Съвет на
Европейския съюз

Брюксел, 18 октомври 2023 г.
(OR. en)

14372/23

JAI 1332	**COPEN 363**
COSI 179	**FREMP 292**
ENFOPOL 431	**JAIEX 66**
ENFOCUSTOM 110	**CFSP/PESC 1410**
IXIM 194	**COPS 489**
CT 155	**HYBRID 73**
CRIMORG 137	**DISINFO 85**
FRONT 327	**TELECOM 306**
ASIM 92	**DIGIT 223**
VISA 208	**COMPET 1008**
CYBER 247	**RECH 456**
DATAPROTECT 278	**CULT 122**
CATS 58	**COTER 185**
DROIPEN 151	**CORDROGUE 94**

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	18 октомври 2023 г.
До:	Г-жа Thérèse BLANCHET, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2023) 665 final
Относно:	СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА относно Шестия доклад за напредъка по изпълнението на Стратегията на ЕС за Съюза на сигурност

Приложено се изпраща на делегациите документ COM(2023) 665 final.

Приложение: COM(2023) 665 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 18.10.2023 г.
COM(2023) 665 final

СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

относно Шестия доклад за напредъка по изпълнението на Стратегията на ЕС за Съюза на сигурност

I. Въведение

Преди три години Комисията прие Стратегията на ЕС за Съюза на сигурност за периода 2020—2025 г.[1], в която се определят основните приоритети на Съюза в областта на сигурността. Оттогава насам сме постигнали осезаем напредък по всички четири стълба на стратегията, като е прието ключово законодателство във всички сфери — от защита на критични субекти до повишаване на киберустойчивостта. Междувременно обаче картината на заплахите за сигурността в Европа и в съседните ни държави продължава да търпи промени. Терористичните атаки в едно училище във Франция и на улицата в Брюксел от последните дни рязко припомнят колко е наложително да продължим да адаптираме и укрепваме нашата архитектура в областта на сигурността. Опасността от кибератаки продължава да нараства, подхранвана също и от злонамерени субекти, които вземат страна по текущите конфликти. Хибридните заплахи, включително дезинформацията, продължават да се множат. Европол определи агресивната война на Русия срещу Украйна като причината за чувствителен ръст на кибератаките срещу цели в ЕС, като основните атаки са с политически мотиви и се координират от проруски настроени хакерски групи[2]. Това беше усетено като блокиране на достъпа до интернет и прекъсване на ключови услуги, например на енергийни мрежи[3].

Стратегията на ЕС за Съюза на сигурност беше разработена, за да оборудва ЕС така, че да противостои по-ефективно на променящата се картина на заплахите. Докато се сблъсквахме с кризите, породени от пандемията и войната, събитията ни показаха значението на подхода, възприет в рамките на стратегията — нашата решимост да свържем точките в цялата екосистема на сигурността и да премахнем разделението между киберизмерението и физическото измерение на сигурността, в т.ч. справянето с организираната престъпност и тероризма, както и борбата с радикализацията.

Бдителността обаче налага да продължим да подлагаме на проверка какво не достига в усилията ни да осигурим безопасността на нашите граждани. В стратегията са определени приоритетни области, в които Съюзът може да допринесе с добавена стойност, за да подпомогне държавите членки в укрепването на сигурността на всички хора, живеещи в Европа. От приемането ѝ насам се работи по всички заложени действия и са включени нови такива, за да се отговори на постоянните предизвикателства в областта на сигурността.

Като цяло Комисията е представила 36 законодателни инициативи в рамките на Стратегията на ЕС за Съюза на сигурност. За повече от половината от тези предложения преговорите между институциите вече са завършили с изготвянето на солидно ново законодателство, както е описано в таблицата в приложението. Въпреки това по няколко ключови инициативи, предложени от Комисията, продължават да текат преговори между

---

1 COM(2020) 605.

2 Разпределена атака тип „отказ от обслужване“ (DDoS): вж. доклада на Europol Spotlight „Cyber-attacks: the apex of crime-as-a-service (Кибератаките: върхна точка на „престъплението като услуга“), 13 септември 2023 г.

3 По време на конфликта в Украйна е използван масирано зловреден софтуер, изтриващ или унищожаващ достъпа на организации до файлове и данни (т.нар. wiper), за унищожаване на данни и системи, като например беше засегнат достъпът до интернет на хиляди абонати в ЕС, както и на голямо германско енергийно дружество, което загуби достъпа до наблюдение от разстояние на над 5800 вятърни турбини. „Ролята на кибератаките във войната на Русия срещу Украйна: тяхното въздействие и последици за бъдещето на въоръжените конфликти“ (The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict), проучване на Европейския парламент, септември 2023 г. — PE 702.594.

Европейския парламент и Съвета. Тъй като настоящият парламентарен мандат приключва с изборите за Европейски парламент през юни 2024 г., е необходима експедитивна работа, за да се постигнат резултати по тези нерешени досиета, така че гражданите да могат да се ползват от Съюза на сигурност в пълна степен. Поради това настоящият 6[и] доклад за напредъка на Съюза на сигурност е съсредоточен върху очертаването на тези решаващи за Съюза на сигурност законодателни и незаконодателни досиета, приети от Комисията, за чието финализиране и ефективно прилагане трябва да бъдат положени допълнителни усилия.

Що се отнася до вече договорените правни актове на ЕС, ползите от тях ще бъдат усетени едва след като те бъдат приложени на практика. Работата трябва да се съсредоточи върху правилното и пълното им транспониране, изпълнение и прилагане от държавите членки. През 2023 г. Комисията продължи да гарантира, че Стратегията на ЕС за Съюза на сигурност дава резултати, като използваше институционалните си правомощия да образува производства за установяване на нарушение всеки път, когато държавите членки не бяха транспонирали или бяха транспонирали неправилно законодателството на ЕС.

В настоящия доклад също така е обобщено в кои случаи от решаващо значение за постигането на резултати са действията на държавите членки и/или на агенциите на ЕС. Агенциите на ЕС играят решаваща роля в подпомагането на изпълнението на инициативи в рамките на Съюза на сигурност и техните отговорности претърпяха развитие през последните години. В доклада са очертани някои от основните нови задачи, които са им възложени, за да се обезпечи по-голяма подкрепа за държавите членки при изпълнението на ключови инициативи в рамките на Съюза на сигурност.

Освен това поради геополитическата обстановка се откроi значението на външната сигурност за нашата вътрешна сигурност. По-солидната вътрешна рамка на ЕС в областта на сигурността е неразривно свързана с по-силни партньорства и сътрудничество с трети държави. ЕС трябва да продължи активно да търси начини, по които поемането на ангажименти в световен план може да помогне за гарантиране на сигурността на неговите граждани у дома.

II. Среда на сигурност, която е подготвена за бъдещето

Киберсигурност и устойчивост на критичната инфраструктура

В рамките на Съюза на сигурност Съюзът е поел ангажимент да гарантира, че всички европейски граждани и предприятия са добре защитени, както онлайн, така и офлайн, и да насърчава отворено, сигурно и стабилно киберпространство. Увеличаващите се мащаби, честота и въздействие на киберинцидентите представляват сериозна заплаха за функционирането на мрежите и информационните системи и за вътрешния пазар. Агресивната война на Русия срещу Украйна допълнително изостри тази заплаха, а настоящото геополитическо напрежение се утежнява от намесата на множество участници, подкрепящи държавни, престъпни или хактивистки интереси. Саботажът през миналата есен на тръбопроводите „Северен поток“ подчерта как основни сектори като енергетиката, цифровата инфраструктура, транспорта и космическото пространство зависят от устойчива критична инфраструктура. Неотдавнашният инцидент с подводен газопровод и кабел за пренос на данни между Естония и Финландия илюстрира

необходимостта от висока степен на готовност за справяне с подобни ситуации. Въпреки че причината за щетите остава неясна и разследванията продължават, обменът на информация на различни равнища между държавите членки и Комисията е окуражителен. Прекъсванията нямаха непосредствен ефект върху интернет свързаността, нито върху сигурността на доставките на газ на европейско или местно равнище. Това е знак за постигнатия напредък и засилените усилия за готовност през последните месеци.

Ето защо наличието на ясна и солидна правна рамка е от съществено значение, за да се гарантират защитата и устойчивостта на тези критични инфраструктури. В този контекст важен пробив беше постигнат с успоредното приемане на преработената Директива относно мерките за високо общо ниво на киберсигурност в Съюза (МИС 2)[4] и Директивата относно устойчивостта на критичните субекти (УКС)[5], които влязоха в сила едновременно на 16 януари 2023 г. Сега държавите членки се приканват да транспонират тези основни законодателни актове бързо и изцяло, най-късно до 17 октомври 2024 г., за да въведат солидна рамка на Съюза за защита на критичната инфраструктура на Съюза срещу физически заплахи и киберзаплахи.

