Съвет на
Европейския съюз

Брюксел, 23 май 2022 г.
(OR. en)

9364/22

CYBER 183	**EUMC 170**
COPEN 202	**IPCR 54**
COPS 228	**HYBRID 46**
COSI 142	**DISINFO 45**
DATAPROTECT 166	**COTER 126**
IND 189	**CSDP/PSDC 304**
JAI 698	**CFSP/PESC 685**
JAIEX 57	**CIVCOM 93**
POLMIL 120	**RECH 262**
RELEX 681	**PROCIV 65**
TELECOM 237	

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
Дата:	23 май 2022 г.
До:	Делегациите
Относно:	Заключения на Съвета относно установяването на позицията на Европейския съюз в киберпространството - Заключения на Съвета, одобрени от Съвета на заседанието му от 23 май 2022 г.

Приложено се изпращат на делегациите заключенията на Съвета относно установяването на позицията на Европейския съюз в киберпространството, одобрени от Съвета на заседанието му от 23 май 2022 г.

ПРИЛОЖЕНИЕ

Заключения на Съвета относно установяването на позицията на Европейския съюз в киберпространството

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като ПРИПОМНЯ своите заключения относно:

– съвместното съобщение от 25 юни 2013 г. до Европейския парламент и Съвета относно Стратегията на Европейския съюз за киберсигурност: „Отворено, безопасно и сигурно киберпространство“[1],

– рамката за политиката на ЕС за кибернетична отбрана[2],

– управлението на интернет[3],

– кибердипломацията[4],

– укрепването на отбранителната способност на Европа срещу кибератаки и изграждането на конкурентен и иновативен сектор на киберсигурността[5],

– съвместното съобщение от 20 ноември 2017 г. до Европейския парламент и Съвета „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“[6],

– рамка за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството („инструментариум за кибердипломация“)[7],

– координираната реакция на ЕС при мащабни инциденти и кризи в областта на киберсигурността[8],

– насоките на ЕС за изграждане на външен киберкапацитет[9],

– Решение за изпълнение (ЕС) 2018/1993 на Съвета от 11 декември 2018 г. относно договорености за интегрирана реакция на ЕС при политическа криза[10],

1 Док. 12109/13.
2 Док. 15585/14.
3 Док. 16200/14.
4 Док. 6122/15 + COR 1.
5 Док. 14540/16.
6 Док. 14435/17 + COR 1.
7 Док. 10474/17.
8 Док. 10086/18.
9 Док. 10496/18.

– капацитета за киберсигурност и изграждането на способности в ЕС[11],

– значението на 5G за европейската икономика и необходимостта от смекчаване на рисковете за сигурността, свързани с 5G[12],

– бъдещето на една високо цифровизирана Европа след 2020 г.: „Стимулиране на цифровата и икономическата конкурентоспособност в Съюза и цифровото сближаване“[13],

– допълнителни усилия за укрепване на устойчивостта на хибридни заплахи и за борба с тях[14],

– изграждането на цифровото бъдеще на Европа[15],

– киберсигурността на свързаните устройства[16],

– стратегията на ЕС за киберсигурност за цифровото десетилетие[17],

– сигурността и отбраната[18],

– проучване на потенциала на инициативата за съвместно киберзвено – допълване на координираната реакция на ЕС при мащабни инциденти и кризи в областта на киберсигурността[19],

– Стратегически компас за сигурността и отбраната — За Европейски съюз, който защитава своите граждани, ценности и интереси и допринася за международния мир и сигурност[20],

---

10 ОВ L 320, 17.12.2018 г., стр. 28 – 34.
11 Док. 7737/19.
12 Док. 14517/19.
13 Док. 9596/19.
14 Док. 14972/19.
15 Док. 8711/20.
16 Док. 13629/20.
17 Док. 7290/21.
18 Док. 8396/21.
19 Док. 13048/21.
20 Док. 7371/22.

1. ПОДЧЕРТАВА засилването през последните години на злонамереното поведение в киберпространството както на държавни, така и на недържавни участници, включително рязкото и постоянно нарастване на злонамерените дейности, насочени срещу критичната инфраструктура, веригите на доставки и интелектуалната собственост на ЕС и неговите държави членки, повишения риск от разпространение на ефектите, както и увеличаването на атаките със софтуер за изнудване срещу нашите предприятия, организации и граждани. ОТБЕЛЯЗВА, че със завръщането на силовата политика зачестяват опитите на някои държави за оспорване и подкопаване на основания на правила международен ред в киберпространството, които превръщат киберпространството, наред с откритото море, въздушното и космическото пространство, във все по-оспорвана област. ПРИЗНАВА, че широкомащабните кибератаки или опити за намеса, нарушаване или разрушаване на мрежи и информационни системи, предизвикващи системни последици, са зачестили, че те могат да подкопаят нашата икономическа сигурност и да засегнат демократичните ни институции и процеси и че демонстрират готовността на някои участници да изложат на опасност международната сигурност и стабилност. ПОДЧЕРТАВА, че военната агресия на Русия срещу Украйна е показала, че офанзивните действия в киберпространството могат да бъдат неразделна част от хибридни стратегии, съчетаващи сплашване, дестабилизация и икономически сътресения.

