Съвет на
Европейския съюз

Брюксел, 9 март 2021 г.
(OR. en)

6722/21

CYBER 55	RECH 86
JAI 227	COMPET 151
JAIEX 23	IND 52
EJUSTICE 25	COTER 25
COSI 39	ENFOPOL 80
DATAPROTECT 54	COPS 79
COPEN 103	MI 136
TELECOM 88	IXIM 43
PROCIV 21	POLMIL 25
CSC 85	HYBRID 10
CIS 35	CSCI 34
RELEX 168	POLGEN 33

БЕЛЕЖКА ПО ТОЧКИ I/A

От:	Генералния секретариат на Съвета
До:	Комитета на постоянните представители/Съвета
Относно:	Проект за заключения на Съвета относно стратегията на ЕС за киберсигурност за цифровото десетилетие

1. На 16 декември 2020 г. Комисията и върховният представител на Съюза по въпросите на външните работи и политиката на сигурност публикуваха съвместно съобщение до Европейския парламент и Съвета „Стратегия на ЕС за киберсигурност за цифровото десетилетие“[1]. Целта на новата стратегия за киберсигурност е да се засили колективната устойчивост на Европа срещу киберзаплахи и да се гарантира, че всички граждани и предприятия могат да се възползват в пълна степен от надеждни и заслужаващи доверие услуги и цифрови инструменти.

[1] Док. 14133/20.

2. Комисията и ЕСВД представиха съвместното съобщение по време на неформалните видеоконференции на Хоризонталната работна група по въпроси на кибернетичното пространство (HWPCI) на 17 декември 2020 г. и 12 януари 2021 г. На неформалната видеоконференция на HWPCI на 17 декември 2020 г. встъпващото португалско председателство обяви намерението си да изготви проект за заключения на Съвета относно стратегията на ЕС за киберсигурност за цифровото десетилетие.

3. Председателството представи първия проект за заключения на Съвета на неформалната видеоконференция на HWPCI на 2 февруари 2021 г. Впоследствие тези заключения бяха обсъдени на неформалните видеоконферентни заседания на HWPCI, които се проведоха на 9 и 19 февруари 2021 г. и на 1 и 9 март 2021 г.

4. Тъй като проектът за заключения съдържа и позоваване на политиките на ЕС за отбрана (точка 30), Политико-военната група обсъди съответната точка на заседанието си от 10 февруари 2021 г.

5. Различни точки от заключенията се отнасят до общата външна политика и политика на сигурност (точки 1, 4, 7, 8, 9, 20, 23, 24, 26, 27, 28, 29, 30, 31, 32 и 33), поради което бяха представени на Комитета по политика и сигурност и съответно одобрени на заседанието му от 4 март 2021 г.

6. На неформалната си видеоконференция от 9 март 2021 г. HWPCI постигна съгласие по проекта за заключения на Съвета, изложен в док. 6722/21.

7. В контекста на изложеното по-горе Комитетът на постоянните представители се приканва да представи на Съвета поместения в приложението проект за заключения на Съвета и да предложи на Съвета да приеме този проект за заключения като точка А от дневния си ред.

ПРИЛОЖЕНИЕ

Проект за заключения на Съвета относно стратегията на ЕС за киберсигурност за цифровото десетилетие

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“[2],

– управлението на интернет[3],

– съвместното съобщение от 20 ноември 2017 г. до Европейския парламент и Съвета: „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“[4],

– капацитета за киберсигурност и изграждането на способности в ЕС[5],

– значението на 5G за европейската икономика и необходимостта от смекчаване на рисковете за сигурността, свързани с 5G[6],

– бъдещето на една високо цифровизирана Европа след 2020 г.: „Стимулиране на цифровата и икономическата конкурентоспособност в Съюза и цифровото сближаване“[7],

– допълнителните усилия за укрепване на устойчивостта на хибридни заплахи и за борба с тях[8],

– изграждането на цифровото бъдеще на Европа[9],

---

2 Док. 12109/13.
3 Док. 16200/14.
4 Док. 14435/17 + COR 1.
5 Док. 7737/19.
6 Док. 14517/19.
7 Док. 9596/19.
8 Док. 14972/19.
9 Док. 8711/20.

