски софтуер, фишинг и спам, пречат на функционирането на цифровата и физическата инфраструктура и оказват сериозно въздействие върху живота на хората. За да се справи с тези престъпления, ЕС прие редица законодателни и незаконодателни мерки за засилване на трансграничното сътрудничество както на равнище ЕС, така и на международно равнище.

През 2021 г. ЕС се присъедини към **Международната инициатива за борба със софтуера за изнудване**, която обединява усилията на повече от 50 партньори от ЕС и трети държави, за да се потърси отговорност от основните участници, **използващи софтуер за изнудване,** за техните престъпления и да им бъде отказано сигурно убежище. Инициативата помага да се попречи на основните участници, използващи софтуер за изнудване, да печелят от незаконни приходи, да се възпрепятства тяхната дейност и да се изправят пред правосъдието.

Сексуалното насилие над деца е разпространено до силно притеснителна степен — само през 2023 г. в световен мащаб е сигнализирано за над сто милиона снимки и видеоматериали, показващи сексуално насилие над деца, а за много други дори не се съобщава. Фактът, че децата прекарват повече време онлайн, ги направи по-податливи на сприятеляване с цел сексуална злоупотреба, което доведе до увеличаване на самостоятелно произвежданите експлоатационни материали. **В съответствие със Стратегията на ЕС за по-ефективна борба срещу сексуалното насилие над деца**[43] и

[41] COM(2021) 170.
[42] ENISA, Обстановка по отношение на заплахите от атаки със софтуер за изнудване.
[43] COM(2020) 607, прието през юли 2020 г.

Всеобхватната стратегия на ЕС за правата на детето[44] Комисията прие предложение за определяне на правила за предотвратяване и борба със сексуалното насилие над деца[45] с нови задължения за доставчиците на онлайн услуги. Когато превенцията не успее да намали значителния риск, на доставчиците на услуги може да бъде наредено да откриват, докладват, премахват и блокират сексуалното насилие над деца онлайн. С предложението ще се създаде и **специален център на ЕС,** за да се улесни прилагането на регламента. Срокът на действие на временното законодателство, прието с цел да се позволи на доставчиците на онлайн услуги да продължат доброволно да разкриват и съобщават за онлайн сексуално насилие над деца, беше удължен до 3 април 2026 г., за да се осигури достатъчно време за постигане на споразумение относно дългосрочната уредба. Тази инициатива беше допълнена от предложение за актуализиране на **Директивата от 2011 г. относно борбата със сексуалното насилие и сексуалната експлоатация на деца и материалите, съдържащи сексуално насилие над деца.**[46]. Съгласно преразгледаните правила са разширени определенията на престъпленията, най-вече за да не изостават от нарастващата престъпна дейност онлайн, и са въведени по-строги наказания и по-конкретни изисквания за превенция и помощ на жертвите.

Смята се, че половината от всички млади жени преживяват **основано на пола кибернасилие**[47]**.** В приетата през май 2024 г. **Директива относно борбата с насилието над жени и домашното насилие** са криминализирани някои форми на насилие, които непропорционално засягат жените, по-специално споделянето на интимни изображения без съгласие (включително дълбоки фалшификати), киберпреследването, кибертормоза и речта на омразата срещу жени. С директивата също така ще се подобри достъпът на жертвите до правосъдие.

IV.2. Трафик на наркотици

Незаконната търговия с **наркотици** е една от най-значимите заплахи за сигурността пред ЕС днес. Пазарът на търговията с наркотици на дребно в ЕС възлиза на поне 30 млрд. евро годишно[48]. Изземването на кокаин в ЕС достигна рекордни нива[49]. Нарастват притесненията във връзка с производството и разпространението на синтетични наркотици в Европа и връзката между трафика на наркотици и насилието[50]. В **Програмата и Плана за действие на ЕС относно наркотиците за периода 2021—2025 г.**[51] са определени конкретни действия за ускоряване на дейността на равнището на ЕС, включително усилия за засилване на международното сътрудничество в областта на трафика на наркотици и превръщането на Европейския център за мониторинг на наркотиците и наркоманиите в **Агенция на ЕС по наркотиците**[52]. Агенцията ще започне дейността си през юли 2024 г.

---

[44] COM(2021) 142, прието през март 2021 г.

[45] COM/2022/209, прието през май 2022 г.

[46] COM/2024/60, прието през февруари 2024 г.

[47] Служба на ЕП за парламентарни изследвания (EPRS), „Борба с насилието, основано на пола: кибернасилие, оценка на европейската добавена стойност“, 2021 г.

[48] Европол, 2024 г.

[49] През 2021 г. са задържани 303 тона кокаин. Европейски доклад за наркотиците за 2023 г., ЕЦМНН.

[50] В началото на 2024 г. в Барбате (Испания) бяха убити двама полицаи от заподозрени трафиканти на наркотици, а в Брюксел (Белгия) имаше редица престрелки заради наркотрафика, с няколко ранени и убити.

[51] COM(2020) 606.

[52] Регламент (ЕС) 2023/1322 от 27 юни 2023 г. относно Агенцията на Европейския съюз по наркотиците (EUDA).

Програмата беше допълнена от **Пътната карта на ЕС**, приета от Комисията през октомври 2023 г.[53], в която са определени допълнителни мерки за борба с трафика на наркотици и организираната престъпност, включително създаването на нов **Европейски пристанищен алианс** за повишаване на устойчивостта на пристанищата срещу проникването на престъпна дейност чрез укрепване на работата на митническите органи, правоприлагащите органи, участниците както от публичния, така и от частния сектор в пристанищата в целия ЕС. Изпълнението на пътната карта също така доведе до тематична оценка по Шенген, с помощта на която бяха оценени възможностите на държавите членки по отношение на полицейското сътрудничество, защитата на външните граници и управлението на информационните системи за борба с трафика на наркотици, като бяха установени 40 най-добри практики.

IV.3. Незаконен трафик на стоки

Незаконният трафик на стоки е изключително доходоносен бизнес и разходите за обществото са свързани не само с липсващите приходи, но и с опасността за здравето и безопасността на гражданите, за което са необходими координирани действия от страна на правителствата, правоприлагащите органи и частните участници.