2. ИЗТЪКВА ОТНОВО, че в контекста на настоящите геополитически промени силата на нашия Съюз е в единството, солидарността и решимостта и че прилагането на Стратегическия компас ще засили стратегическата автономност на ЕС и способността му да работи с партньори за защита на неговите ценности и интереси, включително в киберпространството. ПОДЧЕРТАВА, че един по-силен и по-способен ЕС в областта на сигурността и отбраната ще допринесе положително за световната и трансатлантическата сигурност и допълва НАТО – организацията, която за държавите, членуващи в нея, продължава да бъде основата на колективната им отбрана. ПОТВЪРЖДАВА намерението на ЕС да засили своята подкрепа за основания на правила международен ред, в сърцевината на който стои ООН.

3. В съответствие със Заключенията на Съвета относно Стратегията на ЕС за киберсигурност и Стратегическия компас ИЗТЪКВА ОТНОВО, че позицията на Съюза в киберпространството трябва да се развива, като се повишава способността ни за предотвратяване на кибератаки посредством изграждане на капацитет, развиване на способностите, обучение, учения и повишена устойчивост, както и чрез решителен отпор на кибератаките срещу ЕС и неговите държави членки, като се използват всички налични инструменти на ЕС. Това включва още по-голяма демонстрация на решимостта на ЕС да дава незабавен и дългосрочен отговор на участниците в заплахи, които се стремят да възпрепятстват нашия сигурен и отворен достъп до киберпространството и да засегнат стратегическите ни интереси, включително сигурността на нашите партньори. В този контекст ИЗТЪКВА, че позицията в киберпространството има за цел да обедини различните инициативи в действията на ЕС, които целят укрепването на мира и стабилността в киберпространството и са в полза на едно отворено, свободно, глобално, стабилно и сигурно киберпространство, като същевременно се координират по-добре краткосрочните, средносрочните и дългосрочните действия за предотвратяване, обезкуражаване, възпиране и реагиране на киберзаплахи и атаки и се използват киберспособностите. НАБЛЯГА, че тези елементи следва да станат част от позицията на ЕС в киберпросранството, в съответствие с петте функции на ЕС в киберпространството: укрепване на нашата киберустойчивост и капацитет за защита; засилване на солидарното и всеобхватно управление на кризи; популяризиране на нашата визия за киберпространството; засилване на сътрудничеството с държави партньори и международни организации; предотвратяване, защита и реагиране на кибератаки.

I. УКРЕПВАНЕ НА НАШАТА КИБЕРУСТОЙЧИВОСТ И КАПАЦИТЕТ ЗА ЗАЩИТА

4. ИЗТЪКВА ОТНОВО необходимостта от повишаване на общото равнище на киберсигурност в ЕС, ОЧАКВА бързото приемане на проекта за директива относно мерки за високо общо ниво на киберсигурност в Съюза (МИС), проекта за регламент относно оперативната устойчивост на цифровите технологии във финансовия сектор (DORA) и проекта за директива относно устойчивостта на критичните субекти и ВЗЕМА ПОД ВНИМАНИЕ предложението за регламент за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза, чиято цел е да способства за постигането на Европейски съюз, който защитава своите граждани, обществени услуги и предприятия в киберпространството. НАСЪРЧАВА Комисията да финализира приемането на ключовите предложения, за да се гарантира сигурността на цифровите инфраструктури, технологии, продукти и услуги, да се изпрати ясен сигнал за амбициите на ЕС по тези въпроси и да се улесни предоставянето на подкрепа за предприятията, с цел те да се справят с това предизвикателство. ПРИЗОВАВА Комисията да предложи общи изисквания на ЕС за киберсигурността на свързаните устройства и съответните процеси и услуги чрез Законодателния акт за киберустойчивост, за който Комисията следва да представи предложение до края на 2022 г., като се отчита необходимостта от хоризонтален и цялостен подход, обхващащ целия жизнен цикъл на цифровите продукти и услуги, както и съществуващата нормативна уредба, по-конкретно в областта на киберсигурността.

5. ПРИКАНВА съответните органи, като Органа на европейските регулатори в областта на електронните съобщения (ОЕРЕС), Агенцията на Европейския съюз за киберсигурност (ENISA) и Групата за сътрудничество в областта на мрежовата информационна сигурност (МИС), заедно с Европейската комисия, да формулират препоръки към държавите членки и Европейската комисия въз основа на оценка на риска с цел укрепване на устойчивостта на комуникационните мрежи и инфраструктури в рамките на Европейския съюз, включително текущото прилагане на инструментариума на ЕС за 5G технологиите.

