ЕВРОПЕЙСКА
КОМИСИЯ

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

Брюксел, 13.6.2018г.
JOIN(2018) 14 final

СЪВМЕСТЕН ДОКЛАД ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, ЕВРОПЕЙСКИЯ СЪВЕТ И СЪВЕТА

относно изпълнението на Съвместната рамка за борба с хибридните заплахи за периода юли 2017—юни 2018 г.

ВЪВЕДЕНИЕ

В Съвместната рамка за борба с хибридните заплахи — ответни действия на Европейския съюз[1], ситуационната осведоменост, устойчивостта и ответните действия се поставят в основата на действията на ЕС по отношение на хибридните заплахи. Усъвършенстването на способността ни за ранно откриване и разбиране на злонамерени хибридни дейности и повишаването на устойчивостта на критичната инфраструктура (например транспорт, далекосъобщения, енергетика, космически технологии и финанси) на нашите общества и институции са от съществено значение за подобряване на способността ни да устояваме на атаки и да се възстановяваме от тях. Борбата с хибридните заплахи изисква действия както от страна на държавите членки, така и от страна на европейските институции. Първият доклад за изпълнението на 22-те действия, определени в съвместната рамка, беше представен на Съвета на 19 юли 2017 г.[2] В настоящата актуализация от 2018 г. се представя преглед на напредъка, постигнат от лятото на миналата година.

Постигнат е значителен напредък във всичките четири приоритетни области на действие:

- 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;
- засилване на сътрудничеството с НАТО, за да се гарантира взаимното допълване на мерките.

РАЗПОЗНАВАНЕ НА ХИБРИДНОТО ЕСТЕСТВО НА ЗАПЛАХИТЕ

<u>Действие 1</u>: Провеждане на проучване от държавите членки във връзка с хибридните рискове

За да бъде постигнат напредък, Съветът създаде група „Приятели на председателството“, която се оглавява от ротационното председателство. През декември 2017 г. държавите членки започнаха проучване, за да оценят основните си уязвими места при евентуални хибридни заплахи. Въз основа на отговорите на държавите членки председателството ще представи доклад пред Комитета на постоянните представители (Корепер) вероятно преди края на юни 2018 г.

С оглед на изтичането на мандата на групата в края на юни 2018 г., на своето заседание през април „Приятели на председателството“ започна обсъждания относно бъдещия мандат въз основа на предложението на председателството. Така ще се удължи настоящият мандат до 2020 г. и ще се разшири съдържанието му; в съответствие с настоящия проект в мандата ще бъдат включени задачи, свързани с анализиране на възможностите за засилване на готовността и устойчивостта на държавите членки, наблюдение на националните развития и подпомагане на координацията на политиките в областта на хибридните заплахи, подкрепа за работата на Съвета, насочена към сътрудничеството между ЕС и НАТО в областта на борбата с хибридните заплахи,

[1] JOIN (2016) 18 final.

[2] Съвместен доклад до Европейския парламент и Съвета относно изпълнението на Съвместната рамка за борба с хибридните заплахи — ответни действия на Европейския съюз, JOIN(2017) 30 final.

както и обмен на информация и разработване на общо разбиране за хибридните заплахи.

ОРГАНИЗИРАНЕ НА ОТВЕТНИТЕ ДЕЙСТВИЯ НА ЕС: ПОДОБРЯВАНЕ НА ОСВЕДОМЕНОСТТА

<u>Действие 2</u>: Създаване на звено на ЕС за синтез на информацията за хибридните заплахи

Звеното на ЕС за синтез на информацията за хибридните заплахи, създадено в рамките на Центъра на ЕС за анализ на информация като част от гражданското/военното единно звено за анализ на разузнавателна информация на ЕС, разчита на граждански и на военни анализатори и на приноса на разузнавателните служби и службите за сигурност на държавите членки. През юли 2017 г. то достигна пълния си оперативен капацитет — статус, потвърден по време на паралелното и координирано учение с НАТО през 2017 г. (PACE17). Звеното на ЕС за синтез на информацията за хибридните заплахи получава и анализира класифицирана информация и информация от открити източници, която се отнася до хибридните заплахи и се предоставя от широк кръг заинтересовани страни. След това докладите и анализите се споделят между институциите на ЕС и държавите членки с цел осигуряване на информация за процеса на вземане на решения. Звеното на ЕС за синтез на информацията за хибридните заплахи досега е създало над 100 продукта, свързани с хибридните заплахи. CERT-EU (екипът за незабавно реагиране при компютърни инциденти за институциите на ЕС) допринася за работата на звеното на ЕС за синтез на информацията за хибридните заплахи чрез обмен на информация относно нови или текущи кибернетични заплахи. Въпреки това в областите на химическите, биологичните, радиационните и ядрените заплахи и кибернетичното разузнаване и контраразузнаването специфичният опит понастоящем е ограничен.

За да се подкрепи тази работа, звеното на ЕС за синтез на информацията за хибридните заплахи създаде мрежа от национални звена за контакт. Към днешна дата 26 от 28 държави членки са определили координационни звена, които организират редовни срещи със звеното на ЕС, за да споделят своя експертен опит.

Освен това тази мрежа се дублира от еквивалентна съвместна мрежа на Европейската служба за външна дейност (ЕСВД) и Комисията, насочена към постигане на резултати чрез различни действия за устойчивост. Тези срещи се провеждат ежемесечно, като техният акцент е върху тематични въпроси, включително транспорт, инфраструктура, енергетика, киберсигурност и враждебни разузнавателни дейности.

На стратегическо ниво звеното на ЕС за синтез на информацията за хибридните заплахи развива своите взаимоотношения с Европейския център за високи постижения в борбата с хибридните заплахи в Хелзинки, като участва в работни семинари, учения, както и посредством рутинни дискусии по различни теми с цел изграждане на компетентност в борбата с хибридните заплахи.

Съгласно съвместната декларация контактите между служителите на звеното за синтез и служителите на клона на НАТО за анализ на хибридните заплахи продължават да се осъществяват и са ежедневни. През септември 2017 г. бе публикувана особено значима паралелна и координирана оценка по въпроса за хибридните заплахи, а продуктите, които се планира да бъдат създадени през 2018 г., ще са съсредоточени върху хибридните предизвикателства, които произтичат от Южното и Източното съседство.

<u>Действие 3:</u> Стратегическа комуникация

Стратегическата комуникация придобива все повече сила в ЕС благодарение на множеството различни участници, които допринасят за развитието на способностите. В

съобщението „Европейски подход за борба с дезинформацията, разпространявана онлайн“[3] от 26 април 2018 г. дезинформацията се признава за хибридна заплаха и се определят редица действия, включително създаване на по-силна мрежа между Комисията, Европейската служба за външна дейност и държавите членки. Положителният опит на оперативната група на ЕС за стратегическа комуникация с Източното съседство (East Stratcom Task Force), създадена с мандат на Европейския съвет през март 2015 г., трябва да бъде подкрепен и засилен, както се предлага в съвместното съобщение „Посрещане на хибридните заплахи: защита на европейците“[4].

