ЕВРОПЕЙСКА
КОМИСИЯ

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

Брюксел, 16.12.2020 г.
JOIN(2020) 18 final

СЪВМЕСТНО СЪОБЩЕНИЕ ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Стратегия на ЕС за киберсигурност за цифровото десетилетие

СЪВМЕСТНО СЪОБЩЕНИЕ ДО ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И СЪВЕТА

Стратегия на ЕС за киберсигурност за цифровото десетилетие

I. ВЪВЕДЕНИЕ: КИБЕРСИГУРНОСТ ЗА ЦИФРОВАТА ТРАНСФОРМАЦИЯ В СЛОЖНА И НАСИТЕНА СЪС ЗАПЛАХИ ОБСТАНОВКА

Киберсигурността е неразделна част от сигурността на европейците. Независимо дали става въпрос за свързани устройства, електроенергийни мрежи, банки, въздухоплавателни средства или за публичните администрации или болници, към които хората се обръщат или посещават, те заслужават увереност, че при действията си ще бъдат защитени от киберзаплахи. Икономиката, демокрацията и обществото на ЕС зависят повече от всякога от наличието на сигурни и надеждни цифрови инструменти и свързаност. Поради това киберсигурността е от съществено значение за изграждането на устойчива, екологосъобразна и цифрова Европа.

Транспортът, енергетиката и здравеопазването, телекомуникациите, финансите, сигурността, демократичните процеси, космическото пространство и отбраната са силно зависими от мрежовите и информационните системи, които са все по-взаимосвързани. Отделните отрасли силно зависят един от друг, тъй като мрежите и информационните системи от своя страна функционират само при непрекъснатост на електроснабдяването. Свързаните устройства вече надхвърлят по брой населението на света и се очаква техният брой да нарасне до 25 милиарда до 2025 г.[1]; една четвърт от тях ще бъдат в Европа. Обвързването на моделите на работа с цифровите технологии беше ускорено под въздействието на пандемията от COVID-19, когато 40 % от работниците в ЕС преминаха към дистанционна работа, вероятно с трайно отражение върху тяхното ежедневие[2]. Това ни прави по-уязвими откъм кибератаки[3]. Потребителите често получават свързани предмети с добре известни пробойни в сигурността, което допълнително увеличава „повърхността за атака“ при злонамерени кибератаки[4]. Промишлеността в ЕС разчита все повече на цифровите технологии и интернет, което също прави потенциалните кибератаки срещу промишлеността и екосистемите по-опасни от всякога.

---

[1] Оценка на далекосъобщителната търговска асоциация GSMA; https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf). Транснационалната корпорация за данни (IDC) прогнозира 42,6 милиарда свързани машини, датчици и камери; https://www.idc.com/getdoc.jsp?containerId=prUS45213219.

[2] Според проучване от юни 2020 г. 47 % от ръководителите на предприятия са заявили, че възнамеряват да позволят на служителите си да работят дистанционно на пълно работно време, дори когато стане възможно завръщането на работното място; 82 % са възнамерявали да позволят на служителите си да работят от разстояние поне частично; https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82-percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time.

[3] https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf

[4] Една от най-опасните зловредни програми до днес, позната като „Мирай“, създава ботмрежи от над 600 000 устройства, които сриват множество големи уебсайтове в Европа и Съединените щати.

Ситуацията със заплахите се утежнява от геополитическото напрежение около глобалния и отворен интернет, както и от контрола на технологиите по цялата верига на доставки[5]. Това напрежение намира отражение в нарастващия брой национални държави, издигащи цифрови прегради. Ограниченията на и в интернет застрашават глобалното и отворено киберпространство, както и принципите на правовата държава, основните права, свободата и демокрацията, тоест основните ценности на ЕС. Киберпространството все повече се използва за политически и идеологически цели, а засиленото противопоставяне на международно равнище възпрепятства ефективното многостранно сътрудничество. Хибридните заплахи съчетават кампании за дезинформация с кибератаки срещу инфраструктура, икономически процеси и демократични институции, при които са възможни физически щети, незаконно проникване до лични данни и кражби на промишлени или държавни тайни, което сее недоверие и отслабва социалното единство. Тези дейности подриват международната сигурност и стабилност и осуетяват ползите от киберпространството за икономическото, социалното и политическото развитие.

Злонамерените атаки срещу критична инфраструктура представляват сериозен риск в световен мащаб[6]. Интернет има децентрализирана архитектура без централна структура и се управлява с участието на множество заинтересовани страни. Световната мрежа успя да понесе експоненциалното увеличение на пренасяните обеми, като същевременно беше обект на постоянни и злонамерени опити за предизвикване на сривове[7]. Едновременно с това все повече се разчита на основните функции на глобалния и отворен интернет, като например системата за имена на домейни (DNS), и на основни интернет услуги за комуникации и хостинг, приложения и данни. Тези услуги все повече се концентрират в ръцете на няколко частни дружества[8]. Това прави европейската икономика и общество уязвими при дестабилизиращи геополитически или технически събития, които засягат базисните функции на интернет или едно или повече от въпросните дружества. Интернет се използва все повече и по различни начини вследствие на пандемията, което допълнително разкри колко нестабилни са веригите на доставки, които зависят от тази цифрова инфраструктура.

[5]Включително електронни компоненти, анализ на данни, изчисления в облак, по-бързи и по-интелигентни мрежи от пето (5G) и последващи поколения, криптиране, изкуствен интелект (ИИ) и нови компютърни и надеждни парадигми за обработка на данни, като блок-веригите, изчисления от облака към периферията на мрежата и квантови изчисления.

[6]Световен икономически форум, Доклад за глобалните рискове за 2020 г.

[7]Пандемията доведе до увеличение на интернет трафика с 60 % според Организацията за икономическо сътрудничество и развитие; https://www.oecd.org/coronavirus/policy-responses/keeping-the-internet-up-and-running-in-times-of-crisis-4017c4c9/. Органът на европейските регулатори в областта на електронните съобщения и Комисията редовно публикуват доклади относно капацитета на интернет по време на мерките за изолация във връзка с коронавируса. Според доклад на ENISA общият брой на т. нар. разпределени атаки тип „отказ от обслужване“ (DDoS) се е увеличил с 241 % през третото тримесечие на 2019 г. в сравнение със същия период на 2018 г. DDoS атаките стават все по-интензивни, като най-голямата засега се случи през февруари 2020 г., като при нея пиковият трафик достигна 2,3 терабита в секунда. При „срива на CenturyLink“ през август 2020 г. проблем с маршрутизацията в американския доставчик на интернет услуги доведе до спад от 3,5 % в световния интернет трафик; https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

[8]Internet Society, The Global Internet Report: Consolidation in the Internet Economy (Интернет общество, Глобален доклад за интернет: консолидиране на интернет икономиката); https://www.internetsociety.org/blog/2019/02/is-the-internet-shrinking-the-global-internet-report-consolidation-in-the-internet-economy-explores-this-question/

Опасенията за сигурността са основен възпиращ фактор при използването на онлайн услуги[9]. Около 40 % от потребителите в ЕС са се сблъсквали с проблеми, свързани със сигурността, а 60 % не смятат, че са способни да се защитят срещу киберпрестъпността[10]. Една трета са получавали фалшиви електронни писма или телефонни обаждания с искане за лични данни през последните три години, но 83 % никога не са докладвали за киберпрестъпление. Едно от всеки осем предприятия е било обект на кибератаки[11]. Над половината от служебните или лични компютри, които са били заразени със зловреден софтуер, биват повторно заразени в рамките на една и съща година[12]. Всяка година се губят стотици милиони записи поради нарушения на сигурността на данните; средните финансови загуби на предприятие вече надхвърлят 3,5 млн. EUR през 2018 г.[13]. Последствията от кибератаките често пъти не могат да бъдат ограничени и се получават верижни реакции в икономиката и обществото като цяло, а това засяга милиони хора[14].

Разследването на почти всички видове престъпления има цифрово измерение. През 2019 г. бе докладвано, че броят на инцидентите на годишна база се е утроил. Според оценки съществуват около 700 милиона нови образци на зловреден софтуер, който е най-често срещаното средство за кибератака[15]. През 2020 г. годишните разходи за световната икономика, свързани с киберпрестъпността, се оценяват на 5,5 трилиона евро, което е два пъти повече в сравнение с 2015 г.[16]. Това е най-големият трансфер на икономическо благосъстояние в историята, който надхвърля световната търговия с наркотици. Според оценки, един сериозен инцидент — нападението със софтуера за изнудване WannaCry през 2017 г. — ощети световната икономика с над 6,5 милиарда евро[17].

Най-често обект на кибератаки са цифровите услуги и финансовият сектор, наред с публичния сектор и производството, и въпреки това както предприятията, така и физическите лица все още не са достатъчно осведомени и готови да реагират[18], а

---

[9] https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[10] Индекс за навлизането на цифровите технологии в икономиката и обществото за 2020 г.; https://ec.europa.eu/digital-single-market/en/news/digital-economy-and-society-index-desi-2020; https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[11] Съобщение за медиите на Евростат, „Мерки за сигурност в областта на ИКТ, предприети от по-голямата част от предприятията в ЕС“, 6/2020 — 13 януари 2020 г. „Кибератаките срещу жизненоважна инфраструктура са вече обичайна практика в различни отрасли като енергетиката, здравеопазването и транспорта“; WEF, The Global Risks Report 2020 (Доклад за глобалните рискове за 2020 г.).

[12] Източник: Comparitech.

[13] Annual Cost of a Data Breach Report, 2020 Ponemon Institute и въз основа на количествен анализ на 524 скорошни нарушения в 17 географски области и 17 промишлени отрасъла; https://www.capita.com/sites/g/files/nginej146/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf

[14] Доклад на Съвместния изследователски център (JRC), „Киберсигурността — нашето подсигуряване в цифровата сфера“; https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor

[15] Източник: AV-TEST, https://www.av-test.org/en/statistics/malware/

[16] Доклад на Съвместния изследователски център (JRC), „Киберсигурността — нашето подсигуряване в цифровата сфера“.

[17] Източник: Cyence.

[18] Предприятията и особено сред МСП все още не осъзнават достатъчно опасността от киберкражби на търговски тайни; PwC, Проучване за мащаба и въздействието на промишления шпионаж и кражбата на търговски тайни чрез киберсредства (The scale and impact of industrial espionage and theft of trade secrets through cyber); Доклад за разпространението на мерките за борба и предотвратяване на киберкражбите на търговски тайни, 2018 г.

сред кадрите се наблюдава сериозен недостиг на умения в областта на киберсигурността[19]. През 2019 г. бяха регистрирани почти 450 киберинцидента, свързани с европейски жизненоважни инфраструктури в областта на финансите и енергетиката[20]. Здравните структури и специалисти бяха засегнати особено тежко по време на пандемията. Тъй като технологиите са вече неразривно свързани с физическия свят, кибератаките излагат на риск живота и здравето на най-уязвимите[21]. Над две трети от дружествата, по-специално МСП, се считат за „начинаещи“ в областта на киберсигурността, а европейските дружества се считат за по-малко подготвени от дружествата в Азия и Америка[22]. В Европа приблизително 291 000 длъжности за специалисти в областта на киберсигурността остават незаети. Наемането и обучаването на експерти в областта на киберсигурността е бавен процес, което поражда по-големи рискове за киберсигурността за организациите[23].

В ЕС няма колективно възприятие на обстановката в областта на киберзаплахите. Това е така, защото националните органи не събират и не обменят систематично информация, като онази, с която разполага частният сектор и която би могла да помогне за оценката на състоянието на киберсигурността в ЕС. Само част от инцидентите се докладват от държавите членки, а обменът на информация не е нито систематичен, нито изчерпателен[24]. Кибератаките са може би само един от аспектите на съгласуваните злонамерени атаки срещу европейските общества. Понастоящем държавите членки си съдействат оперативно в ограничена степен и не съществува оперативен механизъм за взаимодействие между тях и институциите, агенциите и органите на ЕС в случай на мащабни трансгранични киберинциденти или кризи[25].

Поради това е особено важно да се подобри киберсигурността, за да могат хората да се ползват уверено и пълноценно от иновациите, мрежовата свързаност и автоматизацията, както и за да се гарантират основните права и свободи, включително правото на неприкосновеност на личния живот и на защита на личните данни, а също и свободата на изразяване на мнение и свободата на информация. Киберсигурността е абсолютно необходима за мрежовата свързаност и глобалния и отворен интернет, на които разчитаме за трансформацията на икономиката и обществото в периода 2020—2030 г. Тя допринася за по-добри и повече работни места, по-гъвкава работна среда, по-ефективен и устойчив транспорт и селско стопанство и по-лесен и по-справедлив достъп до здравни услуги. Тя играе също така

[19] Вж. ENISA, Текущи заплахи (Threat Landscape), 2020 г. Също така, доклад за 2020 г. на Verizon относно разследванията на нарушения на сигурността на данните (Verizon Data Breach Investigations Report, 2020); https://enterprise.verizon.com/resources/reports/dbir/

[20] https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

[21] Софтуер за изнудване беше използван срещу болници и хранилища на медицински досиета, например в Румъния (юни 2020 г.), Дюселдорф (септември 2020 г.) и Вастаамо (октомври 2020 г.).

