ЕВРОПЕЙСКА
КОМИСИЯ

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

Брюксел, 6.4.2016 г.
JOIN(2016) 18 final

СЪВМЕСТНО СЪОБЩЕНИЕ ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Съвместна рамка за борба с хибридните заплахи

— ответни действия на Европейския съюз

1. ВЪВЕДЕНИЕ

През последните години обстановката в Европейския съюз в областта на сигурността се промени драстично. Големите предизвикателства пред мира и стабилността в източните и южните съседки на ЕС продължават да подчертават необходимостта Съюзът да се адаптира и да увеличи капацитета си като гарант на сигурността, със силен акцент върху тясната връзка между външната и вътрешната сигурност. Голяма част от настоящите предизвикателства пред мира, сигурността и просперитета са резултат от нестабилността в съседните на ЕС държави и променящите се видове заплахи. През 2014 г. председателят на Европейската комисия Жан-Клод Юнкер подчерта в своите Политически насоки необходимостта „да работим за по-силна Европа в областта на сигурността и отбраната“ и да съчетаваме европейските и националните инструменти по по-ефективен начин, отколкото в миналото. Освен това вследствие на призива, отправен от Съвета по външни работи на 18 май 2015 г., върховният представител, в тясно сътрудничество със службите на Комисията и Европейската агенция по отбрана (EDA) и в консултация с държавите — членки на ЕС, предприе действия за представянето на настоящата съвместна рамка с практически предложения за подпомагане на борбата с хибридните заплахи и за укрепване на устойчивостта на ЕС и неговите държави членки, както и на техните партньори[1]. През юни 2015 г. Европейският съвет припомни необходимостта да се мобилизират инструментите на ЕС за подпомагане на борбата с хибридните заплахи[2].

Макар че определенията за хибридните заплахи се различават и трябва да се запазят гъвкави, за да отразяват тяхното развитие, понятието обхваща комбинацията от насилнически и подривни дейности, конвенционални и неконвенционални методи (т.е. дипломатически, военни, икономически, технологични), които се използват по координиран начин от държавни или недържавни субекти с цел постигане на конкретни цели, в отсъствието на официално обявена война. Обикновено акцентът е върху използването на слабите места на набелязаната цел и създаването на неяснота, с което да се възпрепятстват процесите на вземане на решения. Масовите дезинформационни кампании, използването на социалните медии за контрол на политическия наратив или за радикализиране, набиране и командване на подставени лица могат да бъдат средства за хибридни заплахи.

Дотолкова доколкото борбата с хибридните заплахи е свързана с националната сигурност и отбраната и с поддържането на законността и реда, държавите членки носят основната отговорност, защото като цяло уязвимите места са специфични за всяка държава. При все това много държави — членки на ЕС, са изправени пред общи заплахи, които могат да са насочени и към трансгранични мрежи или инфраструктури. На такива заплахи може да се противодейства по-ефективно чрез

[1] Заключения на Съвета относно общата политика за сигурност и отбрана (ОПСО), май 2015 г. (док. 8971/15).
[2] Заключения на Европейския съвет, юни 2015 г. (док. EUCO 22/15).

координирани действия на равнище ЕС, като се използват политиките и инструментите на ЕС, за да се черпи от европейската солидарност, взаимната помощ и пълния потенциал на Договора от Лисабон. Политиките и инструментите на ЕС могат да имат основна роля и добавена стойност за повишаването на осведомеността и в значителна степен вече го правят. Това помага да се повиши устойчивостта на държавите членки за ответни действия на общите заплахи. Предложената в настоящата рамка външна дейност на Съюза се ръководи от принципите, залегнали в член 21 от Договора за Европейския съюз (ДЕС), сред които са демокрацията, правовата държава, универсалността и неделимостта на правата на човека и зачитането на принципите на Устава на Организацията на обединените нации и на международното право[3].

Целта на настоящото съвместно съобщение е да се способства за цялостен подход, който ще даде възможност на ЕС, в координация с държавите членки, да противодейства конкретно на заплахите от хибридно естество, като се създадат синергии между всички значими инструменти и се изгради тясно сътрудничество с всички значими субекти[4]. Действията се основават на съществуващите стратегии и секторни политики, които допринасят за постигането на по-голяма сигурност. По-специално, Европейската програма за сигурност[5], предстоящата глобална стратегия на Европейския съюз в областта на външните работи и политиката на сигурност и предстоящият европейски план за действие в областта на отбраната[6], Стратегията на ЕС за киберсигурност[7], Стратегията за енергийна сигурност[8], Стратегията на Европейския съюз за морска сигурност[9] са инструменти, които също могат да допринесат за борбата с хибридните заплахи.

Тъй като НАТО също полага усилия за борба с хибридните заплахи, а Съветът по външни работи предложи да се активизират сътрудничеството и координацията в тази област, някои от предложенията имат за цел да се засили сътрудничеството между ЕС и НАТО в борбата с хибридните заплахи.

Предлага се ответните действия да се съсредоточат върху следните елементи: подобряването на осведомеността, изграждането на устойчивост, предотвратяването, реакцията при кризи и възстановяването.

---

[3] Хартата на основните права на ЕС има задължителен характер за институциите и за държавите членки, когато те прилагат правото на Съюза.

[4] Към евентуалните законодателни предложения ще се прилагат изискванията за по-добро регулиране на Комисията в съответствие с Насоките на Комисията за по-добро регулиране (SWD (2015) 111).

[5] COM(2015) 185 final.

[6] Предстои да бъдат представени през 2016 г.

[7] Рамка за политиката на ЕС за кибернетична отбрана (док. 15585/14 на Съвета) и съвместно съобщение „Стратегия на Европейския съюз за киберсигурност: отворено, безопасно и сигурно киберпространство“ (JOIN(2013)1, февруари 2013 г.).

[8] Съвместно съобщение „Европейска стратегия за енергийна сигурност“ (SWD (2014) 330, май 2014 г.).

[9] Съвместно съобщение „За отворено и сигурно общо морско пространство: елементи за изготвянето на стратегия на Европейския съюз за морска сигурност“ (JOIN(2014) 9 final от 6 март 2014 г.).

