Съвет на
Европейския съюз

Брюксел, 22 май 2023 г.
(OR. en)

9618/23

COPS 269	**JAI 656**
POLMIL 123	**RELEX 639**
CYBER 130	**JAIEX 22**
HYBRID 31	**TELECOM 154**
EUMC 230	**IPCR 38**
CIVCOM 144	**PROCIV 35**
COPEN 162	**COTER 101**
COSI 103	**DISINFO 34**
DATAPROTECT 146	**CSC 252**
IND 256	**CSDP/PSDC 402**
RECH 191	**CFSP/PESC 748**

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
До:	Делегациите
№ предх. док.:	ST 9124/23 COPS 224 POLMIL 104 CYBER 113 HYBRID 20 EUMC 210 CIVCOM 111 COPEN 138 COSI 86 DATAPROTECT 129 IND 232 RECH 173 JAI 574 RELEX 563 JAIEX 16 TELECOM 135 IPCR 31 PROCIV 25 COTER 86 DISINFO 28 CSC 216 CSDP/PSDC 349 CFSP/PESC 674
Относно:	Заключения на Съвета относно политиката на ЕС за киберотбрана

Приложено се изпращат на делегациите заключенията на Съвета относно политиката на ЕС за киберотбрана, одобрени от Съвета на заседанието му от 22 май 2023 г.

Заключения на Съвета относно политиката на ЕС за киберотбрана

1. Въз основа на политическата рамка за кибернетична отбрана от 2014 г. и актуализацията ѝ през 2018 г. Съветът приветства амбициозното съвместно съобщение относно политиката на ЕС за киберотбрана, което има за цел увеличаване на инвестициите в нашите модерни и оперативно съвместими въоръжени сили, авангардни технологии, съвременни способности за киберотбрана и укрепване на партньорствата за справяне с общите предизвикателства. В условията на нарастваща зависимост от цифровите технологии киберпространството се превърна в област на стратегическа конкуренция. Ето защо е от съществено значение да се поддържа отворено, свободно, стабилно и сигурно киберпространство. Използването на кибероперации, които подпомогнаха и съпътстваха непредизвиканата и неоправдана агресивна война на Русия срещу Украйна, засяга глобалната стабилност и сигурност, представлява значителен риск от ескалация и допринася за вече значителното увеличаване на злонамерените действия в киберпространството извън контекста на въоръжен конфликт през последните години.

2. Войната в Украйна предостави нов стратегически контекст и потвърди необходимостта ЕС, неговите държави членки и техните партньори допълнително да укрепят устойчивостта на ЕС срещу киберзаплахи и да повишат общата ни киберсигурност и киберотбрана срещу злонамерено поведение и актове на агресия в киберпространството. Съвместното съобщение относно политиката на ЕС за киберотбрана показва решимостта ни да осигурим незабавни и дългосрочни мерки, с които да гарантираме свобода на действията в киберпространството и ответни действия срещу участниците в заплахи, които се стремят, наред с другото, към намеса в мрежите и информационните системи на ЕС и неговите партньори или към тяхното нарушаване или унищожаване. В допълнение към Стратегията на ЕС за киберсигурност и в съответствие със Стратегическия компас въпросното съвместно съобщение представлява значителна стъпка към цялостния подход на ЕС за устойчивост, реакция, предотвратяване на конфликти, сътрудничество и стабилност в киберпространството. В този контекст Съветът подчертава необходимостта от подходящи и съгласувани ответни мерки от страна на ЕС, неговите държави членки и техните партньори, като очаква и преразглеждането на насоките за прилагане на инструментариума на ЕС за кибердипломация като друга ключова стъпка напред в развитието на позицията на ЕС в киберпространството.