6. ПРИЗОВАВА ЕС и неговите държави членки да увеличат усилията си за повишаване на цялостното равнище на киберсигурност, например чрез улесняване на появата на надеждни доставчици на услуги в областта на киберсигурността, и ИЗТЪКВА, че насърчаването на развитието на такива доставчици следва да бъде приоритет за промишлената политика на ЕС в областта на киберсигурността. С цел по-добра издръжливост и противодействие на кибератаки с потенциални системни последици и извличане на поуки от работата по уязвимостите на Solarwinds, Microsoft Exchange и Apache Log4J, ПРИКАНВА Комисията да предложи варианти за насърчаване на появата на надежден сектор на услуги за киберсигурност, за укрепване на киберсигурността на веригата на доставки в областта на ИКТ, за преодоляване на потенциалните последици от софтуерните уязвимости за ЕС и неговите държави членки, включително с оглед на бъдещия Законодателен акт за киберустойчивост, и за подобряване на капацитета за откриване на киберзаплахи и споделяне на съответната информация във и между държавите членки.

7. КАТО ИЗТЪКВА ОТНОВО, че инвестирането в иновации и по-доброто използване на гражданските технологии е от ключово значение за укрепването на технологичния ни суверенитет, включително в киберпространството, ПРИЗОВАВА Комисията бързо да приведе в действие Европейския център за експертни познания в областта на киберсигурността с цел развиване на силна европейска екосистема за научни изследвания, промишленост и технологии в киберпространството, ПОДЧЕРТАВА необходимостта от стимулиране на научните изследвания и иновациите, от повече инвестиции в граждански и отбранителни области с цел укрепване на отбранителната технологична и индустриална база на ЕС (ЕОТИБ) и от развиване на киберспособностите на ЕС и неговите държави членки, включително способностите за стратегическа подкрепа. ИЗТЪКВА колко е важно да се използват интензивно новите технологии, по-специално квантовите изчислителни технологии, изкуствения интелект и големите информационни масиви, за да се постигнат сравнителни предимства, включително по отношение на операциите за реагиране при киберинциденти.

8. КАТО ОТЧИТА, че укрепването на киберсигурността е начин за повишаване на ефективността и сигурността на действията ни по суша, въздух и море и в космическото пространство, ИЗТЪКВА, че е важно съображенията относно киберсигурността да бъдат интегрирани във всички публични политики на ЕС, включително в секторното законодателство, допълващо Директивата за МИС 2, и ПРИКАНВА Комисията да проучи възможностите за повишаване на киберсигурността по цялата верига на доставки на отбранителната технологична и индустриална база на ЕС (ЕОТИБ).

9. ОТЧИТА, че е от съществено значение да се осигурят подходящи финансови и човешки ресурси за киберсигурността и да се предприемат мерки, насочени към създаването на благоприятна среда за конкурентоспособността на частния сектор, с цел развитие на позицията на ЕС в киберпространството, както и че въпросът за стабилно и дългосрочно финансиране на киберсигурността следва също да бъде разгледан на равнището на ЕС чрез разработване и прилагане на хоризонтален механизъм, съчетаващ множество източници на финансиране, като се включат разходите за висококвалифицирани човешки ресурси. Във връзка с това ПРИЗОВАВА Комисията да проучи до края на 2022 г. вариантите за такъв механизъм, които да бъдат обсъдени в съответните органи на Съвета.

10. НАБЛЯГА на необходимостта от укрепване на нашите действия и от засилване на сътрудничеството в борбата с международната киберпрестъпност, по-специално софтуера за изнудване, чрез механизма на Европейската мултидисциплинарна платформа за борба с криминални заплахи (EMPACT), чрез обмен между секторите на киберсигурността, правоприлагането и дипломацията, и чрез укрепване на капацитета за правоприлагане при разследването и наказателното преследване на киберпрестъпления. ИЗТЪКВА ОТНОВО ангажимента си да информира обществеността относно киберзаплахите и относно мерките, предприети на национално равнище и на равнище ЕС срещу тези заплахи, чрез приобщаване на гражданското общество, частния сектор и академичните среди, така че да се повиши осведомеността и да се насърчава подходящо равнище на киберзащита и киберхигиена. ИЗТЪКВА, че е необходимо вниманието да бъде насочено към уменията и способностите на гражданите в областта на киберсигурността на равнището на ЕС и на държавите членки, както и потребителите да бъдат приобщени да участват активно в собствената си защита.

