Съвет на
Европейския съюз

Брюксел, 3 април 2025 г.
(OR. en)

7750/25

JAI 415	**COPEN 79**
COSI 55	**FREMP 76**
ENFOPOL 109	**RELEX 413**
CRIMORG 59	**CFSP/PESC 530**
ENFOCUSTOM 53	**PROCIV 32**
IXIM 73	**CIVCOM 85**
CT 42	**COPS 157**
COTER 48	**IPCR 22**
CORDROGUE 43	**HYBRID 29**
CYBER 87	**DISINFO 20**
MIGR 121	**TELECOM 104**
FRONT 80	**DIGIT 58**
ASIM 28	**MI 197**
VISA 51	**COMPET 226**
SCHENGEN 20	**UD 73**
JAIEX 32	**ENV 237**
CATS 13	**TRANS 114**
DATAPROTECT 59	**CULT 27**
DROIPEN 36	**RECH 138**
EU-LISA	***EUDA***
CH	***FRA***
FRONTEX	***NO***
EUAA	***LI***
EUROJUST	***IS***
EPPO	***CEPOL***
EUROPOL	

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	2 април 2025 г.
До:	Г-жа Thérèse BLANCHET, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	COM(2025) 148 final
Относно:	СЪОБЩЕНИЕ НА КОМИСИЯТА ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, СЪВЕТА, ЕВРОПЕЙСКИЯ ИКОНОМИЧЕСКИ И СОЦИАЛЕН КОМИТЕТ И КОМИТЕТА НА РЕГИОНИТЕ ProtectEU: европейска стратегия за вътрешна сигурност

Приложено се изпраща на делегациите документ COM(2025) 148 final.

Приложение: COM(2025) 148 final

ЕВРОПЕЙСКА
КОМИСИЯ

Страсбург, 1.4.2025 г.
COM(2025) 148 final

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

ProtectEU: европейска стратегия за вътрешна сигурност

1. ProtectEU: европейска стратегия за вътрешна сигурност

Сигурността е основата, върху която се градят всички наши свободи. Демокрацията, върховенството на закона, основните права, благосъстоянието на европейците, конкурентоспособността и просперитетът — всичко това зависи от способността ни да гарантираме основно нашата сигурност. Живеем в нова ера на заплахи за сигурността, в която способността на държавите — членки на ЕС, да гарантират сигурността на своите граждани повече от всякога зависи от **единен европейски подход за защита на вътрешната ни сигурност**. В една променяща се геополитическа обстановка Европа трябва да продължи да спазва неизменното си обещание за мир.

Вече са предприети първите стъпки към изграждането на европейски апарат за сигурност. През последното десетилетие осигурихме на Съюза подобрени колективни механизми за действие в областта на правоприлагането и съдебното сътрудничество, сигурността на границите, борбата с тежката и организираната престъпност, борбата с тероризма и насилническия екстремизъм и защитата на физическата и цифровата критична инфраструктура на ЕС. Правилното прилагане на вече приетото законодателство и разработените политики продължава да бъде от ключово значение.

Естеството на днешните заплахи и неразривната връзка между вътрешната и външната сигурност на ЕС изискват от нас да отидем по-далеч.

Картината на заплахите е ясна, но границите между **хибридните заплахи** и откритата война са размити. Русия води онлайн и офлайн хибридна кампания срещу ЕС и неговите партньори, за да наруши и подкопае социалното сближаване и демократичните процеси и да постави на изпитание солидарността на ЕС с Украйна. Враждебни чужди държави и държавно спонсорирани участници се стремят да проникнат и да навредят на нашата критична инфраструктура и вериги на доставките, да крадат чувствителни данни и да се подготвят за нанасяне на максимална вреда в бъдеще. Те използват престъпността в услуга на своите цели, а престъпниците — като свои марионетки. Също така нашата зависимост от трети държави по отношение на веригите на доставките ни прави по-уязвими към хибридните кампании на враждебни държави.

В Европа се роят мощни **мрежи на организираната престъпност**, развиват се онлайн, проникват в нашата икономика и засягат нашето общество, както бе подчертано в оценката на заплахата от тежка и организирана международна престъпност в ЕС (SOCTA), представена неотдавна от Европол[1]. Веднъж проникнала в общност или икономически сектор, изкореняването на организираната престъпност се превръща в неравна битка: една трета от най-опасните престъпни мрежи са активни в продължение на повече от десет години. Криптовалутите и паралелните финансови системи им помагат при изпирането и укриването на облагите от престъпната им дейност.

Заплахата от тероризъм в Европа остава. Регионалните кризи извън ЕС имат верижен ефект, което предоставя нова мотивация на терористите от целия идеологически спектър да вербуват, мобилизират или надграждат своя капацитет. Усилията им за радикализация и вербуване се насочват по-конкретно към най-уязвимите слоеве на нашите общества, и по-специално към някои млади хора. Те вдъхновяват нападения, извършвани от единствен участник, и рязко нарастване на антисистемния екстремизъм, чиято цел е да се накърни демократичният правен ред.

Стремителното **развитие на технологиите** предоставя основни инструменти за подобряване на нашия апарат за сигурност. Кибератаките и чуждестранното

[1] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

манипулиране на информация обаче стават все по-чести, като се използват нови технологии, като изкуствения интелект. Децата, младежите и хората в третата възраст са особено изложени на риск онлайн, а разпространението на омразата онлайн застрашава свободата на изразяване на мнение и социалното сближаване.

Животът ни е станал по-несигурен и у европейците това чувство е все по-силно. **Усещането им за безопасността и сигурността в ЕС** е подронено до такава степен, че на въпрос относно бъдещето им 64 % изразяват разтревоженост за сигурността на ЕС.[2] Предприятията също показват все по-голяма загриженост; невярната информация и дезинформацията, престъпността и незаконната дейност и кибершпионажът са сред десетте най-големи риска, установени в Доклада за глобалните рискове за 2025 г.[3] на Световния икономически форум.

Европейците трябва да **могат да водят живот без страх**, независимо дали са у дома, на улицата, на обществено място, в метрото, или в интернет. Централен елемент на работата на ЕС в областта на сигурността е защитата на хората, особено на най-уязвимите, от нападения, които обикновено засягат в по-голяма степен децата, жените и малцинствата, включително еврейските и мюсюлманските общности. Това е от съществено значение за изграждането на устойчиви и сплотени общества.

Комисията подготвя **европейска стратегия за вътрешна сигурност** с цел по-добро противодействие на заплахите през идните години. С прецизиран правен инструментариум, по-задълбочено сътрудничество и засилен обмен на информация ще повишим устойчивостта и колективната си способност за ефективно предвиждане, предотвратяване, откриване и реагиране на заплахи за сигурността. С единен подход към вътрешната сигурност държавите членки ще могат да бъдат подпомогнати да използват силата на технологиите за укрепване, а не за отслабване, на сигурността, като същевременно се насърчава сигурно цифрово пространство за всички. Освен това стратегията ще оказва подкрепа за общ отговор от страна на държавите членки на глобалните политически и икономически промени, засягащи вътрешната сигурност на Съюза.

Тази стратегия се ръководи от **три принципа** и в ядрото си включва зачитането на върховенството на закона и основните права.

Първо, в нея е заложена амбицията за промяна на културата в областта на сигурността. Нуждаем се от **подход, обхващащ цялото общество**, в който са съпричастни всички граждани и заинтересовани страни, включително гражданското общество, научноизследователската общност и академични средите, както и частни субекти. Поради това действията в рамките на стратегията се провеждат, когато това е възможно, чрез интегриран подход с участието на множество заинтересовани страни.

Второ, **съображенията за сигурност трябва да бъдат интегрирани и взети предвид във всички законодателни актове, политики и програми на ЕС**, включително външната дейност на ЕС. Законодателството, политиките и програмите ще трябва да бъдат изготвяни, преразглеждани и прилагани с оглед на сигурността, като се гарантира, че се отчитат необходимите съображения за сигурност, и така да се насърчи съгласуван и всеобхватен подход към сигурността.

И накрая, една безопасна, сигурна и устойчива Европа изисква **сериозни инвестиции от страна на ЕС, неговите държави членки и частния сектор**. Приоритетите и

[2] Експресно проучване „Евробарометър“ № FL550: предизвикателства и приоритети на ЕС.
[3] https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf, стр.17.

действията, заложени в тази стратегия, изискват достатъчно човешки и финансови ресурси, за да се гарантира тяхното изпълнение. Както се посочва в съобщението относно пътя към следващата многогодишна финансова рамка[4], Европа ще трябва да увеличи публичните разходи за сигурност и да насърчи научните изследвания и инвестициите в областта на сигурността, като повиши стратегическата си автономност.

Настоящата стратегия допълва **европейската стратегия за Съюз на подготвеност**[5], в която се определя интегриран, обхващаш всички опасности, подход към подготвеността за конфликти, причинени от човека бедствени ситуации, природни бедствия и кризи, и **Бялата книга за европейската отбранителна готовност до 2030 г.**[6], в която се подкрепят развитието и придобиването на отбранителни способности в целия ЕС с цел възпиране на чуждестранни противници. Комисията също така ще предложи **европейски щит за демокрацията** с цел укрепване на демократичната устойчивост в ЕС. Заедно тези инициативи очертават визия за безопасен, сигурен и устойчив ЕС.

Ново европейско управление на вътрешната сигурност

Комисията ще работи в тясно сътрудничество с държавите членки и агенциите на ЕС за подобряване на подхода на ЕС към вътрешната сигурност както на стратегическо, така и на оперативно равнище.

Това ще се постигне чрез:

- **последователно определяне на възможните последици за сигурността и подготвеността от новите и преразгледаните инициативи на Комисията от самото начало и по време на целия процес на договаряне на инициативите и политиките;**
- **редовни заседания на проектната група на Комисията по въпросите на европейската вътрешна сигурност, подкрепени от стратегическо междусекторно сътрудничество в рамките на Комисията;**
- **представяне на анализите на заплахите, свързани с вътрешната сигурност, в подкрепа на работата на колегиума по сигурността;**
- **обсъждания с държавите членки в Съвета на променящите се предизвикателства пред вътрешната сигурност въз основа на анализа на заплахите и обмена на мнения по ключови приоритети на политиката;**
- **редовно докладване пред Европейския парламент и Съвета с цел проследяване и подпомагане на систематичното изпълнение на ключови инициативи в областта на сигурността.**

2. Интегрирана ситуационна осведоменост и анализ на заплахите

Ще осигурим на ЕС нови начини за обмен и съчетаване на информацията и ще предоставяме редовен анализ на заплахите за вътрешната сигурност на ЕС, което ще допринесе за цялостна оценка на рисковете и заплахите.

Сигурността започва с **ефективно предвиждане**. ЕС трябва да разчита на ситуационна осведоменост и анализ на заплахите, които са всеобхватни, достатъчно автономни и

[4] COM (2025) 46 final.
[5] JOIN (2025) 130 final.
[6] JOIN (2025) 120 final.

актуални. Оперативната информация, която държавите членки се насърчават да подобряват допълнително чрез единното звено за анализ на разузнавателна информация като единна входна точка за разузнавателна информация на държавите членки, е от жизненоважно значение за оценката и противодействието на заплахите, като в крайна сметка служи за основа на политическите и законодателните действия[7]. На равнището на ЕС трябва да използваме по по-ефективен и съгласуван начин **основания на разузнавателни данни анализ** и **оценките на заплахите**.

Въз основа на различните оценки на рисковете и заплахите, изготвени на равнището на ЕС и за конкретни сектори[8], Комисията ще изготвя **редовни анализи на заплахите за вътрешната сигурност на ЕС**, за да открои основните предизвикателства пред сигурността и да предостави информация за определянето на приоритетите на политиката. Анализите ще спомогнат за разработването на гъвкава и адаптивна политика за вътрешна сигурност, която ефективно се справя с променящите се заплахи, защитава по-добре хората и предприятията от нападения и дава възможност за своевременна целенасочена политическа намеса. Анализите на заплахите за вътрешната сигурност на ЕС ще допринесат и за **цялостна (междусекторна и на всички опасности) оценка на ЕС на рисковете и заплахите**, разработена от Комисията и върховния представител, както е посочено в европейската стратегия за Съюз на подготвеност.

Доверието и безопасното боравене са от съществено значение за обмена на информация и това изисква надеждна и сигурна инфраструктура. Институциите, органите, службите и агенциите на ЕС трябва да гарантират способността си да използват **сигурни канали за комуникация** за обмен на чувствителна и класифицирана информация помежду си и с държавите членки. Инвестициите в **оперативно съвместими сигурни системи** и надеждни технологии ще укрепят автономността на ЕС и ще подобрят способността му да управлява кризи и да гарантира оперативна устойчивост. В този контекст Комисията настоятелно призовава съзаконодателите да приключат преговорите по **предложения регламент относно информационната сигурност в институциите, органите, службите и агенциите на Съюза**, по-специално да осигурят обща рамка за боравене с чувствителна некласифицирана и класифицирана информация[9].

За да гарантира собствената си оперативна сигурност и ситуационна осведоменост, Комисията ще преразгледа своята рамка за корпоративно управление на сигурността и ще създаде **Интегриран център за операции по сигурността (ISOC)**, който да защитава хората, физическите активи и операциите във всички обекти на Комисията. Комисията също така ще увеличи своите оперативни и аналитични възможности за идентифициране и смекчаване на хибридните заплахи.

В съответствие с европейската стратегия за Съюз на подготвеност съображенията за подготвеност и сигурност ще бъдат интегрирани и взети предвид в законодателството, политиките и програмите на ЕС. При изготвянето или преразглеждането на политики, програми или законодателство, като се отчитат съображения за подготвеността и сигурността, Комисията неизменно ще набелязва потенциалните въздействия на

[7] Safer Together — Strengthening Europe's Civilian and Military Preparedness and Readines („Заедно в по-голяма безопасност – укрепване на гражданската и военната готовност и подготвеност на Европа“), стр. 23

[8] Секторните оценки на заплахите, които ще допринесат за оформянето на анализа на заплахите, включват оценката на заплахата от тежка и организирана международна престъпност в ЕС (SOCTA), доклада за ситуацията и тенденциите при тероризма (TE-SAT), съвместния доклад за оценка на киберсигурността (JCAR) и бъдещите оценки на заплахите, рисковете и методите при изпирането на пари и финансирането на тероризма, които ще бъдат извършени от Комисията и Органа за борба с изпирането на пари.

