ЕВРОПЕЙСКА
КОМИСИЯ

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

Брюксел, 13.6.2018г.
JOIN(2018) 16 final

СЪВМЕСТНО СЪОБЩЕНИЕ ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ, ЕВРОПЕЙСКИЯ СЪВЕТ И СЪВЕТА

Повишаване на устойчивостта и укрепване на способностите за борба с хибридните заплахи

1. ВЪВЕДЕНИЕ

Хибридните дейности от страна на държавни и недържавни участници продължават да бъдат сериозна заплаха за ЕС и неговите държави членки. Усилията за дестабилизиране на държави чрез подкопаване на общественото доверие в правителствените институции и разклащане на основните ценности на обществата станаха по-чести. Обществата ни са изправени пред сериозно предизвикателство в лицето на хора, които желаят да навредят на ЕС и неговите държави членки — от кибератаки, смущаващи икономиката и обществените услуги, през целенасочени кампании за дезинформация до враждебни военни действия.

Хибридните кампании са многоизмерни и съчетават принудителни и подривни мерки, използвайки както традиционни, така и нетрадиционни инструменти и тактики (дипломатически, военни, икономически и технологични) за дестабилизиране на противника. Целта им е да бъдат трудни за откриване и трудно да се разбира кой стои зад тях, като те могат да бъдат използвани както от държавни, така и от недържавни субекти. Нападението през март 2018 г. с нервнопаралитично вещество в Солсбъри[1] допълнително подчерта многостранността на хибридните заплахи и множеството налични понастоящем тактики. В отговор на тези предизвикателства Европейският съвет[2] подчерта необходимостта от укрепване на капацитета на ЕС и неговите държави членки за откриване, предотвратяване и реагиране на хибридни заплахи в области като киберсигурността, стратегическата комуникация и контраразузнаването. Освен това бе обърнато специално внимание на необходимостта от подобряване на устойчивостта по отношение на химичните, биологичните, радиологичните и ядрените заплахи.

Заплахите от неконвенционални оръжия попадат в отделна категория поради потенциалния размер на щетите, които могат да причинят. Освен че е трудно да бъдат открити и да се установи извършителят, тези заплахи също така са сложни за преодоляване. Химичните, биологичните, радиологичните и ядрените заплахи, излизащи извън рамките на хибридните заплахи и включващи също терористичните заплахи, също са предмет на обща загриженост от страна на международната общност[3], по-специално по отношение на променящия се риск от тяхното разпространение както в географски аспект, така и към недържавни участници.

Укрепването на устойчивостта на тези заплахи и увеличаването на способностите за справяне с тях са отговорност предимно на държавите членки. Въпреки това институциите на ЕС вече предприеха редица действия, с които да подпомогнат усилията на национално равнище. Сред тях са тясното сътрудничество с други международни участници, включително Организацията на Северноатлантическия

[1] По отношение на нападението в Солсбъри, на 22 март 2018 г. Европейският съвет „изрази съгласие със становището на правителството на Обединеното кралство, че е много вероятно Руската федерация да е отговорна за това нападение и че няма правдоподобно алтернативно обяснение.“

[2] Заключения на Европейския съвет от март 2018 г.

[3] Включително от Съвета за сигурност на ООН, Резолюция S/RES/2325 (2016), 14 декември 2016 г.

договор (НАТО)[4], като това сътрудничество може да допринесе за подкрепа на държавите членки в области като бързата реакция[5].

Настоящото съвместно съобщение е в отговор на призива на Европейския съвет за продължаване на работата в тази област. То е част от по-широк пакет, включващ и последния доклад за напредъка по създаването на Съюз на сигурност[6], в който се обобщават и представят следващите стъпки в изпълнението на плана за действие на ЕС в областта на химичните, биологичните, радиологичните и ядрените материали от октомври 2017 г.[7], както и втория доклад за напредъка[8] относно изпълнението на 22-те действия по Съвместната рамка за борба с хибридните заплахи — ответни действия на Европейския съюз[9].

2. ОТГОВОРЪТ НА ЕС

Комисията и върховният представител положиха последователни усилия за изграждане на способностите на ЕС и за ефективно подпомагане на държавите членки в борбата с хибридните и с химичните, биологичните, радиологичните и ядрените заплахи. Вече бяха постигнати осезаеми резултати в области като стратегическата комуникация, ситуационната осведоменост и укрепването на готовността, устойчивостта и на капацитета за реакция при кризи.