– цифровата дипломация[10],

– укрепване на устойчивостта и борба с хибридните заплахи, включително дезинформацията в контекста на пандемията от COVID-19[11],

– кибердипломацията[12],

– координирана реакция на ЕС при мащабни инциденти и кризи в областта на киберсигурността[13],

– рамка за съвместен дипломатически отговор на ЕС срещу злонамерени действия в киберпространството („инструментариум за кибердипломация“)[14],

– насоките на ЕС за изграждане на външен киберкапацитет[15],

– възстановяване, осигуряващо напредък в прехода към една по-динамична, по-издръжлива и по-конкурентоспособна европейска промишленост[16],

– киберсигурността на свързаните устройства[17],

– укрепването на отбранителната способност на Европа срещу кибератаки и изграждането на конкурентен и иновативен сектор на киберсигурността[18],

– Резолюцията на Съвета относно криптирането – Сигурност чрез криптиране и въпреки него[19],

---

10 Док. 12804/20.
11 Док. 14064/20.
12 Док. 6122/15 + COR 1.
13 Док. 10086/18.
14 Док. 10474/17.
15 Док. 10496/18.
16 Док. 13004/20.
17 Док. 13629/20.
18 Док. 14540/16.
19 Док. 13084/1/20 REV 1.

– Декларацията на държавите членки от 15 октомври 2020 г. относно изграждането на облак от следващо поколение за предприятията и публичния сектор в ЕС,

КАТО ПРИПОМНЯ заключенията на Европейския съвет от 1–2 октомври 2020 г., които включват въпроси, свързани с COVID-19, единния пазар, промишлената политика, цифровите технологии и външните отношения[20], както и заключенията на Европейския съвет от 20 юни 2019 г., в които се разглеждат дезинформацията и хибридните заплахи и нова стратегическа програма за периода 2019–2024 г.[21],

КАТО ПРИПОМНЯ публикуваната на 28 юни 2016 г. глобална стратегия за външната политика и политика на сигурност на Европейския съюз – обща визия, общи действия: по-силна Европа,

КАТО ПРИПОМНЯ съобщенията на Европейската комисия от 19 декември 2020 г. „Изграждане на цифровото бъдеще на Европа“[22] и от 24 юли 2020 г. относно Стратегията на ЕС за Съюза на сигурност[23],

КАТО ПРИПОМНЯ съвместното съобщение на Европейската комисия и на върховния представител от 2 декември 2020 г. „Нова програма на ЕС и САЩ за глобална промяна“[24],

1. ИЗТЪКВА факта, че киберсигурността е изключително важна за изграждането на устойчива, екологична и цифрова Европа, и ПРИВЕТСТВА съвместното съобщение до Европейския парламент и Съвета „Стратегия на ЕС за киберсигурност за цифровото десетилетие“, в което се очертава новата рамка за действия на ЕС в областта „Устойчивост, технологичен суверенитет и лидерство“ и за защита на неговите граждани, предприятия и институции срещу киберинциденти и заплахи при повишаване на доверието на хората и организациите в способността на ЕС да насърчава изграждането на сигурни и надеждни мрежи и информационни системи, инфраструктура и свързаност, и да насърчава и защитава глобално, отворено, свободно, стабилно и сигурно киберпространство, което се основава на човешките права, основните свободи, демокрацията и принципите на правовата държава.

---

20 Док. EUCO 13/20.
21 Док. EUCO 9/19.
22 COM(2020) 67 final (19.2.2020 г.).
23 COM(2020) 605 final (24.7.2020 г.).
24 JOIN(2020) 22 final (2.12.2020 г.).

2. ОТЧИТА, че пандемията от COVID-19 изведе на преден план в нашето ежедневие по-голямата необходимост от доверие в инструментите и системите на информационните и комуникационните технологии (ИКТ) и тяхната сигурност. ПОДЧЕРТАВА, че киберсигурността и глобалният и отворен интернет са изключително важни за функционирането на публичната администрация и институции и на национално равнище, и на равнище ЕС, както и за нашето общество и икономика като цяло.

3. ПОДЧЕРТАВА, че е необходимо на равнището, на което се вземат политически и стратегически решения, да се повиши осведомеността по въпросите на киберпространството, като на отговорните за вземането на решения се предоставят необходимите знания и информация, и ИЗТЪКВА нуждата от повишаване на осведомеността на широката общественост и насърчаване на киберхигиена.