[9] COM(2022) 119 final.

предпочитания вариант на политиката върху подготвеността и сигурността. Това ще бъде подкрепено с редовни обучения за лицата, които създават политиките, в Комисията.

За да подпомага държавите членки, Комисията ще обсъжда със Съвета променящите се предизвикателства пред вътрешната сигурност и ключовите приоритети на политиката и редовно ще го информира за изпълнението на стратегията. Освен това Комисията ще държи Европейския парламент и съответните заинтересовани страни информирани и съпричастни по отношение на всички свързани със стратегията действия.

Ключови действия

Комисията:

- **ще разработва и представя редовни анализи на заплахите във връзка с предизвикателствата пред вътрешната сигурност на ЕС.**

Държавите членки се приканват:

- **да подобряват обмена на разузнавателна информация с единната входна точка за разузнавателна информация и да осигурят по-добър обмен на информация с агенциите и органите на ЕС.**

Европейският парламент и Съветът се приканват:

- **да приключат преговорите по предложения регламент относно информационната сигурност в институциите, органите, службите и агенциите на Съюза.**

3. Укрепване на способностите на ЕС в областта на сигурността

Ще разработим нови инструменти за правоприлагане, като например обновен мандат на Европол, и по-добри средства за координиране и гарантиране на сигурен обмен на данни и законен достъп до данни.

За да противодейства ефективно на променящите се заплахи, ЕС трябва да подобрява способностите си в областта на сигурността и да насърчава иновациите. Като основни органи, действащи срещу заплахите за вътрешната сигурност, правоприлагащите и съдебните органи се нуждаят от подходящи оперативни инструменти и способности, за да действат бързо и ефективно. Важно е тези органи да могат да осъществяват комуникация и координация отвъд националните граници и между отделните служби с цел ефективно предотвратяване, разкриване, разследване и наказателно преследване.

Агенции и органи на ЕС в областта на вътрешната сигурност

Агенциите и органите на ЕС в областта на правосъдието, вътрешните работи и киберсигурността играят ключова роля в архитектурата за сигурност на ЕС — роля, която продължава да нараства с разширяването на техните отговорности.

Днес, 25 години след създаването си, **Европол** заема повече от всякога централно място в рамката за сигурност на ЕС. Агенцията подпомага сложни трансгранични разследвания, улеснява обмена на информация, разработва иновативни инструменти за полицейска дейност и предоставя експертен опит на правоприлагащите органи. Няколко фактора обаче пречат на Европол да разгърне напълно оперативния си потенциал при подкрепата на дейностите по разследване и оперативните дейности за борба с трансграничната престъпност: те варират от недостатъчното равнище на ресурсите до факта, че настоящият мандат на агенцията не обхваща нови заплахи за сигурността, като саботаж, хибридни заплахи или манипулиране на информация. Ето защо Комисията ще

предложи **амбициозна реформа на мандата на Европол**, за да го превърне в наистина оперативна полицейска агенция, която да оказва по-добра подкрепа на държавите членки. Целта е да се укрепят технологичният експертен опит и капацитетът на Европол за подпомагане на националните правоприлагащи служби, подобряване на координацията с други агенции и органи и с държавите членки, усилване на стратегическите партньорства с държавите партньори и частния сектор и гарантиране на засилен надзор над Европол.

Освен това Комисията ще работи за по-нататъшно **подобряване на ефективността и взаимното допълване на агенциите и органите на ЕС в областта на вътрешната сигурност и укрепване на гладкото сътрудничество** между тях.

Мандатът на **Евроюст** ще бъде оценен и укрепен с цел по-ефективно съдебно сътрудничество при засилване на взаимното допълване и сътрудничеството с Европол. Това включва повишаване на ефективността на Евроюст, както и на капацитета на агенцията да предоставя проактивна подкрепа и анализ на съдебните органи на държавите членки. Освен това, като се има предвид уникалната компетентност на **Европейската прокуратура** да разследва и преследва по наказателен ред престъпления, засягащи финансовите интереси на Съюза, Комисията ще обмисли по какъв начин да подобри оптимално капацитета ѝ за защита на средствата на Съюза. Това ще включва засилване на сътрудничеството между Европейската прокуратура и Европол.

От решаващо значение за сътрудничеството е **ефикасният и сигурен обмен на информация между агенциите**. Европол и Frontex се нуждаят от бърз обмен на информация помежду си, включително за оперативни цели. Като последващо действие във връзка със съвместното изявление от януари 2024 г.[10] **eu-LISA** играе централна роля за осигуряване на сигурно съхранение и наличност на данни за целите на по-добрата координация и по-ефективния обмен на информация между агенциите. **Агенцията на ЕС за основните права** предоставя експертен опит в областта на защитата на основните права при разработването и прилагането на политики за сигурност.

Органът на ЕС за борба с изпирането на пари (ОБИП) е оправомощен да сравнява информация въз основа на наличието/липсата на съвпадение с информация, предоставена от Европол, Европейската прокуратура, Евроюст и Службата на ЕС за борба с измамите, за да извършва съвместни анализи на трансгранични случаи.

Агенцията на Европейския съюз за киберсигурност (ENISA) играе централна роля в прилагането на европейското законодателство в областта на киберсигурността. При предстоящото преразглеждане на **Акта за киберсигурността** Комисията ще направи оценка на мандата ѝ и ще предложи той да бъде модернизиран, за да се засили европейската добавена стойност на ENISA.

Сътрудничеството между митническите и други правоприлагащи органи ще бъде засилено с предложеното създаване на **Митническия орган на ЕС** и **центъра за митнически данни на ЕС** в рамките на пакета за реформа на митниците на ЕС. Информацията от бъдещия център и свързаните с нея данни от Европол, Евроюст, Европейската прокуратура, OLAF, ОБИП и Frontex, в рамките на съответните им правомощия, ще подобрят съвместния анализ и ще допринесат за по-съгласувани оперативни дейности, по-специално по външните граници. Комисията насърчава съзаконодателите да приключат бързо преговорите по реформата на митниците на ЕС и ще продължи да ги подпомага за постигането на тази цел.

[10] https://www.europol.europa.eu/cms/sites/default/files/documents/europol-frontex_joint_statement_signed_31.1.2024.pdf.

По-доброто взаимно допълване между Европейската прокуратура, OLAF, Европол, Евроюст, ОБИП и предложения Митнически орган на ЕС също ще се основава на резултатите от текущия преглед на **архитектурата на ЕС за борба с измамите**. Този цялостен подход може да окаже благотворно въздействие върху вътрешната сигурност чрез поставянето на акцент върху по-доброто използване както на наказателни, така и на административни средства, оперативната съвместимост на информационните системи и подобреното сътрудничество.

Комуникации от критично значение

Днес **системите за комуникации от критично значение**[11] се експлоатират в повечето случаи изолирано на национално равнище. Това означава, че често оказващите първа помощ не могат да комуникират със своите колеги, когато преминават през границата в други държави членки. В някои държави членки съществуват и ограничения по отношение на комуникацията между различните видове екипи, оказващи първа помощ (напр. полиция и линейки). Стандартите на повечето системи не отговарят на днешните изисквания по отношение на функционалност и устойчивост, което значително ограничава капацитета за реагиране на оказващите първа помощ, особено през граница.

За да се подобри капацитетът на ЕС за реагиране на кризи, Комисията ще предложи законодателство за създаване на **европейска система за комуникации от критично значение**, която да свързва следващото поколение системи за комуникации от критично значение на държавите членки в ЕС. Целта е тази европейска система да се основава на три стратегически стълба: оперативна мобилност, силна устойчивост и стратегическа автономност. Инициативата за европейската система за комуникации от критично значение ще определи хармонизирани изисквания и ще спомогне за модернизирането на системите за комуникации от критично значение на държавите членки, което ще им позволи да функционират безпрепятствено. Обхватът на системата ще се разшири също така чрез бъдещата мултиорбитална система IRIS[212]. Техническите способности на европейската система за комуникации от критично значение ще бъдат изградени с финансирани от ЕС проекти, като се разчита предимно на европейски доставчици на технологии, така че да се насърчи стратегическата автономност на ЕС в този чувствителен сектор.

Законен достъп до данни

Правоприлагащите и съдебните органи трябва да могат да разследват и да предприемат действия срещу престъпността. Днес почти всички форми на тежката и организираната престъпност имат цифров отпечатък[13]. Понастоящем около 85 % от наказателните разследвания разчитат на способността на правоприлагащите органи да имат достъп до цифрова информация.[14]

Групата на високо равнище относно достъпа до данни за целите на ефективното правоприлагане подчерта в своя заключителен доклад[15], че през последното десетилетие правоприлагащите и съдебните органи са загубили позиции спрямо престъпниците, тъй като последните се възползват от инструменти и продукти от други

[11] Това са мрежите, използвани от правоприлагащите органи, граничните служители, митническите органи, гражданската защита, пожарникарите, екипите за спешна медицинска помощ и други ключови участници в областта на обществената сигурност и безопасност.
[12] Инфраструктура на ЕС за устойчивост, взаимосвързаност и сигурност чрез спътници.
[13] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
[14] https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX:52019PC0070.
[15] Заключителен доклад на Групата на високо равнище относно достъпа до данни за целите на ефективното правоприлагане — 15.11.2024 г., 4802e306-c364-4154-835b-e986a9a49281_en.

юрисдикции, предоставени им от доставчици, намерили начин да не оказват сътрудничество при законни искания по отделни наказателни дела. Поради това системното сътрудничество между правоприлагащите органи и частните субекти, включително доставчиците на услуги, е от съществено значение в бъдещите усилия за разбиване на дейността на най-опасните престъпни мрежи и престъпници в Съюза и извън него.

Тъй като цифровите технологии са все по-широко разпространени и представляват все по-сериозен източник на нови инструменти за престъпниците, от съществено значение е наличието на рамка за достъп до данни, която отговаря на нуждите от прилагане на нашите закони и защита на нашите ценности. Все пак еднакво важно за запазването на киберсигурността и защитата от нововъзникващи заплахи за сигурността е да се гарантира, че цифровите системи остават предпазени от непозволен достъп. Тези рамки за достъп трябва също така да зачитат основните права, като гарантират, наред с другото, че неприкосновеността на личния живот и личните данни са адекватно защитени.

През последните години, с приемането на правила за електронните доказателства, които ще се прилагат изцяло от август 2026 г.[16], ЕС предприе действия както за борба с **престъпността онлайн, така и за улесняване на достъпа до цифрови доказателства за всички престъпления**. Тези разпоредби ще бъдат допълнени от международни инструменти за обмен на информация и на доказателства. Комисията ще предложи скоро подписването и сключването на новата **Конвенция на ООН срещу киберпрестъпността**.

С цел последващи действия на препоръките на групата на високо равнище[17], през първата половина на 2025 г. Комисията ще представи **пътна карта с правните и практическите мерки**, които тя предлага, **за да гарантира законен и ефективен достъп до данни**. В последващите действия по пътната карта приоритетно значение за Комисията ще има оценката на въздействието на **правилата за съхраняване на данни** на равнището на ЕС, както и изготвянето на **технологична пътна карта относно криптирането**, за да се набележат и оценят технологичните решения, които ще дадат възможност на правоприлагащите органи да имат законен достъп до криптирани данни, като се гарантират киберсигурността и основните права.

Оперативно сътрудничество

Комисията ще работи с държавите членки, агенциите и органите на ЕС, както и с държавите партньори за укрепване на оперативното сътрудничество, което е от съществено значение за по-ефективен подход към борбата с транснационалната организирана престъпност и тероризма.

Като основна рамка на ЕС за съвместни действия срещу тежката и организираната престъпност, **Европейската мултидисциплинарна платформа за борба с криминални заплахи (EMPACT)** постигна значителни оперативни резултати. Следващият цикъл на EMPACT за периода 2026—2029 г. представлява възможност за допълнително укрепване на тази рамка. За да се разбият най-опасните престъпни мрежи и престъпници, Съюзът трябва да рационализира и съсредоточи усилията си върху най-

[16] Регламент (ЕС) 2023/1543 на Европейския парламент и на Съвета 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, ОВ L 191, 28.7.2023 г.

[17] Заключения на Съвета относно достъпа до данни за целите на ефективното правоприлагане (12 декември 2024 г.) https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/bg/pdf.

неотложните приоритети, като засили ангажиментите на държавите членки и гарантира ефективното използване на ресурсите.

За тази цел Комисията ще работи с председателствата на Съвета и държавите членки за **максимално увеличаване на потенциала на EMPACT и за реализиране на ключовите приоритети за следващия цикъл на EMPACT за периода 2026—2029 г.** Във всичките тези приоритетни области е необходима разузнавателна информация относно най-опасните престъпни мрежи, съвместни разследвания и оперативни групи, както и категорични съдебни ответни действия, включително и подход „следвай парите“. Освен това Съюзът трябва да се справи с вербуването от престъпници и проникването на престъпни елементи и да засили междуведомственото и международното сътрудничество и обучение в областта на правоприлагането.

Комисията ще подкрепя и други форми на **трансгранично оперативно сътрудничество в областта на правоприлагането между държавите членки и асоциираните към Шенген държави**. Шенгенското пространство, по чиито вътрешните граници не се извършват проверки, изисква тясно сътрудничество и обмен на информация между правоприлагащите органи на държавите членки, за да се гарантира високо равнище на вътрешна сигурност. Служителите на правоприлагащите органи продължават да се сблъскват и към момента с предизвикателства при наблюдението или извършването на спешни действия през граница[18], а борбата с хибридните заплахи изисква и засилено трансгранично сътрудничество. Следва да се създаде **група на високо равнище относно бъдещето на оперативното сътрудничество в областта на правоприлагането**, която да разработи обща стратегическа визия.

