



ВЪРХОВЕН ПРЕДСТАВИТЕЛ
НА СЪЮЗА ПО ВЪПРОСИТЕ
НА ВЪНШНИТЕ РАБОТИ И
ПОЛИТИКАТА НА СИГУРНОСТ

Брюксел, 19.7.2017 г.
JOIN(2017) 30 final

СЪВМЕСТЕН ДОКЛАД ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

**относно изпълнението на Съвместната рамка за борба с хибридните заплахи —
ответни действия на Европейския съюз**

1. ВЪВЕДЕНИЕ

ЕС е изправен пред едно от най-големите предизвикателства за сигурността в своята история. Заплахите във все по-голяма степен приемат неконвенционални форми: някои заплахи са физически, като например новите форми на тероризъм, докато други се изразяват в използването на цифровото пространство за сложни кибератаки. Съществуват и не толкова ясно забележими заплахи, които са насочени към оказване на натиск, включително дезинформационни кампании и манипулиране на медиите. Те целят подкопаването на основни европейски ценности, като зачитането на човешкото достойнство, свободата и демокрацията. Неотдавнашните координирани кибератаки в целия свят, разкриването на извършителите на които се оказва много трудно, показва уязвимостта на нашите общества и институции.

През април 2016 г. Европейската комисия и върховният представител приеха Съвместно съобщение относно борбата с хибридните заплахи¹ (съвместната рамка). Като се отчита трансграничният и сложен характер на хибридните заплахи, с тази рамка се предлага подход, който обхваща всички нива на управление, за укрепване на цялостната устойчивост на нашите общества. Съветът² приветства инициативата и предложените действия и прикани Комисията и върховния представител да докладват за напредъка през юли 2017 г. ЕС може да оказва съдействие на държавите членки за изграждане на устойчивост срещу хибридните заплахи, но основната отговорност се носи от държавите членки, доколкото борбата с хибридните заплахи е свързана с националната сигурност и отбрана.

Тази съвместна рамка за борба с хибридните заплахи представлява важна част от цялостния по-интегриран подход на ЕС към сигурността и отбраната. Тя допринася за създаването на една Европа, която гарантира закрила, както призова председателят Юнкер в речта за състоянието на Съюза през септември 2016 г. През 2016 г. Европейският съюз също така положи основите за изграждането на по-силна европейска отбранителна политика в отговор на очакванията на гражданите за по-добра защита. В Глобалната стратегия за външната политика и политиката на сигурност на Европейския съюз³ подробно бе изложена необходимостта от интегриран подход за обвързване на вътрешната устойчивост с външната дейност на ЕС и бе отправен призив за единодействие между отбранителната политика и политиките за вътрешния пазар, промишлеността, правоприлагането и разузнавателните служби. След приемането през ноември 2016 г. на Европейския план за действие в областта на отбраната Комисията представи конкретни инициативи, които ще допринесат за укрепването на капацитета на ЕС за реагиране на хибридните заплахи чрез подпомагане на устойчивостта на веригите за доставки в областта на отбраната и укрепване на единния пазар в областта на отбраната. По-специално на 7 юни 2017 г. Комисията стартира Европейския фонд за отбрана с предложено финансиране в размер на 600 млн. евро до 2020 г. и 1,5 млрд. евро годишно в периода след 2020 г. В Съобщението относно Съюза на сигурност⁴ бе

¹ Съвместно съобщение до Европейския парламент и Съвета, озаглавено *Съвместна рамка за борба с хибридните заплахи — ответни действия на Европейския съюз*, JOIN (2016) 18 final.

² *Заключения на Съвета относно борбата с хибридните заплахи*, Съобщение за пресата 196/16, 19 април 2016 г.

³ Представена от върховния представител пред Европейския съвет на 28 юни 2016 г.

⁴ COM(2016) 230 final, 20.4.2016 г.

отчетена необходимостта от противодействие на хибридните заплахи, както и значението на гарантирането на по-голяма съгласуваност между вътрешните и външните действия в областта на сигурността.

Ръководителите на ЕС поставиха сигурността и отбраната на централно място в дебата за бъдещето на Европа⁵. Това беше отразено в Декларацията от Рим от 25 март 2017 г., в която се представя виждането за безопасен и сигурен Съюз, решен да засили своите общи сигурност и отбрана. Председателите на Европейския съвет и на Европейската комисия и генералният секретар на НАТО подписаха съвместна декларация във Варшава на 8 юли 2016 г. с оглед на това да се даде нов тласък и ново съдържание на стратегическото партньорство между ЕС и НАТО. В съвместната декларация бяха посочени седем конкретни области, включително борбата с хибридните заплахи, в които сътрудничеството между двете организации следва да бъде засилено. Впоследствие Съветът на ЕС и Съветът на НАТО одобриха общ набор от 42 предложения за прилагане, а през юни 2017 г. бе изготвен първоначален доклад, показващ наличието на значителен напредък⁶.

В документа за размисъл на Комисията относно бъдещето на европейската отбрана⁷, представен през юни 2017 г., се очертават три различни сценария за това как да се противодейства на нарастващите заплахи в областта на сигурността и отбраната, пред които е изправена Европа, и как да се укрепят собствените способности на Европа в областта на отбраната до 2025 г. И в трите сценария сигурността и отбраната се считат за неразделна част от европейския проект, за да се защитават и утвърждават интересите ни у дома и в чужбина. Европа трябва да се превърне в гарант за сигурността и постепенно да осигури собствената си сигурност. Нито една държава членка не може сама да се справи с предстоящите предизвикателства, и по-специално тези по борбата с хибридните заплахи. Поради това сътрудничеството в областта на отбраната и сигурността въобще не е въпрос на избор, а представлява необходимост за постигане на една Европа, която гарантира закрила.

Целта на настоящия доклад е да се представи отчет за напредъка и да се очертаят следващите стъпки за изпълнение по действията в четирите области, предложени в съвместната рамка: подобряване на ситуационната осведоменост; изграждане на устойчивост; укрепване на способността на държавите членки и на Съюза за предотвратяване и реагиране на кризи и за координирано възстановяване; както и засилване на сътрудничеството с НАТО, за да се гарантира взаимното допълване на мерките. Той следва да се чете във връзка с месечните доклади за напредъка по създаването на ефективен и истински Съюз на сигурност.

⁵ Пътната карта от Братислава на Европейския съвет от 16 септември 2016 г. и Декларацията от Рим на ръководителите на 27 държави членки и на Европейския съвет, Европейския парламент и Европейската комисия от 25 март 2017 г.

⁶ <http://www.consilium.europa.eu/en/press/press-releases/2017/06/19-conclusions-eu-nato-cooperation>

⁷ Документ за размисъл относно бъдещето на европейската отбрана, 7.6.2017 г., https://ec.europa.eu/commission/sites/beta-political/files/reflection-paper-defence_en.pdf

2. РАЗПОЗНАВАНЕ НА ХИБРИДНОТО ЕСТЕСТВО НА ДАДЕНА ЗАПЛАХА

Хибридните дейности стават често срещана характеристика на европейската обстановка в областта на сигурността. Интензивността на тези дейности се увеличава, като нарастват опасенията за намеси в избори, кампании за дезинформация, злонамерени кибернетични дейности и опити на извършителите на хибридни актове да радикализират уязвими членове на обществото, за да изпълняват техните поръчения. Уязвимостта към хибридни заплахи се простира отвъд националните граници. Поради това за хибридните заплахи е необходима координирана ответна реакция на равнището на ЕС и НАТО. Събитията от април 2016 г. насам показват, че макар заплахите все още често да се оценяват поотделно, е налице все по-широко признаване и разбиране в рамките на Съюза на хибридното естество на някои от наблюдаваните дейности и необходимостта от координирани действия. ЕС ще продължи да полага усилия за подобряване на ситуационната осведоменост и сътрудничеството.