През юли 2023 г. Комисията определи в делегиран регламент основните услуги в 11-те сектора, обхванати от Директивата за УКС[6]. Следващата стъпка е държавите членки да извършат оценка на риска за тези услуги. Вследствие на препоръката на Съвета[7] от 8 декември 2022 г. се активизира работата по стрес тестове на критичната инфраструктура, като на първо място бе поставен енергийният сектор, както и по укрепване на сътрудничеството с НАТО и ключови държави партньори. Тази работа доведе до изготвянето през юни 2023 г. на доклад на работната група ЕС-НАТО относно устойчивостта на критичната инфраструктура, като в него бяха очертани настоящите предизвикателства в областта на сигурността пред критичната инфраструктура в четири ключови сектора (енергетика, транспорт, цифрова инфраструктура и космическо пространство) и бяха отправени препоръки за повишаване на устойчивостта. Препоръките, включително относно засилената координация, обмена на информация и ученията, понастоящем се прилагат от служителите на ЕС и НАТО в контекста на структурирания диалог относно устойчивостта.

Успоредно с това на 6 септември 2023 г. Комисията прие предложение[8] за препоръка на Съвета относно подробен план за координиран отговор на равнището на Съюза на смущения в критичната инфраструктура със значително трансгранично значение. На 4 октомври 2023 г. беше организирано учение под формата на основано на сценарий обсъждане на подробния план, за да се провери как той би бил приложен на практика и да се осигури информация за текущите преговори по предложението в Съвета.

Вследствие на призиви от страна на Съвета[9] Комисията, върховният представител и групата за сътрудничество по МИС извършват оценки на риска и изготвят сценарии

---

[4] Директива (ЕС) 2022/2555 от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза и Директива (ЕС) 2018/1972 (Директива МИС 2).

[5] Директива (ЕС) 2022/2557 на Европейския парламент и на Съвета от 14 декември 2022 г. за устойчивостта на критичните субекти и за отмяна на Директива 2008/114/ЕО на Съвета.

[6] C(2023)4878.

[7] Препоръка на Съвета от 8 декември 2022 г. относно координиран подход на равнището на Съюза за укрепване на устойчивостта на критичната инфраструктура.

[8] COM(2023) 526.

[9] Заключения на Съвета от 23 май 2022 г. относно позицията на ЕС в киберпространството и Призив от Невер от 9 март 2022 г. за укрепване на капацитета на ЕС за киберсигурност.

относно рисковете от гледна точка на киберсигурността. Работата първоначално се съсредоточава върху секторите на далекосъобщенията и електроенергията. Участието на всички съответни агенции и мрежи от гражданския и от военния сектор за първи път дава възможност за изчерпателна и всеобхватна оценка в целия Съюз. Освен това тя ще допълни координираните оценки на риска за сигурността на критични вериги за доставки, които се провеждат съгласно МИС 2, както и оценките на риска и стрес текстовете на критична инфраструктура в секторите на енергетиката, комуникациите по цифрова инфраструктура, транспорта и космическото пространство. В интерес на координацията и съгласуваността тези дейности следва взаимно да се допълват, за да спомогнат за установяването на стандартизиран подход, и следва да осигуряват насоки за разработването на бъдещи учения. Понастоящем успехът на тези дейности ще зависи от активното ангажиране на държавите членки.

Функционирането на икономиките и обществата във все по-голяма степен зависи от свързаните с космоса услуги и данни, особено в областта на сигурността и отбраната. Космическото пространство е все по-оспорвана стратегическа сфера, а значението му за сигурността нарасна особено след нахлуването на Русия в Украйна. Космическата стратегия на ЕС за сигурност и отбрана беше приета през март 2023 г. с цел да укрепим своята стратегическа позиция и автономност в областта на космическото пространство. Като ключово действие, произтичащо от тази стратегия, Европейската комисия ще предложи през 2024 г. законодателен акт на ЕС относно космическото пространство, в който се уреждат безопасността, устойчивостта и гъвкавостта/сигурността на космическите дейности в ЕС.

Що се отнася до външното измерение, сигурната инфраструктура е в основата на устойчивостта на световната икономика и веригите на доставките[10] и по тази причина в стратегията на ЕС за Global Gateway измерението, свързано със сигурността, е силно застъпено. Също така, с оглед на взаимната свързаност между инфраструктурите на ЕС и на държавите партньори по-нататъшното международно сътрудничество е жизненоважно за укрепване на киберсигурността на световно равнище и за подкрепа на свободно, отворено, безопасно и сигурно киберпространство.

Законодателен акт за киберустойчивост.

Осигуряването на това, че потребителите и предприятията могат да разчитат на сигурни цифрови продукти, е от основно значение за европейската киберсигурност. Комисията положи усилия да отговори на тази потребност в предложението си за Законодателен акт за киберустойчивост[11], прието на 15 септември 2022 г. С него ще бъдат въведени задължителни хоризонтални изисквания във връзка с киберсигурността за продукти с цифрови компоненти за срок от пет години или за целия им жизнен цикъл (който от двата периода е по-кратък). С него ще бъдат създадени условия за разработване на защитени продукти с цифрови елементи, като се гарантира, че на пазара се пускат хардуерни и софтуерни продукти с възможно най-малко уязвимости. Това ще бъде ключово постижение в повишаването на европейските стандарти в областта на киберсигурността във всички сфери и вероятно ще се превърне в международен еталон, като осигури ясни предимства за промишлеността на Съюза в сектора на киберсигурността на световните пазари. Европейският парламент и Съветът приеха съответните си позиции през юли 2023 г. и преговорите следва да отбележат бърз напредък.

[10] JOIN(2021) 30.
[11] COM(2022) 454.

Сертифицирането за киберсигурност също играе жизненоважна роля за повишаване на доверието в продуктите и услугите на информационните технологии, като позволява на потребителите, предприятията и органите да правят информиран избор с подходящо равнище на киберсигурност. Работата по сертифицирането за киберсигурност напредва с оценяването в рамките на процедурата на комитет на основаната на общи критерии схема на ЕС за сертифициране на киберсигурността. Проектът за схема на ЕС за сертифициране на услуги в облак (EUCS) понастоящем се подготвя от Агенцията на Европейския съюз за киберсигурност (ENISA) и се обсъжда в рамките на Европейската група за сертифициране на киберсигурността. Интензивната работа с експерти от редица сектори, с потребители и доставчици, следва да доведе до надежден от правна и техническа гледна точка подход, който предоставя необходимите гаранции за сигурността в съответствие с правото на Съюза, международните ангажименти и задълженията в рамките на СТО. Освен това ENISA подготвя проекта за европейска схема за сертифициране на киберсигурността EU5G и портфейла на ЕС за цифрова самоличност (EUIDW). Съвместните усилия на всички държави членки са от решаващо значение за повишаване на цялостната сигурност на продуктите, услугите и процесите на информационните технологии.

Регламенти относно информационната сигурност и киберсигурността на институциите, органите и агенциите на ЕС (ИОАЕС)

Предложени заедно през март 2022 г., предложенията за регламенти, с които се уреждат киберсигурността и информационната сигурност за собствените институции на Съюза, се движат към целта с различни темпове. През юни миналата година беше постигнато политическо споразумение по Регламента за киберсигурността, което позволява укрепване на киберсигурността на всички институции, органи, служби и агенции на ЕС и отразява значението, което ЕС отдава на бързото прилагане на това предложение. В тази ситуация особена загриженост буди фактът, че успоредното предложение относно информационната сигурност, което е от съществено значение за завършването на една солидна законодателна рамка за ИОАЕС, бележи неочаквано бавен напредък. И двете предложения следва да бъдат приети преди изборите за Европейски парламент, за да може европейската администрация да бъде надеждна и устойчива в настоящия геополитически контекст. Минимален набор от правила и стандарти относно информационната сигурност за всички ИОАЕС би създал сигурност за всички участващи страни и би гарантирал последователна защита срещу променящите се заплахи за информацията на ЕС, с която те боравят, както класифицирана, така и некласифицирана. Взети заедно, тези нови правила ще осигурят стабилна основа за сигурен обмен на информация между ИОАЕС и държавите членки със стандартизирани практики и мерки за защита на информационните потоци. По този начин те отговарят на многобройните призиви от страна на Съвета да се повиши устойчивостта на ИОАЕС и да се защити по-добре процесът на вземане на решения в Съюза от злонамерена намеса.

Законодателен акт за киберсолидарност

Въз основа на стабилната стратегическа, политическа и законодателна рамка, която вече е въведена, предложеният от Комисията на 18 април 2023 г. законодателен акт за киберсолидарност[12] ще подобри допълнително откриването на киберзаплахи, устойчивостта и готовността на всички равнища на екосистемата на киберсигурност на Съюза. Тези цели ще бъдат осъществени чрез три основни действия:

[12] COM(2023) 209.

(1) разгръщане на ***европейски киберщит*** за изграждане и подобряване на общите способности за откриване и ситуационна осведоменост. Той ще се състои от национални центрове за операции по сигурността („национални ЦОС“) и трансгранични оперативни центрове по сигурността („трансгранични ЦОС“);
(2) създаване на ***Механизъм за действие при извънредни ситуации в областта на киберсигурността***, който да подпомага държавите членки при подготовката, реагирането и незабавното възстановяване след значителни и мащабни инциденти в областта на киберсигурността. Подкрепата за реагиране при инциденти ще включва киберрезерва на ЕС, който ще бъде на разположение и на институциите, органите, службите и агенциите на Европейския съюз (ИОАЕС), както и на трети държави, асоциирани към програма „Цифрова Европа“, при условие че това е предвидено в тяхното споразумение за асоцииране към програма „Цифрова Европа“;
(3) създаване на ***европейски Механизъм за преглед на киберинциденти***, чрез който да се разглеждат и оценяват конкретни значителни или мащабни киберинциденти. Докладът от последващ преглед след инцидент ще бъде координиран и изготвян от ENISA.

