ЕВРОПЕЙСКА
КОМИСИЯ

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

Брюксел, 10.11.2022 г.
JOIN(2022) 49 final

СЪВМЕСТНО СЪОБЩЕНИЕ ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Политика на ЕС за киберотбрана

I. ВЪВЕДЕНИЕ

Завръщането на войната в Европа с неоправданата и непровокирана военна агресия на Русия срещу Украйна е сигнал за тревога за всички, които поставят под въпрос подхода на ЕС към сигурността и отбраната, способността му да популяризира своята визия и да защитава интересите си, включително в киберпространството. Авторитарните режими се опитват да оспорят и подкопаят основания на правила международен ред в киберпространството, превръщайки го във все по-спорна област наред със сушата, морето, въздуха и космоса. Злонамереното поведение в киберпространството, идващо от държавни и недържавни субекти, се засили през последните години, включително нарастващият брой кибератаки, насочени срещу военна и гражданска критична инфраструктура в ЕС, както и срещу разгърнати мисии и операции.

Границите между гражданското и военното измерение на киберпространството са размити, както се вижда от неотдавнашните атаки срещу енергийни мрежи, транспортна инфраструктура и космически активи. Това илюстрира също така взаимозависимостта между физическата и цифровата инфраструктура и потенциала значителни инциденти в областта на киберсигурността да предизвикат смущения или да имат вредни последствия за критичната инфраструктура. Това е сериозно напомняне, че ЕС се нуждае от тясно военно и гражданско сътрудничество в киберпространството, за да стане по-силен фактор за сигурността.

ЕС трябва да поеме по-голяма отговорност за собствената си сигурност. За това са необходими модерни и оперативно съвместими европейски въоръжени сили. Ето защо държавите членки трябва спешно и приоритетно да се ангажират с увеличаване на инвестициите в целия спектър от способности за киберотбрана, включително активни отбранителни способности. Макар да продължава да бъде напълно ангажиран с международното право и международните норми в киберпространството, ЕС следва да изрази готовността си да използва тези способности по координиран начин в случай на кибератака срещу държава членка.

За да успее да направи това, ЕС трябва да гарантира своя технологичен и цифров суверенитет в киберпространството. Капацитетът на ЕС за действие ще зависи от способността му да овладее и разработи авангардни технологии за киберсигурност и киберотбрана в ЕС. Тъй като кибертехнологиите имат силен потенциал за двойна употреба, киберсигурността и киберотбраната, научноизследователската и развойната дейност и дейностите в областта на иновациите трябва да се осъществяват по начин, осигуряващ по-големи полезни взаимодействия, за да се развиват по-добри способности.

Общото предотвратяване и откриване са важна част от отбранителните способности на ЕС. ЕС трябва да разполага с капацитет за откриване на атаки на ранен етап. Данните от откриването трябва да се превърнат в полезна информация, която може да послужи както на киберсигурността, така и на киберотбраната. Подобно сътрудничество между отбранителната и гражданската киберобщност е основата за една по-добра обща ситуационна осведоменост в киберпространството и е също толкова важно за координираните действия за реагиране при кризи на техническо и на оперативно равнище.

Въоръженият конфликт в Украйна също така показа значението на тясното сътрудничество с частния сектор и необходимостта от достъп до частни доверени доставчици, действащи като кибернетични резерви, за да се подобрят действията за реагиране в случай на мащабни кибератаки. Ето защо е необходимо да се гарантира, че държавите членки могат да разчитат на подкрепа от надеждни кибернетични резерви и че това става по сигурен и координиран начин.

В настоящото съвместно съобщение, макар и да се основава на рамката за политика на ЕС за киберотбрана[1], се предлага амбициозна стратегия, която да позволи на ЕС и неговите държави членки да действат със самочувствие и увереност в киберпространството. То има за цел да се повишат способностите за киберотбрана чрез индивидуални или съвместни действия на държавите членки и да се засилят координацията и сътрудничеството между киберобщностите на ЕС. То ще спомогне също така за намаляване на стратегическите зависимости на ЕС в областта на критичните кибертехнологии и за укрепване на европейската отбранителна технологична и индустриална база (ЕОТИБ). Политиката ще определи „правилата на играта“ на ЕС и ще предложи начини за укрепване на солидарността в ЕС в областта на киберотбраната, както и на сътрудничеството с частния сектор с цел подобряване на действията за реагиране в случай на големи кибератаки. Като се има предвид транснационалният характер на киберзаплахите, с нея ще се развиват взаимноизгодни и съобразени с нуждите партньорства в областта на киберотбраната, включително изграждане на капацитет за киберотбрана, и ще се повиши киберустойчивостта на държавите партньори.

Както е предложено в Стратегическия компас за сигурността и отбраната[2], приет от Съвета през март 2022 г., настоящата политика за киберотбрана ще подобри способността за предотвратяване и откриване на кибератаки, насочени срещу ЕС и неговите държави членки, за защита и възстановяване от кибератаки и за тяхното възпиране, като се използват всички налични средства. Това е в съответствие с приоритетите на Комисията в областта на цифровите технологии, с амбицията, заложена в Стратегията на ЕС за киберсигурност от 2020 г.[3], с изявлението на председателя Фон дер Лайен в нейната реч за състоянието на Съюза през 2021 г.[4] и със заключенията на Съвета относно установяването на позицията на ЕС в киберпространството[5] от 23 май 2022 г. В Съвместното съобщение от 2022 г. относно недостига на инвестиции в отбраната[6] ЕС и неговите държави членки се насърчават също така да започнат работа за изграждане на целия спектър от способности за киберотбрана — от научни изследвания, откриване и защита до реагиране.

II. КИБЕРОТБРАНА НА ЕС ЗА ЗАЩИТА, ОТКРИВАНЕ, ВЪЗПИРАНЕ И ПРЕДПАЗВАНЕ ОТ КИБЕРАТАКИ

[1] Актуализация на рамката за политиката на ЕС за киберотбрана за 2018 г., 19 ноември 2018 г., http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/bg/pdf
[2] Стратегически компас за сигурността и отбраната — за Европейски съюз, който защитава своите граждани, ценности и интереси и допринася за международния мир и сигурност
[3] Стратегия на ЕС за киберсигурност за цифровото десетилетие (JOIN/2020/18 final).
[4] https://ec.europa.eu/commission/presscorner/detail/bg/SPEECH_21_4701
[5] 9364/22
[6] JOIN(2022) 24 final

1. Да действаме заедно за по-силна киберотбрана

Кибератаките често имат трансграничен характер и могат да окажат физическо въздействие върху критична инфраструктура в ЕС. Значителни инциденти в областта на киберсигурността могат да доведат до големи смущения, с които една или няколко засегнати държави членки не могат да се справят сами. Те може също така да бъдат част от по-големи хибридни атаки, извършвани от трети държави с цел дестабилизиране на икономиката и обществото, отслабване на критичната инфраструктура, необходима за гарантиране на сигурността на ЕС, или подкопаване и увреждане на функционирането на демокрациите, включително чрез атаки срещу инфраструктури за провеждане на избори.

През 2018 г. ЕС определи киберпространството като област на военни операции. Военната визия и стратегия относно киберпространството като област на операции[7], приета през 2021 г., определя рамковите условия и описва целите, начините и средствата, необходими за използването на киберпространството като област на операции в подкрепа на операциите по линия на общата политика за сигурност и отбрана (ОПСО) на ЕС. Киберотбраната и използването на свързаните с нея способности в целия спектър на военните операции в киберпространството са национален прерогатив на държавите членки, като същевременно се разчита на по-широка екосистема, включително на силна индустриална база, подкрепена от развитието на способностите на равнището на ЕС.

Общността на ЕС за киберотбрана, съставена от отбранителните органи на държавите членки и подкрепяна от институциите, органите и агенциите на ЕС, има някои особености в сравнение с другите киберобщности[8] и следва различен модел на управление. Липсата на установена рамка за обмен на информация и сътрудничество между военните екипи на ЕС за незабавно реагиране при компютърни инциденти (milCERT), включително в подкрепа на военните мисии и операции по линия на ОПСО, е проблематична с оглед на повишеното ниво на киберзаплахи от страна на държавни и недържавни участници.

Сътрудничеството между гражданските, дипломатическите и правоприлагащите киберобщности и техните партньори в областта на отбраната ще има голяма добавена стойност за всички заинтересовани страни. Ето защо от решаващо значение е да се даде възможност за такова сътрудничество, като се осигурят подходящи и сигурни средства за обмен на информация и се участва в учения и други дейности, които изграждат доверие и общо разбиране.

Освен това понастоящем взаимната оперативна помощ между държавите членки е ограничена. Следва да се проучи по-нататъшното разширяване на концепцията за екипи за бързо реагиране при кибератаки в целия ЕС, като се стъпи на свързания с нея проект „Екипи за бързо реагиране при кибератаки и взаимопомощ в областта на киберсигурността“ (CRRT) по линия на постоянното структурирано сътрудничество

[7] EEAS(2021) 706 REV4

[8] Граждански, дипломатически и правоприлагащи киберобщности

(ПСС)[9], включително в контекста на член 42, параграф 7 от Договора за Европейския съюз (ДЕС)[10] („клауза за взаимопомощ“) и член 222 от Договора за функционирането на Европейския съюз (ДФЕС)[11] („клауза за солидарност“). По подобен начин една от извлечените поуки от успешната киберотбрана на Украйна в контекста на руската агресивна война е решаващата роля на частния сектор. Ето защо следва да се проучи до каква степен частният сектор също би могъл да допринесе за подобряване на реагирането при киберинциденти.