***Действие 1:** държавите членки, с подходяща подкрепа от Комисията и върховния представител, се приканват да започнат проучване на хибридните рискове, за да се установят основните потенциално уязвими места на националните и паневропейските структури и мрежи и специфични свързани с хибридните заплахи показатели.*

Съветът създаде група „Приятелите на председателството“, обединяваща експерти от държавите членки с цел извършване на общо проучване, което би им позволило да определят по-добре ключовите показатели за хибридните заплахи, да ги включат в механизмите за ранно предупреждение и съществуващите механизми за оценка на риска и да ги споделят по подходящ начин. Бяха договорени общи условия и работата вече започна. Общото проучване следва да бъде завършено до края на 2017 г., след което да започнат конкретните проучвания. Мерките за защита срещу хибридните заплахи следва взаимно да подсилват действието си. Ето защо държавите членки се приканват да извършат тези проучвания възможно най-бързо, тъй като те ще предоставят ценна информация за степента на уязвимост и подготвеност в цяла Европа.

А. ПОВИШАВАНЕ НА ОСВЕДОМЕНОСТТА

Споделянето на резултатите от работата по анализ и оценка на разузнавателни данни е ключов инструмент за намаляване на несигурността и повишаване на ситуационната осведоменост. През изминалата година бе постигнат значителен напредък. Бяха създадени звеното на ЕС за синтез на информацията за хибридните заплахи, което вече е напълно оперативно, и оперативната група East StratCom, а Финландия учреди Европейския център за борба с хибридните заплахи. Голяма част от работата бе съсредоточена върху анализа на инструментите и механизмите за дезинформация или пропаганда, като е налице добро сътрудничество между оперативната група на ЕС East StratCom, звеното за синтез на информацията за хибридните заплахи и НАТО. Това създава добра основа за доизграждането и по-дълбокото внедряване на културата на анализ и оценка на заплахите за нашата външна и вътрешна сигурност, при което се следи за техните хибридни аспекти.

Звено за синтез на информацията за хибридните заплахи

***Действие 2:** създаване на звено на ЕС за синтез на информацията за хибридните заплахи в рамките на съществуващата структура на Центъра на ЕС за анализ на информация, което да може да получава и анализира класифицирана информация и информация от*

открити източници за хибридните заплахи. Държавите членки се приканват да създадат национални звена за контакт по въпросите на хибридните заплахи, за да се изгради сътрудничество и да се установят сигурни канали за комуникация със звеното на ЕС за синтез на информацията за хибридните заплахи.

Звеното на ЕС за синтез на информацията за хибридните заплахи бе създадено в рамките на Центъра на ЕС за анализ на информация, за да получава и анализира класифицирана информация и информация от открити източници, предоставяна от различни заинтересовани страни, относно хибридните заплахи. След това резултатите от анализа се обменят в рамките на ЕС и между държавите членки и на свой ред залягат в основата на процесите за вземане на решения на ЕС, включително чрез предоставянето на данни за оценките на риска за сигурността, извършвани на равнище ЕС. Дирекция „Разузнаване“ към Военния секретариат на ЕС допринася за работата на звеното за синтез на информация с военен анализ. До момента са изготвени над 50 оценки и брифинги относно хибридните заплахи. От януари 2017 г. насам звеното издава периодичен „Бюлетин относно хибридните заплахи“, в който се анализират актуалните хибридни заплахи и свързани с тях проблеми, и който се споделя директно с институциите и органите на ЕС и националните звена за контакт⁸. Оперативният капацитет на звеното бе постигнат, както беше планирано, през май 2017 г. Накрая, продължава ангажиментът между служителите на звеното за синтез и служителите на новосъздадения в рамките на НАТО клон за анализ на хибридните заплахи както за споделяне на придобития опит във връзка със създаването на звеното за синтез, така и за обмен на информация (осъществяван при пълно спазване на правилата на ЕС за обмен на класифицирана информация). Звеното на ЕС за синтез на информацията за хибридните заплахи понастоящем набелязва по-нататъшни инициативи за подобряване на бъдещото сътрудничество и ще играе ключова роля в паралелните учения на ЕС и НАТО, планирани за есента на 2017 г., при които ще бъде проверена способността за реагиране на това звено и направените изводи ще бъдат взети предвид при по-нататъшните действия.

Стратегическа комуникация

***Действие 3:** върховният представител ще разгледа съвместно с държавите членки начини да се адаптира и координира капацитетът за осигуряване на активна стратегическа комуникация и да се оптимизират мониторингът на медиите и използването на езиковите специалисти.*

В последните месеци се засилиха кампаниите за дезинформация и систематичното разпространение на фалшиви новини в социалните медии е сред широката гама от действия за подкопаване на позициите на противниците. Там където социалните мрежи са предпочитаната платформа, информацията, която изглежда достоверна и легитимна, може да промени общественото мнение в полза на определени лица, организации или правителства. Тези хибридни тактики имат по-широкообхватната цел да се създаде объркване в нашите общества и дискредитиране на нашите демократични правителства и нашите структури, институции и избори. Често фалшивите новини се разпространяват чрез онлайн платформи (вж. също действие 17). Комисията и

⁸ Досега 21 държави членки са определили национални звена за контакт. Това са лица, работещи в столиците на държавите членки в сферата на политиката/устойчивостта.

Върховният представител приветстват неотдавнашните стъпки, предприети от онлайн платформите и издателите на информационни медии, за противодействие на дезинформационните кампании. Комисията ще продължи да насърчава подобни доброволни мерки.

Върховният представител създаде оперативната група East StratCom, която прогнозира случаи и кампании на дезинформация и предприема ответни действия. Това значително подобрява комуникацията относно политиките на Съюза в държавите от източното съседство, като същевременно укрепва медийната среда в тези държави. През последните две години оперативната група разкри над 3000 случая на дезинформация на 18 езика. Предстоящото стартиране на нов уебсайт # *EUvsdisinformation* с възможност за онлайн търсене ще подобри значително достъпа на потребителите. При все това тези изследвания и анализи сочат, че броят на каналите за дезинформация и дезинформационните съобщения, разпространявани всекидневно, е значително по-голям. По проекта EU-STRAT, финансиран по „Хоризонт 2020“, се анализират политиката и медиите в държавите от Източното партньорство.

Върховният представител приканва държавите членки да подкрепят работата на оперативните групи StratCom, за да се противодейства по-ефективно на увеличението на хибридните заплахи. Това ще подпомогне оперативната група за стратегическа комуникация за южното съседство да подобри комуникацията и повишаването на информираността на арабския свят, включително на арабски език, като се разбият някои митове и се установят фактите за Европейския съюз и неговите политики. Взаимодействието с местните журналисти ще спомогне за културното адаптиране на разпространяваните новини. Двете оперативни групи, с подкрепата на звеното на ЕС за синтез на информацията за хибридните заплахи, имат за цел да подпомагат и допълват усилията на държавите членки в тази сфера. Освен това Комисията съфинансира Европейската мрежа за стратегически комуникации — мрежа за сътрудничество на 26 държави членки, чрез която се споделят анализи, добри практики и идеи във връзка с използването на стратегическите комуникации в борбата с насилническият екстремизъм, включително по въпроса за дезинформацията.

Център за високи постижения в борбата с хибридните заплахи

Действие 4: държавите членки се приканват да обмислят създаването на център за високи постижения в областта на борбата с хибридните заплахи.

В отговор на призива за създаване на център за високи постижения през април 2017 г. Финландия учреди Европейския център за борба с хибридните заплахи. Десет държави — членки на ЕС⁹, Норвегия и САЩ са членове, а Европейският съюз и НАТО бяха приканени да оказват подкрепа на управителния съвет¹⁰. Мисията на центъра е да насърчава стратегическия диалог, както и да провежда проучвания и анализи, като работи съвместно със заинтересованите общности, за да се повишат устойчивостта и способността за реагиране с цел подпомагане на борбата с хибридните заплахи. Очаква се центърът също така да служи като място за бъдещи учения за борба с хибридните

⁹ Финландия, Франция, Германия, Латвия, Литва, Полша, Швеция, Обединеното кралство, Естония и Испания.

¹⁰ Центърът е отворен за други държави членки на ЕС и съюзници от НАТО, които желаят да се присъединят.

заплахи. Центърът вече е установил тясно сътрудничество със звеното на ЕС за синтез на информацията за хибридните заплахи и дейностите на двете организации следва взаимно да се допълват. ЕС е в процес на оценка за начините, по които той може да предостави конкретна подкрепа за центъра.