По-голямата част от работата на оперативната група за стратегическа комуникация с Източното съседство е съсредоточена върху подкрепата на делегациите на ЕС главно в региона на Източното партньорство и Русия и до известна степен в Централна Азия с цел да се подобри изпращането на положителни послания и да се повиши информираността в държавата или в региона. Комисията подкрепя тези дейности чрез многогодишна регионална информационна и комуникационна програма. Оперативната група на ЕС за стратегическа комуникация с Източното съседство редовно координира своите дейности както с държавите членки, така и с НАТО. Освен наблюдение на дезинформацията оперативната група на ЕС за стратегическа комуникация с Източното съседство провежда дейности за повишаване на осведомеността в държавите от Източното партньорство и в държавите членки относно въздействието на дезинформацията с произход от Русия. Тя също така засили обучението на персонала в държавите от Източното партньорство с цел повишаване на възможностите им за стратегическа комуникация и устойчивостта им на дезинформация. В бъдеще се предвижда засилено сътрудничество с щаба на НАТО и центровете за високи постижения в Рига и Хелзинки, например споделяне на анализи и обучителни семинари за журналисти от региона на Източното партньорство или Русия.

Съгласно новата стратегия на ЕС за Западните Балкани бе създадена оперативна група, насочена към Западните Балкани, с цел разпространение по по-ефективен начин на информация относно политиките на ЕС и към по-широка аудитория в региона, като същевременно се повишава осведомеността за дезинформационните дейности, насочени към Западните Балкани, и се дава отпор на тези дейности. Оперативната група и Комисията работят в тясно сътрудничество, за да постигнат по-стратегическа и целенасочена комуникация и отправяне на послания в региона, основаващи се на най-добри практики и акцент върху тематични кампании. Въпреки това липсва осведоменост относно нарастващите заплахи, насочени конкретно към институциите. Необходимо е да се изгради култура на осведоменост относно сигурността и да се увеличи капацитетът на институциите за справяне с хибридните заплахи.

Оперативната група за стратегическа комуникация за Южното съседство, създадена през 2017 г., адаптира мандата си, за да отрази изместването на акцента от борбата с тероризма към по-диференциран подход с оглед подобряване на комуникацията и повишаване на информираността на арабския свят, включително на арабски език. Тъй като Даиш, наричана също ИДИЛ, не е единствената заплаха от гледна точка на радикализацията, оперативната група работи за смекчаване на широкоразпространената дезинформация и погрешното възприемане на ЕС. Това се постига чрез разработване в тясно сътрудничество с Комисията на положителни послания относно Европейския съюз и неговите политики с цел изграждане на по-добро разбиране на Съюза, чрез по-стратегическа комуникация относно дейностите на Съюза в арабския свят, както и чрез

[3] COM(2018) 236 final.

[4] Да се въведе препратка, когато е налична

насърчаване на споделени ценности и интереси. Комисията подкрепя тези дейности чрез многогодишна регионална информационна и комуникационна програма.

<u>Действие 4:</u> Център за високи постижения в борбата с хибридните заплахи

Европейският център за високи постижения в борбата с хибридните заплахи, създаден през 2017 г., служи като център за експертен опит, който посредством научни изследвания, обучение, образование и учения подкрепя индивидуалните и колективните усилия на участващите държави да се борят с хибридните заплахи. Центърът е отворен за участие както за държавите — членки на ЕС, така и за съюзниците на НАТО. Наскоро Италия, Нидерландия, Дания и Чешката република станаха членове, като с тях държавите станаха общо 16. Както ЕС, така и НАТО участват в управителния съвет като наблюдатели.

През 2018 г. центърът постигна споразумение относно бюджета и работния план, разработи концептуална рамка и създаде три общности по интереси: за влиянието на хибридните заплахи, за уязвимостта и устойчивостта, както и за стратегията и отбраната. Създадена бе подгрупа относно недържавните субекти, която проучва как действат различните терористични групи и подставени лица. Центърът публикува редица анализи на хибридни заплахи и бе домакин на няколко срещи на високо равнище с цел да се изгради общо разбиране за хибридните заплахи, да се обменят най-добри практики и да се потърсят общи ответни действия в общностите на ЕС и на НАТО.

ОРГАНИЗИРАНЕ НА ОТВЕТНИТЕ ДЕЙСТВИЯ НА ЕС: ИЗГРАЖДАНЕ НА УСТОЙЧИВОСТ

Изграждането на устойчивост изисква действия в редица области на политиката. Тези действия не са непременно специфични за хибридния характер на заплахите, но взети заедно те могат да гарантират, че един по-устойчив ЕС е по-добре подготвен да посрещне хибридните заплахи. Поради това, когато е относимо за направеното по-долу описание на постигнатия при всяко действие напредък, се прави препратка към конкретната рамка на политиката и действията, предприети от Съюза, и по-специално действията, предприети като част от работата по създаването на Съюз на сигурност. Ето защо настоящият доклад следва да се чете във връзка с месечните доклади за напредъка по създаването на ефективен и истински Съюз на сигурност, приети на същия ден[5].

<u>Действие 5</u>: Защита и устойчивост на критичната инфраструктура

Комисията разработи проект на наръчник за показатели за уязвимост и устойчивост по отношение на хибридни заплахи за критичните инфраструктури в ЕС. Този проект на наръчник понастоящем е в процес на валидиране чрез консултации с държавите членки. Окончателният вариант на наръчника се очаква да бъде приет през ноември 2018 г. Освен това показателите за уязвимост ще бъдат изпитани по време на паралелното и координирано учение с НАТО (PACE 18) през 2018 г., но също и от отделни държави членки, които са изявили интерес. Следва да се обърне специално внимание на по-нататъшното разработване на показатели за разкриване, насочени към улесняване на ранното предупреждение още при самото настъпване на хибридни атаки срещу критична инфраструктура. Хибридните заплахи ще бъдат взети предвид и в предстоящата оценка на Директивата на ЕС относно защитата на критичната инфраструктура. Освен това Комисията засилва научната подкрепа с цел справяне с многобройните и трансверсални характеристики на хибридните заплахи, като се

[5] COM(2018) 470 final.

съсредоточава по-специално върху установяване на уязвими места, ранно разкриване и показатели, устойчивост, повишаване на осведомеността и учения.