1.1 *Укрепване на общата ситуационна осведоменост и координацията в рамките на общността за отбрана*

Предвид мащаба на риска, свързан с кибератаките, държавите членки трябва да разполагат с най-пълна колективна ситуационна осведоменост, включително с капацитет за ранно откриване, както и с ресурси за адекватна реакция и възстановяване по солидарен и координиран начин.

Що се отнася до военната ситуационна осведоменост, необходимо е да се създаде **Координационен център на ЕС за киберотбрана (КЦК на ЕС)**, който да подпомага по-добрата ситуационна осведоменост в рамките на общността за отбрана, включително всички военни командири на ЕС по линия на ОПСО. Върховният представител ще представи за разглеждане от държавите членки предложението за КЦК на ЕС, основано на проекта „Координационен център в областта на киберсигурността и информацията (КЦКИ)“ по линия на ПСС[12]. Целта на предложението е да се предостави цялостен анализ на киберпространството, електромагнитната обстановка и когнитивната област, като се обединят различни източници на информация на военностратегическо и оперативно равнище. Следва да се установят подходящи връзки между КЦК на ЕС и Центъра на ЕС за анализ на информацията (INTCEN), както и с Дирекция „Разузнаване“ към Военния секретариат на ЕС в рамките на единното звено за анализ на разузнавателна информация. В допълнение към външните източници на информация КЦК на ЕС следва да създаде и интегрира независима активна сензорна система на основата на информационните технологии, за да засили мониторинга на звената на ЕС, които подпомагат военните мисии и операции по линия на ОПСО. Тя ще предостави по-добри възможности за откриване и ще създаде нов слой информация, за да се подобри допълнително информационната база за оценка на киберриска и ситуационната осведоменост.

За тези цели са необходими способности, които позволяват и обезпечават създаването и поддържането на постоянно оперативна и по възможност призната картина на киберпространството, включително текущи и непосредствени кибероперации както на противниците, така и на приятелските сили. Подобна картина ще допринесе за

[9] Екипи за бързо реагиране при кибератаки и екипи за взаимопомощ в областта на киберсигурността

[10] Договор за Европейския съюз, консолидирана версия: Официален вестник C 326, 26.10.2012 г., стр. 0001—0390.

[11] Договор за функционирането на Европейския съюз, консолидирана версия: Официален вестник C 326, 26.10.2012 г., стр. 0001—0390.

[12] Целта на проекта е да се разработи, създаде и управлява многонационален координационен център в областта на киберсигурността и информацията (CIDCC) като постоянен многонационален военен елемент.

планирането и провеждането на военни мисии и операции на ЕС по линия на ОПСО. Това ще бъде военният принос за повишаване на осведомеността и реакцията на ЕС по отношение на злонамерени действия в киберпространството.

За да се повиши доверието и да се обменя надеждна и навременна стратегическа информация за големи киберинциденти, **конференцията на киберкомандирите на ЕС** ще бъде разширена и засилена[13]. С участието на Европейската агенция по отбрана (EDA) в качеството ѝ на секретариат и с участието на Военния секретариат на Европейския съюз конференцията ще се провежда поне два пъти годишно, за да се обсъждат оперативни въпроси и други значими теми.

Ще бъде създадена оперативна мрежа за **milCERT (MICNET)** с подкрепата на Европейската агенция по отбрана. Всички държави членки са призовани да участват в MICNET, която се очаква да започне да функционира през януари 2023 г.

Като улеснява обмена на информация между milCERT, MICNET ще насърчава действия за по-категорична и координирана реакция при киберзаплахи, засягащи системите за отбрана в ЕС, включително тези, използвани във военните мисии и операции по линия на ОПСО. MICNET ще позволи също така процесите по отношение на обучението и непрекъснатото определяне на нови изисквания за общността на milCERT да се поддържат във времето. През следващите четири години Европейската агенция по отбрана, съвместно с държавите членки, ще разработи инфраструктура за обмен на информация, както и свързани с нея инструменти и процедури, за да се подпомогне обменът на информация между milCERT. MICNET също така ще предостави рамката за годишна процедура за изпитване, валидиране и набелязване на нови изисквания и решения.

1.2. Подобряване на координацията с гражданските общности

MICNET следва да служи като рамка и инфраструктура за обмен на информация между различните равнища в рамките на общността за киберотбрана и външните заинтересовани страни.

Когато MICNET достигне по-висока степен на зрялост, Европейската агенция по отбрана ще подкрепи държавите членки в проучването на възможностите за сътрудничество с мрежата на **екипите за реагиране при инциденти с компютърната сигурност (CSIRT)**, която обединява националните CSIRT и екипите за незабавно реагиране при компютърни инциденти на институциите, органите и агенциите на ЕС (CERT-EU). Това сътрудничество може да включва съвместни срещи и учения. Следва да се проучи и участието на частния сектор в усилията за обмен на значима информация и за реагиране при инциденти.

За да се даде възможност за по-ефективно управление на киберкризи, Конференцията на киберкомандирите на ЕС следва да се ангажира с мрежата на ЕС за връзка на организациите при кибернетични кризи (EU-CyCLONe), която обединява държавите членки и Комисията, за да подпомогне координацията и управлението на мащабни

[13] Въз основа на първите две заседания на стратегическите конференции на европейските киберкомандири (CyberCo) през януари и юни 2022 г., киберкомандирите на ЕС решиха да създадат по-постоянен форум на своето равнище.

киберинциденти в ЕС. Тази ангажираност ще съчетае военен опит и гражданска ситуационна осведоменост на стратегическо и оперативно равнище.

Като се има предвид, че КЦК на ЕС следва да действа като център за събиране, анализиране, оценяване и окончателно разпространение на информация, свързана с киберотбраната, по-специално за военни мисии и операции по линия на ОПСО, той би могъл също така да се свърже с междуинституционалната работна група за киберкризи[14], която беше създадена, за да се осигурят информирано вземане на решения и реагиране на институциите, органите и агенциите на ЕС при мащабни киберкризи на стратегическо и оперативно равнище.

КЦК на ЕС може също така да обменя значима информация с центъра за киберситуация и анализ, който е в процес на създаване в Комисията с подкрепата на ENISA и CERT-EU, за да се предоставят анализ и по-ефективна подкрепа за управление на кризи.

Освен това липсата на общи или оперативно съвместими инструменти и платформи за сигурна комуникация между държавите членки и съответните институции, органи и агенции на ЕС продължава да бъде основна пречка. Понастоящем Комисията и съответните институции извършват картографиране на съществуващите инструменти за сигурна комуникация в киберпространството. Въз основа на това картографиране на съществуващите инструменти Комисията ще представи своите препоръки на Съвета в края на 2022 г., за да се постигне договореност относно по-нататъшни действия.

Киберсолидарност на ЕС за по-силно общо откриване и ситуационна осведоменост

Гражданските действия за подкрепа могат допълнително да повишат общата ситуационна осведоменост. Общността за киберотбрана ще може да се възползва от по-силните граждански способности за откриване и ситуационна осведоменост, разработени за защитата на критичната инфраструктура на ЕС. За тази цел Комисията подготвя инициатива за насърчаване на разгръщането на инфраструктура на ЕС от центрове за операции по сигурността (ЦОС) въз основа на първа фаза, която ще стартира през следващите седмици и която след това ще бъде разширена и разгърната в по-голям мащаб[15]. В крайна сметка тази инфраструктура ще бъде съставена от няколко многонационални платформи за ЦОС, всяка от които ще обединява национални ЦОС, с подкрепа от програма „Цифрова Европа“[16], която ще допълва националното финансиране. Законодателните промени в програма „Цифрова Европа“ биха позволили по-дългосрочна финансова подкрепа за съвместно възлагане на обществени поръчки за свръхсигурни инструменти и инфраструктура от следващо поколение. С предвидената инфраструктура на ЕС от ЦОС ще се даде възможност да се подобрят способностите за колективно откриване чрез използване на най-новите технологии за изкуствен интелект

[14] Неформална група, включваща съответните служби на Комисията, ЕСВД, Агенцията на Европейския съюз за киберсигурност (ENISA), CERT-EU и Европол, която се председателства съвместно от Комисията и върховния представител.

[15] Стратегия на ЕС за киберсигурност за цифровото десетилетие (JOIN/2020/18 final) и Стратегия на ЕС за Съюза на сигурност (COM(2020) 605)

[16] В съответствие с Регламент (ЕС) 2021/694 на Европейския парламент и на Съвета от 29 април 2021 г. за създаване на програма „Цифрова Европа“ и за отмяна на Решение (ЕС) 2015/2240 (ОВ L 166, 11.5.2021 г., стр. 1—34), подлежащ на евентуални изменения.

(ИИ) и анализ на данни, обхващащи гражданските комуникационни мрежи. Това генериране на оперативни разузнавателни сведения за киберзаплахи ще даде възможност за своевременно предупреждаване на органите и съответните структури, за да могат те да откриват мащабни инциденти и да реагират ефективно. Мащабът и обхватът на инфраструктурата ще зависят от общото финансиране, което може да бъде осигурено на национално равнище и от Съюза, в зависимост от наличния бюджет по многогодишната финансова рамка.

Такива многонационални ЦОС биха могли също така да позволят участието на структури за отбрана чрез създаване на „стълб за отбрана“ по отношение на управлението и вида на споделяната информация. Този „стълб за отбрана“ би могъл да бъде разработен съвместно с върховния представител и да включва специален механизъм за обмен на информация с военни участници, включително с КЦК на ЕС, за който биха могли да бъдат разработени стандарти за сигурност на равнището на отбраната.