В Съвета и в Европейския парламент започнаха обсъждания. Приключването на преговорите преди края на настоящия мандат на Европейския парламент ще даде значителен тласък на усилията за защита на гражданите и предприятията в целия Съюз.

Академия на ЕС за киберумения

Докато киберзаплахите се увеличават, ЕС се нуждае спешно от специалисти с умения и познания за предотвратяване, откриване, възпиране и защита на ЕС от кибератаки. Работната сила на Съюза в областта на киберсигурността понастоящем се оценява на 883 000 специалисти, а през 2022 г. незаетите свободни работни бяха в порядъка между 260 000 и 500 000. Всички слоеве на обществото следва да бъдат насърчавани да помагат за запълването на този недостиг, но по-конкретно през 2022 г. жените представляват едва 20 % от завършилите специалности в сферата на киберсигурността и едва 19 % от специалистите по информационни и комуникационни технологии. Като част от изданието през 2023 г. на Европейската година на уменията на 18 април 2023 г.[13] Комисията прие приветствана от държавите членки инициатива[14] за създаване на Академия на ЕС за киберумения с цел преодоляване на недостига на таланти в областта на киберсигурността. В рамките на Академията на ЕС за киберумения ще бъдат обединени съществуващите инициативи за изграждане на умения в областта на киберсигурността и ще бъде подобрена координацията. Комисията насърчава държавите членки, регионалните и местните власти, както и европейските публични субекти, да приемат специални стратегии или инициативи относно уменията в областта на киберсигурността или да интегрират уменията в областта на киберсигурността в съответните стратегии или инициативи с по-широк обхват (например киберсигурност, цифрови умения, заетост и т.н.). Жизненоважно за намаляване на недостига на умения в областта на киберсигурността и свързания с това недостиг на работна ръка в Европа ще бъде и участието на заинтересованите страни от частния сектор.

[13] COM(2023) 207.
[14] Заключения на Съвета от 22 май 2023 г. относно политиката на ЕС в областта на киберотбраната.

Безпилотни летателни апарати

Друга нарастваща заплаха за обществените пространства и критичните инфраструктури е използването на безпилотни летателни апарати за злонамерени цели. Инцидентите с безпилотни летателни апарати зачестиха в Съюза и извън него, а решенията за противодействие на безпилотни летателни апарати са ключов инструмент за правоприлагащите и други публични органи в Съюза, както и за частните оператори на критична инфраструктура. В същото време законосъобразното използване на безпилотни летателни апарати има важен принос за двойния екологичен и цифров преход[15]. Както бе обявено в приетата през ноември 2022 г. Стратегия 2.0 за безпилотни летателни апарати, днес Комисията приема съобщение относно начините за противодействие на потенциални заплахи от безпилотни летателни апарати, подкрепено от два наръчника, съдържащи практически насоки относно ключови технически аспекти[16]. Инициативата има за цел да предложи всеобхватна и хармонизирана рамка на политиката с общо разбиране на правилата за борба с възможните заплахи от безпилотни летателни апарати и възможност за адаптиране при необходимост към бързото развитие на технологиите. Държавите членки и съответните частни оператори се приканват да работят в тясно сътрудничество с Комисията, за да гарантират пълното ѝ прилагане.

Морска сигурност и сигурност на въздухоплаването

Незаконните дейности, като пиратството, въоръжените грабежи в морето, контрабандата на мигранти и трафика на хора, трафика на оръжия и наркотици, както и тероризма, продължават да бъдат предизвикателства за морската сигурност и се усложняват от променящите се заплахи, включително хибридни атаки и кибератаки. На 10 март 2023 г. Комисията и върховният представител приеха Съвместно съобщение относно актуализиране на Стратегията на ЕС за морска сигурност[17], която сега следва да бъде изпълнявана в съответствие с актуализирания план за действие.

В областта на сигурността на въздухоплаването на 2 февруари 2023 г. Комисията прие работен документ на службите на Комисията „Усилия за постигане на усъвършенствана и по-устойчива политика в областта на сигурността на въздухоплаването“[18], който съдържа амбициозна програма за 1) модернизиране на регулаторната архитектура в областта на сигурността на въздухоплаването; 2) насърчаване на разработването и внедряването на по-иновативни решения; и 3) актуализиране на базовото равнище на сигурност на въздухоплаването, така че летищата на Съюза да могат да се възползват изцяло от новите и авангардни технологии за справяне със заплахите с най-висок приоритет. В рамките на две години трябва да бъдат изпълнени четиринадесет водещи действия.

Комисията призовава Европейския парламент и Съвета да приключат в спешен порядък, във всички случаи преди края на мандата на настоящия Европейски парламент, преговорите по следните досиета:

- предложението за законодателен акт за киберустойчивост;
- предложението за законодателен акт за киберсолидарност;
- предложението за регламент относно информационната сигурност на ИОАЕС.

[15] COM(2022) 652.
[16] COM(2023) 659.
[17] JOIN(2023) 8.
[18] SWD(2023) 37.

Комисията призовава държавите членки:

- да продължат приоритетно с транспонирането на Директивата относно устойчивостта на критичните субекти, както и с провеждането на стрес тестове на критичната инфраструктура в енергийния сектор;
- да приемат препоръката на Съвета относно подробен план за координиран отговор на смущения в критичната инфраструктура със значително трансгранично значение;
- да транспонират изцяло и спешно Директивата за МИС 2, за да се повиши киберсигурността на съществените и важните субекти;
- активно да се ангажират с извършването на оценки на рисковете за киберсигурността и изготвянето на сценарии за риска, свързан с критичната инфраструктура и веригите на доставките;
- да осъществят последващи действия във връзка с Академията на ЕС за киберумения, включващи силна ангажираност на европейско равнище и специални национални стратегии или инициативи за изграждане на умения в областта на киберсигурността, като привлекат ключови заинтересовани страни, включително регионални и местни власти;
- да работят със съответните частни оператори и с Комисията, за да се гарантира изпълнението на всички действия, изброени в съобщението относно начините за противодействие на потенциални заплахи от безпилотни летателни апарати;
- да приложат плана за действие по стратегията на ЕС за морска сигурност и да докладват редовно за постигнатите резултати;
- да изпълнят набелязаните 14 водещи действия за повишаване на сигурността на въздухоплаването.

III. Справяне с променящите се заплахи

Нововъзникналите геополитически напрежения са ярко доказателство за това, че предизвикателствата пред сигурността на ЕС не само се увеличават, но и стават все по-взривоопасни и са допълнително изострени поради хибридния характер на много от заплахите. Сигурността също трябва да бъде адаптирана и към промените в обществото и технологиите. Пандемията от COVID-19 увеличи възможностите за киберпрестъпниците и доведе по-специално до увеличена заплаха от разпространението в интернет на материали, съдържащи сексуално насилие над деца. Престъпниците и злонамерените участници винаги са готови да се възползват от технологичното развитие. При сблъскването с такива често комплексни и многоизмерни заплахи са необходими решителни и последователни действия от страна на ЕС.

Регламент относно борбата с онлайн сексуалното насилие над деца

Оценката на Европол на заплахата от организирана престъпност в Интернет разкри, че през 2022 г. сексуалната експлоатация и малтретирането на деца са продължили да нарастват като честота и тежест, като извършителите продължават да се възползват от техническите възможности, за да прикриват действията и самоличността си[19]. Настоящата система, основана на доброволно разкриване и докладване от страна на

[19] Европол (2023 г.), Оценка на заплахата от организирана престъпност в Интернет (IOCTA), 2023 г.

дружествата, се оказа недостатъчна за защита на децата. Временният регламент позволява доброволно разкриване и докладване от страна на дружествата, при условие че това е законосъобразно съгласно Общия регламент относно защитата на данните (ОРЗД). Срокът на действие на този регламент ще изтече през август 2024 г. През май 2022 г. Комисията представи предложение за регламент[20] за справяне със злоупотребата с онлайн услуги за целите на сексуалното насилие над деца. В предложената рамка се поставя силен акцент върху превенцията. Дружествата ще бъдат задължени да оценяват риска от сексуално насилие над деца чрез своите системи и да предприемат превантивни действия. Като крайна мярка, само в случай на съществен риск, националните съдилища или независими административни органи могат да издават целеви заповеди за откриване на доставчиците на услуги. Нов независим център на ЕС ще улеснява усилията на доставчиците на услуги, като изпълнява ролята на център за експертен опит, предоставя надеждна информация за идентифицирани материали, получава и анализира доклади за онлайн сексуално насилие над деца от доставчиците, за да идентифицира погрешни доклади, както и като предоставя подкрепа на жертвите. От съществено значение е новите правила да бъдат приети и приложени възможно най-скоро, за да се предпазят децата от по-нататъшно насилие, да се предотврати повторната поява на материали онлайн и извършителите да се изправят пред съда. Понастоящем в Съвета и в Парламента се водят преговори с цел постигане на споразумение по досието преди изтичането на мандата на Парламента.