II. **ЗАСИЛВАНЕ НА СОЛИДАРНОТО И ВСЕОБХВАТНО УПРАВЛЕНИЕ НА КРИЗИ**

11. Въз основа на годишните киберучения, други учения с киберизмерение и ученията EU CyCLES 2022, ИЗТЪКВА, че е важно да се изготви програма за редовни междуобщностни и многостепенни киберучения с цел изпитване и развиване на вътрешната и външната реакция на ЕС при мащабни киберинциденти, с участието на Съвета, ЕСВД, Комисията и съответните заинтересовани страни като ENISA и частния сектор, която ще бъде разработена и ще допринася за общата политика на ЕС за ученията. НАБЛЯГА на значението на по-нататъшното развиване на ученията Cyber Europe и BlueOLEx, които съчетават ответни действия на различни равнища. ОТЧИТА, че е необходимо да се оценят и консолидират съществуващите учения и да се проучи възможността за допълнителни учения по конкретни сегменти на киберпространството, по-конкретно за учение между военните екипи за незабавно реагиране при компютърни инциденти (CERT) или учение, съсредоточено върху сътрудничеството при кризи между институциите, органите и агенциите на ЕС. ОТЧИТА, че позицията на Съюза в киберпространството ще укрепи способността ни да предотвратяваме кибератаки чрез различни действия, включително обучение, и във връзка с това ПРИКАНВА държавите членки да засилят гражданско-военното сътрудничество в областта на киберобучението и съвместните учения.

12. ПОДЧЕРТАВА необходимостта от по-нататъшно изпитване и укрепване на оперативното сътрудничество и споделената ситуационна осведоменост между държавите членки, включително чрез установените мрежи като мрежата на екипите за реагиране при инциденти с компютърната сигурност (CSIRT) и мрежата за връзка на организациите при кибернетични кризи (EU-CyCLONe), така че да се повиши готовността на ЕС за справяне с мащабни киберинциденти. ПОДЧЕРТАВА, че е важно да се работи върху разработването на общ език между държавите членки и с институциите, органите и агенциите на ЕС, който да е пригоден за обсъжданията на политическо равнище, за да се подкрепи изготвянето на консолидирана оценка на сериозността и въздействието на съответните киберинциденти, както и възможните сценарии за развитие и произтичащите от тях нужди, по целесъобразност. ПОДЧЕРТАВА в това отношение, че е необходимо да се подобри взаимното допълване на докладите за споделената ситуационна осведоменост, включително докладите на EU-CyCLONe относно въздействието и сериозността на широкомащабните киберинциденти сред държавите — членки на ЕС, и оценките на заплахите, предоставяни от Центъра на ЕС за анализ на информация (INTCEN) в рамките на инструментариума на ЕС за кибердипломация. ПРИКАНВА Комисията, върховния представител и групата за сътрудничество за МИС, в координация със съответните граждански и военни органи и агенции и установените мрежи, включително EU-CyCLONe, да извършат до края на 2022 г. оценка на риска и да разработят сценарии на риска от гледна точка на киберсигурността в ситуация на заплаха или евентуална атака срещу държави членки или държави партньори и да ги представят на съответните органи на Съвета. НАБЛЯГА на необходимостта от подходяща и координирана публична комуникация относно реакцията на ЕС при мащабни киберинциденти.

13. В случай на мащабен киберинцидент ИЗТЪКВА необходимостта от засилване на координацията и по целесъобразност, въз основа на постигнатия напредък и работата на екипите за бързо реагиране при кибератаки по линия на ПСС, както и на работата на мрежата ЕРИКС и мрежата на ЕС CyCLONe, доброволното обединяване на способностите на държавите членки за реагиране при инциденти. ПРИЗНАВА, че изграждането на връзки с частния сектор би могло да засили публичния капацитет, по-специално в контекста на недостига на умения в целия ЕС, и че определянето и координирането на тези частни партньори би могло да има решаващо значение в случай на мащабни инциденти. С оглед на постигането на пълна подготвеност за мащабни киберинциденти ПРИКАНВА Комисията да предложи до края на третото тримесечие на 2022 г. нов фонд за реагиране при извънредни ситуации в областта на киберсигурността.

14. В съответствие със Стратегическия компас ИЗТЪКВА ОТНОВО необходимостта да се инвестира в нашата взаимопомощ съгласно член 42, параграф 7 от Договора за Европейския съюз, както и в нашата солидарност съгласно член 222 от Договора за функционирането на Европейския съюз, по-специално чрез чести учения. В този контекст ИЗТЪКВА необходимостта от по-нататъшна работа за предоставянето и координирането на двустранна гражданска и/или военна подкрепа, включително чрез проучване на възможности за подкрепа от ЕС при изрично искане от държавите членки, и за определянето на подходящи ответни мерки, включително чрез разработването на координирана комуникационна стратегия, в контекста на прилагането на член 42, параграф 7. ОТБЕЛЯЗВА, че това следва да включва и проучване на връзките със съществуващите механизми на ЕС за управление на кризи и механизма на ЕС за гражданска защита.