Киберсолидарност на ЕС в областта на готовността, реагирането и възстановяването

Значителните инциденти в областта на киберсигурността могат да нанесат прекалено големи вреди, с които една или няколко засегнати държави членки не могат да се справят сами. В такива случаи държавите членки трябва да могат да разчитат на взаимопомощ и солидарност, включително в контекста на член 42, параграф 7 от ДЕС и член 222 от ДФЕС. Върховният представител, в сътрудничество с Комисията и държавите членки, ще проучи възможностите за **разширяване на концепцията за екипи за бързо реагиране при кибератаки (CRRT)**, като се стъпи на свързания с нея проект „Екипи за бързо реагиране при кибератаки и екипи за взаимопомощ в областта на киберсигурността“ по линия на ПСС, за да се окаже по-добра подкрепа на държавите — членки на ЕС, и на мисиите и операциите по линия на ОПСО. Ролята на тези екипи ще бъде да предоставят съобразена с нуждите и целенасочена краткосрочна помощ при поискване и в зависимост от конкретните нужди във всеки отделен случай. Когато е уместно, тя може да включва и варианти за подкрепа от доверени частни партньори, за да се гарантират ефикасни действия за реагиране и възстановяване.

Комисията подготвя действия за укрепване на готовността и за реагиране в целия ЕС като част от инициативата за киберсолидарност на ЕС. Това би включвало **изпитване на основни структури, опериращи с критична инфраструктура, за потенциални уязвимости въз основа на оценки на ЕС на риска —** на основата на действия, които вече са започнати от Комисията съвместно с ENISA — , както и действия за реагиране при инциденти с цел смекчаване на въздействието на тежки инциденти, подпомагане на незабавното възстановяване и/или възстановяване на функционирането на основни услуги[17].

Инициативата на ЕС за киберсолидарност би могла да подпомогне **постепенното създаване на киберрезерв на равнището на ЕС с услуги от надеждни частни доставчици,** които биха били готови да се намесят по искане на държавите членки в случаи на значителни трансгранични инциденти. Ролите и отговорностите следва да

[17] Призив от Невер за укрепване на капацитета на ЕС за киберсигурност

бъдат ясно определени и напълно координирани със съществуващите органи, за да се гарантира, че подкрепата от киберрезерва на равнището на ЕС се предоставя там, където е необходима, и допълва други потенциални форми на помощ. Макар че обхватът на действията и разпределението на разходите за конкретните интервенции ще зависят от наличното финансиране от ЕС, ЕС би добавил стойност и като обезпечи наличието и готовността на такъв резерв на равнището на ЕС. За да се гарантира високо ниво на доверие, Комисията ще разгледа и възможностите за подкрепа на разработването на схеми за сертифициране за киберсигурност за такива частни дружества в областта на киберсигурността.

Ученията са ключов елемент от изграждането на готовност. Те насърчават развитието на обща база знания и общо разбиране за киберотбраната, което от своя страна повишава оперативната готовност. Общите учения по киберотбрана също така ще изградят оперативна съвместимост и доверие между заинтересованите страни, включително в подкрепа на военните мисии и операции по линия на ОПСО. Въз основа на ученията от поредицата CYBER PHALANX[18] и ученията на milCERT **Европейската агенция по отбрана ще създаде нов проект CyDef-X, който ще обединява всички държави членки** и **ще служи като рамка за ученията на ЕС в областта на киберотбраната**. Този проект би могъл да послужи за осъществяване на взаимопомощ съгласно член 42, параграф 7 от ДЕС. Следва да се проучи и използването на специализирани среди за изпитване, обучение и учения в областта на киберотбраната (напр. федериране на киберполигони), включително чрез използване на проекта „Федериране на киберполигони“ по линия на ПСС[19].

Ученията могат да играят важна роля и за подобряване на сътрудничеството между гражданските и военните структури. Ето защо при организирането на учения ENISA, Европейската агенция по отбрана и други съответни структури следва систематично да обмислят включването на участници от други киберобщности.

Като част от укрепването на капацитета на ЕС за предотвратяване, възпиране и реагиране на кибератаки и в съответствие със Стратегията на ЕС от 2020 г. за киберсигурност за цифровото десетилетие. и със Стратегическия компас върховният представител ще предложи през 2023 г. варианти за по-нататъшно укрепване на инструментариума на ЕС за кибердипломация[20], като се опира на елементите от установяването на позицията на ЕС в киберпространството и на извлечените поуки от прилагането на инструментариума от създаването му досега.

Действия за киберотбрана

- Създаване на Координационен център на ЕС за киберотбрана като център за обща военна ситуационна осведоменост и за проучване на условията за сътрудничество с центъра за киберситуация и анализ в Комисията.
- По-нататъшно развитие и укрепване на Конференцията на киберкомандирите на ЕС.

[18] https://eda.europa.eu/publications-and-data/factsheets/factsheet-cyber-phalanx

[19] https://www.pesco.europa.eu/project/cyber-ranges-federations-crf/

[20] Заключения на Съвета относно рамка за съвместен дипломатически отговор на ЕС срещу злонамерени дейности в киберпространството („инструментариум за кибердипломация“).

- Насърчаване на държавите членки да участват активно в MICNET — мрежата на военните екипи за незабавно реагиране при компютърни инциденти, и да работят за установяване на сътрудничество с мрежата на гражданските CSIRT.
- Разработване на нов рамков проект CyDef-X в подкрепа на ученията на ЕС в областта на киберотбраната.
- Проучване на възможностите за доразвиване на концепцията за екипи за бързо реагиране при кибератаки, като се стъпи на проекта „Екипи за бързо реагиране при кибератаки и екипи за взаимопомощ в областта на киберсигурността“ по линия на ПСС.
- Проучване на възможностите за по-нататъшно развитие на проектите за федериране на киберполигони.

Граждански действия за подкрепа

- Подготовка на инициатива на ЕС за киберсолидарност, включително евентуален акт за законодателни промени в програма „Цифрова Европа“, с цел:
    - укрепване на общите способности на ЕС за откриване, ситуационна осведоменост и реагиране;
    - постепенно изграждане на киберрезерв на равнището на ЕС от услуги от доверени частни доставчици;
    - подпомагане на изпитването на критични обекти за потенциални уязвимости въз основа на оценки на ЕС на риска.
- Проучване на възможностите за разработване на схеми за сертифициране за киберсигурност на равнището на ЕС в сектора на киберсигурността и за частни дружества в областта на киберсигурността.
- Засилване на сътрудничеството на стратегическо, оперативно и техническо равнище между общността за киберотбрана и други киберобщности.

2. Защита на отбранителната екосистема на ЕС

През последните години броят на кибератаките се увеличи значително, включително атаките на веригата за доставки, целящи кибершпионаж, софтуер за изнудване или смущения. През 2020 г. атаката на веригата за доставки SolarWinds[21] засегна повече от 18 000 организации в световен мащаб, включително правителствени агенции, големи предприятия и дружества в областта на отбраната. Използването на уязвимост в софтуера log4j на Apache[22] показа, че дори софтуерни компоненти, които не се считат за високорискови или критични, могат да бъдат приспособени за бойна употреба за извършване на успешни атаки в ЕС срещу големи дружества или правителства, включително в областта на отбраната. Това показва ясна необходимост от по-нататъшно укрепване на киберустойчивостта на субектите, които са активни в отбранителната екосистема на ЕС, включително военните структури, отбранителната промишленост и частните оператори.

[21] https://cybernews.com/security/solarwinds-hack-the-mystery-of-one-of-the-biggest-cyberattacks-ever/
[22] https://english.ncsc.nl/topics/log4j-vulnerability

Въоръжените сили зависят до голяма степен от гражданската критична инфраструктура, независимо дали става въпрос за мобилност, комуникации или енергия. Пример за такава взаимовръзка е руската атака срещу сателитната мрежа KA-SAT[23], която причини смущения в комуникацията на няколко публични органа, както и на украинските въоръжени сили. Това показва необходимостта от защита на такава критична инфраструктура.

За да се справят с проблемите, свързани със сигурността на своите комуникационни и информационни системи (КИС), държавите членки разработват свои собствени стандарти и изисквания за сигурност за военните системи, които невинаги отчитат необходимостта от оперативна съвместимост, нито наличието на граждански стандарти за продуктите с двойна употреба. Това оказва отрицателно въздействие върху способността на държавите членки да действат заедно в киберпространството, също и в контекста на военните мисии и операции по линия на ОПСО, и създава пречки пред взаимната помощ. Освен това е необходимо да се насърчават по-силни полезни взаимодействия между военните и гражданските пътища за стандартизация, тъй като необходимостта да се следват сходни, но различни стандарти за граждански и военни клиенти, увеличава производствените разходи за разработването на продукти с двойна употреба от промишлеността.

2.1. Повишаване на киберустойчивостта на отбранителната екосистема

Повишаването на киберустойчивостта на отбранителната екосистема изисква целенасочени действия и инвестиции в широк набор от структури — от военната инфраструктура на държавите членки и мисиите и операциите по линия на ОПСО до критичната инфраструктура, отбранителната промишленост и съответните научноизследователски структури.

Защитата на информацията, която се изисква за вземането на информирани решения, е необходима за успешните мисии и операции по линия на ОПСО. ЕС и неговите държави членки трябва да укрепят още повече своите военни структури за командване и контрол и да развиват и защитават своите инфраструктури. Това важи и за политическите и военните консултации на ранните етапи от управлението на кризи за ефективното използване на щаба на операцията, включително на способностите за планиране и провеждане на военни операции (МРСС). Това ще бъде постигнато по-специално чрез по-нататъшното развитие на оперативната мрежа на ЕС за отдалечена връзка.