Директива относно борбата с насилието над жени и домашното насилие

Кибернасилието над жени, включително в контекста на домашното насилие, се превърна в нова форма на такова насилие, която чрез интернет и ИТ инструменти се разпространява отвъд границите на отделните държави членки. През март 2022 г. Комисията представи предложение за директива за противодействие на насилието над жени и домашното насилие, включително конкретни правила относно кибернасилието и мерки за запълване на пропуските в защитата, достъпа до правосъдие и превенцията. Приемането и прилагането на ранен етап ще даде на държавите членки допълнителни инструменти за борба с тази форма на престъпления. Съзаконодателите започнаха междуинституционални преговори през юли 2023 г. и се стремят да приключат преговорите преди края на настоящия мандат на Европейския парламент.

Киберсигурност на 5G технологиите

Сигурността на 5G мрежите е основен приоритет за Комисията и основен елемент от нейната Стратегия на ЕС за Съюза на сигурност. 5G мрежите са централна инфраструктура, която осигурява основата за широк спектър от услуги от съществено значение за функционирането на вътрешния пазар и за жизненоважни обществени и икономически функции. На 15 юни 2023 г. органите на държавите — членки на ЕС, представени в групата за сътрудничество за МИС, с подкрепата на Комисията и ENISA, публикуваха втори доклад за напредъка по прилагането на инструментариума на ЕС за киберсигурност на 5G технологиите. Според описаното в доклада 24 държави членки са приели или подготвят законодателни мерки, които предоставят на националните органи правомощия да извършват оценка по отношение на доставчиците и да налагат ограничения, а 10 държави членки са наложили такива ограничения. Необходими са обаче по-нататъшни действия, за да се избегнат уязвимости за Съюза като цяло, които могат да имат значително отрицателно въздействие върху сигурността на отделните потребители и дружества в Съюза, както и върху критичната инфраструктура на Съюза.

[20] COM(2022) 209.

Всички държави членки трябва незабавно да приложат инструментариума. В същия ден Комисията прие съобщение относно прилагането на инструментариума от държавите членки и относно дейностите на Комисията в областта на корпоративните комуникации и дейностите по финансиране от Съюза. Това подчертава силната загриженост относно рисковете за сигурността на ЕС, свързани с доставчиците на комуникационно оборудване за мобилни мрежи Huawei и ZTE. В този контекст Комисията предприема мерки, за да избегне излагането на корпоративните си комуникации на въздействието на мобилните мрежи, които използват като доставчици Huawei и ZTE. От обществените поръчки ще бъдат изключени нови услуги за свързаност, разчитащи на оборудване от тези доставчици, и Комисията ще работи с държавите членки и телекомуникационните оператори, за да гарантира, че тези доставчици постепенно ще бъдат отстранени от съществуващите услуги за свързаност на обектите на Комисията. Комисията също така проучва как това решение да бъде отразено в съответните програми и инструменти за финансиране на Съюза при пълно спазване на правото на Съюза.

Достъп до данни за целите на ефективното правоприлагане

В днешната ера на цифровите технологии почти всяко престъпление съдържа цифров елемент. Технологиите и инструментите се използват и за престъпни цели, включително онези от тях, които са необходими, за да се обезпечи необходимостта на нашето общество от киберсигурност, защита на данните и неприкосновеност на личния живот. Това затруднява все повече поддържането на ефективно правоприлагане в целия ЕС с цел опазване на обществената сигурност и предотвратяване, разкриване, разследване и наказателно преследване на престъпления, и въпреки че са положени значителни усилия на равнището на Съюза и на национално равнище, включително чрез законодателство, както и чрез инициативи за изграждане на капацитет и иновации, правните и техническите предизвикателства продължават да са на лице. Комисията, в сътрудничество с председателството на Съвета, създаде експертна група на високо равнище относно достъпа до данни за ефективно правоприлагане, за да предостави платформа за сътрудничество на широк кръг заинтересовани страни и експерти за проучване на предизвикателствата, пред които са изправени специалистите в областта на наказателното правоприлагане (например криптиране, съхраняване на данни, 5G и стандартизация). Комисията очаква до юни 2024 г. експертната група да формулира балансирани, солидни и изпълними препоръки, в които да бъде взета предвид сложността на тези въпроси, включително от гледна точка на киберсигурността и защитата на данните. Ето защо държавите членки и участващите експерти се насърчават да се вземат активно участие в този процес и да работят за намирането на ефективни, законосъобразни и общоприети решения.

Хибридни заплахи

В геополитически контекст, в който степента на сложност и техническо развитие на хибридните заплахи нараства, чрез Стратегическия компас за сигурност и отбрана на ЕС[21] („Стратегическия компас“) бе предоставена обща оценка на заплахите и предизвикателствата, пред които е изправен Съюзът, както и стратегически план за действие. Увеличаването на злонамерените действия в киберпространството от страна на държави и недържавни участници, включително в контекста на войната срещу Украйна, допълнително изведе на преден план киберпространството като област на външната политика и политиката в областта на сигурността. Потенциалните рискове от

[21] Документ на Съвета 7371/22.

злонамерени действия и дезинформация налагат особена бдителност в периодите на избори, включително в навечерието на изборите за Европейски парламент през 2024 г.

Предвид високите рискове от разпространение на отрицателни последици ЕС продължи да развива дейности за изграждане на капацитет за киберсигурност и да насърчава партньорства с трети държави, включително чрез специални кибердиалози, за да допринесе активно за цялостната си устойчивост. Бяха разработени, преразгледани и подсилени редица инструменти, за да се повиши способността на Съюза да се справя ефективно с хибридните заплахи, както е описано в седмия Доклад за напредъка в противодействието на хибридните заплахи, публикуван на 14 септември 2023 г.[22]. Те включват:

- инструментариума на ЕС за борба с хибридните заплахи, за да се осигури рамка за координирана и добре информирана реакция на хибридни заплахи и кампании;
- продължаващата работа за установяването на екипи на ЕС за бързо реагиране при хибридни заплахи за краткосрочна съобразена с нуждите подкрепа за държавите членки, държавите партньори и мисиите и операциите, свързани с общата политика за сигурност и отбрана (ОПСО);
- преразгледания протокол на ЕС за борба с хибридните заплахи (EU Playbook)[23], в който са описани процесите и структурите на Съюза за справяне с хибридни заплахи и кампании;
- преразгледаните насоки за прилагане на рамката за съвместен дипломатически отговор на ЕС срещу злонамерени дейности в киберпространството[24] („инструментариум за кибердипломация“), която дава възможност за разработване на устойчиви, адаптирани, съгласувани и координирани стратегии за борба с настойчиви участници в киберзаплахи;
- инструментариума за чуждестранно манипулиране на информация и вмешателство (FIMI), за да се укрепят съществуващите инструменти на Съюза за предотвратяване, възпиране и отговор на FIMI;
- европейската политика за киберотбрана[25], за да се засилят способностите на ЕС в областта на киберотбраната, да се подобри ситуационната осведоменост и да се координират всички налични възможности за защита, така че да се укрепи устойчивостта, да се реагира на кибератаки и да се осигурят солидарност и взаимопомощ.

Ето защо държавите членки се насърчават да продължат и активизират сътрудничеството си в тази област, като гарантират ефективното прилагане на горепосочените инструментариуми, включително чрез редовни учения, и като постигнат съгласие по концепцията за екипи за бързо реагиране при хибридни заплахи, което ще даде насоки за по-нататъшните стъпки към създаването на екипите.

Изкуственият интелект в контекста на правоприлагането

Изкуственият интелект (ИИ) бързо се превърна в обичаен елемент от ежедневието. Последиците от използването на изкуствен интелект върху киберпрестъпността и киберсигурността все още не са напълно известни, но със сигурност ще създадат нови предизвикателства. Въпреки че изкуственият интелект може да донесе ползи, когато се използва по безопасен и контролиран начин, той може да има опасен потенциал в ръцете

[22] SWD(2023) 315.
[23] SWD(2023) 116.
[24] 10289/23 от 8 юни 2023 г.
[25] JOIN(2022) 49.

на злонамерени участници, включително като помага на престъпниците да скрият самоличността си в престъпления като тероризъм и сексуално насилие над деца. Ето защо е изключително важно органите да бъдат в крак с новостите, за да предотвратяват насилие и да реагират в случаи на неправилна употреба[26]. Преговорите по предложения Законодателен акт за изкуствения интелект имат за цел да дадат отговор на тези въпроси и навлязоха в решаващ етап, като в момента съзаконодателите обсъждат технически и политически въпроси, които ще определят взаимодействието с тази технология през следващите години. От съществено значение ще бъде намирането на балансирани решения, особено по отношение на високорисковите приложения, включително в областта на правоприлагането.

Комисията призовава Европейския парламент и Съвета да приключат спешно междуинституционалните преговори, във всички случаи преди края на мандата на настоящия Европейски парламент, по следните висящи досиета:

- предложение за Регламент относно борбата с онлайн сексуалното насилие над деца;
- предложение за Директива относно борбата с насилието над жени и домашното насилие;
- предложение за Регламент за определяне на хармонизирани правила относно изкуствения интелект (Законодателен акт за изкуствения интелект).