2. РАЗПОЗНАВАНЕ НА ХИБРИДНОТО ЕСТЕСТВО НА ДАДЕНА ЗАПЛАХА

Хибридните заплахи са насочени към уязвимите места на дадена държава и често тяхната цел е да подкопаят основните демократични ценности и свободи. Като първа стъпка върховният представител и Комисията ще работят съвместно с държавите членки за повишаване на ситуационната осведоменост чрез мониторинг и оценка на рисковете, на които са изложени уязвимите места в ЕС. Комисията разработва методологии за оценка на риска за сигурността, които да спомогнат за информираността на вземащите решения лица и за насърчаването на основано на риска формулиране на политики в различни области — от сигурността на въздухоплаването до финансирането на тероризма и изпирането на пари. Освен това би било уместно държавите членки да направят проучване, с което да определят кои области са уязвими спрямо хибридните заплахи. Целта е да се установят показатели за хибридните заплахи, които да бъдат включени в съществуващите механизми за ранно предупреждение и оценка на риска и да бъдат споделяни по подходящ начин.

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

3. ОРГАНИЗИРАНЕ НА ОТВЕТНИТЕ ДЕЙСТВИЯ НА ЕС: ПОДОБРЯВАНЕ НА ОСВЕДОМЕНОСТТА

3.1. Звено на ЕС за синтез на информацията за хибридните заплахи

Жизненоважно е ЕС, в координация с държавите членки, да има задоволително ниво на ситуационна осведоменост, така че да може да идентифицира всяка свързана с хибридна дейност промяна в обстановката по отношение на сигурността, предизвикана от държавни и/или недържавни субекти. За да се противодейства ефективно на хибридните заплахи, е важно да се подобри обменът на информация и да се насърчи съответният обмен на разузнавателни данни между различните сектори и между Европейския съюз и неговите държави членки и партньори.

Звеното на ЕС за синтез на информацията за хибридните заплахи, създадено в рамките на Центъра на ЕС за анализ на информация (EU INTCEN) към Европейската служба за външна дейност (ЕСВД), ще представлява сборна точка за анализ на хибридните заплахи. Това звено за синтез ще получава, анализира и обменя класифицирана информация и информация от открити източници, която се отнася конкретно до показателите и предупрежденията, свързани с хибридните заплахи, и се предоставя от различни отдели на ЕСВД (включително делегациите

на ЕС), Комисията (и агенциите на ЕС[10]) и държавите членки. Съвместно с другите подобни органи на равнището на ЕС[11] и на национално равнище звеното за синтез ще анализира външните аспекти на хибридните заплахи, засягащи ЕС и съседните му държави, като целта е да се анализират бързо значимите инциденти и да се предоставят сведения, които да бъдат използвани при вземането на стратегически решения в ЕС, включително при оценките на риска за сигурността, извършвани на равнище ЕС. Аналитичните резултати от работата на звеното за синтез ще бъдат обработвани и третирани в съответствие с правилата на Европейския съюз за класифицираната информация и защитата на данни[12]. Звеното следва да поддържа връзка със съществуващите органи на равнището на ЕС и на национално равнище. Държавите членки следва да създадат национални звена за контакт, свързани със звеното на ЕС за синтез на информацията за хибридните заплахи. Служителите във и извън ЕС (включително тези в делегациите на ЕС и командированите по линия на операции и мисии) и в държавите членки следва да бъдат обучени да разпознават ранните признаци на хибридни заплахи.

<u>Действие 2</u>: създаване на звено на ЕС за синтез на информацията за хибридните заплахи в рамките на съществуващата структура на INTCEN на ЕС, 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.

3.2. Стратегическа комуникация

Създателите на хибридните заплахи могат систематично да дезинформират, включително чрез целенасочени кампании в социалните медии, като по този начин се опитват да радикализират отделни лица, да дестабилизират обществото и да контролират политическия наратив. От основно значение е способността да се реагира на хибридните заплахи, като се използва силна **стратегическа комуникация**. Предоставянето на бързи и основани на факти отговори и повишаването на обществената осведоменост относно хибридните заплахи са основни фактори за изграждането на устойчивост у обществото.

Стратегическата комуникация следва да използва пълноценно съществуващите инструменти на социалните медии, както и традиционните визуални, аудио и онлайн медии. Въз основа на дейностите на работните групи за стратегическа комуникация в Източна и Арабския свят ЕСВД следва да оптимизира използването на лингвисти, владеещи необходимите езици, и на специалисти по социалните

[10] В съответствие с техния мандат.
[11] Например Европейският център за борба с киберпрестъпността и Центърът за борба с тероризма към Европол, Frontex, Екипът на ЕС за незабавно реагиране при компютърни инциденти (CERT-EU).
[12] Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г.

медии, които могат да следят информацията с произход извън ЕС и да осигурят целенасочена комуникация в случай на дезинформация. Освен това държавите членки следва да разработят съгласувани механизми за стратегическа комуникация, които да способстват за откриването на източниците на дезинформация и за борбата с тях с цел разкриване на хибридните заплахи.

<u>Действие 3</u>: 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.

3.3. Център за високи постижения в борбата с хибридните заплахи

Въз основа на опита на някои държави членки и партньорски организации[13] един международен институт или мрежа от международни институти биха могли да действат като център за високи постижения в борбата с хибридните заплахи. Този център би могъл да се съсредоточи върху изследването на начините, по които се прилагат хибридните стратегии, и би могъл да насърчи разработването на нови концепции и технологии в частния сектор и индустрията, с които да се помогне на държавите членки да изградят устойчивост. Изследванията биха могли да спомогнат за хармонизирането на националните политики, доктрини и концепции и тези на ЕС, и да гарантират, че при вземането на решения се отчитат комплексността и неопределеността, свързани с хибридните заплахи. Центърът следва да разработва програми за напредък в изследванията и учения с цел намирането на практически решения на предизвикателствата, свързани с хибридните заплахи. Този център ще черпи сила от експертния опит на участващите в него многонационални и междусекторни субекти от гражданския, военния и частния сектор и академичните среди.

Центърът би могъл да работи в тясно сътрудничество със съществуващите центрове за високи постижения на ЕС[14] и НАТО[15], за да може да използва задълбочените познания за хибридните заплахи, придобити чрез дейности в областта на киберотбраната, стратегическата комуникация, гражданско-военното сътрудничество, енергетиката и реакцията при кризи.

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

[13] Центрове за високи постижения на НАТО.
[14] Напр. Институтът на ЕС за изследване на сигурността (EU ISS), тематичните центрове за високи постижения на ЕС в областта на ХБРЯ.
[15] http://www.nato.int/cps/en/natohq/topics_68372.htm.