15. ПОДЧЕРТАВА, че укрепването на позицията на ЕС в киберпространството ще изисква засилени сигурни комуникации. За тази цел ИЗТЪКВА ОТНОВО относимите насоки на Стратегическия компас и ПРИКАНВА Комисията и другите съответни институции, органи и агенции да картографират до края на 2022 г. съществуващите инструменти за сигурна комуникация в киберпространството, за да бъдат те обсъдени в съответните органи на Съвета и със съответните групи за сътрудничество, като мрежата на екипите за реагиране при инциденти с компютърната сигурност (CSIRT) и мрежата за връзка на организациите при кибернетични кризи (EU CyCLONe).

III. ПОПУЛЯРИЗИРАНЕ НА НАШАТА ВИЗИЯ ЗА КИБЕРПРОСТРАНСТВОТО

16. ПРИПОМНЯ, че общият и всеобхватен подход на ЕС към кибердипломацията има за цел да допринася за предотвратяване на конфликтите, ограничаване на заплахите за киберсигурността и по-голяма стабилност в международните отношения. В този контекст ПОТВЪРЖДАВА ангажираността на ЕС с уреждането на международни спорове в киберпространството чрез мирни средства и прилагането на международното право, включително международното право в областта на правата на човека и международното хуманитарно право, когато това е приложимо за действията на държавите в киберпространството. ПОДЧЕРТАВА ангажимента на ЕС и неговите държави членки да действат в съответствие с доброволните, необвързващи норми за отговорно поведение на държавите в киберпространството, договорени от всички държави – членки на ООН. НАБЛЯГА на значението на отвореното, свободно, глобално, стабилно и сигурно киберпространство, в което правата на човека, основните свободи и принципите на правовата държава се прилагат изцяло в полза на социалното благоденствие, икономическия растеж, просперитета и целостта на нашите свободни и демократични общества, и ПОТВЪРЖДАВА ангажимента на ЕС и неговите държави членки да продължат да утвърждават тези ценности и принципи. С оглед на разработването на канали за конструктивен, откровен и открит диалог с ключови заинтересовани страни в областта на киберпространството ИЗТЪКВА, че е важно въпросите на киберпространството, включително инструментариумът на ЕС за кибердипломация, да станат неразделна част от преговорите за присъединяване към Съюза и от стратегическите и политическите диалози на ЕС както с международните партньори, така и с конкурентите, и същевременно ПРИЗОВАВА върховния представител да направи преглед на съществуващите двустранни диалози в областта на киберпространството и при необходимост да предложи стартиране на подобно сътрудничество с други държави или съответни международни организации.

17. ПРИПОМНЯ значението на многостранното сътрудничество, тъй като други заинтересовани страни също носят отговорност за киберсигурността, особено когато става въпрос за изпълнение на препоръките и решенията, взети в международните и регионалните форуми. ПРИЗОВАВА ЕС и неговите държави членки да продължат да популяризират нашия модел на киберпространство и интернет въз основа на подхода с участието на множество заинтересовани страни и чрез инициативи като Призива от Париж за доверие и сигурност в киберпространството и Декларацията относно бъдещето на интернет, като подчертават споделените ползи от стабилността в киберпространството и повишават осведомеността в световен мащаб относно опасностите от една държавоцентрична и авторитарна визия за интернет, и ПРИЗОВАВА ЕС и неговите държави членки да продължат да укрепват сътрудничеството с общността от множество заинтересовани страни, включително чрез използване на съответни проекти, като например инициативата на ЕС за кибердипломация по линия на Инструмента на ЕС за външна политика.

18. АНГАЖИРА СЕ да участва и занапред в съответните международни организации, по-специално в процесите по линия на Първи и Трети комитет на ООН, като набляга, че съществуващото международно право се прилага без резерви във и по отношение на киберпространството. ИЗТЪКВА значението на постоянните усилия за отстояване и утвърждаване на рамката на ООН за отговорно поведение на държавите и ПОДЧЕРТАВА, че ЕС и неговите държави членки ще работят активно за укрепването на нейното прилагане, включително чрез установяването на Програмата за действие за насърчаване на отговорното поведение на държавите в киберпространството. ИЗТЪКВА, че ЕС и неговите държави членки ще участват активно в преговорите за бъдеща конвенция на ООН, която да бъде ефективен инструмент за правоприлагащите и съдебните органи в световната борба срещу киберпрестъпността, като се отчита в пълна степен съществуващата рамка от международни и регионални инструменти в тази област, и по-специално Конвенцията от Будапеща за престъпления в кибернетичното пространство. ИЗТЪКВА колко е важна по-нататъшната подкрепа за разработването и привеждането в действие на мерки за изграждане на доверие (МИД) на регионално и международно равнище, както и по-нататъшните мерки, насърчаващи използването в ОССЕ на съществуващите МИД в кибернетичното пространство, включително във времена на международно напрежение.