Комисията призовава държавите членки:

- да постигнат незабавно пълно прилагане на инструментариума на ЕС за киберсигурност на 5G технологиите;
- да съдействат на работата на експертната група на високо равнище относно достъпа до данни за ефективно правоприлагане, за да формулира ясни, солидни и изпълними препоръки за справяне по балансиран начин с настоящите и очакваните предизвикателства;
- да предприемат стъпки, в сътрудничество с върховния представител, за гарантиране на ефективното прилагане на инструментариума на ЕС за борба с хибридните заплахи, преразгледания набор от инструменти за кибердипломация и набора от инструменти за FIMI, включително чрез редовни учения и отчитане на глобалната динамика;
- да достигнат до споразумение по отношение на концепцията за екипи за бързо реагиране при хибридни заплахи.

IV. Защита на европейците от тероризма и организираната престъпност

Рискът глобални или местни събития да предизвикат нови огнища на терористична дейност постоянно съществува. Същевременно организираната престъпност и трафикът на наркотици са сред най-сериозните заплахи за сигурността на ЕС. За да се активизират колективните усилия на Съюза в борбата срещу тези заплахи, се работи съвместно по

[26] Вж. например доклада на Европол, публикуван на 17 април 2023 г.: ChatGPT — the impact of Large Language Models on Law Enforcement. (ChatGPT — въздействието, което големите езикови модели (LLM) оказват върху правоприлагането).

изпълнението на стратегията на ЕС за борба с организираната престъпност[27], стратегията на ЕС за борба с трафика на хора[28], програмата и плана за действие на ЕС относно наркотиците[29] и програмата на ЕС за борба с тероризма[30]. Въпреки това, за да се отговори на тревожно влошаващата се ситуация по отношение на организираната престъпност и трафика на наркотици, е необходимо допълнително засилване на работата от страна на държавите членки и на ЕС, за да се утвърди колективният отговор срещу престъпните мрежи и да се осигури по-добра защита на жертвите на престъпления; едновременно с настоящия доклад се публикува и пътна карта на ЕС за борба с трафика на наркотици и организираната престъпност[31].

В областта на борбата с тероризма ЕС укрепва и външния си инструментариум[32], като използва пълноценно диалозите за борба с тероризма на високо равнище и мрежата от експерти в областта на борбата с тероризма/сигурността в делегациите на ЕС, както и, когато е уместно, чрез участието си в многостранни форуми, включително като заема ролята на съпредседател на Глобалния форум за борба с тероризма (GCTF).

Трафик на наркотици

С новия мандат на Агенцията на Европейския съюз по наркотиците (EUDA), който ще се прилага от юли 2024 г., ЕС ще бъде по-добре подготвен за предприемане на действия за справяне със сложен проблем в областта на сигурността и здравеопазването, засягащ милиони хора в ЕС и по света. Комисията също така преразглежда[33] регламентите относно прекурсорите на наркотични вещества[34], за да отговори на основните предизвикателства, установени в оценката от 2020 г.[35], в която се подчертава необходимостта от справяне с предизвикателствата, породени от дизайнерските прекурсори[36], за да се намали предлагането на незаконни наркотици.

Въпреки това, в условията на безпрецедентно нарастване на предлаганите в Европа незаконни наркотици, борбата с трафика на наркотици трябва да се засили в сътрудничество с международните партньори. Необходими са допълнителни действия от страна на държавите членки и на ЕС за разбиване на престъпните мрежи и по-добра защита на жертвите на престъпления. Днес Комисията представя пътна карта на ЕС за борба с трафика на наркотици и организираната престъпност. В нея са заложени 17 действия в четири приоритетни области: укрепване на устойчивостта на логистичните центрове с Европейски пристанищен алианс, разбиване на престъпни мрежи, засилване на усилията за превенция и засилване на сътрудничеството с международни партньори. Тези действия трябва да бъдат изпълнени през 2024 г. и 2025 г.

---

27 COM(2021) 170.
28 COM(2021) 171.
29 COM(2020) 606.
30 COM(2020) 795.
31 COM(2023) 641.
32 Както се призовава в Стратегическия компас и в заключенията на Съвета относно „Справяне с външното измерение на постоянно изменящата се заплаха от тероризъм и насилствен екстремизъм с акцент върху външното измерение“, приети през юни 2022 г.
33 Прекурсори на наркотични вещества — законодателство на ЕС (преразглеждане на правилата) (europa.eu).
34 Регламент (ЕО) № 273/2004 относно прекурсорите на наркотични вещества и Регламент (ЕО) 111/2005 на Съвета за определяне на правила за мониторинг на търговията между Общността и трети страни в областта на прекурсорите.
35 COM(2020) 768.
36 Действие 23 от Плана за действие на ЕС относно наркотиците, COM(2020) 606.

Огнестрелни оръжия

Трафикът на огнестрелни оръжия подхранва организираната престъпност в ЕС, както и в съседните му страни. 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 бързите доставки на колетни пратки и на нови технологии като триизмерния печат трафикът на огнестрелни оръжия приема нови форми, за да се изплъзне от проверките. Агресивната война на Русия срещу Украйна също увеличи риска от широко разпространение на огнестрелни оръжия. През октомври 2022 г. Комисията прие предложение за актуализиране на съществуващото законодателство относно вноса, износа и транзита на огнестрелни оръжия за граждански цели, за да се отстранят пропуските в съществуващите правила, които могат да увеличат броя на огнестрелните оръжия, внасяни контрабандно и пренасочвани в ЕС[37]. В средносрочен план тези нови правила ще спомогнат да се намали рискът от заобикаляне на евентуално ембарго в случай на износ на огнестрелни оръжия за граждански цели и да се увеличи контролът върху вноса на този вид огнестрелни оръжия от държави извън ЕС. Двамата съзаконодатели все още трябва да приемат позициите си по това досие с цел да се постигне споразумение по него преди изтичането на мандата на Парламента.

Трафик на хора

Трафикът на хора представлява особено тежка форма на организирана престъпност и опасно нарушение на основните права. Жертвите са обект на трафик в рамките на ЕС, главно с цел сексуална експлоатация и експлоатация на труда, но също така и с цел принудителна просия и престъпност, както и други форми. През декември 2022 г. Комисията предложи да внесе изменения по Директивата за борба с трафика на хора[38], с които да актуализира правилата, за да се отстранят недостатъците в действащата правна рамка. По-специално, след като бъде приета изменената директива, към приложното ѝ поле ще бъдат добавени принудителният брак и незаконното осиновяване и ще бъде въведено изрично позоваване на онлайн измерението на трафика на хора. Тя ще включва също така задължителен режим на санкции за извършителите и ще официализира създаването на Национален механизъм за насочване и подпомагане на жертви на трафик, за да се подобрят ранното идентифициране и трансграничното насочване за помощ и подкрепа на жертвите. Съзнателното използване на услуги, предоставяни от жертви на трафик, ще се счита за престъпление, а ежегодното събиране на данни за трафика на хора, които ще се публикуват от Евростат, ще стане задължително. Съветът прие общия си подход през юни 2023 г., а Европейският парламент все още трябва да приеме своята позиция. Необходими са експедитивни действия за постигане на споразумение преди края на настоящия мандат на Парламента.

Престъпления против околната среда

Престъпленията против околната среда се превърнаха в глобална заплаха, чийто темп на нарастване се оценява на 5—7 % всяка година. Значителните печалби, които могат да бъдат генерирани, пропуските в законодателството между държавите членки и ниският риск от разкриване — всичко това привлича организираната престъпност. Според Европол има данни, че приходите от тези дейности се използват за финансиране на тероризъм. През декември 2021 г. Комисията прие предложение за замяна на Директивата от 2008 г. относно защитата на околната среда чрез наказателното право.

[37] COM(2022) 480.
[38] COM(2022) 732.

Предложението е съсредоточено върху прецизиране и актуализиране на определенията на категориите престъпления против околната среда и към определяне на ефективни, възпиращи и пропорционални видове и нива на санкции за физически и юридически лица. Новодефинираните престъпления включват престъпления, свързани с незаконно обезлесяване, нарушения на законодателството на ЕС в областта на химикалите, незаконен добив на повърхностни или подземни води и незаконно рециклиране на кораби. Предложението има за цел да се укрепят осезаемо веригата на правоприлагането и трансграничното сътрудничество между органите на държавите членки и агенциите и органите на ЕС. Европейският парламент и Съветът приеха съответните си позиции по предложението и са в процес на преговори, които те следва да успеят да приключат до края на годината. Преразгледаният план за действие[39] срещу трафика на екземпляри от дивата флора и фауна трябва да се изпълнява, за да се подсилят допълнително превенцията и правоприлагането.