В контекста на военните мисии и операции участниците в киберотбраната боравят с информация в различни формати и класификации, идваща от различни източници. Поради това използването на сигурни съвременни технологии, като например изкуствения интелект, с подкрепата на сектора е от изключителна важност.

Сигурността на инфраструктурата на КИС трябва да бъде подобрена чрез прилагане на взаимно съгласувани процедури за управление, като по този начин се укрепва доверието

[23] Декларация на върховния представител от името на Европейския съюз относно злонамерени действия в киберпространството, извършвани от хакери и хакерски групи в контекста на агресията на Русия срещу Украйна https://www.consilium.europa.eu/bg/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/

в целостта на наличната информация сред заинтересованите страни. Освен това върховният представител, включително в качеството си на ръководител на Европейската агенция по отбрана, с подкрепата на Комисията, ще подпомага държавите членки при разработването на **правно необвързващи препоръки за отбранителната общност, вдъхновени от Директивата относно мерки за високо общо ниво на киберсигурност в Съюза (МИС 2)**[24], тъй като отбраната е изключена от обхвата на директивата. Това ще допринесе за повишаване на цялостната зрялост на киберотбраната.

Предложението на Комисията за законодателен акт за киберустойчивост[25], чиято цел е да се определят изисквания за киберсигурност за продукти с цифрови елементи, също ще намали допълнително повърхността, уязвима за атаки, в продукти с двойна употреба, използвани например в КИС от отбранителната промишленост и от държавни участници в отбраната. Съгласно предложението от производителите ще се изисква да докладват в срок от 24 часа на ENISA за активно експлоатирани уязвимости, като тя ще информира съответните национални CSIRT. В това отношение е важно също така да се гарантира, че отбранителната общност е информирана своевременно за уязвимостите в продукти с цифрови елементи, както и за наличните и/или прилаганите актуализации и мерки за намаляване на риска.

Поради зависимостта на военните от гражданската критична инфраструктура **е необходимо да се засили защитата на критичната инфраструктура от широкомащабни кибератаки**. По искане на Съвета[26] Комисията, върховният представител и групата за сътрудничество за МИС[27] разработват сценарии за риска относно сигурността на цифровата инфраструктура. Акцентът ще бъде на първо място върху киберсигурността в секторите на енергетиката, телекомуникациите и транспорта, както и в космическото пространство. В допълнение към това ще бъдат изготвени и целеви оценки на киберрисковете за комуникационната инфраструктура и мрежите в ЕС (включително фиксирана и мобилна инфраструктура, сателити, подводни кабели и интернет маршрутизация)[28]. Що се отнася до защитата на критичната инфраструктура от причинени от човека заплахи, включително хибридни заплахи, в предложението за препоръка на Съвета относно координиран подход на Съюза за укрепване на устойчивостта на критичната инфраструктура[29] се призовава държавите членки да осигурят, наред с другото, подходящи тестове за устойчивостта и подходяща координация при кризи. Критичната морска инфраструктура, включително защитата на подводните кабели за данни, ще бъде допълнително разгледана по време на предстоящото преразглеждане на Стратегията на ЕС за морска сигурност и нейния план за действие. Допълнителни действия за укрепване на киберсигурността на критичната

[24] Директивата относно мерки за високо общо ниво на киберсигурност в Съюза, с която се отменя Директива (ЕС) 2016/1148, наскоро беше одобрена от съзаконодателите и се очаква да бъде официално приета до края на тази година.
[25] Предложение за регламент относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020, COM/2022/454 final
[26] Заключения на Съвета относно установяването на позицията на Европейския съюз в киберпространството; ST09364/22, 23 май 2022 г.
[27] https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group
[28] Призив от Невер за укрепване на капацитета на ЕС за киберсигурност
[29] Предложение за препоръка на Съвета относно координиран подход на Съюза за укрепване на устойчивостта на критичната инфраструктура (COM/2022/551 final).

инфраструктура в енергийната система са посочени в плана за действие на ЕС за цифровизация на енергийната система[30].

Космическите услуги са от все по-голямо значение за отбраната, независимо дали става въпрос за наблюдение, ситуационна осведоменост, точно позициониране или изключително сигурна комуникация. Следователно те са ключови стратегически активи за технологичния суверенитет. Смущения в космическите услуги могат да окажат сериозно въздействие върху системите за отбрана, както и върху обществото и икономиката като цяло. Устойчивостта на тези услуги е от основно значение за цялостната устойчивост на киберотбраната, тъй като те могат да бъдат обект на злонамерени атаки. По-специално, както се видя от атаките срещу мрежите на KA-SAT, космическите системи са все по-изложени на киберзаплахи, които могат да засегнат наличността или непрекъснатостта на космическите услуги. Това създава риск за стратегическите интереси и интересите в областта на сигурността на ЕС в космическото пространство, както и за космическите способности, които дават възможност за киберотбрана и я подпомагат. Космическата стратегия на ЕС за сигурност и отбрана, обявена в Стратегическия компас[31], ще очертае мерки за повишаване на надеждността и киберустойчивостта на космическите инфраструктури и свързаните с тях услуги, както и за възпиране и реагиране на всякакви заплахи за чувствителни космически системи и услуги в ЕС, като се обърне специално внимание на киберзаплахите.

Комисията също така призовава държавите членки спешно да приложат мерките, препоръчани в инструментариума на ЕС за киберсигурност на 5G технологиите[32]. Държавите членки, които все още не са въвели ограничения за високорисковите доставчици, следва да го направят незабавно, като се има предвид, че загубеното време може да увеличи уязвимостта на мрежите в ЕС. Такива рискове могат да бъдат от значение за военните активи и да окажат въздействие върху цялостната среда в областта на отбраната на държавите членки.

Що се отнася до **киберустойчивостта на европейската отбранителна промишленост, както и на научноизследователските и развойни структури в областта на отбраната**, такива структури попадат в обхвата на Директивата за МИС 2, освен ако не са изрично изключени от държавите членки. Това ще изисква от тези структури да разполагат с програма за управление на киберриска, която включва сигурността на веригата на доставки, както и докладването на инциденти. Тъй като частният сектор играе голяма роля в предоставянето на услуги за киберсигурност в отбранителната екосистема, държавите членки следва освен това да използват схеми за сертифициране на киберсигурността. Може да се проучи възможността за създаване на **схема на ЕС за сертифициране на киберсигурността за дружества, предоставящи услуги на отбранителната промишленост**, като начин за въвеждане на хармонизирано равнище на доверие на пазара, въз основа на опита на ENISA.

[30] Цифровизация на енергийната система — план за действие на ЕС (COM/2022/552 final).

[31] Стратегически компас за сигурността и отбраната, 21 март 2022 г. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

[32] Киберсигурност на 5G мрежите — инструментариум на ЕС от мерки за смекчаване на риска | Стратегия в областта на цифровите технологии (europa.eu)

2.2. Осигуряване на оперативна съвместимост и съгласуваност на стандартите в областта на киберотбраната на ЕС

Оперативната съвместимост и общото ползване са важни изисквания, които трябва да се вземат предвид още на етапа на проектиране на способностите за киберотбрана, като се отчитат и извлечените поуки от текущи мисии и операции, определени под ръководството на Военния секретариат на Европейския съюз, с подкрепата на Европейската агенция по отбрана. Принципите, процесите и стандартите, които са договорени в рамките на федерираните мрежи за управление на мисиите (FMN)[33], следва да осигурят водещите елементи за развитието на националните способности за киберотбрана, за да се гарантира оперативната съвместимост.

Съвместните усилия може да бъдат улеснени чрез хармонизиране на изискванията за способности за киберотбрана от следващо поколение, което евентуално може да доведе до съвместни инициативи за разработване и възлагане на обществени поръчки и за интегрирана поддръжка през целия жизнен цикъл. Поради тази причина Европейската агенция по отбрана и Военният секретариат на Европейския съюз ще разработят **препоръки за набор от изисквания за оперативна съвместимост на киберотбраната на ЕС**. Тези изисквания трябва да се вземат предвид през всички периоди на планиране, за да се гарантират всички аспекти на стандартизацията като решаващ стратегически инструмент за оперативната съвместимост. Изискванията за изпитване, оценка и сертифициране са други важни стратегически инструменти.

Ще бъдат разработени хармонизирани стандарти за киберсигурност за хардуерни и софтуерни продукти и компоненти в контекста на предложения законодателен акт за киберустойчивост[34]. Тези стандарти ще се отнасят за всички граждански продукти и продукти с двойна употреба с цифрови елементи, които съставляват голяма част от продуктите, използвани в сектора на отбраната. Където е възможно, Комисията ще насърчава съгласуваност със свързаните с отбраната стандарти за киберсигурност на цифровите продукти. Както е посочено в плана за действие относно полезните взаимодействия между гражданската, отбранителната и космическата промишленост[35] („План за действие относно полезните взаимодействия“), Комисията в тясно сътрудничество с ключови заинтересовани страни ще представи план за насърчаване на използването на съществуващите хибридни стандарти в гражданската и отбранителната промишленост и за разработването на нови стандарти. Сътрудничеството следва да продължи да се развива между всички заинтересовани страни, включително европейските организации за стандартизация, Организацията на Северноатлантическия договор (НАТО) и други партньори, като за тази цел се използва по най-добрия начин Европейският комитет по стандартизация в областта на отбраната. По подобен начин, когато военните органи за стандартизация разработват нови стандарти, свързани с киберсигурността, за продукти с цифрови елементи за използване в отбраната,

[33] https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx
[34] COM(2022) 454 final.
[35] COM(2021) 70 final

хармонизираните стандарти, разработени съгласно Законодателния акт за киберустойчивост, следва да се използват като базови[36].