4. ОРГАНИЗИРАНЕ НА ОТВЕТНИТЕ ДЕЙСТВИЯ НА ЕС: ИЗГРАЖДАНЕ НА УСТОЙЧИВОСТ

Устойчивостта е способността за издържане на стрес и възстановяване, която се увеличава постепенно вследствие на придобития от предизвикателствата опит. За да се противодейства ефективно на хибридните заплахи, трябва да се обърне внимание на потенциалните уязвими места на ключовите инфраструктури, веригите за доставки и обществото. Инфраструктурата на равнище ЕС може да стане по-устойчива чрез използването на инструментите и политиките на ЕС.

4.1. Защитаване на критичната инфраструктура

Важно е критичните инфраструктури (например веригите за енергийни доставки, транспорта) да се защитават, тъй като едно неконвенционално нападение от създатели на хибридни заплахи върху която и да е „лесна мишена“ би могло да доведе до сериозни икономически или социални сътресения. За да се осигури защитата на критичната инфраструктура, в Европейската програма за защита на критичната инфраструктура[16] (EPCIP) се предвижда подход, който обхваща всички опасности за междусекторните системи, отчита взаимозависимостите и се основава на изпълнението на дейности за предотвратяване, подготвеност и ответни действия. С Директивата за европейските критични инфраструктури[17] се създава процедура за установяване и означаване на европейските критични инфраструктури (ЕКИ) и за оценка на необходимостта от подобряване на тяхната защита. По-конкретно, следва да бъде възобновена работата съгласно Директивата за повишаване на устойчивостта на критичните инфраструктури, свързани с транспорта (напр. основните летища и търговски пристанища на ЕС). Комисията ще направи оценка на необходимостта от разработване на общи инструменти, включително показатели, за подобряване на устойчивостта на критичната инфраструктура спрямо хибридните заплахи във всички съответни сектори.

<u>Действие 5</u>: 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 във всички съответни сектори.

4.1.1. Енергийни мрежи

Безпрепятственото производство и разпределение на електроенергия е от жизненоважно значение за ЕС, а големите сривове в електрозахранването могат да нанесат щети. Съществен елемент в борбата с хибридните заплахи е по-нататъшното диверсифициране на енергийните източници, доставчици и

[16] Съобщение на Комисията относно Европейска програма за защита на критичната инфраструктура (COM(2006) 786 final от 12.12.2006 г.).
[17] Директива 2008/114/ЕО на Съвета от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита (ОВ L 345 от 23.12.2008 г.)

маршрути, с което да се осигурят по-сигурни и устойчиви енергийни доставки. Освен това Комисията прави оценки на риска за електроцентралите в ЕС и тяхната безопасност (т.нар. „стрес тестове“). С цел да се постигне енергийна диверсификация, беше засилена работата в контекста на Стратегията за енергийния съюз. Така например, Южният газов коридор дава възможност за доставяне на природен газ от Каспийския регион, а в Северна Европа се създават газови хъбове за втечнен газ с няколко доставчици. Този пример трябва да бъде последван в Централна и Източна Европа и в региона на Средиземно море, където в момента се изгражда газов хъб[18]. Развиващият се пазар на втечнен природен газ също ще допринесе за постигането на тази цел.

Що се отнася до ядрените материали и съоръжения, Комисията подпомага разработването и приемането на най-високите стандарти за безопасност, с което се повишава устойчивостта. Комисията насърчава последователното транспониране и прилагане на Директивата за ядрената безопасност[19], с която се определят правила за предотвратяването на аварии и ограничаването на последиците от тях, както и на Директивата за основните норми на безопасност[20] относно международното сътрудничество за аварийна готовност и реагиране, по-специално между съседни държави членки и със съседни държави.

<u>Действие 6</u>: 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.

4.1.2 Сигурност на транспорта и веригите за доставки

Транспортът е от съществено значение за функционирането на Съюза. Хибридните нападения срещу транспортната инфраструктура (като например летища, пътни инфраструктури, пристанища и железопътни линии) могат да имат сериозни последици и да доведат до преустановяване на пътуванията и прекъсване на веригите за доставки. В процеса на прилагане на законодателството за въздухоплавателната и морската сигурност[21] Комисията извършва периодични

[18] Относно постигнатия до този момент напредък вж. Съобщението за състоянието на енергийния съюз през 2015 г. (COM(2015) 572 final).

[19] Директива 2009/71/Евратом на Съвета от 25 юни 2009 г. за установяване на общностна рамка за ядрената безопасност на ядрените инсталации, изменена с Директива 2014/87/Евратом на Съвета от 8 юли 2014 г.

[20] Директива 2013/59/Евратом на Съвета от 5 декември 2013 г. за определяне на основни норми на безопасност за защита срещу опасностите, произтичащи от излагане на йонизиращо лъчение, и за отмяна на директиви 89/618/Евратом, 90/641/Евратом, 96/29/Евратом, 97/43/Евратом и 2003/122/Евратом.

[21] Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета от 11 март 2008 г. относно общите правила в областта на сигурността на гражданското въздухоплаване и за отмяна на Регламент (ЕО) № 2320/2002; Регламент за изпълнение (ЕС) 2015/1998 на Комисията от 5 ноември 2015 г. за установяване на подробни мерки за прилагането на общите основни стандарти за сигурност във въздухоплаването; Директива 2005/65/ЕО на Европейския парламент и на Съвета от 26 октомври 2005 г. за повишаване на сигурността на пристанищата;Регламент (ЕО) № 725/2004 на Европейския парламент и на Съвета от 31 март 2004 г. относно подобряване на сигурността на корабите и на пристанищните съоръжения

инспекции[22] и чрез своята работа по сигурността на сухопътния транспорт се стреми да противодейства на нововъзникващите хибридни заплахи. Във връзка с това съгласно преразгледания Регламент за сигурността на въздухоплаването[23] е в ход обсъждането на рамка на ЕС като част от Стратегията за въздухоплаването в Европа[24]. В Стратегията на Европейския съюз за морска сигурност и свързания с нея план за действие се разглеждат заплахите за морската сигурност[25]. Този план дава възможност на ЕС и неговите държави членки да се справят с предизвикателствата в областта на морската сигурност във всички техни аспекти, включително да противодействат на хибридните заплахи, чрез междусекторно сътрудничество между гражданските и военните субекти, целящо защитата на критичната морска инфраструктура, глобалната верига за доставки, морската търговия и морските природни и енергийни ресурси. Сигурността на международната верига за доставки е разгледана и в стратегията и плана за действие на ЕС за управление на риска в областта на митниците[26].