Трафикът на огнестрелни оръжия подхранва организираната престъпност в ЕС, както и в съседните му държави. Смята се, че в ЕС близо 35 милиона незаконни огнестрелни оръжия са притежание на цивилни лица, а около 630 000 огнестрелни оръжия са вписани в Шенгенската информационна система като откраднати или изгубени. С развитието на нови технологии, като например триизмерния печат, трафикът на огнестрелни оръжия намира нови начини за избягване на контрола. Заедно с **Плана за действие на ЕС относно трафика на огнестрелни оръжия за периода 2020—2025 г.**[54] всички държави членки вече са транспонирали **Директивата относно огнестрелните оръжия**[55] в националното си законодателство, което води до значителни подобрения в сигурността, като прави по-трудно законното придобиване на най-опасните оръжия. Съветът и Европейският парламент също така постигнаха споразумение относно преразгледаните **правила за разрешителни за износ, внос и транзит за огнестрелни оръжия,**[56] за да се подобри проследимостта на огнестрелните оръжия за граждански цели, с по-широк акцент върху цифровизацията

Незаконният трафик на културни ценности също е доходоносен бизнес за организираните престъпни групи, а в някои случаи и за участниците в конфликта и терористите[57]. През декември 2022 г. Комисията прие план за действие на ЕС за засилване на борбата срещу **трафика на културни ценности**[58], включително диалога със заинтересованите страни за насърчаване на справедлив пазар на изкуството с добра репутация, който защитава културното наследство.

IV.4. Контрабанда на мигранти и трафик на хора

Счита се, че над 90 % от мигрантите, които пристигат незаконно в ЕС, използват услугите на контрабандисти. Изчислено е, че печалбите от контрабандата на мигранти

[53] COM/2023/641 final.
[54] COM(2020) 608 final.
[55] Директива (ЕС) 2021/555 относно контрола на придобиването и притежаването на оръжие.
[56] COM(2022) 480.
[57] Вж. например резолюции 2199 (2015 г.), 2253 (2015 г.), 2322 (2016 г.), 2347 (2017 г.), 2462 (2019 г.) и 2617 (2021 г.) на Съвета за сигурност на ООН; Декларация от Рим на министрите на културата от Г-20 от 30 юли 2021 г.
[58] COM(2022) 800.

възлизат на между 4,7 и 6 млрд. евро годишно в световен мащаб, а смъртните случаи вследствие на тази престъпна търговия само в Средиземно море се оценяват на над 28 000 от 2014 г. насам.

За да увеличи усилията срещу **контрабандата на мигранти**, Комисията предложи действащата нормативна уредба да бъде осъвременена[59] с помощта на предложена директива, която има за цел да гарантира по-ефективно разследване и наказателно преследване на контрабандистите, както и предложен регламент за подобряване на координацията в ЕС чрез укрепване на **Европейския център за борба с контрабандата на мигранти** в Европол и подобряване на обмена на информация между отговорните органи. Комисията призовава Европейския парламент и Съвета да постигнат споразумение по тези досиета в най-кратък срок. Едновременно с това на 28 ноември 2023 г. Комисията стартира **Световен алианс за борба с контрабандата на мигранти**, с **Призив за действие**, който сега се осъществява със съответните заинтересовани страни. През април 2024 г. Комисията беше домакин на събитие за създаване на общност от заинтересовани страни и компетентни органи за справяне с използването на цифрови услуги за контрабанда на мигранти. Комисията също така оказва подкрепа на правоприлагащите и съдебните органи на ключови трети държави, за да повиши капацитета им за разследване и наказателно преследване на организирани групи за контрабанда и трафик на хора.

Много от престъпните мрежи, занимаващи се с контрабанда на мигранти, се занимават също и с **трафик на хора**. Европол изчислява печалбите от трафик на хора на над 29,4 млрд. евро годишно в световен мащаб[60]. По-голямата част от жертвите са жени и момичета, но трафикът на мъже също нараства, особено с цел експлоатация на труда. През април 2021 г. Стратегията на ЕС за борба с трафика на хора за периода 2021—2025 г.[61] предостави всеобхватна рамка за действие. В обхвата на наскоро преразгледаната Директива за борба с трафика на хора попадат нови форми на експлоатация (експлоатация на сурогатно майчинство, на принудителен брак и на незаконно осиновяване), в нея са засилени инструментите за правоприлагане и тези, с които разполагат съдебните органи, както и е поставено изискване държавите членки да налагат санкции на хората, които съзнателно използват услуги, разчитащи на жертвите на трафик. Евроюст, в сътрудничество с координатора на ЕС за борбата с трафика на хора, създаде целева група от специализирани прокурори срещу трафика на хора.

IV.5. Престъпления против околната среда

Престъпленията против околната среда често причиняват необратими и дългосрочни вреди върху човешкото здраве, както и върху екосистемите и околната среда. Те са изключително доходоносни и често включват организирана престъпност, и не е лесно да бъдат разкривани и наказателно преследвани. Престъпленията против околната среда са третата по големина престъпна дейност в света по отношение на приходите, като незаконното поведение и печалбите нарастват значително всяка година[62], както и понастоящем.

Въпреки че според оценките печалбите от престъпна дейност против околната среда са в размер на 200 млрд. евро годишно и имат сериозно отрицателно въздействие върху икономиката, не може да бъде поставена цена на вредите за нашата околна среда,

[59] COM/2023/754 и COM/2023/755.
[60] Проучване на икономическата, социалната и човешката цена на трафика на хора в ЕС (2020 г.).
[61] COM(2021) 171.
[62] Заради организираните престъпни групи екологичната сигурност е на повратна точка (interpol.int)

биологичното разнообразие, човешкото здраве и сигурността. Действията на равнището на ЕС за справяне с екологичните престъпления бяха засилени чрез **новата Директива относно престъпленията против околната среда**[63], в която е разширен обхватът на престъпленията, които трябва да бъдат разследвани и наказателно преследвани, и са предвидени конкретни видове и нива на санкции за физически и юридически лица, извършили престъпления против околната среда. Бяха предприети допълнителни действия чрез приемане на регламента относно превозите на отпадъци и чрез по-ефективни мерки, насочени към незаконния дърводобив чрез въвеждане на нови правила за несвързаните с обезлесяване продукти. Освен това в преразгледания **План за действие на ЕС срещу трафика на екземпляри от дивата флора и фауна** са актуализирани приоритетите на ЕС за по-ефективно предотвратяване и справяне с първопричините за този феномен.

IV.6. Икономически и финансови престъпления

Изпирането на пари и финансирането на тероризма представляват сериозна заплаха за почтеността в икономиката и финансовата система на ЕС и за сигурността на неговите граждани. Според оценката на Европол съмнителната финансова дейност съставлява около 1 % от годишния брутен вътрешен продукт на ЕС[64].