Действия за киберотбрана

- Подкрепа за държавите членки при разработването на незадължителни препоръки за отбранителната общност, вдъхновени от МИС 2, които да допринесат за повишаване на цялостната зрялост на киберотбраната на национално равнище.
- Разработване на препоръки относно изискванията за оперативна съвместимост на киберотбраната на ЕС.
- Засилване на сътрудничеството с всички заинтересовани страни в областта на свързаните с отбраната стандарти в рамките на Европейския комитет по стандартизация в областта на отбраната.

Действия за гражданска подкрепа

- Разработване на рискови сценарии за критична инфраструктура от значение за военната комуникация и мобилност с цел насочване на действията за готовност, включително чрез изпитване на проникването.
- Насърчаване на сътрудничеството между гражданските и военните органи по стандартизация за разработване на хармонизирани стандарти за продукти с двойна употреба.

3. Инвестиране в способности за киберотбрана

През последните години инвестициите за киберотбрана в ЕС се увеличиха на фона на нарастващите злонамерени кибернетични дейности от страна на държавни и недържавни участници. Изключително важно е ЕС да укрепи способностите си за киберотбрана. Агресивната война на Русия срещу Украйна допълнително засилва необходимостта от увеличаване на инвестициите, за да се гарантира, че държавите членки разполагат с най-съвременни способности за киберотбрана — както стационарни, така и за разгръщане.

Технологичните подобрения са от съществено значение за поддържане на предимство пред конкурентите и противниците, които също инвестират много в нови технологии. Ето защо ЕС и държавите членки трябва да засилят сътрудничеството и оперативната си съвместимост в областта на киберотбраната чрез съвместно разработване на способности и увеличаване на инвестициите в научноизследователска и развойна дейност.

[36] Понастоящем се извършва стандартизация във връзка с изискванията за киберсигурност по отношение на радио оборудването въз основа на Делегиран регламент (ЕС) 2022/30. Ако Комисията отмени или измени този делегиран регламент, вследствие на което той престане да се прилага за някои продукти, попадащи в обхвата на Законодателния акт за киберустойчивост, Комисията и европейските организации за стандартизация следва да вземат предвид стандартизацията, извършена в контекста на Решение за изпълнение C(2022)5637 на Комисията относно искането за стандартизация за горепосочения делегиран регламент, при подготовката и разработването на хармонизирани стандарти за улесняване на прилагането на Законодателния акт за киберустойчивост.

Освен това е необходимо да се обърне внимание на уязвимостите, произтичащи от стратегическите зависимости и разпокъсаността на европейската отбранителна технологична и индустриална база[37]. По-специално, уменията и правомощията са от съществено значение за преодоляване на стратегическите зависимости в областта на киберсигурността и киберотбраната в Европа. Европейската отбранителна промишленост трябва да запази ключовите си умения и да придобие нови, за да продължи да бъде в състояние да предоставя високотехнологични решения в глобален план38. Липсата на умения има отрицателно въздействие върху отбранителния сектор, тъй като възпрепятства развитието на способности във всички области. Всички действия ще бъдат в пълно съответствие с подходите, обявени в Плана за действие относно полезните взаимодействия, с Пътната карта относно критичните технологии за сигурността и отбраната („пътната карта“)[39] и с анализа на пропуските[40].

3.1. Разработване на пълен спектър от съвременни способности за киберотбрана

Държавите членки носят отговорността и имат правомощията за използването на способности за киберотбрана, докато ЕС играе важна роля за подкрепата на по-нататъшното развитие на специфични военни способности в целия спектър на доктрината, организацията, обучението, материалите, персонала, ръководството, съоръженията и оперативната съвместимост (DOTMLPF-I), за да се предостави свобода на действие в киберпространството. Необходимо е подходът към киберотбраната във всички области на способностите да се унифицира допълнително и да се адаптира към променящата се геополитическа среда. Ето защо е необходимо да се определят липсващите елементи в съществуващите способности и да се подкрепи развитието на нови способности по координиран и измерим начин.

Въпреки това степента на ангажираност на държавите членки в съвместни проекти за развитие на киберотбраната продължава да бъде недостатъчна към днешна дата и следва да се увеличи, за да се постигне максимално въздействие на равнището на ЕС. Всички държави членки трябва да увеличат инвестициите си в развитието на пълния спектър от способности за киберотбрана и да ги развиват, като си сътрудничат. Държавите членки следва да обмислят възможността за **разработване на набор от доброволни ангажименти за развиването на национални способности за киберотбрана**, както и на многонационални способности извън съществуващите проекти за киберотбрана по линия на ПСС[41]. Процесът на координиран годишен преглед на отбраната (КГПО) би

[37] Например както е посочено в анализа на дефицита на инвестиции в отбраната.

[38] Стартирани са няколко инициативи, например европейското партньорство за умения в областта на отбраната.

[39] В Пътната карта относно критичните технологии Комисията призовава за засилване на сътрудничеството в областта на технологиите, които са критични за дългосрочната сигурност и отбрана на Европа, както и на усилията за намаляване на свързаните стратегически зависимости.

[40] Съвместно съобщение относно анализа на недостига на инвестиции в отбраната и бъдещите действия, в което Комисията и върховният представител предложиха няколко мерки, за да се гарантира, че промишлеността на ЕС е подготвена за постигане на резултати както в краткосрочен, така и в дългосрочен план.

[41] Екипи за бързо реагиране при кибератаки и екипи за взаимопомощ в областта на киберсигурността (CRRT), Координационен център в областта на киберсигурността и информацията (CIDCC), Платформа

могъл да се използва за започване на диалог с държавите членки относно изискванията за киберотбрана и националните цели за развитие на способностите за киберотбрана и за оценка на изпълнението на ангажиментите. Чрез Европейския фонд за отбрана (ЕФО) Комисията подкрепя и съфинансира целия спектър от научноизследователска и развойна дейност по отношение на способностите за киберотбрана, включително по отношение на активните отбранителни способности. Комисията вече увеличи инвестициите в киберотбрана чрез ЕФО, което следва да доведе до разработването на общи и/или оперативно съвместими европейски инструменти за операции и управление на инциденти в киберпространството, за защитни операции и превантивни мерки в областта на информационната война, както и до повишаване на устойчивостта на комуникационните и информационните системи. Инвестициите са насочени към области като киберситуационна осведоменост, способности за улавяне на заплахи и реагиране в реално време, способности за кибероперации, кибернетични обучения и учения[42]. За да се гарантира, че държавите членки са в състояние да провеждат съвместни кибероперации, през следващите години по линия на ЕФО ще бъдат подпомагани способности за реагиране и кибероперации. И накрая, държавите членки се насърчават да участват активно в различните рамки за сътрудничество и да използват всички инструменти, създадени на равнището на ЕС, включително екипа на проекта за киберотбрана към Европейската агенция по отбрана[43].

Текущото преразглеждане на приоритетите за развитие на способностите на ЕС за 2018 г.[44] представлява навременна възможност за определяне на актуализирани приоритети за развитие на сътрудничеството и съвместното разработване, което от своя страна ще позволи това повишаване на способността за съвместно разработване. При преразглеждането на специфичния приоритет за киберотбрана следва да се вземат предвид резултатите от КГПО за 2022 г., както и констатациите от анализа на недостига, представен на държавите членки през май 2022 г. Впоследствие КГПО ще предлага редовна рамка за преглед на напредъка по изпълнението на този актуализиран приоритет на национално равнище и ще проучва новите възможности за съвместно разработване на способности за киберотбрана с държавите членки. Актуализираните приоритети на ЕС за развитие на способностите ще послужат като основен ориентир за проектите по линия на ПСС в областта на киберотбраната.

Във връзка с това, въз основа на задачата, възложена от Военния комитет на ЕС, Военният секретариат на ЕС ще разработи план за изпълнение на операциите в киберпространството в тясна координация с държавите членки, за да осигури преглед на актуалното състояние на прилагането на способностите за киберотбрана, както и да

за обмен на информация относно киберзаплахи и реагиране при инциденти (CTIRISP), федериране на киберполигони (CRF), Център на ЕС за академично и иновационно сътрудничество в кибернетичната област (EU CAIH).

[42] В рамките на Европейската програма за промишлено развитие в областта на отбраната (EDIDP) са финансирани 6 проекта (PANDORA, DISCRETION, CYBER4DE, ECYSAP, SMOTANET и HERMES) с бюджет от 39 милиона евро. В рамките на ЕФО за 2021 г ще бъдат отделени почти 40 милиона евро за 3 съвместни проекта за НИРД в областта на киберотбраната, избрани за финансиране (ACTING, AInception, EU-GUARDIAN).

[43] Екипът на проекта за киберотбрана предоставя на държавите членки форум за обсъждане на въпроси, свързани с киберотбраната, с военни последици.

[44] EDA CDP factsheet [Информационна справка на Европейската агенция по отбрана за ПРС] (28.6.2018 г.): CDP Factsheet [Информационна справка за ПРС]

предостави подкрепа на държавите членки за по-добро съгласуване на техните усилия и дейности. Тези усилия се основават на концепцията на ЕС за киберотбрана за ръководените от ЕС военни операции и мисии, която отразява приоритетите на Плана за развитие на способностите (ПРС).