Освен това, за да защити ключовите активи на Съюза, Комисията представи предложение за регламент за създаване на рамка за скрининг на преки чуждестранни инвестиции в Европейския съюз, ако те могат да имат последствия за сигурността или обществения ред[6]. Предложението на Комисията се отнася до преките инвестиции на лица или предприятия от трети държави, които могат, наред с другото, да засегнат критичните инфраструктури (включително енергетика, транспорт, далекосъобщения, съхранение на данни, космически и други чувствителни съоръжения), критични технологии (включително изкуствен интелект, киберсигурност, технологии с евентуална двойна употреба), сигурността на доставките на критични суровини, или инвестиции, които осигуряват достъп до чувствителна информация или възможност за контрол на такава информация.

Консултативният форум за устойчива енергия в сектора на отбраната и сигурността (CF SEDSS II), като част от втората фаза на Европейската агенция по отбрана, ще продължи да оказва подкрепа за разработването на концептуалния документ, изготвен от експертната група за защита на критичните енергийни инфраструктури (PCEI), като го превърне в ръководещ политиката документ на равнище ЕС. По този начин се предлага рамка за определяне на най-добрите управленски практики за министерствата на отбраната при укрепване на защитата и устойчивостта на всички критични енергийни инфраструктури (КЕИ), свързани с отбраната.

<u>Действие 6:</u> Подобряване на сигурността на енергийните доставки на ЕС и повишаване на устойчивостта на ядрените инфраструктури

Съобразно ангажимента си от септември 2017 г. (съвместното съобщение „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“[7]) Комисията ще продължи да подкрепя Европейския център за обмен и анализ на информация в енергетиката по отношение на киберсигурността.

За да се предотвратят кризи с доставките на газ, държавите членки изпълняват Регламента за сигурността на доставките на газ, приет миналата година, докато Комисията улеснява неговото изпълнение и сътрудничеството между държавите членки, попадащи в рисковите групи. Общите оценки на риска трябва да бъдат съобщени на Комисията до 1 октомври 2018 г. Комисията ще получи превантивните планове за действие и плановете за действие при извънредни ситуации до 1 март 2019 г. Държавите членки следва да сключат двустранните договорености за солидарност до 1 декември 2018 г.

За да се преодолее съществуващият регулаторен пропуск по отношение на готовността за справяне с рискове в електроенергийния сектор, в Регламента за готовността за справяне с рискове, който е предмет на преговори, ще бъдат предвидени правила за оценка на рисковете, задължение за държавите членки да изготвят план за готовност за справяне с рискове с някои задължителни елементи, правила за справяне с кризисни ситуации и правила за мониторинг на сигурността на доставките. Плановете за готовност за справяне с рискове следва да включват също така договорености за регионално сътрудничество, по-специално мерки за справяне в случай на криза в електроснабдяването едновременно в няколко района. При прилагането на Регламента за готовността за справяне с рискове държавите членки ще трябва да изготвят първия национален план за готовност за справяне с рисковете две години след влизането в сила на регламента. След това плановете следва да се актуализират на всеки три години. В

[6] COM(2017) 487 final.

[7] JOIN(2017) 450 final

бъдещия Регламент за готовността за справяне с рискове също ще се изисква провеждането на редовни и съвместни учения между държавите членки за симулиране на криза в електроснабдяването. Комисията вече започна подготовка на такива съвместни учения със заинтересованите държави членки, Съвместния изследователски център и Групата за координация в областта на електроенергетиката.

Що се отнася до устойчивостта на ядрените инфраструктури, обменът на информация по въпросите на ядрената сигурност със и между държавите членки и Комисията ще бъде подобрен в краткосрочен план, като е предвиден анализ на допълнителни инициативи. Ще бъде извършен анализ на Регламента за ядрената безопасност, както и на възможността за изготвяне на ръководство с цел подпомагане на държавите членки да управляват по-добре (радиоактивните) високоактивни закрити източници. В дългосрочен план Комисията възнамерява да засили дейностите в областта на ядрените технологии, в която държавите членки имат общ интерес и в която са налице договорени ползи от обмена на информация и сътрудничеството. Тя ще проучи също така подходящи мерки за ефективното изпълнение в рамките на ЕС на Международната конвенция за физическа защита на ядрения материал и ядрените съоръжения.

Що се отнася до сектора на отбраната, Консултативният форум за устойчива енергия в сектора на отбраната и сигурността подготви „Пътна карта за управление на устойчивата енергия в сектора на отбраната и сигурността“ с цел да подкрепи сектора на отбраната в усилията му за подобряване на управлението на енергийната инфраструктура. Консултативният форум ще продължи да проучва как секторът на отбраната може да използва по-ефективно енергийните ресурси и ще прегледа редица технологии за генериране на проекти за евентуална експлоатация от сектора на отбраната (например вятърна енергия, слънчева енергия, интелигентни мрежи, съхранение на енергия, биогорива, биомаса и производство на енергия от отпадъци).

В този контекст работата по линия на Програмата за енергетика и околна среда на Европейската агенция по отбрана ще продължи чрез научноизследователския проект „Интелигентни лагери в сини води“, за да се проучат възможностите за технологични интервенции в областта на устойчивото управление на водите във военните лагери на собствена територия, както и чрез научноизследователския договор за техническия опитен образец за интелигентни лагери, чрез който се проучва възможността за по-мащабно интегриране на по-широк кръг от енергийни и екологични технологии във военна среда с цел да се намерят решения на проблеми, свързани енергията, водите и отпадъците, като същевременно се подобрят разходната и военната ефективност на мисиите по линия на общата политика за сигурност и отбрана (ОПСО).

<u>Действие 7</u>: Сигурност на транспорта и веригите за доставки

Що се отнася до всички области на транспорта, и по-специално гражданското въздухоплаване и морския и сухопътния транспорт, Комисията задълбочи обсъжданията с държавите членки, промишлеността и други заинтересовани страни относно възникващите заплахи за сигурността от хибридно естество с цел придобиване на знания и извличане на поуки от опита.

В контекста на дейностите по изпълнение и преразглеждане на плана за действие във връзка с Европейската стратегия за морска сигурност Комисията анализира тенденциите в областта на морската сигурност — включително пиратството и морските спорове — които биха могли да засегнат корабоплаването и търговските маршрути, както и интересите на ЕС. Като се има предвид фактът, че държавите — членки на ЕС, и държавите от ЕИП контролират над 40 % от световния търговски флот, както и че ЕС е голям търговски блок, хибридните атаки срещу морските търговски маршрути биха причинили значителни вреди на веригите за създаване на стойност и веригите на

доставките в Европа. Анализът на риска и мониторингът на възникващите заплахи в морската област биха могли да доведат до предложения за актуализиране на конкретното законодателство в областта на транспорта, когато е подходящо. Също така този анализ представлява основата за непрекъсната работа по подобряване на осведомеността относно морското дело, включително в контекста на развитието на общата среда за обмен на информация (CISE), като в рамките на нова покана за представяне на предложения, които подкрепят усилията на държавите членки за подобряване на оперативната съвместимост на информационните технологии между националните морски органи, наскоро бяха наградени три нови проекта (началото на 2018 г.).