Оперативната група на ЕС за стратегическа комуникация с Източното съседство (East Stratcom), създадена след заседанието на Европейския съвет през март 2015 г., е начело на работата по прогнозиране, проследяване и справяне с дезинформацията, разпространявана от чуждестранни източници. Нейните експертни анализи и обществени продукти[10] послужиха за значително повишаване на осведомеността относно въздействието на руската дезинформация. През последните две години тя разкри над 4000 отделни случаи на дезинформация, много от които умишлено насочени към Европа. Работата на оперативната група бе съсредоточена и върху по-доброто предоставяне на положителни послания, насочени в по-голяма степен към държавите от източното съседство. Предвид този успех, бяха създадени други две работни групи с различна географска насоченост — работна група за Западните Балкани и специална работна група за южното съседство, ориентирана към държавите от арабския свят.

Бяха предприети важни стъпки за изграждане на структурите, необходими за подобряване на ситуационната осведоменост и подкрепа на процеса на вземане на решения. През 2016 г. беше създадено звено за синтез на информацията за хибридните заплахи в рамките на Центъра на ЕС за анализ на информация към Европейската служба за външна дейност. Звеното за синтез на информацията за хибридни заплахи получава и анализира класифицирана и общодостъпна информация от различни заинтересовани страни във връзка с хибридните заплахи.

---

4 Борбата с хибридните заплахи е една от седемте области на сътрудничество с Организацията на Северноатлантическия договор, посочени в съвместната декларация, подписана през юли 2016 г. във Варшава от председателя на Европейския съвет, председателя на Европейската комисия и генералния секретар на Организацията на Северноатлантическия договор.

5 На срещата на върха на Г-7 в Шарльовоа през юни 2018 г. лидерите се споразумяха също така да се разработи механизъм за бързо реагиране на Г-7 за справяне със заплахите за демокрациите: https://g7.gc.ca/en/official-documents/charlevoix-commitment-defending-democracy-from-foreign-threats/

6 Петнадесети доклад за напредъка по създаването на ефективен и истински Съюз на сигурност, COM(2018) 470.

7 COM(2017) 610 final.

8 Съвместен доклад относно изпълнението на съвместната рамка за борбата с хибридните заплахи (юли 2017 г. — юли 2018 г.), JOIN (2018) 14.

9 JOIN(2016) 18 final.

10 Вж. www.euvsdisinfo.eu

Досега са изготвени над 100 оценки и брифинги, споделени в рамките на ЕС и между държавите членки с цел да бъдат използвани в процеса на вземане на решения. Звеното за синтез на информацията за хибридните заплахи работи в тясно сътрудничество с Европейския център за високи постижения в борбата с хибридните заплахи в Хелзинки. Създаден през април 2017 г. с цел насърчаване на стратегическия диалог и провеждане на изследвания и анализи относно хибридните заплахи, днес в центъра за високи постижения вече членуват 16 държави[11] и той получава постоянна подкрепа от страна на ЕС.

Предприети бяха и важни мерки за укрепване на готовността и устойчивостта, по-специално по отношение на химичните, биологичните, радиологичните и ядрените заплахи. През последните шест месеца станахме свидетели на значими стъпки в установяването на пропуските в готовността за реагиране на химични, биологични, радиологични и ядрени инциденти, свързани със сигурността, по-специално по отношение на капацитета за откриване с цел подпомагане на предотвратяването на химични, биологични, радиологични и ядрени нападения. По инициатива на Комисията консорциум от национални експерти извърши анализ на пропуските в оборудването за откриване във връзка с различни сценарии, свързани с химични, биологични, радиологични и ядрени заплахи. Докладът от анализа на пропуските бе споделен с държавите членки, което им позволява да вземат информирани решения относно стратегиите за откриване и да предприемат оперативни мерки за отстраняване на установените пропуски.

Тази работа беше подкрепена с учения за изпробване на степента на напредък. Паралелното и координирано учение за 2017 г. (PACE17) с Организацията на Северноатлантическия договор позволи подробно изследване на способностите на ЕС за реагиране при широкомащабни хибридни кризи. В рамките на ученията — безпрецедентно по отношение на своя обхват — бяха изпитани не само оперативният протокол на ЕС за борбата с хибридните заплахи (EU Playbook), различните механизми на ЕС за реагиране и тяхната способност да си взаимодействат ефективно, а и как реакцията на ЕС спрямо хибридните заплахи си взаимодейства с действията на Организацията на Северноатлантическия договор. Учението за 2018 г. е във фазата на планиране, като целта е то не само да стане ежегодна практика, а и да помогне на държавите членки да укрепят своята способност за реагиране при кризи.

Тези конкретни стъпки показват как установените от ЕС политически рамки дават резултати — през последните две години бяха въведени редица рамки с цел подпомагане и насочване на работата на ЕС.