4. ПРИЗОВАВА да се утвърждават и защитават основните ценности на ЕС — демокрацията, принципите на правовата държава, правата на човека и основните свободи, включително правото на свободно изразяване на мнение и на информация, свободата на събранията и сдруженията и правото на неприкосновеност на личния живот в киберпространството. Във връзка с това ПРИВЕТСТВА продължаването на постоянните усилия за закрила на правозащитниците, гражданското общество и академичните среди, работещи по въпроси като киберсигурност, защита на личните данни, наблюдение и цензура онлайн, като се предоставят допълнителни практически насоки, насърчават се най-добрите практики и се активизират усилията на ЕС за предотвратяване на нарушенията и погазването на човешките права и злоупотребите с нововъзникващи технологии, по-специално чрез използване на дипломатически мерки, когато е необходимо, както и чрез контрол върху износа на такива технологии. В този контекст ИЗТЪКВА значението на Плана за действие на ЕС относно правата на човека и демокрацията за периода 2020—2024 г. и Насоките на ЕС в областта на правата на човека относно свободата на изразяване онлайн и офлайн.
5. ИЗТЪКВА, че постигането на стратегическа автономност, като същевременно се запазва отворената икономика, е ключова цел на Съюза с оглед самоопределяне на неговия икономически път и интереси. Това включва укрепване на способността да се вземат автономни решения в областта на киберсигурността с цел утвърждаване на водещите позиции на ЕС в сферата на цифровите технологии и повишаване на неговия стратегически капацитет. ПРИПОМНЯ, че това предполага идентифицирането и намаляването на стратегическите зависимости и укрепването на издръжливостта в най-чувствителните промишлени екосистеми и конкретни области. ПОДЧЕРТАВА, че това може да включва диверсифициране на веригите за производство и доставка, насърчаване и привличане на инвестиции и производство в Европа, проучване на алтернативни решения и кръгови модели и насърчаване на широко промишлено сътрудничество между държавите членки.

6. Като се има предвид недостигът на умения на работната сила в областта на цифровите технологии и киберсигурността, ИЗТЪКВА, че за да се постигне киберсигурна цифровизация на обществото, е важно да се удовлетвори търсенето на квалифицирана работна сила в областта на цифровите технологии и киберсигурността, по-специално посредством развитие, задържане и привличане на най-талантливите, например чрез образование и обучение. НАСЪРЧАВА по-голямото участие на жените и момичетата в образованието в областта на науките, технологиите, инженерството, математиката (НТИМ) и повишаването на квалификацията и преквалификацията в областта на цифровите умения на работните места в сферата на ИКТ като един от инструментите за преодоляване на неравенство между половете в областта на цифровите технологии.

7. 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 ОТНОВО ангажимента си за уреждане на международните спорове в киберпространството с мирни средства и че всички дипломатически усилия на ЕС следва приоритетно да бъдат насочени към насърчаване на сигурността и стабилността в киберпространството чрез засилено международно сътрудничество и към намаляване на риска от погрешни представи, ескалация на напрежението и конфликти, които могат да възникнат след инциденти в областта на ИКТ, и ПОДКРЕПЯ по-нататъшното развитие и оперативното прилагане на мерки за изграждане на доверие на регионално и международно равнище. ИЗТЪКВА ОТНОВО призива на Общото събрание на ООН, договорен с консенсус, при използването на ИКТ държавите — членки на ООН, да се ръководят от препоръките в докладите на групата от правителствени експерти на ООН и ПОТВЪРЖДАВА ОТНОВО прилагането в на международното право в киберпространството, по-специално на Устава на ООН в неговата цялост.

8. ПОТВЪРЖДАВА ОТНОВО, че с оглед на съдържателното оформяне на международните норми и стандарти в областта на нововъзникващите технологии и техническата и логическата инфраструктура, която е от съществено значение за общата наличност и интегритета на обществения ядро на интернет, така че те да съответстват на универсалните ценности и ценностите на ЕС и да се прилага подход с участието на множество заинтересовани страни, по-нататъшното разработване на норми и стандарти в рамките на Съюза е от съществено значение. Това ще гарантира, че интернет ще остане глобален, отворен, свободен, стабилен и сигурен, както и че при използването и развитието на цифровите технологии се зачитат правата на човека и че тяхното използване е законосъобразно, безопасно и етично. ВЗЕМА ПОД ВНИМАНИЕ предстоящата стратегия за стандартизация и СЕ АНГАЖИРА с проактивни и координирани информационни дейности за утвърждаване на водещите позиции на ЕС и неговите цели на международно равнище, включително в рамките на различни международни органи по стандартизация и чрез сътрудничество с партньори със сходни възгледи, гражданското общество, академичните среди и частния сектор.

9. КАТЕГОРИЧНО ПОДКРЕПЯ многостранния модел за управление на интернет и киберсигурност и се ангажира с укрепването на редовния и структуриран обмен със заинтересованите страни, включително частния сектор, академичните среди и гражданското общество, в рамките на международни форуми, включително в контекста на Парижкия призив за доверие и сигурност в киберпространството. НАСЪРЧАВА универсален, финансово приемлив и равноправен достъп до интернет, чрез който да се преодолее цифровото разделение, и по-специално овластяването на жените и момичетата и на хората в уязвимо или маргинализирано положение, както при разработването на политики, така и при използването на интернет.