ЕС постигна съгласие по нови правила за **предотвратяване на изпирането на пари и финансирането на тероризма**, за да подобри предотвратяването и разкриването на опити от престъпници да изпират незаконни приходи или да финансират терористични дейности чрез финансовата система на Съюза[65], като определи пряко приложими изисквания в целия Съюз за операторите от частния сектор, включително извършването на комплексна проверка на клиента и докладването при подозрения. Задачите и правомощията на националните надзорни органи и звената за финансово разузнаване ще бъдат подсилени и хармонизирани, за да се гарантира, че отговорните органи изпълняват задачите си и си сътрудничат по-ефективно. Освен това ясните правила укрепват превантивната функция на действителната собственост и банковите регистри. Ще бъде създаден **нов орган за борба с изпирането на пари**, който ще има правомощия на пряк надзор върху най-рисковите трансгранични субекти във финансовия сектор и ще предоставя оперативна подкрепа за съвместния анализ на трансграничните случаи на звената за финансово разузнаване.

В допълнение към новите правила за борба с изпирането на пари, наскоро приетата **Директива относно отнемането и конфискацията на активи** ще бъде важен инструмент в борбата срещу тежката и организираната престъпност, като установи по-строги мерки за конфискуване на незаконни печалби от широк кръг от престъпления. Службата за отнемане на активи ще има мандат за установяване, проследяване и обезпечаване на активи, придобити от престъпна дейност. В комбинация с наскоро приетата **Директива относно определянето на престъпленията, свързани с нарушаване на ограничителните мерки на Съюза**, с която се хармонизират определянето и санкциите за такива престъпления в целия Съюз, тези правила ще позволят също проследяване, обезпечаване, управление и конфискация на облаги, придобити от престъпни лица чрез нарушаване на санкциите на Съюза.

IV.7. Борба с корупцията

[63] Директива 99/2008/ЕО относно защитата на околната среда чрез наказателно право.
[64] Група за финансово разузнаване на Европол, *От подозрение към действие,* (2017 г.).
[65] COM/2021/420 , COM/2021/421, COM/2021/422 и COM/2021/423.

Корупцията нанася сериозни вреди на обществото, като подкопава публичните институции, изпълнението от тяхна страна на обществени политики и предоставянето на обществени услуги, както и доверието на гражданите в демократичните институции. Корупцията в частния сектор подкопава единния пазар и осигурява нови възможности на организираната престъпност.

С цел преодоляване на рисковете и предизвикателствата, свързани с корупцията, Комисията предложи[66] **Директива относно борбата с корупцията**, за да засили правилата за криминализиране на престъпленията, свързани с корупция, и за хармонизиране на наказанията в целия ЕС. Европейският парламент прие своята позиция през февруари 2024 г. За да гарантира, че в ЕС няма тайни места за корупцията, Комисията призовава Съвета да продължи с обсъжданията си и да подкрепи целите на предложението на Комисията.

В **Директивата за защита на финансовите интереси**[67] са определени конкретни правила за защита на бюджета на ЕС от престъпна дейност, включително корупция. Заедно с предложената директива за борба с корупцията, строгото прилагане на тази мярка е наложително, за да се защитят финансите на ЕС от измами и корупционна дейност, а Комисията участва в този процес чрез производства за установяване на нарушения, когато това е необходимо. Европейската служба за борба с измамите (OLAF) и **Европейската прокуратура** играят ключова роля в това, като разследват нередности и преследват престъпления, засягащи финансовите интереси на Съюза[68]. Новата **мрежа на ЕС за борба с корупцията**[69], която служи като форум за всички заинтересовани страни в ЕС за обмен на добри практики, възможности, идеи и планове за по-нататъшна работа, проведе първото си заседание през септември 2023 г.

IV.8. Защита на жертвите на престъпления

Жертвите на всички видове престъпления заслужават подкрепа и внимание. Комисията вече е постигнала повечето от действията по първата **Стратегия на ЕС за правата на жертвите (2020—2025 г.)**[70]. На 12 юли 2023 г. Комисията предложи директива за изменение на **Директивата за правата на жертвите**[71] от 2012 г., за да утвърди още повече правата на всички жертви на престъпления в ЕС, по-специално правата на най-уязвимите жертви.

ЕС в действие

На 5 април 2024 г., като ключов резултат от пътната карта на ЕС за борба с трафика на наркотици и организираната престъпност, Европол публикува доклад с първо картографиране на престъпните мрежи, които представляват най-голямата заплаха. Констатациите показват, че най-голямата заплаха идва от 821 високорискови престъпни мрежи, съставени от общо 25 000 членове. 34 % от високорисковите престъпни мрежи

66 COM/2023/234.

67 Директива (ЕС) 2017/1371 от 5 юли 2017 г. относно борбата с измамите, засягащи финансовите интереси на Съюза, по наказателноправен ред. От декември 2021 г. насам Комисията е започнала 19 производства за установяване на нарушения за неспазване на Директивата за защита на финансовите интереси.

68 Полша официално се присъедини към Европейската прокуратура през февруари 2024 г.

69 JOIN(2023) 12.

70 COM(2020) 258.

71 COM/2023/424.

извършват дейност в ЕС повече от 10 години, 76 % от тях присъстват или извършват дейност в до 7 държави, а техните членове представляват 112 националности.

При акция срещу трансграничната престъпност („Операция „Mobile 6“) 400 служители на правоприлагащите органи от 25 държави откриха 505 откраднати автомобила, 2000 части за автомобили, 16 лодки, 32 извънбордови двигателя и 248 фалшиви документа. Спрени са 209 заподозрени контрабандисти на хора. През 2022 г. и 2023 г. Европейската прокуратура проведе мащабно разследване в над 30 държави на организирани престъпни групи, заподозрени, че са отговорни за трансгранични измами с ДДС, оценявани на 2,2 млрд. евро (операция „Адмирал“).

V ГАРАНТИРАНЕ НА СИГУРНОСТТА НА НАШИТЕ ГРАНИЦИ И ПОДКРЕПА ЗА ПРАВОПРИЛАГАНЕТО И СЪДЕБНОТО СЪТРУДНИЧЕСТВО

В пространството без контрол по вътрешните граници полицейските служители в една държава членка следва да имат достъп до информацията, достъпна за техните колеги в друга държава членка. Ефективното сътрудничество трябва да бъде правило. Ето защо е от съществено значение да се засилят инструментите, с които разполагат правоприлагащите и съдебните органи в целия ЕС за обмен на информация и трансгранично сътрудничество.