Ефикасният обмен на данни между правоприлагащите органи също е от съществено значение за резултатното трансгранично сътрудничество. След като бъде създадена, **архитектурата за оперативна съвместимост** ще осигури на правоприлагащите органи и Европол ефективен достъп до ключова информация. Същевременно ЕС и неговите държави членки следва да дадат приоритет на двустранния и многостранния обмен на информация чрез правното и техническото прилагане на **Регламент Прюм II**[19] в сътрудничество с eu-LISA и Европол. Това ще даде възможност за сигурен автоматизиран обмен на пръстови отпечатъци, ДНК профили, данни за регистрацията на превозни средства, портретни снимки и полицейски досиета чрез маршрутизаторите на ЕС. На национално равнище държавите членки трябва да прилагат **Директивата относно обмена на информация**[20], като подобрят каналите за обмен на информация с цел безпрепятствен поток на информация през граница, като същевременно гарантират своето участие в системите на равнището на Съюза, като например SIENA[21].

Ефективното трансгранично сътрудничество се опира и на развиването на **обща култура на ЕС в областта на правоприлагането**. Съвместното обучение, центровете за високи постижения и програмите за мобилност са от съществено значение за постигането на

[18] Както се посочва в оценката на Комисията на изпълнението от държавите членки на Препоръка (ЕС) 2022/915 на Съвета от 9 юни 2022 г. относно оперативното сътрудничество в областта на правоприлагането (5909/25).

[19] Регламент (ЕС) 2024/982 на Европейския парламент и на Съвета от 13 март 2024 г. за автоматизираното търсене и обмен на данни за целите на полицейското сътрудничество и за изменение на решения 2008/615/ПВР и 2008/616/ПВР на Съвета и регламенти (ЕС) 2018/1726, (ЕС) 2019/817 и (ЕС) 2019/818 на Европейския парламент и на Съвета (Регламент Прюм II), ОВ L 2024/982, 5.4.2024 г.

[20] Директива (ЕС) 2023/977 на Европейския парламент и на Съвета от 10 май 2023 г. относно обмена на информация между правоприлагащите органи на държавите членки и за отмяна на Рамково решение 2006/960/ПВР на Съвета, ОВ L 134, 22.5.2023 г., стр. 1—24.

[21] Мрежово приложение за защитен обмен на информация.

тази цел. Комисията ще проучи най-добрите начини, по които ЕС може да подкрепи обучения за органите на държавите членки, като разчита на **CEPOL** — агенцията на ЕС за обучение в областта на правоприлагането.

Укрепване на сигурността на границите

Укрепването на устойчивостта и сигурността на външните граници е от решаващо значение за борбата с хибридните заплахи, като например използването на миграцията като оръжие, за предотвратяването на влизането в ЕС на субекти и стоки, представляващи заплаха, и за ефективната борба с трансграничните престъпност и тероризъм. За 2026 г. **се планира обновяване на Шенгенската информационна система (ШИС)**, което ще даде възможност на държавите членки да въвеждат сигнали за граждани на трети държави, участващи в тероризъм, включително чуждестранни бойци терористи, и в други тежки престъпления, въз основа на данни, които трети държави споделят с Европол.

Подобрената **оперативна съвместимост** на широкомащабните информационни системи на ЕС ще предоставя на държавите членки съществена информация за лица от трети държави, които преминават или възнамеряват да преминат външните граници, като това помага на органите да преценят дали да разрешат влизане на територията на държавите членки[22]. Комисията ще продължи да работи в тясно сътрудничество с държавите членки и eu-LISA за бързото внедряване на тези системи, по-специално на **Системата за влизане/излизане (СВИ), Европейската система за информация за пътуванията и разрешаването им (ETIAS) и изменената Визова информационна система (ВИС)**, за да се гарантират гладкото им функциониране и ползите за сигурността.

За да се повиши допълнително сигурността на границите и да се засили сътрудничеството в рамките на ЕС в контекста на променящите се заплахи, **Комисията ще предложи да се укрепи ролята на Frontex.** Съставът на европейската гранична и брегова охрана следва постепенно да се утрои до 30 000 души. Агенцията следва да разполага с авангардни технологии за наблюдение и ситуационна осведоменост, включително разузнавателни данни, които са от значение за европейското интегрирано управление на границите, и с достъп до надеждни правителствени услуги на ЕС за наблюдение на Земята за целите на граничния контрол, които ще бъдат на разположение не по-късно от 2027 г. Това допълнително ще подобри способността за откриване, предотвратяване и борба с трансграничната престъпност по външните граници, както и ще засили подкрепата на Frontex за държавите членки при осъществяването на връщанията, по-специално по отношение на граждани на трети държави, които представляват риск за сигурността.

Документните измами и използването на фалшива самоличност улесняват контрабандата на мигранти, трафика на хора, незаконните престъпни движения и трафика на незаконни стоки. След като започне да функционира, **детекторът за множество самоличности (ДМС)**[23] ще подобри способността на националните органи

[22] По-специално Системата за влизане/излизане (СВИ) ще даде възможност на държавите членки да идентифицират граждани на трети държави на външните граници на Шенгенското пространство и да регистрират влизанията и излизанията им, което ще позволи системно идентифициране на лицата, надвишили срока си на престой. Преди пристигането на гражданин на трета държава на външните граници Европейската система за информация за пътуванията и разрешаването им (ETIAS) и Визовата информационна система (ВИС) ще позволяват на държавите членки да правят предварителна оценка на присъствието на гражданин на трета държава на територията на ЕС като риск за сигурността.

[23] ДМС е един от компонентите за оперативна съвместимост, въведени с Регламент (ЕС) 2019/818 и Регламент 2019/817.

да идентифицират лицата, които използват множество самоличности, и да противодействат на използването на фалшива самоличност. Комисията ще проучи начини за повишаване на сигурността на документите за пътуване и пребиваване, издавани на граждани на ЕС и на граждани на трети държави. Освен това Комисията ще оцени как европейските портфейли за цифрова самоличност, които ще бъдат въведени до края на 2026 г. съгласно Европейската рамка за цифрова самоличност, могат да допринесат за повишаване на сигурността на документите за пътуване и за подобряване на проверките на самоличността. Това ще допълни предложенията относно цифровите удостоверения за самоличност за пътуване и цифровото приложение на ЕС за пътуване[24].

Информацията за пътуванията е от решаващо значение, за да могат органите да идентифицират и разследват движенията на престъпници, терористи и други лица, представляващи заплахи за сигурността. Въпреки че съществува рамка на ЕС относно информацията за търговския въздушен транспорт[25], обработката на данните от другите видове транспорт за целите на правоприлагането е разпокъсана. Следователно престъпниците и терористите могат да използват другите видове транспорт, за да останат незаконните им дейности неразкрити. Комисията ще работи с държавите членки и транспортния сектор за **укрепване на рамката за информацията за пътуванията**, като проучи възможността за създаване на режим в Съюза, изискващ от операторите на частни полети да събират и предават данните на пътниците, и като направи оценка на правилата за обработване на резервационните данни на пътниците, а също и на начините за рационализиране на обработването на информация за пътуванията по море. По отношение на автомобилния транспорт Комисията ще направи оценка на евентуално разширено използване на системите за **автоматично разпознаване на регистрационни номера (ANPR)** и ще увеличи възможностите за полезни взаимодействия с ШИС.

Прогнозен, иновативен и основан на способностите подход

Въз основа на най-добрите практики, установени на национално равнище, Комисията ще разработи **всеобхватен прогнозен подход към вътрешната сигурност на равнището на ЕС**. Този подход ще подпомага изготвянето на политиките и ще насочва инвестициите в съответните финансирани от ЕС научни изследвания и иновации в областта на сигурността.

Научните изследвания и иновациите играят решаваща роля за вътрешната сигурност, като предоставят решения за противодействие на нововъзникващите заплахи, включително от злоупотреби с технологии[26]. Чрез финансирани от ЕС научни изследвания и иновации в областта на сигурността[27] ЕС трябва да продължи да инвестира в разработването на иновативни инструменти и решения за справяне със заплахите за сигурността, като същевременно се придържа към правилата на ЕС и основните права. Комисията следва да подкрепя прехода от научни изследвания към внедряване, за да гарантира ефективното внедряване на тези съвременни способности, с

[24] https://ec.europa.eu/commission/presscorner/detail/bg/ip_24_5047.

[25] Рамка за резервационни данни на пътниците (PNR) и за предварителна информация за пътниците (API), създадена с Директива (ЕС) 2016/681 („Директива относно PNR данните“) и Регламент (ЕС) 2025/12, Регламент (ЕС) 2025/13 („Регламенти за API“).

[26] Вж. доклада на Съвместния изследователски център на Комисията „Нововъзникващи рискове и възможности за вътрешната сигурност на ЕС, произтичащи от новите технологии“ https://publications.jrc.ec.europa.eu/repository/handle/JRC139674.

[27] Проучване относно укрепването на финансираните от ЕС научни изследвания и иновации в областта на сигурността — 20 години финансирани от ЕС научни изследвания и иновации в областта на гражданската сигурност — 2025 г., https://data.europa.eu/doi/10.2837/0004501.

приоритет на **новите технологии** като ИИ. Този подход следва да включва обучения за подобряване на използването на системи с ИИ и други технически способности от страна на правоприлагащите и съдебните органи. Още повече, когато е уместно, потенциалът на технологиите за двойна употреба следва да се използва и в двете посоки (от граждански към отбранителни цели и от отбранителни към граждански цели)[28].

Иновационният център на ЕС за вътрешна сигурност[29] — мрежа от лаборатории за иновации, представящи последните новости в областта на иновациите и ефективни решения в подкрепа на работата на участниците в областта на вътрешната сигурност в ЕС и държавите членки, ще спомогне за интегрирането на научните изследвания в практиката и политиката. Повишаването на ефективността на Европол изисква укрепване на хранилището за инструменти на Европол, което да му даде възможност да идентифицира, разработва, съвместно възлага обществени поръчки и прилага оперативно модерни технологии. В допълнение Комисията ще създаде в рамките на своя Съвместен изследователски център **Център за научни изследвания и иновации в областта на сигурността**, който ще обединява изследователи, за да се съкрати цикълът от резултатите от научните изследвания до иновациите, разработването и успешното изпълнение, като същевременно се намалят разходите за разработване, изпитване и валидиране.

По своята същност нашето **европейско научноизследователско пространство** разчита на сътрудничеството и следователно може да има пролуки за външна намеса и дезинформация. След приемането на препоръката на Съвета относно сигурността на научните изследвания[30] Комисията и държавите членки предприемат мерки за предоставяне на възможности на съответните участници да реагират, наред с другото, чрез създаването на експертен център в областта на сигурността на научните изследвания.

Ключови действия

През 2026 г. Комисията ще приеме:

- **законодателно предложение за превръщането на Европол в наистина оперативна правоприлагаща служба;**
- **законодателно предложение за укрепване на Евроюст;**
- **законодателно предложение за засилване на ролята и задачите на Frontex;**
- **законодателно предложение за създаване на европейска система за комуникации от критично значение.**

Комисията:

- **ще представи през 2025 г. пътна карта, в която се очертават бъдещите стъпки за законен и ефективен достъп до данни за правоприлагащите органи;**
- **ще изготви през 2025 г. оценка на въздействието с оглед актуализиране на правилата за съхраняване на данни на равнището на ЕС, когато е целесъобразно;**
- **ще представи през 2026 г. технологична пътна карта относно криптирането с цел идентифициране и оценка на технологични решения, които да предоставят законен достъп до данни на правоприлагащите органи;**

[28] Както се посочва в доклада на Нийнистьо.
[29] Иновационен център на ЕС за вътрешна сигурност |Европол.
[30] ОВ C, C/2024/3510, 30.5.2024 г.

- **ще работи за създаването на група на високо равнище за укрепване на оперативното сътрудничество в областта на правоприлагането;**
- **ще създаде през 2026 г. Център за научни изследвания и иновации в областта на сигурността в рамките на своя Съвместен изследователски център.**

Комисията, в сътрудничество с държавите членки и съответните агенции на ЕС:

- **ще укрепи архитектурата на EMPACT;**
- **ще работи за бързото разгръщане на архитектурата за оперативна съвместимост и прилагане на Регламент Прюм II;**
- **ще укрепи рамката за информацията за пътуванията.**

Държавите членки се приканват:

- **да транспонират и прилагат изцяло Директивата относно обмена на информация.**

4. Устойчивост срещу хибридните заплахи и други враждебни действия

Ще изградим устойчивост срещу хибридните заплахи чрез подобряване на защитата на критичната инфраструктура, укрепване на киберсигурността, усилване на сигурността на транспортните центрове и пристанищата и борба с онлайн заплахите.

Свидетели сме на нарастване както на честотата, така и на сложността на враждебните действия, които подкопават сигурността на ЕС, а злонамерените участници значително разшириха своя арсенал. Зачестиха хибридните кампании, насочени срещу ЕС, неговите държави членки и партньори, в това число актове на саботаж срещу критична инфраструктура, палежи, кибератаки, намеса в избори, външна намеса и манипулиране на информация, включително дезинформация, и използване на миграцията като оръжие. Поради политическата и оперативната си роля и естеството на информацията, с която боравят, институциите, органите, службите и агенциите на Съюза („субектите на Съюза“) не са пощадени.

ЕС трябва да **подобри своята устойчивост**, да използва ефективно настоящите инструменти и да разработи нови начини за справяне сега и в бъдеще с тези променящи се заплахи, произтичащи от държавни и недържавни участници.

Критична инфраструктура

Заплахите за **критичната инфраструктура**, включително хибридните заплахи като саботаж и злонамерени действия в киберпространството, са основен проблем, особено за инфраструктурата, която свързва държавите членки — било то енергийни междусистемни връзки, или трансгранични комуникационни кабели, и за транспорта. След началото на агресивната война на Русия срещу Украйна актовете на саботаж срещу критична инфраструктура се увеличиха, особено през 2024 г., като засегнаха много държави членки. Сътрудничеството между правоприлагащите органи, службите за сигурност и киберсигурност, военната и гражданската защита и частните оператори е от съществено значение за ефективното предвиждане, откриване, предотвратяване и реагиране на такива действия.