[22] PwC, Състояние на информационната сигурност в глобален мащаб, (The Global State of Information Security), 2018 г.; ESI Thoughtlab, Императивът на киберсигурността (The CyberSecurity Imperative), 2019 г.

[23] Агенция на ЕС за киберсигурност, развитие на уменията в областта на киберсигурността в ЕС: Сертифицирането на образователните степени в областта на киберсигурността и базата данни на ENISA за висше образование, декември 2019 г.

[24] От държавите членки се изисква да представят на групата за сътрудничество годишен обобщен доклад относно уведомленията, получени съгласно член 10, параграф 3 от Директивата относно сигурността на мрежите и информационните системи (Директива (ЕС) 2016/1148).

[25] Въведени са стандартни оперативни процедури за взаимопомощ между членовете на мрежата на CSIRT.

съществена роля и в прехода към по-чиста енергия по линия на Европейския зелен пакт[26] чрез трансграничните мрежи и интелигентните измервателни уреди и чрез избягването на ненужното дублиране при съхранението на данни. Освен всичко, от киберсигурността зависи международната сигурност и стабилност, както и развитието на икономиките, демокрациите и обществата в световен мащаб. Затова правителствата, предприятията и гражданите трябва да използват цифровите инструменти по отговорен и съобразен със сигурността начин. Цифровите технологии преобразяват нашите ежедневни дейности и в този процес особено внимание и грижи трябва да се отделят на киберсигурността.

Новата стратегия на ЕС за киберсигурността за цифровото десетилетие е ключов елемент в стратегията за изграждане на цифровото бъдеще на Европа[27], плана на Комисията за възстановяване на Европа[28], стратегията на ЕС за Съюза на сигурност в периода 2020—2025 г.[29], глобалната стратегия за външната политика и политиката за сигурност на ЕС[30] и стратегическата програма на Европейския съвет за периода 2019—2024 г.[31]. В стратегията се посочва как ЕС ще защитава своите граждани, предприятия и институции от кибернетични заплахи, как ще развива международното сътрудничество и ще играе водеща роля в осигуряването на отворен и глобален интернет.

II. ДА МИСЛИМ ГЛОБАЛНО, ДА ДЕЙСТВАМЕ ЕВРОПЕЙСКИ

Настоящата стратегия има за цел да гарантира глобален и отворен интернет със силни предпазни механизми в отговор на рисковете за сигурността и основните права и свободи на хората в Европа. В рамките на предходни стратегии беше постигнат напредък, въз основа на който настоящата стратегия представя конкретни предложения за задействане на **три основни инструмента — регулаторен, инвестиционен и политически — засягащи три области на действие на ЕС — (1) устойчивост, технологичен суверенитет и лидерство, (2) изграждане на оперативен капацитет за предотвратяване, възпиране и реагиране и (3) постигане на напредък в създаването на световно и отворено киберпространство**. ЕС се ангажира да подкрепи тази стратегия **през следващите седем години чрез безпрецедентни инвестиции в цифровия преход на ЕС, в размер вероятно четирикратно по-голям от този на досегашните вложения**, в рамките на нови технологични и промишлени политики и програмата за възстановяване[32].

Киберсигурността трябва да стане част от всички тези инвестиции в цифровата сфера, особено при ключови технологии като изкуствения интелект (ИИ),

[26]Европейски зелен пакт, COM(2019) 640 final.
[27]Изграждане на цифровото бъдеще на Европа, COM(2020) 67 final.
[28]Часът на Европа: възстановяване и подготовка за следващото поколение, COM (2020) 98 final.
[29] Стратегия на ЕС за Съюза на сигурност в периода 2020—2025 г., COM(2020) 605 final.
[30] https://eeas.europa.eu/topics/eu-global-strategy_en
[31] https://www.consilium.europa.eu/bg/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/
[32]Инвестициите в цялата верига на доставки на цифрови технологии, допринасящи за цифровия преход или за посрещането на произтичащите от прехода предизвикателства, следва да достигнат най-малко 20 % — тоест 134,5 млрд. евро — от Механизма за възстановяване и устойчивост (672,5 млрд. евро), съставен от безвъзмездни средства и заеми. Финансирането на киберсигурността по многогодишната финансова рамка за периода 2021—2027 г. по линия на програмата „Цифрова Европа“ и на научните изследвания в областта на киберсигурността по линия на рамковата програма „Хоризонт Европа“, със специален акцент върху подкрепата за МСП, може да достигне общо 2 млрд. евро, освен инвестициите от страна на държавите членки и промишлеността.

криптирането и квантовите изчислителни технологии, като се използват стимули и се наложат задължения и сравнителни показатели. Това може да стимулира растежа на европейския сектор на киберсигурността и да осигури необходимата сигурност за по-лесното и постепенно премахване на предходните системи. Европейският фонд за отбрана (ЕФО) ще подкрепя европейските решения за киберотбрана като част от европейската отбранителна технологична и индустриална база. Киберсигурността е включена във външните финансови инструменти в подкрепа на нашите партньори, по-специално в Инструмента за съседство, сътрудничество за развитие и международно сътрудничество. Предотвратяването на злоупотребата с технологии, защитата на критичната инфраструктура и гарантирането на целостта на веригите на доставки също така дава възможност на ЕС да се придържа към нормите, правилата и принципите на ООН за отговорно поведение на държавите[33].

1. УСТОЙЧИВОСТ, ТЕХНОЛОГИЧЕН СУВЕРЕНИТЕТ И ЛИДЕРСТВО

Критичната инфраструктура и основните услуги на ЕС са все по-взаимозависими и цифровизирани. Всички свързани с интернет неща в ЕС, независимо дали са автоматизирани автомобили, промишлени системи за управление или домакински уреди, както и всички вериги на доставки, които ги предоставят, трябва още на етапа на проектиране да бъдат сигурни, устойчиви на киберинциденти и да се връщат бързо към нормално функциониране при откриване на пробойни. Това е от основно значение, за да могат частният и публичният сектор в ЕС да избират измежду най-сигурните инфраструктури и услуги. Предстоящото десетилетие е шанс за ЕС да поведе в разработването на сигурни технологии по цялата верига на доставки. За осигуряването на устойчивост и по-силен промишлен и технологичен капацитет в областта на киберсигурността следва да се използват всички необходими регулаторни, инвестиционни и политически инструменти. Осигуряването на киберсигурност от етапа на проектиране при промишлените процеси, операции и устройства може да намали рисковете, разходите за дружествата, както и за обществото като цяло, и по този начин да се повиши устойчивостта.

1.1 Устойчива инфраструктура и услуги от критично значение

В основата на единния пазар за киберсигурност са заложени **правилата на ЕС относно сигурността на мрежите и информационните системи (МИС)**. Комисията предлага реформа на тези правила при преразглеждането на Директивата за МИС, за да се повиши **киберустойчивостта на всички значими публични и частни сектори, които изпълняват важна функция за икономиката и обществото[34]**. Преразглеждането е необходимо, за да се намалят несъответствията в рамките на вътрешния пазар чрез хармонизиране на обхвата, изискванията за сигурност и докладването на инциденти, националния надзор и правоприлагане, както и на капацитета на компетентните органи.

Реформираната директива за МИС ще осигури основа за по-конкретните правила, които също са необходими за стратегически важни сектори, сред които са енергетиката, транспортът и здравеопазването. За да се гарантира последователен подход, както бе обявено в стратегията за Съюза на сигурност за периода 2020—2025 г., реформата на директивата се предлага заедно с преразглеждане на

[33] https://undocs.org/A/70/174
[34] [*insert reference to NIS proposal*]

законодателството относно устойчивостта на критичната инфраструктура[35]. Енергийните технологии с цифрови компоненти и сигурността на свързаните с тях вериги на доставки са важни за осигуряването на непрекъснатост на основните услуги и за стратегическия контрол на критичната енергийна инфраструктура. Поради това Комисията ще предложи мерки, включително „мрежов кодекс“ за определяне на правила за киберсигурност при трансграничните потоци на електроенергия, които да бъдат приети до края на 2022 г. Финансовият сектор трябва също така да повиши свързаната с цифровите технологии оперативна издръжливост и да си осигури устойчивост на всякакви инциденти или заплахи, свързани с ИКТ, както предложи Комисията[36]. В областта на транспорта Комисията добави разпоредби относно киберсигурността[37] в законодателството на ЕС в областта на сигурността на въздухоплаването и ще продължи да полага усилия за повишаване на киберустойчивостта във всички видове транспорт. Укрепването на киберустойчивостта на **демократичните процеси и институции** е основна част от Плана за действие за европейската демокрация с цел опазване и поощряване на свободните избори, демократичния дискурс и медийния плурализъм[38]. Не на последно място, с оглед на сигурността на инфраструктурата и услугите в рамките на бъдещата космическа програма, Комисията ще доразвие стратегията за киберсигурност на програмата „Галилео“ за следващото поколение услуги на глобалната навигационна спътникова система и за други нови компоненти на космическата програма[39].

1.2 Изграждане на европейски киберщит

С все по-високата степен на свързаност и с нарастващата сложност на кибератаките центровете за споделяне и анализ на информация (ISAC) изпълняват ценна функция, включително на секторно равнище, като позволяват обмен на информация относно киберзаплахите между множество заинтересовани страни[40]. Освен това мрежите и компютърните системи се нуждаят от постоянно наблюдение и анализ за засичане на пробиви и аномалии в реално време. Поради това много частни дружества, публични организации и национални органи създадоха екипи за реагиране при инциденти с компютърната сигурност (CSIRT) и центрове за операции по сигурността (ЦОС).

Центровете за операции по сигурността са от жизненоважно значение за събиране на регистрирани данни[41] и локализиране на подозрителни операции в комуникационните мрежи под наблюдение. Те правят това като разпознават сигнали и модели и извличат информация за заплахите от големите количества данни, които подлежат на оценка. Центровете допринесоха за засичането на злонамерени изпълними програми, с което

[35] [insert reference to *proposal* for a directive on resilience of critical entities]

[36]Предложение за Регламент относно оперативната устойчивост на цифровите технологии във финансовия сектор и за изменение на регламенти (ЕО) № 1060/2009, (ЕС) № 648/2012, (ЕС) № 600/2014 и (ЕС) № 909/2014, COM/2020/595 final.

[37]Регламент за изпълнение (ЕС) 2019/1583 на Комисията.

[38]Съобщение относно „План за действие за европейската демокрация“ COM(2020) 790. Съгласно плана Европейската мрежа за сътрудничество в областта на изборите и изборните мрежи на държавите членки ще подкрепят задействането на съвместни експертни екипи за борба със заплахите за изборните процеси, включително с киберзаплахите, https://ec.europa.eu/info/policies/justice-and-fundamental-rights/eu-citizenship/electoral-rights/european-cooperation-network-elections_en

[39]Това включва нова инициатива за правителствени спътникови комуникации (GOVSATCOM) и дейностите, свързани с космическите отпадъци (КНП).

[40]https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

[41]Така че правоприлагащите и съдебните органи да могат да ги използват като доказателство.

помогнаха да се ограничат кибератаките. Работата в тези центрове е изключително трудна и на високи обороти, поради което ИИ и по-специално техниките за машинно самообучение могат да помогнат неимоверно на специалистите[42].

Комисията предлага да се изгради **мрежа от центрове за операции по сигурността в целия ЕС[43] и** да се подкрепи подобряването на съществуващите центрове, както и създаването на нови. Тя също така ще подпомага обучението и развитието на уменията на персонала, който работи в тези центрове. Въз основа на анализ на нуждите, извършен със съответните заинтересовани страни и подкрепен от Агенцията на ЕС за киберсигурност (ENISA), Комисията може да осигури над 300 млн. евро в подкрепа на публично-частното и трансграничното сътрудничество при създаването на национални и секторни мрежи, включващи и МСП, въз основа на подходящи разпоредби за управление, сигурност и обмен на данни.

Държавите членки се приканват също да инвестират в този проект. Така центровете ще могат по-ефективно да споделят и установяват връзка между отделните сигнали, чрез което да създават висококачествени разузнавателни данни за заплахите, които да бъдат споделяни с ISAC и националните органи. Това ще позволи пълноценно ориентиране в обстановката. Целта е постепенно да се установи връзка между възможно най-много центрове в целия ЕС за обединяване на знанията и обмен на най-добри практики. На центровете ще се предостави подкрепа за подобряване на скоростта на засичане на инциденти, за анализ и реагиране чрез най-съвременни технологии като ИИ и машинно самообучение, допълнени от инфраструктура за изчисления със суперкомпютри, разработена в ЕС от Съвместното предприятие за европейски високопроизводителни изчислителни технологии[44].