Както е подчертано в Доклада за състоянието на Шенген за 2024 г.[72], непрекъснатото укрепване на **Шенгенското пространство**, разрешаването на проблемите, установени в оценките, и насочването на колективните усилия към по-съгласувано управление на Шенгенското пространство допринасят не само за свободното движение, но и за сигурността на гражданите в цяла Европа. Доброто функциониране на Шенгенското пространство се основава на три стълба: ефективно управление на външните граници на ЕС, укрепване на вътрешните мерки за компенсиране на липсата на контрол по вътрешните граници, по-специално по отношение на полицейското сътрудничество, сигурността и управлението на миграцията, и осигуряване на солидна подготовка и управление[73].

Управлението на външните граници ще бъде засилено с ново законодателство относно проверката[74] на незаконно пристигащите. Новото определение на инструментализирането на мигрантите[75] ще помогне за справянето с експлоатацията на мигранти при хибридни атаки по външната граница на ЕС, както се вижда например на границата с Беларус през 2021 г. Ефективното управление на миграцията с безпроблемен процес на границата[76] ще укрепи Шенгенското пространство, като гарантира по-тясно сътрудничество и споделяне на отговорностите между държавите членки. Кодексът на шенгенските граници, след като бъде приет, ще доведе до по-голяма координация на ЕС и ще подготви по-добре държавите членки да се справят с възникващите предизвикателства по общата външна граница на ЕС и в рамките на Шенгенското пространство, докато агенциите на ЕС ще продължат да помагат на

[72] COM(2024)173.

[73] През март 2024 г. България и Румъния станаха членки на Шенгенското пространство, които прилагат изцяло достиженията на правото от Шенген, а контролът по вътрешните граници беше премахнат по въздушните и морските граници.

[74] COM(2020)612.

[75] COM(2020) 613.

[76] Регламент за установяване на обща процедура за международна закрила в Съюза, COM(2016) 467 final и COM(2020) 614 final.

държавите членки да поддържат високо равнище на вътрешната сигурност в Шенгенското пространство.

С **пакета за полицейско сътрудничество**[77] се предлага значително надграждане на наличните инструменти за подобряване на трансграничните операции, предоставят се ясни канали и срокове за обмен на информация между правоприлагащите органи в държавите членки, а на **Европол** се предоставя по-значима роля. Освен това преразгледаните правила за **автоматизиран обмен** ще помогнат за преодоляване на пропуските в информацията, ще подобрят превенцията, разкриването и разследването на престъпления в ЕС. Значителен напредък беше постигнат и в разработването на ефективни инструменти за осигуряване на безпроблемното пътуване по въздух до, от и в рамките на ЕС, като същевременно беше повишен капацитетът на органите за откриване на заплахи за сигурността, чрез преразглеждане на правната рамка за използването на **Системата за предварителна информация за пътниците**.

По отношение на тероризма, приетото през 2023 г. изменение на **Регламента за Евроюст** относно цифровия обмен на информация по дела за тероризъм[78] ще направи обмена на информация между отговорните национални органи и Евроюст по-ефективен чрез съдебния регистър в областта на борбата с тероризма.

За наказателното преследване на киберпрестъпници са необходими определени видове доказателства и е постигнат съществен напредък за подобряване на трансграничното сътрудничество при **обмена на електронни доказателства**. Очаква се, че с помощта на Втория допълнителен протокол към Конвенцията на Съвета на Европа за престъпленията в кибернетичното пространство[79] ще се засили борбата с киберпрестъпността чрез укрепване на възможностите на съдебните органи за събиране на електронни доказателства за престъпленията (например чрез създаване на съвместни екипи за разследване). Благодарение на вътрешните **правила на ЕС за електронните доказателства**[80], приети през 2023 г., ще бъде въведена нова система за получаване на електронни доказателства в наказателни производства, като на правоприлагащите и съдебните органи ще бъде предоставена възможност пряко да се обръщат към частни доставчици на услуги, разположени в друга държава членка.

Изкуственият интелект се превърна в многостранен и важен компонент в технологиите, на разположение на правоприлагащите органи и други участници във вътрешната сигурност; същевременно при неговото използване за тази цел следва да се зачитат основните права на човека. Генеративният изкуствен интелект обаче може да бъде използван от киберпрестъпниците за организиране на сложни кибератаки и други злоумишлени действия. **Регламентът относно изкуствения интелект (Законодателен акт за изкуствения интелект)** е първата стъпка към регулиране на използването на изкуствен интелект в рамките на ЕС, като в него са предвидени предпазни мерки за отговорното използване на системите с изкуствен интелект в тази област, като

[77] COM/2021/780, COM/2021/782 и COM/2021/784.

[78] Регламент (ЕС) 2023/2131 по отношение на цифровия обмен на информация по дела за тероризъм.

[79] Приет от Комитета на министрите на 17 ноември 2021 г.

[80] Регламент (ЕС) 2023/1543 от 12 юли 2023 г. относно европейските заповеди за предоставяне и европейските заповеди за запазване на електронни доказателства в рамките на наказателните производства и за изпълнението на наказания лишаване от свобода вследствие на наказателни производства и Директива (ЕС) 2023/1544 от 12 юли 2023 г. за установяване на хармонизирани правила относно определянето на определени форми на установяване и определянето на представители за целите на събирането на електронни доказателства по наказателни производства.

същевременно се зачитат основните права и безопасността на гражданите. Европейската служба по изкуствен интелект ще подпомогне прилагането на акта, като гарантира спазването на мерките и процедурните правила, изложени в него. Комисията ще участва в разработването на подходящи насоки в подкрепа на правоприлагащите органи и други участници в областта на сигурността за използване на изкуствения интелект по уместен и ефективен начин в тяхната работа.

Докато работата по **система на ЕС за комуникации от критично значение** продължава, с нов регламент за създаване на платформа за сътрудничество за съвместните екипи за разследване[81] на участниците се предоставят сигурни средства за обмен на доказателства и информация, ефективна комуникация и лесно сътрудничество с трети държави.

С увеличаването на трансграничната престъпност ЕС все по-често се сблъсква със ситуации, при които няколко държави членки са компетентни да разглеждат едно и също дело. Новите правила **за трансфера на наказателни производства** ще помогнат за предотвратяване както на неефективното дублиране на производства, така и на случаите на безнаказаност, когато е отказано предаване съгласно европейска заповед за арест, като същевременно се гарантира, че правата на заподозрените и жертвите са надлежно зачетени. Ефикасното трансгранично съдебно сътрудничество изисква сигурна, надеждна и ефикасна във времето комуникация между съдилищата. Това вече ще бъде възможно благодарение на **Пакета за цифрово правосъдие**. Органите ще могат да комуникират помежду си и да обменят данни по граждански, търговски и наказателни дела по сигурни и надеждни цифрови канали. Това ще улесни борбата с престъпността и бързото прилагане от държавите членки ще бъде от ключово значение.