10. АКЦЕНТИРА върху необходимостта през следващите години киберсигурността да стане част от инвестициите и инициативите в цифровата сфера, както и върху нуждата от постепенно установяване на еднакви условия на конкуренция в областта на киберсигурността, и ОТБЕЛЯЗВА плана на Комисията за увеличаване на публичните разходи и привличане на частни инвестиции в областта на киберсигурността. ИЗТЪКВА значението на малките и средните предприятия (МСП) в екосистемата на киберсигурност и ОТЧИТА приложимите налични финансови инструменти, чрез които да се способства за по-силен акцент върху киберсигурността при цифровата трансформация за периода на многогодишната финансова рамка (МФР) 2021—2027 г., както и по линия на Механизма за възстановяване и устойчивост.

11. ОЧАКВА бързото прилагане на Регламента за създаване Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и на мрежа от национални координационни центрове, включително бързото създаване и започване на дейността на Европейския експертен център в областта на киберсигурността в Букурещ. Бързото приемане на програмата му ще допринесе да се постигне максимално въздействие на инвестициите за укрепване на водещите позиции на Съюза и неговата стратегическа автономност в областта на киберсигурността, за подпомагане на технологичния капацитет и технологичните умения и за повишаване на глобалната конкурентоспособност на Съюза с принос от промишления сектор и академичната общност в областта на киберсигурността, включително МСП и научноизследователските центрове, които ще могат да се възползват от по-систематично, приобщаващо и стратегическо сътрудничество, като се има предвид сближаването в рамките на Съюза и на всички негови държави членки.

12. ПРИВЕТСТВА текущата работа под ръководството на Агенцията на Европейския съюз за киберсигурност (ENISA) и съвместно с държавите членки и заинтересованите страни, която е насочена към предоставяне на ЕС на схеми за сертифициране на ИКТ продукти, услуги и процеси, които следва да допринесат за повишаване на цялостното ниво на киберсигурност в рамките на цифровия единен пазар. Във връзка с това ОЧАКВА непрекъсната работна програма на Съюза с оглед на разработването на схеми на ЕС за сертифициране на киберсигурността в рамките на Акта за киберсигурността. ОТЧИТА в този контекст ключовата роля на ЕС за разработването на стандарти, които могат да оформят ситуацията в областта на киберсигурността и които способстват да се гарантира лоялна конкуренция в рамките на ЕС и в глобален мащаб, да се насърчи достъпът до пазара, както и да се преодолеят рисковете за сигурността, като същевременно се осигури приложимостта на законодателната рамка на ЕС.

13. ИЗТЪКВА ОТНОВО, че е важно да се оцени необходимостта от хоризонтално законодателство, като се определят и необходимите условия за пускането на пазара, за да бъдат обхванати в дългосрочен план всички съответни аспекти на киберсигурността на свързаните устройства, като например наличност, интегритет и поверителност. Във връзка с това ПРИВЕТСТВА дискусията за проучване на обхвата на това законодателство и връзките му с рамката за сертифициране на киберсигурността, както е определена в Акта за киберсигурността, с цел повишаване на нивото на сигурност в рамките на цифровия единен пазар. ПОДЧЕРТАВА, че изискванията за киберсигурност следва да бъдат определени в съответствие с приложимото законодателство на Съюза, включително Акта за киберсигурността, новата законодателна рамка, Регламента за европейската стандартизация и евентуалното бъдещо хоризонтално законодателство, за да се избегнат неяснотата и разпокъсаността в законодателството.

14. ОТЧИТА, че е важно в рамките на Съюза да се възприеме всеобхватен и хоризонтален подход към киберсигурността, при пълно зачитане на компетентностите и потребностите на държавите членки, както и че е важно да продължи да се осигурява подкрепа за техническото подпомагане и сътрудничеството за изграждане на капацитета на държавите членки. Като отчита динамичния характер на ситуацията, свързана с киберзаплахите, ВЗЕМА ПОД ВНИМАНИЕ новото предложение за директива относно мерки за високо общо ниво на киберсигурност в Съюза, която се базира на директивата за мрежовата и информационна сигурност, и изразява отново своята подкрепа за укрепването и хармонизирането на националните рамки за киберсигурност и за трайно сътрудничество между държавите членки. Освен това ИЗТЪКВА необходимостта от хармонизация и формулиране на секторното законодателство в тази област.