Със *Съвместната рамка за борба с хибридните заплахи — ответни действия на Европейския съюз*[12] от април 2016 г. се насърчава подход, който обхваща всички равнища на управление, и се определят 22 области на действие за подпомагане на борбата с **хибридните заплахи** и за укрепване на устойчивостта на ЕС и държавите членки, както и на международните партньори. Повечето действия, включени в съвместната рамка, са насочени към подобряване на ситуационната осведоменост и изграждането на устойчивост и към подобряване капацитета за реагиране. Те варират от укрепване на капацитета на ЕС за анализ на разузнавателна информация

[11] От настоящите 16 членове 14 са държави членки на ЕС: Германия, Дания, Естония, Финландия, Франция, Испания, Италия, Латвия, Литва, Нидерландия, Полша, Швеция, Обединеното кралство и Чешката република. Инициативата за създаването му се съдържа в съвместната рамка за борбата с хибридните заплахи. Центърът получи също така активна подкрепа от ЕС и Организацията на Северноатлантическия договор в рамките на тяхното сътрудничество.

до подобряване на защитата на критичната инфраструктура и кибесигурността и борба срещу радикализацията и насилническия екстремизъм. Заплахите, свързани с киберпространството, и кибератаките също са в основата на съвместната рамка. Вторият доклад за напредъка в изпълнението на съвместната рамка, приет успоредно с настоящото съобщение, свидетелства за осезаем напредък по тези действия и потвърждава укрепването и задълбочаването на усилията на ЕС за борба с хибридните заплахи[13].

По отношение на **киберсигурността**, 9 май 2018 г. бе важна дата като краен срок за всички държави — членки на ЕС, да транспонират първия общоевропейски правно обвързващ набор от правила в областта на киберсигурността — Директивата за сигурността на мрежите и информационните системи. Това е важна част от по-широкия подход, изложен през септември 2017 г. в *съвместното съобщение „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“*[14] наред с широкообхватни конкретни мерки, чрез които да бъдат укрепени структурите и способностите на ЕС в областта на киберсигурността. Централно място в съобщението бе отредено на изграждането на устойчивостта на ЕС срещу кибератаки и повишаването на капацитета на ЕС за киберсигурност, предприемането на ефективни наказателноправни мерки и укрепването на глобалната стабилност чрез международно сътрудничество. То беше придружено от предложение за правен акт в областта на киберсигурността с цел засилване на подкрепата на равнище ЕС[15] и подкрепено от редица предложения, които следва да бъдат изпълнени (вж. по-долу).

Дезинформацията вреди на нашите демокрации, като възпрепятства способността на гражданите да вземат информирани решения и да участват в демократичния процес. Интернет значително увеличи обема и разнообразието на достъпни за гражданите новини. Новите технологии обаче могат да се използват за разпространяване на невярна информация с безпрецедентен мащаб и скорост, чиято цел е да породи недоверие и да създаде обществено напрежение. В съобщението на Комисията *Европейски подход за борба с дезинформацията, разпространявана онлайн*[16] се определя европейски подход в отговор на проблема с дезинформацията, като различните заинтересовани страни, по-специално онлайн платформи, но и медийни компании, се призовават да предприемат действия. Действията обхващат широк кръг от подходящи области, включително по-голяма прозрачност; надеждност и отчетност на онлайн платформите; по-сигурни и устойчиви изборни процеси; насърчаване на образованието и медийната грамотност; подкрепа за качествената журналистика и борба с дезинформацията посредством стратегическа комуникация. Първите конкретни стъпки включват Кодекс за поведение във връзка с дезинформацията, който ще бъде разработен от многостранен форум по въпросите на дезинформацията, и мрежа от проверители на фактите, която следва да бъде създадена преди лятото. Първото заседание на многостранния форум по въпросите на дезинформацията се състоя на 29 май 2018 г., като участниците договориха стъпките, необходими за приемане на кодекса през юли 2018 г. До края на 2018 г. Комисията ще оцени постигнатия напредък в решаването на проблема и ще реши дали е необходима допълнителна намеса в тази област. Предвидените дейности ще бъдат съгласувани и ще допълват дейностите на оперативната група East StratCom.

Що се отнася до **химичните, биологичните, радиологичните и ядрените** рискове, в *плана за действие*[17] на Комисията от октомври 2017 г. бяха предложени 23 конкретни

---

13 За първия доклад за изпълнение (юли 2017 г.): JOIN(2017) 30 final.
14 JOIN(2017) 450 final.
15 COM (2017) 477, вж. по-долу.
16 COM(2018) 236 final.
17 COM(2017) 610 final.