3. Съветът изтъква, че неотдавнашните кибератаки срещу европейската критична инфраструктура, бързо изменящата се обстановка на киберзаплахи и бързият темп на технологично развитие също показват необходимостта от засилено гражданско-военно координиране и сътрудничество, като същевременно подчертава, че няма йерархия между гражданските и военните общности.
Политиката на ЕС за киберотбрана дава възможност на ЕС и неговите държави членки да засилят способността си да защитават, откриват, отбраняват и възпират, като използват по подходящ начин целия набор от отбранителни възможности, с които разполагат гражданските и военните общности, за по-широката сигурност и отбрана на ЕС, в съответствие с международното право, включително правото в областта на правата на човека и международното хуманитарно право.

4. Въпреки че националната сигурност, включително в киберсферата, продължава да бъде отговорност единствено на всяка държава членка, както е посочено в член 4, параграф 2 от ДЕС, Съветът същевременно подчертава необходимостта от значителни индивидуални и съвместни инвестиции в повишена устойчивост и разгръщане на пълен спектър отбранителни способности за киберотбрана, както и от оползотворяване на рамките на ЕС за сътрудничество и неговите финансови стимули. Съветът изтъква необходимостта от по-нататъшно укрепване на действията на държавите членки и институциите, органите и агенциите на ЕС с цел защита на Съюза, нашите граждани, институциите, органите и агенциите на ЕС и мисиите и операциите по линия на ОПСО в киберпространството. Освен това той подчертава значението на устойчивостта на ЕС в киберпространството чрез развиване на способности за киберотбрана и засилване на сътрудничеството с надеждна частна екосистема.

I. **Да действаме заедно за по-силна киберотбрана**

5. Съветът изтъква отново, че постепенният, прозрачен и приобщаващ процес е от съществено значение за повишаване на доверието, което е от решаващо значение за по-нататъшното разработване на рамка на ЕС за управление на кризи в областта на киберсигурността, което трябва да се осъществи в съответствие с разработената в Съвета пътна карта за управление на киберкризи. Съветът изтъква отново нуждата да се продължи укрепването на нашата способност за защита, откриване, отбрана и възпиране на кибератаки посредством подобряване на ситуационната осведоменост, изграждане на капацитет, развитие на способностите, обучение, учения, повишена устойчивост и чрез решителен отпор на кибератаки срещу Съюза, неговите държави членки институции, органи и агенции,
мисии и операции по линия на ОПСО, като се използват всички подходящи средства. Същевременно Съветът насърчава върховния представител и Комисията към намаляване на сложността в областта на киберпространството, избягване на ненужното дублиране и осигуряване на сътрудничество и полезни взаимодействия със съществуващи инициативи. Необходимо е да се засилят сътрудничеството и координацията между участниците от ЕС и държавите членки в областта на киберотбраната на равнище ЕС и на национално равнище, между военните и гражданските киберобщности и между публичната сфера и надеждна частна екосистема. В този контекст
Държавите членки се насърчават да продължат да проучват и укрепват националните гражданско-военни механизми за координация, да улесняват общия доброволен обмен на информация, да споделят извлечените поуки, да допринасят за разработването на оперативно съвместими стандарти и да извършват оценки на риска и да изготвят сценарии за риска, както и да провеждат съвместни учения, особено на европейско равнище, при пълно спазване на разпоредбите на Директивата относно мерки за високо общо ниво на киберсигурност в Съюза (МИС 2).

6. Като отчита усилията за по-нататъшно повишаване на устойчивостта на Съюза посредством МИС 2 и Директивата относно устойчивостта на критичните субекти, Съветът изтъква отново препоръката си за координиран подход на равнище ЕС за укрепване на устойчивостта на критичната инфраструктура[1]. В нея се призовава за мерки за допълнително повишаване на устойчивостта на критичните субекти, инфраструктура, цифрови продукти и услуги, като същевременно се отбелязва, че правилното прилагане на МИС 2 продължава да бъде най-важната стъпка. Въпреки че тези мерки са предимно отговорност на гражданския сектор, те допринасят и за укрепване на киберотбраната. В този контекст институциите, органите и агенциите на ЕС, както и държавите членки се насърчават да подкрепят по-нататъшното разработване и внедряване на нови и съществуващи механизми на ЕС за координация, оценки на риска, оценки и сценарии, общ доброволен обмен на информация и учения по начин, който добавя стойност и избягва ненужното дублиране със съществуващи инициативи.