***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.**

4.1.3 Космическо пространство

Хибридните заплахи биха могли да бъдат насочени към космическите инфраструктури, което би засегнало редица сектори. ЕС създаде рамка за подкрепа на космическото наблюдение и проследяване[27], която свързва такива инфраструктури, притежавани от държавите членки, с цел да се осигурят услуги за

[22] Съгласно правото на ЕС от Комисията се изисква да прави инспекции, за да гарантира, че държавите членки прилагат правилно изискванията за въздухоплавателна и морска сигурност. Това включва инспекции на компетентния орган в държавата членка, както и инспекции на летища, пристанища, въздушни превозвачи, кораби и субекти, прилагащи мерки за сигурност. Инспекциите на Комисията целят да се гарантира, че държавите членки прилагат напълно стандартите на ЕС.

[23] Регламент (ЕС) 2016/4 на Комисията от 5 януари 2016 г. за изменение на Регламент (ЕО) № 216/2008 на Европейския парламент и на Съвета по отношение на изпълнението на съществените изисквания за защита на околната среда; Регламент (ЕО) № 216/2008 от 20 февруари 2008 г. относно общи правила в областта на гражданското въздухоплаване и за създаване на Европейска агенция за авиационна безопасност.

[24] Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Стратегия за въздухоплаването в Европа“ (COM(2015)0598 final от 7.12.2015 г.).

[25] През декември 2014 г. Съветът прие План за действие за изпълнение на Стратегията на Европейския съюз за морска сигурност; http://data.consilium.europa.eu/doc/document/ST-17002-2014-INIT/bg/pdf

[26] Съобщение на Комисията до Европейския парламент, Съвета и Европейския икономически и социален комитет относно стратегия и план за действие на ЕС за управление на риска в областта на митниците: справяне с рисковете, укрепване на сигурността на веригата на доставки и създаване на благоприятни условия за търговия (COM(2014) 527 final).

[27] Вж. Решение № 541/2014/ЕС на Европейския парламент и на Съвета.

космическо наблюдение и проследяване[28] за определени ползватели (държави членки, институции на ЕС, собственици и оператори на космически апарати и органи за гражданска защита). В контекста на предстоящата космическа стратегия за Европа Комисията ще разгледа възможностите за по-нататъшно развитие на рамката с цел наблюдение на хибридните заплахи за космическите инфраструктури.

Спътниковите комуникации (SatComs) са основни средства за управлението на кризи, реакцията при бедствия и полицейското, граничното и бреговото наблюдение. Те са гръбнакът на мащабни инфраструктури, като например транспортните и космическите системи и дистанционно управляемите летателни системи. В съответствие с искането на Европейския съвет да се подготви следващото поколение правителствени спътникови комуникации (GovSatCom) Комисията, в сътрудничество с Европейската агенция по отбрана, извършва понастоящем оценка на начините за обединяване на търсенето в контекста на предстоящата космическа стратегия и предстоящия план за действие в областта на отбраната.

Много критични инфраструктури разчитат на информация за точно време, за да синхронизират своите мрежи (например в енергетиката и телекомуникациите) или за да издават времеви печати за сделки (напр. във финансовите пазари). Зависимостта от един-единствен сигнал за времева синхронизация, подаван от глобалната навигационна спътникова система, не гарантира устойчивостта, която е необходима за борба с хибридните заплахи. „Галилео“ — европейската глобална навигационна спътникова система — ще предостави втори надежден източник за времева синхронизация.

<u>Действие 8</u>: в контекста на предстоящата космическа стратегия и предстоящия европейски 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.

4.2. Отбранителни способности

Отбранителните способности трябва да се засилят, за да се повиши устойчивостта на ЕС спрямо хибридните заплахи. Важно е да бъдат установени съответните способности от първостепенно значение, напр. наблюдателни и разузнавателни способности. Европейската агенция по отбрана може да бъде катализатор за

[28] Като например предупреждения за избягване на сблъсък в орбита, сигнали за разпадане или сблъсък и опасно повторно навлизане на космически обекти в атмосферата на Земята.

развитието на военни способности, свързани с хибридните заплахи (например чрез скъсяване на циклите за разработване на отбранителни способности, инвестиции в технологии, системи и прототипи и отваряне на отбранителната индустрия за иновативни търговски технологии). Възможните действия могат да бъдат разгледани в предстоящия европейски план за действие в областта на отбраната.

<u>Действие 9</u>: 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.

4.3. Защита на общественото здраве и продоволствената сигурност

Манипулирането на заразни болести и замърсяването на храната, почвата, въздуха и питейната вода с химични, биологични, радиологични и ядрени (ХБРЯ) вещества могат да изложат на опасност здравето на населението. Освен това умишленото разпространение на заболявания по животните или растенията може да засегне сериозно продоволствената сигурност на Съюза и да има големи икономически и социални последици за ключови елементи на хранителната верига в ЕС. За да се реагира на хибридните заплахи, използващи тези методи, могат да се използват съществуващите структури на ЕС за сигурност на общественото здраве, опазване на околната среда и безопасност на храните.

Съгласно правото на ЕС в областта на трансграничните заплахи за здравето[29] готовността за посрещане на сериозни трансгранични заплахи за здравето се координира чрез съществуващите механизми, като държавите членки, агенциите на ЕС и научните комитети[30] са свързани чрез системата за ранно предупреждение и реагиране. Комитетът за здравна сигурност, който координира ответните действия на държавите членки спрямо тези заплахи, може да действа като координационно звено във връзка с уязвимите места в областта на общественото здраве[31] и да включи хибридните заплахи (по-специално биотероризма) в насоки за комуникация при кризи и в учения за изграждане на капацитет (симулиране на криза) с държавите членки. В областта на безопасността на храните компетентните органи обменят информация за анализ на риска с цел да се контролират рисковете за здравето, породени от замърсени храни, чрез Системата за бързо предупреждение за храни и фуражи (RASFF) и чрез Общата система за управление на риска (CRMS) за митниците. Що се отнася до здравето на животните и

[29] Решение № 1082/2013/ЕС на Европейския парламент и на Съвета от 22 октомври 2013 г. за сериозните трансгранични заплахи за здравето и за отмяна на Решение № 2119/98/ЕО (ОВ L 293, 5.11.2013 г., стр. 1).
[30] Решение на Комисията C(2015) 5383 от 7.8.2015 г. за създаване на научни комитети в областта на общественото здраве, безопасността на потребителите и околната среда.
[31] В съответствие с Решение № 1082/2013/ЕС на Европейския парламент и на Съвета от 22 октомври 2013 г. за сериозните трансгранични заплахи за здравето и за отмяна на Решение № 2119/98/ЕО (ОВ L 293, 5.11.2013 г., стр. 1).