15. ВЗЕМА ПОД ВНИМАНИЕ предложението на Комисията за подпомагане на държавите членки при създаването и укрепването на центрове за операции по сигурността с цел изграждане на мрежа от такива центрове в целия ЕС, за да се осигури допълнително наблюдение и предвиждане на сигналите за атаки срещу мрежи. В този контекст ОЧАКВА подробните планове на Комисията за мрежата от центрове за операции по сигурността при зачитане на компетенциите на държавите членки. ПРИПОМНЯ усилията, предприети от държавите членки и подкрепяни от ЕС, за създаване на секторни, национални и регионални екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) и национални или европейски центрове за споделяне и анализ на информация (ISAC) като част от ефективна мрежа от партньорства в областта на киберсигурността в Съюза. ОЧАКВА да се проучи потенциалът на тази мрежа за укрепване на центровете за операции по сигурността, както и тяхната допълняемост и координация със съществуващите мрежи и участници (най-вече мрежата ЕРИКС), за да се насърчи ефективна, сигурна и надеждна култура на споделяне на информация. ИЗТЪКВА, че този процес ще се основава на работата, извършена в контекста на инициативите в областта на изкуствения интелект и високопроизводителните изчислителни технологии и от европейските цифрови иновационни центрове.

16. ВЗЕМА ПОД ВНИМАНИЕ възможното разработване на сигурна система за свързаност, която се основава на европейската квантова комуникационна инфраструктура (EuroQCI) и на правителствените сателитни комуникации на Европейския съюз (GOVSATCOM), и ОТЧИТА факта, че всяко евентуално бъдещо развитие следва да се основава на стабилна рамка за киберсигурност и да отразява цялата инфраструктура за електронна комуникация, като например космическите, наземните и подводните мрежови системи.

17. ОЧАКВА обсъжданията с Комисията, ENISA, двата оператора на базови DNS сървъри в ЕС и множеството заинтересовани страни, за да се анализира ролята на операторите за гарантиране, че достъпът до интернет ще бъде осигурен и занапред в световен мащаб и няма да бъде разпокъсан. ПРИВЕТСТВА по-нататъшните обсъждания във връзка с намерението на Комисията да разработи алтернативна европейска услуга за достъп до световния интернет (инициатива DNS4EU), която ще се основава на прозрачен модел, ще отговаря още от етапа на проектиране и по подразбиране на най-новите стандарти и правила в областта на сигурността, защитата на данните и неприкосновеността на личния живот, за да се способства за постигане на по-голяма устойчивостта, като същевременно се поддържа и подобрява международната свързаност за всички държави членки.

18. ОТЧИТА необходимостта от съвместни усилия от страна на Комисията и държавите членки за ускоряване на въвеждането на ключови интернет стандарти, включително IPv6, и утвърдени стандарти за сигурност в интернет, тъй като те са от основно значение за повишаване на общото ниво на сигурност, устойчивост, откритост и оперативна съвместимост на глобалния интернет, като едновременно с това повишават конкурентоспособността на европейския сектор, и по-специално на операторите на интернет инфраструктура.

19. ПОДЧЕРТАВА, че е важно да се възприеме координиран подход, както и да се разработят и прилагат ефективни мерки на национално равнище за укрепване на киберсигурността на 5G мрежите. ПОДКРЕПЯ следващите стъпки, които трябва да бъдат предприети по отношение на киберсигурността на 5G мрежите, представени в допълнението към Стратегията на ЕС за киберсигурност, и въз основа на резултатите от доклада относно въздействието на препоръката на Комисията върху сигурността на 5G мрежите, например по отношение на определянето на дългосрочен и всеобхватен подход, обхващащ цялата верига за създаване на стойност и екосистемата на технологията 5G. С оглед на по-нататъшното укрепване на координирания подход към сигурността на 5G мрежите, НАСТОЙЧИВО ПРИКАНВА държавите членки, институциите на ЕС и другите заинтересовани страни да продължат да правят периодичен преглед, съпроводен от обмен на информация и най-добри практики, в рамките на специалното работно направление за киберсигурност на 5G на групата за сътрудничество за МИС и редовно да докладват на Съвета за постигнатия напредък. ПОДЧЕРТАВА, като акцентира върху отговорността на държавите членки за защита на националната сигурност, твърдия си ангажимент за въвеждане и бързо приключване на изпълнението на мерките във връзка с инструментариума на ЕС за 5G и за продължаване на усилията за гарантиране на сигурността на 5G мрежите и развитието на бъдещите поколения мрежи. Тясното сътрудничество между държавите членки, Комисията и ENISA в областта на сигурността на 5G мрежите би могло да послужи като пример за други въпроси в областта на киберсигурността, като същевременно се зачитат компетенциите на държавите членки и принципите на субсидиарност и пропорционалност.