Благодарение на работа в режим на непрекъснато сътрудничество мрежата ще алармира навреме органите и всички заинтересовани страни, включително съвместното звено за киберсигурност (вж. раздел 2.1) за инциденти, свързани с киберсигурността. С плътното си покритие от наблюдателници мрежата ще бъде истински щит за сигурността на киберпространството на ЕС, способен да открива потенциални заплахи, преди те да са нанесли големи щети.

1.3 Свръхсигурна комуникационна инфраструктура

Правителствените спътникови далекосъобщения на Европейския съюз[45], които са част от космическата програма, ще осигурят надежден и икономически ефективен комуникационен капацитет, базиран на околоземни спътници, за да се гарантират мисиите и операциите от критично значение за сигурността и безопасността, които се управляват от ЕС и неговите държави членки, включително от субекти в областта на националната сигурност и от институции, органи и агенции на ЕС.

---

[42] Източник: проучване на Ponemon Institute Research, Improving the Effectiveness of the SOC, 2019; за изследвания върху използването на ИИ в центрове за операции по сигурността вж. например: Khraisat, A., Gondal, I., Vamplew, P. *et al.* Survey of intrusion detection systems: techniques, datasets and challenges, *Cybersecur* 2**,** 20 (2019).

[43]Ще бъдат разработени по-подробни правила за управлението, принципите на функциониране и финансиране на центровете и ще бъдат допълнени съществуващите структури, като например центровете за цифрови иновации.

[44]https://ec.europa.eu/digital-single-market/en/eurohpc-joint-undertaking

[45]GOVSATCOM е част от космическата програма на Съюза.

Държавите членки поеха ангажимент да работят съвместно с Комисията за създаване на сигурна квантова комуникационна инфраструктура (QCI) за Европа[46]. QCI ще предложи на публичните органи съвсем нов начин за предаване на поверителна информация чрез изключително сигурна форма на криптиране с цел защита срещу кибератаки въз основа на европейска технология. Тя ще е съставена от два основни компонента: съществуващите наземни кабелни съобщителни мрежи, свързващи стратегически обекти на национално и трансгранично равнище, и свързаните космически спътници, покриващи целия ЕС, включително неговите отвъдморски територии[47]. Инициативата за разработване и внедряване на нови и по-сигурни форми на криптиране и за разработване на нови начини за защита на стратегическите средства за комуникация и данни може да помогне за защитата на чувствителната информация и съответно на критичните инфраструктури.

Предвид всичко това и в по-далечна перспектива Комисията ще проучи възможността за разгръщане на многоорбитална сигурна система за свързаност. Използвайки за основа GOVSATCOM и QCI, тя ще интегрира авангардни технологии (квантови комуникации, 5G, ИИ, периферни изчисления) и ще се придържа към най-рестриктивната рамка за киберсигурност, в подкрепа на услугите, при които сигурността е взета предвид още на етапа на проектиране, като например надеждната, сигурна и икономически ефективна свързаност и криптираната комуникация за правителствените дейности от критично значение.

1.4 Осигуряване на широколентови мобилни мрежи от следващо поколение

Гражданите и дружествата в ЕС, които използват модерни и иновативни приложения, **базирани на 5G и на следващи поколения мрежи**, трябва да могат да разчитат на най-високи стандарти за сигурност. Държавите членки, заедно с Комисията и с подкрепата на ENISA, въведоха с инструментариума на ЕС за 5G[48], приет през януари 2020 г., всеобхватен и обективен подход към киберсигурността на 5G, който се основава на оценка на възможните планове за ограничаване на рисковете и на установяване на най-ефективните мерки. Освен това ЕС консолидира способностите си в областта на 5G и мрежите от следващи поколения, за да избегне зависимости и да насърчи изграждането на устойчива и диверсифицирана верига на доставки.

[46]Декларацията на EuroQCI е подписана от повечето държави членки, а развитието и разгръщането на инфраструктурата ще се осъществи в периода 2021—2027 г. с финансиране по линия на „Хоризонт Европа“ и „Цифрова Европа“ и от Европейската космическа агенция, при спазване на подходящи механизми за управление; https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network

[47]Разработването на космически компонент е необходимо за постигане на връзки от точка до точка на дълги разстояния (>1000 km), които наземната инфраструктура не може да поддържа. Като използва свойствата на квантовата механика, QCI първоначално ще даде възможност на страните да споделят сигурно случайни секретни ключове, които да се използват за криптиране и дешифриране на съобщения. QCI ще включва също така разполагането на инфраструктура за изпитване и съответствие за оценка на съответствието на европейските квантови комуникационни устройства и системи с инфраструктурата за QCI и тяхното сертифициране и валидиране преди интегрирането им в QCI. Тя ще бъде проектирана така, че да поддържа допълнителни приложения, когато те достигнат необходимото равнище на технологична зрялост. Настоящият пилотен проект OpenQKD (https://openqkd.eu/) е предшественик на тази инфраструктура за изпитване и съответствие.

[48]Съобщение „Сигурно внедряване на 5G в ЕС — прилагане на инструментариума на ЕС“, (COM(2020) 50).

През декември 2020 г. Комисията публикува доклад за отражението на препоръката от 26 март 2019 г. относно киберсигурността на 5G мрежите[49]. В него се посочва, че след приемането на инструментариума е постигнат значителен напредък и повечето държави членки са на път да приключат скоро прилагането на значителна част от инструментариума, макар и в различна степен и въпреки някои нерешени проблеми, както вече беше посочено в доклада за напредъка, публикуван през юли 2020 г.[50].

През октомври 2020 г. Европейският съвет призова ЕС и държавите членки „да използват пълноценно инструментариума на ЕС за киберсигурност на 5G технологиите“ и „да прилагат съответните ограничения за високорискови доставчици на ключови активи, определени като критични и чувствителни в координираните оценки на риска на равнището на ЕС, въз основа на общи обективни критерии“[51].

В бъдеще ЕС и неговите държави членки трябва да гарантират, че установените рискове се ограничават по подходящ и координиран начин, особено що се отнася до целта да се сведе до минимум използването на високорискови доставчици и да се избягва всяка зависимост от тях на национално равнище и на равнище ЕС, както и че се отчитат всички съществени промени или рискове. Държавите членки се приканват да използват пълноценно инструментариума, когато инвестират в цифров капацитет и свързаност.

Въз основа на доклада за отражението на препоръката от 2019 г. Комисията насърчава държавите членки да ускорят работата си с цел завършване на прилагането на основните мерки от инструментариума до второто тримесечие на 2021 г. Тя също така призовава държавите членки да продължат да следят заедно постигнатото до момента и да гарантират по-нататъшното съгласуване на подходите. На равнище ЕС ще се преследват три основни цели в подкрепа на този процес: осигуряване на по-нататъшно сближаване на подходите за намаляване на риска в целия ЕС, подпомагане на непрекъснатия обмен на знания и изграждането на капацитет и насърчаване на устойчивостта на веригата на доставки и на други стратегически цели на ЕС в областта на сигурността. В специалното приложение към настоящото съобщение са изложени конкретни действия, свързани с тези ключови цели.

С подкрепата на ENISA Комисията ще продължи да работи в тясно сътрудничество с държавите членки за изпълнението на целите и действията (вж. приложението).

Освен това подходът, основан на инструментариума на ЕС за 5G, привлече интереса на държави извън ЕС, които понастоящем разработват свои подходи за гарантиране на сигурността на комуникационните си мрежи. Службите на Комисията, заедно с Европейската служба за външна дейност и мрежата от делегации на ЕС, са готови при поискване да предоставят допълнителна информация на съответните органи по света относно нейния всеобхватен, обективен и основан на анализ на риска подход.

[49]Доклад на Комисията за отражението на препоръката на Комисията от 26 март 2019 г. относно киберсигурността на 5G мрежите, 15 декември 2020 г.
[50]Вж. доклада от 24 юли 2020 г. на групата за сътрудничество по въпросите на МИС относно прилагането на инструментариума.
[51]EUCO 13/20, Специално заседание на Европейския съвет (1 и 2 октомври 2020 г.) — Заключения.

1.5 Интернет на сигурните предмети

Всеки свързан с интернет предмет е по определен начин уязвим и това може да се използва по злонамерен начин, като последствията могат да бъдат мащабни. Правилата на вътрешния пазар съдържат предпазни мерки срещу несигурни продукти и услуги. Комисията вече работи за гарантиране на **прозрачни решения в областта на сигурността и сертифицирането съгласно Акта за киберсигурността**, както и за насърчаване на използването на безопасни продукти и услуги без компромис с качеството[52]. Тя ще приеме първата си непрекъсната работна програма на Съюза през първото тримесечие на 2021 г. (която ще се актуализира поне веднъж на всеки три години), за да позволи на промишлеността, националните органи и органите по стандартизация да се подготвят предварително за бъдещите европейски схеми за сертифициране на киберсигурността[53]. Тъй като все повече предмети са свързани с интернет, приложимите правила трябва да станат по-стриктни, за да се гарантира цялостната устойчивост и да се стимулира киберсигурността.

Комисията ще обмисли всеобхватен подход, включително евентуални **нови хоризонтални правила за подобряване на киберсигурността на всички свързани с интернет продукти и съответните услуги, предлагани на вътрешния пазар**[54]. Възможно е те да включват ново изискване за производителите на свързани устройства, а именно задължението да полагат необходимото старание и да предотвратяват пробойни в софтуера, включително осигуряването на непрекъснатост на софтуерните актуализации и актуализациите на защитата, както и гарантирано заличаване на личните и други чувствителни данни в края на жизнения цикъл. Тези правила ще се отразят положително на инициативата за „правото на ремонт на остарелия софтуер“, представена в плана за действие за кръгова икономика. Те ще допълнят някои мерки, насочени към конкретни видове продукти, като например бъдещото предложение за задължителни изисквания спрямо достъпа до пазара на някои безжични продукти **(**чрез делегиран акт съгласно Директивата за радиосъоръженията[55]), и целта за прилагане на правилата за киберсигурност от юли 2022 г. спрямо моторните превозни средства за всички нови видове превозни средства[56]. Освен това те ще се основават на предложеното преразглеждане на общите

[52]Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и относно сертифицирането на киберсигурността на информационните и комуникационните технологии и за отмяна на Регламент (ЕС) № 526/2013 („Акт за киберсигурността“). С Акта за киберсигурността се насърчава сертифицирането на ИКТ на равнище ЕС посредством европейска рамка за сертифициране на киберсигурността, целяща създаването на доброволни европейски схеми за сертифициране на киберсигурността, за да се гарантира адекватно ниво на киберсигурност за продукти, услуги и процеси в сферата на ИКТ в Съюза, както и да се намали разпокъсаността на вътрешния пазар по отношение на схемите за сертифициране на киберсигурността в Съюза. Наред с това дружествата за оценка на киберсигурността обикновено са установени извън ЕС, което се отразява отрицателно на прозрачността и надзора; https://www.uschamber.com/issue-brief/principles-fair-and-accurate-security-ratings

[53]Съгласно член 47, параграф 5 от Акта за киберсигурността.

[54]В заключенията на Съвета се отправя призив за хоризонтални мерки относно киберсигурността на свързаните устройства; 13629/20, 02 декември 2020 г.

[55]Директива 2014/53/ЕС

[56]Следва правилото на ООН, прието през юни 2020 г.; http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf

правила за безопасност на продуктите, които не засягат пряко аспектите на киберсигурността[57].

1.6 По-голяма сигурност на интернет в глобален мащаб

Функционирането и целостта на интернет в световен мащаб се осигуряват от пакет основни протоколи и поддържаща инфраструктура[58]. Пакетът включва DNS и неговата йерархична и делегирана система от зони, като се започне от върха на йерархията с кореновата зона и тринадесетте базови сървъра на DNS[59], от които зависи световната хипертекстова мрежа. Комисията смята да разработи **план за действие в извънредни ситуации, подкрепен финансово от ЕС, за справяне при екстремни случаи, които засягат целостта на глобалната коренова система за DNS и нарушават достъпа до нея**. Комисията ще работи с ENISA, държавите членки, двата оператора на базови DNS сървъри в ЕС[60] и множеството заинтересовани страни, за да анализира ролята на операторите за гарантиране, че достъпът до интернет ще бъде осигурен и занапред в световен мащаб при всички обстоятелства.

За да има даден клиент достъп до ресурс под определено име на домейн в интернет, неговата заявка (обикновено URL адрес) трябва да бъде „преобразувана“ в IP адрес чрез справка с DNS сървъри. Хора и организации в ЕС все повече разчитат обаче на няколко публични DNS преобразувателя, управлявани от субекти извън ЕС. Подобно концентриране на DNS преобразуването в ръцете на няколко дружества[61] прави самия процес на преобразуване уязвим в случай на сериозни проблеми при някой основен доставчик и затруднява органите на ЕС в борбата им с евентуални кибератаки и значителни геополитически и технически инциденти[62].