растенията, при преразглеждането на правната уредба на ЕС[32] ще бъдат добавени нови елементи към съществуващия „инструментариум“ [33] с цел по-добра подготвеност за реакция на хибридните заплахи.

<u>Действие 10</u>: 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 Комитета за здравна сигурност.

4.4. Киберсигурност

Взаимносвързаното и цифровизирано общество е от голяма полза за ЕС. Кибератаките могат да прекъснат цифровите услуги в целия ЕС и поради тази причина могат да бъдат използвани от създателите на хибридни заплахи. Повишаването на устойчивостта на комуникационните и информационните системи в Европа е важно, за да се поддържа цифровият единен пазар. Стратегията на ЕС за киберсигурност и Европейската програма за сигурност осигуряват цялостната стратегическа рамка за инициативите на ЕС в областта на киберсигурността и киберпрестъпността. ЕС работи активно за повишаване на осведомеността и за разработване на механизми за сътрудничество и ответни действия съгласно поставените в Стратегията за киберсигурност цели. По-конкретно, с предложението за Директива за мрежова и информационна сигурност (МИС)[34] вниманието се насочва към рисковете, свързани с киберсигурността, за широк спектър от основни доставчици на услуги в областта на енергетиката, транспорта, финансите и здравеопазването. Тези доставчици, както и доставчиците на основни цифрови услуги (напр. изчисления в облак) следва да вземат подходящи мерки за сигурност и в случай на сериозни инциденти да уведомяват компетентните национални органи, като отбелязват евентуални характеристики на хибридна заплаха. След като Директивата бъде приета от съзаконодателите, нейното ефективно транспониране и прилагане ще благоприятстват създаването на способности за киберсигурност в държавите членки, засилвайки сътрудничеството им в областта на киберсигурността посредством обмен на информация и най-добри практики за борба с хибридните заплахи. По-конкретно, в Директивата се предвижда създаването на мрежа от 28 национални екипа за реагиране при инциденти с компютърната сигурност (ЕРИКС) и Екипа за незабавно реагиране

[32] Регламент (ЕС) 2016/429 на Европейския парламент и на Съвета за заразните болести по животните и за изменение и отмяна на определени актове в областта на здравеопазването на животните (Законодателство за здравеопазването на животните) (ОВ L 84, 31.3.2016 г.) На 16 декември 2015 г. Европейският парламент и Съветът постигнаха политическо споразумение по текста на предложението за регламент на Европейския парламент и на Съвета относно защитните мерки срещу вредителите по растенията („законодателство в областта на здравето на растенията“).

[33] Например банките за ваксини на ЕС, сложната електронна информационна система за болестите по животните, по-строгите задължения за мерки за сигурност в лаборатории и други структури, боравещи с патогени.

[34] Предложение на Комисията за Директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза (COM(2013) 48 final от 7.2.2013 г.). Съветът на ЕС и Европейският парламент постигнаха политическо споразумение по предложената директива и тя следва скоро да бъде официално приета.

при компютърни инциденти за институциите на ЕС[35], която да осъществява оперативното сътрудничество на доброволна основа.

За да насърчи публично-частното сътрудничество и приложими в целия ЕС подходи към киберсигурността, Комисията създаде Платформата за мрежова и информационна сигурност, която публикува насоки с най-добри практики в управлението на риска. Държавите членки определят изискванията за сигурност и реда и условията за уведомяване при инциденти на национално равнище, а Комисията насърчава висока степен на сближаване на подходите за управление на риска, по-специално чрез Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA).

<u>Действие 11</u>: Комисията насърчава държавите членки приоритетно да създадат мрежа между 28-те ЕРИКС и CERT-EU 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.

4.4.1. Промишленост

Засиленото използване на изчисления в облак и на големи информационни масиви доведе до по-голяма уязвимост на хибридни заплахи. В Стратегията за цифров единен пазар се предвижда създаването на договорно публично-частно партньорство по киберсигурността[36], което ще се съсредоточи върху научноизследователската дейност и иновациите и ще помогне на Съюза да запази висок технологичен капацитет в тази област. С договорното публично-частно партньорство ще се изгради доверие между различните участници на пазара и ще се постигнат синергии между търсенето и предлагането. Докато договорното публично-частно партньорство и съпътстващите го мерки ще бъдат съсредоточени главно върху продукти и услуги за кибернетична сигурност за граждански цели, в резултат на тези инициативи потребителите би трябвало да бъдат по-добре защитени и от хибридните заплахи.

<u>Действие 12</u>: 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.

[35] CERT-EU.
[36] Предстои да бъде започнато през 2016 г.

4.4.2. Енергетика

Появата на интелигентни домове и уреди, развитието на интелигентни мрежи и нарастващата цифровизация на енергийната система също водят до повишаване на уязвимостта спрямо кибератаки. Европейската стратегия за енергийна сигурност[37] и Стратегията за енергийния съюз[38] подкрепят подход, обхващащ всички опасности, в който е интегрирана устойчивостта спрямо хибридните заплахи. Тематичната мрежа за защита на критичната енергийна инфраструктура насърчава сътрудничеството между операторите в сектора на енергетиката (нефт, газ, електричество). Комисията откри интернет платформа за анализ и обмен на информация относно заплахите и инцидентите[39]. Съвместно със заинтересованите страни[40] тя разработва също така всеобхватна стратегия за енергийния сектор във връзка с киберсигурността при операциите в интелигентната мрежа с цел да се намалят уязвимите места. Въпреки че пазарите на електроенергия са все по-интегрирани, правилата и процедурите за справяне с кризисни ситуации са все още само национални. Трябва да се направи така, че правителствата да си сътрудничат при подготовката за рискове и тяхното предотвратяване и ограничаване на въздействието им и че всички съответни участници да действат въз основа на набор от общи правила.

<u>Действие 13</u>: 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.