действия и мерки, насочени към по-добра защита на гражданите и инфраструктурата срещу тези заплахи, включително чрез по-тясно сътрудничество между ЕС и неговите държави членки, както и с Организацията на Северноатлантическия договор. Като част от мерките в рамките на Съюза на сигурност за подобряване на защитата и устойчивостта срещу тероризма, Комисията възприе превантивен подход, базиран на аргумента, че химичните, биологичните, радиологичните и ядрените рискове са с ниска вероятност, но със сериозни и трайни последици в случай на нападение. Междувременно, нападението в Солсбъри, както и нарастващата загриженост относно терористичните интереси и способността за използване на химични, биологични, радиологични и ядрени материали, както в рамките на ЕС, така и извън него[18], показват, че заплахата от подобни вещества е реална. Това допълнително засилва спешната необходимост от пълно прилагане на плана за действие. В него се следва подход, обхващащ всички рискове, и се поставя акцент върху следните четири цели: намаляване достъпността на химичните, биологичните, радиологичните и ядрените материали; осигуряване на по-добра подготвеност и реакция при химични, биологични, радиологични и ядрени инциденти, свързани със сигурността; изграждане на по-здрави вътрешни и външни връзки в областта на химичната, биологичната, радиологичната и ядрената сигурност с ключови регионални и международни партньори на ЕС и укрепване на познанията за химичните, биологичните, радиологичните и ядрените рискове. Подробни данни за постигнатия осезаем напредък в прилагането на плана за действие са включени в последния доклад за напредъка по създаването на Съюз на сигурност, приет успоредно с настоящото съвместно съобщение.

И накрая, за повишаване на ефективността на усилията за борба с хибридните заплахи и за подсилване на посланието за единство между държавите от ЕС и съюзниците в рамките на Организацията на Северноатлантическия договор (НАТО), сътрудничеството в борбата с хибридните заплахи бе определено като ключова област в **сътрудничеството между ЕС и НАТО**, както е посочено в *съвместната декларация, подписана във Варшава*[19] през юли 2016 г. Почти една трета от всички настоящи общи предложения за сътрудничество са насочени към хибридните заплахи[20]. През тази година ученията и EU Playbook[21], описани по-горе, се доразвиват с действия за задълбочено сътрудничество.

3. ЗАСИЛВАНЕ НА ДЕЙСТВИЯТА В ОТГОВОР НА ПРОМЕНЯЩИТЕ СЕ ЗАПЛАХИ

3.1. Ситуационна осведоменост — подобрена способност за откриване на хибридни заплахи

Усилията за предотвратяване и реагиране на хибридните заплахи трябва да бъдат подкрепени с капацитет за ранно откриване на злонамерени хибридни дейности и източници, вътрешни и външни, и за разбиране на евентуалните връзки между често привидно несвързани събития. За тази цел, от съществено значение е да се използват всички налични източници на данни, включително разузнаване от открити източници.

---

[18] Европол, Доклад от 2017 г. за обстановката и тенденциите, свързани с тероризма (TE-SAT), стр. 16, който може да бъде намерен на адрес: www.europol.europa.eu/sites/default/files/documents/tesat2017.pdf. Вж. също изявленията на генералния директор на Организацията за забрана на химическото оръжие (ОЗХО): www.globaltimes.cn/content/1044644.shtml.

[19] Декларацията, подписана от председателя Юнкер, председателя Туск и генералния секретар на НАТО Столтенберг, представлява настоящата основа за сътрудничеството между ЕС и НАТО.

[20] 15283/16 и 14802/17.

[21] SWD (2016) 227 final

Звеното за синтез на информацията за хибридните заплахи, създадено в рамките на Европейската служба за външна дейност като единен европейски пункт за анализ на хибридните заплахи, е важен инструмент, който обаче се нуждае от необходимите експертни познания, за да обхване пълния спектър от хибридни заплахи, включително в областта на химичните, биологичните, радиологичните и ядрените вещества и контраразузнаването. Разширяването на експертните познания ще увеличи подкрепата за бъдещи реакции на ЕС при кризи, като предложи по-завършени продукти от сферата на гражданското и военното разузнаване в тези конкретни области. Това може да бъде подкрепено от действия от страна на държавите членки за увеличаване на приноса за звеното за синтез на информацията за хибридните заплахи от разузнавателни данни на техните национални служби и за укрепване на способността на съществуващата мрежа от национални звена за контакт към звеното да предоставя и обработва критична информация. Друга възможност би била държавите членки да обмислят увеличаване на предоставянето на разузнавателни данни от техните национални служби на Центъра на ЕС за анализ на информация (INTCEN) с цел по-задълбочен анализ на потенциалните заплахи.