ЕС в действие

През 2022 г. EMPACT е довела до:

- 9 922 ареста
- идентифицирането на 4 019 жертви на трафика на хора
- ареста на 3 646 контрабандисти на мигранти
- изземването на повече от 180 млн. евро активи и парични средства
- изземването на над 62 тона наркотици

VI ВРЪЗКА МЕЖДУ ВЪТРЕШНАТА И ВЪНШНАТА СИГУРНОСТ: СИГУРНОСТ В ЕС, В СЪСЕДНИТЕ МУ ДЪРЖАВИ И В ПАРТНЬОРСКИТЕ ДЪРЖАВИ

Нарастващата взаимосвързаност между вътрешната и външната сигурност става все по-очевидна през последните няколко години предвид настоящия геополитически контекст. Сигурността в ЕС е по-голяма, когато и сигурността на неговите партньори е по-голяма. Само през 2023 г. около 700 млн. евро бяха изразходени за подпомагане на капацитета на трети държави и за укрепване на нашето сътрудничество с тях за борба с тероризма и предотвратяване и противодействие на насилническия екстремизъм, като 72 % от тях

[81] Регламент (ЕС) 2023/969 от 10 май 2023 г. за създаване на платформа за сътрудничество за подпомагане на функционирането на съвместните екипи за разследване.

бяха насочени към Африка предвид нарастващата нестабилност и присъствието на терористични групи в Сахел. Това е пет пъти повече в сравнение с разходите преди 10 години. Междувременно сътрудничеството в областта на правоприлагането с трети държави е включено във всички оперативни планове за действие по EMPACT.

Комисията предприе спешни действия, за да предотврати заплахите за вътрешната сигурност, произтичащи от агресивната война на Русия срещу **Украйна,** като гарантира максимална бдителност по отношение на използването на конфликта и потоците от хора, търсещи безопасност в Европа, от организираната престъпност и групите за трафик. Службите на Комисията и ЕСВД, заедно с координатора на ЕС за борбата с тероризма, се споразумяха с Украйна да установят структуриран диалог за вътрешна сигурност, включително в области, като например трафика на огнестрелни оръжия и управлението на границите. Кибердиалогът между ЕС и Украйна, заедно с координираната политическа, техническа, финансова и материална подкрепа от ЕС, помогна на Украйна да засили своята киберустойчивост. Обявената служба на ЕС за иновации в областта на отбраната в Киев ще действа като мост между стартиращи предприятия и новатори в ЕС и украинската промишленост и въоръжените сили, включително в областта на киберотбраната. Това ще спомогне за предаване на технологични пробиви, които може да окажат влияние на бойното поле.

Република **Молдова** също е изложена в голяма степен на последиците, свързани с престъпността и сигурността, породени от нахлуването на Русия в Украйна и редица хибридни и киберзаплахи. През юли 2022 г. службите на Комисията, в сътрудничество с ЕСВД, създадоха център за подкрепа на ЕС за вътрешна сигурност и управление на границите с Република Молдова. ЕС оказва подкрепа на Молдова за подобряване на нейната устойчивост и способност да се противопоставя на хибридни и киберзаплахи, включително чрез прилагане на препоръките от повторното проучване на хибридния риск и чрез мисията за партньорство на ЕС в Република Молдова.

Предвид тяхната близост, сигурността на партньорите от Западните Балкани е тясно свързана с вътрешната сигурност на ЕС и сътрудничеството в областта на правоприлагането между ЕС и **държавите от Западните Балкани** продължи да се засилва през настоящия мандат. По съвместния план за действие за борба с тероризма, подписан през 2018 г. с всички партньори от Западните Балкани, беше постигнат добър напредък, и след завършване на повечето действия в Северна Македония, Албания и Черна гора, бяха подписани актуализирани споразумения. ЕС също така продължава да повишава колективната киберустойчивост на партньорите от Западните Балкани чрез оперативна и техническа подкрепа, обучение и участие на региона в механизмите на ЕС за киберсигурност.

Настоящата ситуация в **Близкия изток** също би могла да окаже въздействие върху вътрешната сигурност на ЕС, включително значително увеличаване на инцидентите в някои държави членки. Мрежата от финансови следователи за борба с тероризма даде възможност на държавите членки да споделят информация за случаи, свързани с дейностите по набиране на средства на Хамас в ЕС, като предостави на следователите по-добро разбиране за това как да се справят с такива заплахи.

В светлината на събитията в **Афганистан**, в координация с Комисията, върховния представител, председателството и ключови агенции на ЕС, координаторът на ЕС за борба с тероризма изготви План за действие за борба с тероризма за Афганистан, одобрен от Съвета през октомври 2021 г. ЕС остава ангажиран в Афганистан и засилва ролята си

в по-широк регионален мащаб чрез засилено сътрудничество по въпроси, свързани със сигурността, **с държавите от Централна Азия** и диалог във връзка с борбата с тероризма с **Пакистан**.

ЕС засили сътрудничеството с държавите от **Латинска Америка и Карибския басейн,** по-специално по отношение на борбата с организираната престъпност, трафика на наркотици и финансирането на тероризма.

Многостранното сътрудничество е в основата на подхода на ЕС. ЕС работи в тясно сътрудничество с ООН, със Службата на ООН за борба с тероризма и най-вече с Изпълнителната дирекция на ООН за борба с тероризма. ЕС също така работи с над 40-те организации на ООН, които съставляват Глобалния договор на ООН за координация на борбата срещу тероризма. От септември 2022 г. ЕС е съпредседател на Глобалния форум за борба с тероризма с Египет, като многостранен форум за подкрепа на гражданските аспекти на противодействието на тероризма и насилническия екстремизъм, със силен акцент върху Африка. ЕС е също невоенен партньор на Световната коалиция за борба срещу Даеш и работи активно съвместно с НАТО, Интерпол и ОССЕ. В областта на борбата срещу изпирането на пари, борбата с тероризма и финансирането на разпространението на оръжия Комисията активно допринася за работата на Специалната група за финансови действия. Участието в Световната коалиция за борба срещу Даеш е важен компонент от реакцията на външната политика на ЕС срещу тероризма/насилническия екстремизъм и свързаните с тях заплахи.