20. ОТЧИТА значението на по-нататъшното интегриране на киберсигурността в механизмите на ЕС за реакция при кризи и тестването им в съответните учения и ИЗТЪКВА, че е важно да се засилят сътрудничеството и обменът на информация между различните киберобщности в рамките на ЕС и да се свържат съществуващите инициативи, структури и процедури (като интегрираните договорености на ЕС за реакция на политическо равнище при кризи, мрежата ЕРИКС, групата за сътрудничество за МИС, мрежата CyCLONe, Европейския център за борба с киберпрестъпността, Центъра на ЕС за анализ на информация (INTCEN) и други компетентни органи на ЕС) в случай на мащабни и трансгранични киберинциденти и заплахи. КАТО ВЗЕМА ПРЕДВИД вече постигнатия напредък в тази област, ОЧАКВА предложението на Комисията относно процеса, етапите и сроковете за определяне на мандата на съвместното звено за киберсигурност, с цел да се осигури добавена стойност, ясна насоченост и рационализиране на рамката на ЕС за управление на кризи в областта на киберсигурността, включително чрез подготвеност, споделена ситуационна осведоменост, засилване на координираната реакция и учения по прозрачен и поетапен начин, като същевременно се избягва дублирането и припокриването и се зачитат компетенциите на държавите членки.

21. ПОДЧЕРТАВА, че е важно, от една страна, да се насърчават сътрудничеството и обменът на информация между съответните участници в областта на киберсигурността и компетентните органи в сферата на сигурността и наказателното правосъдие, например правоприлагащите и съдебните органи, а от друга, че е необходимо да се разшири и подобри капацитетът на тези органи за разследване и наказателно преследване на киберпрестъпността и да се насърчават международните преговори и правилата на ЕС относно трансграничния достъп до електронни доказателства. Независимо от днешната технологична среда, от съществено значение е да се запазят правомощията на компетентните органи в областта на сигурността и наказателното правосъдие чрез законен достъп за изпълнение на техните задачи, както е предвидено и разрешено от закона. Такива закони, предвиждащи правомощия за правоприлагане, трябва винаги изцяло да зачитат правото на справедлив процес и другите гаранции, както и основните права, по-специално правото на зачитане на личния живот и комуникациите и правото на защита на личните данни.

22. ПОТВЪРЖДАВА ОТНОВО подкрепата си за разработването, прилагането и използването на стабилно криптиране като необходимо средство за защита на основните права и цифровата сигурност на физическите лица, правителствата, промишления сектор и обществото и същевременно ПРИЗНАВА необходимостта да се гарантира, че компетентните органи в областта на сигурността и наказателното правосъдие, например правоприлагащите и съдебните органи, могат да упражняват своите законни правомощия – както онлайн, така и офлайн, за да защитават нашите общества и граждани Компетентните органи трябва да имат достъп до данните по законен и целенасочен начин, при пълно зачитане на основните права и съответните закони за защита на данните, като същевременно утвърждават киберсигурността. ИЗТЪКВА, че всички предприети действия трябва внимателно да балансират тези интереси с принципите на необходимост, пропорционалност и субсидиарност.

23. ПОДКРЕПЯ и ПОПУЛЯРИЗИРА Конвенцията от Будапеща за престъпления в кибернетичното пространство и текущата работа по Втория допълнителен протокол към тази конвенция. Освен това продължава да участва в многостранния обмен по въпросите на киберпрестъпността, включително в процеси, свързани със Съвета на Европа, Службата на ООН по наркотиците и престъпността (СНПООН) и Комисията по предотвратяване на престъпленията и наказателно правосъдие (CCPCJ), за да се гарантира засилено международно сътрудничество за противодействие на киберпрестъпността, включително обмен на най-добри практики и технически знания и подкрепа за изграждането на капацитет, като същевременно се зачитат, утвърждават и защитават правата на човека и основните свободи.

24. Въпреки че националната сигурност остава единствено в рамките на отговорността на всяка държава членка, ОТЧИТА значението на стратегическото сътрудничество в областта на разузнаването в сферата на киберзаплахите и дейностите в киберпространството и ПРИКАНВА държавите членки, чрез своите компетентни органи, да продължат да допринасят за работата на EU INTCEN в качеството му на център на ЕС за ситуационна осведоменост и оценки на заплахите по свързани с киберпространството въпроси и да проучат предложението за евентуално създаване на работна група на държавите членки за киберразузнаване с цел укрепване на специализирания капацитет на INTCEN в тази област, въз основа на доброволен принос от държавите членки в областта на разузнаването и без да се засягат техните компетенции.