Б. ИЗГРАЖДАНЕ НА УСТОЙЧИВОСТ

Съвместната рамка поставя устойчивостта (напр. на транспорта, комуникациите, енергетиката, финансите или регионалните инфраструктури за сигурност) в центъра на действията на ЕС, за да се окаже отпор на пропагандата и информационните кампании, опитите за подкопаване на стопанската дейност, обществата и икономическите потоци, както и на атаките срещу информационните технологии и инфраструктурата, свързана с киберпространството. В нея се предвижда засилване на устойчивостта като превантивно и възпиращо действие с цел заздравяване на обществата и избягване на ескалация на кризите в рамките на ЕС и извън него. Добавената стойност на ЕС се състои в оказването на помощ на държавите членки и партньорите за изграждане на тяхната устойчивост, разчитайки на широк набор от съществуващи инструменти и програми. Значителен напредък бе постигнат при действията за изграждането на устойчивост в области като киберсигурността, критичната инфраструктура, защитата на финансовата система от незаконна употреба и противодействието на насилническият екстремизъм и радикализацията.

Защита на критичната инфраструктура

Действие 5: в сътрудничество с държавите членки и заинтересованите страни Комисията ще набележи общи инструменти, включително показатели, за подобряване на защитата и устойчивостта на критичната инфраструктура спрямо хибридните заплахи в съответните сектори.

В контекста на Европейската програма за защита на критичната инфраструктура (ЕПЗКИ) Комисията продължи започнатата работа за идентифициране на общи инструменти, включително показатели за уязвимост, с оглед подобряване на устойчивостта на критичната инфраструктура срещу хибридните заплахи в съответните сектори. През май 2017 г. Комисията организира работна среща относно хибридните заплахи за критичната инфраструктура, в която взеха участие почти всички държави членки, оператори на критична инфраструктура, звеното на ЕС за синтез на информацията за хибридните заплахи, както и НАТО в качеството на наблюдател. Бе постигнато съгласие относно обща пътна карта и стъпки за бъдещата работа въз основа на въпросник, изпратен на националните органи в държавите членки. Комисията ще се консултира допълнително със заинтересованите страни през есента с цел да се постигне съгласие относно показателите до края на 2017 г.

Европейската агенция по отбрана работи по набелязването на общи слаби места на способностите и научните изследвания, произтичащи от връзката между енергийните инфраструктури и отбранителните способности. Европейската агенция по отбрана ще разработи концептуален документ през есента на 2017 г., както и пилотни действия за цялостни методологии.

Подобряване на сигурността на енергийните доставки на ЕС

Действие 6: Комисията, в сътрудничество с държавите членки, ще подкрепя усилията за диверсифициране на енергийните източници и ще поощрява възприемането на стандарти за безопасност и сигурност с цел да се повиши устойчивостта на ядрените инфраструктури.

Комисията направи конкретни предложения в пакета за сигурност на доставките през декември 2016 г., а през април 2017 г. Съветът и Европейският парламент постигнаха съгласие относно новия регламент за сигурността на доставките на газ, който цели предотвратяването на кризи в доставките на газ. Новите правила ще осигурят координиран на регионално равнище общ подход на държавите членки към мерките за сигурност на доставките. Това ще постави ЕС в по-добра позиция за подготовка и управление на недостига на газ в случай на криза или хибридно нападение. За първи път ще се прилага принципът на солидарност: държавите членки ще бъдат в състояние да подпомогнат съседите си в случай на сериозна криза или нападение, така че европейските домакинства и предприятия да не бъдат засегнати от прекъсвания в електроснабдяването.

ЕС постигна напредък и в разработването на ключови проекти за диверсифициране на маршрутите и източниците на енергийни доставки в съответствие с Рамковата стратегия за енергийния съюз и Европейската стратегия за енергийна сигурност. Например за южния газов коридор са в ход конкретни строителни работи по всички големи проекти за газопроводи: разширяване на южнокавказкия, трансанадолския и трансадриатическия газопроводи, за добива от находището „Шах Дениз II“, както и разширяване на южния газов коридор към Централна Азия, в частност Туркменистан. Вносът на втечен природен газ (LNG) в Европа се увеличава и произхожда от нови източници, като например САЩ. Примерът на терминала в Литва показва как проектите за разнообразяване могат да намалят зависимостта от един-единствен доставчик. Укрепването на енергийните усилия и по-доброто използване на местни енергийни източници, по-специално възобновяеми енергийни източници, също допринася за диверсификацията на енергийните маршрути и източници.

В областта на ядрената безопасност Комисията активно подкрепя — по-специално чрез работни срещи с националните органи и регулатори — последователното и ефективно прилагане на двете директиви относно ядрената безопасност и основните стандарти за безопасност, които държавите членки са задължени да транспонират до края съответно на 2017 г. и 2018 г. Освен това програмата на Евратом за научни изследвания и обучения допринася за повишаване на ядрената безопасност.

Сигурност на транспорта и веригите за доставки

Действие 7: Комисията ще следи за нововъзникващи заплахи в транспортния сектор и ще актуализира законодателството, когато е целесъобразно. При прилагането на Стратегията на ЕС за морска сигурност и Стратегията на ЕС за управление на риска в областта на митниците и свързания с нея план за действие Комисията и върховният представител, в рамките на съответните им компетенции и в сътрудничество с държавите членки, ще преценят каква да бъде реакцията спрямо хибридните заплахи, по-специално спрямо тези, които засягат критичната транспортна инфраструктура.

В съответствие със Съобщението относно Съюза на сигурност Комисията спомага за оценките на риска за сигурността на равнището на ЕС заедно с държавите членки, Центъра на ЕС за анализ на информация и съответните агенции с цел идентифициране

на заплахи за сигурността на транспорта и подкрепа за разработването на ефективни и пропорционални мерки за ограничаване на риска. Свалянето на самолета на „Малайзия Еърлайнс“ при полет МН17 над Източна Украйна през 2014 г. беше показателно за риска при прелитане над конфликтни зони. В съответствие с препоръките на европейската оперативна група на високо равнище относно конфликтните зони¹¹ Комисията разработи методология за „обща за ЕС оценка на риска“ с подкрепата на националните експерти по въздухоплаването и сигурността и ЕСВД, която дава възможност за обмен на класифицирана информация и определянето на обща картина на риска. През март 2017 г. Европейската агенция за авиационна безопасност (ЕААБ) издаде първия „Информационен бюлетин за конфликтните зони“¹² въз основа на резултатите от посочената обща за ЕС оценка на риска. Комисията обмисля разширяването на дейностите по оценката на риска в областта на авиационната сигурност, за да се обхванат и други видове транспорт (напр. железопътен и морски), и през 2018 г. ще направи предложения. През юни 2017 г. Комисията, ЕСВД и държавите членки предприеха оценка на риска относно сигурността на железопътния транспорт, за да установят евентуални недостатъци и възможни мерки за смекчаване на рисковете.

Значителни усилия в областта на сигурността на въздухоплаването и управлението на въздушното движение (УВД) също бяха направени в рамките на изследователски проекти в областта на сигурността по Седмата рамкова програма и „Хоризонт 2020“. В областта на гражданското въздухоплаване Комисията заедно с Европейската агенция за авиационна безопасност и със заинтересованите страни разработва две нови инициативи за укрепване на киберсигурността, целящи и борба с хибридните заплахи: създаването на екип за незабавно реагиране при компютърни инциденти във въздухоплаването, както и създаването на оперативна група за кибернетична сигурност към Съвместното предприятие за изследване на управлението на въздушното движение в единното европейско небе (SESAR), отговорно за управлението на въздушното движение в единното европейско небе. Европейската агенция по отбрана предоставя военна информация относно кибернетичната сигурност във въздухоплаването на Съвместното предприятие SESAR, както и на Европейската агенция за авиационна безопасност посредством „Европейската платформа за стратегическа координация на кибернетичната сигурност“, която по искане на държавите членки и промишлеността ще подпомага координацията на равнището на ЕС на всички дейности в областта на въздухоплаването. В съответствие с Пътната карта за киберсигурността във въздухоплаването през 2016 г. Европейската агенция за авиационна безопасност направи анализ на недостатъците на съществуващите правила, и по-специално планирането и създаването на Европейския център за кибернетична сигурност във въздухоплаването; последният вече функционира и си сътрудничи с Екипа на ЕС за незабавно реагиране при компютърни инциденти (CERT-EU) (меморандум за разбирателство, подписан през февруари 2017 г.) по изготвянето на анализи на заплахите в областта на въздухоплаването и с Евроконтрол (бе приета пътна карта за сътрудничество), а също така бе разработен и уебсайт за разпространение на анализите от открити източници. До есента на 2017 г. ще бъдат приети програма за стандартизация и сигурен обмен на информация.