Повишаване на научноизследователските усилия в областта на ключови технологии за киберотбрана

Поддържането на съвременни способности за киберотбрана изисква да сме в крак с технологичното развитие и неговите приложения в системите, свързани с отбраната, и по-специално с нововъзникващите и революционни технологии (EDT, напр. изкуствен интелект, криптиране и квантови изчислителни технологии)[45]. По-специално, ЕС трябва да инвестира в постквантова криптография, за да гарантира, че отбранителните му системи ще продължат да бъдат сигурни. Предвид бързите темпове на развитие на технологиите, съвместните усилия в областта на научните изследвания и технологичното развитие трябва да бъдат адаптирани така, че да достигнат достатъчно високо равнище на технологична готовност, за да може резултатите от тях да бъдат по-бързо включени в съществуващите и бъдещите способности.

В рамките на ЕФО Комисията финансира технологични иновации в областта на отбраната и подкрепя развитието на нововъзникващи и революционни технологии, както и на авангардни технологии, включително за киберотбрана. До 8 % от бюджета на ЕФО се отпускат за теми, свързани с революционни технологии за отбрана, включително някои теми, свързани с киберотбраната. Специално внимание в рамките на ЕФО през следващите години ще бъде отделено на научноизследователски дейности и проекти, насочени към нови технологии, разработени срещу нововъзникващи и променящи се заплахи, както и за повишаване на устойчивостта, киберсигурността и тяхното интегриране в способностите за отбрана.

В съответствие с плана за действие за нововъзникващи и революционни технологии[46] Европейската агенция по отбрана ежегодно ще информира държавите членки за състоянието на нововъзникващите технологии, включително тези, които могат да се прилагат за киберотбрана. Освен това Европейската агенция по отбрана ще разработи европейска стратегическа оценка за нововъзникващи и революционни технологии, за да подпомогне държавите членки при определянето на дългосрочни стратегически насоки, полезни взаимодействия и възможности за сътрудничество. Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността ще приеме стратегическа програма за инвестиции в ключови области на киберсигурността, която от своя страна ще насочва подготовката на бъдещите работни програми на програмите „Цифрова Европа“ и „Хоризонт Европа“ във връзка с киберсигурността, съответно в подкрепа на научните изследвания, иновациите и пазарното внедряване. За да се насърчат полезните взаимодействия, Европейският център за промишлени, технологични и изследователски експертни познания в областта

[45] Както е посочено в програмата за стратегически научни изследвания в областта на киберотбраната и във всеобхватната стратегическа изследователска програма.

[46] Управителния съвет на Европейската агенция по отбрана, който се състои от директори по научни изследвания и технологии, одобри на 16 декември 2021 г. „Нововъзникващи и революционни технологии: План за действие на основата на способностите“.

на киберсигурността и Европейската агенция по отбрана ще изготвят също така работно споразумение за улесняване на обмена на информация между съответните служители относно приоритетите в областта на гражданските технологии, технологиите с двойна употреба и отбранителните технологии.

Действия по отношение на технологичните нужди за киберотбрана

Необходими са по-нататъшни действия и координация, за да се гарантира, че бързите технологични развития в киберпространството се възприемат бързо от сектора на отбраната. Това включва активизиране на усилията за идентифициране на критични технологии за киберотбрана и киберсигурност, които следва да бъдат приоритизирани, за да се намалят технологичните зависимости на ЕС и да се направи оценка дали настоящите инструменти за определяне на приоритети и финансиране са насочени в достатъчна степен към тези зависимости.

За тази цел през 2023 г. Комисията, заедно с Европейската агенция по отбрана и държавите членки, ще предложи **технологична пътна карта за критични кибертехнологии** въз основа на съответните консултации, включително с промишлеността, когато е целесъобразно. В пътната карта за технологиите ще бъдат набелязани кибертехнологиите, които са важни за технологичния суверенитет на ЕС, ще бъдат обхванати както киберотбраната, така и киберсигурността, ще бъдат набелязани технологичните разработки и стратегическите зависимости и ще бъдат предприети действия за тяхното намаляване. Пътната карта за кибертехнологиите ще даде информация за стратегическите приоритети на инструментите за финансиране на ЕС и ще предложи пълноценно използване на програмите и инструментите за финансиране в областта на научните изследвания и развойната дейност и развитието на способностите в гражданската и отбранителната сфера в съответствие със съответните им правила за управление. В нея ще се предложат и допълнителни начини за насърчаване на развитието на научните изследвания, технологичното развитие и иновациите с двойна употреба в областта на киберсигурността и киберотбраната на равнището на ЕС и на държавите членки.

Във връзка с това през 2023 г. Комисията[47], в сътрудничество с Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Европейската агенция по отбрана, ще направи оценка на технологиите, които вече са определени като критични за киберотбраната, и евентуално, с подкрепата на Обсерваторията за критични технологии, ще картографира и определи съществуващите зависимости по-нататък[48]. При това ще бъде взета предвид работата, извършена в контекста на годишния мониторингов документ на Европейската агенция по отбрана[49] и стратегическата оценка на европейските нововъзникващи и революционни технологии[50]. Освен това Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността

[47] Включително Съвместния изследователски център.
[48] Обсерватория за критични технологии, обявена в плана за действие относно полезните взаимодействия между гражданската, отбранителната и космическата промишленост.
[49] Първа фаза на плана за действие относно нововъзникващите и революционните технологии за 2021 г. на Европейската агенция по отбрана.
[50] Втора фаза на плана за действие относно нововъзникващите и революционните технологии за 2021 г. на Европейската агенция по отбрана.

може да стартира специален проект за подкрепа на политиката, който да се включи в процеса на изготвяне на пътна карта за технологиите и да събере и ангажира съответните заинтересовани страни от гражданската и военната сфера.

Като част от дейностите, очертани в плана за действие относно полезните взаимодействия, в пътната карта и в анализа на недостига, вече се провеждат няколко действия за укрепване на полезните взаимодействия, за да се използва по-добре пълният потенциал на технологиите с двойна употреба, включително в киберпространството.

Освен това държавите членки се насърчават да използват пълноценно съществуващите инициативи в подкрепа на научните изследвания и технологичното развитие, а именно за отбраната — технологичните групи за отбранителни способности на Европейската агенция по отбрана[51] и всеобхватната стратегическа изследователска програма и нейните технологични градивни елементи[52], *ad hoc* рамката на Европейската агенция по отбрана[53], ЕФО и ПСС. По отношение на гражданските технологии и технологиите с двойна употреба Европейският център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и мрежата могат да управляват проекти както с отбранително, така и с гражданско измерение, както е установено в неговото правно основание[54]. Както е обявено в плана за действие относно полезните взаимодействия и пътната карта, Комисията ще се стреми също така да засили полезните взаимодействия в дейностите по киберсигурност и киберотбрана на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на ЕФО в съответствие с правилата за управление на ЕФО.

3.2. Гъвкава, конкурентоспособна и иновативна европейска отбранителна промишленост

ЕС се нуждае от силна, гъвкава, конкурентоспособна и иновативна европейска отбранителна промишленост, която да е в състояние да предостави пълния спектър от най-съвременни отбранителни способности, включително способности за киберотбрана. Въпреки това, що се отнася до киберотбрана, отбранителната промишленост на ЕС

[51] CapTechs предоставят на експертите от държавите членки форуми за работа в мрежа и гъвкава рамка за съвместни проекти. Повече информация за CapTechs, свързана с киберпространството (киберпространство, информация, компоненти), можете да намерите на: https://eda.europa.eu/what-we-do/research-technology/capability-technology-areas-(captechs).

[52] Във всеобхватната стратегическа изследователска програма се картографират съответните научни изследвания и технологии в областта на отбраната и се предоставят конкретни възможности за сътрудничество. Съществуват 17 технологични градивни елемента, заедно с техните технологични пътни карти, свързани с кибертехнологиите, които се отнасят до ситуационната осведоменост в областта на киберотбраната, защитата на военните комуникационни системи, обработката на информация от хетерогенни източници, моделирането и симулацията, квантовите изчислителни технологии и криптографията, както и до проучването на полезните взаимодействия между кибероперациите и електронната война. Изкуственият интелект и големите данни играят ключова роля в обработката на информация.

[53] *Ad hoc* рамката на Европейската агенция по отбрана е определена с Решение (ОВППС) 2015/1835 на Съвета. Понастоящем в тази рамка се изпълняват 6 проекта с елементи на кибертехнологии с бюджет от около 20 милиона евро (ANQUOR, CERERE, EDA SOC 2, MASFAD II, PASEI II, ASSAI).

[54] Регламент (ЕС) 2021/887 на Европейския парламент и на Съвета от 20 май 2021 г. за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове.

понастоящем разчита в значителна степен на граждански решения и на външни пазари, за да осигури най-съвременни решения. Въпреки че технологичният напредък в гражданската сфера е бърз и пазарът на граждански продукти за информация и киберсигурност расте бързо, има специфични военни изисквания, които не се изпълняват от готовите граждански продукти. Важни части от хардуера и софтуера, които понастоящем се използват за киберотбрана, не се произвеждат в ЕС, което може да доведе до промишлени и технологични зависимости. Също така ЕС няма силно присъствие в световната отбранителна промишленост за киберсигурност и киберотбрана. Силно фрагментираната **европейска отбранителна технологична и индустриална база (ЕОТИБ)** на ЕС значително намалява способността му да подобрява своята конкурентоспособност[55], като по-голямата част от дружествата за киберсигурност в ЕС са малки и средни предприятия (МСП)[56]. Наличието на технологично независим промишлен капацитет е крайъгълен камък за способността на ЕС да действа.