7. С оглед допълнителното укрепване на доверието, консолидирането на сътрудничеството и улесняването на навременния обмен на информация относно значими и мащабни киберинциденти, засягащи отбранителните системи, Съветът приветства инициативата за по-нататъшно развитие на Конференцията на киберкомандирите на ЕС, която да се организира от всяко председателство на Съвета на ЕС с подкрепата на Европейската агенция по отбрана (EDA) и с участието на Европейската служба за външна дейност (ЕСВД). Съветът насърчава всички държави членки да участват в тези срещи. С цел засилване на устойчивостта на ЕС срещу мащабни киберинциденти, Съветът приканва
мрежата на ЕС за връзка на организациите при кибернетични кризи (EU-CyCLONe) и Конференцията на киберкомандирите на ЕС да установят възможни начини за сътрудничество и извличане на ползи от съвместна военна и гражданска перспектива.

[1] Предложение за препоръка на Съвета относно координиран подход на Съюза за укрепване на устойчивостта на критичната инфраструктура (COM/2022/551 final).

8. За да се насърчи по-силно и координирано реагиране на равнище ЕС, Съветът приветства и очаква постигането на начална оперативна способност на оперативната мрежа на военните екипи от ЕС за незабавно реагиране при компютърни инциденти (MICNET) до средата на 2024 г. с цел подобряване на обмена на техническа информация относно киберинциденти, засягащи отбранителните системи, между участващите държави членки. Съветът насърчава всички държави членки да участват в MICNET, за да се гарантира ефективността на мрежата. Освен това Съветът приканва държавите членки да използват поуките, извлечени от мрежата на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС), и силно насърчава създаването на ефективен механизъм за сътрудничество и координация между двете мрежи в подходящ момент, при пълно зачитане на механизмите за управление и състава на тези отделни мрежи.

9. Предвид увеличаването на злонамерените действия на държавни и недържавни субекти в киберпространството по отношение на
мисии и операции на ЕС по линия на ОПСО Съветът приканва ЕС и неговите държави членки да засилят своите способности за защита и гарантиране на сигурността на мисиите и операциите по линия на ОПСО. Във връзка с това Съветът приветства целите за по-нататъшно развитие на защитата на военните мрежи и структури на ЕС, в съответствие, наред с другото, с Военната визия и стратегия на ЕС относно киберпространството като област на операции[2].

[2] EEAS(2021) 706 REV4

10. Съветът изтъква отново заключенията на Съвета от май 2022 г.[3] и необходимостта да се инвестира във взаимопомощта ни съгласно член 42, параграф 7 от ДЕС, както и клаузата за солидарност съгласно член 222 от ДФЕС. Съветът подчертава, че е важно да се задълбочи общото разбиране на ЕС
и неговите държави членки относно прилагането на член 42, параграф 7, включително в сложни сценарии, включващи кибератака, в съответствие със съответните принципи на международното право. Той приветства възможността, по изрично искане на засегнатата(ите) държава(и) членка(и), за подкрепа от страна на ЕС в случай на кибератака, без да се засяга специфичният характер на политиката за сигурност и отбрана на някои държави членки.

11. Съветът подчертава напредъка, постигнат по проекта по линия на ПСС за екипи за бързо реагиране при кибератаки и екипи за взаимопомощ в областта на киберсигурността, както и готовността на тези екипи да действат при поискване като способност за нуждите на държавите членки и ЕС в подкрепа на мисиите и операциите по линия на ОПСО и да предоставят помощ на партньорите на ЕС. Съветът приветства по-нататъшното развитие на способностите на екипите за бързо реагиране при кибератаки и екипите за взаимопомощ в областта на киберсигурността по линия на ПСС, на националните екипи за реагиране при киберинциденти и когато е целесъобразно, на допълнителни способности за реагиране при инциденти, като например бъдещите екипи за бързо реагиране при хибридни заплахи, предвидени в Стратегическия компас, включително чрез насърчаване на координацията и сътрудничество между тях на равнище ЕС.