Задължително за намаляването на уязвимостта и укрепването на устойчивостта на критичните субекти е да се гарантира непрекъснатото предоставяне на основните услуги, които са от жизненоважно значение за икономиката и обществото. Ето защо в това

отношение от решаващо значение е своевременното и правилно транспониране от страна на всички държави членки на **Директивата за устойчивостта на критичните субекти (ИКС)**[31] и **Директивата относно мерки за високо общо ниво на киберсигурност в Съюза (МИС 2)**[32].

За да се гарантира бърз напредък, Комисията ще подкрепя държавите членки при идентифицирането на критичните субекти[33] и обмена на добри практики относно националните стратегии и оценките на риска по отношение на основните услуги в сътрудничество с **Групата по въпросите на устойчивостта на критичните субекти и групата за сътрудничество за МИС**. В случай на смущения в критичната инфраструктура със значително трансгранично отражение реакцията на равнището на ЕС ще бъде координирана от **подробния план за координиран отговор на смущения в критичната инфраструктура със значително трансгранично значение.** Комисията насърчава Съвета бързо да приеме **подробния план на ЕС за киберсигурността**, който допълнително ще засили координацията в контекста на управлението на кризи, като улесни по-тясното сътрудничество между органите в областта на физическата и цифровата устойчивост. След успешното провеждане през 2023 г. на стрес тестове в енергийния сектор Комисията ще насърчава **доброволните стрес тестове** в други ключови сектори за вътрешната сигурност. Комисията ще предостави освен това **преглед на равнището на Съюза на трансграничните и междусекторните рискове** за основните услуги, за да подпомогне оценките на риска на държавите членки и да постави основите за цялостна оценка на риска на равнището на ЕС. В съответствие с европейската стратегия за Съюз на подготвеност Комисията ще работи с държавите членки с цел определяне на други сектори и услуги, които не са обхванати от действащото законодателство и за които може да е необходимо да бъдат предприети действия.

Работната група ЕС—НАТО по въпросите на устойчивостта на критичната инфраструктура създаде условията за отлично сътрудничество при обмена на най-добри практики и повишаването на устойчивостта в секторите на енергетиката, транспорта, цифровата инфраструктура и космическото пространство. Работата ще продължи в рамките на **структурирания диалог между ЕС и НАТО относно устойчивостта**. **Инструментариумът на ЕС срещу хибридни заплахи** предлага солидна подкрепа на държавите членки и партньорите в подготовката и борбата с хибридните заплахи. **Екипите за бързо реагиране при хибридни заплахи**[34] предоставят, при поискване, краткосрочна и съобразена с нуждите помощ на държавите членки, различните мисии и партньорите на ЕС. Освен това Комисията ще задълбочи сътрудничеството в ЕС в борбата със саботажите чрез експертни дейности[35],

[31] 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.

[32] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2).

[33] Секторите, обхванати от директивата, са енергетика, транспорт, банково дело, инфраструктура на финансовите пазари, здравеопазване, питейна вода, отпадъчни води, цифрова инфраструктура, публична администрация, космическо пространство, производство, преработка и разпространение на храни.

[34] Стратегически компас на ЕС за сигурността и отбраната за 2022 г., стр. 22.

[35] Консултанти на ЕС в областта на сигурността, Европейска мрежа за обезвреждане на взривни устройства (EEODN), мрежа „Атлас“, Мрежа на ЕС за сигурност при висока степен на риск (EU HRSN), Консултативна група по химическата, биологичната, радиологичната и ядрената сигурност, Група по въпросите на устойчивостта на критичните субекти (CERG).

включително **специална съвместна работна програма** за експертите с цел рационализиране на обмена на информация и очертаване на мерките за противодействие.

Инцидентите, засягащи **подводните кабели** в Европа, подчертават необходимостта от по-строги мерки и по-ясни ответни действия. Както се посочва в **Плана за действие на ЕС относно сигурността на кабелите**[36], Комисията, заедно с върховния представител, ще си сътрудничи с държавите членки, агенциите на ЕС и партньорите, като НАТО, за предотвратяване, откриване, реагиране и възпиране на заплахи срещу подводните кабели. За да очертае интегрирана картина на заплахите, Комисията ще работи с държавите членки за разработване и внедряване, на доброволен принцип, на интегриран механизъм за наблюдение на подводните кабели във всеки морски басейн, като започне с регионален център за скандинавския/балтийския регион.

Киберсигурност

Упоритите по своя характер **злонамерени действия в киберпространството**, които често са част от по-широк спектър от многоизмерни и хибридни заплахи, изискват постоянно внимание и действия на европейско равнище. През последните години Съюзът прие редица нормативни актове в областта на киберсигурността, които укрепват киберустойчивостта на субектите по МИС 2, извършващи дейност в критични сектори на ЕС, както и на субектите на Съюза[37], подобряват сигурността на цифровите продукти (Законодателен акт за киберустойчивост) и създават рамка на подкрепа за готовността и реакцията в случай на инциденти (Законодателен акт за киберсолидарност). През януари 2025 г. Комисията прие **Европейския план за действие относно киберсигурността на болниците и доставчиците на здравно обслужване**[38], за да се подобрят откриването на заплахи, подготвеността и реакцията при кризи. Пълното му прилагане е от ключово значение. Същевременно, за да се справим с новите заплахи и съответното развитие, трябва да засилим действията си, по-специално в областта на обмена на информация, сигурността на веригите на доставка, софтуера за изнудване и кибератаките, както и по отношение на технологичния суверенитет.

Освен това прилагането изисква преодоляването на настоящия недостиг на умения в областта на киберсигурността, който засяга 299 000 души. Комисията ще работи с държавите членки в рамките на съюза на уменията[39] за увеличаване на работната сила в областта на киберсигурността, по-специално чрез използване на новата Академия на ЕС за киберумения. Стратегическият план за образованието по НТИМ[40] допринася за нарастването на резерва от таланти и подобряването на отговора на Европа на нуждите на пазара на труда в областта на киберсигурността.

Успоредно с повишаването на своята устойчивост ЕС ще продължи да използва пълноценно рамката за съвместен дипломатически отговор на ЕС срещу злонамерени кибердейности (**инструментариум за кибердипломация**), за да предотвратява, възпира и реагира на киберзаплахи, произтичащи от държавни и недържавни участници.

Сигурност на веригите на доставка на ИКТ

[36] JOIN (2025) 9 final.
[37] Регламент (ЕС, Евратом) 2023/2841 на Европейския парламент и на Съвета от 13 декември 2023 г. за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза, ОВ L, 2023/2841, 18.12.2023 г.
[38] https://digital-strategy.ec.europa.eu/en/library/european-action-plan-cybersecurity-hospitals-and-healthcare-providers.
[39] COM (2025) 90 final.
[40] COM (2025) 89 final.

Инструментариумът на ЕС за киберсигурност на 5G технологиите предоставя съответната рамка за защита на 5G мрежите, но понастоящем не се прилага в достатъчна степен от държавите членки. Продължават да съществуват неприемливи рискове за сигурността, по-специално по отношение на замяната на високорискови доставчици. Чрез хармонизиран подход към сигурността на веригите на доставка на ИКТ може да се преодолее настоящата разпокъсаност на вътрешния пазар, причинена от различните подходи на национално равнище, да се избегнат критичните зависимости и да се намали рискът за нашите вериги на доставка на ИКТ от високорискови доставчици, като по този начин се направи безопасна критичната инфраструктура.

В съответствие с този подход, при предстоящото **преразглеждане на Акта за киберсигурността** Комисията ще разгледа в по-широк план сигурността и устойчивостта на веригите на доставка и инфраструктурата на ИКТ. Комисията ще предложи освен това да се подобри **Европейската рамка за сертифициране на киберсигурността**, за да се гарантира, че бъдещите схеми за сертифициране могат да бъдат своевременно приемани и да отговарят на нуждите на политиката.

Въз основа на съществуващите или текущите секторни оценки[41] Комисията ще разработи, заедно с държавите членки, **стратегическо планиране за координирани оценки на рисковете за киберсигурността.**

Услугите в облак и телекомуникационните услуги се превърнаха в основен елемент на веригите на доставка за критичните инфраструктури, предприятията и публичните органи. Комисията ще предприеме действия за насърчаване на критичните субекти да избират **услуги в облак и телекомуникационни услуги, които предлагат подходящо ниво на киберсигурност**, като се вземат предвид не само техническите рискове, но и стратегическите рискове и зависимости.

Софтуер за изнудване и кибератаки

Софтуерът за изнудване е трайно и сериозно предизвикателство в ЕС и по света, като в един доклад общите годишни разходи, свързани с него, до 2031 г. се оценяват на над 250 милиарда евро[42]. Както **Директивата МИС 2**, така и **Законодателният акт за киберустойчивост** значително ще подобрят състоянието на киберсигурността на различните субекти, което ще оскъпи атаките на мрежите, използващи софтуер за изнудване. В допълнение Комисията ще работи в тясно сътрудничество с държавите членки, за да гарантира, че на правоприлагащите органи се докладват повече случаи на атаки със софтуер за изнудване, по-специално случаи на съвременни упорити заплахи, и плащания на откуп, което ще улеснява разследванията.

За да предотврати и спре кибератаките, ЕС трябва да засили обмена на информация между правоприлагащите органи, органите и субектите в областта на киберсигурността, както и частните субекти, под егидата на Европол и Агенцията на ЕС за киберсигурност (ENISA).

Европол и Евроюст следва да продължат да надграждат успехите си по елиминирането на операции, използващи софтуер за изнудване, като така подкрепят сътрудничеството в областта на правоприлагането. За тази цел правоприлагащите органи следва да използват в максимална степен механизмите за сътрудничество, в това число **международния**

[41] Като например на 5G мрежи, телекомуникациите, електроенергията, енергията от възобновяеми източници и свързаните превозни средства.
[42] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/.

модел на Европол за реагиране на софтуер за изнудване и **международната инициатива за противодействие на софтуера за изнудване**[43], а ENISA и Европол следва да си сътрудничат за разширяване на хранилището на инструменти за декриптиране на различни видове софтуер за изнудване[44].

Технологичен суверенитет

Киберсигурността и технологичният суверенитет са тясно свързани и по технологичните зависимости трябва да се действа приоритетно. Съюзът трябва да **направлява разработването и внедряването на нови технологии**, като Комисията работи за **подобряването на способностите в стратегически технологии**, например ИИ, квантовите технологии, усъвършенстваната свързаност, изчисленията в облак, периферните изчисления и интернет на нещата[45], чрез предстоящи инициативи, като плана за действие „Континент на ИИ“, стратегията за квантовите технологии и други[46]. Комисията ще продължи да подкрепя навременното внедряване на най-новите международно договорени **интернет протоколи**, които са от съществено значение за поддържането на подлежащ на развитие и ефикасен интернет с високо ниво на киберсигурност. Необходими са и допълнителни действия, в това число използване на квантови сензорни технологии и проучване на развитието на капацитета за наблюдение чрез радиочестоти, за справяне с **предизвикателствата, свързани с радиочестотния спектър**, като например фалшифицирането на ГНСС, заглушаването, рисковете и зависимостите на веригите на доставка.

Внедряването на решения за **пост-квантова криптография** ще бъде от решаващо значение за защитата на чувствителните комуникации, данните в покой и цифровите самоличности в новата квантова ера. Въз основа на Препоръката от 2024 г. относно пътна карта за координирано изпълнение на прехода към пост-квантова криптография [47]Комисията работи с държавите членки за насърчаването на този преход. Във връзка с това държавите членки следва да идентифицират високорискови случаи в критични субекти и да гарантират квантово безопасно криптиране за тези високорискови случаи възможно най-скоро и не по-късно от края на 2030 г. Комисията също така работи с държавите членки и Европейската космическа агенция (ЕКА) за разработването и разполагането на **европейската квантова комуникационна инфраструктура (EuroQCI)**[48], основана на разпределение на криптографски ключ по квантов път (QKD), като част от **IRIS²** — Програмата на ЕС за сигурна свързаност. И двете инициативи, в крайна сметка, ще позволят на субектите да предават данни и да съхраняват информацията по сигурен начин.

Квантовите технологии също ще играят ключова роля в приложенията за сигурност: като част от **стратегията за квантовите технологии** ще бъде разработена **пътна карта за измерване с квантови сензори в приложенията за сигурност**. В същия дух Комисията работи за подобряване на устойчивостта на своите корпоративни системи от

[43] https://counter-ransomware.org/.
[44] Достъпен чрез проекта No More Ransom, https://www.nomoreransom.org/en/index.html.
[45] https://strategic-technologies.europa.eu/about_en#step-scope.
[46] напр. EuropHPC JU https://eurohpc-ju.europa.eu/index_en, Водеща инициатива в областта на квантовите технологииНачална страница на Водещата инициатива в областта на квантовите технологии |Водеща инициатива в областта на квантовите технологии, мрежи 3С (COM(2024) 81 final) и План за действие на ЕС относно сигурността на кабелите (JOIN(2025) 9 final).
[47] Препоръка относно пътна карта за координирано изпълнение на прехода към пост-квантова криптография | Стратегия в областта на цифровите технологии.
[48] https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci.

критично значение за сигурността, включително на своите класифицирани информационни системи.

Благоприятна за бизнеса рамка за киберсигурност

Предстоящото преразглеждане на Акта за киберсигурността представлява възможност за **опростяване на законодателството на ЕС в областта на киберсигурността** в съответствие с компаса за конкурентоспособността. Комисията ще работи в тясно сътрудничество с държавите членки, за да гарантира бързото, съгласувано и благоприятно за бизнеса прилагане на хоризонталната рамка за киберсигурност, определена в Директивата МИС 2, Законодателния акт за киберустойчивост и Законодателния акт за киберсолидарност, като се насърчават опростяването и съгласуваността и се избягва разпокъсаността или дублирането на правилата за киберсигурност в законодателството на ЕС и в националното законодателство.