Отнемане и конфискация на активи

Лишаването на престъпниците от незаконните им приходи е от ключово значение за възпирането на организираната престъпност. Ето защо в допълнение към предложението за предоставяне на достъп на правоприлагащите органи до информация за банковите сметки в целия ЕС[40] (за което беше постигнато политическо споразумение през юни 2023 г.) през май 2022 г. Комисията представи предложение за отнемане и конфискация на активи[41] с цел укрепване на възможностите за проследяване, установяване, обезпечаване, конфискация и управление на активи. Основните разпоредби, присъстващи в предложението, засягат изискванията за финансовите разследвания и допълнителните правомощия и инструменти на службите за отнемане на активи, както и по-ефективните мерки за обезпечаване и конфискация за разширен кръг от престъпления. Едно от новите престъпления, за които ще се прилагат тези мерки, е нарушаването на ограничителните мерки на Съюза. През декември 2022 г. Комисията прие отделно предложение за хармонизиране на наказателноправните определения и санкциите за нарушаване на ограничителните мерки на Съюза. Ефективното въвеждане и прилагане на ограничителните мерки на Съюза остава водещ приоритет за Комисията, подпомогнат от работата на работната група „Обезпечаване и изземване“, създадена от Комисията в отговор на агресивната война на Русия срещу Украйна. И по двете предложения Европейският парламент и Съветът приеха своите позиции с цел постигане на споразумение до края на тази година.

Пакет относно мерките за борба с изпирането на пари

Изпирането на пари е свързано с почти всички престъпни дейности, генериращи незаконно придобити приходи в ЕС[42], и следователно е ключов инструмент за борба с престъпността в ЕС. През юли 2021 г. Комисията представи амбициозни предложения за укрепване на мерките на ЕС за предотвратяване на изпирането на пари и финансирането на тероризма[43] с четири законодателни предложения за засилване на предотвратяването и разкриването на опитите на престъпниците да изпират незаконни приходи или да финансират терористични дейности чрез финансовата система. Една от четирите

[39] COM(2022) 581.
[40] COM(2021) 429.
[41] COM(2022) 245.
[42] Европол, Предприемчиви престъпници — Борбата на Европа с глобалните мрежи от финансови и икономически престъпления, 2020 г.
[43] COM(2021) 420.

инициативи в пакета — за осигуряване на проследяемост на прехвърлянето на криптоактиви, беше приета от съзаконодателите през май 2023 г.[44]. Този регламент ще започне да се прилага на 30 декември 2024 г., като до тази дата всички доставчици на услуги за криптоактиви ще трябва да събират и съхраняват информация за наредителя и получателя на прехвърлянето на криптоактиви. Останалите три предложения са насочени към i) създаване на нов орган на ЕС за борба с изпирането на пари и финансирането на тероризма (ОБИП), който да осигури последователен висококачествен надзор на целия вътрешен пазар, включително на най-рисковите трансгранични субекти, като подпомага и координира работата на звената за финансово разузнаване, ii) определяне на хармонизирани правила за частния сектор, включително въвеждане на общоевропейски таван от 10 000 EUR за големи плащания в брой в замяна на услуги и стоки, и iii) укрепване на правомощията и инструментите за сътрудничество на компетентните органи. Очаква се този пакет значително да подобри способността на ЕС да се бори с изпирането на пари и да защитава гражданите на ЕС от тероризъм и организирана престъпност. По трите оставащи предложения в момента се водят преговори от съзаконодателите с цел постигане на споразумение по това досие преди края на мандата на настоящия Парламент.

Комисията призовава Европейския парламент и Съвета да приключат спешно междуинституционалните преговори, във всички случаи преди края на мандата на настоящия Европейски парламент, по следните висящи досиета:

- предложение за Директива относно отнемането и конфискацията на активи;
- предложение за Директива за хармонизиране на наказателноправните определения и санкциите за нарушаване на ограничителните мерки на Съюза;
- предложение за Директива за борба с трафика на хора;
- предложение за Директива за подобряване на защитата на околната среда чрез наказателното право;
- предложение за пакет относно мерките за борба с изпирането на пари;
- предложение за актуализиране на съществуващото законодателство относно вноса, износа и транзита на огнестрелни оръжия за граждански цели.

Комисията призовава държавите членки и агенциите и органите на ЕС:

- да работят заедно за изпълнението на 17-те действия от пътната карта на ЕС за борба с трафика на наркотици и организираната престъпност през 2023 г. и 2024 г.

V. Силна европейска екосистема за сигурност

През последните години заплахите за сигурността придобиват все по-трансграничен характер, което изисква допълнителни полезни взаимодействие и по-тясно сътрудничество на всички равнища. След приемането на Стратегията на ЕС за Съюза на сигурност бяха предприети важни инициативи за максимално засилване на трансграничното сътрудничество, рационализиране и осъвременяване на наличните инструменти и процедури както по външните граници, така и в рамките на Шенгенското пространство, както и за подобряване на обмена на информация между

[44] Регламент (ЕС) 2023/1113 от 31 май 2023 г. относно информацията, придружаваща преводите на средства и прехвърлянията на определени криптоактиви, и за изменение на Директива (ЕС) 2015/849.

правоприлагащите и съдебните органи с цел по-успешна борба с организираната престъпност. В този контекст ефективното прилагане на рамката за оперативна съвместимост за обмен на данни е важен стълб за повишаване на сигурността и за ефективен европейски отговор на трансграничните заплахи, като същевременно се гарантира вътрешното свободно движение.

Засилен обмен на информация в рамките на Шенгенското пространство: предварителна информация за пътниците (ПИП), резервационни данни на пътниците (РДП) и Прюм II

Двете предложения относно ПИП, приети от Комисията през декември 2022 г.[45], ще засилят вътрешната сигурност на Съюза, като предоставят на правоприлагащите органи на държавите членки допълнителни инструменти за борба с тежката престъпност и тероризма. По-специално, предварителната информация за пътниците при полети в рамките на ЕС, използвана заедно с резервационните данни на пътниците във въздушния транспорт, би позволила на правоприлагащите органи на държавите членки значително да повишат ефективността на своите разследвания чрез по-целенасочени интервенции. Важно е предложените правила да бъдат приети възможно най-скоро: това не само ще бъде в подкрепа на борбата с организираната престъпност и тероризма, но и ще намали значително необходимостта от системни проверки на всички пътници в случай на временно повторно въвеждане на граничните проверки по вътрешните граници, като улесни пътуването със самолет и свободното движение на хора. На 6 септември 2023 г. Европейската комисия препоръча на Съвета да разреши провеждането на преговори с Швейцария, Исландия и Норвегия за споразумения относно предаването на сведения относно резервационните данни на пътниците. Приемането на тези три препоръки ще подпомогне последователната и ефективна външна политика на ЕС в областта на резервационните данни на пътниците.

Обменът съгласно рамката от Прюм се използва ежедневно от полицията в борбата с организираната престъпност, наркотиците, тероризма, сексуалната експлоатация и трафика на хора. С предложението за регламент относно за автоматизирания обмен на данни за целите на полицейското сътрудничество („Прюм II“)[46] се преразглежда съществуващата рамка от Прюм с оглед преодоляване на пропуските в информацията и засилване на превенцията, разкриването и разследването на престъпления в ЕС. Преразгледаните правила за автоматизиран обмен на данни за целите на полицейското сътрудничество допълват предложенията за полицейско сътрудничество в този мандат, наред с вече приетата препоръка на Съвета за засилване на оперативното трансгранично сътрудничество и директивата за обмен на информация между правоприлагащите органи. Бързото приемане и привеждане в изпълнение на тези свързани инструменти би подобрило, улеснило и ускорило обмена на данни между правоприлагащите органи и би спомогнало за идентифицирането на престъпниците.

Напълно оперативно съвместима система за управление на границите за сигурно, силно, цифрово и единно Шенгенско пространство

В основите на добре функциониращото Шенгенско пространство без вътрешни граници стои взаимното доверие между държавите членки. Това от своя страна зависи от

[45] COM(2022) 729, COM(2022) 73.
[46] COM(2021) 784.

ефикасния контрол, както по външните граници на Съюза, така и като алтернативни мерки на територията на държавите членки. В предложеното от Комисията изменение на Кодекса на шенгенските граници[47] се посочва по какъв начин държавите членки могат да използват по-добре алтернативите на контрола по вътрешните граници, които могат да осигурят високо равнище на сигурност. Важно е изменението на Кодекса на шенгенските граници да бъде прието и приложено изцяло, за да се осигури високо и пропорционално равнище на сигурност в Шенгенското пространство. Продължава и разработването на новата архитектура на информационните системи на ЕС, за да се предостави по-добра подкрепа на работата на националните органи за гарантиране на сигурността и управлението на границите. Това включва обновената Шенгенска информационна система, Европейска система за информация за пътуванията и разрешаването им, Системата за влизане/излизане, актуализираната Визова информационна система и рамката за оперативна съвместимост за свързване на системите заедно в условия на пълна сигурност. След като бъде напълно завършена, тази нова архитектура ще предоставя на националните органи по-изчерпателна и надеждна информация във връзка със сигурността. Всички компоненти на рамката за оперативна съвместимост са от съществено значение, което означава, че забавяне в един аспект или в една държава членка води до забавяне на внедряването за всички. Забавянията в техническото разработване на Системата за влизане/излизане (СВИ) следва да бъдат сведени до минимум, за да може СВИ да започне да функционира възможно най-скоро и да бъдат въведени всички ключови елементи на рамката за оперативна съвместимост.

Предложението за скрининг[48] ще повиши сигурността в Шенгенското пространство чрез създаване на единни правила за идентифициране на граждани на трети държави, които не отговарят на условията за влизане, посочени в Кодекса на шенгенските граници, и подлагането им на проверки за здравословно състояние и сигурност на външните граници. Предложената система „Евродак“ ще подпомогне постигането на тези цели, като показва случаите, когато след скрининга бъде установено, че дадено лице би могло да представлява заплаха за вътрешната сигурност. Това от своя страна ще улесни прилагането на предложения Регламент относно убежището и управлението на миграцията. Комисията насърчава съзаконодателите да приключат бързо преговорите по тези досиета преди края на настоящия законодателен период.