Управление на риска в областта на митниците

¹¹https://www.easa.europa.eu/system/files/dfu/208599_EASA_CONFLICT_ZONE_CHAIRMAN_REPORT_no_B_update.pdf

¹²<https://ad.easa.europa.eu/czib-docs/page-1>

По отношение на митниците Комисията се съсредоточава върху значителното модернизиране на системата за предварителна информация за товарите и управлението на риска в областта на митниците. Това обхваща пълния спектър от митнически рискове, включително по отношение на заплахите за сигурността и целостта на международните вериги за доставки и на съответните критични инфраструктури (напр. преки заплахи при вноса за пристанищните съоръжения, летищата или сухопътните граници). Модернизирането има за цел да гарантира, че митниците в ЕС получават цялата необходима информация от търговците по отношение на движението на стоки; че са в състояние да споделят тази информация по-ефективно между държавите членки; че прилагат общите и специфичните за държавите членки правила за риска; и че са в състояние по-ефективно да насочат действията си към рисковите пратки чрез интензивно сътрудничество с други органи, по-специално с други агенции в областта на правоприлагането и сигурността. Необходимите разработки в областта на ИТ за извършване на посоченото модернизиране от Комисията са в своята начална фаза и се очаква инвестирането на централно равнище да започне през идните месеци.

Космическо пространство

Действие 8: в контекста на космическата стратегия и европейския план за действие в областта на отбраната Комисията ще предложи да се увеличи устойчивостта на космическата инфраструктура спрямо хибридните заплахи, по-специално чрез възможно разширяване на обхвата на космическото наблюдение и проследяване, така че да включва хибридните заплахи, чрез подготовка за следващото поколение правителствени спътникови комуникации на европейско равнище и чрез въвеждане на „Галилео“ за критичните инфраструктури, които са зависими от времевата синхронизация.

При подготовката на нормативната уредба за правителствените сателитни комуникации (GovSatCom) и за космическото наблюдение и проследяване през 2018 г. Комисията ще включи в своята оценка аспектите на устойчивостта срещу хибридните заплахи. В съответствие с космическата стратегия при подготовката на развитието на „Галилео“ и „Коперник“ Комисията ще направи оценка на потенциала на тези услуги за компенсиране на уязвимостта на критичните инфраструктури. Докладът за оценка следва да бъде готов през есента на 2017 г., а предложението за следващото поколение на „Коперник“ и „Галилео“ — през 2018 г. Европейската агенция по отбрана работи по съвместни проекти за развиване на способности в областта на спътниковите комуникации, военното позициониране, навигация и синхронизация и наблюдението на Земята. Всички проекти ще се съсредоточат върху изискванията за устойчивост в светлината на настоящите и нововъзникващите хибридни заплахи.

Отбранителни способности

Действие 9: върховният представител, със съответната подкрепа от държавите членки и поддържайки връзка с Комисията, ще предложи проекти за адаптиране на отбранителните способности и за развойна дейност от значение за ЕС, които са конкретно предназначени за борба с хибридните заплахи, насочени срещу дадена държава членка или няколко държави членки.

През 2016 и 2017 г. Европейската агенция по отбрана проведе заедно с Комисията, ЕСВД и експерти от държавите членки три симулационни учения във връзка със сценарии за хибридни заплахи. Констатациите от тях ще бъдат взети предвид при

прегледа на плана за развитие на способностите, така че развитието на ключови способности, необходими за борба с хибридните заплахи, ще бъде включено в новите приоритети на ЕС за развитие на способностите. В работата по прегледа на Каталога на изискванията за 2005 г. ще се вземе предвид измерението, свързано с хибридните заплахи. През април 2017 г. Европейската агенция за отбрана финализира доклад за извършен анализ на военните последици от хибридните атаки, насочени срещу критични пристанищни инфраструктури, който ще бъде обсъден на работна среща с експерти по морско дело през октомври 2017 г. Друг специфичен анализ на военната роля в контекста на борбата с малките безпилотни летателни апарати е насрочен за 2018 г. Освен това приоритетите по отношение на способностите за засилване на устойчивостта срещу хибридните заплахи, установени от държавите членки, също биха могли да бъдат допустими за подпомагане по линия на Европейския фонд за отбрана, считано от 2019 г. нататък. Комисията призовава съзаконотелите да гарантират бързото приемане, а държавите членки — да представят предложения за проекти по отношение на способностите за засилване на устойчивостта на ЕС срещу хибридните заплахи.

Действие 10: *Комисията, в сътрудничество с държавите членки, ще повиши осведомеността относно хибридните заплахи и устойчивостта спрямо тях в рамките на съществуващите механизми за готовност и координация, най-вече чрез Комитета за здравна сигурност.*

С оглед укрепване на подготвеността и устойчивостта срещу хибридните заплахи, включително и изграждане на капацитет в системите на здравеопазването и храните, Комисията подкрепя държавите членки чрез обучения и симулационни учения, а също и като предоставя насоки за улесняване на обмена на опит и финансира съвместни действия. Това се осъществява по-конкретно съгласно Рамката на ЕС за здравна сигурност във връзка със сериозни трансгранични заплахи за здравето и съгласно Програмата за обществено здравеопазване за прилагане на Международните здравни правила — законодателен стълб, обвързващ 196 държави, включително държавите членки, с цел предотвратяване и реагиране на остри обществени трансгранични рискове за здравето в световен мащаб. С цел проверка на междусекторната готовност и реагиране в сектора на здравеопазването през есента на 2017 г. службите на Комисията ще проведат учение във връзка със сложните и многоизмерните хибридни заплахи. Комисията и държавите членки подготвят съвместно действие относно ваксините, включващо прогнозиране на търсенето и предлагането на ваксини и изследвания в областта на иновативните процеси за производство на ваксини с оглед укрепване на предлагането на ваксини и подобряване на здравната сигурност на равнището на ЕС (2018—2020 г.). Комисията също така си сътрудничи с Европейския орган за безопасност на храните и Европейския център за профилактика и контрол върху заболяванията, за да се адаптира към авангардните техники за научни изследвания с цел по-прецизно идентифициране и откриване на източниците на заплахи за здравето и като резултат от това — бързо справяне със заплашващи безопасността на храните огнища на зараза. Комисията създаде мрежа от организации, финансиращи научни изследвания — „Световно сътрудничество в областта на научните изследвания за готовност при заразни болести“ — за координирана реакция от страна на научноизследователската общност в рамките на 48 часа от появата на значително огнище на зараза.

Действие 11: *Комисията насърчава държавите членки приоритетно да създадат мрежа от 28-те ЕРИКС и CERT-EU (екипа на ЕС за незабавно реагиране при компютърни*

инциденти) и да я използват пълноценно, както и да установят рамка за стратегическо сътрудничество. Комисията, в сътрудничество с държавите членки, следва да гарантира, че секторните инициативи в областта на кибернетичните заплахи (например във въздухоплаването, енергетиката, мореплаването) съответстват на междусекторните способности, уредени в Директивата за МИС, за събиране на информация, експертен опит и бързи ответни действия.