С цел да се даде възможност за сигурен достъп до онлайн услуги и да се укрепи цифровата сигурност в целия ЕС, **Европейската рамка за цифрова самоличност** ще предложи на всички граждани и на пребиваващите в ЕС надеждни портфейли за цифрова самоличност преди края на 2026 г. Предстоящият **европейски бизнес портфейл** ще улесни сигурните трансгранични взаимодействия между предприятията и публичните администрации. И двата вида портфейли са предпоставка за сигурното и по-ефективно функциониране на основания на данни единен пазар с инструменти като единна цифрова платформа, електронното фактуриране, електронните обществени поръчки и цифровия продуктов паспорт.

Онлайн сигурност

Интернет е мястото на някои от най-сериозните хибридни заплахи, застрашаващи сигурността и безопасността на хората в Европа и под прицела на които е демократичната сфера на ЕС. Тези заплахи включват незаконни дейности и незаконно съдържание онлайн, както и манипулиране на информация, включващо изкуствено „раздуване“ на дезинформация, подвеждаща информация и чуждестранно манипулиране на информация и вмешателство (ЧМИВ).

Строгото прилагане на **Акта за цифровите услуги** е от първостепенно значение, за да се гарантира безопасна и достъпна онлайн среда с отговорни участници, която е устойчива и на хибридни заплахи. Актът за цифровите услуги задължава доставчиците на много големи онлайн платформи и много големи онлайн търсачки да извършват оценки на риска и да въвеждат мерки за смекчаване на системните рискове, произтичащи от параметрите, функционирането или използването на техните услуги. Тези рискове могат да включват отрицателни последици за гражданския дискурс и изборните процеси, както и за обществената сигурност, като например мащабна намеса на злонамерени чуждестранни държавни участници, например в изборните процеси. От значение е обучението на компетентните органи на държавите членки относно използването на правни инструменти за бързо премахване на незаконно съдържание онлайн, особено по отношение на кибернасилието, основано на пола. В Акта за цифровите услуги се предвижда механизъм за реакция при кризи, който може да бъде задействан, когато извънредни обстоятелства водят до сериозна заплаха за обществената сигурност или общественото здраве в Съюза или в значителна част от него. За да допълнят този механизъм, Комисията и националните компетентни органи, определени за координатори за цифровите услуги, разработиха и доброволна **рамка за реагиране при инциденти съгласно Акта за цифровите услуги**. Координаторите за цифровите услуги също така предприеха действия, за да помогнат за защитата на почтеността на изборите,

например чрез организиране на изборни кръгли маси и стрес тестове[49]. Актът за цифровите услуги, заедно с Регламента относно политическото рекламиране[50], е едно от няколкото законодателни направления, свързани със защитата на демокрацията и целостта на демократичните процеси, които са уязвими и могат да бъдат на прицела на враждебни участници, включително чрез цифрови инструменти и в социалните медии.

Прилагането на инструментариума срещу **ЧМИВ** е друг важен компонент, който предлага ключова подкрепа на равнището на ЕС. Подкрепата за цифровата и медийната грамотност, както и критичното мислене също е в центъра на тези усилия[51].

Противодействие на използването на миграцията като оръжие

Русия, с помощта и решителната подкрепа на Беларус, целенасочено използва миграцията като оръжие, при което незаконно улеснява миграционни потоци към външните граници на ЕС с цел дестабилизиране на нашите общества и подкопаване на единството на Европейския съюз. Това застрашава не само националната сигурност и суверенитета на държавите членки, но и сигурността и целостта на Шенгенското пространство и сигурността на Съюза като цяло. В заключенията си от октомври 2024 г. Европейският съвет подчерта, че нито на Русия и Беларус, нито на която и да е друга държава може да се позволи да злоупотребяват с нашите ценности, включително правото на убежище, и да подкопават нашата демокрация.

Както се посочва в съобщението на Комисията от 2024 г. относно използването на миграцията като оръжие, в допълнение към силната политическа подкрепа Съюзът предприе финансови, оперативни и дипломатически мерки, включително сътрудничество с държавите на произход и транзитно преминаване, за ефективно справяне с тези заплахи[52]. Този отговор включва използването на новата рамка, създадена от Съвета, за санкциониране на лицата и организациите, участващи в действия и политики като използването на миграцията като оръжие от страна на Русия, чрез налагане на замразяване на активи и забрана за пътуване[53]. ЕС ще продължи да използва тази рамка, когато е необходимо, и ще подкрепя държавите членки в борбата с тази заплаха.

Сигурност на транспорта

Морските пристанища, летищата и наземната инфраструктура са ключови входни и изходни точки. Те играят жизненоважна роля в икономиката и обществото на ЕС и са от съществено значение за военната мобилност. Тези транспортни центрове и средства обаче са също така основни мишени на външни заплахи и престъпна дейност. Неотдавнашните инциденти, включително пробивите на сигурността на въздушния превоз на товари и атаките срещу железопътната инфраструктура, изкараха наяве сериозните рискове. **Транспортните оператори** могат да бъдат както цели, така и инструменти за злонамерени участници. Действащите правни инструменти на ЕС

[49] DSA Elections Toolkit for Digital Services Coordinators 2025 https://digital-strategy.ec.europa.eu/en/library/dsa-elections-toolkit-digital-services-coordinators (Акт за цифровите услуги — Набор от инструменти за избори, предназначен за координатори на цифрови услуги, 2025 г.).

[50] Регламент (ЕС) 2024/900 на Европейския парламент и на Съвета от 13 март 2024 г. относно прозрачността и таргетирането на политическото рекламиране (ОВ L 2024/900, 20.3.2024 г.).

[51] План за действие в областта на цифровото образование (2021—2027 г.) — Европейско пространство за образование.

[52] COM (2024) 570 final.

[53] Регламент (ЕС) 2024/2642 на Съвета от 8 октомври 2024 г. относно ограничителни мерки с оглед на дестабилизиращите дейности на Русия, ST/8744/2024/INIT (ОВ L, 2024/2642, 9.10.2024 г.).

повишиха сигурността на въздухоплаването[54], но високото равнище на заплаха за гражданското въздухоплаване изисква начин за предвиждане на инциденти и бързо провеждане на консултации със съответните държави членки. Комисията ще си сътрудничи с държавите членки за изменение на съществуващото законодателство за прилагане в областта на сигурността на въздухоплаването с цел обмен на класифицирана информация за **събития, свързани със сигурността на въздухоплаването**. Освен това Комисията ще обмисли **регулаторни мерки** за справяне с нови заплахи, като например **инциденти с въздушни товари**, и за укрепване на стандартите за сигурност на въздухоплаването. Това ще включва и укрепване на **законодателството в областта на сигурността на въздухоплаването**, за да се даде възможност за незабавни ответни мерки, като същевременно се запази зоната на сигурност на летищата в ЕС.

При разработването на предстоящата **стратегия на ЕС за пристанищата** въз основа на **Европейския пристанищен алианс** Комисията ще проучи начини за по-нататъшно укрепване на законодателството в областта на морската сигурност с цел ефективно справяне с възникващите заплахи, обезопасяване на пристанищата и повишаване на сигурността на веригата на доставки в ЕС. За тази цел Комисията ще гарантира стабилното ѝ прилагане и ще работи за хармонизирането на националните практики и засилването на цялостните проверки в пристанищата. В допълнение към протоколите за сигурност, установени за въздушните товари, Комисията ще работи с държавите членки и частния сектор за разширяването обхвата на тези протоколи, за да се направят сигурни веригите на морския транспорт.

Предложеният митнически орган на ЕС ще анализира и оценява рисковете въз основа на **митническата информация**, свързана със стоки, които влизат в ЕС, излизат от него и преминават транзитно през него, за да подкрепя държавите членки при предотвратяването на използването на международните вериги на доставки от злонамерени участници. В съответствие със Стратегията на ЕС за морска сигурност[55] предстоящият **европейски пакт за океаните** ще играе ключова роля за засилване на морската сигурност в морските басейни около ЕС и отвъд тях, включително в посока на увеличаването на мащаба на многоцелевите морски операции и учения.

Устойчивост на веригите на доставки

Европа трябва да разчита в по-малка степен на технологии на трети държави, защото това може да доведе до зависимост и рискове за сигурността. Комисията има за цел понижаването на зависимостите от единствени чуждестранни доставчици, намаляването на риска за нашите вериги на доставки поради високорискови доставчици и гарантирането на сигурността на критично важните инфраструктура и промишлен капацитет на територията на ЕС, както е посочено в **компаса за конкурентоспособността[56]** и **Пакта за чиста промишленост[57]**. Комисията ще прокарва **промишлена политика за вътрешна сигурност**, като си сътрудничи с промишлеността на ЕС в ключови сектори (напр. транспортни центрове, критични инфраструктури) за създаване на решения за сигурност, като оборудване за откриване, биометрични технологии и безпилотни летателни апарати, включващи елементи на сигурност още при проектирането. При **преразглеждането на правилата на ЕС за обществените поръчки**

[54] Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета от 11 март 2008 г. относно общите правила в областта на сигурността на гражданското въздухоплаване (ОВ L 97, 9.4.2008 г., стр. 72—84).
[55] JOIN (2023) 8 final.
[56] COM/2025/30 final.
[57] COM/2025/85 final.

Комисията ще прецени дали съображенията за сигурност в Директивата за обществените поръчки в областта на отбраната и сигурността от 2009 г.[58] са достатъчни, за да се отговори на нуждите на правоприлагащите органи и устойчивостта на критичните субекти.

Комисията ще подкрепя държавите членки при **скрининга на преките чуждестранни инвестиции (ПЧИ)** и възлагането на обществени поръчки за оборудване за логистични центрове, като гарантира, че критично важните инфраструктура и технологии остават сигурни.

След като влезе в сила, **Законодателният акт за извънредните ситуации и устойчивостта на вътрешния пазар** ще помогне на ЕС да управлява кризи, които нарушават критично важните вериги на доставки и свободното движение на стоки, услуги и хора. С акта ще се даде възможност за бърза координация при кризи, идентифициране на стоки и услуги от особено значение при криза и ще се осигури инструментариум, за да се гарантира тяхната наличност. Освен това, в тясно сътрудничество с държавите членки, Комисията ще предложи да се създаде **многоведомствен механизъм за предупреждение във връзка със сигурността на транспорта и веригата на доставки**, за да се гарантира сигурен и навременен обмен на съответната информация, необходима за предвиждане и противодействие на заплахите.

Същевременно, с прилагането на Законодателния акт за суровините от критично значение и Законодателния акт за промишленост с нулеви нетни емисии, повишеното използване на критерии за устойчивост, издръжливост и европейски предпочитания в обществените поръчки на ЕС ще насърчи развитието на водещи пазари. Засилените търговски връзки, например чрез партньорства в областта на суровините и партньорства за чиста търговия и инвестиции, ще спомогнат за диверсифицирането на веригите на доставки.

Устойчивост и готовност за химични, биологични, радиологични и ядрени заплахи

Агресивната война на Русия срещу Украйна увеличи риска от **химични, биологични, радиологични и ядрени (ХБРЯ) заплахи**. За да се справи с потенциалното придобиване и използване като оръжие на ХБРЯ материали, Комисията ще подкрепя държавите членки и държавите партньори чрез специални обучения и учения. Комисията също така ще повиши капацитета за готовност и реакция в областта на ХБРЯ материалите чрез приоритизиране на заплахите, финансиране на иновациите за мерки за противодействие, способностите на rescEU и натрупването на резерв от медицински мерки за противодействие, в рамките на нов **план за действие за готовност и реакция в областта на ХБРЯ материалите**. Освен това със **стратегията на ЕС за медицинските мерки за противодействие** ще се подкрепя разработването на медицински мерки за противодействие — от научните изследвания до производството и разпространението — с цел да се защити ЕС от пандемии и ХБРЯ заплахи.

Въз основа на опита от пандемията от COVID-19 ЕС укрепи рамката за здравна сигурност[59]. Понастоящем Комисията определя референтни лаборатории на ЕС в областта на общественото здраве с цел укрепване на капацитета за наблюдение и бързо откриване на равнището на ЕС и на национално равнище. През 2025 г. ще бъде публикуван план на Съюза за предотвратяване, готовност и реакция в областта на здравната сигурност.

[58] Директива 2009/81/ЕО относно координирането на процедурите за възлагане на някои поръчки за строителство, доставки и услуги от възлагащи органи или възложители в областта на отбраната (ОВ L 216, 20.8.2009 г.).

[59] По-специално чрез Регламент (ЕС) 2022/2371 относно сериозните трансгранични заплахи за здравето.

Ключови действия

Комисията:

- **ще преразгледа и измени през 2025 г. Акта за киберсигурността;**
- **ще разработи мерки за гарантиране на киберсигурността при използването на услуги „в облак“;**
- **ще предложи през 2025 г. стратегия на ЕС за пристанищата;**
- **ще преразгледа през 2026 г. правилата на ЕС за обществените поръчки в областта на отбраната и сигурността;**
- **ще представи през 2026 г. нов план за действие за готовност и реакция в областта на ХБРЯ материалите.**

В сътрудничество с държавите членки Комисията:

- **ще разработи и внедри европейската квантова комуникационна инфраструктура (EuroQCI);**
- **ще гарантира ефективното прилагане на Акта за цифровите услуги;**
- **ще работи за противодействие на използването на миграцията като оръжие;**
- **ще създаде информационна система за събития, свързани със сигурността на въздухоплаването;**
- **ще работи за създаването на многоведомствен механизъм за предупреждение в областта на транспорта и сигурността на веригата на доставки.**

Съветът се приканва:

- **да приеме препоръката на Съвета относно концепцията на ЕС в областта на киберсигурността.**

Държавите членки се приканват:

- **да транспонират и приложат изцяло Директивата относно УКС и Директивата МИС 2.**

5. Затягане на примката около тежката и организираната престъпност

Ще помогнем за изкореняването на организираната престъпност, като предложим по-строги правила за справяне с мрежите на организираната престъпност, включително относно разследванията, за намаляване на уязвимостта на младежите в ЕС по отношение на въвличането им в престъпления и за засилване на мерките за премахване на достъпа до престъпни инструменти и активи.