4.4.3. Гарантиране на стабилни финансови системи

За да функционира, икономиката на ЕС се нуждае от сигурна финансова и платежна система. Защитата на финансовата система и нейната инфраструктура от кибератаки, независимо от подбудите или естеството на нападателя, е от съществено значение. За да се справи с хибридните заплахи за финансовите услуги в ЕС, секторът трябва да разбира заплахата, да е изпробвал своите способности за отбрана и да разполага с необходимата технология, с която да се защитава от нападения. Следователно обменът на информация относно заплахите сред участниците на финансовите пазари и със съответните органи и основни доставчици на услуги и клиентите е от първостепенно значение, но е необходимо той да се извършва по сигурни канали и да отговаря на изискванията за защита на

[37] Съобщение на Комисията до Европейския парламент и Съвета „Европейска стратегия за енергийна сигурност“ (COM(2014)0330 final).
[38] Съобщение относно рамкова стратегия за устойчив енергиен съюз с ориентирана към бъдещето политика по въпросите на изменението на климата (COM/2015/080 final).
[39] Център на ЕС за обмен на информация относно инцидентите и заплахите — ITIS.
[40] В рамките на Платформата на експертите в енергийния сектор по въпросите на киберсигурността (EECSP).

данните. В съответствие с работата в рамките на международни форуми, включително работата на Г-7 в тази сфера, Комисията ще се стреми да идентифицира факторите, които възпрепятстват адекватния обмен на информация за заплахите, и да предложи решения. Важно е да се осигурят редовното изпитване и усъвършенстване на протоколите за защита на търговците и съответните инфраструктури, включително постоянното осъвременяване на технологиите за повишаване на сигурността.

<u>Действие 14</u>: Комисията, в сътрудничество с ENISA[41], държавите членки, съответните международни, европейски и национални органи и финансови институции, ще поощрява и способства създаването на мрежи и платформи за обмен на информация и ще обърне внимание на факторите, които възпрепятстват обмена на такава информация.

4.4.4. Транспорт

Съвременните транспортни системи (железопътни, автомобилни, въздушни и морски) разчитат на информационни системи, които са уязвими на кибератаки. Като се има предвид трансграничното измерение на тези системи, ролята на ЕС е особено важна. Комисията, в сътрудничество с държавите членки, ще продължи да анализира кибернетичните заплахи и рискове, свързани с незаконна намеса в транспортните системи. В сътрудничество с Европейската агенция за авиационна безопасност (ЕААБ)[42] Комисията работи по изготвянето на пътна карта за киберсигурността във въздухоплаването. Кибернетичните заплахи за морската сигурност са разгледани в Стратегията на Европейския съюз за морска сигурност и свързания с нея план за действие.

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

4.5. Действия срещу финансирането на хибридните заплахи

Създателите на хибридни заплахи се нуждаят от финансиране, за да осъществяват своята дейност. Финансирането може да се използва за подпомагане на терористични групи или по-трудно различими форми на дестабилизация, като подкрепа за групи за оказване на натиск и крайни политически партии. ЕС засили

[41] Агенция на Европейския съюз за мрежова и информационна сигурност.

[42] През декември 2015 г. Комисията представи предложение за нов регламент за ЕААБ, което понастоящем се обсъжда в Европейския парламент и Съвета. Предложение за регламент на Европейския парламент и на Съвета относно общи правила в областта на гражданското въздухоплаване и за създаването на Агенция за авиационна безопасност на Европейския съюз и за отмяна на Регламент (ЕО) № 216/2008 на Европейския парламент и на Съвета (COM(2015) 613 final, 2015/0277 (COD).

усилията за борба с престъпността и финансирането на тероризма, както е посочено в Европейската програма за сигурност, и по-специално в свързания с нея план за действие[43]. В този контекст с преработената европейска рамка за борба с изпирането на пари се засилва борбата с финансирането на тероризма и изпирането на пари и се улеснява работата на националните звена за финансово разузнаване (ЗФР) с цел откриване и проследяване на подозрителни парични преводи и обмен на информация, като същевременно се гарантира проследимостта на преводите на средства в Европейския съюз. Рамката би могла да допринесе и за борбата с хибридните заплахи. В контекста на инструментите на ОВППС биха могли да бъдат проучени възможностите за ефективни и целенасочени ограничителни мерки за борба с хибридните заплахи.

<u>Действие 16</u>: Комисията ще използва изпълнението на Плана за действие с цел засилване на борбата с финансирането на тероризма, за да допринесе и за противодействието на хибридните заплахи.

4.6. Изграждане на устойчивост спрямо радикализацията и насилническия екстремизъм

Макар че сами по себе си терористичните актове и насилническият екстремизъм нямат хибриден характер, създателите на хибридни заплахи могат да се възползват от уязвими членове на обществото и да ги вербуват, радикализирайки ги чрез съвременни комуникационни канали (включително социални медии в интернет и групи от подставени лица) и пропаганда.

С цел да се противопостави на екстремисткото съдържание в интернет, Комисията — в контекста на Стратегията за цифров единен пазар — анализира необходимостта от потенциални нови мерки, като обърна специално внимание на тяхното въздействие върху основните права на свобода на изразяване на мнение и на информация. Тези мерки биха могли да включват строги процедури за премахване на незаконно съдържание, като същевременно се избягва отстраняването на законно съдържание (процедури за уведомяване и предприемане на действия), както и поемането на по-голяма отговорност и извършването на надлежни проверки от страна на посредниците при управлението на техните мрежи и системи. Това ще допълни съществуващия доброволен подход, при който интернет дружествата и дружествата, управляващи социални медии (по-специално под егидата на Интернет форума на ЕС), и в сътрудничество със звеното на ЕС за сигнализиране за незаконно съдържание в интернет към Европол, бързо премахват материали с терористична пропаганда.

В контекста на Европейската програма за сигурност на радикализацията се противодейства чрез обмен на опит и разработване на най-добри практики, включително сътрудничество с трети държави. Консултативният екип за

[43] Съобщение на Комисията до Европейския парламент и Съвета относно план за действие с цел засилване на борбата с финансирането на тероризма (COM(2016)50 final).

стратегическа комуникация относно Сирия има за цел да засили създаването и разпространението на алтернативни послания за противодействие на терористичната пропаганда. Мрежата за осведоменост по въпросите на радикализацията подкрепя държавите членки и практикуващите специалисти, които трябва да взаимодействат с радикализирани лица (включително чуждестранни бойци терористи) или с лица, считани за податливи на радикализация. Мрежата за осведоменост по въпросите на радикализацията предлага обучения и съвети и ще предостави помощ на приоритетни трети държави, в които е налице воля за действия в тази област. Освен това Комисията насърчава съдебното сътрудничество между субектите в областта на наказателното правосъдие, включително Евроюст, за борба с тероризма и радикализацията в държавите членки, включително за работа с чуждестранни бойци терористи и завърнали се бойци.