За да се намалят свързаните със сигурността проблеми, породени от пазарната концентрация, Комисията ще насърчи съответните заинтересовани страни, включително дружества, доставчици на интернет услуги и продавачи на браузъри от ЕС, да приемат стратегия за диверсификация на DNS преобразуването. Комисията смята също така да допринесе за сигурността на интернет, като подкрепи разработването на публична **европейска услуга за DNS преобразуване**. Тази

[57]Преразглеждане на действащите правила относно общата безопасност на продуктите (Директива 2001/95/ЕО); планирано е предложение и за адаптиране на правилата относно отговорността на производителите в цифровата сфера в обхвата на нормативната уредба на ЕС в областта на отговорността.

[58]„Обществеността ядро на отворения интернет, а именно неговите основни протоколи и инфраструктура, които са всеобщо обществено благо, осигурява основната функционалност на интернет като цяло и лежи в основата на неговото нормално функциониране. ENISA следва да допринася за сигурността на обществеността ядро на отворения интернет и стабилността на неговото функциониране, включително, но не само — ключовите протоколи (по-специално DNS, BGP и IPv6), за експлоатацията на системата за имена на домейни (като тези на всички домейни от първо ниво), и за функционирането на кореновата зона“; Съображение 23 от Акта за киберсигурността.

[59]https://www.iana.org/domains/root/servers

[60]Сървърите i.root, управлявани от Netnod в Швеция и сървърите k.root, управлявани от RIPE NCC в Нидерландия.

[61]Консолидиране на пазара на DNS преобразуването — в каква степен, колко бързо, доколко опасно? Доказателства за намаляване на ентропията на интернет — липсата на резервиране (дублиране) при DNS преобразуването от страна на основни уебсайтове и услуги

[62]Налице са и доказателства, които показват, че DNS данните могат да се използват за профилиране, което засяга неприкосновеността на личния живот и правата на защита на данните.

инициатива (DNS4EU) ще предложи алтернативна европейска услуга за достъп до световния интернет. DNS4EU ще бъде прозрачна, 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 и ще бъде част от Европейския индустриален алианс за данни и компютърни услуги в облак[63].

В сътрудничество с държавите членки и отрасъла Комисията също така **ще ускори въвеждането на ключови интернет стандарти, включително IPv6[64], и утвърдени стандарти за сигурност в интернет и добри практики за сигурността на DNS, маршрутизацията и електронната поща[65]**, без да изключва регулаторни мерки като европейска клауза за прекратяване на използването на IPv4 с цел насочване на пазара, ако въпросните стандарти не се възприемат достатъчно бързо. ЕС следва да насърчава прилагането на тези стандарти (например по линия на стратегията ЕС-Африка[66]) в страните партньори и по този начин да подкрепя развитието на глобалния и отворен интернет и да противодейства на затворените и основани на контрол модели на интернет. Най-сетне, Комисията ще разгледа необходимостта от механизъм за по-систематично наблюдение и събиране на обобщени данни за интернет трафика и за предоставяне на съвети относно потенциални инциденти[67].

1.7 Засилено присъствие във веригата за доставки на технологии

С планираната финансова подкрепа за сигурна в кибернетично отношение цифрова трансформация по линия на многогодишната финансова рамка за периода 2021—2027 г. ЕС има уникалната възможност да обедини активите си, за да даде тласък на своята промишлена стратегия[68] и да утвърди своята водеща роля в областта на цифровите технологии и киберсигурността по цялата цифрова верига на доставки (включително данни и изчисления в облак, технологии за процесори от следващо поколение, свръхсигурна свързаност и 6G мрежи), в съгласие със своите ценности и приоритети. Намесата на публичния сектор следва да използва инструментите от регулаторната рамка на ЕС за обществените поръчки и тези за важните проекти от общоевропейски интерес. Освен това тя може да отключи частни инвестиции чрез публично-частни партньорства (включително въз основа на опита от договорното публично-частно партньорство в областта на киберсигурността и неговото изпълнение чрез Европейската организация за киберсигурност), чрез рисков капитал в подкрепа на МСП или чрез промишлени съюзи и стратегии за постигане на технологичен капацитет.

---

[63] Съвместна декларация „Изграждане на облак от следващо поколение за предприятията и публичния сектор в ЕС“; https://ec.europa.eu/digital-single-market/en/news/towards-next-generation-cloud-europe

[64] Със сериозното намаляване на предлагането и поскъпване на IPv4 адресите внедряването на IPv6 вече напредва значително. То обаче е неравномерно в отделните държави от ЕС.

[65] Тези стандарти включват DNSSEC, HTTPS, DNS по HTTPS (DoH), DNS по TLS (DoT), SPF, DKIM, DMARC, STARTTLS, DANE и добри практики и норми за маршрутизиране, например взаимно съгласувани норми за сигурно маршрутизиране (MANRS).

[66] Съвместно съобщение „Към всеобхватна стратегия с Африка“, JOIN(2020) 4 final от 9 март 2020 г.

[67] Подобна „Обсерватория на интернет“ може да бъде включена в обхвата на дейностите на Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността; Предложение за Регламент за създаване на Европейски център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове, COM(2018) 630 final.

[68] Съобщение „Нова промишлена стратегия за Европа“, COM/2020/102 final.

Специален акцент ще бъде поставен също върху Инструмента за техническа подкрепа[69] и най-подходящото използване на най-новите инструменти за киберсигурност от страна на МСП — особено онези, които не попадат в обхвата на преразгледаната Директива за МИС — включително чрез специални дейности в рамките на центровете за цифрови иновации по линия на програмата „Цифрова Европа“. Целта е да се привлекат сходни по размер инвестиции от страна на държавите членки и съответстващо финансово участие на промишления сектор в рамките на партньорство, управлявано съвместно с държавите членки, в предложения **Център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността и Мрежа от национални координационни центрове (CCCN).** Мрежата CCCN трябва да играе ключова роля с участието на промишлеността и академичните общности за развитието на технологичния суверенитет на ЕС в областта на киберсигурността, за изграждането на капацитет за гарантиране на сигурността на инфраструктури от стратегическо значение като 5G и за намаляване на зависимостта от други части на света при най-важните технологии.

Комисията смята да подкрепи, евентуално съвместно с мрежата CCCN, разработването на специална магистърска програма в областта на киберсигурността и да помогне за изготвянето на обща европейска пътна карта за научни изследвания и иновации в областта на киберсигурността след 2020 г. Инвестициите чрез мрежата CCCN ще се основават и на сътрудничество в областта на научноизследователската и развойната дейност между мрежи от центрове за високи постижения в областта на киберсигурността, и ще обединяват усилията на най-добрите научноизследователски екипи в Европа и на промишлеността с цел разработване и изпълнение на общи научноизследователски програми в съответствие с пътната карта на Европейската организация за киберсигурност[70]. Комисията ще продължи да разчита на научноизследователската работа на ENISA и Европол и по линия на „Хоризонт Европа“ да подкрепя отделни новатори в областта на интернет, разработващи комуникационни технологии за подобряване на неприкосновеността на личния живот и сигурността на комуникациите въз основа софтуер и хардуер с отворен код, както прави понастоящем в рамките на инициативата Интернет от следващо поколение.

1.8 Европейска квалифицирана работна сила в информационното пространство

Усилията на ЕС да повишава квалификацията на работната сила, да развива, привлича и задържа най-добрите таланти в областта на киберсигурността и да инвестира в научни изследвания и иновации на световно равнище са важен компонент на защитата срещу киберзаплахите като цяло. Това е поле за развитие с огромен потенциал. Затова на развитието, привличането и задържането на разнородни таланти трябва да се обръща специално внимание. Преразгледаният план за действие в областта на цифровото образование ще повиши грамотността по отношение на киберсигурността, особено сред децата, младите хора и организациите, особено МСП[71]. Той ще насърчи също така участието на жените в обучението в областта на науките, технологиите, инженерството и математиката (НТИМ), в повишаването на квалификацията на заетите в областта на ИКТ и в преквалификацията с цел добиване на цифрови умения. Освен това Комисията, заедно със Службата на ЕС за интелектуална собственост към

[69] https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=COM:2020:0409:FIN .
[70] https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies
[71] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_bg

Европол, ENISA, държавите членки и частния сектор, ще разработи инструменти за развитие на компетентността, както и насоки за повишаване на способността на предприятията в ЕС да се защитават срещу **кражбите на интелектуална собственост онлайн**[72].

Образованието — включително професионалното образование и обучение (ПОО), грамотността и уменията — следва също така допълнително да повиши уменията в областта на киберсигурността и киберотбраната на равнище ЕС. За тази цел съответните участници от ЕС, като ENISA, Европейската агенция по отбрана (EDA) и Европейския колеж по сигурност и отбрана (ЕКСО)[73] следва да търсят полезни взаимодействия между своите дейности в тази област.

Стратегически инициативи

ЕС следва да гарантира:

- Приемането на преразгледаната Директива за МИС;
- Регулаторни мерки за интернет на сигурните предмети;
- Увеличаване на инвестициите в киберсигурността до 4,5 млрд. евро под формата на публични и частни инвестиции в периода 2021—2027 г. чрез мрежата CCCN (по-специално чрез програмите „Цифрова Европа“ и „Хоризонт Европа“ и чрез механизма за възстановяване);
- Изграждане на мрежа на ЕС от центрове за операции по сигурността, използващи ИИ, както и на свръхсигурна комуникационна инфраструктура, използваща квантови технологии;
- Широко разпространение на технологиите за киберсигурност чрез специална подкрепа за МСП в рамките на центровете за цифрови иновации;
- Разработване на европейска услуга за DNS преобразувател като алтернатива за безопасен и отворен достъп до интернет за гражданите, предприятията и публичната администрация на ЕС; както и
- Довършване на въвеждането на инструментариума за 5G до второто тримесечие на 2021 г. (вж. приложението).

2. ИЗГРАЖДАНЕ НА ОПЕРАТИВЕН КАПАЦИТЕТ ЗА ПРЕДОТВРАТЯВАНЕ, ВЪЗПИРАНЕ И РЕАГИРАНЕ

Киберинцидентите, били те случайни, или умишлени действия на престъпници, държавни и недържавни субекти, могат да причинят огромни щети. Техният мащаб и сложност, които често включват използването на услуги, хардуер и софтуер на трети страни за проникване в дадена крайна цел, затрудняват противодействието на колективната заплаха за ЕС, ако няма систематичен и всеобхватен обмен на информация и сътрудничество с цел обща реакция. **Чрез цялостно прилагане на**

[72] https://ec.europa.eu/commission/presscorner/detail/bg/IP_20_2187

[73] Чрез Платформата за образование, обучения, учения и оценка в областта на кибернетичното пространство (ETEE).

регулаторните инструменти, мобилизиране и сътрудничество ЕС се стреми да подкрепи усилията на държавите членки да защитят своите граждани, икономически интереси и интересите си в областта на националната сигурност, при пълно зачитане на основните права и свободи и на принципите на правовата държава. Общностите от мрежи, институции, органи и агенции на ЕС, както и органите на държавите членки отговарят за предотвратяване, възпиране и реагиране на киберзаплахите, като използват инструментите и инициативите, с които разполагат[74]. Тези общности включват: i) органите, отговорни за МИС, като например CSIRT, и за реагиране при бедствия; ii) правоприлагащите и съдебните органи; iii) кибердипломацията; и iv) киберотбраната.

2.1 Съвместно звено за киберсигурност

Съвместното звено за кибернетична сигурност ще служи като виртуална и физическа платформа за сътрудничество между различните общности в областта на киберсигурността в ЕС, като обръща особено внимание върху оперативната и техническата координация срещу най-големите трансгранични киберинциденти и заплахи.

Съвместното звено за кибернетична сигурност ще бъде важна стъпка към завършването на **европейската рамка за управление на кризи в областта на киберсигурността.** Както е посочено в политическите насоки на председателя на Комисията[75], звеното трябва да позволи на държавите членки и на институциите на ЕС, на органите и агенциите пълноценно да използват съществуващите структури, ресурси и способности и да насърчава нагласата за признаване на „**необходимостта от споделяне**“. То ще осигури средствата за консолидиране на направения до сега напредък в изпълнението на Препоръката от 2017 г. относно координирана реакция при мащабни киберинциденти и кризи („План за действие“)[76]. Звеното ще даде възможност и да се задълбочи сътрудничеството във връзка с основните компоненти на плана и ще използва напредъка, постигнат по-специално в рамките на групата за сътрудничество за МИС и мрежата CyCLONe.