Организираната престъпност използва променящата се среда и експоненциално се разраства. Тя се възползва от авангардни технологии, извършва дейност в множество юрисдикции и има силни връзки отвъд границите на ЕС. Като се имат предвид тези комплексни транснационални заплахи, координацията и подкрепата на равнището на ЕС са от жизненоважно значение.

Превенция на престъпността

Набирането на млади хора от организираната престъпност поражда все по-голяма загриженост в ЕС. Борбата с организираната престъпност изисква справяне с **първопричините** за нея чрез предлагане на образование и алтернативи на престъпния начин на живот посредством подход, обхващащ цялото общество. Комисията ще подкрепи интегрирането на съображенията за сигурност в политиките на ЕС в областта на образованието, социалната сфера, заетостта и регионите. ЕС ще **насърчава основани**

на доказателства политики за превенция на престъпността[60] , съобразени с местните условия.

За да се защитят получателите на онлайн услуги, по-специално малолетните и непълнолетните, от сексуално насилие над деца, трафиканти на хора и набиране онлайн за престъпления или насилнически екстремизъм, мерките съгласно **Акта за цифровите услуги** изискват от доставчиците на онлайн платформи, достъпни за малолетни и непълнолетни, да управляват рисковете и да предприемат действия във връзка с незаконното съдържание, включително изказванията, подбуждащи към омраза. Комисията планира да издаде **насоки относно защитата на малолетните и непълнолетните**, за да помогне на доставчиците на онлайн платформи да гарантират на малолетните и непълнолетните високо равнище на неприкосновеност на личния живот, безопасност и сигурност в интернет. Насоките ще съдържат набор от препоръки за всички цифрови услуги, извършвани в Съюза, така че да се подобри защитата на малолетните и непълнолетните лица онлайн. През 2025 г. Комисията планира също така да улесни въвеждането на решение на ЕС за **проверка на възрастта за защита на неприкосновеността на личния живот**, което ще запълни липсата, преди европейският портфейл за цифрова самоличност да бъде на разположение в края на 2026 г. Комисията ще приеме и план за действие срещу кибертормоза.

Освен това Комисията ще продължи да подкрепя доброволното ангажиране на множество заинтересовани страни с онлайн платформите и други съответни участници, включително чрез интернет форума на ЕС и целеви кодекси за поведение съгласно Акта за цифровите услуги, като например Кодекса за поведение във връзка с незаконните изказвания онлайн, пораждащи омраза, от 2025 г. Целта е да се повиши осведомеността, да се реагира съвместно на настоящите и нововъзникващите заплахи и да се изготвят и споделят добри практики за мерки за смекчаване на последиците.

В локален аспект въздействието на организираната престъпност прави по-належаща необходимостта от регионални решения за намаляване на уязвимостта и привлекателността на незаконните дейности. Програмата на ЕС за градовете ще се занимае с предизвикателствата пред сигурността в градовете въз основа на инициативата на ЕС „Градовете срещу радикализацията“. Комисията ще подкрепя държавите членки при повишаването на градската и регионалната сигурност чрез Европейския фонд за регионално развитие**.**

По-крепките образователни основи и умения представляват опора на устойчивите и сплотени общества. Чрез **съюза на уменията** и **Плана за действие за интеграция и приобщаване** Съюзът ще работи, за да помогне на хората да повишат устойчивостта си срещу невярната информация и дезинформацията, радиакализацията и вербуването за престъпни цели.

Защитата на децата от всички форми на насилие, включително престъпления, физическо или психическо насилие както онлайн, така и офлайн, е основна цел на ЕС. За да отговори на специфичните нужди на особено уязвимите групи, като например децата, които са все по-изложени на вербуване и радикализация, сприятеляване с цел сексуална злоупотреба и сексуално насилие над деца, кибертормоз, дезинформация и други заплахи, ЕС ще разработи **план за действие за защита на децата от престъпления**, обхващащ онлайн и офлайн измеренията. С него ще бъде начертан съгласуван и координиран подход въз основа на наличните рамки и инструменти, включително бъдещия Център на ЕС по

[60] https://www.eucpn.org/.

въпросите на сексуалното насилие над деца, и други органи и агенции на ЕС, и ще се предложат начини за постигане на напредък там, където все още има пропуски.

Разбиване на престъпните мрежи и техните способстващи фактори

Борбата с високорисковите престъпни мрежи, техните ръководители и способстващи фактори трябва да се засили. Макар че напоследък се отчитат значителни успехи[61], остарелите правила и непоследователните определения на престъпните мрежи възпрепятстват ефективната реакция на наказателното правосъдие и трансграничното сътрудничество. Комисията ще преразгледа остарялото законодателство в тази област, като предложи обновена **правна рамка относно организираната престъпност** с цел засилване на отговора на това явление.

Административното правоприлагане може да допълва съдебното правоприлагане с цел постигане на по-бързи резултати — както показват Европейската прокуратура и Европейската служба за борба с измамите (OLAF) в борбата с **трансграничните измами и престъпленията срещу финансовите интереси на ЕС**. Измамниците със субсидии се съсредоточават върху сектори като възобновяемата енергия, научноизследователските програми и селскостопанския сектор[62]. Комисията ще проучи начини за координиране на използването на наказателноправни и административни инструменти, като засили сътрудничеството с Европол, Евроюст и Европейската прокуратура. Комисията също така ще продължи да подкрепя по-широкото прилагане на **административния подход** за оправомощаване на местните и други административни органи да предотвратяват проникването на престъпни елементи.[63]

ЕС работи за укрепване на правната си рамка за борба с **корупцията**[64]. Европейският парламент и Съветът следва бързо да приключат преговорите по актуализираната рамка за борба с корупцията, предложена от Комисията. Комисията ще представи стратегия на ЕС за борба с корупцията с цел насърчаване на почтеността и засилване на координацията между всички съответни органи и заинтересовани страни в тази област.

Огнестрелните оръжия са ключов фактор за нарастващото насилие, извършвано от организирани престъпни групи. Комисията ще предложи общи наказателноправни стандарти относно незаконния трафик на огнестрелни оръжия. Новият **План за действие на ЕС относно трафика на огнестрелни оръжия** ще се съсредоточи върху защитата на законния пазар, ограничаването на престъпните дейности въз основа на по-добро разузнаване и укрепването на международното сътрудничество със специален акцент върху Украйна и Западните Балкани.

Незаконно търгуваните пиротехнически изделия, използвани в престъпления, изискват мерки за подобряване на превенцията и проследимостта. Понастоящем Комисията извършва оценка на Директивата за пиротехническите изделия и ще обмисли и **наказателни санкции за трафик на пиротехнически изделия**.

---

[61] Включително скорошни случаи на Европейската мултидисциплинарна платформа за борба с криминални заплахи.

[62] https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf.

[63] https://administrativeapproach.eu/sites/default/files/page/files/eu-jha-council-9-10-june-conclusions-administrative-approach-org-crime.pdf.

[64] Предложение за Директива на Европейския парламент и на Съвета относно борбата с корупцията, за замяна на Рамково решение 2003/568/ПВР на Съвета и на Конвенцията за борба с корупцията, в която участват длъжностни лица на Европейските общности или длъжностни лица на държавите — членки на Европейския съюз, и за изменение на Директива (ЕС) 2017/1371 на Европейския парламент и на Съвета, COM(2023) 234 final, Брюксел, 3.5.2023 г.

Проследяване на парите

Проследяването на парите е от решаващо значение за борбата с организираната престъпност и тероризма, но при все това продължава да е изпълнено с трудности. Връзката между организираната престъпност и паричните потоци изисква интензивни и комбинирани усилия за спиране на достъпа на престъпните мрежи до източници на финансиране и за по-добра защита на хората, предприятията и публичните бюджети.

ЕС укрепи усилията си с новите правила за борба с изпирането на пари, включително създаването на **Органа на ЕС за борба с изпирането на пари (ОБИП)**[65]. Сътрудничеството между ОБИП, OLAF, Европейската прокуратура, Евроюст и Европол е от съществено значение за провеждането на ефективни финансови разследвания. Комисията ще подкрепи създаването на **партньорства** както такива с цел улесняване на междуведомственото сътрудничество, така и партньорства с участието на частния сектор.

За да се елиминират финансовите мотиви, стоящи зад организираната престъпност, изземването на активите и конфискацията на печалбите от престъпна дейност са от съществено значение. Наскоро приетите по-строги правила относно **отнемането и конфискацията на активи**[66] следва да бъдат транспонирани незабавно от държавите членки и да бъдат използвани в пълния им потенциал. Борбата с паралелните финансови системи, заобикалящи рамката на ЕС за борба с изпирането на пари, включително системите, основани на криптоактиви, също изисква иновативни действия, споделяне на най-добри практики между държавите членки и по-голяма подкрепа от страна на Европол и Евроюст. Комисията ще проучи осъществимостта на нова общоевропейска система за проследяване на печалбите от организираната престъпност и финансирането на тероризма и също така ще насърчава навременните и разширени информационни потоци от **звената за финансово разузнаване** към правоприлагащите органи. Комисията ще проучи начини за отстраняване на пропуските, ще подкрепи държавите членки при изграждането на капацитет и ще продължи да работи за засилване на сътрудничеството с трети държави, с които престъпниците злоупотребяват за операции по нелегално банкиране.

Борба с тежките престъпления

Освен разбиването на престъпните мрежи, целенасочени усилия са необходими за справянето с тежките престъпления. За да се укрепи способността ни за борба с **онлайн измамите**, които причиняват много значителни финансови вреди[67], Комисията ще подкрепя мерки за превенция и по-ефективни действия по правоприлагане и ще работи с държавите членки и заинтересованите страни за подкрепа и защита на жертвите, включително чрез подпомагане при възстановяването на загубените им средства. Тези усилия ще бъдат формализирани в **план за действие относно онлайн измамите**.

По отношение на борбата със **сексуалното насилие над деца**[68] Комисията ще подкрепи съзаконодателите при финализирането на двете законодателни предложения[69] за предотвратяване и борба със сексуалното насилие над деца онлайн и за повишаване на ефективността на действията по правоприлагане, насочени срещу сексуалното насилие над деца и тяхната сексуална експлоатация. С действащи временни правила до април

[65] https://www.amla.europa.eu/index_en.
[66] Директива (ЕС) 2024/1260 на Европейския парламент и на Съвета от 24 април 2024 г. относно възстановяването и конфискацията на активи (ОВ L, 2024/1260, 2.5.2024 г.).
[67] Global Anti-Scam Report 2024.
[68] COM (2020) 607 final
[69] COM (2022) 209 final и COM (2024) 60 final.

2026 г., от съществено значение е да се създаде постоянна правна рамка и Комисията насърчава съзаконодателите да започнат преговори по проекта на регламент за определяне на правила за предотвратяване и борба със сексуалното насилие над деца. Съзаконодателите се приканват също така да постигнат напредък в преговорите по Директивата относно борбата със сексуалното насилие над деца и сексуалната експлоатация на деца, както и с материалите, съдържащи сексуално насилие над деца, с която ще се установят минимални правила относно определянето на престъпленията и санкциите в областта на сексуалната експлоатация на деца.

Половината от най-опасните престъпни мрежи в ЕС са замесени в **трафик на наркотици**, свързан с насилие. Въпреки че неотдавна ЕС засили борбата си с това престъпление[70], по-специално чрез разширяване на мандата на **Агенцията на ЕС по наркотиците**, са необходими допълнителни действия. Комисията ще работи в тясно сътрудничество с държавите членки, за да предложи нова **стратегия на ЕС за борба с наркотиците**. Тя също така ще преразгледа **правната рамка относно прекурсорите на наркотични вещества** и ще предложи **план за действие на ЕС срещу трафика на наркотици** с цел нарушаване на маршрутите и бизнес моделите**. Публично-частното партньорство на Европейския пристанищен алианс** за засилена защита на пристанищата ще бъде разширено, за да включи по-малките и вътрешните пристанища и да гарантира прилагането на правилата за морска сигурност. Като отчита тежките последици от трафика на наркотици на местно равнище, Комисията ще продължи да подкрепя балансирана, основана на доказателства и мултидисциплинарна политика в областта на наркотиците с готовност за внезапно заливане на пазара с наркотици, особено със синтетични опиоиди.

За да се бори с експлоатацията на хора, ЕС прие нови правила[71] и ще въведе **обновена стратегия на ЕС за борба с трафика на хора** (2026—2030 г.), обхващаща всички етапи от превенцията до наказателното преследване, с акцент върху подкрепата за жертвите както на равнището на ЕС, така и на международно равнище.

В борбата с **контрабандата на мигранти** Комисията ще ръководи усилията с ключови партньори чрез новия Световен алианс за борба с контрабандата на мигранти, в сътрудничество с Европол, Евроюст и Frontex, включително в онлайн пространството. Предложенията на Комисията относно борбата с контрабандата[72] следва да бъдат приети и приложени незабавно. Освен това, след приемането на **инструментариума за транспортните оператори**[73], Комисията увеличи контактите с чуждестранни органи и оператори и ще продължи да работи с авиационния сектор и организациите за гражданско въздухоплаване[74] с цел повишаване на осведомеността относно контрабандата на мигранти по въздуха[75].

Престъпленията срещу околната среда застрашават околната среда, общественото здраве и икономиките в дългосрочен план. Комисията ще подкрепя държавите членки

[70] COM/2023/641 final.

[71] Директива (ЕС) 2024/1712 от 13 юни 2024 г. за изменение на Директива 2011/36/ЕС относно предотвратяването и борбата с трафика на хора и защитата на жертвите от него (ОВ L, 2024/1712, 24.6.2024 г.).

[72] COM (2023) 755 final и COM (2023) 754 final.

[73] Инструментариум за противодействие на използването на търговски транспортни средства за улесняване на незаконната миграция към ЕС.

[74] Включително Международната организация за гражданско въздухоплаване (ИКАО).