[3] Заключения на Съвета относно установяването на позицията на Европейския съюз в киберпространството, 23 май 2022 г., 9364/22.

12. Съветът приветства работата на проекта „Координационен център в областта на киберсигурността и информацията (КЦКИ)“ по линия на ПСС, чиято цел е да осигури военна способност за събиране и анализиране на информация от значение за обща оперативна картина на киберпространството. Освен това Съветът приветства предложението за интегриране на доказателството за концепцията, ако тя бъде успешна като координационен център в областта на информацията, от 2025 г. нататък в Координационен център на ЕС за киберотбрана (КЦК на ЕС), който да подобрява координацията и ситуационната осведоменост, по-специално на командирите на мисии и операции на ЕС по линия на ОПСО, и да укрепва общата структура за командване и контрол в ЕС. Съветът призовава върховния представител да представи концепция и пътна карта за създаването на КЦК на ЕС, в които се извличат поуки от подобни международни структури, определят се необходимите ресурси, избягва се ненужното дублиране и се търси взаимно допълване с по-широката рамка на ЕС за киберсигурност.

13. Съветът подчертава значението на стратегическото сътрудничество в областта на разузнаването във връзка с киберзаплахите и дейностите в киберпространството и приканва държавите членки, чрез своите компетентни органи, да продължат да допринасят за работата на Центъра на ЕС за анализ на информацията (INTCEN), дирекцията „Разузнаване“ на Военния секретариат на ЕС (ВСЕС) и държавите членки в рамките на единното звено за анализ на разузнавателна информация (SIAC). Освен това Съветът подчертава, че е важно да укрепим капацитета си за киберразузнаване, за да повишим устойчивостта си в киберпространството и да осигурим ефективна подкрепа за нашите граждански и военни мисии и операции по линия на ОПСО, както и капацитета на нашите въоръжени сили и SIAC в киберсферата, въз основа на доброволен принос с разузнавателни данни от държавите членки и без да се засягат техните правомощия.

14. Съветът взема под внимание центъра за киберситуация и анализ в Европейската комисия, чиято цел е да се повиши ситуационната осведоменост на Комисията. Съветът изтъква значението на установяването на взаимноизгодно сътрудничество между този център и други институции, органи и агенции на ЕС, по-специално ENISA и ЕРИКС. Съветът подчертава, че е важно да се осигури тясно сътрудничество с мрежите за сътрудничество на ЕС при развиването на ситуационна осведоменост, както и да се зачита поверителността. ЕС отбелязва необходимостта от засилване на общата ситуационна осведоменост на равнище ЕС и от по-нататъшно развитие на рамката на ЕС за управление на кризи в областта на киберсигурността, като същевременно се избягва ненужното дублиране на усилия.

15. Съветът припомня, че образованието, обучението и ученията в кибернитичната област са от съществено значение за осигуряване на подготвеност и ефективност, и приветства дейностите на национално равнище, както и дейностите, осигурявани от ЕС чрез Европейския колеж по сигурност и отбрана (ЕКСО), EDA, ENISA и текущите проекти по линия на ПСС, като например проекта „Федериране на киберполигони“ и Центъра на ЕС за академично и иновационно сътрудничество в кибернетичната област (CAIH). С оглед на по-нататъшното увеличаване на тези усилия Съветът очаква създаването на рамковия проект CyDef-X на EDA за синхронизиране и подкрепа на ученията в областта на киберотбраната. Съветът насърчава EDA да проучи, в тясно сътрудничество с държавите членки и ЕСВД, как CyDef-X би могъл да продължи подкрепата за учения като CYBER PHALANX, включително за взаимопомощ съгласно член 42, параграф 7 от ДЕС и клаузата за солидарност съгласно член 222 от ДФЕС, както и за граждански учения, в сътрудничество с Комисията и ENISA. Освен това Съветът насърчава използването и по-нататъшното развитие в рамките на CyDef-X на съществуващите среди за изпитване и учения в областта на киберотбраната, като например проекта „Федериране на киберполигони“. За да се осигури гъвкав и ефикасен процес на вземане на решения по въпроси, свързани с киберкризи, Съветът подчертава, че е важно да се провеждат редовни симулационни учения, предназначени за равнището на вземане на решения в държавите членки.