Бъдещи действия

- Върховният представител ще разшири звеното на ЕС за синтез на информацията за хибридните заплахи като добави специалисти в областта на химичните, биологичните, радиологичните и ядрените вещества, контраразузнаването и киберанализите. Държавите членки се приканват да увеличат приноса на разузнавателни данни за звеното за синтез на информацията за хибридните заплахи за целите на анализа на съществуващи и нововъзникващи хибридни заплахи.

- Комисията, в сътрудничество с върховния представител, ще приключи работата по показателите за уязвимост, за да позволи на държавите членки да оценяват по-добре потенциала на хибридните заплахи в различни сектори. Тази дейност ще подкрепи също така анализа на ЕС на тенденциите по отношение на хибридните заплахи.

3.2. **Засилени действия срещу химични, биологични, радиологични и ядрени заплахи**

В плана за действие за подобряване на готовността за действие срещу химически, биологични, радиологични и ядрени рискове за сигурността от октомври 2017 г. се представя рамката за действия за укрепване на готовността, устойчивостта и координацията на равнище ЕС. Действията, определени в нея, обхващат широк кръг от мерки за подпомагане на държавите членки чрез обединяване на опита, съвместно изграждане на капацитет, обмен на знания и добри практики и засилване на оперативното сътрудничество. Държавите членки и Комисията трябва спешно да пристъпят към съвместна работа за цялостно прилагане на плана за действие. Освен това, като се основава на вече постигнатия напредък по отношение на анализа на пропуските в капацитета за откриване и на обмена на добри практики в рамките на новосъздадената консултативна група по въпросите на химичните, биологичните, радиологичните и ядрените вещества, сега Съюзът следва да предприеме допълнителни мерки за справяне с развиващите се и нововъзникващите заплахи. Това се отнася най-вече до химичните заплахи. Следвайки примера на работата за ограничаване на достъпа до прекурсори на взривни вещества[22], ЕС трябва да предприеме бързи оперативни мерки за по-ефикасен

[22] Като част от работата в рамките на Съюза на сигурност за ограничаване на пространството за действие на терористи и престъпници, Комисията предприе решителни действия за ограничаване на достъпа до прекурсори на взривни вещества, които могат да се използват неправомерно за

контрол на достъпа до високорискови химически материали и за оптимизиране на способността за откриване на такива материали на възможно най-ранен етап. Държавите членки следва също така да предвидят извършването на допълнителен анализ и набелязване на пропуските на равнище ЕС, например по отношение на химичната, биологичната, радиологичната и ядрената устойчивост и на активите и подходите за обеззаразяване. Подготовката за химични, биологични, радиологични и ядрени нападения и управлението на последиците от тях изисква засилено сътрудничество и координация между държавите членки, включително органите за гражданска защита. Механизмът за гражданска защита на Съюза може да играе ключова роля в този процес с цел укрепване на общата способност на Европа за подготовка и реагиране.

Международното сътрудничество също е важен елемент от тази дейност, като ЕС може да се опре върху връзките с регионалните центрове за високи постижения в областта на химичните, биологичните, радиологичните и ядрени вещества, включително търсейки полезни взаимодействия с Организацията на Северноатлантическия договор, и върху програмите за предотвратяване, подготвеност и реакция при природни и причинени от човека бедствия, предназначени за южните и източните съседи на ЕС[23].

Бъдещи действия

- ЕС следва да проучи мерки, чрез които да се гарантира спазването на международните правила и стандарти за предотвратяване на употребата на химически оръжия, включително чрез евентуален режим на санкции на ЕС за забрана на химическо оръжие.
- За да бъде постигнат напредък по плана за действие относно химичните, биологичните, радиологичните и ядрените вещества, Комисията ще работи с държавите членки за завършване на следните стъпки до края на 2018 г.:
  - изготвяне на списък на химическите вещества, които представляват особена заплаха, като основа за оперативните действия за намаляване на тяхната достъпност;
  - установяване на диалог с частни участници във веригата на доставки с цел съвместна работа за справяне с променящите се заплахи от химически вещества, които могат да се използват като прекурсори;
  - ускоряване на прегледа на сценарии за заплахи и анализ на съществуващите методи за откриване с цел подобряване на откриването на химически заплахи с оглед на изготвянето на оперативни насоки за държавите членки да засилят своите способности за откриване.
- Държавите членки следва да направят инвентаризация на запасите от основни медицински мерки за противодействие, лаборатории, лечения и други способности. Комисията ще работи с държавите членки за редовно картографиране на наличността на тези запаси в целия ЕС, за се подобри достъпът до тях и бързото им използване в случай на атаки.