[75] Комисията също така ще подкрепи финализирането на Регламента относно мерки срещу превозвачите, които улесняват трафика на хора или незаконното превеждане през граница на мигранти, COM(2021) 753 final.

при прилагането на Директивата относно престъпленията срещу околната среда[76] и ще подкрепя оперативните мрежи и действия в тази област[77]. Енергичното правоприлагане е от основно значение. В допълнение наскоро приетата Конвенция на Съвета на Европа за опазване на околната среда чрез наказателното право[78] ще спомогне да се гарантират силни и сравними усилия за борба с престъпленията срещу околната среда както в Европа, така и извън нея.

Наказателноправните действия в отговор на престъпленията

Престъпността и тероризмът могат да окажат въздействие върху всички, поради което е от съществено значение да се подкрепят и защитават правата на **жертвите**, за да се намалят вредите и да се повиши цялостната сигурност и доверие в органите. Въз основа на Директивата за правата на жертвите Комисията ще въведе нова **стратегия на ЕС за правата на жертвите**.

Системите на ЕС за наказателно правосъдие се нуждаят от ефективни инструменти за справяне с възникващите заплахи. За да се постигне това, Комисията стартира **форум на високо равнище относно бъдещето на наказателното правосъдие на ЕС**. Този форум обединява държавите членки, Европейския парламент, агенциите и органите на ЕС и други заинтересовани страни. Неговата цел е да се обсъдят начини да се гарантира, че нашите системи за наказателно правосъдие продължават да бъдат ефективни, справедливи и устойчиви на променящите се предизвикателства, като същевременно се укрепва съдебното сътрудничество и се засилва взаимното доверие, включително чрез цифровизация[79].

Ключови действия

Комисията:

- **ще представи през 2026 г. законодателно предложение за осъвременяване на правилата относно организираната престъпност;**
- **ще представи през 2025 г. законодателно предложение за преразглеждане на правната рамка относно прекурсорите на наркотични вещества;**
- **ще представи през 2025 г. законодателно предложение за общи наказателноправни стандарти относно незаконния трафик на огнестрелни оръжия;**
- **ще направи оценка на необходимостта от преразглеждане на директивите относно пиротехническите изделия и взривните вещества за граждански цели;**
- **ще направи оценка на необходимостта от по-нататъшно укрепване на европейската заповед за разследване и европейската заповед за арест;**
- **ще представи през 2026 г. нова стратегия на ЕС за борба с трафика на хора;**
- **ще представи през 2026 г. нова стратегия на ЕС за правата на жертвите;**

[76] Директива (ЕС) 2024/1203 на Европейския парламент и на Съвета от 11 април 2024 г. относно защитата на околната среда чрез наказателно право (ОВ L 2024/1203, 30.4.2024 г.).

[77] Мрежа на ЕС за прилагане и спазване на правото в областта на околната среда (IMPEL), Европейска мрежа на прокурорите за околната среда (ENPE), EnviCrimeNet и Форум на съдиите на ЕС за околната среда (EUFJE).

[78] Комитет от експерти по опазване на околната среда чрез наказателното право (PC-ENV) — Европейски комитет по проблемите на престъпността.

[79] По-специално чрез създаването на комуникация в областта на електронното правосъдие посредством онлайн обмен на данни (eCODEX) и Европейска информационна система за съдимост — граждани на трети държави (ECRIS-TCN).

- **ще представи до 2027 г. план за действие на ЕС за защита на децата от престъпления;**
- **ще представи през 2025 г. план за действие на ЕС срещу трафика на наркотици;**
- **ще представи през 2026 г. план за действие на ЕС срещу трафика на огнестрелни оръжия;**
- **ще разширява последователно Европейския пристанищен алианс от 2025 г. нататък;**
- **ще приеме през 2026 г. насоки за Законодателния акт за цифровите услуги относно защитата на малолетните и непълнолетните лица;**
- **ще представи през 2026 г. план за действие на ЕС срещу кибертормоза.**

Държавите членки се приканват:

- **да транспонират изцяло до края на 2026 г. новите правила относно отнемането и конфискацията на активи и да ги използват в пълния им потенциал;**
- **да прилагат административния подход в борбата срещу проникването на престъпни елементи;**
- **да създават публично-частни партньорства срещу изпирането на пари;**
- **да транспонират и да прилагат изцяло Директивата за превенция и борба с насилието над жени и домашното насилие.**

Европейският парламент и Съветът се приканват:

- **да постигнат напредък в преговорите по Регламента за определяне на правила за предотвратяване и борба със сексуалното насилие над деца и Директивата относно борбата със сексуалното насилие и сексуалната експлоатация на деца, както и с материалите, съдържащи сексуално насилие над деца;**
- **да приключат преговорите по Директивата относно борбата с корупцията.**

6. Борба с тероризма и насилническия екстремизъм

Ще въведем всеобхватна програма за борба с тероризма с цел предотвратяване на радикализацията, гарантиране на сигурни онлайн и обществени пространства, както и ответни действия на евентуални атаки.

Равнището на заплахата от тероризъм в ЕС продължава да е високо. То е тясно свързано със страничните ефекти от геополитическите събития, новите технологии и новите средства за финансиране на тероризма. Трябва да гарантираме, че ЕС е добре подготвен да предвижда заплахите, да предотвратява радикализацията (както офлайн, така и онлайн), да защитава гражданите и обществените пространства от нападения и да реагира ефективно на евентуални нападения. През 2025 г. ще бъде представена **нова програма на ЕС за предотвратяване и борба с тероризма и насилническия екстремизъм**, в която ще бъдат очертани бъдещите действия на ЕС. В съответствие с новата програма през 2025 г. ЕС и Западните Балкани ще подпишат новия **съвместен план за действие** за предотвратяване и борба с тероризма и насилническия екстремизъм.

Предотвратяване на радикализацията и защита на хората онлайн

Подобно на борбата с организираната престъпност, борбата с тероризма и насилническия екстремизъм започва със **справяне с първопричините за тях**. **Центърът за знания на ЕС за предотвратяване на радикализацията** ще засили подкрепата си за специалистите и създателите на политики с нов **всеобхватен инструментариум за**

превенция, така че да се даде възможност за ранно идентифициране и интервенции, насочени към уязвимите лица, по-специално малолетните и непълнолетните**.** Радикализацията често се случва в затворите и за да подкрепи държавите членки при решаването на този въпрос, Комисията ще издаде нови препоръки.

Терористичните и насилствените екстремисти използват онлайн платформи, за да разпространяват терористично и вредно съдържание, да събират средства и да вербуват. Уязвимите потребители, особено малолетните и непълнолетните, биват радикализирани онлайн с тревожни темпове. **Регламентът относно терористичното съдържание онлайн** изигра важна роля в борбата с разпространението на терористично съдържание онлайн, като даде възможност за бързото премахване на най-жестокия и опасен материал[80]. Понастоящем Комисията извършва оценка на функционирането на регламента и ще прецени как най-добре да се укрепи неговата уредба.

Протоколът на ЕС за действие при кризи, предназначен за съвместни и бързи ответни действия на правоприлагащите и технологичните сектори във връзка с терористична атака, ще бъде изменен, за да се гарантира възможност за разрастване и гъвкавост на отговора на увеличаващото се онлайн измерение на терористичните нападения. Интернет форумът на ЕС ще продължи да бъде основната платформа за доброволно сътрудничество с технологичния сектор за борба с терористичното и вредното онлайн съдържание. Освен това Комисията участва в международни инициативи, като фондацията „Призив след Крайстчърч“ и Глобалния интернет форум за борба с тероризма.

Борба с финансирането на тероризма

Терористите финансират дейностите си с кампании за колективно финансиране, криптоактиви, необанки или платформи за онлайн плащания. Правоприлагащите органи трябва да разкриват и разследват тези финансови потоци. Това изисква средства, инструменти и експертен опит. **Мрежата на финансовите следователи в областта на борбата с тероризма** играе ключова роля. Комисията ще проучи възможността за създаване на **нова общоевропейска система за проследяване на финансирането на тероризма**, обхващаща трансакции в рамките на ЕС и SEPA, прехвърляне на криптоактиви, онлайн и електронни плащания, която да допълва Споразумението между ЕС и САЩ относно Програмата за проследяване на финансирането на тероризма (ППФТ).

Бюджетът на ЕС трябва да бъде **защитен от злоупотреби, с които се насърчават радикални/екстремистки възгледи** в държавите членки. В преразгледаният **Финансов регламент** сред основанията за изключване от финансиране от ЕС вече е включена и присъда за „подбуждане към дискриминация, омраза или насилие“. Комисията ще продължи да проучва най-добрия начин за пълноценно използване на инструментариума, включително при подбора на потенциални бенефициери. Защитата на бюджета на ЕС зависи и от тясното сътрудничество и обмена на информация с националните органи, агенциите и органите на ЕС.

Защита от нападения

Освен инвестициите в предотвратяването на радикализацията, важен елемент от защитата на гражданите е ограничаването на средствата за извършване на нападения от

[80] До 31 декември 2024 г. са издадени 1426 заповеди за премахване с цел отстраняването на терористично съдържание или блокирането на достъпа до него, по-голямата част от които са насочени срещу джихадистко терористично съдържание, но също и срещу дясно терористично съдържание.

терористи и престъпници. Необходими са действия както спрямо инструментите, използвани от терористите, така и за защита от нападение на евентуалните цели.

В допълнение към действията по отношение на огнестрелните оръжия Комисията **ще преразгледа и правилата** относно **прекурсорите на взривни вещества**, за да включи високорисковите химикали. **Обществените пространства** продължават да бъдат най-често избираните цели за терористични нападения, особено за самотните извършители. За да се защитят гражданите от вреди, **консултативната програма на ЕС за защита на сигурността** ще бъде укрепена, за да се извършват оценки на уязвимостта на обществени пространства, критична инфраструктура и високорискови събития по искане на държавите членки и с финансиране от бюджета на ЕС по линия на фонд „Вътрешна сигурност“. ЕС ще се стреми да увеличи наличното финансиране за защита на обществените пространства. Комисията предлага подкрепа на органите на държавите членки и частните оператори чрез специални насоки и инструменти, например Центъра за знания относно защитата на обществените пространства[81], като от 2020 г. насам вече са предоставени 70 милиона евро в подкрепа на защитата на обществените пространства.

Комисията също така ще проучи въвеждането на изисквания към организациите да обмислят или да прилагат мерки за сигурност на публично достъпни места чрез взаимодействие с местните органи и частни партньори.

Като се имат предвид очевидните уязвимости, **стратегията на ЕС за борба с антисемитизма и подкрепа на еврейския живот (2021—2030 г.)** ще продължи да направлява действията на Комисията за защита на еврейската общност. Комисията също така ще гарантира, че са налице подходящи инструменти в подкрепа на държавите членки в борбата с **омразата срещу мюсюлманите**.

Използването на **безпилотни летателни апарати** за шпионаж и атаки представлява все по-голямо предизвикателство за сигурността. Комисията ще разработи **хармонизирана методика за изпитване на системите за противодействие на безпилотни летателни апарати**, ще създаде **център за високи постижения в борбата с безпилотните летателни апарати** и ще прецени необходимостта от хармонизиране на законите и процедурите на държавите членки[82].

Чуждестранни бойци терористи

За да се идентифицират чуждестранните бойци терористи, които се завръщат или влизат на външните граници на ЕС, са необходими данни за лицата, представляващи терористична заплаха. За тази цел Комисията, заедно с Европол, ще засили **сътрудничеството си с ключови трети държави за придобиване на биографични и биометрични данни за лица, които биха могли да представляват терористична заплаха**, включително чуждестранни бойци терористи, като след това данните могат да бъдат въведени в Шенгенската информационна система в пълно съответствие с приложимите правни рамки на ЕС и национални правни рамки. Ето защо от решаващо значение е държавите членки да използват всички съществуващи инструменти. Това включва въвеждане на цялата необходима информация в **ШИС**, подобряване на биометричните проверки и извършване на задължителни систематични проверки на всички лица по външните граници на ЕС[83]. Освен това разработените от Frontex **общи показатели за риска** ще продължат да подкрепят органите за граничен контрол на

[81] Център за знания относно защитата на обществените пространства.

[82] Като продължение на набора от ключови действия, посочени в Съобщението относно борбата със заплахите от безпилотни летателни апарати от 2023 г., COM(2023) 659 final.

[83] При пълно спазване на Кодекса на шенгенските граници и Регламента за скрининга.

държавите членки при установяването и оценката на риска от подозрителни пътувания на потенциални чуждестранни бойци терористи.

В допълнение, за да се гарантира, че държавите членки поддържат достъп до **доказателствата от бойното поле**, събрани от разследващия екип на ООН за насърчаване на отчетността за престъпления, извършени от Даиш/ИДИЛ (UNITAD), за наказателното преследване на чуждестранни бойци терористи, Комисията, заедно с Евроюст, ще направи оценка на възможността за съхраняване на тези доказателства в базата данни на Евроюст с доказателства за основни международни престъпления. Към това новият европейски **съдебен регистър за борба с тероризма** ще продължи да подкрепя съдебните системи на държавите членки при бързото идентифициране на трансграничните връзки по дела за тероризъм.

Ключови действия

Комисията:

- **ще приеме нова програма на ЕС за предотвратяване и борба с тероризма и насилническия екстремизъм;**
- **ще подпише през 2025 г. нов съвместен план за действие за предотвратяване и борба с тероризма и насилническия екстремизъм със Западните Балкани;**
- **ще разработи с Центъра на ЕС за знания нов всеобхватен инструментариум за превенция;**
- **ще направи през 2026 г. оценка на прилагането на Регламента относно терористичното съдържание онлайн;**
- **ще измени през 2025 г. Протокола на ЕС при кризи;**
- **ще представи през 2026 г. законодателно предложение за преразглеждане на правната рамка относно прекурсорите на наркотични вещества;**
- **ще проучи възможността за нова общоевропейска система за проследяване на финансирането на тероризма.**

Държавите членки се приканват:

- **да подобрят биометричните проверки и да извършват задължителни систематични проверки по външните граници на ЕС;**
- **да използват пълноценно Европейския съдебен регистър за борба с тероризма.**

7. ЕС като силен глобален фактор в областта на сигурността

За да повишим сигурността на ЕС, ще засилим оперативното сътрудничество чрез партньорства с ключови региони, като например нашите партньори — обхванатите от процеса на разширяване и по съседство, Латинска Америка и Средиземноморския регион. Интересите на ЕС в областта на сигурността ще бъдат вземани предвид в международното сътрудничество, включително чрез използване на средствата и инструментите на ЕС.