ЕС значително задълбочи и разшири **сътрудничеството си с НАТО**, по-специално в области като устойчивост, критична инфраструктура, здравна сигурност, противодействие на кибернетични и хибридни заплахи, включително дезинформация, военна мобилност, космическо пространство , нововъзникващи и революционни технологии, климат и отбрана. През януари 2022 г. започна структуриран диалог относно устойчивостта, засилен от работната група ЕС-НАТО по въпросите на устойчивостта на критичната инфраструктура. През юни 2023 г. работната група публикува доклад, в който бяха очертани настоящите предизвикателства в областта на сигурността пред критичната инфраструктура в четири ключови сектора (енергетика, транспорт, цифрова инфраструктура и космическо пространство). Изпълнението на препоръките за по-нататъшно сътрудничество между ЕС и НАТО, съдържащи се в доклада, продължава да е задоволително, с акцент върху учения, гражданско-военна координация и сътрудничество с частния сектор.

Преразгледаните насоки за прилагане на **инструментариума на ЕС за кибердипломация** позволяват разработването на устойчиви, специализирани, съгласувани и координирани стратегии за борба с настойчиви участници в киберзаплахи, като допринасят за по-добро справяне с предизвикателствата на продължаващите заплахи от по-ниско ниво в сивата зона и дейности, произтичащи от настойчиви участници в киберзаплахи. ЕС продължава работата по повишаване на киберустойчивостта, подкрепата на партньорите и насърчаването на рамката на ООН за отговорно поведение в киберпространството и сигурна цифрова инфраструктура чрез Global Gateway. ЕС засили **сътрудничество в областта на киберсигурността с НАТО** чрез специален структуриран диалог **и с международните партньори**. Диалогът със Съединените щати, който води до Съвместния план за действие на ЕС и САЩ за кибербезопасност, съвместната техническа работа по картографиране и сравняване на законодателството и усилията за стандартизация, е добър пример за конкретното сътрудничество на ЕС с партньори в подкрепа на глобалната киберсигурност. През

2023 г. ЕС също така възобнови кибердиалозите с Япония и Индия и стартира първия диалог с Обединеното кралство, като даде възможност за обмен на информация относно картината на заплахите, изграждане на киберкапацитет и сътрудничество в многостранни и регионални форуми.

През последните години ЕС започна **диалози по въпросите на борбата с тероризма** с ключови държави партньори и многостранни организации, включително ООН, Австралия, Египет, Индия, Пакистан, Саудитска Арабия, Турция и САЩ. ЕС разполага и с мрежа от 20 експерта в областта на борбата с тероризма/сигурността, разположени в делегациите на ЕС по целия свят, които подкрепят целите на външната политика и политиката на сигурност на ЕС, свързани с противодействието на тероризма и насилническия екстремизъм. Комисията продължава да работи за премахване на терористично съдържание онлайн, като същевременно зачита основните свободи в духа на Призива за действие, свързан с Крайстчърч[82]. Като част от прилагането на Споразумението за търговия и сътрудничество, през декември 2023 г. и февруари 2024 г. се проведе първият кръг от диалози между ЕС и Обединеното кралство относно кибертероризма и борбата с тероризма.

Във връзка с **трафика на наркотици**, проведената през февруари 2024 г. среща на високо равнище на механизма за координация и сътрудничество относно наркотиците между ЕС и Общността на латиноамериканските и карибските държави (EU-CELAC) доведе до приемането на декларация[83], с която се определят приоритетите за сътрудничество през следващите пет години. ЕС участва в работата на Глобалната коалиция за справяне със заплахите от синтетични наркотици, създадена от Съединените щати. Европейският център за мониторинг на наркотици и наркомании засилва сътрудничеството с Колумбия, Еквадор и Чили чрез сключването на работни споразумения.

Ефективните **мерки за отнемане и конфискация на активи** на глобално равнище са от съществено значение в борбата срещу тежката и организираната престъпност. Комисията е поела ангажимент да осигури общ подход на ЕС в предстоящите преговори по допълнителен протокол към Варшавската конвенция на Съвета на Европа относно изпиране, издирване, изземване и конфискация на облагите от престъпление и относно финансирането на тероризма, която се нуждае от актуализация, като се има предвид бързо развиващата се престъпна среда и промените на международно равнище. През април 2024 г. Комисията прие препоръка за решение, с което иска разрешение от Съвета Комисията да преговаря по протокола от името на ЕС.

В контекста на **хибридните заплахи**, които стават все по-сложни и усъвършенствани, прилагането на Стратегическия компас на ЕС за сигурност и отбрана е от решаващо значение. Службите на Комисията и Европейската служба за външна дейност допринесоха за създаването на инструментариума на ЕС за борба с хибридните заплахи, който предоставя рамка за координиран отговор на хибридни кампании, обединявайки всички подходящи вътрешни и външни инструменти и мерки. Актуализираният през април 2023 г. Оперативен протокол на ЕС за борба с хибридните заплахи помага да се осигури ефективното прилагане на процеси и инструменти в отговор на хибридни

[82] Свързан с Крайстчърч призив за действие, отправен през 2019 г. от Франция и Нова Зеландия.

[83] Механизъм за координация и сътрудничество относно наркотиците между ЕС и Общността на латиноамериканските и карибските държави (EU-CELAC) — Декларация от Ла Пас, 22 февруари 2024 г.

заплахи през целия цикъл на управление на кризи. Създават се екипи на ЕС за бързо реагиране при хибридни заплахи, които предоставят краткосрочна специализирана помощ за противодействие на хибридните заплахи в държавите — членки на ЕС, и партньорските държави.

Стратегическото и координирано използване на **чуждестранно манипулиране на информация и вмешателство** (FIMI) представлява ясна заплаха за нашата собствена сигурност и тази на нашите партньори, тъй като половината земно кълбо ще гласува на избори през 2024 г. През последните години, въз основа на Плана за действие за европейската демокрация и прилагайки Стратегическия компас на ЕС за сигурност и отбрана, ЕС засили действията си в противодействие на FIMI и създаде работна група на Комисията за стратегическа комуникация, за да помогне за напредък в действията.

Опитите за чужда намеса бяха подчертани от обвинения в корупция чрез плащания, направени от трети държави към политици в ЕС. Рискът от чужда намеса е особено силно изразен в навечерието на изборите за Европейски парламент. За да рационализира споделянето на информация преди изборите, през април 2024 г. Съветът приведе в действие договореностите за интегрирана реакция при политическа криза (ICPR).

В **Стратегическия компас на ЕС и анализа на заплахите** се признава, че изменението на климата и влошаването на състоянието на околната среда имат все по-голямо влияние върху мира, сигурността и отбраната. Тези фактори, в съчетание с недостига на вода, представляват заплаха за нестабилната обстановка в съседните на ЕС държави и може да доведат до кризи с насилствено разселване на населението, вътрешни сътресения или конфликти между държавите. През юни 2023 г. Комисията и върховният представител по въпросите на външните работи и политиката на сигурност приеха съвместно съобщение относно връзката между климата и сигурността[84].