25. ПОДЧЕРТАВА значението на солидна и съгласувана рамка за сигурност, която да защитава целия персонал на ЕС, данните, комуникационните мрежи и информационните системи и процесите на вземане на решения, въз основа на всеобхватни, последователни и еднородни правила. По-специално, това следва да се постигне чрез повишаване на устойчивостта и подобряване на културата на сигурност на ЕС по отношение на киберзаплахи и чрез повишаване на сигурността на класифицираните и некласифицираните мрежи на ЕС, като същевременно се гарантира подходящо управление и осигуряване на достатъчно ресурси и капацитет, включително в контекста на укрепването на мандата на екипа за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на ЕС (CERT-EU). Във връзка с това ПРИВЕТСТВА текущите дискусии относно установяването на общи правила за сигурност на информацията при надлежно отчитане на правилата за сигурност на Съвета за защита на класифицираната информация на ЕС, както и дефинирането на общи задължителни правила относно киберсигурността за всички институции, органи и агенции на ЕС.

26. КАТО СЕ ОСНОВАВА на усилията на ЕС в областта на кибердипломацията, СЕ АНГАЖИРА да повиши ефективността и ефикасността на инструментариума за кибердипломация и ОЧАКВА задълбочаването на обсъжданията относно неговия обхват и използване, въз основа на поуките, извлечени от прилагането на този инструмент до момента. Тези обсъждания следва да допринесат за насърчаване на сигурността на международно равнище чрез стимулиране на диалога и формирането на споделена визия по въпросите на киберсигурността, укрепване на превенцията, стабилността, сътрудничеството и повишаването на доверието и изграждането на капацитет и, когато е необходимо, чрез прилагане на ограничителни мерки, с цел предотвратяване, обезсърчаване, възпиране и реагиране на злонамерени действия в киберпространството, насочени срещу интегритета и сигурността на ЕС и неговите държави членки, като по този начин се допринесе за международната сигурност и стабилност и се консолидира позицията на ЕС в киберпространството, при пълно зачитане на националните компетенции и прерогативи. По-специално, следва да се обърне специално внимание на предотвратяването и противодействието на кибератаки със системни последици, които биха могли да засегнат нашите вериги на доставки, критичната инфраструктура и основните услуги, демократичните институции и процеси и да подкопаят нашата икономическа сигурност, включително кражби на интелектуална собственост, извършвани чрез киберметоди. Държавите членки и институциите на ЕС следва допълнително да обмислят съгласуването на рамката на ЕС за управление на кризи в областта на киберсигурността, инструментариума за кибердипломация и разпоредбите на член 42, параграф 7 от ДЕС и член 222 от ДФЕС, по-специално, като разработят сценарии за изграждане на общо разбиране за практическите условия за прилагането на член 42, параграф 7 от ДЕС.

27. ПРИЗНАВА, че е важно да се засили сътрудничеството с международни организации и държави партньори, за да се постигне напредък в общото разбиране на ситуацията, свързана с киберзаплахите, да се развие диалог и да се разработят механизми за сътрудничество, да се установят по целесъобразност съвместни дипломатически ответни действия, както и да се подобри обменът на информация, включително чрез образование, обучение и учения. По-специално ИЗТЪКВА, че стабилното трансатлантическо партньорство в областта на киберсигурността допринася за общата ни сигурност, стабилност и просперитет, и ОТБЕЛЯЗВА разпоредбите относно сътрудничеството в областта на киберсигурността, предвидени в Споразумението за търговия и сътрудничество между ЕС и Обединеното кралство. КАТО ПРИПОМНЯ основните постижения на сътрудничеството между ЕС и НАТО в областта на киберсигурността в рамките на изпълнението на съвместните декларации, подписани съответно във Варшава през 2016 г. и в Брюксел през 2018 г., отново изтъква значението на засиленото, взаимно укрепващо и ползотворно сътрудничество чрез образование, обучение, учения и координирана реакция срещу злонамерени действия в киберпространството, при пълно зачитане на самостоятелното вземане на решения и процедурите на двете организации, въз основа на принципите на прозрачност, реципрочност и приобщаване.

28. С цел да се допринесе за глобално, отворено, свободно, стабилно и сигурно киберпространство, което е от все по-голямо значение за трайния просперитет, растеж, сигурност, благоденствие, свързаност и интегритет на нашите общества, СЕ АНГАЖИРА да продължи да участва в процесите на нормотворчество в международните организации, по-специално в процесите, свързани с Първия комитет на ООН, като насърчава и допринася за признаване на прилагането на международното право в киберпространството и придържането към нормите, правилата и принципите на отговорно поведение на държавите в киберпространството, включително чрез насърчаване на бързото създаване на програма за действие за насърчаване на отговорното поведение на държавите в киберпространството, като конструктивни, приобщаващи и основани на консенсус последващи действия в контекста на текущите процеси в рамките на групата от правителствени експерти към ООН (UN GGE) и на Отворената работна група (OEWG).