Борба с корупцията

Корупцията нанася значителни вреди на нашите демокрации, на икономиката и на нашата сигурност, тъй като е стимул за организираната престъпност и за враждебната външна намеса. Успешното предотвратяване на корупцията и борбата с нея са от съществено значение както за защитата на ценностите на ЕС, така и за ефективността на неговите политики, а така също и за поддържането на върховенството на закона и на доверието в управляващите и в публичните институции. Спазвайки обявеното от председателя фон дер Лайен в речта ѝ за състоянието на Съюза през 2022 г., на 3 май 2023 г. Комисията прие пакет от мерки за борба с корупцията[49]**.** Предложението на Комисията за директива за борба с корупцията включва по-строги правила за криминализиране на престъпленията, свързани с корупция, и за хармонизиране на наказанията в целия ЕС. То също така предоставя възможност за провеждане ефективни разследвания и съдебни преследвания и поставя силен акцент върху превенцията и създаването на култура на почтеност, в която корупцията не се толерира. Дискусиите по

[47] COM(2021) 891.
[48] COM(2020) 612.
[49] COM(2023) 234.

това предложение започнаха в Европейския парламент и в Съвета. Освен това държавите членки се призовават да привеждат в действие препоръките, произтичащи от стълба за борба с корупцията в доклада за върховенството на закона от 2023 г., приет на 5 юли 2023 г. Също така в предложение на върховния представител, подкрепено от Комисията, се предлага установяването на специален режим на санкции по линия на общата външна политика и политика на сигурност (ОВППС), който ще е насочен срещу сериозни корупционни деяния по целия свят.

Укрепване на правата на жертвите

На 12 юли 2023 г. Комисията предложи изменения на Директивата за правата на жертвите, за да се подобри достъпът на жертвите до информация, подкрепа и защита, участие в наказателното производство и достъп до обезщетение. Една от общите цели на преразглеждането е да допринесе за високо равнище на сигурност чрез създаване на по-сигурна среда за жертвите, за да се насърчи съобщаването на престъпления, като се намалят страховете от репресии.

Комисията призовава Европейския парламент и Съвета да приключат спешно междуинституционалните преговори, във всички случаи преди края на мандата на настоящия Европейски парламент, по следните висящи досиета:

- предложение относно Регламента Прюм II;
- предложения относно предварителната информация за пътниците (ПИП);
- предложения относно борбата с корупцията и по-специално за създаване на специално предназначен режим на санкции в рамките на общата външна политика и политика на сигурност (ОВППС);
- предложение за изменение на Регламента относно Кодекса на шенгенските граници;
- предложение за Директива за правата на жертвите;
- предложение относно скрининга.

Комисията призовава държавите членки:

- да осигурят влизането в сила на системата за влизане/излизане във възможно най-кратък срок, за да завърши прилагането на архитектурата на ЕС за обмен на информация.

VI. Изпълнение

Гарантирането на сигурността на Европа като цяло е споделена отговорност, в която всеки участник трябва да изиграе своята роля — от приемането от страна на Комисията и съзаконодателите на нови, солидни, изчерпателни и практически приложими правила, до своевременното транспониране, привеждане в действие и прилагане на тези правила от държавите членки и оперативната работа, извършвана на място от различни органи, организации и заинтересовани страни. Агенциите на ЕС в областта на правосъдието, вътрешните работи и киберсигурността също играят решаваща роля, която се увеличи благодарение на неотдавнашното разширяване на техните отговорности.

Засилена проверка на бенефициерите на финансиране от ЕС

При изпълнението на бюджета на ЕС Комисията носи отговорност да гарантира, че бенефициерите на финансиране от ЕС зачитат ценностите на ЕС. Механизмите и системите за контрол, с които се определя кой може да се възползва от финансиране

от ЕС, вече са стабилни, а текущите преговори за преработване на Финансовия регламент имат за цел да предоставят на Комисията по-силни правни средства за действие, когато е необходимо. Освен това в момента Комисията работи по начини за по-нататъшно подобряване на проверката на настоящите и потенциалните бъдещи бенефициери на финансиране от ЕС чрез подобряване на насоките относно задълженията, свързани със зачитането на ценностите на ЕС, и последиците, които следва да настъпват при нарушаване на тези ценности. Това ще внесе яснота относно отговорностите както на бенефициерите, така и на лицата, извършващи контрол на равнището на ЕС, и може да послужи като източник на вдъхновение за националното равнище. В случай на нарушение на условията за финансиране Комисията не се колебае и няма да се поколебае да прекрати сътрудничеството с бенефициерите на съответния проект и при необходимост да събере отпуснатите средства. Важно е държавите членки по собствена инициатива да споделят информация с Комисията, когато са наясно с възможни рискове, свързани с организации, кандидатстващи за финансиране от ЕС.

Нарушения

В областта на сигурността Комисията е провела множество производства за установяване на нарушение. Например през 2023 г. са образувани голям брой дела за нарушения поради неизпълнение на задълженията по Регламента от 2021 г. относно разпространението на терористично съдържание онлайн (16 държави членки)[50], а през 2022 г. и 2023 г. 20 държави членки са получили допълнителни официални уведомителни писма поради неправилно прилагане на Директивата от 2011 г. относно борбата със сексуалното насилие над деца[51]. Все още не са приключени значителен брой дела за нарушения за несъответствие на националното законодателство с Директивата от 2017 г. относно борбата с тероризма[52] и поради нетранспониране на правилата, с които се улеснява използването на финансова и друга информация за предотвратяването, разкриването, разследването или наказателното преследване на определени престъпления[53]. Други области, в които се водят производства за установяване нарушения, включват законодателството за огнестрелните оръжия; правилата относно психоактивните вещества, използвани в производството на лекарства, борбата с измамите и фалшифицирането на непарични платежни средства, борбата с изпирането на пари, обмена на данни за съдимост между държавите — членки на ЕС, и Директивата за правата на жертвите. На държавите членки, които изпълняват договорените инициативи и действия, е предоставена подкрепа (техническа и финансова), а Комисията остава на разположение за сътрудничество с държавите членки с цел оптимизиране на изпълнението.

Наблюдение чрез оценките по Шенген и новата система за управление

Механизмът за оценка и наблюдение по Шенген продължи да допринася за ефективното прилагане на шенгенските правила, насочени към повишаване на сигурността в зоната

---

[50] Регламент (ЕС) 2021/784 относно справянето с разпространението на терористично съдържание онлайн.

[51] Директива (ЕС) 2011/93 относно борбата със сексуалното насилие над деца.

[52] Директива (ЕС) 2017/541 на Европейския парламент и на Съвета от 15 март 2017 г. относно борбата с тероризма и за замяна на Рамково решение 2002/475/ПВР на Съвета, и за изменение на Решение 2005/671/ПВР на Съвета.

[53] Директива (ЕС) 2019/1153 на Европейския парламент и на Съвета от 20 юни 2019 г. за установяване на правила, с които се улеснява използването на финансова и друга информация за предотвратяването, разкриването, разследването или наказателното преследване на определени престъпления, и за отмяна на Решение 2000/642/ПВР на Съвета.

без вътрешен контрол. През 2023 г. бяха извършени първите оценки в рамките на укрепения механизъм за оценка и наблюдение по Шенген, което позволи своевременно идентифициране и отстраняване на стратегически слабости с трансгранично въздействие върху сигурността и безопасността в рамките на ЕС. Освен това през 2023 г. Комисията започна тематична оценка по Шенген, за да оцени практиките на държавите членки, които са изправени пред сходни предизвикателства в борбата с трафика на наркотици в ЕС, като се съсредоточи по-специално върху трафика на наркотици в големи количества. Тези оценки поставиха засилен и по-всеобхватен акцент върху елементите на сигурността в Шенген. Въз основа на резултатите от периодичните, тематичните и необявените шенгенски оценки през юни 2023 г. Съветът определи приоритетите на шенгенския цикъл за периода 2023—2024 г. В него се посочват целевите области, в които е необходим допълнителен тласък за постигане на по-сигурно и укрепено Шенгенско пространство. Ефективното и бързо изпълнение на тези приоритети, заедно със засилената координация на политиките на Шенгенския съвет, ще засили допълнително борбата с организираната престъпност и ще увеличи максимално трансграничното оперативно сътрудничество.