През декември 2023 г. в **пакета от мерки за защита на демокрацията** беше определено как да се използват стандартите за прозрачност за представителство на интереси, за да се защитят демокрациите в ЕС от риска от скрита намеса[85], и беше обяснена работата на ЕС във връзка с борбата с дезинформацията, като например интензивен обмен между институциите в реално време, използване на мрежи за проверка на фактите и интензивна работа с ключовите платформи чрез Кодекса за поведение във връзка с дезинформацията, а сега и чрез Акта за цифровите услуги.

ЕС в действие

В глобализирания свят, където тежката престъпност и тероризмът все по-често имат транснационално измерение, сътрудничеството и обменът на информация между правоприлагащите и съдебните органи на трети държави са от съществено значение.

Европол и Евроюст са сключили споразумения за сътрудничество с трети държави, за да подобрят обмена на информация в борбата срещу тероризма и организираната престъпност. През юли 2023 г. влезе в сила Споразумение между ЕС и Нова Зеландия за обмен на лични данни с Европол и все още са в процес на преговори споразумения с Европол с Боливия, Бразилия, Мексико, Перу и Еквадор.

[84] JOIN(2023) 19.
[85] COM(2023) 637.

Евроюст улеснява съдебното сътрудничество за борба с тежката престъпност и с трети държави посредством 13 споразумения за сътрудничество, с международни съдебни мрежи, чрез работни договорености и в рамките на мрежа от над 70 юрисдикции по целия свят и чрез звена за контакт. В Евроюст са командировани 12 прокурори за връзка от трети държави. В процес на преговори са споразумения за международно съдебно сътрудничество с Евроюст с Бразилия, Аржентина и Колумбия.

ENISA също засили своето сътрудничество и международен обсег и наскоро подписа работни споразумения с агенциите за киберсигурност на Украйна и САЩ.

VII ВЪВЕЖДАНЕ В ДЕЙСТВИЕ НА СЪЮЗА НА СИГУРНОСТ

Правилното въвеждане в действие на Съюза на сигурност е споделена отговорност, при която всеки участник трябва да изиграе своята роля. Комисията подкрепя стратегиите, политиката, законодателството, организацията и изграждането на капацитет на държавите членки с оглед въвеждането в действие на Съюза на сигурност, включително чрез Инструмента за техническа подкрепа.

VII.1. Нарушения

Въпреки че в законодателството на ЕС са утвърдени солидни нови правила за по-добра защита на гражданите на ЕС, отговорност на държавите членки е своевременно да транспонират, изпълняват и прилагат такива правила. Нивото на прилагане от държавите членки на законодателството на ЕС в областта на Съюза на сигурност като цяло е задоволително, но в тази деликатна област няма място за слаби звена.

При необходимост Комисията изпълнява задължението си да открива производства за установяване на нарушение и предявява искове срещу държавите членки пред Съда на ЕС, за да бъдат разгледани случаите на нарушение на правото на Съюза. Благодарение на тясното сътрудничество между Комисията и държавите членки, много от производствата за установяване на нарушение, открити във връзка със законодателството съгласно Стратегията за Съюза на сигурност, бяха разгледани.

VII.2. Ролята на агенциите и органите на ЕС

Агенциите и органите на ЕС в областта на правосъдието, вътрешните работи и киберсигурността играят ключова роля в прилагането на достиженията на правото на ЕС в областта на сигурността, която продължава да нараства с разширяването на техните отговорности. Това сътрудничество доведе до конкретни резултати, както се вижда например от **EMPACT,** която улеснява структурираното мултидисциплинарно сътрудничество на държавите членки, подкрепяно от всички институции, органи и агенции на ЕС. При операциите, извършвани от EMPACT, включително чрез специализирани оперативни работни групи, се координират усилията на държавите членки и оперативните партньори в борбата с престъпните мрежи и тежките престъпления.

ENISA има ключова роля за укрепването на капацитета на ЕС за предотвратяване, откриване, възпиране и реагиране на кибератаки, като същевременно насърчава киберустойчивостта, защитава нашите комуникации и данни и поддържа сигурността на обществото и икономиката онлайн. Чрез експертни съвети и подкрепа по въпроси, свързани с киберсигурността, включително чрез доклади за ситуационна осведоменост и оценки на риска, тя улеснява сътрудничеството и споделянето на информация между

държавите членки, институциите на ЕС и други заинтересовани страни. Нейните задачи са засилени в съответствие с новите правила за киберсигурност. Неотдавнашната актуализация на Сборника с практически насоки относно киберсигурността и устойчивостта на изборите или докладът за най-добрите практики за управление на киберкризи са някои от примерите за приноса на ENISA към киберсигурността.

Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността, заедно с мрежата от национални координационни центрове, представлява новата рамка на Европа за подкрепа на иновациите и промишлената политика в областта на киберсигурността. След като бъдат напълно установени, центърът и мрежата ще вземат стратегически инвестиционни решения и ще обединяват ресурси за подобряване и укрепване на технологичния и промишления капацитет за киберсигурност. Поради това центърът ще играе ключова роля в постигането на целите в областта на киберсигурността, заложени в програмите„Цифрова Европа“ и „Хоризонт Европа“.

От 2022 г. насам мандатът на **Европол** е засилен, за да оказва по-голяма подкрепа на държавите — членки на ЕС, в борбата с тероризма, тежката и организираната престъпност. Европол вече е в състояние да подкрепя държавите членки при използването на нововъзникващи технологии и разработването на общи технологични решения. Освен това понастоящем той може да получава данни директно от частни лица (което спомага за справяне например с онлайн разпространението на материали, съдържащи сексуално насилие над деца). Освен това изпълнителният директор на Европол вече може да предлага национално разследване, ако престъпление в отделна държава членка засяга общ интерес, който попада в обхвата на политика на Съюза. Мандатът също така укрепи рамката на Европол за защита на данните и надзора от страна на Европейския надзорен орган по защита на данните. Непрекъснатата работа на Европол доведе до голям брой успешни операции, като например делото Encrochat, което досега е довело до над 6 500 ареста по целия свят. Мандатът също така укрепи рамката на Европол за защита на данните и надзора от страна на Европейския надзорен орган по защита на данните.

През октомври 2023 г. влезе в сила изменение на Регламента за **Евроюст**, с което се повишават възможностите на Евроюст да установи връзки между разследванията и наказателните преследвания за тероризъм, да въведе модерна система за управление на делата, да осигури сигурен цифров канал за комуникация между държавите членки и Евроюст, както и да улесни сътрудничеството с трети държави. Изменението също така гарантира, че Евроюст има правомощия за запазване, анализ и съхранение на доказателства, свързани с основни международни престъпления.