16. Съветът отбелязва предложението за законодателен акт в областта на киберсолидарността и намерението да се подобрят способностите за откриване и реагиране на заплахи и инциденти в областта на киберсигурността в ЕС. Съветът подчертава, че предложенията в тази област могат да бъдат ефективни само когато са съгласувани с рамките и нуждите на държавите членки за управление на кризи. Съветът подчертава, че е важно критичната инфраструктура да се изпитва за потенциални уязвимости, когато се счита, че това е полезно, в рамките на националната компетентност, като се вземат предвид наличните оценки на ЕС относно риска.

17. Съветът отбелязва предложението на Комисията за създаване на механизъм за действие при извънредни ситуации в кибернетичното пространство, който би могъл да подпомогне наличието на услуги в областта на киберсигурността от надеждни частни доставчици, които при поискване да подпомагат държавите членки в случай на мащабни киберинциденти, като същевременно подчертава необходимостта от увеличаване на европейския сектор на киберсигурността с подкрепата на Европейския център за експертни познания в областта на киберсигурността като основен стълб за функционирането на този механизъм. Съветът подчертава ключовата роля на всяка държава членка при следенето и оценката на националните ѝ нужди.

II. **Защита на отбранителната екосистема на ЕС**

18. Съветът припомня, че насърчава държавите членки да доразвият собствените си способности за провеждане на операции по киберотбрана, включително, когато е целесъобразно, проактивни отбранителни мерки за защита, откриване, отбрана и възпиране срещу кибератаки. Като се има предвид, че МИС 2 не се прилага за субекти от публичната администрация, които извършват дейности в областта на отбраната, Съветът приканва EDA, по целесъобразност с подкрепата на Комисията и ЕСВД, да подпомага държавите членки при разработването на правно необвързващи доброволни препоръки, вдъхновени от МИС 2, за повишаване на киберсигурността в отбранителната общност, и приканва всички държави членки да се включат активно в тези усилия. В препоръките следва да се вземат предвид подобни усилия, предприети в други рамки.

19. Както се признава в Стратегическия компас, способността на ЕС да действа зависи от способността му да намали стратегическите си зависимости във връзка с всички свои способности и вериги на доставки в областта на киберотбраната, както и да разработва и овладява авангардни технологии за киберотбрана. Това включва укрепване на европейската отбранителна технологична и индустриална база в целия ЕС и способността ѝ да си сътрудничи с единомислещи партньори по света на реципрочна основа, за да се гарантират взаимни ползи. Ето защо Съветът призовава за тясно сътрудничество между секторите на киберсигурността и киберотбраната, за да се създадат полезни взаимодействия с цел разработване и осигуряване на пълен спектър от способности за киберотбрана. Съветът приканва Комисията, в тясно сътрудничество с Европейския център за експертни познания в областта на киберсигурността, когато е целесъобразно, да продължи да подкрепя развитието на силна, гъвкава, конкурентоспособна в световен мащаб и иновативна европейска индустриална и технологична база в областта на киберотбраната, включително на малките и средните предприятия (МСП), чрез допълнителни инвестиции и политически действия.

20. Като се има предвид значението на оперативната съвместимост и общите характеристики на способностите за киберотбрана, включително когато става въпрос за съвместното разработване на способности за киберотбрана от следващо поколение, Съветът приканва EDA и ВСЕС да работят по набор от изисквания на ЕС за оперативна съвместимост в областта на киберотбраната, които ще се основават на съществуващите принципи, процеси и стандарти установени по-специално в рамката на Организацията на Северноатлантическия договор (НАТО), и ще бъдат съвместими с тях. Освен това Съветът приканва държавите членки, в тясно сътрудничество с всички съответни заинтересовани страни, включително европейските организации за стандартизация и НАТО, когато е целесъобразно, да проучат в рамките на Европейския комитет по стандартизация в областта на отбраната дали би имало нужда от специфични доброволни стандарти за отбранителни системи.