С негова помощ може да се намери решение на **два основни пропуска**, които понастоящем увеличават уязвимостта и внасят неефективност при реагирането на трансгранични заплахи и инциденти, както и на инциденти, засягащи Съюза. Първо, **общностите в областта на киберсигурността** от гражданската сфера, дипломацията,

[74]Включително подкрепата за оперативното сътрудничество и управлението на кризи от страна на Агенцията на Европейския съюз за киберсигурност (ENISA); мрежата на CSIRT; мрежата за връзка на организациите при кибернетични кризи (CyCLONe, която ще стане EU-CyCLONe съгласно с предложеното в преразгледаната Директива за МИС); групата за сътрудничество за МИС; „rescEU“; Европейския център за борба с киберпрестъпността, съвместната работна група за действия в областта на киберпрестъпността към Европол и Протокола за реагиране при извънредни ситуации на правоприлагащите органи в ЕС; Центъра на ЕС за анализ на информация (EU INTCEN) и инструментариума за кибердипломация; единното звено за анализ на разузнавателна информация (SIAC) и проектите от областта на киберпространството в рамките на постоянното структурирано сътрудничество (ПСС), по-специално екипите за бързо реагиране при кибератаки и за взаимопомощ в областта на киберсигурността (CRRT).

[75]„Съюз с по-големи амбиции: моята програма за Европа“, Политически насоки за следващата Европейска комисия (2019—2024 г.) от кандидата за председател на Европейската комисия Урсула фон дер Лайен.

[76]Препоръка C(2017) 6100 final от 13.9.2017 г. относно координирана реакция на мащабни киберинциденти и кризи

правоприлагането и отбраната все още нямат общо пространство за насърчаване на структурирано сътрудничество и улесняване на оперативното и техническото сътрудничество. Второ, съответните заинтересовани страни в областта на киберсигурността все още не са успели пълноценно да използват целия **потенциал** на оперативното сътрудничество и взаимната помощ в рамките на съществуващите мрежи и общности. Това включва липсата на платформа, която дава възможност за оперативно сътрудничество с частния сектор. Звеното следва да подобри и ускори координацията и да позволи на ЕС да посреща решително мащабни киберинциденти и кризи и да реагира на тях.

Съвместното звено за киберсигурност няма да бъде допълнителен, самостоятелен орган, нито ще засяга компетенциите и правомощията на националните органи в областта на киберсигурността или на участниците от ЕС. То по-скоро ще действа като предпазен механизъм, при който всеки участник може да се възползва от подкрепата и експертния опит на останалите, особено в ситуация, в която различни киберобщности трябва да работят в тясно сътрудничество. Същевременно неотдавнашните събития показаха необходимостта ЕС да си постави по-амбициозни цели и да повиши готовността за посрещане на кибернетичните заплахи и реалностите в тази област. Като част от приноса си към съвместното звено за кибернетична сигурност, участниците от ЕС (Комисията и агенциите и органите на ЕС) ще бъдат готови значително да увеличат ресурсите и способностите си, така че да изравнят своята подготвеност и устойчивост.

Съвместното звено за киберсигурност ще работи за изпълнението на три главни цели. Първо, то ще осигури **готовност** сред общностите в областта на киберсигурността; Второ, чрез споделяне на информация то ще осигури непрекъснато споделено ориентиране в обстановката; Трето, то ще повиши способността за координирана **реакция** и възстановяване. За да постигне посочените цели, звеното следва да се опира на добре определени елементи и цели, например гарантирането на сигурно и бързо споделяне на информация, подобряването на сътрудничеството между участниците, включително на взаимодействието между държавите членки и съответните субекти на ЕС, създаването на **структурирано партньорство с надеждна промишлена база** и улесняването на координиран подход към **сътрудничеството с външни партньори.** За целта, въз основа на обзор на наличните способности на национално равнище и на равнище ЕС, звеното би могло да улесни разработването на рамка за сътрудничество.

За да може съвместното звено за кибернетична сигурност да бъде в центъра на оперативното сътрудничество, Комисията ще работи с държавите членки и съответните институции, органи и агенции на ЕС, включително ENISA, CERT-EU и Европол, за да насърчава **поетапен и приобщаващ подход** при пълно зачитане на компетенциите и мандатите на всички участници. В съответствие с този подход звеното би могло да допринесе за по-нататъшно сътрудничество между участниците в конкретна киберобщност, когато те сметнат това за необходимо.

За създаването на съвместното звено за киберсигурност се предлагат четири основни стъпки:

- *определяне* чрез обзор на наличните способности на национално равнище и на равнище ЕС;

- *подготвяне* чрез създаване на рамка за структурирано сътрудничество и помощ;

- *разполагане* чрез прилагане на рамката, като се използват ресурсите, предоставени от участниците така, че съвместното звено за киберсигурност да започне работа;

- *разширяване* чрез укрепване на капацитета за координиран отговор с принос от страна на промишлеността и партньорите.

Въз основа на резултатите от консултацията с държавите членки, институциите, органите и агенциите на ЕС[77], Комисията с участието на върховния представител в съответствие с неговите компетенции, до февруари 2021 г. ще представи процеса, основните етапи и графика за **определянето, подготовката, въвеждането и разширяването на съвместното звено за киберсигурност**.

2.2 Борба с киберпрестъпността

Зависимостта ни от онлайн инструменти увеличи експоненциално площта за атака от страна на киберпрестъпниците и доведе до ситуация, при която в разследването на почти всички видове престъпления има и цифров компонент. Освен това основни аспекти на нашето общество са застрашени от действащи в киберпространството лица, както и от такива, които използват киберинструменти, за да планират и осъществяват незаконни действия. Следователно има тесни връзки с цялостната политика на ЕС по отношение на сигурността, за което свидетелстват и свързаните с киберсигурността елементи, които са включени в стратегията за Съюза на сигурност от 2020 г. и в програмата на ЕС за борба с тероризма [78].

Ефективната борба с киберпрестъпността е основен фактор за гарантиране на киберсигурността: възпирането не може да бъде постигнато само чрез устойчивост, но изисква също и идентифициране и преследване на извършителите на престъпления. Поради това е от съществено значение да се насърчават сътрудничеството и обменът между участниците в сферата на киберсигурността и органите по правоприлагане. Поради това на равнището на ЕС Европол и ENISA вече са изградили силно сътрудничество, в чиито рамки са организирали съвместни конференции и семинари, и са предоставили съвместни доклади на Комисията, държавите членки и други заинтересовани страни по въпросите на киберсигурността и технологичните предизвикателства. Комисията ще продължи да подкрепя този интегриран подход с оглед на това да осигури съгласуван и ефективен отговор въз основа на информация, позволяваща съставянето на изчерпателна картина.

Като важен елемент от този отговор органите на ЕС и националните органи трябва да разширят и подобрят капацитета на правоприлагащите органи за разследване на киберпрестъпления при пълно зачитане на основните права и постигане на баланс между различните права и интереси. ЕС трябва да е в състояние да се бори с киберпрестъпността с помощта на изцяло прилагано подходящо за целта законодателство, като обръща особено внимание на борбата със сексуалното насилие над деца в интернет и върху разследванията, без да пропуска и престъпността в

[77]Консултация с държавите членки (включително по време на учението Blue OLEx20, на което се събират ръководителите на националните органи в областта на киберсигурността), институциите, органите и агенциите на ЕС, проведена между юли и ноември 2020 г.
[78]Съобщение относно Програма на ЕС за борба с тероризма:: Предвиждане, предотвратяване, защита, реагиране, 9.12.2020 г., COM (2020) 795 final.,

„даркнет“. Правоприлагащите органи трябва да бъдат напълно оборудвани за цифрови разследвания. Комисията ще представи план за действие за подобряване на цифровия капацитет на правоприлагащите органи, като им предостави необходимите умения и инструменти. Освен това, Европол ще продължи да развива ролята си на експертен център в подкрепа на националните правоприлагащи органи за борба с компютърната и зависимата от киберпространството престъпност, като допринася за определянето на общи криминологични стандарти (чрез лабораторията и центъра за иновации на Европол).Всички тези дейности изискват подходящо приемане и подкрепа от страна на държавите членки, които настоятелно се приканват да използват националните програми на Фонд „Вътрешна сигурност“ и да предлагат проекти в отговор на поканите за представяне на предложения като част от тематичния инструмент.

Комисията ще използва всички подходящи средства, включително процедурите за нарушение, за да гарантира, че Директивата от 2013 г. относно атаките срещу информационните системи[79] е изцяло транспонирана и се прилага, включително предоставянето на статистически данни от държавите членки. С това тя ще противодейства по-добре на злоупотребата с имена на домейни, включително, когато е целесъобразно, във връзка с разпространението на незаконно съдържание, и ще се направят усилия за осигуряване на прецизни регистрационни данни чрез продължаването на контактите с Интернет корпорацията за присвоени имена и адреси (ICANN) и други заинтересовани страни в системата за управление на интернет, по-специално с помощта на работната група по въпросите на обществената безопасност към Правителствения консултативен комите на ICANN. Предложението в преразгледаната Директива за МИС съответно предвижда поддържането на точни и пълни бази данни за имена на домейни и регистрационни данни, или данни „WHOIS“, и осигуряване на законен достъп до такива данни, които са от основно значение за осигуряване на сигурността, стабилността и устойчивостта на DNS.

Комисията също така ще продължи да работи за осигуряване на подходящи канали и изясняване на правилата за получаване на трансграничен достъп до електронни доказателства при наказателни разследвания (необходими при 85 % от разследванията, като 65 % от всички заявки се отнасят до доставчици, установени в друга юрисдикция), като улеснява приемането и последващото прилагане на „пакета за електронните доказателства“ и практическите мерки[80]. Бързото приемане от Европейския парламент и Съвета на предложенията за електронните доказателства е от ключово значение за предоставянето на ефективен инструментариум на практикуващите специалисти. Електронните доказателства трябва да бъдат четими, поради което Комисията ще продължи да работи за подкрепата на правоприлагащите органи в областта на цифровите разследвания, включително по отношение на криптирането при наказателни разследвания, като същевременно напълно запазва функциите им за защита на основните права и киберсигурността.

[79]Директива 2013/40/ЕС относно атаките срещу информационните системи.

[80]COM(2018) 225 и 226; C(2020) 2779 final. По-специално, проектът SIRIUS наскоро получи допълнително финансиране съгласно Инструмента за партньорство за подобряване на каналите за получаване на законен трансграничен достъп до електронни доказателства при наказателни разследвания (необходими при 85 % от разследванията на тежки престъпления, като 65 % от всички искания се отправят към доставчици, които са установени в друга юрисдикция)), и създаване на съвместими правила на международно равнище.

2.3 Инструментариум за кибердипломация на ЕС

ЕС използва своя **инструментариум за кибердипломация**[81], за да предотвратява, разколебава, възпира и реагира на злонамерени действия в киберпространството. След като през май 2019 г.[82] бе въведена правна рамка, позволяваща целенасочени ограничителни мерки срещу кибератаките, през юли 2020 г.[83] ЕС предприе санкции съгласно посочената рамка срещу шест лица и три образувания, отговорни за кибератаки или участващи в кибератаки, които са засегнали ЕС и неговите държави членки. Мерки бяха предприети и през октомври 2020 г. срещу две лица и едно образувание[84]. На злонамерените действия в киберпространството, включително такива, чиито последствия се проявяват след време, следва да се противодейства чрез ефективна и всеобхватна съвместна дипломатическа реакция от страна на ЕС, като се използват всички налични мерки на равнище ЕС.

Бързата и ефективна съвместна дипломатическа реакция на ЕС изисква надеждно и споделено ориентиране в обстановката и способност за бързо изготвяне на обща позиция на ЕС. Върховният представител на Съюза по въпросите на външните работи и политиката на сигурност ще насърчава и улеснява създаването на **работна група на държавите — членки на ЕС за киберразузнаване** в рамките на Центъра на ЕС за анализ на информация EU (INTCEN), за да стимулира стратегическото сътрудничество в областта на разузнаването в сферата на киберзаплахите и дейностите в киберпространството. Тази работа ще подпомогне допълнително ЕС да се ориентира в обстановката и да взема решения за съвместна дипломатическа реакция. Работната група следва да работи със съществуващите структури[85], включително, когато е необходимо, с онези, които отговарят за всеобхватната заплаха от хибридни атаки или намеса отвън, за да събират информация и да оценяват ситуационната осведоменост.

С цел да се укрепи способността на ЕС за предотвратяване, разколебаване, възпиране и реагиране спрямо злонамерени действия в киберпространството, върховният представител, с участието на Комисията и в съответствие със своите правомощия, ще представи предложение ЕС да определи допълнително **позицията си по кибервъзпирането**. Въз основа на досегашната работа в рамките на инструментариума

[81] https://www.consilium.europa.eu/bg/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

[82] Решение (ОВППС) 2019/797 на Съвета от 17 май 2019 г. относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки (ОВ L 129 I, 17.5.2019 г., стр. 13). и Регламент (ЕС) 2019/796 на Съвета
от 17 май 2019 г. относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки (ОВ L 129 I, 17.5.2019 г., стр. 1) 1)

[83] Решение (ОВППС) 2020/1127 на Съвета от 30 юли 2020 г. за изменение на Решение (ОВППС) 2019/797 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки (ST/9564/2020/INIT) (ОВ L 246, 30.7.2020 г., стр. 12). и Регламент за изпълнение (ЕС) 2020/1125 на Съвета от 30 юли 2020 г. за прилагане на Регламент (ЕС) 2019/796 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки (ОВ L 246, 30.7.2020 г., стр. 4).