От началото на оперативната си дейност през юни 2021 г. насам **Европейската прокуратура** доказа, че съществено важна за разследването и наказателното преследване на престъпления, засягащи финансовите интереси на Съюза, когато фокусът е върху престъпленията срещу бюджета на Съюза. До 31 декември 2023 г. Европейската прокуратура е имала 1 927 текущи разследвания за щети на приблизителна стойност от над 19,2 млрд. евро. През 2023 г. са били внесени 139 обвинителни акта, което сочи към увеличаване на броя на обвиненията, повдигнати от Европейската прокуратура пред националните съдилища срещу заподозрени в измами с европейско измерение лица .

Frontex също е била активна по въпросите на сигурността, докато изпълнява своите задачи, свързани с границите, особено в областта на контрабандата на мигранти, както и

морската сигурност и трафика на хора. През януари 2024 г. Frontex и Европол подписаха споразумение, в което е очертано как двете агенции могат да координират дейностите си по-добре, за да се допълват взаимно и да определят конкретни приоритетни действия, които да бъдат постигнати в краткосрочен и дългосрочен план. На практика ролята на Frontex е да предоставя сведения от наблюдение и мониторинг на границите. От друга страна, ролята на Европол е да осигури реакция на правоприлагащите органи срещу организираната трансгранична престъпност и тероризма в рамките на ЕС. Освен това Frontex, **Европейската агенция по морска безопасност** и **Европейската агенция за контрол на рибарството** засилиха сътрудничеството си с подновяването на тристранното работно споразумение относно функциите за брегова охрана през 2021 г., като допринесоха за по-голямата сигурност по море.

VIII С ПОГЛЕД В БЪДЕЩЕТО

Благодарение на изобилието от законодателни и оперативни мерки, предприети през последните четири години, ЕС е по-добре подготвен да посрещне предизвикателствата в областта на сигурността, отколкото в началото на мандата на тази Комисия. Постоянно променящата се картина на заплахите обаче означава, че всяка една възможност за справяне с потенциалните уязвимости трябва да се използва. **Настоящата стратегия е приета с хоризонт до 2025 г. Работата ще трябва да продължи и след тази дата с постоянна бдителност и решителност.**

Понятието за сигурност, което традиционно е съсредоточено върху военните въпроси и вътрешните работи, трябва да бъде в крак с променящите се заплахи. Рисковете и уязвимостите трябва да бъдат взети под внимание — от икономическата сигурност до прекъсванията на доставките и готовността за действия при кризи, и на практика обхващащи всеки сектор на нашето общество — от здравеопазването, околната среда/климата до енергетиката и транспорта. Цифровото измерение вече е от основно значение за всички аспекти на сигурността и разделенията между онлайн и офлайн заплахите постепенно се изместват от нови реалности, като повечето заплахи включват кибер елемент и хибриден характер. В настоящата ситуация повече от всякога са видими присъщите връзки между вътрешните и външните измерения на сигурността. Ето защо **са необходими постоянни усилия, за да се гарантира, че аспектите на сигурността са включени във всички политики** и процеси на вземане на решения на ЕС.

Европейската стратегия за икономическа сигурност от 20 юни 2023 г. допълва „подхода, обхващащ цялото общество“, предложен в Стратегията на ЕС за Съюза на сигурност, като добавя стратегически компонент, който е насочен към защитата на интересите на ЕС, неговите държави членки и гражданите от заплахите за нашата икономика или от използването на икономически средства. В нея е определена рамка за постигане на **икономическа сигурност** чрез насърчаване на икономическата база и конкурентоспособността на ЕС; защита от рискове, както и установяване на партньорство с възможно най-широк кръг от държави с цел преодоляване на общите притеснения и вземане под внимание на общите интереси, и това ще бъде **ключов елемент в бъдещите съображения за сигурността на ЕС**.

Новата политика на ЕС в областта на киберотбраната е само една област, в която се вижда необходимостта от **подобряване на координацията между цивилните общности и военната/отбранителната екосистема,** като връзките между тези две области вероятно ще се увеличават в бъдеще.

Извършителите на престъпления бързо се адаптират и използват нови технологии в своята дейност. **Експертната група на високо равнище относно достъпа до данни за ефективно правоприлагане**, която се председателства съвместно от Комисията и председателството на Съвета, разглежда предизвикателствата, пред които са изправени практикуващите специалисти в областта на правоприлагането, по-специално достъпът до данни. При разглеждането в бъдеще на въпроса за сигурността ще трябва да бъде **проучено как правоприлагащите органи могат да използват цифровите технологии,** като същевременно гарантират пълното зачитане на основните права, когато става въпрос за достъп до данни в области като квантова комуникационна инфраструктура, изкуствен интелект и модерни технологии за наблюдение.

Политиките за сигурност в бъдеще ще трябва да продължат да търсят ефективен отговор на променящите се рискове. За тази цел ще бъде необходимо да се преосмисли начинът, по който институциите и органите на ЕС, както и държавите членки следва да реагират на предизвикателствата и да гарантират способността на ЕС да реагира бързо, когато това е необходимо. **Трябва да се избягва разделението и механизмите за реагиране, които дублират оценката на риска или усложняват реакцията при кризи**.

Освен това, тъй като ЕС продължава да демонстрира способността си да се адаптира към променящите се рискове, не следва да се допуска развитието на нови уязвимости чрез неравномерно прилагане на вече договорените инструменти. **Ефективното изпълнение и прилагане на законодателството на национално равнище е от съществено значение**.

Въпреки че капацитетът на ЕС беше подсилен от нарастващата роля за сигурността на агенциите на ЕС, той **може да бъде оптимизиран чрез по-нататъшно подобряване на координацията и взаимното допълване между агенциите**. Уместно е да се разгледа възможността за задълбочаване на сътрудничеството не само между агенциите, които обичайно се занимават с въпросите на сигурността, като Европол, Евроюст, ENISA, Frontex и Европейската прокуратура, но и между секторните агенции, включително новата Агенция на ЕС по наркотиците, Органа за борба с изпирането на пари, Европейската агенция за авиационна безопасност, Европейската агенция по морска безопасност и Европейската агенция за контрол на рибарството.

В Стратегията за Съюза на сигурност за периода 2020—2025 г. инструментариумът на ЕС за сигурност е консолидиран и представлява надеждна основа за защитата на европейците в бъдеще. Занапред действията, предприети по всички направления на Съюза на сигурност, ще продължат да бъдат съществено важни за гарантиране, че ЕС е способен да се приспособи, дори да е изправен пред изключителни и неочаквани заплахи.