ЕС подкрепя развитието на силна ЕОТИБ чрез редица програми и инициативи. Като се има предвид, че ЕФО финансира технологични иновации за отбрана и подкрепя разработването на технологии, което в крайна сметка води до съвместно разработване на авангардни военни способности и допринася за конкурентоспособността на отбранителната промишленост на ЕС, рамковата програма за научни изследвания и иновации „Хоризонт Европа“ и програма „Цифрова Европа“ подкрепят научните изследвания в областта на киберсигурността и разработването на технологии с двойна употреба, включително квантови технологии, криптиране, защитени изчислителни облаци и изкуствен интелект[57].

Следва да бъдат разгледани по-нататъшни действия, свързани с критичните технологии за киберотбрана и промишлени нужди, както е установено в **технологичната пътна карта за критични кибертехнологии**. Необходимо е да се определят подходящи потоци на подкрепа, например за стимулиране на усилията за възлагане на съвместни обществени поръчки, например чрез бъдещата Европейска инвестиционна програма в областта на отбраната, или за улесняване на достъпа до собствен капитал и заеми чрез Европейския инвестиционен фонд и Европейската инвестиционна банка.

За да се създаде силна ЕОТИБ, трябва да се гарантират използването и оползотворяването на полезни взаимодействия между гражданските дружества и дружествата в областта на отбраната. Иновативните действия, предложени в рамките на иновационната схема на ЕС в областта на отбраната, включително работата с МСП и проучването на технологии, биха могли да имат положително въздействие върху отбранителната промишленост на ЕС и ЕОТИБ.

[55] Както е посочено в съвместното съобщение относно анализа на недостига на инвестиции в отбраната и бъдещите действия.

[56] Общият брой на МСП в ЕС, работещи в многопластови и често трансгранични вериги на доставки в областта на отбраната, възлиза на 2500. Те обслужват клиенти в областта на отбраната, като 7,8 % от дейността им е свързана с киберпространството.

[57] В рамковата програма „Хоризонт Европа“ се предвижда полезните взаимодействия с ЕФО да бъдат от полза за гражданските научни изследвания и научните изследвания в областта на отбраната, въпреки че дейностите по рамковата програма ще бъдат съсредоточени изключително върху гражданските приложения.

Комисията също така ще започне диалог с промишлеността с цел развитие на промишлеността за киберотбрана в ЕС, като включи, ако е необходимо, Европейската агенция по отбрана.

Комисията и върховният представител предлагат да се въведат няколко мерки, за да се гарантира, че промишлеността е подготвена да постигне резултати в краткосрочен и дългосрочен план. В краткосрочен план това включва задълбочено картографиране на промишлените производствени способности на ЕС в областта на отбраната, за да се установят точно пропуските и областите, в които е необходимо да се увеличат способностите.

Намаляването на критичните зависимости в сферата на киберпространството, които могат да бъдат установени в технологичните пътни карти, би могло да бъде разгледано и от новия Европейски фонд за суверенитет, обявен от председателя Фон дер Лайен в нейната реч за състоянието на Съюза през септември 2022 г.

Рамката на ЕС за скрининг на преките чуждестранни инвестиции ще продължи да се използва за намаляване на рисковете от придобиване на европейски технологии или решения, които крият рискове в областта на отбраната и сигурността. Държавите членки, които все още не са създали национални механизми за скрининг, следва да го направят незабавно.

3.3. Работна сила на ЕС в областта на киберотбраната

Европа е изправена пред реален и тревожен недостиг на кибернетични умения, като Европейската организация за киберсигурност (ECSO) изчислява, че през 2022 г. вече ще са необходими общо 500 000 специалисти. Този недостиг на умения възпрепятства ЕС да разработва нови технологии и да защитава критичната си инфраструктура. За държавните структури, като например министерствата на отбраната и армията, ожесточената конкуренция за умения и атрактивните заплати, предлагани от частния сектор, допълнително засилват трудностите при привличането и задържането на квалифицирани киберспециалисти.

В контекста на Европейската година на уменията (2023 г.) **Комисията ще стартира инициатива за създаване на академия за кибернетични умения.** Академията ще действа като обща инициатива с цел увеличаване на броя на специалистите, обучени в областта на киберсигурността. Тя ще обедини многобройните различни инициативи в областта на кибернетичните умения и ще осигури координация, интеграция и обща комуникация по тях. Академията за кибернетични умения, организирана около няколко стълба на действие, като финансиране, подпомагане от общността, обучение и сертифициране, участие на заинтересовани страни и генериране на знания, ще може да бъде от полза и за работната сила в областта на киберотбраната. Европейският колеж по сигурност и отбрана (ЕКСО) ще проучи как да се улесни обменът на най-добри практики и по-нататъшни полезни взаимодействия между военната и гражданската сфера по отношение на обучението и развитието на специфични за киберпространството военни умения.

Въз основа на анализ на изискванията за обучение в ЕС, както и на нуждите от обучение, ЕКСО, Европейската агенция по отбрана и държавите членки ще продължат да разработват и организират дейности за обучение и учения по киберотбрана за

институциите на ЕС, операциите и мисиите по линия на ОПСО и длъжностни лица на държавите членки. Ще бъде проучено и по-нататъшното **развитие на платформата на ЕКСО за киберобразование, обучение, учения и оценка (ETEE)**, за да се създаде по-голям капацитет за обучение. Това следва да включва и курсове за обучение за конкретна оперативна област и операции в няколко области. По-специално следва да се търсят полезни взаимодействия с проекта по линия на ППС за Център на ЕС за академично и иновационно сътрудничество в кибернетичната област (EU CAIH) [58].

Държавите членки се насърчават да разработват специални образователни програми в областта на киберотбраната, като привличат висши училища и академични институции (граждански и военни) за разработване и създаване на общи учебни програми по киберотбрана, обмен на най-добри практики, създаване на партньорства и общи проекти и улесняване на обмена на обучители и обучаеми. За да осигури оперативна съвместимост и обща култура в ЕС, ЕКСО ще насърчава обмена между държавите членки чрез ETEE.

Държавите членки следва да засилят по-широкото сътрудничество между участниците в обучението и образованието, като съчетаят граждански и военни аспекти в техническата, оперативната, стратегическата и правната област и поставят основата за създаване на общи и стандартизирани програми за обучение на различни равнища за гражданските, правоприлагащите, дипломатическите общности и общностите за киберотбрана. Освен това държавите членки следва да си сътрудничат с европейски доставчици на обучение от частния сектор, както и с академични институции, за да повишат равнището на компетентност и умения на персонала във военните мисии и операции по линия на ОПСО.

Също така е необходимо да се насърчава сътрудничеството в областта на стандартите за обучение и сертифициране в сферата на киберотбраната между държавите членки, институциите, органите и агенциите на ЕС , международните партньори и другите участници, включително от частния сектор и академичните среди. Въз основа на съществуващите граждански инициативи, като например Европейската рамка за умения в областта на киберсигурността (ECSF), разработена от ENISA, ЕКСО ще разработи рамка за сертифициране на уменията в областта на киберотбраната. Комисията също така ще разгледа подходи за сертифициране на кибернетични умения, които са налични на пазара и в академичните среди, като същевременно ще се стреми да стимулира чрез Академията за кибернетични умения полезните взаимодействия между тези подходи и запълването на пропуските, по-специално с целево финансиране от ЕС.

Действия за киберотбрана

- Разработване на стратегическата оценка за нововъзникващи и революционни технологии в подкрепа на дългосрочни стратегически инвестиционни решения.
- Разработване на технологична пътна карта за критични кибертехнологии за ЕС, обхващаща критични технологии за киберотбрана и киберсигурност, за да се оцени равнището на зависимости.

[58] https://www.pesco.europa.eu/project/eu-cyber-academia-and-innovation-hub-eu-caih/

- Предлагане на начини за намаляване на зависимостите, като се използват всички инструменти на ЕС, включително „Цифрова Европа“, „Хоризонт Европа“ и ЕФО, и предвиждане на технологичното развитие, за да се повиши технологичният суверенитет и да се осигури възможност за действие.
- Подкрепа за разработването на рамка за сертифициране на уменията в областта на киберотбраната.
- Разработване на учения за киберотбрана на ЕС и проучване на начините за по-нататъшно развитие на платформата на ЕКСО за образование, обучение, учения и оценка в областта на киберсигурността с цел създаване на по-голям капацитет за обучение.

Действия за гражданска подкрепа

- Създаване на академия на ЕС за кибернетични умения, като се отчитат нуждите от специфични умения за различните професионални профили и сектори на дейност, включително за работната сила в областта на отбраната.
- Анализиране на подходи за сертифициране на кибернетичните умения, като стремежът е да се насърчават полезните взаимодействия и да се запълват пропуските, включително чрез финансиране от ЕС.

4. Партньорство за справяне с общите предизвикателства

Партньорите ще се възползват от един по-способен и устойчив ЕС в киберпространството, както и от помощта на ЕС за киберотбрана и изграждането на капацитет, предоставяни чрез съответните инструменти на ЕС. ЕС ще се стреми да установява специално пригодени партньорства в областта на киберотбраната, когато те са взаимноизгодни. Партньорствата в областта на киберотбраната ще бъдат разгледани и в контекста на участието на държавите партньори във военни мисии и операции по линия на ОПСО.

Когато е уместно, тази работа ще се основава на съществуващите кибердиалози, както и на диалози в областта на сигурността и отбраната. Върховният представител ще проучи също така полезните взаимодействия между **неформалната мрежа на ЕС за кибердипломация и мрежата на аташетата по отбраната в делегациите на Съюза.**

4.1. Сътрудничество с НАТО

Стратегическото партньорство на ЕС с НАТО продължава да бъде от съществено значение за евроатлантическата сигурност, както е подчертано в Стратегическия компас и Стратегическата концепция на НАТО за 2022 г.[59] ЕС продължава да бъде изцяло ангажиран с укрепването на това ключово партньорство, включително в областта на киберотбраната, и трябва да се предприемат допълнителни стъпки за разработване на съвместни решения по отношение на общите заплахи и предизвикателства. В съответствие със съвместните декларации от Варшава и Брюксел относно

[59] https://www.nato.int/strategic-concept/

сътрудничеството между ЕС и НАТО[60] и въз основа на принципите на прозрачност, реципрочност и приобщаване, откритост и автономност при вземането на решения от двете организации, киберсигурността и киберотбраната представляват ключови приоритетни области на ЕС за сътрудничество.