21 Съветът приветства усилията на Комисията да представи план за насърчаване на използването на съществуващите стандарти за гражданска киберсигурност и киберотбрана, както и разработването на нови доброволни стандарти. Съветът изтъква необходимостта от хармонизиране на стандартите за киберсигурност и киберотбрана, когато е целесъобразно. Съветът отчита, че такива доброволни стандарти биха могли да бъдат полезни за секторите на киберсигурността и киберотбраната на ЕС, и настоятелно призовава за по-тясно сътрудничество между органите по стандартизация в гражданската сфера и органите по стандартизация в областта на отбраната.

22. Съветът призовава за бързо разработване на препоръки въз основа на картографирането на съществуващите инструменти за сигурна комуникация в киберпространството, извършено от Комисията и съответните институции. Когато е възможно, препоръките следва да бъдат приведени в съответствие със съществуващите инициативи за обмен на информация и следва също така да отчитат рисковете, породени от нововъзникващи и революционни технологии, за настоящите методи за криптиране.

23. Освен това Съветът приветства осъществената първоначална работа по оценката на риска и сценариите, разработвани от Комисията, върховния представител и групата за сътрудничество за МИС във връзка, първоначално, с енергийния и телекомуникационния сектор, по искане на Съвета. Съветът отчита, че се изготвят и целеви оценки на риска за киберсигурността на инфраструктурата и мрежите за комуникации в ЕС. Съветът изтъква отново, че общото разбиране на възможните последици от киберинциденти между държавите членки, но и между институциите, органите и агенциите на ЕС е от първостепенно значение. Във връзка с това Съветът приканва посочените по-горе участници да гарантират, че оценките на риска, сценариите и последващите препоръки се вземат предвид при определянето и приоритизирането на мерките и подкрепата на равнището на ЕС и когато е целесъобразно, на национално равнище. Освен това Съветът призовава сценариите за риска да бъдат разглеждани от всички съответни участници в процесите за оценка на риска, както и при разработването на учения в областта на киберсигурността.

III. **Инвестиране в способности за киберотбрана**

24. Съветът насърчава държавите членки да увеличат инвестициите си за изграждане, поддържане и по-нататъшно развитие на оперативно съвместими способности за киберотбрана. Съветът подкрепя изготвянето на набор от доброволни ангажименти за по-нататъшно развитие на националните способности за киберотбрана, като се имат предвид подобни усилия, предприети в други рамки.

25. Съветът призовава държавите членки и EDA да използват възможността за преразглеждане на плана за развитие на способностите, за да определят високо равнище на амбиция по отношение на развитието на съвместна киберотбрана на равнище ЕС. Освен това Съветът насърчава държавите членки да се основават на актуализирания набор от приоритети и на ангажиментите си по линия на ПСС с цел повишаване на равнището на ангажираност в съвместни проекти на ЕС за развитие на способностите за киберотбрана, отчитайки пряката полза от съвместните проекти на равнище ЕС за подкрепата на развитието на националните способности за киберотбрана.