изработката на самоделни експлозиви. През октомври 2017 г. Комисията представи Препоръка за определяне на незабавни действия с цел предотвратяване на злоупотребата с прекурсори на взривни вещества въз основа на съществуващите правила (Препоръка C(2017) 6950 final). Въз основа на това, през април 2018 г. Комисията прие предложение за преразглеждане и укрепване на съществуващия Регламент (ЕС) № 98/2013 относно предлагането на пазара и използването на прекурсори на взривни вещества (COM(2018) 209 final).

[23] В източните и южните съседни на ЕС държави се организират обучения и учения за гражданска защита в рамките на регионалните програми за предотвратяване, готовност и реагиране при природни и причинени от човека бедствия.

3.3. **Стратегическа комуникация — съгласувано разпространение на информация**

Важно предизвикателство по отношение на хибридните заплахи е да се повиши осведомеността и да се образова широката общественост, за да може да различава информацията от дезинформацията. Основавайки се върху опита на оперативната група East StratCom, звеното на ЕС за синтез на информацията за хибридните заплахи и Европейския център за високи постижения в областта на борбата с хибридните заплахи, както и върху други усилия от страна на Комисията[24], Комисията и върховният представител ще продължат да развиват и усъвършенстват способностите на ЕС за стратегическа комуникация, като осигуряват системно взаимодействие и съгласуваност между съществуващите структури. В бъдеще това ще обхване и други институции на ЕС и държавите членки, включително чрез използване на обявената сигурна онлайн платформа по въпросите на дезинформацията.

Подобряването на координацията и сътрудничеството в областта на стратегическата комуникация в рамките на институциите на ЕС, с държавите членки и с партньори и международни организации ще бъде от съществено значение и изисква подготовка и практика преди да се реагира на кризи в реално време.

Периодите на избори са се доказали като особено стратегическа и чувствителна цел за кибератаки и онлайн заобикаляне на конвенционалните („офлайн“) предпазни мерки и правила, като например периоди за размисъл, прозрачни правила за финансирането и равно третиране на кандидатите. Те включват атаки срещу изборна инфраструктура и информационни системи на кампании, както и политически мотивирани масови онлайн кампании за дезинформация и кибератаки на трети държави с цел дискредитиране и лишаване от легитимност на демократичните избори. ЕС работи в няколко направления за повишаване на осведомеността в държавите членки и за подготовка и реагиране на тези променящи се заплахи. В рамките на Съвета органите по киберсигурност на държавите членки[25] ще публикуват незадължителни насоки и ще определят общи добри практики за киберсигурността на изборните технологии през целия изборен цикъл. Това включва информационни системи и решения, основани на ИКТ, които се използват за регистриране на избиратели и кандидати, събиране и преброяване на гласовете и за оповестяване на резултатите, както и спомагателни системи, пряко свързани с легитимността на резултатите от изборите.

Необходимо е също така да се осигурява бърза, надеждна и последователна информация на широката общественост в случай на хибридни атаки. Всякакви химични, биологични, радиологични и ядрени инциденти или подобни събития предизвикват обществено недоволство, тъй като гражданите настояват за бързи отговори. Стратегическите съобщения са от ключово значение, включително за международните организации, които могат да задействат поотделно своите планове за реагиране.

---

[24] Представителствата на Комисията например също са активни в областта на проверката на факти и развенчаването на митове. Някои от тях разработиха инструменти на местно равнище, като например *Les Décodeurs de l'Europe* във Франция, UE Vero Falso в Италия, обществен конкурс за комикс в Австрия на тема „Развенчаване на митовете за ЕС“, подобна поредица комикси в Румъния и поредицата на Представителството в Обединеното кралство — Евромитове от А до Я. Още подобни проекти са в процес на подготовка.

[25] Дейностите са под егидата на групата за сътрудничество, създадена по силата на Директивата относно сигурността на мрежите и информационните системи.

Бъдещи действия

- Европейската служба за външна дейност и Комисията ще работят заедно в рамките на своите компетенции за установяването на по-структурирано сътрудничество в областта на стратегическите комуникации с цел справяне с дезинформацията с произход от ЕС и извън него, както и за да се предотврати враждебното създаване на дезинформация и хибридната намеса от страна на чужди правителства.

- През есента Комисията ще организира мероприятия на високо равнище с държавите членки и съответните заинтересовани страни, в т.ч. колоквиум за основните права, посветен на демокрацията, за да се популяризират най-добрите практики и насоките за това как да се предотвратяват, смекчават и как да се реагира на заплахите от кибератаки и дезинформация, свързани с избори.

- Върховният представител и Комисията ще обсъдят начини за по-добро подпомагане, по отношение на инструменти и ресурси, на работата на трите работните групи за стратегическа комуникация, за да се гарантира, че мащабът на усилията на ЕС е подходящ за справяне със сложността на кампаниите за дезинформация на враждебно настроени лица.