С приемането на пакета за гранична и бреговата охрана[8] през септември 2016 г. Европейският парламент и Съветът въведоха общ член в учредителните регламенти на Европейската агенция за гранична и брегова охрана, Европейската агенция за контрол на рибарството (EFCA) и Европейската агенция по морска безопасност (ЕАМБ), според който те се задължават да засилят сътрудничеството, всяка в рамките на своя мандат, както помежду си, така и с националните органи, изпълняващи функции за брегова охрана[9], с оглед повишаване на морската ситуационна осведоменост и подкрепяне на съгласувани и икономически ефективни действия. През 2017 г.10 по този въпрос бе публикувано проучване, в което бяха идентифицирани допирни точки и начини за засилване на оперативната съвместимост и сътрудничеството в областта на оценката на риска между органите, изпълняващи функции за брегова охрана.

Свързаните с транспорта въпроси и възникващи заплахи — включително, но не само, по отношение на пристанищата — включват кибернетични заплахи за сигурността на въздухоплаването, заглушаване и заблуждаване на глобалната система за определяне на местоположението (GPS), заплахи за сателитите или проблеми в Далечния Север и Арктическия регион. Европейският център за високи постижения в борбата с хибридните заплахи в Хелзинки също допринася за анализа на тези свързани с транспорта хибридни заплахи и наскоро предприе изготвянето на анализ за защитата на пристанищата.

Митниците на ЕС играят ключова роля за гарантиране на сигурността на външната граница и на веригата на доставките, като по този начин допринасят за сигурността на Европейския съюз. Комисията значително подобрява системата за предварителна информация за товарите и митническата система за управление на риска, за да гарантира, че митниците в ЕС получават цялата необходима информация, споделят я по-ефективно между държавите членки, прилагат общи и специфични за държавите членки правила за риска и по-ефективно насочват действията си към рисковите пратки. Основен приоритет на Плана за действие на ЕС в областта на химическите, биологичните, радиологичните и ядрените материали[11] е да се гарантират сигурността на границите и капацитетът за откриване на незаконно влизащи химически, биологични, радиологични и ядрени материали. Адаптирането на системите за информация за товарите е от съществено значение за засилването на наблюдението и

---

[8] Регламент (ЕС) 2016/1624 за европейската гранична и брегова охрана

[9] Функциите за брегова охрана включват: 1) морска безопасност и управление на движението на плавателни съдове; 2) корабни аварии и услуги за морска помощ; 3) инспектиране и контрол на рибарството; 4) морски граничен контрол; 5) опазване на морската среда; 6) предотвратяване и възпиране на трафика и контрабандата и свързаното с това прилагане на морското право; 7) издирване и спасяване по море; 8) морски контрол и наблюдение; 9) митнически дейности по море; 10) реагиране при злополуки и бедствия по море; и 11) морска сигурност и сигурност на корабите и пристанищата

[10] https://publications.europa.eu/bg/publication-detail/-/publication/217db2fc-15d6-11e7-808e-01aa75ed71a1/language-bg

[11] COM(2017) 610 final, 18.10.2017 г.

основания на риска контрол на международните вериги на доставки, за да се гарантира, че в ЕС не влизат незаконно химически, биологични, радиологични и ядрени материали. В Петнадесетия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност се предоставят повече подробности относно мерките на ЕС за повишаване на готовността за борба с химическите, биологичните, радиологичните и ядрените рискове и по-специално относно действията, предприети на равнище ЕС в рамките на Плана за действие на Комисията за подобряване на готовността за действие срещу химически, биологични, радиологични и ядрени рискове за сигурността.

С цел да се премахнат пречките пред военната мобилност в ЕС, на 28 март 2018 г. върховният представител и Комисията представиха план за действие за проучване на възможностите за гражданско-военна употреба на трансевропейската мрежа с оглед опростяване на митническите формалности по отношение на военния транспорт и за разрешаване на регулаторни и процедурни проблеми, свързани с превоза на опасни товари за военни цели. Комисията предложи бюджет от 6,5 милиарда евро в рамките на клъстера „Отбрана“ от многогодишната финансова рамка, който ще бъде изпълняван чрез Механизма за свързване на Европа с цел подпомагане на адаптирането на транспортната инфраструктура към изискванията за военната мобилност. Целта е да се осигури възможност за двойна гражданско-военна употреба на транспортната инфраструктура.

<u>Действие 8</u>: Осигуряване на устойчивост на космическите активи

В допълнение към мерките, които вече са в сила за „Галилео“ и Европейската геостационарна служба за навигационно покритие (EGNOS), аспекти на сигурността са включени в предложението на Комисията за космическа програма на Съюза[12], както и в програмата „Коперник“, правителствените сателитни комуникации и рамката за подкрепа на космическото наблюдение и проследяване, като ще бъдат обхванати и аспектите на устойчивостта срещу хибридни заплахи.

Целта на космическото наблюдение и проследяване[13] е да се подкрепи дългосрочната наличност на европейските и националните космически инфраструктури, съоръжения и услуги. През юли 2016 г. в рамките на космическото наблюдение и проследяване започна предоставянето на начални услуги за избягване на сблъсъци, образуване на отломки и неконтролирано повторно навлизане на космически обекти. Националните оперативни центрове за космическо наблюдение и проследяване и Сателитният център на ЕС са въвели мерки за сигурност на данните, при които се вземат предвид препоръките на Съвета относно свързаните със сигурността аспекти на политиката по отношение на данните в областта на осведомяването относно ситуацията в космическото пространство[14].

Що се отнася до „Галилео“, Комисията предприема нови стъпки, за да гарантира по-добра защита на предоставянето на данни, които са от ключово значение за правилното функциониране на критичните инфраструктури, които зависят от сателитната навигация по отношение на точното време и синхронизацията. Използването на „Галилео“ се взема предвид при предоставянето на услуги за критични инфраструктури, като например енергийни мрежи, телекомуникационни мрежи и финансови пазари. В този контекст в предложението на Комисията за регламент за

[12] COM(2018) 447 final, 6.6.2018 г.

[13] Решение № 541/2014/ЕС на Европейския парламент и на Съвета от 16 април 2014 г. за създаване на рамка за подкрепа на космическото наблюдение и проследяване

[14] Политика по отношение на данните в областта на осведомяването относно ситуацията в космическото пространство (14698/12), 9.10.2012 г.