В допълнение към гореизложените подходи, със своята **външна дейност** ЕС допринася за борбата с насилническия екстремизъм, включително чрез външна ангажираност и осведоменост, предотвратяване (борба с радикализацията и финансирането на тероризма), както и чрез мерки за справяне с основните икономически, политически и социални фактори, които предоставят на терористичните групи възможността да процъфтяват.

<u>Действие 17:</u> 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.

4.7. Засилване на сътрудничеството с трети държави

Както се подчертава в Европейската програма за сигурност, ЕС засили вниманието си върху изграждането на капацитет 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[44]. Тези действия също могат да допринесат за устойчивостта на партньорите спрямо хибридни дейности.

Комисията възнамерява да засили допълнително обмена на оперативна и стратегическа информация с държавите, обхванати от процеса на разширяване, и по целесъобразност в рамките на Източното партньорство и Южното съседство, за да се подпомогне борбата с организираната престъпност, тероризма, незаконната миграция и трафика на малки оръжия. Що се отнася до борбата с тероризма, ЕС

[44] Съвместно съобщение до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „ Преглед на европейската политика за съседство“ (JOIN(2015) 50 final от 18.11.2015 г.).

активизира сътрудничеството с трети държави чрез установяването на осъвременени диалози за сигурност и планове за действие.

Инструментите за външно финансиране на ЕС имат за цел изграждането на функциониращи и отговорни институции в трети държави[45], което е предпоставка за ефективността на ответните действия срещу заплахите за сигурността и за повишаването на устойчивостта. В този контекст реформата на сектора на сигурността и изграждането на капацитет в подкрепа на сигурността и развитието[46] са инструменти от основно значение. По линия на Инструмента, допринасящ за стабилността и мира[47], Комисията подготви действия за увеличаване на устойчивостта на киберпространството и на способностите на партньорите за откриване и реакция на кибернетични атаки и престъпления, с които може да се противодейства на хибридните заплахи в трети държави. ЕС финансира дейности за изграждане на капацитет в партньорските държави с цел намаляване на рисковете за сигурността, свързани с химични, биологични, радиологични и ядрени въпроси[48].

Накрая, съгласно всеобхватния подход към управлението на кризи държавите членки биха могли да разработят инструменти и мисии по линия на общата политика за сигурност и отбрана (ОПСО), независимо или в допълнение към вече използвани инструменти на ЕС, така че да се помогне на партньорите да повишат своите способности. Могат да се разгледат следните дейности: i) подкрепа за стратегическата комуникация, ii) консултантска помощ за ключови министерства, изложени на хибридни заплахи, iii) допълнителна подкрепа за управлението на границите в случай на извънредна ситуация. Биха могли да се проучат възможностите за допълнителни синергии между инструментите на ОПСО и субектите в сферата на сигурността, митниците и правосъдието, включително съответните агенции на ЕС[49], Интерпол и Европейските жандармерийски сили в съответствие с техния мандат.

---

[45] Пак там; Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Стратегия на ЕС за разширяване“ (COM(2015) 611 final от 10.11.2015 г.); Съобщение на Комисията до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите „Повишаване на въздействието на политиката на ЕС за развитие: програма за промяна“ (COM(2011) 637 final от 13.10.2011 г.).

[46] Съвместно съобщение „Изграждане на капацитет в подкрепа на сигурността и развитието — създаване на способности в нашите партньори за предотвратяване и управление на кризи“ (JOIN(2015) 17 final).

[47] Регламент (ЕС) № 30/2014 на Европейския парламент и на Съвета от 11 март 2014 г. за създаване на Инструмент, допринасящ за стабилността и мира (ОВ L 77, 15.3.2014 г., стр. 1).

[48] Обхванатите области включват наблюдението на границите, управлението на кризи, незабавното реагиране, незаконния трафик и контрола на износа на изделия с двойна употреба, наблюдението и контрола на болестите, ядрената криминалистика, възстановяването след инцидент и защитата на високорискови съоръжения. Най-добрите практики от инструментите, разработени в рамките на Плана за действие на ЕС в областта на ХБРЯ, като Европейския център за обучение по ядрена сигурност, и от участието на ЕС в Международната работната група по наблюдение на границите могат да бъдат споделяни с трети държави.

[49] Европол, Frontex, Cepol, Евроюст.

<u>Действие 18</u>: 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 спрямо хибридните 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.

5. ПРЕДОТВРАТЯВАНЕ, РЕАКЦИЯ ПРИ КРИЗИ И ВЪЗСТАНОВЯВАНЕ

Както е посочено в раздел 3.1, предложеното звено на ЕС за синтез на информацията за хибридните заплахи има за задача да анализира съответните показатели с цел предотвратяване и реагиране на хибридните заплахи и информиране на лицата, отговорни за вземането на решения в ЕС. Макар че слабостите 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. Във връзка с това подпомагането от страна на Европейския координационен център за реагиране при извънредни ситуации[50] на националните действия и капацитет за гражданска защита може да бъде ефективен механизъм за реагиране спрямо аспектите на хибридните заплахи, които налагат реакцията на гражданската защита. То би могло да се постигне в координация с други механизми за реагиране и системи за ранно предупреждение на ЕС, по-специално със Ситуационната зала на ЕСВД по въпросите на външните измерения на сигурността и Центъра за стратегически анализ и реакция в областта на вътрешната сигурност.

Клаузата за солидарност (член 222 от ДФЕС) дава възможност за действия на Съюза, както и за действия между държавите членки, ако дадена държава членка стане обект на терористично нападение или жертва на природно или предизвикано от човека бедствие. Действията на Съюза за подпомагане на тази държава членка се осъществяват чрез прилагането на Решение 2014/415/ЕС на Съвета[51]. Договореностите за координация в рамките на Съвета следва да се основават на интегрираните договорености за реакция на ЕС на политическо равнище в кризисни ситуации[52]. Съгласно тези договорености Комисията и върховният представител (в рамките на съответните им компетенции) определят съответните

[50] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en
[51] Решение 2014/415/ЕС на Съвета относно договореностите за прилагане от страна на Съюза на клаузата за солидарност (ОВ L 192, 1.7.2014 г., стр. 53).
[52] http://www.consilium.europa.eu/bg/documents-publications/publications/2014/eu-ipcr/

инструменти на Съюза и представят на Съвета предложения за решения за извънредни мерки.