3.4. **Изграждане на устойчивост и възпиращ ефект в сектора на киберсигурността**

Киберсигурността е от съществено значение за нашето благоденствие и сигурност. С повишаването на зависимостта на нашето ежедневие и нашите икономики от цифровите технологии все по-често сме изложени на евентуални заплахи.

Ефективната киберсигурност в ЕС днес е възпрепятствана от недостатъчните инвестиции и недостатъчната координация. ЕС се стреми да намери решение на този проблем чрез изграждане на капацитет посредством мерки за подкрепа, по-добра координация и нови структури за развитие и внедряване на технологиите в областта на киберсигурността[26]. С Директивата относно сигурността на мрежите и информационните системи[27] бе установено минимално ниво на сигурност на мрежите и информационните системи в Съюза. Нейното пълно прилагане от страна на всички държави членки е от съществено значение за подобряване на устойчивостта на киберпространството — това е важна първа стъпка. Общият регламент относно защитата на данните въвежда задължение за уведомяване на компетентния надзорен орган при нарушаване на сигурността на личните данни. Други основни мерки са по-силна и модернизирана агенция за киберсигурност на Европейския съюз и европейска рамка за сертифициране на ИКТ продукти и услуги[28] с цел изграждане на доверие у потребителите. В ход са и дейности за подпомагане на мрежата от експертни центрове в държавите членки, за да се стимулира разработването и внедряването на решения, свързани с киберсигурността, и да се допълнят усилията за изграждане на капацитет в тази област на европейско и национално равнище. Тези дейности ще се опрат на работата

[26] В рамките на укрепването на иновациите в регионите на Европа, през декември 2017 г. започна ново междурегионално пилотно действие, обединяващо регионите на ЕС с цел активизиране на работата в областта на киберсигурността.

[27] Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза.

[28] COM (2017) 477.

по представената на 6 юни от Комисията програма „Цифрова Европа“[29], с която се дава нов приоритет на инвестициите на ЕС в областта на киберсигурността.

Същевременно в препоръка относно координирана реакция на мащабни киберинциденти и кризи[30] се определя как следва да действа сътрудничеството между държавите членки и различните участници от ЕС при реакция на мащабни трансгранични кибератаки. В препоръката се подчертава съществената роля на ситуационната осведоменост за ефективната координация на техническо, оперативно и стратегическо/политическо равнище. Групата за сътрудничество, създадена съгласно Директивата относно сигурността на мрежите и информационните системи, също работи за подобряване на обмена и споделянето на информация между съответните страни, като разработва обща таксономия за описание на инцидентите. Този подход ще бъде тестван в рамките на бъдещи учения. Стратегическият анализ на настоящите и нововъзникващите заплахи за киберсигурността, основан на приноса от разузнавателните служби на държавите членки, се извършва от звеното за синтез на информацията за хибридните заплахи.

Рамката за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството („инструментариум за кибердипломация“) бе важна стъпка напред в оперативен план, като определи мерките в рамките на общата външна политика и политика на сигурност, включително ограничителни мерки, които могат да се използват за укрепване на реакцията на ЕС спрямо дейности, които нарушават неговите политически, икономически и свързани със сигурността интереси. Колкото по-цялостно се използва рамката от държавите членки, толкова повече тя ще бъде ефективно възпиращо средство. През април на заседанието на Съвета по външни работи бяха приети заключения относно злонамерените кибернетични дейности, които категорично осъждат злонамереното използване на информационни и комуникационни технологии, включително при атаките WannaCry и NotPetya, които нанесоха значителни щети и икономически загуби в ЕС и извън него.

ЕС и неговите държави членки трябва да подобрят способността си за установяване на отговорните за кибернетичните атаки лица, не на последно място чрез засилен обмен на разузнавателни данни. Уличаването на извършителите на дадена атака би възпряло потенциалните агресори и би повишило шансовете от извършителите да бъде потърсена отговорност. Увеличаването на възпиращите действия е ключова цел в стратегическия подход на Комисията за подобряване на киберсигурността. Неотдавнашните предложения на Комисията, насочени към подобряване на трансграничното събиране на електронни данни за наказателни производства, също ще допринесат значително за увеличаване на способността на правоприлагащите органи да разследват и преследват престъпления в кибернетичното пространство.

Добрата устойчивост на киберпространството се нуждае от колективен и широкообхватен подход. Това налага изграждането на по-стабилни и ефективни структури за насърчаване на киберсигурността и за реакция на кибератаки в държавите членки, но също и в рамките на самите институции, агенции, делегации, мисии и операции на ЕС. Липсата на съвместна сигурна комуникационна мрежа между европейските институции е важен недостатък. Осведомеността за кибернетичната сигурност в институциите на ЕС и сред техните служители следва да бъде повишена чрез подобрена култура на сигурност и по-интензивно обучение.