създаване на рамка за скрининг на преки чуждестранни инвестиции програмите за европейската глобална навигационна спътникова система (ГНСС) „Галилео“ и EGNOS се посочват като примери за проекти или програми от интерес за Съюза, които могат да бъдат от значение за скрининга на преки чуждестранни инвестиции съгласно предложения регламент[15].

Инициативата на ЕС за правителствени сателитни комуникации ще осигури гарантиран и сигурен достъп до сателитни комуникации за мисии, операции и ключови инфраструктури на Съюза и държавите членки. Това е важен инструмент за борба с хибридните заплахи за редица инфраструктури, включително космическите, транспортните и енергийните инфраструктури.

<u>Действие 9</u>: Адаптиране на отбранителните способности и развойната дейност от значение за ЕС

Европейският фонд за отбрана, създаден на 7 юни 2017 г., представлява значителна стъпка напред в стимулирането на усилията на държавите членки за увеличаване и поддържане на сътрудничеството в областта на отбраната в Европа, за да се отговори по ефективен начин на стратегическите предизвикателства. В рамките на компонента „способности“ на фонда ЕС ще допълни по-специално националното финансиране на проекти за развитие на съвместно сътрудничество в областта на отбраната. За тази цел през юни 2017 г. Комисията предложи регламент за създаване на Европейска програма за промишлено развитие в областта на отбраната с бюджет от 500 милиона евро за периода 2019—2020 г. На 22 май 2018 г. Европейският парламент и Съветът постигнаха предварително споразумение относно проекта за регламент. За следващата многогодишна финансова рамка на ЕС Комисията предложи интегриран Европейски фонд за отбрана с амбициозен бюджет от 13 милиарда евро, в който се предвиждат повече от 8,90 милиарда евро за свързаните със сътрудничество проекти за развитие на отбранителните способности. Потенциалното въздействие на борбата с хибридните заплахи върху развитието на способностите ще бъде интегрирано в преработения план за развитие на способностите, който предстои да бъде договорен от държавите членки през юни 2018 г.

<u>Действие 10</u>:Подготвеност срещу заплахи за здравето и механизми за координация

Подготвеността срещу заплахи за здравето е много важен елемент от цялостната подготвеност срещу химически, биологични, радиологични и ядрени рискове. Ето защо Комисията предприе стъпки в рамките на плана за действие на Комисията с цел засилване на подготвеността срещу химически, биологични, радиологични и ядрени рискове за сигурността. По-специално бяха положени усилия по отношение на инициативи за ефективно споделяне на експертен опит.

Поради това Комисията създаде „Химера“ — учение за секторите на здравеопазването, гражданската защита и сигурността в целия ЕС и в трети държави за изпитване на подготвеността и планирането на ответни действия срещу сериозни трансгранични заплахи. Във фиктивния сценарий на ученията беше включено умишленото разпространяване на заразна болест в комбинация с кибератаки върху критични инфраструктури, включително болници, с цел да се изпитат съществуващите механизми, системи и инструменти за комуникация на национално и европейско равнище при отговор на хибридна заплаха. Ученията на равнище ЕС се проведе на 30—31 януари 2018 г. в Люксембург. То допринесе за подпомагане на междусекторното изграждане на капацитет и подобряване на оперативната съвместимост и координацията между секторите на здравеопазването, гражданската защита и

[15] Вж. приложението в документ COM(2017) 487 final.

сигурността на равнище ЕС и държави членки, както и на сътрудничеството с международни партньори. Ученията също така помогна да се идентифицират настоящите отговорности и роли на всички заинтересовани страни при управление на кризи, породени от хибридни заплахи. Беше изпитан начинът, по който си взаимодействат системата за ранно предупреждение и реагиране (CPIP), междусекторната система за предупреждение на Комисията (ARGUS), общата система за спешна комуникация и информация (CECIS) и интегрираните договорености за реакция на политическо равнище в кризисни ситуации (IPCR) на Съвета. В Петнадесетия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност се предоставят повече подробности относно мерките на ЕС за повишаване на подготвеността за борба с химически, биологични, радиологични и ядрени рискове.

През април 2018 г. Комисията публикува съобщение и представи предложение за препоръка на Съвета за засилване на сътрудничеството в борбата срещу болести, предотвратими чрез ваксинация, с цел тя да бъде приета преди края на 2018 г. Целта ѝ е да бъдат преодолени колебанията относно ваксинацията, да се подобри устойчивостта на програмите за ваксинация и да се засили ефективността на научноизследователската и развойната дейност в областта на ваксините.

Що се отнася до Европейския медицински корпус, норвежкият екип за спешна медицинска помощ бе сертифициран от Световната здравна организация (СЗО), което означава, че той изпълнява минималните стандарти за качество. През април 2018 г. се проведе първата регионална среща на екипите за спешна медицинска помощ от европейския регион на СЗО; тази среща беше организирана съвместно от Комисията, Световната здравна организация и белгийските здравни органи в качеството им на председател на регионалната група.

Понастоящем в тясно сътрудничество с Европейската асоциация по изгаряния и държавите членки е в ход подготовка за разработването на механизъм за управление на бедствия с масови поражения от изгаряне. В началото на октомври 2018 г. Комисията и държавите членки ще се срещнат в рамките на работен семинар, за да финализират работата.

<u>Действие 11</u>:Мрежа на екипите за реагиране при инциденти с киберсигурността (CSIRT), CERT-EU и Директивата за сигурност на мрежите и информационните системи (Директива за МИС)

Периодично или на *ad hoc* принцип CERT-EU изготвя свързани с критични сектори продукти за оценка на кибернетичните заплахи. По отношение на различните видове транспорт (въздушен, морски и наземен) Комисията редовно наблюдава и гарантира, че секторните инициативи в областта на кибернетичните заплахи съответстват на междусекторните способности, обхванати от Директивата за сигурност на мрежите и информационните системи (Директивата за МИС).

През септември 2017 г. Европейската агенция по отбрана и естонското председателство на Съвета на ЕС организираха стратегическо симулационно кибернетично упражнение за министрите на отбраната на ЕС, наречено „CYBRID17“, с цел повишаване на осведомеността относно координацията на политическо равнище при инциденти, свързани с киберсигурността, и относно потенциалните последици от агресивни киберкампании. То бе с акцент върху ситуационната осведоменост, механизмите за реагиране при кризи и стратегическата комуникация. Европейската агенция по отбрана ще включи елементите на това упражнение в платформата за образование, обучение, оценка и учения на Европейския колеж по сигурност и отбрана, която ще бъде създадена през септември 2018 г. Понастоящем се разглежда възможността за

провеждането в бъдеще на подобни учения на високо равнище от председателствата на ЕС .