Неотдавнашните глобални кибератаки, използващи софтуер за изнудване и зловреден софтуер, за да се блокират хиляди компютърни системи, отново показаха спешната необходимост от засилване на киберустойчивостта и от действия в областта на сигурността в рамките на ЕС. Както бе съобщено в междинния преглед на цифровия единен пазар, Комисията и върховният представител в момента правят преглед на Стратегията на ЕС за киберсигурност от 2013 г., по-специално чрез приемането на пакет, планиран за септември 2017 г. Целта ще бъде да се осигури по-ефикасен междусекторен отговор на тези заплахи, като се повиши доверието в цифровото общество и икономика. Също така ще бъде преразгледан мандатът на ENISA — Агенцията на Европейския съюз за мрежова и информационна сигурност, за да се определи нейната роля в променената среда на киберсигурността. Европейският съвет¹³ приветства намерението на Комисията да направи преглед на стратегията за киберсигурност.

Приемането на Директивата относно мрежовите информационни услуги (МИУ)¹⁴ през юли 2016 г. бе ключова стъпка към изграждането на устойчивост на европейско равнище срещу киберзаплахите. Директивата определя първите общоевропейски правила в областта на киберсигурността, подобрява възможностите за гарантиране на киберсигурността и засилва сътрудничеството между държавите членки. Тя също така задължава дружествата в особено важни сектори да предприемат подходящи мерки за сигурност и да уведомяват за всички сериозни инциденти в кибернетичното пространство съответния национален орган. Сред тези сектори са инфраструктурите на енергетиката, транспорта, водоснабдяването, здравеопазването, банковото дело и на финансовите пазари. Трябва да се предприемат подобни стъпки и по отношение на онлайн пазарите, компютърните услуги в облак и интернет търсачките. Последователното прилагане в различните сектори, както и отвъд границите, ще бъде осигурено чрез групата за сътрудничество в областта на мрежовите информационни услуги (създадена от Комисията през 2016 г.), която има за задача да се избегне разпокъсаността на пазара. Във връзка с това Директивата за мрежовите информационни услуги се счита за референтната рамка за всички секторни инициативи в областта на киберсигурността. Освен това с Директивата се създава мрежа от екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС), която обединява всички съответни заинтересовани страни. Успоредно с това Комисията и CERT-EU активно наблюдават кибернетичните заплахи и обменят информация с националните органи с цел да се гарантира, че системите на информационните технологии на институциите на ЕС са добре защитени и устойчиви срещу кибератаки. Инцидентът със софтуера за изнудване WannaCry от май 2017 г. предостави за първи път възможност на мрежата да започне оперативен обмен на информация и сътрудничество чрез разпространението на

¹³ Заключение на Европейския Съвет от 22—23 юни 2017 г.

¹⁴ Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

съвети. Екипът за незабавно реагиране при компютърни инциденти на ЕС също поддържаше тясна връзка с Европейския център за борба с киберпрестъпността (ЕСЗ) към Европол, с екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС) на засегнатите държави, звената за борба с киберпрестъпността и ключови партньори от сектора с цел да бъде намалена заплахата и да се окаже съдействие на пострадалите. Обменът на национални доклади за ситуацията гарантира обща ситуационна осведоменост в целия ЕС. Този опит позволи на мрежата да бъде по-добре подготвена за следващите инциденти (напр. „NonPetya“). Бяха идентифицирани също така редица предизвикателства и по отношение на тях се предприемат мерки.

Действие 12: Комисията, в сътрудничество с държавите членки, ще работи съвместно с промишления сектор в рамките на договорно публично-частно партньорство по киберсигурността с цел разработване и изпитване на технологии за по-добра защита на потребителите и инфраструктурите от кибернетичните аспекти на хибридните заплахи.

През юли 2016 г. Комисията, в координация с държавите членки, подписа с представители на промишлеността договорно публично-частно партньорство (дПЧП) в областта на киберсигурността, в което ще се инвестират до 450 млн. евро по линия на програмата на ЕС за научни изследвания и иновации „Хоризонт 2020“ с цел разработване и изпитване на технологии за по-добра защита на потребителите и инфраструктурите срещу кибернетични и хибридни заплахи. Резултат от партньорството е първата общеевропейска програма за стратегически изследвания, която е съсредоточена върху подобряването на устойчивостта на критичната инфраструктура, както и на гражданите срещу кибератаки. Партньорството засили сътрудничеството между заинтересованите страни, което доведе до повишаване на ефективността и ефикасността на финансирането по линия на „Хоризонт 2020“ за сектора на киберсигурността. В рамките на партньорството се работи успоредно по въпроси, свързани със сертифицирането по отношение на киберсигурността на информационните и комуникационните технологии, както и по начините за преодоляване на острия недостиг на пазара на квалифицирани специалисти в сферата на киберсигурността. С оглед на значителните потребности от изследвания за граждански цели и изискваната голяма устойчивост в сферата на отбраната, групата за кибернетични технологии и изследвания към Европейската агенция по отбрана допринася към научноизследователските области, определени от Европейската организация за киберсигурност в нейната стратегическа програма за научни изследвания и иновации.

Действие 13: Комисията ще публикува насоки за собствениците на активи в интелигентни мрежи с цел подобряване на киберсигурността на техните инсталации. В контекста на инициативата за структурата на пазара на електроенергия Комисията ще разгледа възможността да предложи „планове за готовност за справяне с рискове“ и процедурни правила за обмен на информация и осигуряване на солидарност сред държавите членки при криза, включително правила за предотвратяване на кибератаки и ограничаване на последиците от тях.

В енергийния сектор Комисията понастоящем подготвя секторна стратегия за киберсигурността със създаването на платформата на експертите в енергийния сектор по въпросите на киберсигурността за засиленото прилагане на Директивата относно мрежовата и информационната сигурност. В проучване от февруари 2017 г. бяха определени най-добрите налични техники, за да се повиши равнището на

киберсигурността на интелигентните измервателни системи, в подкрепа на тази платформа. Освен това Комисията създаде интернет платформа „Център на ЕС за обмен на информация относно инцидентите и заплахите“, която анализира и обменя информация за компютърни заплахи и инциденти в енергийния сектор.

Повишаване на устойчивостта на финансовия сектор срещу хибридни заплахи

Действие 14: Комисията, в сътрудничество с ENISA¹⁵, държавите членки, съответните международни, европейски и национални органи и финансови институции, ще поощрява и подпомага създаването на платформи и мрежи за обмен на информация и ще обърне внимание на факторите, които възпрепятстват обмена на такава информация.

Като отчете, че киберзаплахите спадат към най-големите рискове за финансовата стабилност, Комисията направи преглед на регулаторната рамка относно платежните услуги в Европейския съюз, която се прилага сега. В преработената Директива за платежните услуги¹⁶ бяха въведени нови разпоредби за повишаване на сигурността на платежните инструменти и задълбочено установяване на идентичността на клиента с цел намаляване на измамите, по-специално при онлайн плащанията. Новата законодателна рамка ще се прилага от януари 2018 г. Понастоящем Комисията, подпомагана от Европейския банков орган и в консултация със заинтересовани страни, разработва регулаторни технически стандарти, които се очаква да бъдат публикувани до края на 2017 г., относно задълбоченото установяване на идентичността на клиента и общите и сигурни комуникации за действителна сигурност в платежните операции. Освен това в международен план Комисията работеше в тясно сътрудничество със съответните партньори от Г-7 по „Основни принципи на Г-7 за киберсигурност във финансовия сектор“, одобрени през октомври 2016 г. от министрите на финансите и управителите на централните банки на държавите от Г-7. Принципите са предназначени за предприятия (частни и публични) от финансовия сектор и допринасят за координиран подход към киберсигурността във финансовия сектор за съвместно справяне с киберзаплахите, включително при нарастването на техния брой и усложняването им.

Транспорт

Действие 15: Комисията и върховният представител (в рамките на съответните им компетенции), в сътрудничество с държавите членки, ще преценяват каква да бъде реакцията спрямо хибридните заплахи, по-специално тези, свързани с кибератаки в транспортния сектор.

Изпълнението на плана за действие във връзка с Европейската стратегия за морска сигурност¹⁷ ще спомогне за скъсване с тясноведомственото мислене в обмена на информация и за съвместното използване на активи от гражданските и военните органи. Прилагането на подход, който обхваща всички нива на управление, доведе до увеличаване на сътрудничеството между различните участници. Планирано е до края

¹⁵ Агенция на Европейския съюз за мрежова и информационна сигурност.