29. ПРИПОМНЯ категоричната си ангажираност за ефективно многостранно сътрудничество и основан на правила световен ред, в центъра на който стои ООН, и решимостта си да засили сътрудничеството и координацията с международни и регионални организации, а именно системата на ООН, НАТО, Съвета на Европа, ОССЕ, ОИСР, Африканския съюз, ОАД, АСЕАН, Регионалния форум на АСЕАН, Съвета за сътрудничество в Персийския залив и Лигата на арабските държави, във връзка с обсъжданията по въпроси, свързани с киберпространството, както и продължаването и разширяването на структурираните кибердиалози и консултации на ЕС с трети държави. ИЗТЪКВА активната си подкрепа за ООН, по-специално във връзка с Програмата до 2030 г., включително целите за устойчиво развитие, и ПРИВЕТСТВА пътната карта за сътрудничество в областта на цифровите технологии и програмата за разоръжаване, изготвени от генералния секретар на ООН, които насърчават отчетността и спазването на нормите в киберпространството и допринасят за предотвратяване и мирно уреждане на конфликти, произтичащи от злонамерени действия в киберпространството. Приветства предложението на върховния представител по въпросите на външните работи и политиката на сигурност за създаване на неформална мрежа на ЕС за кибердипломация с оглед на развиването на ангажираността и експертния опит на ЕС и на държавите членки по международни въпроси, свързани с киберпространството, с цел засилване на координираните информационни дейности.

30. ОЧАКВА предстоящото предложение за преразглеждане на политическата рамка за кибернетична отбрана (CDPF) и СЕ АНГАЖИРА да продължи да полага усилия за укрепване на измеренията, свързани с киберсигурността и киберотбраната, за да се гарантира, че те са напълно интегрирани в по-широките рамки на сигурността и отбраната, по-специално в контекста на работата по стратегическия компас. СЧИТА, че предстоящата „Военна визия и стратегия на ЕС относно киберпространството като област на операции“ ще допринесе за постигането на напредък в тези обсъждания. ПРИВЕТСТВА инициативата на Европейската агенция по отбрана (EDA) за насърчаване на сътрудничеството между военните екипи за незабавно реагиране при компютърни инциденти (CERT) и ПОДКРЕПЯ положените усилия за засилване на полезните взаимодействия и координация между гражданските и военните способности в областта на киберотбраната и киберсигурността, включително по отношение на свързаните с космическото пространство аспекти, в т.ч. чрез специалните проекти по линия на ПСС.

31. ПРИВЕТСТВА предложението за разработване на програма на ЕС за изграждане на външен киберкапацитет, предложението за създаване на Съвет на ЕС за изграждане на киберкапацитет и създаването и внедряването на Мрежа на ЕС за изграждане на киберкапацитет (CyberNet) с цел повишаване на устойчивостта и капацитета на киберпространството в световен мащаб. Във връзка с това ПРИВЕТСТВА сътрудничеството с държавите членки, както и с партньорите от публичния и частния сектор, по-специално Световния форум за експертни киберпознания (GFCE) и други международни органи, работещи в тази област, за да се осигури координация и да се избегне дублиране. По-специално НАСЪРЧАВА сътрудничеството с партньорите от Западните Балкани и региона на източното и южното съседство на ЕС.

32. За да се гарантира, че всички държави могат да се възползват от социалните, икономическите и политическите ползи на интернет и използването на технологиите, СЕ АНГАЖИРА да помогне на държавите партньори да се справят с все по-големите предизвикателства, свързани със злонамерените действия в киберпространството, по-специално тези, които вредят на развитието на техните икономики, общества и на интегритета и сигурността на демократичните системи, включително в съответствие с усилията в рамките на Плана за действие за европейската демокрация.

33. С цел да се гарантира разработването, изпълнението и наблюдението на предложенията, представени в стратегията на ЕС за киберсигурност, и като се вземе предвид многогодишният характер на някои от инициативите, НАСЪРЧАВА Комисията и върховния представител по въпросите на външните работи и политиката на сигурност да изготвят подробен план за изпълнение, в който да се определят приоритетите и графикът на планираните действия. Ще СЛЕДИ напредъка в изпълнението на настоящите заключения посредством план за действие, който ще бъде редовно преразглеждан и актуализиран от Съвета, в тясно сътрудничество с Европейската комисия и върховния представител.