<u>Действие 12</u>:Договорно публично-частно партньорство за киберсигурност

Комисията сключи публично-частно партньорство (ПЧП) за киберсигурност с Европейската организация за киберсигурност (ECSO), за да стимулира конкурентоспособността и капацитета за иновации на промишлеността за цифрова сигурност и защита на личния живот в Европа. ЕС ще инвестира до 450 милиона евро в това партньорство, за да защити потребителите и инфраструктурите от кибератаки. Очаква се ПЧП да привлече инвестиции от 1,8 милиарда евро до 2020 г.

Що се отнася до киберсигурността, в *съвместното съобщение от септември 2017 г. „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност в ЕС*[16]“ се посочват мерки, които да дадат значителен тласък на структурите и капацитета на ЕС за киберсигурност, както е определено в това съобщение. Въпреки това ефективната кибесигурност в ЕС е възпрепятствана от недостатъчни инвестиции и недостатъчна координация. ЕС се стреми да разреши този въпрос, както е посочено в съвместното съобщение.

<u>Действие 13</u>:Устойчивост на сектора на енергетиката

През юни 2018 г. Комисията ще създаде работен поток за сектора на енергетиката в рамките на групата за сътрудничество във връзка с МИС, за да разгледа особеностите на сектора на енергетиката и да предостави ръководство за държавите членки относно изпълнението в този сектор на Директивата за сигурност на мрежите и информационните системи (Директивата за МИС). Успоредно с това Комисията работи върху специфично ръководство за киберсигурността, което надхвърля Директивата за МИС, с цел да се определят добри практики в областта на киберсигурността в сектора на енергетиката и да бъде обърнато внимание на операторите, които не са обхванати от Директивата за МИС. Комисията ще продължи да организира мероприятия за обмен на информация по въпросите на киберсигурността в сектора на енергетиката, с цел повишаване на осведомеността, споделяне на най-добри практики, засилване на сътрудничеството (в трансграничен план и между операторите на електропреносни системи и операторите на разпределителни системи), разглеждане на въпроси, свързани с физическите мерки, новите рискове, както и образованието и уменията.

В дългосрочен план Комисията ще изготви мрежови кодекс за специфичните за сектора правила за киберсигурност, както се предлага в преработения текст на предложението за Регламент за електроенергията[17], по отношение на което е в ход законодателна процедура.

<u>Действие 14</u>:Устойчивост на финансовия сектор: платформи и мрежи за обмен на информация

В плана за действие на Комисията в областта на финансовите технологии се разглеждат потенциалните пречки, които ограничават обмена на информация относно кибернетичните заплахи между участниците на финансовите пазари, и се идентифицират потенциални решения за преодоляването им. В допълнение към това на CERT-EU е поверена роля в обмена на информация относно инциденти.

---

[16] JOIN(2017) 450 final.

[17] Предложение за Регламент на Европейския парламент и на Съвета относно вътрешния пазар на електроенергия (преработен текст) — COM(2016) 861 final.

<u>Действие 15</u>: Устойчивост срещу кибератаки в транспортния сектор

Защитата на различните видове транспорт от атаки срещу киберсигурността е основен приоритет за Комисията. В областта на гражданското въздухоплаване е налице значителен напредък от гледна точка на киберсигурността, но уязвимостта на системите от техническа неизправност или от заплаха за киберсигурността никога не може да бъде отхвърлена, както показа скорошният инцидент в областта на ИТ с ЕВРОКОНТРОЛ, който засегна половината от полетите в Европа. Комисията тясно си сътрудничи с Европейската агенция за авиационна безопасност в тази област на транспорта. CERT-EU подписа споразумение за нивото на обслужване с ЕВРОКОНТРОЛ и Меморандум за сътрудничество с Европейската агенция за авиационна безопасност, за да помогне на тези субекти и свързаните с тях заинтересовани страни да се справят с кибернетичните заплахи.

Що се отнася до морския транспорт, корабната индустрия публикува насоки за киберсигурност, в които перспективата и подходът са предимно глобални и които впоследствие бяха обсъдени и приети от Международната морска организация. Киберсигурността в европейските пристанища и пристанищни съоръжения остава важен приоритет на политиката, който редовно се разглежда и обсъжда с държавите членки, промишлеността и заинтересованите страни в контекста на прилагането на Директивата за сигурност на мрежите и информационните системи и последващите действия във връзка с тази директива.

Комисията възнамерява да разработи цялостен и интерактивен набор от инструменти за знания в областта на киберсигурността, включващ препоръчителни добри практики, с цел подпомагане на ръководителите по сигурността и специалистите в транспортния сектор по-добре да идентифицират, оценяват и смекчават рисковете за кибесигурността.

<u>Действие 16</u>: Борба с финансирането на тероризма

През изминалата година Комисията положи значителни усилия за борба с финансирането на тероризма, както се съобщава в редовните доклади за Съюза на сигурност. Наскоро в пакета си за сигурността от април 2018 г.[18] Комисията предприе по-нататъшни мерки, за да се задълбочи сътрудничеството между органите, които отговарят за борбата с тежката престъпност и тероризма, както и да се подобри достъпът на тези органи до финансова информация и използването на тази информация от тяхна страна, като предложи директива[19] за улесняване на използването на финансова и друга информация за целите на предотвратяването, разкриването, разследването или наказателното преследване на тежки престъпления. Повече подробности относно неотдавнашната дейност на равнище ЕС за борба с финансирането на тероризма са посочени в Петнадесетия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност.

За да се хармонизират санкциите за престъпленията, свързани с изпиране на пари, Комисията предложи законодателство, което да бъде прието в средата на 2018 г. Освен това през май тази година беше приета Петата директива относно борбата с изпирането на пари с цел укрепването на редица мерки, като например подобряване на проверките на високорискови трети държави, проверки на платформите за обмен на виртуални валути, мерки за прозрачност, приложими за предплатени инструменти, нови правомощия на звената за финансово разузнаване и бърз достъп за звената за финансово разузнаване до информация относно притежателите на банкови и

[18] COM(2018) 211 final.

[19] COM(2018) 213 final.

разплащателни сметки чрез централизирани регистри или електронни системи за извличане на данни.

<u>Действие 17</u>:Действия срещу радикализацията и анализ на необходимостта да се подобрят процедурите за премахване на незаконно съдържание

Предотвратяването на радикализация, която води до насилие, както офлайн, така и онлайн, през последните години представлява приоритет за Комисията. За да се ускори работата на равнище ЕС, Комисията създаде експертна група на високо равнище по въпросите на радикализацията, която да отправя препоръки относно координацията, обхвата и въздействието на политиките на ЕС за превенция. Експертната група на високо равнище по въпросите на радикализацията представи своя окончателен доклад на 18 май 2018 г., в който е включена препоръка за създаване на механизъм за сътрудничество на равнището на ЕС.