[84] Решение (ОВППС) 2020/1537 на Съвета от 22 октомври 2020 г. за изменение на Решение (ОВППС) 2019/797 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки (ОВ L 351I, 22.10.2020, г. стр. 5–7);. Регламент за изпълнение (ЕС) 2020/1536 на Съвета от 22 октомври 2020 г. за прилагане на Регламент (ЕС) 2019/796 относно ограничителни мерки срещу кибератаки, застрашаващи Съюза или неговите държави членки (ОВ L 246, 30.7.2020 г., стр. -4).

[85] Например Единното звено на ЕС за анализ на разузнавателна информация (SIAC) и, когато е необходимо, проектите, разработени съгласно PESCO, както и системата за бързо предупреждение (RAS) от 2018 г., която беше създадена в подкрепа на цялостния подход на ЕС за борба с дезинформацията.

за кибердипломация позицията следва да допринесе за отговорно поведение на държавите в киберпространството и сътрудничество помежду им, като даде конкретни насоки за противодействие на кибератаките с най-значими последствия, по-специално онези, които засягат критичната ни инфраструктура, демократичните институции и процеси[86], както и атаките срещу веригата на доставки и кражбата на интелектуална собственост, извършвана чрез кибератаки. Тази позиция трябва да очертае как ЕС и държавите членки биха могли да използват своите инструменти за политическа, икономическа, дипломатическа, законова и стратегическа комуникация срещу злонамерени действия, както и да се занимае с начина по който ЕС и държавите членки биха могли да подобрят способността си да идентифицират отговорните за злонамерените действия лица. Освен това, заедно със Съвета и Комисията, върховният представител има за цел да разгледа възможността за **допълнителни мерки в рамките на инструментариума за кибердипломация**, включително възможността за допълнителни ограничителни мерки, както и да проучи възможността за **гласуване с квалифицирано мнозинство (ГКМ) за вписване в списъците по режима на хоризонтални санкции срещу кибератаките**. Освен това, ЕС следва да положи допълнителни усилия за **засилване на сътрудничеството с международните партньори**, включително НАТО, с цел по-добро споделено разбиране на ситуацията по отношение на заплахите, за разработване на механизми за сътрудничество и определяне на дипломатически реакции.

Върховният представител с участието на Комисията ще предложи също така актуализиране на насоките за **прилагане на инструментариума за кибердипломация**[87], включително с оглед повишаване на ефективността на процеса на вземане на решения, и ще продължи редовно да организира учения и оценки на интрументариума. Освен това, ЕС следва да продължи **да интегрира инструментариума за кибердипломация в механизмите на ЕС за действие при кризи**, да търси полезни взаимодействия с усилията за борба с хибридните заплахи, дезинформацията и външната намеса в съответствие с общата рамка за борба с хибридните заплахи[88] и Европейския план за действие за демокрация. В този контекст ЕС следва да обмисли взаимодействието между инструментариума за кибердипломация и възможностите за употреба на член 42.7 от ДЕС и член 222 от ДФЕС[89].

2.4 Укрепване на способностите за киберотбрана

ЕС като цяло и държавите членки поотделно трябва да укрепят способностите си за предотвратяване и реагиране на киберзаплахи в съответствие с амбициозните цели на ЕС, определени в глобалната стратегия на ЕС от 2016 г.[90]. За целта върховният представител заедно с Комисията ще представи **преглед на Политическата рамка на ЕС за кибернетична отбрана (ПРКО),** за да подобри по-нататъшната координация и

[86] Например като се търсят полезни взаимодействия с инициативите в рамките на Плана за действие за европейска демокрация.
[87] 13007/17
[88] https://eur-lex.europa.eu/legal-content/BG/TXT/HTML/?uri=CELEX:52016JC0018&qid=1608555320383&from=EN
[89] Съответно клаузата за взаимна отбрана, клаузата за солидарност.
[90] Заключения на Съвета (14149/16) относно изпълнението на глобалната стратегия на ЕС в областта на сигурността и отбраната.

сътрудничество между участниците от ЕС[91], както и с държавите членки и помежду тях, включително по отношение на мисиите и операциите по линия на общата политика за сигурност и отбрана (ОПСО). ПРКО следва да предостави информация за предстоящия стратегически курс[92], като гарантира, че киберсигурността и киберотбраната са допълнително интегрирани в по-широката програма за сигурност и отбрана.

През 2018 г. ЕС определи киберпространството като област на операции[93]. **„Военната визия и стратегия за киберпространството като област на операции“** предстои да бъде публикувана от Военния комитет на ЕС и чрез нея допълнително да се определи по какъв начин киберпространството като сфера на операции открива възможност за военни мисии и операции на ЕС по линия на ОПСО. Военната мрежа CERT[94], създадена от Европейската агенция по отбрана (EDA), ще допринесе допълнително за значително засилване на сътрудничеството между държавите членки. Освен това, за да се гарантира киберсигурността на критичните космически инфраструктури, за които отговаря космическата програма, ролите на Агенцията на Европейския съюз за космическата програма и по-специално Центърът за наблюдение на сигурността на „Галилео“ ще бъдат подсилени, а мандатът на Агенцията ще бъде разширен и ще включва и други активи с ключово значение на космическата програма.

ЕС и неговите държави членки следва да дадат допълнителен импулс за **разработването на най-съвременни способности за киберотбрана** чрез различни политики и инструменти на ЕС, по-специално CDPF, и където е подходящо, да използват за основа извършеното от EDA. Това изисква по-настойчиво разработване и използване на ключови технологии като ИИ, криптиране и квантови изчисления. В съответствие с приоритетите за развитие на способностите на ЕС[95] и въз основа на констатациите на доклада за първия координиран годишен преглед на отбраната (CARD)[96], ЕС следва допълнително да насърчи сътрудничеството между държавите членки в **научните изследвания, иновациите и развитието на способности в областта на киберотбраната**, като окуражава държавите членки да използват целия потенциал на **постоянното структурирано сътрудничество (PESCO)[97]** и **Европейския фонд за отбрана[98]**.

---

[91] По-специално EEAS, включително Военният секретариат на ЕС (ВСЕС), Европейският колеж по сигурност и отбрана (ЕКСО), Комисията, агенциите на ЕС, по-специално Европейската агенция по отбрана (EDA).

[92] Заключения на Съвета относно сигурността и отбраната от 17 юни 2020 г. (8910/20).

[93] https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

[94] Създаването на военната мрежа CERT на ЕС отваря на цел, която беше определена в Политическата рамка за кибернетична отбрана от 2018 г. и която има за цел да насърчава активното взаимодействие и обмена между военните мрежи CERT на държавите — членки на ЕС.

[95] През юни 2018 г. държавите членки се споразумяха в рамките на Управителния съвет на EDA да направляват сътрудничеството в сферата на отбраната на равнище ЕС.

[96] Одобрено от министрите на отбраната на Управителния съвет на EDA през ноември 2020 г. https://www.eda.europa.eu/what-we-do/our-current-priorities/coordinated-annual-review-on-defence-(card)

[97] Понастоящем съществуват няколко проекта по линия на PESCO, по-специално платформа за обмен на информация относно киберзаплахи и реагиране при инциденти, екипи за бързо реагиране при кибератаки и за взаимопомощ в областта на киберсигурността (CRRT), Център на ЕС за академично и иновационно сътрудничество в кибернетичната област и Координационен център в областта на киберсигурността и информацията (CIDCC).

[98] В рамките на Европейския фонд за отбрана Комисията вече набеляза възможности за евентуални съвместни научноизследователски и развойни действия в областта на киберотбраната, насочени към

Предстоящият **план за действие на Комисията относно полезните взаимодействия между гражданската, отбранителната и космическата промишленост**, който ще бъде представен през първото тримесечие на 2021 г., ще включва действия за по-нататъшно подпомагане на полезните взаимодействия на равнище програми, технологии, иновации и стартиращи предприятия, в съответствие с управлението на съответните програми[99].

Освен това следва да се разработят подходящи полезни взаимодействия и интерфейси между инициативите за киберотбрана, предприети в други рамки, включително свързаните с киберпространството съвместни проекти[100] на държавите членки в рамките на ПСС, както и със структурите на ЕС в областта на киберсигурността, за да се подпомогне обменът на информация и взаимната подкрепа.

Стратегически инициативи

ЕС трябва да:

- завърши изграждането на рамката за управление на кризи в областта на киберсигурността и да определи процеса, етапите и графика за създаване на съвместното звено за киберсигурност;
- продължи изпълнението на програмата за киберпрестъпността в рамките на стратегията за Съюза на сигурност;
- окуражи и улесни създаването на работна група за киберразузнаване на държавите членки в рамките на Центъра на ЕС за анализ и информация (EU INTCEN);
- усъвършенства подхода на ЕС за възпиране цел да предотвратява, разколебава, възпира и реагира на злонамерени действия в киберпространството;
- преразгледа политическата рамка за кибернетична сигурност;
- улесни разработването на „Военната визия и стратегия на ЕС относно киберпространството като област на операции“ за военни мисии и операции по линия на ОПСО;
- подкрепи полезните взаимодействия между гражданската, отбранителната и космическата промишленост; както и
- да повиши кибернетичната сигурност на космическите инфраструктури с ключово значение в рамките на космическата програма.

3. ПОСТИГАНЕ НА НАПРЕДЪК В СЪЗДАВАНЕТО НА СВЕТОВНО И ОТВОРЕНО КИБЕРПРОСТРАНСТВО

ЕС трябва да продължи да работи с международните партньори за насърчаване на политически модел и виждане за основано на първенството на правото, човешките

укрепване на сътрудничеството, капацитета за иновации и конкурентоспособността на отбранителната промишленост.

[99] Например „Хоризонт Европа“, „Цифрова Европа“ и ЕФО

[100] https://pesco.europa.eu/

права, основните свободи и демократичните ценности киберпространство, което работи за социалното, икономическото и политическото развитие в световен мащаб и допринася за Съюза на сигурност. Международното сътрудничество е от съществено значение за запазването на световното киберпространство отворено, стабилно и сигурно. ЕС следва да продължи да работи с трети държави, международни организации, както и с общността от заинтересовани страни, за да разработва и прилага последователна и цялостна международна политика в областта на кибернетичната сигурност, като има предвид нарастващата взаимосвързаност между икономическите аспекти на новите технологии, вътрешната сигурност, политиките в областта на външната политика, сигурността и отбраната. ЕС, като силен икономически и търговски блок, изграден върху основни демократични ценности, зачитане на правовата държава и основните права, има освен това и уникалната позиция да играе водеща роля при определянето и насърчаването на международните норми и стандарти.

3.1. Водеща роля на ЕС по отношение на стандартите, нормите и рамките в киберпространството

Засилване на процеса на стандартизация в международен план

За да популяризира и защити своето виждане за киберпространството на международно равнище, ЕС трябва да затвърди своите ангажименти и лидерска позиция в международните процеси на стандартизация и да засили представителството си в международните и европейските органи по стандартизация, както и в други организации за разработване на стандарти[101]. Тъй като цифровите технологии се развиват с бързи темпове, международните стандарти придобиват все по-голямо значение за допълването на традиционните регулаторни усилия в области като изкуствения интелект, изчисленията в облак, квантовите изчислителния и квантовата комуникация. Международната стандартизация все повече се използва от трети държави за прокарване на техните политически и идеологически програми, които не винаги съвпадат с ценностите на ЕС. Освен това съществува нарастващ риск от конкуриращи се рамки за международна стандартизация, което води до разпокъсаност.

Определянето на международните стандарти в областта на нововъзникващите технологии и основната архитектура на интернет в съответствие с ценностите на ЕС е от съществено значение, за да се гарантира, че интернет остава глобален и отворен, че технологиите са насочени към човека и запазването на неприкосновеността на личния живот, както и че тяхното използване е законно, безопасно и етично. Като част от бъдещата си стратегия за стандартизация ЕС трябва да определи своите **цели в областта на международната стандартизация** и да проведе активни и координирани дейности за тяхното популяризиране на международно равнище. Следва да се търси по-тясно сътрудничество и разпределяне на задачите със споделящи същите ценности партньори и европейски заинтересовани страни.

[101] Например Международната организация по стандартизация (ISO), Международната електротехническа комисия (IEC), Международния съюз по далекосъобщения (ITU), Европейски комитет по стандартизация(CEN), Европейския комитет за стандартизация в електротехниката (CENELEC), Европейския институт за стандарти в далекосъобщенията (ETSI), Работната група за интернет инженеринг (IETF), Проектът за партньорство от трето поколение (3GPP) и Институтът на инженерите по електричество и електроника (IEEE) (IEEE).