26. Съветът приветства съвместните научноизследователски усилия на равнище ЕС за проучване на възможните приложения на нововъзникващи и революционни технологии в свързаните с отбраната системи, като отбелязва също така необходимостта да се гарантира, че тези технологични постижения се включват бързо в съществуващи и бъдещи способности. Съветът насърчава държавите членки и индустриалния сектор на ЕС да използват по най-добрия начин възможностите за съвместни научни изследвания на равнището на ЕС, например в рамките на EDA, текущи проекти по линия на ПСС, като например Центъра на ЕС за академично и иновационно сътрудничество в кибернетичната област (CAIH), Европейския фонд за отбрана и когато е уместно, „Хоризонт Европа“ и програмата „Цифрова Европа“ за проекти с двойно предназначение. Освен това Съветът приветства използването на специалните рамки за подкрепа на иновациите в областта на отбраната, при които се използват вторични отбранителни и космически разработки, почиващи на постижения в гражданската област, по-специално схемата на ЕС за иновации в областта на отбраната и Центъра за европейски иновации в областта на отбраната. Освен това Съветът насърчава Европейския център за експертни познания в областта на киберсигурността и EDA да изготвят работна договореност за улесняване на обмена на информация между съответните служители относно приоритетите, свързани съответно с гражданските технологии, технологиите с двойна употреба и отбранителните технологии, с оглед на създаването на полезни взаимодействия и избягването на дублиране.

27. Съветът приветства намерението на Комисията да разработи технологична пътна карта за критични кибертехнологии в сътрудничество с EDA и Европейския център за експертни познания в областта на киберсигурността в съответствие със съответните им мандати, с държавите членки и в консултация със съответните заинтересовани страни, като например сектора на индустрията, която карта чрез установяване на критичните кибертехнологии и набелязване на технологичните разработки и стратегическите зависимости предоставя начини за намаляване на тези зависимости и за подкрепа на стратегическата автономност и технологичния суверенитет на ЕС при същевременно запазване на отворената икономика. Съветът отбелязва, че технологичната пътна карта за критичните кибертехнологии може да допринесе за стратегическите приоритети за инструментите на ЕС за финансиране, като същевременно е съобразена със съответните действащи условия за тях. Съветът припомня, че ЕС следва да провежда амбициозна и решителна европейска индустриална политика за създаване на устойчива, привлекателна и конкурентоспособна бизнес среда, която може също така да даде възможност на европейските субекти в киберсферата да се разрастват.

28. Съветът оценява намерението за преодоляване на значителния недостиг на умения в областта на киберсигурността чрез привличане на нови специалисти, включително жени, повишаване на квалификацията и преквалификация и инвестиране в обучения и учения и тяхното организиране с цел изграждане на разнообразна и приобщаваща работна сила в киберсферата. Като отчита предизвикателствата, пред които е изправен ЕС по отношение на човешкия капитал в областта на киберсигурността и киберотбраната, Съветът приветства инициативата „Академия за умения в областта на киберсигурността“, която може да бъде от полза и за работната сила в областта на киберотбраната.

29. Съветът приканва държавите членки да обменят информация относно най-добрите практики за развитие на квалифицирани специалисти в областта на киберсигурността, като използват полезните взаимодействия между инициативите във военната сфера, гражданската сфера и сферата на правоприлагането, и призовава ЕКСО, с подкрепата и експертния опит на EDA и ENISA, да разгледа възможностите за засилване на обмена на най-добри практики и по-нататъшно полезно взаимодействие между военната и гражданската сфера по отношение на обучението и развитието на специфични за киберсферата умения в областта на отбраната.

30. Съветът подчертава, че е важно да има общо разбиране за състава на работната сила в областта на киберсигурността и за свързаните с нея умения, за да се установят и преодолеят случаите на недостиг на пазара на труда в областта на киберсигурността, както и че необходимо да бъдат ангажирани всички заинтересовани страни, включително държавите членки и сектора на индустрията. Съветът отчита, че определянето на показатели за наблюдение на пазара на труда в областта на киберсигурността би спомогнало за установяване на потребностите от умения в областта на киберсигурността и за адекватно насочване на средствата, като същевременно би допринесло за изпълнението на свързаните с политиката задължения, по-специално тези, произтичащи от МИС 2. Съветът приветства предложението за рамка за сертифициране на уменията в областта на киберотбраната и приканва върховния представител, в качеството му на ръководител на ЕКСО, да изготви това предложение в сътрудничество с ЕСВД, Комисията и държавите членки, като използва инициативи в гражданската сфера.