¹⁶ Директива (ЕС) 2015/2366 на Европейския парламент и на Съвета от 25 ноември 2015 г. за платежните услуги във вътрешния пазар (ОВ L 337, 23.12.2015 г., стр. 35).

¹⁷ https://ec.europa.eu/maritimeaffairs/sites/maritimeaffairs/files/docs/body/20141216-action-plan_en.pdf вторият доклад относно изпълнението на плана за действие във връзка с Европейската стратегия за морска сигурност, представен на държавите членки на 21 юни 2017 г.

на 2017 г. със заключителен семинар относно защитата на критичната морска инфраструктура да бъде завършена съвместна гражданско-военна програма на Комисията и ЕСВД за стратегически изследвания. В бъдеще работата в тази насока може да бъде разширена, така че да обхване нововъзникващата заплаха за подводните тръбопроводи, преноса на енергия и съобщителните кабели — от оптични влакна и традиционни, от смущения извън националните води.

В рамките на неотдавнашно проучване¹⁸ беше преценен капацитетът за оценка на риска на националните органи, изпълняващи функции по брегова охрана. Бяха установени най-важните пречки за сътрудничеството и бяха препоръчани практически начини за подобряване на сътрудничеството между морските органи на равнището на ЕС и на национално равнище в тази специфична област. Оценката на риска е от съществено значение за противодействие на морски заплахи и е дори още по-важна за оценката и предотвратяването на хибридни заплахи, тъй като при тях са налице допълнителни и по-сложни съображения. Резултатите от това проучване ще бъдат представени на различни форуми във връзка с бреговата охрана, така че предложените препоръки да могат да бъдат оценени и изпълнени за повишаване на сътрудничеството в тази област с основни цели подготвеност за хибридни заплахи и ответни действия срещу тях.

Борба с финансирането на тероризма

Действие 16: Комисията ще използва изпълнението на Плана за действие относно финансирането на тероризма, за да допринесе и за ответни действия срещу хибридните заплахи.

Извършителите на хибридни атаки и техните поддръжници се нуждаят от средства, за да изпълнят своите планове. Усилията на ЕС за борба с престъпността и финансирането на тероризма съгласно Европейската програма за сигурност и Плана за действие относно финансирането на тероризма могат да допринесат и за борбата с хибридните заплахи. През декември 2016 г. Комисията представи три законодателни предложения, включително относно наказателните санкции за изпирание на пари и незаконни парични плащания, както и относно замразяването и конфискацията на активи¹⁹.

Всички държави членки трябваше да транспонират до 26 юни 2017 г. 4-тата директива относно борбата с изпирането на пари²⁰, а през юли 2016 г. Комисията представи целево законодателно предложение за допълване и засилване на същата директива с още мерки²¹.

¹⁸ Проучване относно „Преценка на капацитета за оценка на риска на равнището на изпълняващите функции по брегова охрана органи на държавите членки“, 2017 г., <https://ec.europa.eu/maritimeaffairs/documentation/studies>

¹⁹ Трети доклад за напредъка по създаването на ефективен и истински Съюз на сигурност (COM(2016) 831 final).

²⁰ Директива (ЕС) 2015/849 на Европейския парламент и на Съвета от 20 май 2015 г. за предотвратяване използването на финансовата система за целите на изпирането на пари и финансирането на тероризма, за изменение на Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета и за отмяна на Директива 2005/60/ЕО на Европейския парламент и на Съвета и на Директива 2006/70/ЕО на Комисията (текст от значение за ЕИП), ОВ L 141, 5.6.2015 г., стр. 73—117.

²¹ За повече подробности вж. третия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност (COM(2016) 831 final) и осмия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност (COM(2017) 354 final).

На 26 юни 2017 г. Комисията издаде наднационалната оценка на риска, предвидена в 4-та директива относно борбата с изпирането на пари. Тя представи и предложение за регламент за предотвратяване на вноса и съхранението в ЕС на паметници на културата, които са изнесени незаконно от трети държави²². По-късно тази година Комисията ще представи доклад за текущата си оценка на необходимостта от евентуални допълнителни мерки за проследяване на финансирането на тероризма в ЕС. Комисията също така прави преглед на законодателството относно борбата срещу измамите и фалшифицирането на непарични платежни средства²³.

Осмият доклад за напредъка по създаването на ефективен и истински Съюз на сигурност предоставя повече подробности относно актуалното състояние във връзка с изпълнението на Плана за действие за борба с финансирането на тероризма

Популяризиране на общите ценности на ЕС и насърчаване на изграждането на приобщаващо, отворено и устойчиво общество

Изграждане на устойчивост срещу радикализацията и насилническият екстремизъм

Религиозна и идеологическа радикализация, етнически конфликт и малцинствени конфликти могат да бъдат предизвикани от външни участници чрез оказване на подкрепа на определени групи или чрез усилия за подклаждане на конфликти между групи. Възникнаха допълнителни предизвикателства, като например заплахи от самостоятелно действащи лица и нови модели на радикализация, включително евентуално в контекста на миграционната криза, както и надигане на десния екстремизъм (включително насилие срещу мигранти) и риск от поляризация. Докато работата по въпросите на радикализацията напредва в контекста на Съюза на сигурност, тя може да бъде и от косвено значение по отношение на хибридните заплахи, доколкото податливи на радикализация лица могат да бъдат манипулирани от извършители на хибридни атаки.

Действие 17: Комисията изпълнява действията срещу радикализацията, посочени в Европейската програма за сигурност, и анализира необходимостта да се подобрят процедурите за премахване на незаконно съдържание, като призовава посредниците да извършват надлежни проверки при управлението на мрежите и системите.

Предотвратяване на радикализацията

Комисията продължава с изпълнението на своите многостранни ответни мерки спрямо радикализацията съгласно съобщението от юни 2016 г. за подпомагане на предотвратяването на радикализацията, водеща до насилнически екстремизъм²⁴, с ключови действия, като например насърчаването за приобщаващо образование и общи ценности, справяне с екстремистката пропаганда в интернет и радикализацията в затворите, засилването на сътрудничеството с трети държави и увеличаване на

²² COM(2017) 26.6.2017, COM(2017) 340 final, SWD(2017) 275 final 0.

²³ Осми доклад за напредъка по създаването на ефективен и истински Съюз на сигурност (COM(2017) 354 final).

²⁴ http://ec.europa.eu/dgs/education_culture/repository/education/library/publications/2016/communication-preventing-radicalisation_en.pdf

изследванията за по-добро разбиране на променящото се естество на радикализацията и по-информирани ответни мерки на политиката. Мрежата за осведоменост по въпросите на радикализацията (RAN) беше на преден план в работата на Комисията да оказва подкрепа на държавите членки в тази област, действайки на общностно равнище с местни специалисти. Повече подробности се дават в осмия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност²⁵.

Онлайн радикализация и език на омразата

В съответствие с Европейската програма за сигурност²⁶ Комисията предприе мерки за намаляване на наличието онлайн на незаконно съдържание, а именно чрез влизащото в състава на Европол звено на ЕС за сигнализиране за незаконно съдържание в интернет и Интернет форума на ЕС²⁷. Значителен напредък е постигнат също така по кодекса за поведение за борба с незаконния език на омразата в интернет²⁸. Повече подробности се дават в осмия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност²⁹. Тези действия ще бъде засилени също и с оглед на заключенията на Европейския съвет³⁰, срещата на върха на Г-7³¹ и срещата на върха на Г-20 в Хамбург³².

Онлайн платформите играят ключова роля в борбата срещу незаконно или потенциално вредно съдържание. Съгласно стратегията за цифров единен пазар, както е посочено в междинния преглед³³, Комисията ще гарантира по-добра координация на диалозите с платформите със съсредоточаване върху механизмите и техническите решения за премахване на незаконно съдържание. Когато е приложимо, целта следва да бъде тези механизми да се основават на насоки относно аспектите, като например уведомяване за незаконно съдържание и премахването му. Комисията ще предостави и насоки относно правилата за отговорността.