19. ПРИПОМНЯ, че възприемането на проактивен, основан на човешките права подход за гарантиране на международните стандарти в областта на нововъзникващите технологии и основната архитектура на интернет в съответствие с демократичните ценности и принципи е от съществено значение, за да се гарантира, че интернет остава глобален, нефрагментиран и отворен, и ПОДКРЕПЯ принципа при използването и разработването на технологии да се зачитат човешките права, неприкосновеността на личния живот да се поставя в центъра, а използването на технологиите да е законосъобразно, безопасно и етично. НАСЪРЧАВА върховния представител и Комисията да разработят стратегическа визия за техническите въпроси в цифровата област, които имат отражение върху външната политика и биха могли да окажат въздействие върху стабилността на киберпространството и по-специално на интернет, включително в съответните специализирани международни организации (Международен съюз по далекосъобщения и др.).

IV. ЗАСИЛВАНЕ НА СЪТРУДНИЧЕСТВОТО С ТРЕТИ ДЪРЖАВИ И МЕЖДУНАРОДНИ ОРГАНИЗАЦИИ

20. ПОДЧЕРТАВА необходимостта от по-добро свързване на стратегията на ЕС за изграждане на киберкапацитет с нормите на ООН за отговорно поведение на държавите в киберпространството, включително чрез разработване на съобразени с потребностите програми за сътрудничество и изграждане на капацитет в подкрепа на усилията на трети държави за изпълнение, и по този начин продължаване и разширяване на усилията ни за популяризиране на Програмата за действие на ООН за насърчаване на отговорното поведение на държавите в киберпространството. ИЗТЪКВА колко е важно изграждането на киберкапацитет да бъде изцяло включено в предложението на ЕС като гарант на сигурността, с подходяща координация на усилията между държавите членки и институциите, органите и агенциите на ЕС, и по-специално ПРИВЕТСТВА сътрудничеството между държавите членки, както и с партньорите от публичния и частния сектор, по-специално чрез CyberNet (мрежата на ЕС за изграждане на киберкапацитет) и Световния форум за експертни киберпознания (GFCE), за да се гарантира координация и да се избегне дублирането.

ПРИЗОВАВА върховния представител и Комисията да създадат до третото тримесечие на 2022 г. съвет за изграждане на киберкапацитет и да провеждат редовен обмен на мнения в Хоризонталната работна група по въпроси на кибернетичното пространство. ПРИЗОВАВА Комисията и върховния представител да продължат да

мобилизират Инструмента за съседство, сътрудничество за развитие и международно сътрудничество (ИССРМС), Инструмента за предприсъединителна помощ (ИПП III) и други финансови инструменти, като Европейския механизъм за подкрепа на мира и инициативата „Глобален портал“, за да се подкрепи засилването на устойчивостта на нашите партньори, техният капацитет за идентифициране и справяне с киберзаплахи и за разследване и наказателно преследване на киберпрестъпления, както и разработването на проекти за сътрудничество, включително в контекста на кризи, и по-специално НАСЪРЧАВА сътрудничеството с партньорите от Западните Балкани и партньорите от източното и южното съседство на ЕС, както и разполагането на експерти от ЕС и държавите членки, които да предлагат подкрепа при киберкризи, като се вземат предвид съществуващите правни мандати.

21. НАБЛЯГА, че е необходимо да се увеличат усилията за разработване на структуриран и отворен подход на ЕС за осведомяване относно начините за насърчаване на общо разбиране в световен мащаб за прилагането на международното право в киберпространството, относно рамката на ООН за отговорно поведение на държавите в киберпространството, включително инициативата за програма за действие за насърчаване на отговорното поведение на държавите в киберпространството, както и относно позицията на ЕС и неговите държави членки в текущите преговори за Конвенция на ООН за престъпления в кибернетичното пространство, и като част от тези усилия ВЪЗЛАГА на върховния представител да внесе в Съвета информационен план до края на 2022 г. НАСЪРЧАВА върховния представител и службите на Комисията да използват пълноценно и систематично своите 145 делегации и да развиват редовно и ползотворно сътрудничество между тях и посолствата на държавите членки в трети държави под егидата на планираната Мрежа на ЕС за кибердипломация. ПРИЗОВАВА върховния представител да създаде до второто тримесечие на 2022 г. Мрежата на ЕС за кибердипломация, която да допринася за обмена на информация, съвместните дейности за обучение на персонала на ЕС и на държавите членки, съгласуваните усилия за изграждане на капацитет и укрепеното прилагане на рамката на ООН за отговорно поведение на държавите, както и на мерките за изграждане на доверие между държавите.