Ролята на агенциите и органите на ЕС

Партньорството е от ключово значение за изпълнението на инициативите по линия на Съюза на сигурност, тъй като за постигането на конкретни резултати е необходима работата на различни национални и европейски органи и структури. Например EMPACT (Европейска мултидисциплинарна платформа за борба с криминални заплахи) дава възможност за структурирано мултидисциплинарно сътрудничество между държавите членки, подкрепено от всички институции, органи и агенции на ЕС (като Европол, Frontex, Евроюст, CEPOL, OLAF, EU-LISA). При операциите, извършвани от EMPACT, включително чрез специализирани оперативни работни групи (ОРГ), се координират усилията на държавите членки и оперативните партньори в борбата с престъпните мрежи и тежките престъпления. Само през 2022 г. в резултат на дейността на EMPACT са извършени общо 9922 ареста, иззети са активи и парични средства на стойност над 180 милиона евро, започнати са 9263 разследвания, установени са 4019 жертви, иззети са над 62 тона наркотици, идентифицирани са 51 обекти от особен интерес (ООИ) и 12 от тях са арестувани, като операциите са в контекста на агресивната война срещу Украйна, по-специално за справяне с трафика на хора и заплахите, свързани с огнестрелни оръжия.[54]

Frontex, Европейската агенция по морска безопасност (ЕАМБ) и Европейската агенция за контрол на рибарството (EFCA) продължават да укрепват сътрудничеството си в областта на функциите на бреговата охрана, за да подпомагат националните органи в повишаването на безопасността и сигурността в морето. Тези агенции ще имат основен принос за изпълнението на Стратегията на ЕС за морска сигурност.

Няколко от инициативите по линия на Съюза на сигурност доведоха до нови отговорности и задачи за съответните агенции, понякога с отражение върху човешките ресурси.

[54] Справки за резултатите от EMPACT за 2022 г.: https://www.consilium.europa.eu/media/65450/2023_225_empact-factsheets-2022_web-final.pdf

Агенция на Европейския съюз за киберсигурност (ENISA)

По отношение на готовността и реагирането при инциденти, за да се повиши киберсигурността, Комисията създаде краткосрочно действие за подпомагане на държавите членки, като прехвърли финансиране от програма „Цифрова Европа“ към **Агенцията на Европейския съюз за киберсигурност (ENISA)** с цел укрепване на готовността и способността за реагиране при големи киберинциденти. Предложението за законодателен акт за киберсолидарност, прието през април 2023 г., се основава на това действие и след като бъде прието от съзаконодателите, с него на ENISA може да бъдат възложени допълнителни задачи, като например функционирането и управлението на бъдещия киберрезерв на ЕС или изготвянето на доклад от преглед след инцидент след мащабни киберинциденти. В предложението за европейски законодателен акт за киберустойчивост на ENISA ще бъде възложена задачата да получава уведомления от производителите за уязвимости, съдържащи се в продукти с цифрови елементи, както и за инциденти, които оказват въздействие върху сигурността на тези продукти, които ENISA ще трябва да препраща до съответните екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) или до съответните единни звена за контакт на държавите членки. От ENISA се очаква също да изготвя двугодишен технически доклад за нововъзникващите тенденции по отношение на киберрисковете в продуктите с цифрови елементи и да го представя на групата за сътрудничество за МИС.

Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността

Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността (ЕЦЕПОК), заедно с мрежата от национални координационни центрове (НКЦ), представлява новият орган на Съюза за подкрепяне на иновациите и промишлената политика в областта на киберсигурността. Тази екосистема ще укрепи капацитета на технологичната общност в сферата на киберсигурността, ще поддържа високи постижения в областта на научните изследвания и ще засили конкурентоспособността на промишлеността на Съюза в този контекст. ЕЦЕПОК и НКЦ ще вземат стратегически инвестиционни решения и ще обединяват ресурси от Съюза, неговите държави членки и, косвено, от промишлеността за подобряване и укрепване на технологичния и промишления капацитет за киберсигурност. Поради това ЕЦЕПОК ще играе ключова роля в постигането на амбициозните цели в областта на киберсигурността, заложени в програмите „Цифрова Европа“ и „Хоризонт Европа“.

ЕЦЕПОК е назначил повече от половината си персонал и скоро ще наеме изпълнителен директор. Работата, която вече е в ход, включва частта относно киберсигурността на програмата DIGITAL и нова стратегическа програма[55] за разработване и внедряване на технологии, в която са определени приоритетни действия за подкрепа на МСП при разработването и използването на стратегически технологии, услуги и процеси в областта на киберсигурността; за подкрепа и развитие на професионалната работна сила; и за укрепване на експертния опит в сферата на научните изследвания, развойната дейност и иновациите в по-широката европейска екосистема за киберсигурност.

Европол

Със своя изцяло нов мандат **Европол** ще бъде по-добре подготвен да оказва подкрепа на държавите членки в борбата с организираната престъпност. Борбата с трафика на

[55] https://cybersecurity-centre.europa.eu/strategic-agenda_en

наркотици е основен приоритет с оглед на нарастващото му значение и увеличаващото се отрицателно въздействие върху сигурността на гражданите на ЕС. След разрешението от страна на Съвета на Европейския съюз от 15 май 2023 г. Комисията работи активно за сключването на международни споразумения с Боливия, Бразилия, Еквадор, Мексико и Перу за обмен на лични данни с Европол с цел предотвратяване и борба с тежките престъпления и тероризма.

Евроюст

С над 20-годишния си опит в предоставянето на съдебна подкрепа на националните органи в противодействието на широк спектър от тежки и сложни трансгранични престъпления, **Eurojust** затвърди позицията си в пространството на ЕС на свобода, сигурност и правосъдие. За да засили сътрудничеството във всички области, Комисията води преговори за сключване на международни споразумения за улесняване на сътрудничеството между Евроюст и 13 трети държави за обмен на лични данни с цел борба с организираната престъпност и тероризма[56]. Вече са приключени преговорите с Армения и Ливан, продължават да текат преговори с Алжир и Колумбия и са започнати преговори с Босна и Херцеговина. Комисията насърчава Европейския парламент и Съвета да финализират сключването на споразумения с тези държави преди края на парламентарния мандат, за да се засили транснационалното съдебно сътрудничество и да се разшири борбата с трансграничната престъпност.

Европейска прокуратура

От началото на оперативната си дейност през юни 2021 г. **Европейската прокуратура** доказа, че е мощен инструмент в инструментариума на Съюза за разследване и наказателно преследване на престъпления, засягащи бюджета на Съюза, включително престъпления, свързани с участие в престъпна организация, когато фокусът е върху престъпленията срещу бюджета на Съюза. Комисията насърчава държавите членки, които все още не са се включили в засиленото сътрудничество на Европейската прокуратура, да направят това възможно най-скоро, за да се използва пълният потенциал на прокуратурата за защита на парите на данъкоплатците в ЕС.

Агенция на Европейския съюз по наркотиците

С нов мандат, приет от съзаконодателите през юни 2023 г., съществуващият Европейски център за мониторинг на наркотици и наркомании (ЕЦМНН) ще се превърне в пълноправна агенция — **Агенцията на Европейския съюз по наркотиците (EUDA*)***, чиято роля ще бъде засилена. Агенцията ще бъде в състояние да оценява по по-всеобхватен начин новите предизвикателства пред здравето и сигурността, породени от незаконните наркотици, и да допринася по-ефективно към работата на равнището на държавите членки, както и на международно равнище. Събирането, анализът и разпространението на данни ще продължат да бъдат основната задача на агенцията, но разширеният мандат ще ѝ позволи също така да изгради общ капацитет за оценка на заплахите за здравето и сигурността, за да идентифицира нововъзникващи заплахи, включително употребата на много вещества, да засили сътрудничеството си чрез национални координатори и да създаде мрежа от лаборатории, които да предоставят на агенцията съдебномедицинска и токсикологична информация. Това ще помогне на агенцията да предупреждава, когато на пазара се появят особено опасни вещества, и да повишава осведомеността.

[56] Алжир, Аржентина, Армения, Босна и Херцеговина, Бразилия, Египет, Израел, Йордания, Колумбия, Ливан, Мароко, Тунис и Турция.

Комисията призовава Европейския парламент и Съвета да приключат спешно междуинституционалните преговори, във всички случаи преди края на мандата на настоящия Европейски парламент, по следните висящи досиета:

- предложение за преработване на Финансовия регламент.

Комисията призовава държавите членки:

- по собствена инициатива да споделят информация с Комисията, когато са наясно с възможни рискове, свързани с организации, кандидатстващи за финансиране от ЕС;
- бързо да приложат приоритетите на шенгенския цикъл за периода 2023—2024 г. за по-сигурно и по-силно шенгенско пространство;
- да обърнат внимание на откритите срещу тях производства за установяване на нарушение, за да гарантират правилното транспониране на съответното

VII. Заключение

Последните три години бяха белязани от постоянни и решителни усилия за вдъхване на живот на амбицията за създаване на Съюз на сигурност на равнището на ЕС. Постигнат е огромен напредък в целия спектър на политиката в областта на сигурността. В наши дни реалността на постоянно променящите се заплахи изисква непрекъснати усилия с подновена мотивация. Работата по законодателната рамка трябва да приключи своевременно преди края на парламентарния мандат през пролетта на 2024 г. Държавите членки имат постоянни отговорности по отношение на транспонирането, изпълнението и прилагането на новите закони. Изпълнението изисква съгласувани усилия, включително с подкрепата на агенциите на ЕС, а много често и все по-интензивно сътрудничество с нашите международни партньори.

Единствено с колективните и решителни усилия на всички заинтересовани страни ще постигнем равнищата на безопасност и сигурност в ЕС, които гражданите очакват — а при днешните обстоятелства за всеки участник изпълнението на ролята му в укрепването на сигурността на ЕС следва да бъде приоритет.