Що се отнася до борбата с незаконното съдържание онлайн, след приемането на препоръката на Комисията от 1 март 2018 г. вниманието бе насочено към ограничаване на достъпността на такова съдържание онлайн. Комисията започна извършването на оценка на въздействието, за да определи дали настоящите усилия са достатъчни или са необходими допълнителни мерки за гарантиране на бързото и проактивно откриване и премахване на незаконно съдържание онлайн, включително евентуални законодателни мерки за допълване на съществуващата нормативна уредба. Работата на Комисията, извършена в тази област, е представена по-подробно в Петнадесетия доклад за напредъка по създаването на ефективен и истински Съюз на сигурност.

Кодексът на поведение за противодействие на незаконните изказвания онлайн, пораждащи омраза, разработен съвместно с Facebook, Twitter, Google (YouTube) и Microsoft, осигурява бързи и положителни резултати. Кодексът на поведение гарантира, че компаниите са постигнали значителен напредък по отношение на бързото преглеждане и премахване на предполагаемите незаконни изказвания онлайн, пораждащи омраза, за които са били уведомени. Третата проверка на Комисията относно изпълнението на Кодекса, публикувана през януари 2018 г., показва, че средно 70 % от съдържанието, включващо изказвания, пораждащи омраза, се отстранява, като прегледът за такива изказвания се извършва в рамките на 24 часа, както е предвидено в Кодекса на поведение. Кодексът се превърна в стандарт в сектора и неотдавнашното решение на Instagram и Google+ да се присъединят към него е обнадеждаващо. През март 2018 г. Комисията също така предложи допълнителни мерки за онлайн платформите, като например автоматично откриване, прозрачност и обратна информация за потребителите, както и гаранции с цел защита на свободата на словото[20].

Освен вече предприетите действия срещу радикализацията и изказванията онлайн, пораждащи омраза, следва да се предприемат стъпки за предотвратяване и смекчаване на заплахите от кибератаки във връзка с изборите.

<u>Действие 18</u>:Засилване на сътрудничеството със съседните на ЕС региони и трети държави

Европейският съюз постави по-голям акцент върху изграждането на капацитет и устойчивост в сектора на сигурността в партньорски държави, наред с другото, чрез развиване на свързаното със сигурността измерение на преразгледаната европейска политика за съседство. С цел повишаване на капацитета на партньорите за борба с хибридните заплахи бяха започнати специални проучвания на хибридните рискове, за да се идентифицират критичните им уязвимости и да се осигури целенасочена

[20] C(2018) 1177 final.

подкрепа. Европейската служба за външна дейност (ЕСВД), в сътрудничество с Комисията, проведе проучване с Република Молдова. През 2018 г. Йордания и Грузия официално поискаха от ЕС да проведе проучвания за уязвимост, като първата стъпка бе въпросникът да се приспособи към техните специфични нужди. В Украйна беше предприета допълнителна работа по изграждане на капацитет за киберсигурност, по-специално по отношение на критичните инфраструктури, чрез мисии за техническа помощ, а в началото на 2018 г. Комисията също така стартира всеобхватна нова програма, насочена към повишаване на киберустойчивостта на трети държави, по-специално в Африка и Азия.

ЕС продължава да обсъжда плановете и програмите за изграждане на капацитет за ядрена сигурност с Международната агенция за атомна енергия и правителството на САЩ в рамките на Работната група по наблюдение на границите. Европейския център за обучение по ядрена сигурност (EUSECTRA) осигурява обучение по предотвратяване и откриване в областта на ядрената сигурност, както и модули за реагиране при ядрени инциденти. В плана за действие на Комисията за подобряване на готовността за действие срещу химически, биологични, радиологични и ядрени рискове за сигурността се посочват конкретни действия за сътрудничество с ключови международни партньори, включително в контекста на диалозите със съответните трети държави относно борбата с тероризма и относно сигурността.

Финансираната от ЕС инициатива за центрове за високи постижения за намаляване на химическите, биологичните, радиологичните и ядрените рискове, която обхваща почти всички партньорски държави[21], продължава работата си по подобряване на националните и регионалните възможности на партньорските държави по въпросите на предотвратяването, подготвеността и ответните действия по отношение на тези заплахи, включително тези, които включват структури с „твърда сигурност“.

В държавите от Южното и Източното съседство обученията и ученията в областта на гражданската защита се организират в рамките на регионалните програми за предотвратяване, подготвеност и отговор на природни и предизвикани от човека бедствия (PPRD). Третата фаза на PPRD Юг стартира през 2018 г., а втората фаза на PPRD Изток ще приключи през ноември 2018 г., като е възможно срокът да бъде удължен. Следва да се осигурят тесни връзки с регионалните центрове за високи постижения за намаляване на химическите, биологичните, радиологичните и ядрените рискове и с програмите ППРР Юг и ППРР Изток.

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 значителен 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. Редовният мониторинг и провеждането на учения ще продължат.

[21] Центрове за високи постижения за намаляване на химическите, биологичните, радиологичните и ядрените рискове съществуват в Рабат, Алжир, Аман и Тбилиси.

<u>Действие 19</u>: Общ оперативен протокол и учения за подобряване на капацитета за вземане на стратегически решения в отговор на комплексни хибридни заплахи

Оперативният протокол на ЕС беше създаден чрез общ работен документ на службите през юни 2016 г. В него се съдържа основното ръководство за общоинституционална реакция в кризисни ситуации. По време на EUPACE17 протоколът беше изпитан спрямо сценария на хибридна заплаха и се оказа безценен инструмент за улесняване на взаимовръзката между службите. Освен това той осигури допирни точки за взаимодействие между различните равнища на отговор: политическо и стратегическо, оперативно и техническо, както и между трите основни механизма за реагиране на ЕС в случай на криза (за външни кризи), ARGUS (основаващата се на информационните технологии вътрешна платформа на Комисията за обмен на информация) и интегрираната платформа на Съвета за реакция на политическо равнище в кризисни ситуации. Протоколът също доказа своята полезност и по време на паралелното учение с НАТО CMX'17. Следващото от поредицата учения PACE'18 ще се проведе през ноември 2018 г. и като се вземат предвид всички извлечени поуки за бъдещето, ще се обмисли актуализирането на протокола.