22. ИЗТЪКВА ангажимента си за по-нататъшно сътрудничество с международните организации и държавите партньори с цел постигане на напредък по споделеното разбиране на ситуацията с киберзаплахите, разработване на механизми за сътрудничество и проактивно набелязване на съвместни дипломатически ответни действия. КАТО ПРИПОМНЯ ключовите постижения на сътрудничеството между ЕС и НАТО в областта на киберсигурността в рамките на изпълнението на съвместните декларации от Варшава от 2016 г. и от Брюксел от 2018 г., при пълно зачитане на автономността и процедурите за вземане на решения на двете организации и въз основа на принципите на прозрачност, реципрочност и приобщаване, НАБЛЯГА на необходимостта от по-нататъшно засилване на киберсътрудничеството с НАТО чрез учения, обмен на информация и обмен между експерти, включително относно развитието на способностите, изграждането на капацитет за партньорите и мисиите и операциите, както и относно приложимостта на международното право и нормите на ООН за отговорно поведение на държавите в киберпространството и евентуалните координирани ответни действия в отговор на злонамерени действия в киберпространството.

V. ПРЕДОТВРАТЯВАНЕ, ЗАЩИТА И РЕАГИРАНЕ НА КИБЕРАТАКИ

23. ОТЧИТА, че киберпространството се е превърнало в място за геополитическа конкуренция и във връзка с това ИЗТЪКВА ОТНОВО, че ЕС трябва да е в състояние да реагира бързо и решително на кибератаки, например ползващи се с държавна подкрепа злонамерени действия в киберпространството, насочени срещу ЕС и неговите държави членки, поради което е необходимо да се укрепи инструментариумът на ЕС за кибердипломация и да се използват пълноценно всички негови инструменти, включително наличните политически, икономически, дипломатически, правни и стратегически инструменти за комуникация с цел предотвратяване, обезкуражаване, възпиране и реагиране на злонамерени действия в киберпространството. ПОДЧЕРТАВА, че враждебните участници трябва да са наясно, че кибератаките срещу държавите членки и институциите на ЕС ще бъдат открити на ранен етап, ще бъдат своевременно идентифицирани и ще бъдат посрещнати с всички необходими инструменти и политики. Като се основава по-специално на съдържащите се там елементи на позицията в киберпространството и на поуките, извлечени от прилагането на инструментариума за кибердипломация от неговото създаване и от учението EU CyCLES, ПРИКАНВА държавите членки и върховния представител, с подкрепата на Комисията, да работят по преработване на насоките за прилагане на инструментариума на ЕС за кибердипломация до края на първото тримесечие на 2023 г., по-конкретно като разглеждат допълнителни ответни мерки.

24. ПОДЧЕРТАВА необходимостта от редовен обмен на информация относно ситуацията с киберзаплахите в съответните органи и комитети на Съвета, като същевременно се работи редовно с частния сектор и въз основа на оценката на въздействието и на сериозността на неотдавнашните инциденти, от повишаване на цялостната осведоменост и готовност за други приложения на инструментариума на ЕС за кибердипломация и от разработване на допълнителни инструменти в подкрепа на неговото прилагане. Въпреки че националната сигурност продължава да е отговорност единствено на отделните държави членки, ОТБЕЛЯЗВА необходимостта от засилване на обмена на разузнавателни данни и информация и на сътрудничеството между държавите членки, както и с INTCEN, така че да е възможен обменът на разузнавателна информация в началото на процеса на вземане на решения, включително по въпроса за определянето на отговорността за кибератака, и по този начин да се улесни даването на бърз, ефективен и обоснован отговор на злонамерени действия в киберпространството, насочени срещу ЕС и неговите партньори. ИЗТЪКВА ОТНОВО значението на укрепването на капацитета на INTCEN в киберпространството въз основа на доброволен принос с разузнавателни данни от държавите членки и без да се засягат техните правомощия, и на разглеждането на предложението за евентуално създаване на работна група за киберразузнаване на държавите членки.

25. КАТО ОТЧИТА, че с декларациите на ЕС и с ограничителните мерки, наложени в рамките на инструментариума на ЕС за кибердипломация, беше изпратено силно послание, че злонамерените действия в киберпространството, представляващи външна заплаха за ЕС и неговите държави членки и партньори, са неприемливи, с което се допринася за предотвратяването, обезкуражаването, възпирането и реагирането на злонамерени действия в киберпространството, ИЗТЪКВА ОТНОВО ангажимента си да използва тези мерки с цел да припомни задълженията, които се прилагат за киберпространството съгласно международното право, включително Устава на ООН в неговата цялост, и да популяризира рамката на ООН за отговорно поведение на държавите в киберпространството, включително задължението, което имат всички държави да не позволяват съзнателно тяхната територия да бъде използвана за неправомерни действия в международен план, при които се използват ИКТ, с оглед допълнително разработване и популяризиране на споделеното виждане на ЕС относно прилагането на международното право в киберпространството. КАТО ОТБЕЛЯЗВА, че подходящите и бързи послания намаляват рисковете от ескалация и могат да обезкуражат онези, които атакуват европейски интереси, ПРИКАНВА върховния представител да разработи и представи на държавите членки съгласувана комуникационна стратегия относно използването на инструментариума на ЕС за кибердипломация.