Последните години показаха неразривните връзки между външната и вътрешната сигурност на ЕС. Агресивната война на Русия срещу Украйна, конфликтът в Газа, положението в Сирия и възникващите конфликти по света имат сериозни последици, засягащи вътрешната сигурност на ЕС. За да се неутрализира въздействието на глобалната нестабилност върху вътрешната си сигурност, **ЕС трябва активно да защитава интересите си** в областта на сигурността, като се справя с външните заплахи,

прекъсва маршрутите за трафик и защитава коридорите от стратегически интерес, като например търговските маршрути. Едновременно с това ЕС ще продължи да бъде силен съюзник на държавите партньори, с които работи съвместно за повишаване на глобалната сигурност и изграждане на взаимна устойчивост срещу заплахи.

През последните години ЕС предприе значителни стъпки за засилване на сътрудничеството си в областта на сигурността. Той сключи оперативни споразумения за правоприлагане и съдебно сътрудничество, както и други видове споразумения с държави партньори. Съюзът работи активно по допълнителни международни споразумения в съответствие с указанията на Съвета за водене на преговори, както и по инициативи за изграждане на капацитет, подпомагани от агенции и органи на ЕС. Инструментът за съседство, сътрудничество за развитие и международно сътрудничество – Глобална Европа също е от решаващо значение за усилването на сигурността заедно с държавите партньори.

Крайъгълен камък на укрепването на глобалната сигурност е **основаният на правила многостранен ред**. Диалозите по въпросите на сигурността, включително тематичните диалози, са решаващи за нарастването на усилията в тази област. Изпълнението на **Стратегическия компас за сигурността и отбраната**, заедно с двустранните и многостранните рамки за сътрудничество, като например споразуменията за стабилизиране и асоцииране и споразуменията за асоцииране, както и сътрудничеството с организации като ООН и НАТО, са от критично значение за разработването на ефективни решения, свързани със сигурността. ЕС ще продължи да играе своята роля в многостранните форуми[84] и ще засили сътрудничеството си със значимите международни и регионални организации и рамки, включително НАТО, Организацията на обединените нации, Съвета на Европа, Интерпол, Г-7, ОССЕ и гражданското общество.

Регионално сътрудничество

Като приоритет продължаването на непоколебимата подкрепа на ЕС за **Украйна** и укрепването на сигурността и устойчивостта на **държавите, обхванати от процеса на разширяване на ЕС**, е политически и геостратегически императив. Подкрепата за сигурността на ЕС следва да върви ръка за ръка с **ускорената интеграция на държавите кандидатки** в **архитектурата за сигурност на ЕС**, успоредно с консолидирането на тяхното регионално сътрудничество. Комисията ще използва политиката на разширяване на ЕС, за да подкрепи капацитета на държавите кандидатки и потенциалните кандидатки за членство в ЕС да реагират на заплахи, за да засили оперативното сътрудничество и обмена на информация и за да гарантира привеждането в съответствие с принципите, законодателството и инструментите на ЕС. Инструментът за предприсъединителна помощ (ИПП III), както и механизмите за Украйна, Молдова и Западните Балкани са изключително важни за укрепването на сигурността както в държавите кандидатки, така и в потенциалните кандидатки.

Освен това ЕС ще интегрира допълнително **съседните партньори** в архитектурата на ЕС за сигурност. Чрез **Новия пакт за Средиземноморието** и предстоящия **стратегически подход към Черно море** Съюзът ще се стреми да продължи да изгражда регионално сътрудничество и двустранни стратегически всеобхватни партньорства в аспекта на сигурността, когато е уместно, с редовни диалози на високо равнище по въпросите на сигурността. Ще бъде засилено оперативното сътрудничество с държави от Северна

[84] Световен форум за борба с тероризма, Световна коалиция срещу Даиш, Световен интернет форум за борба с тероризма (GIFCT), фондация „Призив след Крайстчърч“, Световна коалиция за справяне със заплахите от синтетични наркотици.

Африка, **Близкия изток и Персийския залив**, по специално по отношение на борбата с тероризма, прането на пари, трафика на огнестрелни оръжия и производството и трафика на наркотици, особено каптагон**.**

За да се справи с разрастването на терористичната и престъпната дейност и потенциалното ѝ отражение в **Африка на юг от Сахара**, **по-специално Сахел, Африканския рог и Западна Африка**, ЕС ще засили подкрепата за Африканския съюз, регионалните икономически общности и държавите в региона. В съответствие със Стратегията на ЕС за морска сигурност[85] ЕС ще засили сътрудничеството в **Гвинейския залив, Червено море и Индийския океан** за борба с трафика и пиратството, като подпомага сътрудничеството в рамките на Африка и регионалното сътрудничество и предоставя подкрепа с координираното морско присъствие на ЕС и Центъра за морски анализ и операции (Наркотици) (MAOC-N).

ЕС ще засили оперативното сътрудничество с **Латинска Америка и Карибския басейн** с цел разбиване и наказателно преследване на високорискови престъпни мрежи, както и прекъсване на незаконните дейности и маршрутите за трафик, като укрепва рамките за сътрудничество, например EU-CLASI (Латиноамериканския комитет по вътрешна сигурност) и механизма за координация и сътрудничество в областта на наркотиците между ЕС и Общността на латиноамериканските и карибските държави. Сред приоритетите ще бъдат устойчивостта и партньорствата на логистичните центрове и подходите за проследяване на парите. ЕС ще продължи да подкрепя развитието на Общността на полицейските служби на Северна и Южна Америка (AMERIPOL), за да се превърне тя в регионален еквивалент на Европол и да се засили съдебното сътрудничество между държавите членки и региона. Също така ЕС ще работи с **Южна и Централна Азия** по отношение на общите предизвикателства в областта на сигурността, свързани с тероризма, трафика на незаконни стоки, включително наркотици, трафика на хора и контрабандата на мигранти.

В допълнение ЕС ще подкрепя рамките за регионално сътрудничество в трети държави, за да ги подпомогне допълнително за спирането на незаконния трафик още при източника в съответствие с принципа на споделена отговорност за цялата престъпна верига на доставки. Освен това ЕС ще даде своя принос за укрепване на сигурността на логистичните центрове в чужбина чрез координирането на **съвместните инспекции в пристанищата на трети държави**.

Оперативно сътрудничество

Със стратегията за **Global Gateway** ще се подкрепят устойчиви и висококачествени инфраструктурни проекти в секторите на цифровите технологии, климата и енергетиката, транспорта, здравеопазването, образованието и научните изследвания. Комисията вече ще интегрира съображения за сигурност, когато е уместно, в бъдещите инвестиции по линия на Global Gateway. Това ще включва инициативи, които са от решаващо значение за стратегическата автономност на ЕС и неговите държави партньори, като например инфраструктурни проекти, съдържащи оценки на сигурността и мерки за намаляване на риска.

Комисията ще се стреми към по-нататъшни **споразумения между ЕС и трети държави за сътрудничество с Европол и Евроюст**, по-специално с държавите от Латинска Америка.

[85] JOIN (2023) 8 final.

Освен това проактивното участие на държави извън ЕС в **EMPACT** е едно от най-ефективните средства за укрепване на оперативното сътрудничество. ЕС ще продължи да насърчава участието в тази рамка на трети държави, по-специално Западните Балкани, Източното съседство, Африка на юг от Сахара, Северна Африка, Близкия изток, Латинска Америка и Карибския басейн. Друг инструмент за засилване на сътрудничеството с трети държави в борбата с престъпността са оперативните работни групи между държавите членки, които са координирани от Европол, като в тях могат да участват и трети държави. Комисията има за цел също така да приключи преговорите по международното споразумение между **ЕС и Интерпол**[86], което гарантира по-единен подход към глобалните заплахи за сигурността и е насочено против транснационалните престъпления.

Съюзът трябва да присъства на място в рамките на подхода „Екип Европа“. Специализираният персонал на Съюза и на държавите членки играе решаваща роля, за да се гарантира, че външната дейност на Съюза е добре информирана, координирана и бързо реагираща. За да издигне този подход на по-високо равнище, Комисията, с подкрепата на върховния представител по въпросите на външните работи и политиката на сигурност, ще укрепи **мрежите за връзка** и ще улесни разполагането на **регионални служители за връзка на Европол и Евроюст** в съответствие с оперативните нужди на държавите членки.

ЕС ще се стреми към по-тясно оперативно сътрудничество в областта на правоприлагането и съдебните системи, както и ще насърчава обмена на информация в реално време и съвместните операции чрез **съвместни екипи за разследване** в трети държави с подкрепата на Европол и Евроюст. Комисията също така ще подкрепя държавите членки при създаването на **съвместни центрове за термоядрен синтез**, които обединяват експерти и местни правоприлагащи органи в стратегически трети държави.

Инструменти на Общата външна политика и политика на сигурност (ОВППС)

Мисиите по линия на общата политика за сигурност и отбрана (ОПСО) също ще бъдат използвани в пълния им потенциал за по-добро идентифициране и справяне с външните заплахи за вътрешната сигурност на ЕС в съответствие с техните мандати, определени от Съвета. За да се изгради капацитетът на трети държави, върховният представител по въпросите на външните работи и политиката на сигурност и Комисията ще подкрепят действията по линия на ОПСО със специални инструменти за финансиране и ще проучат всички подходящи начини за финансиране.

Ограничителните мерки на ЕС са утвърден инструмент на ОВППС, използван и за борбата с тероризма. Въз основа на предложения от върховния представител по въпросите на външните работи и политиката на сигурност, държавите членки или Комисията Съветът би могъл да прецени как съществуващите автономни ограничителни мерки на ЕС (антитерористичния списък на ЕС) биха могли да бъдат направени по-ефективни, оперативни и гъвкави. Освен това те биха могли да обмислят проучване на допълнителни ограничителни мерки, насочени срещу престъпните мрежи, в съответствие с целите на ОВППС.

Визова политика и обмен на информация

Визовата политика на ЕС е ключов инструмент за сътрудничество с трети държави и за гарантиране на сигурността на нашите граници чрез контролиране на влизането в ЕС и

[86] Решение (ЕС) 2021/1312 на Съвета от 19 юли 2021 г. и Решение (ЕС) 2021/1313 на Съвета от 19 юли 2021 г.

определяне на условията за това. Комисията ще интегрира изцяло **съображенията за сигурност във визовата политика на ЕС** чрез предстояща стратегия за визовата политика на ЕС. Комисията ще работи със съзаконодателите за приемане на предложението за преразглеждане и рационализиране на механизма за суспендиране на безвизовия режим, особено за конкретни случаи на злоупотреба с безвизовия режим[87]. Третите държави ще бъдат насърчавани да обменят информация за лица, които могат да представляват заплаха за сигурността, която ще бъде въведена в информационните системи и базите данни на ЕС.

За да се постигне координация на политиките и усилия нагоре по веригата, като така се разгърне по-ефикасно, бързо и безпроблемно сътрудничество, Комисията ще работи за установяване на **договорености за потока от данни** и ще проучи начини за **подобряване на обмена на информация** за целите на правоприлагането и управлението на границите с надеждни трети държави в съответствие с основните права и правилата за защита на данните.

Ключови действия

Комисията:

- **ще сключи международни споразумения между ЕС и приоритетни трети държави за сътрудничество с Европол и Евроюст;**
- **ще насърчава участието на държавите партньори в EMPACT за борба с организираната престъпност и тероризма;**
- **ще подпомага агенциите и органите на ЕС при установяването и укрепването на работни договорености с държавите партньори;**
- **ще отчете допълнително съображенията за сигурност във визовата политика на ЕС чрез предстоящата визова стратегия;**
- **ще засили обмена на информация с надеждни трети държави за целите на правоприлагането и управлението на границите.**

Комисията, в сътрудничество с върховния представител по въпросите на външните работи:

- **ще използва пълноценно гражданските мисии по линия на общата политика за сигурност и отбрана (ОПСО);**
- **ще координира съвместни инспекции в пристанища на трети държави до 2027 г.**

Комисията, в сътрудничество с върховния представител по въпросите на външните работи:

- **ще укрепва мрежите за връзка и сътрудничеството в рамките на подхода „Екип Европа“;**
- **ще създаде съвместни оперативни екипи и центрове за ядрен синтез в трети държави от 2025 г. нататък;**

Европейският парламент и Съветът се приканват:

- **да приключат преговорите по преразглеждането на механизма за суспендиране на безвизовия режим.**

[87] COM (2023) 642.

8. Заключение

В свят на несигурност е необходимо да се повиши капацитетът на Съюза за предвиждане, предотвратяване и реагиране на заплахи за сигурността.

Не е достатъчно да се реагира на кризи едва когато те възникнат. Трябва да повишим осведомеността си с пълна картина на заплахите в хода на тяхното развитие. Както и да гарантираме, че нашите инструменти и способности отговарят на задачата.

Цялостният набор от мерки, описани подробно в настоящата стратегия, ще спомогне за създаването на по-силен Съюз в този свят: Съюз, който е в състояние да предвижда, да планира и да се грижи за собствените си нужди в областта на сигурността, който може да реагира ефективно на заплахите за вътрешната си сигурност и да търси отговорност от извършителите, както и да защитава своите отворени, свободни и просперираща общества и демокрации.

Това изисква промяна в нагласата ни. Ще работим за насърчаването на нова култура на сигурност на ЕС, съгласно която съображенията за сигурност се вземат предвид във всички наши законодателни актове, политики и програми — от самото начало до изпълнението им. Култура, в която сътрудничеството между различните области на политиките ни позволява да реализираме нови възможности.

Това не е задача само на една институция, правителство или действащо лице. Това е общ стремеж на Европа.