Засилване на сътрудничеството с трети държави

Действие 18: върховният представител, в сътрудничество с Комисията, ще започне проучване на хибридните рискове в съседните на ЕС региони. Върховният представител, Комисията и държавите членки ще използват инструментите, с които разполагат, за изграждането на капацитет на партньорите и за укрепването на тяхната устойчивост срещу хибридни заплахи. Самостоятелно или като допълнение към инструменти на ЕС могат да се използват мисии по линия на ОПСО, така че да се помогне на партньорите да повишат своя капацитет.

²⁶ За повече подробности вж. осмия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност, COM(2017) 354 final.

²⁷ За повече подробности вж. осмия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност, COM(2017) 354 final.

²⁸ Кодекс за поведение за борба с незаконния език на омразата в интернет, 31 май 2016 г., http://ec.europa.eu/justice/fundamental-rights/files/hate_speech_code_of_conduct_en.pdf.

²⁹ За повече подробности вж. осмия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност, COM(2017) 354 final.

³⁰ Заключение на Съвета от 22—23 юни 2017 г.

³¹ Срещата на върха на Г-7 в Таормина, Италия, 26—27.5.2017 г.

³² Срещата на върха на Г-20 в Хамбург, Германия, 7—8.7.2017 г.

³³ Вж. горепосоченото съобщение на Комисията, COM(2017) 228 final.

Европейският съюз засили вниманието си върху изграждането на капацитет и устойчивост в партньорски държави в сектора на сигурността, наред с другото, въз основа на връзката между сигурността и развитието, както и чрез оформянето на свързаното със сигурността измерение на преразгледаната европейска политика за съседство и започването на диалози по контратероризма и сигурността с държави, разположени около Средиземно море. За тази цел в сътрудничество с Република Молдова беше започнато като пилотен проект проучване на рисковете. Неговата цел е да спомогне за идентифициране на основните уязвимости на тази държава и да гарантира, че съдействието от страна на ЕС е насочено именно към тях. Резултатите от пилотния проект показаха, че проучването само по себе си се счита за полезно. Въз основа на натрупания опит Комисията и ЕСВД ще направят препоръки за определянето на приоритети за действията в раздела за изграждането на ефективност, стратегическите комуникации, защитата на критична инфраструктура и киберсигурността.

В перспектива още съседни държави биха могли да се възползват от проучването въз основа на натрупания от него първоначален опит, макар и със специално приспособяване съобразно различните национални местни условия и специфичните заплахи и като се избягва дублирането с текущите диалози по контратероризма и сигурността. В по-общ план на 7 юни 2017 г. Комисията и върховният представител приеха съвместно съобщение относно „Стратегически подход към устойчивостта във външната дейност на ЕС“³⁴. Целта е подкрепа за партньорските държави, за да станат по-устойчиви спрямо днешните глобални предизвикателства. Отчита се и необходимостта да се премине от ограничаване на кризите към по-структуриран дългосрочен подход към уязвимостите с наблягане върху предвиждането, предотвратяването и подготвеността.

Устойчивост на кибернетичното пространство за развитие

ЕС подпомага държави извън Европа с цел да се засили устойчивостта на информационните им мрежи. На непрекъснато растящата цифровизация е присъщо измерение по отношение на сигурността, което поражда специфични предизвикателства за устойчивостта на мрежите от информационни системи в световен мащаб, тъй като за кибератаките няма граници. ЕС подкрепя трети държави за изграждане на способността им адекватно да предотвратяват и реагират на случайни неизправности и кибератаки. След като през 2016 г. беше завършен пилотен проект в областта на киберсигурността в бившата югославска република Македония, Косово³⁵ и Молдова, Комисията ще стартира нова програма за повишаване на устойчивостта на киберпространството на трети държави — главно в Африка и Азия за периода 2017—2020 г., но също и в Украйна. С нея се цели повишаване на сигурността и подготвеността на критичната информационна инфраструктура и мрежите в трети държави въз основа на подход, обхващащ всички нива на управление, като същевременно се гарантира спазване на правата на човека и върховенство на закона.

³⁴ Съвместно съобщение до Европейския парламент и Съвета: Стратегически подход към устойчивостта във външната дейност на ЕС, JOIN (2017) 21 final.

³⁵ Това название не засяга позициите по отношение на статута и е съобразено с Резолюция 1244 на Съвета за сигурност на ООН и становището на Международния съд относно обявяването на независимост от страна на Косово.

Сигурност на въздухоплаването

Гражданското въздухоплаване остава главна и символична цел за терористите, но може да стане мишена и като част от хибридна кампания. Въпреки че ЕС е разработил надеждна рамка за сигурност на въздухоплаването, произхождащите от трети държави полети могат да се окажат по-уязвими. В съответствие с Резолюция 2309 (2016) на Съвета за сигурност на ООН Комисията увеличава усилията си за изграждане на капацитет в трети държави. През януари 2017 г. Комисията стартира нова интегрирана оценка на риска, за да се гарантира определянето на приоритети и координацията на усилията за изграждане на капацитет, осъществявани на равнището на ЕС и на държавите членки, както и с международни партньори. През 2016 г. Комисията стартира 4-годишен проект за сигурността на гражданското въздухоплаване в Африка и на Арабския полуостров, за да се противодейства на заплахата за него от тероризъм. В проекта се набляга върху обмена на експертен опит между държавите партньори и експерти от държавите — членки на Европейската конференция за гражданска авиация, и дейности по наставничество, обучение и тренинг. Дейностите ще бъдат разширени още през 2017 г.

В. ПРЕДОТВРАТЯВАНЕ, РЕАКЦИЯ ПРИ КРИЗИ И ВЪЗСТАНОВЯВАНЕ

Макар че последиците могат да бъдат ограничени чрез дългосрочни политики на национално равнище и на равнище ЕС, в краткосрочен план от съществено значение е да се увеличи способността на държавите членки и Съюза бързо и координирано да предотвратяват хибридните заплахи, да реагират спрямо тях и да се възстановяват от последствията им. Бързите ответни действия на събития, предизвикани от хибридни заплахи, са от съществено значение. През последната година беше постигнат голям напредък в тази област с въвеждането в ЕС на оперативен протокол, в който се определя процесът на управление на криза в случай на хибридна атака. В бъдеще редовно ще се осъществяват мониторинг и учения.

***Действие 19:** върховният представител и Комисията, в координация с държавите членки, ще установят общ оперативен протокол и ще провеждат редовни учения за подобряване на капацитета за вземане на стратегически решения в отговор на комплексни хибридни заплахи въз основа на процедурите за управление на кризи и интегрираните договорености за реакция на ЕС на политическо равнище в кризисни ситуации.*

В съвместната рамка се препоръчва създаването на механизми за бързи ответни действия спрямо събития, предизвикани от хибридни заплахи, и координиране между механизмите за реагиране³⁶ и системите за ранно предупреждение на ЕС. За тази цел службите на Комисията и ЕСВД издадоха оперативния протокол на ЕС за борбата с хибридните заплахи (EU Playbook)³⁷, в който се очертават редът и условията за координация, синтез и анализ на разузнавателна информация, информационно осигуряване на процесите на създаване на политики, ученията и обучението, и сътрудничество с партньорски организации, по-специално с НАТО, в случай на хибридна заплаха. НАТО също разработи протокол за засилено взаимодействие с ЕС в

³⁶ Интегрираните договорености на Съвета за реакция на ЕС на политическо равнище в кризисни ситуации (IPCR), системата ARGUS на Комисията и CRM на ЕСВД.

³⁷ Работен документ на службите (2016) 227, приет на 7 юли 2016 г.

предотвратяването и борбата с хибридни заплахи в областите на киберотбраната, стратегическите комуникации, ситуационната осведоменост и управлението на кризи. Протоколът EU Playbook ще бъде изпитан чрез учение през есента на 2017 г. като част от паралелното и координирано учение на Европейския съюз, което включва взаимодействие с НАТО.