Насърчаване на отговорното поведение на държавите в киберпространството

ЕС продължава да работи с международните партньори за постигане на напредък и насърчаване на глобално, отворено, стабилно и сигурно киберпространство, в което се спазва международното право, по-специално Уставът на Организацията на обединените нации (ООН)[102], и където се следват **доброволните незадължителни норми, правила и принципи на отговорно поведение на държавите**[103]. С влошаването на ефективния многостранен дебат относно международната сигурност в киберпространството, налице е необходимост ЕС и неговите държави членки да заемат по-активна позиция в дискусиите, в ООН и други съответни международни форуми. ЕС може най-добре да **осигури напредък, да координира и да консолидира позициите на държавите членки на международните форуми**, и трябва да изработи **позиция на ЕС относно прилагането на международното право в киберпространството**. Върховният представител заедно с държавите членки също така трябва да придвижи тяхното приобщаващо и компромисно предложение за политически ангажимент за **програма за действие за насърчаване на отговорното поведение на държавите в киберпространството**[104] в ООН. Въз основа на съществуващите достижения на правото на ЕС, одобрени от Общото събрание на ООН[105], Програмата за действие предлага платформа за сътрудничество и обмен на най-добри практики в рамките на ООН и предлага да се създаде механизъм за прилагане на практика на нормите за отговорно поведение на държавите и за насърчаване на изграждането на капацитет. Освен това, върховният представител трябва да засили и насърчи прилагането на **мерки за изграждане на доверие** между държавите, включително обмен на най-добри практики на регионално и многостранно равнище и да подпомага трансрегионалното сътрудничество.

Нарасналата глобална свързаност не бива да води до цензура, масово наблюдение, пробиви в неприкосновеността на личния живот и репресии срещу гражданското общество, академичните среди и гражданите. ЕС трябва да продължи да играе водеща роля в защитата и насърчаването на **правата на човека и основните свободи** в киберпространството. За целта ЕС трябва да насърчава по-нататъшното спазване на международното право и международните стандарти в областта на правата на човека[106] и да приведе в действие своя план за действие относно правата на човека и демокрацията за 2020—2024 г.[107], да постигне напредък по линия на Насоките на ЕС в областта на правата на човека относно свободата на изразяване онлайн и офлайн[108], **като даде нов тласък на практическото прилагане на инструментите на ЕС**. ЕС трябва да полага постоянни усилия за **закрила на защитниците на правата на човека, гражданското общество и академичните среди, които работят по въпроси**

---

[102] https://www.un.org/en/sections/un-charter/un-charter-full-text/

[103] Както е отразено в съответните доклади на групите от правителствени експерти по развитието в областта на информацията и телекомуникациите в контекста на международната сигурност (UNGGEs), одобрени от Общото събрание на ООН, и по-специално в докладите за 2015 г., 2013 г. и 2010 г.

[104] https://front.un-arm.org/wp-content/uploads/2020/10/joint-contribution-poa-the-future-of-cyber-discussions-at-the-un-10302020.pdf

[105] Както е отразено в съответните доклади на групите правителствени експерти по развитието в областта на информацията и телекомуникациите в контекста на международната сигурност (UNGGEs), одобрени от Общото събрание на ООН, и по-специално в докладите за 2015 г., 2013 г. и 2010 г.

[106] По-специално Хартата на ООН и Всеобщата декларация за правата на човека.

[107] https://www.consilium.europa.eu/bg/press/press-releases/2020/11/19/council-approves-conclusions-on-the-eu-action-plan-on-human-rights-and-democracy-2020-2024/

[108] https://www.consilium.europa.eu/media/28348/142549.pdf

като киберсигурността, неприкосновеността на личните данни, наблюдението и онлайн цензурата. За целта ЕС трябва да осигури допълнителни практически насоки, да насърчава най-добрите практики и да положи допълнителни усилия за предотвратяване на злоупотребите с нововъзникващите технологии, по-специално чрез използването на дипломатически мерки, когато е необходимо, както и чрез контрол на износа на такива технологии. ЕС трябва също да продължи да се бори за защитата на онези членове на обществото, които са най-уязвими онлайн, като предложи законодателство за по-добра защита на децата от сексуално насилие и експлоатация, както и стратегия за правата на детето.

Конвенция от Будапеща за престъпленията в кибернетичното пространство

ЕС продължава да подкрепя трети държави, които желаят да се присъединят към Конвенцията от Будапеща на **Съвета на Европа за престъпленията в кибернетичното пространство**, и да работи за финализирането на **Втория допълнителен протокол към Конвенцията от Будапеща**, който включва мерки и гаранции за подобряване на международното сътрудничество между правоприлагащите и съдебните органи, както и между органите и доставчиците на услуги в други държави, в преговорите по който Комисията участва от името на ЕС[109]. Настоящата инициатива за нов правен инструмент за престъпленията в киберпространството на равнище ООН рискува да задълбочи разделението и да забави така необходимите национални реформи и свързаните с тях усилия за изграждане на капацитет, което би могло да възпрепятства ефективното международно сътрудничество в борбата с престъпленията в киберпространството: ЕС не вижда необходимост от нов правен инструмент относно престъпленията в киберпространството на равнище ООН. ЕС продължава да участва **в многостранния обмен по въпросите на киберпрестъпността**, за да гарантира зачитането на правата на човека и основните свободи чрез приобщаване и прозрачност, като отчита наличния експертен опит, за да осигури ползи за всички.

3.2 Сътрудничество с партньорите и общността от заинтересовани страни

Необходимо е ЕС да **засили и разшири диалога си с трети държави относно киберпространството**, за да популяризира своите ценности и виждане по този въпрос, да споделя най-добри практики и да се стреми към по-ефективно сътрудничество. ЕС следва също така да установи структуриран обмен с регионални организации като Африканския съюз, Регионалния форум на АСЕАН, Организацията на американските държави и Организацията за сътрудничество в областта на сигурността в Европа. Същевременно ЕС следва да се стреми да намери допирни точки с други партньори по въпроси от общ интерес, когато това е възможно и уместно. Като работи заедно с делегациите на ЕС и, когато е уместно, с посолствата на държавите членки по света, ЕС следва да създаде неформална **мрежа за кибердипломация на ЕС**, за да популяризира виждането на ЕС за киберпространството, да обменя информация и да провежда редовни консултации за координация по въпросите на развитието на киберпространството [110].

[109] Решение на Съвета от юни 2019 г. (реф. 9116/19)

[110] ЕС би могъл също така да използва, когато е уместно, дейностите на неформалната мрежа за цифрова дипломация на ЕС, включваща министерствата на външните работи на държавите членки.

Въз основа на съвместните декларации от 8 юли 2016 г.[111] и 10 юли 2018 г.[112] ЕС трябва да продължи да развива **сътрудничеството между ЕС и НАТО**, по-специално по отношение на изискванията за оперативна съвместимост в областта на кибернетичната отбрана. В този контекст ЕС трябва да продължи да работи за свързването на съответните структури на ОПСО към „Federated Mission Networking“ на НАТО, което ще позволи оперативна съвместимост между мрежите на НАТО и партньорите, когато е необходимо. Освен това следва допълнително да се проучи сътрудничеството между ЕС и НАТО в областта на образованието, обучението и ученията, включително чрез търсене на полезни взаимодействия между Европейския колеж по сигурност и отбрана и Съвместния център на НАТО за високи постижения в областта на кибернетичната отбрана.

В съответствие със своите ценности ЕС решително подкрепя и насърчава **многостранния модел за управление на интернет**. Нито един субект, правителство или международна организация не следва да се опитва да контролира интернет. ЕС следва да продължи да участва във форуми[113] за засилване на сътрудничеството и гарантиране на защитата на основните права и свободи, по-специално правото на достойнство, неприкосновеност на личния живот, свобода на изразяване и свобода на информация. С цел постигане на напредък в многостранното сътрудничество по въпросите на киберсигурността, в съответствие със съответните си правомощия Комисията и върховният представител се стремят да засилят **редовния и структуриран обмен със заинтересованите страни**, включително с частния сектор, академичните среди и гражданското общество, като подчертават, че взаимосвързаният характер на киберпространството изисква всички заинтересовани страни да обменят информация и да поемат своите конкретни отговорности за поддържане на глобално, отворено, стабилно и сигурно киберпространство. Тези усилия ще осигурят ценен принос за потенциални важни действия на равнище ЕС.

3.3. Укрепване на световния капацитет с цел повишаване на устойчивостта в световен мащаб

За да се гарантира, че всички държави имат възможност да извлекат социалните, икономическите и политическите ползи от интернет и използването на технологиите, ЕС продължава да подкрепя партньорите си в усилията им да повишават своята киберустойчивост и капацитета си за разследване и наказателно преследване на киберпрестъпността и за справяне с киберзаплахите. За да осигури съгласуваност в глобален мащаб, ЕС трябва да разработи **програма на ЕС за изграждане на външен киберкапацитет**, която да направлява тези усилия в съответствие с насоките на ЕС за изграждане на външен киберкапацитет[114] и с Програмата за устойчиво развитие до 2030 г.[115] . Програмата следва да използва експертния опит на държавите членки и съответните институции, органи, агенции и инициативи на ЕС, включително Мрежата на ЕС за изграждане на киберкапацитет[116], в съответствие с мандатите на посочените

[111] http://www.consilium.europa.eu/en/press/press-releases/2016/07/08-eu-nato-joint-declaration/
[112] https://www.consilium.europa.eu/bg/press/press-releases/2018/07/10/eu-nato-joint-declaration/
[113] Например Интернет корпорацията за присвоени имена и адреси (ICANN) и Форумът за управление на интернет (IGF).
[114] https://data.consilium.europa.eu/doc/document/ST-10496-2018-INIT/en/pdf
[115] https://ec.europa.eu/environment/sustainable-development/SDGs/index_en.htm
[116] https://www.eucybernet.eu/

организации. Създава се **Съвет на ЕС за изграждане на киберкапацитет**, който да обхваща съответните институционални заинтересовани страни от ЕС и да наблюдава напредъка, както и да установява допълнителни възможности за полезно взаимодействие, а също и потенциални пропуски. Освен това той може да подкрепя засиленото сътрудничество с държавите членки, както и с партньори от публичния и частния сектор и други съответни международни органи, за да се осигури координация на усилията и да се избегне дублиране.

Изграждането на киберкапацитета на ЕС трябва да продължи да поставя ударение върху Западните Балкани и съседните на ЕС държави, както и върху държавите партньори, които са в процес на бързо развитие в областта на цифровите технологии. Усилията на ЕС трябва да подкрепят разработването на законодателство и политики на държавите партньори в съответствие с относимите политики и стандарти на ЕС в областта на кибердипломацията. В този контекст усилията на ЕС за изграждане на капацитет в областта на цифровизацията следва да включват киберсигурността като стандартна характеристика. За целта ЕС следва да разработи програма за обучение, предназначена за служителите на ЕС, отговарящи за изпълнението на мерките на ЕС за изграждане на капацитет в областта на цифровите технологии и на външен киберкапацитет. ЕС трябва също така, в съответствие с усилията в рамките на Плана за действие за европейска демокрация, да помогне на тези държави да посрещнат нарастващото предизвикателство от злонамерени действия в киберпространството, които вредят на развитието на техните общества и на **целостта и сигурността на демократичните системи**. В това отношение особено полезно би могло да бъде партньорското обучение между държавите — членки на ЕС, съответните агенции на ЕС и трети държави.

Най-сетне в контекста на Гражданския пакт в областта на ОПСО от 2018 г.[117] гражданските мисии по линия на ОПСО могат също така да допринесат за по-всеобхватния отговор на ЕС за справяне с предизвикателствата в областта на киберсигурността, по-специално чрез укрепване на принципите на правовата държава в партньорските държави, както и на капацитета на техните правоприлагащи органи и граждански администрации.

Стратегически инициативи

ЕС трябва да:

- определи група от цели в международните процеси на стандартизация и да насърчава постигането на тези цели на международно равнище;
- налага сигурността и стабилността на киберпространството в международен аспект, по-специално с помощта на предложение от страна на ЕС и неговите държави членки за програма за действие за налагане на отговорно поведение на държавите в киберпространството (План за действие) в ООН;
- предостави практически насоки за прилагането на правата на човека и основните свободи в киберпространството;
- осигури по-добра защита на децата от сексуално насилие и експлоатация, както и

[117] https://data.consilium.europa.eu/doc/document/ST-14611-2019-INIT/bg/pdf

да приеме стратегия за правата на детето;

- укрепи и популяризира Конвенцията от Будапеща за престъпленията в киберпространството, включително чрез работата по втория допълнителен протокол към Конвенцията от Будапеща;
- разшири диалога в областта на кибернетичното пространство между ЕС и трети държави, регионални и международни организации, включително чрез неформална мрежа за кибердипломация на ЕС;
- засили обмена с многостранната общност, по-специално чрез редовен и структуриран обмен с частния сектор, академичните среди и гражданското общество; както и
- да предложи програма на ЕС за изграждане на външен киберкапацитет и на съвет на ЕС за изграждане на киберкапацитет.