През септември и октомври 2017 г. ЕС проведе първото паралелно и координирано учение с НАТО (PACE17), като тества подготвеността на двете организации и взаимодействието между тях в случай на мащабна хибридна криза. В подготвителния етап се проведе интензивен обмен на персонал във всичките четири области на оперативния протокол на ЕС за борбата с хибридните заплахи (EU Playbook): ранно предупреждение/ситуационна осведоменост; стратегическа комуникация; киберзащита; предотвратяване и реакция на кризи. Мащабът на взаимодействието между екипите на ЕС и НАТО по време на EUPACE17 е безпрецедентен. Това беше и първият случай, в който НАТО участва в кръгла маса относно интегрираните договорености за реакция на политическо равнище в кризисни ситуации, ръководена от председателството. По този повод висши представители на ЕС участваха в обсъжданията в рамките на Северноатлантическия съвет. В процеса, водещ до извличането на поуки, акцентът беше върху няколко аспекта, включително взаимодействието между механизмите за реагиране при кризи на ЕС и НАТО и предизвикателствата, свързани с обмена на класифицирана информация между служителите на двете организации, включително необходимостта от сигурна комуникация, по-специално с цел в бъдеще да се гарантира бърз и сигурен обмен при пълно зачитане на необходимостта от контрол от страна на инициатора.

В процес на планиране е паралелното и координирано учение през 2018 г., в което ЕС ще бъде водещата организация.

<u>Действие 20</u>: Разглеждане на приложимостта и практическите последици на член 222 от ДФЕС и член 42, параграф 7 от ДЕС в случай на мащабна и сериозна хибридна атака

Приложимостта на клаузата за солидарност на ЕС и на механизма му за взаимопомощ, както и взаимодействието помежду им и с механизмите за реагиране на НАТО, включително колективната отбрана по член 5, се обсъждат и изпитват допълнително в учения със сценарий за хибридна атака. Европейският център за високи постижения в борбата с хибридните заплахи в Хелзинки е заинтересован и готов да продължи работата както по отношение на научните изследвания, така и по отношение на ученията, като по този начин спомага за разработването на общо разбиране от страна на държавите членки и съюзниците.

<u>Действие 21</u>: ***Интегриране, използване и координиране на 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 общата външна политика и политиката на сигурност/общата политика за сигурност и отбрана и след семинар с военни експерти, проведен през декември 2016 г., и насоки, приети 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 Общата политика за сигурност и отбрана“. Тази работа се осъществява чрез Плана за изпълнение относно разработването на концепции. След консултация с европейския център за високи постижения в борбата с хибридните заплахи Военният секретариат на ЕС разработва концепция за това как военните могат да допринесат за борбата с хибридните заплахи, включително чрез мисии и операции в рамките на общата политика за сигурност и отбрана.

Освен това ежедневно военният секретариат на ЕС и държавите членки осигуряват възможности за подобряване на ранното предупреждение, като предоставят свързана с военното разузнаване подкрепа за звеното на ЕС за синтез на информацията за хибридните заплахи. Единната способност за аналитично разузнаване подпомага оперативните групи на ЕСВД за стратегическа комуникация чрез осигуряване на военни становища с цел противодействие на дезинформационните кампании, насочени срещу ЕС и отделни държави членки.

Военните способности за борба с хибридните заплахи ще бъдат упражнени по време на паралелното и координирано учение на НАТО през 2018 г. (PACE18). Въз основа на сценария за хибридна атака от PACE18 военният секретариат на ЕС и международният военен щаб на НАТО ще проведат основани на различни сценарии неофициални дискусии между ЕС и НАТО, за да гарантират взаимното допълване в борбата с хибридните заплахи, където изискванията се припокриват, въз основа на принципа на приобщаване, като същевременно зачитат автономията по отношение на вземане на решения на всяка от организациите, както и правилата за защита на личните данни.

СЪТРУДНИЧЕСТВОТО МЕЖДУ ЕС И НАТО

<u>Действие 22</u>: ***Сътрудничество между ЕС и НАТО в областта на ситуационната осведоменост, стратегическата комуникация, кибернетичната сигурност и предотвратяването и реакцията на кризи***

Борбата с хибридните заплахи продължава да бъде ключова област на взаимодействие между ЕС и НАТО. Тя се основава на разбирането, че в случай на хибридна заплаха ресурсите и способностите, които двете организации могат да мобилизират, се допълват и укрепват способността на държавите членки и съюзниците да предотвратяват, възпират и реагират на такива заплахи. По време на ученията PACE17 бяха изпитани оперативните протоколи на двете организации и съответно способността им да работят заедно бързо и ефективно в подкрепа на техните засегнати членове. С оглед на придобития опит двата оперативни протокола ще бъдат преразгледани и актуализирани. Що се отнася до стратегическата комуникация, бяха проведени консултации за оказване на подкрепа на Украйна, Босна и Херцеговина, Република Молдова и Грузия.

През септември 2017 г. на семинара на ЕС и НАТО за устойчивост се събраха експерти в критични стратегически сектори с цел обмен на информация за съответните дейности и проучване на предложения за по-нататъшна работа, по-специално в областта на защитата на критичните инфраструктури.

През 2018 г. ще продължи да се осъществява проектът „Военна мобилност“, който цели улесняване на движението на военни материали и персонал и при който биха могли да се вземат предвид вероятните предизвикателства, свързани с хибридни заплахи, специално предназначени да забавят времето за реакция на държавите членки и съюзниците — това е област, която ще бъде тествана при бъдещо паралелно учение и ще бъде взета предвид в поредицата от учения EUPACE19/20.

Координирането на усилията за обучение в областта на киберсигурността представлява важна област за по-тясно взаимодействие. НАТО участва също така като наблюдател в симулационното учение CyberEurope на Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) през юни 2018 г.

ЗАКЛЮЧЕНИЕ

Подобряването на ситуационната осведоменост и изграждането на устойчивост срещу развиващите се хибридни заплахи от различни източници продължава да бъде предизвикателство и изисква постоянни усилия от страна на ЕС. Съвместната рамка включва широк набор от действия, вариращи от подобряване на синтеза и обмена на информация, засилване на защитата на критичната инфраструктура и киберсигурността до изграждане на общества, устойчиви на радикализацията и насилническия екстремизъм. Рамката на ЕС за борба с хибридните заплахи позволи да се предостави подкрепа на държавите членки посредством различни мерки, насочени към укрепване на капацитета на ЕС и на държавите членки да издържат на стрес, да реагират координирано на вредни атаки и, на последно място, да се възстановяват от последствията им.

Ответните действия на ЕС спрямо хибридните заплахи също така бяха успешно тествани и упражнявани съвместно с НАТО в редица учения, като планът е работата да продължи в тази посока. Тясното сътрудничество между всички съответни участници в рамките на ЕС и с НАТО е ключът към усилията за изграждане на устойчивост. В допълнение подпомагането на съседните партньорски държави при идентифицирането на уязвимите им места и укрепването на изграждането на капацитет срещу хибридните заплахи допринася за по-доброто разбиране на естеството на външните заплахи и по този начин води до повишена сигурност за съседните на ЕС държави.