Действие 20: *Комисията и върховният представител (в рамките на съответните им компетенции) ще разгледат приложимостта и практическите последици на член 222 от ДФЕС и член 42, параграф 7 от ДЕС в случай на мащабна и сериозна хибридна атака.*

Член 42, параграф 7 от ДЕС се отнася за въоръжено нападение на територията на държава членка, докато член 222 от ДФЕС (клауза за солидарност) се отнася за терористично нападение или природно или предизвикано от човека бедствие на територията на държава членка. Вторият член е по-вероятно да бъде използван в случай на хибридни атаки, които представляват смесица от престъпни/поддривни действия. Позоваването на клаузата за солидарност поражда координация на равнището на Съвета (интегрираните договорености за реакция на ЕС на политическо равнище в кризисни ситуации — IPCR) и последици за съответните институции, агенции и органи на ЕС, както и програми и механизми на ЕС за съдействие. Решение 2014/415/ЕС на Съвета предвижда условията и реда за прилагане от страна на Съюза на клаузата за солидарност. Тези условия и ред за прилагане остават в сила и не се налага преразглеждане на решението на Съвета. Ако дадена хибридна атака включва въоръжено нападение, тогава е възможно позоваване и на член 42, параграф 7. В такъв случай помощта и съдействието се оказват както от държавите членки, така и от ЕС. Комисията и върховният представител ще продължат да оценяват най-ефективните начини за справяне с подобни атаки.

Въвеждането на горепосочения оперативен протокол на ЕС пряко подпомага тази оценка и ще бъде упражнено като част от паралелното и координирано учение (PASE) на ЕС през октомври 2017 г. В това учение ще бъдат изпитани различните механизми и способността на ЕС за взаимодействие с цел ускорено вземане на решения, когато дадена хибридна атака поражда неяснота.

Действие 21: *върховният представител, в координация с държавите членки, ще интегрира, използва и координира способностите за военни действия в борбата с хибридните заплахи в рамките на общата политика за сигурност и отбрана.*

В изпълнение на задачата за обединяване на военните способности в подкрепа на ОВПС/ОПСО и след семинар с военни експерти през декември 2016 г. и насоки през май 2017 г. от работната група на Военния комитет на Европейския съюз през юли 2017 г. беше финализирано военното становище относно „военния принос на ЕС към борбата с хибридните заплахи в рамките на ОПСО“ и то ще бъде приложено чрез Плана за изпълнение относно разработването на концепции.

Г. СЪТРУДНИЧЕСТВОТО МЕЖДУ ЕС И НАТО

Действие 22: *върховният представител, в координация с Комисията, ще продължи неформалния диалог и ще засили сътрудничеството и координацията с НАТО в областта на ситуационната осведоменост, стратегическите комуникации, кибернетичната сигурност и предотвратяването и реакцията на кризи с цел борба с хибридните заплахи,*

като се зачитат принципите на приобщаване и независимост в процеса на вземане на решения на всяка организация

Въз основа на съвместната декларация, подписана от председателите на Европейския съвет и Европейската комисия, заедно с генералния секретар на НАТО във Варшава на 8 юли 2016 г., ЕС и НАТО разработиха общ набор от 42 предложения за изпълнение, който впоследствие беше одобрен в отделни, успоредно протичащи процеси на 6 декември 2016 г. както от Съвета на ЕС, така и от Съвета на НАТО³⁸. През юни 2017 г. върховният представител и заместник-председател на Комисията и генералният секретар на НАТО публикуваха доклад за цялостния напредък, постигнат по 42-те действия от съвместната декларация. Борбата с хибридните заплахи е една от седемте области на сътрудничество, идентифицирани в съвместната декларация, като за нея се отнасят десет от четиридесет и двете действия. Докладът показва, че положените през изминалата година съвместни усилия са дали съществени резултати. Вече бяха упоменати много от насочените срещу хибридните заплахи конкретни действия, включително Европейският център за високи постижения в борбата с хибридните заплахи, по-добрата ситуационна осведоменост, създаването на звеното на ЕС за синтез на информацията за хибридните заплахи и взаимодействието му с новосъздадения от НАТО клон за анализ на хибридните заплахи, както и сътрудничество между екипите за стратегически комуникации. За първи път щабове на НАТО и на ЕС ще упражнят в съвместно учение своите ответни действия по сценарий за хибридна атака. Очаква се в рамките на това учение да се провери изпълнението на над една трета от общите предложения. ЕС ще проведе своето собствено паралелно и координирано учение тази година и се подготвя да поеме водеща роля през 2018 г.

По отношение на устойчивостта щабове както на ЕС, така и на НАТО провеждаха кръстосани брифинги, включително по интегрираните договорености за реакция на ЕС на политическо равнище в кризисни ситуации. Редовните контакти между щабове на ЕС и НАТО, включително чрез семинари или участие на НАТО в Управителния съвет на Европейската агенция по отбрана, дадоха възможност за обмен на информация относно базовите изисквания на НАТО за устойчивостта на национално равнище. За есента е планиран по-нататъшен обмен между Комисията и НАТО относно укрепването на устойчивостта. В следващият доклад за напредъка в сътрудничеството между ЕС и НАТО ще бъдат предложени възможности за разширяване на сътрудничеството между двете организации.

3. ЗАКЛЮЧЕНИЕ

В съвместната рамка са очертани действия, предназначени да способстват за противодействието на хибридните заплахи и за укрепването на устойчивостта на равнището на ЕС и на национално равнище, както и на партньорите. Макар че Комисията и върховният представител постигат резултати във всички области в тясно сътрудничество с държавите членки и партньорите, от решаващо значение е тази динамика да се поддържа постоянно спрямо текущите и непрекъснато развиващи се хибридни заплахи. Държавите членки носят основната отговорност за борбата с хибридните заплахи във връзка с националната сигурност и поддържането на законността и реда. Устойчивостта на национално равнище и колективните усилия за

³⁸ <http://www.consilium.europa.eu/en/press/press-releases/2016/12/06-eu-nato-joint-declaration/>

защита срещу хибридните заплахи трябва да се разбират като взаимно подсилващи се елементи на едно и също усилие. Ето защо държавите членки се приканват да извършат тези проучвания на хибридните заплахи възможно най-бързо, тъй като те ще предоставят ценна информация за степента на уязвимост и подготвеност в цяла Европа. Въз основа на постигнатия значителен напредък в подобряването на осведомеността следва да се увеличи максимално потенциалът на звеното на ЕС за синтез на информацията за хибридните заплахи. Върховният представител приканва държавите членки да подкрепят работата на оперативните групи StratCom, за да се противодейства по-ефективно на увеличението на хибридните заплахи. ЕС ще подкрепи изцяло Европейския център за борбата с хибридните заплахи, в който Финландия е водеща.

Уникалното предимство на ЕС се състои в подпомагането на държавите членки и партньорите за изграждане на тяхната устойчивост въз основа на широк набор от съществуващи инструменти и програми. Беше постигнат значителен напредък по действия за изграждането на устойчивост в множество области, като например транспорта, енергетиката, киберсигурността, критичната инфраструктура, защитата на финансовата система от незаконна употреба и противодействието на насилническият екстремизъм и радикализацията. ЕС ще продължи с изграждането на устойчивост, тъй като характерът на хибридните заплахи се развива. По-конкретно ЕС ще разработи показатели с оглед да се подобри защитата и устойчивостта на критичната инфраструктура спрямо хибридните заплахи в съответните сектори.

Европейският фонд за отбрана може да съфинансира заедно с държавите членки работата по приоритетните способности с оглед укрепване на устойчивостта спрямо хибридните заплахи. В предстоящия пакет за киберсигурността, както и в междусекторните мерки, насочени към изпълнението на Директивата за мрежова и информационна сигурност, ще бъдат предвидени нови платформи за борба с хибридните заплахи.

Комисията и върховният представител призовават държавите членки и заинтересованите страни, когато е необходимо, бързо да постигнат споразумение и да осигурят бързото и ефективно изпълнение на очертаните в настоящото съобщение множество мерки, насочени към повишаване на устойчивостта. ЕС ще разчита на своето вече плодотворно сътрудничество с НАТО и ще го задълбочава.

Съюзът потвърждава ангажимента си да мобилизира всички подходящи инструменти на ЕС за справяне с комплексни хибридни заплахи. Подкрепата за усилията на държавите членки остава приоритет за Съюза, действащ заедно с основните си партньори като по-силен и по-бързо реагиращ гарант за сигурността.