IV. **Партньорство за справяне с общите предизвикателства**

31. Съветът призовава върховния представител и Комисията да засилят и доразвият сътрудничеството си, както и да проучат взаимноизгодни и адаптирани за специфичните цели партньорства в областта на политиките за киберотбрана, включително за изграждане на капацитет за киберотбрана чрез Европейския механизъм за подкрепа на мира. За тази цел киберотбраната следва да бъде добавена като точка в диалозите и консултациите на ЕС относно киберсферата, както и в консултациите с партньорите в областта на общата сигурност и отбрана. Освен това следва да се засилят диалогът и сътрудничеството с частния сектор. Съветът подчертава, че международното сътрудничество по стандартите и сертифицирането в областта на киберсигурността ще бъде добавена стойност за европейската индустрия. Ето защо той приветства ангажимента на Комисията да превърне тази тема в съществена част от диалозите на ЕС по въпросите на киберпространството с трети държави и международни организации.

32. Съветът изтъква значението на международното сътрудничество за предотвратяване или намаляване на рисковете от конфликти в киберпространството, особено чрез по-нататъшно разработване и привеждане в действие на мерки за изграждане на доверие на регионално и международно равнище, включително в рамките на ООН, и допълнително насърчаване на използването на свързаните с киберсферата съществуващи мерки за изграждане на доверие, като например тези в рамките на Организацията за сигурност и сътрудничество в Европа (ОССЕ), включително във времена на международно напрежение.
ЕС и неговите държави членки подчертават, че съществуващото международно право се прилага в киберпространството, и изтъкват, че е важно да продължат усилията за поддържане и насърчаване на рамката на ООН за отговорно поведение на държавите и да се работи за нейното прилагане, включително чрез създаването на програма за насърчаване на отговорното поведение на държавите в киберпространството.

33. В съответствие със съвместните декларации относно сътрудничеството между ЕС и НАТО Съветът приканва върховния представител, в качеството му на ръководител на EDA, и Комисията да засилят, задълбочат и разширят още повече партньорството с НАТО в киберсферата, при пълно зачитане на принципите на приобщаване, реципрочност, откритост и прозрачност, както и на автономността на двете организации при вземането на решения. Като отчита необходимостта да се осигурят допълващи се и координирани усилия с възможно най-пълно участие на държавите членки, които не са част от НАТО, и да се избегне ненужно дублиране, Съветът призовава между ЕС и НАТО да бъдат установени връзки на съответните равнища в областта на обучението, образованието, ситуационната осведоменост, ученията и платформите за научноизследователска и развойна дейност, както и да се търсят потенциални полезни взаимодействия между съответните доброволни ангажименти за развитието на националните способности за киберотбрана и рамките за управление на кризи, защитата на критичната инфраструктура и засилването на обмена относно ситуационната осведоменост, координираната реакция срещу злонамерени действия в киберпространството, както и усилията за изграждане на капацитет в трети държави. Това включва техническото споразумение между екипа на НАТО за реагиране при компютърни инциденти (NCIRC) и екипа на ЕС за незабавно реагиране при компютърни инциденти (CERT-EU), както и засилен политически диалог по въпросите на киберотбраната на всички равнища.

V. **Заключение**

34. Съветът призовава върховния представител и Комисията да изготвят до второто тримесечие на 2023 г., въз основа на заключенията на Съвета относно политиката на ЕС за киберотбрана, план за изпълнение на политиката, който да бъде представен за одобрение от държавите членки. Освен това Съветът приканва държавите членки доброволно да заявят своите амбиции и действия по отношение на киберотбраната в контекста на политиката на ЕС за киберотбрана и да използват пълноценно правно необвързващите доброволни препоръки и ангажименти за увеличаване на своите национални и многонационални усилия в областта на киберотбраната с цел постигане на максимално въздействие на равнището на ЕС. Върховният представител, Комисията и държавите членки се приканват да докладват и обсъждат ежегодно напредъка по изпълнението на елементите на съвместното съобщение и плана за неговото изпълнение, като започнат този процес до второто тримесечие на 2024 г.