В член 222 от ДФЕС се предвиждат също така ситуации, в които една или няколко държави членки оказват пряка помощ на държава членка, срещу която е било извършено терористично нападение или която е била засегната от бедствие. Решение 2014/415/ЕС на Съвета не се прилага в тези случаи. Като се има предвид неяснотата, свързана с хибридните дейности, Комисията и върховният представител (в рамките на съответните им компетенции) следва да оценят евентуалната приложимост на клаузата за солидарност като крайна мярка, в случай че държава — членка на ЕС, е обект на значителни хибридни заплахи.

Ако множество сериозни хибридни заплахи представляват въоръжено нападение срещу държава — членка на ЕС, тогава правното основание за предприемането на целесъобразни и навременни ответни действие може да бъде член 42, параграф 7 от ДЕС, а не член 222 от ДФЕС. Освен това при мащабни и сериозни хибридни заплахи може да се наложи по-засилено сътрудничество и координация с НАТО.

При подготовката на своите въоръжени сили държавите членки се приканват да вземат под внимание потенциалните хибридни заплахи. За да бъдат подготвени да вземат решения бързо и ефективно в случай на хибридно нападение, държавите членки трябва да провеждат редовни учения на работно и на политическо равнище с цел проверяване на националната и многонационалната способност за вземане на решения. Целта е да се изготви общ оперативен протокол между държавите членки, Комисията и върховния представител, описващ ефективни процедури, които да бъдат следвани в случай на хибридна заплаха от началния етап на разпознаване на заплахата до крайния етап на нападение, и очертаващ ролята на всяка институция на Съюза и на всеки участник в този процес.

Като важен компонент на ангажираността в рамките на ОПСО биха могли да се осигурят а) гражданско и военно обучение, б) предоставяне на насоки и консултации с цел подобряване на капацитета за сигурност и отбрана на застрашената държава членка, в) планиране за извънредни ситуации с цел идентифициране на сигнали за хибридни заплахи и укрепване на капацитета за ранно предупреждение, г) подкрепа за управлението на граничния контрол в случай на извънредна ситуация, д) подкрепа в специализирани области, като например намаляване на рисковете от ХБРЯ материали и евакуация на цивилно население от една държава в друга.

<u>Действие 19</u>: 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.

<u>Действие 20</u>: 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.

<u>Действие 21</u>: 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.

6. ЗАСИЛВАНЕ НА СЪТРУДНИЧЕСТВОТО С НАТО

Хибридните заплахи представляват предизвикателство не само за ЕС, но и за други големи партньорски организации, включително Организацията на обединените нации (ООН), Организацията за сигурност и сътрудничество в Европа (ОССЕ) и най-вече НАТО. Необходими са диалог и координация както на политическо, така и на оперативно ниво между организациите, за да бъдат ответните действия ефективни. По-тясното взаимодействие между ЕС и НАТО би дало възможност на двете организации да се подготвят по-добре и да реагират ефективно спрямо хибридните заплахи, като се допълват и подпомагат взаимно въз основа на принципа на приобщаване, като същевременно се зачитат независимостта в процеса на вземане на решения на всяка организация и правилата за защита на данните.

Двете организации споделят общи ценности и са изправени пред сходни предизвикателства. Държавите от ЕС и съюзниците на НАТО очакват съответните организации да ги подкрепят и да действа бързо, решително и координирано в случай на криза, а в идеалния случай — да предотвратяват възникването на кризи. Идентифицирани са редица области за по-тясно сътрудничество и координиране между ЕС и НАТО, сред които ситуационната осведоменост, стратегическата комуникация, кибернетичната сигурност и предотвратяването и реакцията на кризи. Воденият понастоящем неофициален диалог между ЕС и НАТО относно хибридните заплахи следва да бъде активизиран, за да се синхронизират дейностите на двете организации в тази област.

С цел да бъдат подготвени допълващи се ответни действия на ЕС и НАТО, е важно и двете организации да имат една и съща степен на ситуационна осведоменост преди и по време на криза. Това би могло да се постигне чрез редовен обмен на анализи и направени изводи, но и чрез пряка връзка между звеното на ЕС за синтез на информацията за хибридните заплахи и звеното на НАТО, занимаващо се с хибридните заплахи. Също толкова важно е да се постигне взаимно познаване на съответните процедури за управление на кризи, за да могат реакциите да бъдат бързи и ефективни. Устойчивостта би могла да се подобри, като се осигури взаимно допълване при установяването на показатели за критичните части на инфраструктурите на двете организации, както и чрез тясно сътрудничество в областта на стратегическата комуникация и кибернетичната отбрана. Съвместните

учения с пълноценно и равностойно участие на политическо и техническо равнище ще направят вземането на решения от страна на двете организации по-ефективно. С проучването на допълнителни възможности за обучение ще се способства за развитието на сравнимо ниво на експертни познания в критични области.

<u>Действие 22</u>: върховният представител, в координация с Комисията, ще продължи неформалния диалог и ще засили сътрудничеството и координацията с НАТО в областта на ситуационната осведоменост, стратегическата комуникация, 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.

7. ЗАКЛЮЧЕНИЯ

В настоящото съвместно съобщение 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. Тъй като акцентът е върху **подобряването на осведомеността**, предлага се да бъдат създадени специални механизми за обмен на информация с държавите членки и за координиране на капацитета на ЕС за осигуряване на стратегическа комуникация. Очертани са действия за **изграждането на устойчивост** в области като киберсигурността, критичната инфраструктура, защитата на финансовата система от незаконна употреба и противодействието на насилническия екстремизъм и радикализацията. Във всяка от тези области изпълнението на приетите от ЕС и държавите членки стратегии и цялостното прилагане на съществуващото законодателство в държавите членки ще бъдат важна първа стъпка, като същевременно са предложени няколко по-конкретни действия, за да се подкрепят тези усилия.

Що се отнася до **предотвратяването, реакцията при кризи и възстановяването от хибридните заплахи**, предлага се да бъде разгледана приложимостта на клаузата за солидарност в член 222 от ДФЕС (както е определена в съответното решение) и на член 42, параграф 7 от ДЕС в случай на мащабна и сериозна хибридна атака. Капацитетът за вземане на стратегически решения може да бъде подобрен чрез създаването на общ оперативен протокол.

И накрая, предлага се **да се засилят сътрудничеството** и **координацията между ЕС и НАТО** в общите усилия за противодействие на хибридните заплахи.

Върховният представител и Комисията се ангажират при изпълнението на настоящата съвместна рамка да мобилизират съответните инструменти на ЕС, с които разполагат. За ЕС е важно да работи заедно с държавите членки за намаляване на рисковете, свързани с излагането на потенциални хибридни заплахи, произтичащи от държавни и недържавни субекти.