III. КИБЕРСИГУРНОСТ В ИНСТИТУЦИИТЕ, ОРГАНИТЕ И АГЕНЦИИТЕ НА ЕС

С оглед на голямата си политическа значимост, важната си мисия да координират чувствителни въпроси и ролята им в управлението на големи суми публични средства **институциите, органите и агенциите на ЕС** редовно са обект на кибератаки, и по-специално на кибершпионаж. Между тези субекти обаче има значителни разлики по отношение на зрелостта на техните способности да засичат злонамерени действия в киберпространството и да реагират спрямо тях. Поради това е необходимо да се подобри общото равнище на киберсигурност чрез последователни и еднородни правила.

В областта на информационната сигурност бе постигнат напредък в посока към по-голяма съгласуваност на **правилата за защита на класифицираната информация на ЕС, както и на чувствителната некласифицирана информация**. Оперативната съвместимост на системите за класифицирана информация обаче остава ограничена, което възпрепятства безпроблемното предаване на информация между различните субекти. Необходим е допълнителен напредък, за да се даде възможност за междуинституционален подход към обработката на класифицирана информация на ЕС и на чувствителна некласифицирана информация, който би могъл да послужи и като модел за оперативна съвместимост между държавите членки. Следва също така да се определи модел за опростяване на процедурите с държавите членки. ЕС следва също така да доразвие способността си да общува по сигурен начин със съответните партньори, като се основава, доколкото е възможно, на съществуващите договорености и процедури.

Както беше обявено в стратегията за Съюза на сигурност, поради изложените причини през 2021 г. Комисията ще направи предложения за **общи задължителни правила относно информационната сигурност и за общи задължителни правила относно**

киберсигурността за всички институции, органи и агенции на ЕС въз основа на текущите междуинституционални обсъждания в ЕС относно киберсигурността[118].

Наблюдаваните в момента и прогнозираните тенденции при работа от разстояние също ще изискват допълнителни инвестиции в сигурно оборудване, инфраструктури и инструменти, които правят възможна работата от разстояние по чувствителни и секретни файлове.

Освен това все по-враждебната обстановка на киберзаплахи и зачестилите случаи на по-сложни кибератаки, засягащи институциите, органите и агенциите на ЕС, пораждат необходимост от повече инвестиции, за да се постигне висока степен на зрялост по отношение на сигурността в киберпространството. Създава се програма за киберграмотност за всички институции, органи и агенции на ЕС с цел запознаване на персонала с тематиката, по-голяма киберхигиена и изграждане на обща култура на киберсигурност.

Укрепването на CERT-EU с помощта на подобрен механизъм за финансиране е необходимо, за да се укрепи способността му да помага на институциите, органите и агенциите на ЕС да прилагат новите правила за киберсигурност и да подобряват своята киберустойчивост. Мандатът на CERT-EU също трябва да бъде подсилен и да му бъдат осигурени надеждни средства за постигане на поставените цели.

Стратегически инициативи

1. Регламент относно информационната сигурност в институциите, органите и агенциите на ЕС
2. Регламент относно общите правила за киберсигурност в институциите, органите и агенциите на ЕС
3. Нова правна уредба за CERT-EU, даваща възможност за по-силен мандат и увеличено финансиране.

IV. ЗАКЛЮЧЕНИЯ

Съгласуваното изпълнение на настоящата стратегия ще допринесе за постигането на киберсигурно цифрово десетилетие за ЕС, за изграждането на Съюз на сигурност и за укрепването на позицията на ЕС в световен мащаб.

ЕС трябва да определи стандарти и норми от най-високо световно равнище за решенията и правилата за киберсигурност по отношение на основните услуги и критичните инфраструктури, а също и за разработването и прилагането на новите технологии. Всяка организация и лице, което използва интернет, е част от решението за гарантиране на киберсигурна цифрова трансформация.

Комисията и върховният представител, в съответствие с правомощията си, ще наблюдават напредъка по тази стратегия и ще разработят критерии за оценка. Данните, които се събират за целите на наблюдението, следва да включват докладите на ENISA и редовните доклади на Комисията относно Съюза на сигурност. Резултатите ще се

[118] Редовните дискусии между институциите на ЕС по въпросите на киберсигурността са част от по-широк обмен на мнения относно възможностите и предизвикателствата на цифровата трансформация за институциите на ЕС.

използват при определянето на предстоящите цели на „Цифровото десетилетие“[119]. В съответствие с правомощията си Комисията и върховният представител ще продължат да поддържат връзка с държавите членки, за да набележат практическите мерки за сближаване на четирите общности в областта на киберсигурността в ЕС — критична инфраструктура и устойчивост на вътрешния пазар, правосъдие и правоприлагане, кибердипломация и киберотбрана, когато това е необходимо. Освен това Комисията и върховният представител ще продължат да работят с общността на заинтересованите страни, като подчертават необходимостта всеки, който използва интернет, да даде своя дял за поддържането на глобално, отворено, стабилно и сигурно киберпространство, в което всеки да може да живее безопасно в киберпространството.

[119]Както беше обявено в Работната програма на Комисията за 2021 г.

Допълнение: Следващи стъпки в областта на киберсигурността на 5G мрежите

Въз основа на резултатите от прегледа на препоръката на Комисията относно киберсигурността на 5G мрежите[120] следващите стъпки в координираната работа на равнище ЕС следва да се съсредоточат върху три ключови цели и върху основните действия в краткосрочен и средносрочен план, изложени в таблицата по-долу, които трябва да бъдат изпълнени от органите на държавите членки, Комисията и ENISA.

Първият приоритет за следващия етап е да се **завърши прилагането на инструментариума на национално равнище и да се решат проблемите, посочени в доклада за напредъка от юли 2020 г.** В този контекст някои от стратегическите мерки в инструментариума биха спечелили от **засилената координация или обмена на информация** в рамките на работния поток за МИС, както вече беше посочено в доклада за напредъка, което потенциално би могло да доведе до разработването на **най-добри практики или на насоки**. Що се отнася до техническите мерки, ENISA би могла да предостави допълнителна подкрепа въз основа на вече извършената от нея работа, като проучи по-задълбочено някои теми, както и като **разработи цялостен преглед на всички съответни насоки относно изискванията по отношение на киберсигурността на мрежите от пето поколение за операторите на мобилни мрежи.**

На второ място държавите членки подчертаха колко важно е да се върви в крак с технологиите, като **непрекъснато се наблюдава развитието им, архитектурата на мрежите от пето поколение, заплахите за тези мрежи, тяхното използване, както и външни фактори, за да се позволи набелязването на нови или нововъзникващи рискове и да се вземат съответните мерки.** Освен това редица аспекти в първоначалния анализ на риска следва да бъдат разгледани допълнително, по-специално за да се гарантира, че анализът обхваща цялата 5G екосистема, включително всички съответни части на мрежовата инфраструктура и на веригата на доставки на 5G. Въпреки че инструментариумът е проектиран да бъде гъвкав и приспособим, ако е необходимо, в средносрочен план могат да се предприемат стъпки той да бъде разширен или изменен, така че да се гарантира, че той остава широко приложим и актуален.

Трето, трябва да продължи предприемането на **действия на равнище ЕС**, за да се подкрепят и допълнят целите на инструментариума и те да бъдат изцяло интегрирани в съответните политики на Съюза и на Комисията, по-специално като се продължат действията, оповестени от Комисията в нейното съобщение относно инструментариума от 29 януари 2020 г.[121] в широк диапазон от области (например финансирането на мрежите от пето поколение, инвестиране в технологии за 5G мрежи и мрежи от последващи поколения, инструменти за защита на търговията и конкуренцията, за да се избегнат нарушения на пазара за доставки на 5G и др.).

[120]Доклад на Комисията за отражението на препоръката на Комисията от 26 март 2019 г. относно киберсигурността на 5G мрежите.

[121] Съобщение на Комисията COM(2020) 50, Сигурно внедряване на 5G в ЕС — прилагане на инструментариума на ЕС, 29 януари 2020 г.

Когато е целесъобразно, в началото на 2021 г. водещите участници трябва да постигнат подробни договорености и да определят етапни цели за основните действия, изложени по-долу.

Основна цел 1: Осигуряване на съгласувани национални подходи за ефективно намаляване на риска в целия ЕС		
Области	**Основни действия в краткосрочен и средносрочен план**	**Водещи участници**
Прилагане на инструментариума от държавите членки	Завършване на изпълнението на мерките, препоръчани в заключенията за инструментариума, до второто тримесечие на 2021 г. с периодичен преглед в рамките на работния поток за МИС.	Органи на държавите членки
Обмен на информация и най-добри практики относно стратегически мерки, свързани с доставчиците	Засилване на обмена на информация и разглеждане на възможни най-добри практики, по-специално относно: - Ограничения за високорискови доставчици (SM03) и мерки, свързани с предоставянето на управлявани услуги (SM04); - Сигурност и устойчивост на веригата на доставки, по-специално след проучването, проведено от ОЕРЕС относно SM05-SM06.	Органи на държавите членки, Комисията
Изграждане на капацитет и насоки за технически мерки	Провеждане на задълбочени технически проучвания и разработване на общи насоки и инструменти, в това число: - всеобхватна и динамична матрица от проверки за сигурност и най-добри практики за сигурността на 5G; Насоки в подкрепа на изпълнението на избрани технически мерки от инструментариума.	ENISA, органите на държавите членки
Основна цел 2: Подкрепа за непрекъснатост на обмена на знания и за изграждането на капацитет		
Области	**Основни действия в краткосрочен и средносрочен план**	**Водещи участници**
Непрекъснато натрупване на знания	Организиране на дейности за натрупване на знания за технологиите и свързаните с тях предизвикателства (отворени архитектури, характеристики на 5G — напр. виртуализация, контейнеризация, нарязване и др.), развитие на опасната среда, инциденти при реалната експлоатация, др.	ENISA, органи на държавите членки, други заинтересовани страни
Оценки на риска	Актуализиране и обмен на информация относно актуализираните национални оценки на риска	Органи на държавите членки, Комисията, ENISA
Съвместни проекти, финансирани от ЕС, в подкрепа на изпълнението на инструментариума	Предоставяне на финансова подкрепа на проекти, които подпомагат изпълнението на инструментариума с финансиране от ЕС, по-специално по линия на програмата „Цифрова Европа“ (напр. проекти за изграждане на капацитет за националните органи, изпитвателни платформи	Органи на държавите членки, Комисията

	или други авангардни капацитети и др.)	
Сътрудничество между заинтересованите страни	Насърчаване на съвместните действия и сътрудничеството между националните органи, ангажирани в областта на киберсигурността на 5G (напр. групата за сътрудничество в областта на МИС, органите за киберсигурност, регулаторните органи в областта на далекосъобщенията), и заинтересованите страни от частния сектор	Органи на държавите членки, Комисията, ENISA
Основна цел 3: Насърчаване на устойчивостта на веригата на доставки и други стратегически цели на ЕС в областта на сигурността		
Области	**Основни действия в краткосрочен и средносрочен план**	**Водещи участници**
Стандартизация	Определяне и прилагане на конкретен план за действие за засилване на представителството на ЕС в органите за определяне на стандарти като част от следващите стъпки от работата на подгрупата по стандартизация за МИС, за постигане на конкретни цели в областта на сигурността, включително насърчаване използването на оперативно съвместими интерфейси за улесняване на диверсификацията на доставчиците.	Органи на държавите членки
Устойчивост на веригата на доставки	— Да се извърши задълбочен анализ на екосистемата на технологията 5G и нейната верига на доставки с цел по-добро идентифициране и наблюдение на ключови активи и потенциални критични зависимости — Да се гарантира, че функционирането на пазара на технологията 5G и нейната верига на доставки е в съответствие с правилата и целите на ЕС в областта на търговията и конкуренцията, определени в съобщението на Комисията от 29 януари, както и че скринингът на ПЧИ се прилага към инвестиционните разработки, които потенциално засягат веригата за създаване на стойност в областта на 5G, като се вземат предвид целите на инструментариума — Да се наблюдават съществуващите и очакваните пазарни тенденции и да се оценяват рисковете и възможностите в областта на отворената RAN, по-специално чрез независимо проучване	Органи на държавите членки, Комисията
Сертифициране	Да се започне подготовката на съответните проекти за схеми за сертифициране за ключови 5G компоненти и процеси на доставчиците, за да се подпомогне преодоляването на определени рискове, свързани с техническата уязвимост, както е определено в плановете на инструментариума за намаляване на риска.	Комисията, ENISA, националните органи, други заинтересовани страни

Капацитет на ЕС и сигурно разгръщане на мрежата	— Да се инвестира в научни изследвания и капацитет, по-специално чрез приемането на Партньорството за интелигентни мрежи и услуги. — Да се прилагат съответните условия за сигурност за програмите на ЕС за финансиране и финансовите инструменти (вътрешни и външни), както беше обявено в съобщението на Комисията от 29 януари.	Държавите членки, Комисията, заинтересованите страни от сектора на 5G
Външни аспекти	Да се отговори положително на исканията на трети държави, които биха желали да разберат и евентуално да използват подхода на инструментариума, разработен от ЕС.	Държавите членки, Комисията, ЕСВД, делегациите на ЕС