На основата на реципрочност ЕС ще продължи да обменя с НАТО информация относно военната концептуална рамка, свързана с интегрирането на аспектите на киберотбраната в планирането и провеждането на военни мисии и операции по линия на ОПСО. ЕС ще се стреми към съвместимост с концепциите и доктрините на НАТО в областта на киберотбраната във възможно най-голяма степен.

Във връзка с голямото търсене на способности за киберотбрана ЕС ще насърчава полезните взаимодействия и взаимното допълване с НАТО отвъд организационните ограничения и националните граници. ЕС ще си партнира с НАТО за укрепване на техническата и процедурната оперативна съвместимост на способностите за киберотбрана, включително за разработване на способности в съответствие с инициативата FMN. Това ще проправи пътя за потенциално взаимно подкрепящо се развиване и използване на способности за киберотбрана. Специално внимание следва да се обърне на оперативната съвместимост на стандартите, които допринасят за киберустойчивостта и оперативната съвместимост на военните комуникационни и информационни системи, като се включва промишлеността, когато е уместно.

За да се осигури съгласувано обучение на съответния персонал по киберотбрана, когато е приложимо, ЕС също така ще засили сътрудничеството си с НАТО за хармонизиране на нуждите от обучение и анализ на изискванията, разработване на съвместни учебни програми, курсове и учения. Въз основа на принципите на реципрочност и недискриминация ЕКСО ще отвори своите курсове за обучение по киберотбрана за служители на НАТО и ще създаде платформа за обявяване на общи курсове. ЕС също така ще насърчава участието на служители на НАТО в учения в областта на киберсигурността и учения за управление на кризи с кибернетични елементи.

ЕС и НАТО ще се ангажират и с по-нататъшното подобряване на взаимната ситуационна осведоменост и ще проучват възможности за координация, включително чрез засилване на сътрудничеството между екипа на НАТО за реагиране при компютърни инциденти (NCIRC) и CERT-EU. За да се насърчи сътрудничеството по отношение на кибернетичните аспекти и последици от управлението и реагирането при кризи, ЕС ще допринесе за обмена между щабовете по военни, граждански и общи инициативи и, когато е приложимо, за разработването на потенциални полезни взаимодействия на съответните рамки и инициативи за управление на кризи, включително в случай на мащабни инциденти. За да се гарантира взаимното допълване и да се избегне ненужното дублиране на усилията, ЕС ще се стреми към засилено сътрудничество и обмен на информация с НАТО относно усилията за изграждане на капацитет в областта на киберотбраната в държави партньори.

4.2. Сътрудничество с единомислещи партньори

[60] Подписани съответно през 2016 г. и 2018 г.

Върховният представител ще включва по-систематично въпроси, свързани с киберотбраната, в съществуващите и бъдещите кибердиалози, както и в диалозите относно сигурността и отбраната с партньорите. Тъй като аспектите на киберотбраната ще се развиват в двустранни диалози, ще има все по-голям потенциал за включване на въпроси, свързани с киберотбраната в други форми на сътрудничество с партньорите на ЕС.

Със стратегическото партньорство на ЕС със **Съединените щати** ще продължи да се задълбочава сътрудничеството в областта на сигурността и отбраната по взаимноизгоден начин, включително чрез структуриран обмен на информация за ситуационната осведоменост. Редовните кибердиалози между ЕС и САЩ и диалозите между ЕС и САЩ в областта на сигурността и отбраната потвърждават силното трансатлантическо партньорство. Върховният представител ще включва съответните аспекти на киберотбраната в тези диалози, когато е целесъобразно.

Заедно със своите международните партньори ЕС ще продължи да подкрепя **Украйна**, включително чрез кибердиалог. С оглед на опита на Украйна в изграждането на капацитет за киберустойчивост и киберотбрана обменът на най-добри практики в областта на киберотбраната, включително по отношение на информация относно картината на заплахите и ситуационната осведоменост, както и на съответните промени в политиката, които са от общ интерес, ще продължи и ще се разшири.

Единомислещите партньори играят важна роля за поддържането на глобално, отворено, стабилно и сигурно киберпространство и могат да допълнят способността на ЕС да предотвратява, обезкуражава, възпира и реагира на злонамерено поведение в киберпространството. ЕС остава отворен за широк, амбициозен и взаимноизгоден ангажимент в областта на сигурността и отбраната, включително киберотбраната, с всички единомислещи партньори.

4.3. Подкрепа за изграждане на капацитет за киберотбрана за държавите партньори

Глобалните и регионалните предизвикателства увеличиха взаимозависимостта на ЕС и неговите партньори и подчертаха необходимостта от установяване на по-тесни партньорства в областта на сигурността и отбраната. Това е особено важно за държавите — кандидатки за членство в ЕС. Неотдавнашните широкомащабни кибератаки показват необходимостта от засилен ангажимент и партньорство на ЕС в областта на киберсигурността и киберотбраната, като се надграждат съществуващите програми. Поради транснационалния характер на киберзаплахите повишаването на киберустойчивостта на държавите партньори, особено на тези с по-ниско равнище на кибернетична зрялост, ще допринесе за по-безопасно и по-сигурно киберпространство. По този начин ЕС ще може по-добре да предотвратява, открива, и възпира кибератаки и да се защитава срещу тях. ЕС ще засили сътрудничеството в областта на сигурността и отбраната с държавите партньори, за да укрепи тяхната киберустойчивост, включително чрез съществуващите диалози. Когато е приложимо и взаимноизгодно, ЕС ще се ангажира с партньори, и по-специално с онези държави — кандидатки за членство в ЕС, чиито усилия за изграждане на капацитет за киберотбрана са в съответствие с общата външна политика и политика за сигурност, както и с общата политика за сигурност и отбрана на ЕС. Това може да включва подкрепа за рамката на политиката и

законодателната рамка, за обучение, консултиране, наставничество и за оборудване на въоръжените сили и силите за сигурност на партньорите. Държавите членки биха могли да решат да предоставят оперативна помощ за киберотбрана на партньорите си. Освен това ЕС ще помогне на партньорите да укрепят капацитета си, за да допринасят за военните мисии и операции по линия на ОПСО, тъй като това е ценен принос към взаимните усилия за насърчаване на мира и сигурността.

Усилията на ЕС за изграждане на способности за отбрана, включително за киберотбрана, в държавите партньори, по-специално в съседните на ЕС държави, ще продължават да бъдат подпомагани от Европейския механизъм за подкрепа на мира, който допълва усилията за управление на кризи в рамките на ОПСО. В тази връзка, когато е необходимо, ЕС ще обвърже по-добре помощта за киберотбрана с изграждането на граждански капацитет за киберсигурност, по-специално чрез Съвета на ЕС за изграждане на киберкапацитет. За успеха на действията за изграждане на капацитет в областта на киберотбраната и киберсигурността ще е необходима ефективна координация между съответните програми и инструменти на ЕС, включително Европейския механизъм за подкрепа на мира, и държавите членки.

Оказвайки подкрепа на държавите партньори в усилията им за изграждане на капацитет за киберотбрана, ЕС ще работи в тясно сътрудничество с други донори за разработване на платформи за ситуационна осведоменост и координация, за да се предостави възможно най-добрата персонализирана подкрепа, да се постигне съгласуваност и да не се допусне дублиране на усилията.

Действия за киберотбрана

- Засилване на сътрудничеството между ЕС и НАТО в сферата на обучението, образованието, ситуационната осведоменост и ученията в областта на киберотбраната.
- Включване на теми от сферата на киберотбраната в ръководените от ЕС кибердиалози, както и в диалозите относно сигурността и отбраната с държавите партньори.
- Сътрудничество с единомислещи държави, включително в контекста на развитието на способностите за киберотбрана и киберустойчивостта.
- Увеличаване на помощта за партньорите за развитието на способности за киберотбрана, включително чрез Европейския механизъм за подкрепа на мира, по-специално в съседните на ЕС държави, и в подкрепа на държавите — кандидатки за членство в ЕС.

Действия за гражданска подкрепа

- Засилване на сътрудничеството между ЕС и НАТО в областта на киберсигурността по отношение на ситуационната осведоменост, реакцията при кризи, защитата на критичната инфраструктура и стандартизацията и сертифицирането.

III. ЗАКЛЮЧЕНИЕ

Върховният представител, включително в качеството си на ръководител на Европейската агенция по отбрана, и Комисията призовават държавите членки да разработят съответните аспекти на настоящата политика за киберотбрана, като си сътрудничат с държавите членки за набелязване на практически мерки за изпълнение. В сътрудничество с държавите членки би могъл да бъде изготвен план за изпълнение. Резултатите от изпълнението на политиката на ЕС за киберотбрана ще допринесат за постигането на общите цели на Стратегията на ЕС за киберсигурност за цифровото десетилетие и на Стратегическия компас.

На Съвета ще бъде представен годишен доклад за мониторинг и оценка на напредъка по изпълнението на политиката за киберотбрана. Държавите членки се насърчават да дадат своя принос за напредъка по мерките за изпълнение, осъществявани на национално равнище или под формата на сътрудничество.