[29] Предложение за Регламент за създаване на програмата „Цифрова Европа“ за периода 2021 — 2027 г., COM(2018) 434.

[30] C(2017) 6100.

Бъдещи действия

- Европейският парламент и Съвета следва да ускорят своята работа по приключване на преговорите относно предложенията за киберсигурността, като постигнат споразумение до края на тази година и бързо се договорят по предложеното законодателство относно събирането на електронни доказателства.

- Комисията и върховният представител ще работят в тясно сътрудничество с държавите членки за постигане на напредък по аспектите на киберсигурността в рамките на общоевропейските механизми за реакция и управление на кризи. Държавите членки се приканват да продължат работата си по установяване на източниците на кибератаки и по практическото използване на инструментариума за кибердипломацията с цел по-решителен политически отговор на кибератаките.

- В отговор на необходимостта от укрепване на нашите способности за кибернетична отбрана бе създадена специална платформа за обучение и образование, която ще помогне за координиране на възможностите за обучение в областта на кибернетичната отбрана, предлагани от държавите членки. Ще се търси и взаимодействие с подобни действия на Организацията на Северноатлантическия договор.

3.5. **Изграждане на устойчивост срещу вражеска разузнавателна дейност**

Противодействието на вражеска разузнавателна дейност изисква преди всичко засилено и ефективно сътрудничество между държавите членки, в съответствие с приложимите европейски и национални правила и разпоредби. Също така обаче е задължително да се увеличат способностите на институциите на ЕС за борба с нарастващата заплаха от такава дейност, насочена специално към институциите, и за изграждане на култура на осведоменост по въпросите на сигурността, подкрепена от по-добро обучение и физическа сигурност. Институциите биха могли да работят с държавите членки и за изграждането на по-стабилна система на ЕС за акредитация. Тази система ще се основава на проактивно докладване, което ще доведе до по-добра осведоменост на държавите членки и институциите за възможни враждебно настроени лица, по-конкретно за вече идентифицираните такива от държавите членки.

Координацията между държавите членки и между държавите членки и други съответни международни организации, по-специално Организацията на Северноатлантическия договор, ще спомогне за засилване на контраразузнаването срещу вражеска дейност в ЕС. Пример за област, която би спечелила от по-добрата координация между държавите членки, е скринингът на инвестициите, въз основа на предложен от Комисията през септември 2017 г. регламент[31] за скрининг на преките чуждестранни инвестиции от страна на държавите членки от съображения за опазване на сигурността и обществения ред. Повишената координация между държавите членки ще бъде също толкова важна за контролиране на финансовите операции, тъй като вражеските разузнавателни служби все по-често финансират своите активни мерки срещу ЕС посредством сложни финансови схеми.

[31] Предложение за Регламент на Европейския парламент и на Съвета за създаване на рамка за скрининг на преки чуждестранни инвестиции в Европейския съюз, COM(2017) 487.

Бъдещи действия

- Европейската служба за външна дейност и Комисията ще въведат по-добри практически мерки за поддържане и развитие на способността на ЕС за взаимодействие с държавите членки с оглед на борбата с вражеска разузнавателна дейност, насочена конкретно към институциите.

- Укрепеното звено за синтез на информацията за хибридните заплахи ще бъде допълнено с експерти в сферата на контраразузнаването, за да предоставя подробни анализи и брифинги относно естеството на вражеската разузнавателна дейност, която има вероятност да е насочена срещу физически лица и институциите.

- Европейският парламент и Съветът следва да ускорят своята работа по приключване на преговорите по предложението за скрининг на инвестициите до края на годината.

4. ЗАКЛЮЧЕНИЕ

Хибридните и химичните, биологичните, радиологичните и ядрените заплахи са приоритет за ЕС. Инцидентът в Обединеното кралство от месец март ясно показа широкия спектър на хибридните военни дейности и крайната необходимост от устойчивост в лицето на химични, биологични, радиологични и ядрени заплахи.

Комисията и върховният представител приеха и предложиха редица инициативи за справяне с предизвикателствата, свързани с хибридните заплахи. Освен това Комисията ускорява прилагането на плана за действие от 2017 г. за подобряване на готовността за действие срещу химически, биологични, радиологични и ядрени рискове за сигурността.

Настоящото съвместно съобщение има за цел да информира Европейския съвет за вече започнатата работа и да набележи областите, в които действията следва да бъдат засилени с цел допълнително да се задълбочи и укрепи съществения принос на ЕС за справяне с тези заплахи. Държавите членки, Комисията и върховният представител трябва да гарантират бързи последващи действия.