26. НАСЪРЧАВА разработването на постепенни, целенасочени и устойчиви подходи и ответни действия по отношение на злонамерените действия в киберпространството, като се използва широкият набор от инструменти, предоставени от дипломатическия инструментариум на ЕС в киберпространството, включително режима на ЕС за киберсанкции, и като се предвиждат допълнителни мерки. НАБЛЯГА, че е необходимо да се увеличат възможностите за мобилизиране, в зависимост от конкретния случай, на всички налични инструменти, вътрешни и външни, с цел предотвратяване, обезкуражаване, възпиране и реагиране на кибератаки, като те се прилагат чрез бърз, ефективен, постепенен, целенасочен и устойчив подход, основан на дългосрочен стратегически ангажимент. ПРИЗОВАВА върховния представител, в сътрудничество с Комисията, да набележи евентуални съвместни ответни действия на ЕС срещу кибератаките, включително опции за налагане на санкции, в целия спектър, за да има готовност за предприемане на бързи и ефективни действия, когато е необходимо, и да ги представи на Съвета до края на първото тримесечие на 2023 г.

27. Като отбелязва, че киберотбраната е преди всичко национална отговорност, НАСЪРЧАВА държавите членки да доразвият своите способности за провеждане на операции за киберотбрана, включително проактивни мерки с цел защита, откриване, отбрана и възпиране на кибератаки, евентуално в подкрепа на други държави членки и ЕС. Всяка държава членка се насърчава да засили, когато е необходимо, своите способности за предоставяне и получаване на помощ и съдействие. НАБЛЯГА, че по-нататъшното развитие на тези способности следва да бъде една от ключовите цели на предстоящата политика на ЕС относно киберотбраната. ОТБЕЛЯЗВА, че в политиката на ЕС относно киберотбраната следва да се обърне повече внимание на ролята, която съответните институции и органи на ЕС могат да играят за засилването на сътрудничеството между съответните участници от ЕС и от държавите членки в областта на киберотбраната и за развиването на собствения им капацитет съгласно съответните им мандати. ПРИКАНВА върховния представител, заедно с Комисията, да допринесе за разработването на позицията на ЕС в киберпространството, като през 2022 г. представи предложение за политика на ЕС относно киберотбраната, което ще проправи пътя за по-нататъшното развитие от Съвета на позицията на ЕС в киберпространството.

28. НАБЛЯГА на необходимостта от увеличаване на оперативната съвместимост и на обмена на информация чрез сътрудничество между военните екипи за незабавно реагиране при компютърни инциденти (milCERT). ПРИКАНВА държавите членки да създадат, въз основа на работата на Европейската агенция по отбрана (EDA), мрежа MilCERT за развитие на сътрудничеството и улесняване на обмена на информация, което би спомогнало също така за насърчаване на координацията с други киберобщности, както и мрежа от военни киберкомандири, с цел да се засили стратегическото сътрудничество между компетентните за киберпространството командвания на държавите — членки на ЕС, или други съответни органи. Създаването на тези мрежи, заедно с проектите относно киберпространството по линия на ПСС, ще допринесе за укрепване на киберотбраната на равнището на ЕС. ИЗТЪКВА значението на сътрудничеството между предложената мрежа milCERT и вече съществуващата мрежа от граждански екипи за реагиране при инциденти с компютърната сигурност (CSIRT) за засилването на обмена на информация и подобряването на ситуационната осведоменост.

29. Въз основа на Военната визия и стратегия на ЕС относно киберпространството като област на операции и като взема под внимание текущото разработване на военната концепция за киберотбраната за ръководените от ЕС военни операции и мисии, ИЗТЪКВА ОТНОВО необходимостта от интегриране на кибернетичното измерение в планирането и провеждането на мисии и операции по линия на ОПСО, включително чрез укрепване на техните киберспособности, и ИЗТЪКВА, че това ще допринесе за по-добра осведоменост за ситуацията в киберпространството на равнище ЕС.

30. В заключение ОТБЕЛЯЗВА, че позицията в киберпространството ще бъде стъпка към установяването на доктрина на ЕС за действие в киберпространството въз основа на повишена устойчивост, способности и опции за реагиране, както и на споделено виждане относно прилагането на международното право в киберпространството. Съветът ЩЕ РАЗГЛЕДА постигнатия напредък по изпълнението на настоящите заключения през 2023 г., за да се гарантира по-нататъшното развитие на позицията на ЕС в киберпространството.