Съвет на
Европейския съюз

Брюксел, 6 декември 2024 г.
(OR. en)

16527/24

CYBER 360
TELECOM 369
COSI 231
COPEN 535
CSDP/PSDC 854
DATAPROTECT 347
RECH 534
HYBRID 146
IPCR 72
JAI 1814
RELEX 1549
POLMIL 420

РЕЗУЛТАТИ ОТ РАБОТАТА

От:	Генералния секретариат на Съвета
До:	Делегациите
Относно:	Заключения на Съвета относно ENISA

Приложено на делегациите се изпращат заключенията на Съвета относно ENISA, одобрени от Съвета на неговото заседание, проведено на 6 декември 2024 г.

ПРИЛОЖЕНИЕ

Проект за заключения на Съвета относно ENISA

СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

1. ПОДЧЕРТАВА, че предизвикателствата, произтичащи от глобалното киберпространство, никога не са били толкова комплексни, разнородни и значими, колкото сега, поради сложността на възникващите киберзаплахи, постоянно променящата се обстановка в областта на сигурността и настоящото геополитическо напрежение. Поради това ЕС и неговите държави членки следва да продължат да полагат усилия за повишаване на устойчивостта с оглед на ефективното идентифициране и справяне с настоящите и нововъзникващите заплахи и предизвикателства. ИЗТЪКВА, че работата за повишаване на киберустойчивостта следва да продължи, като се следва подход, обхващащ цялото общество. ПОДЧЕРТАВА, че през следващите години ЕС и неговите държави членки следва да се съсредоточат върху ефективното прилагане на законодателните и незаконодателните инициативи, които стоят в основата и допринасят за всички действия, предприети до момента в това отношение.

2. Като ПРИПОМНЯ, че всяка държава членка носи пълна отговорност за националната си сигурност, ОТЧИТА, че през последните години ЕС и неговите държави членки положиха огромни съвместни усилия за създаването на необходимата институционална структура и форми на сътрудничество както на национално равнище, така и на равнище ЕС в киберпространството. ПРИВЕТСТВА различните законодателни и незаконодателни инициативи, които предоставиха на ЕС и неговите държави членки стабилна и надеждна рамка в тази област, като повишиха цялостната киберустойчивост на Съюза. Тази рамка се разви, като обхвана няколко аспекта на киберпространството: сигурност, дипломация, правоприлагане и отбрана. ОТБЕЛЯЗВА, че голям брой участници, включително органите за киберсигурност на държавите членки, групата за сътрудничество за МИС, мрежата на ЕРИКС, европейската мрежа за връзка на организациите при кибернетични кризи (EU-CyCLONe), мрежата от националните координационни центрове, европейската група за сертифициране на киберсигурността, Комисията, Европейската служба за външна дейност (ЕСВД), Агенцията на Европейския съюз за киберсигурност (ENISA), Европейският център за експертни познания в областта на киберсигурността, CERT-EU, Европейската агенция по отбрана (EDA) и Европейският център за борба с киберпрестъпността (EC3) на Европол, са част от екосистемата на ЕС на киберсигурност, като всеки от тях изпълнява своята роля в прилагането на рамката в областта на киберсигурността в целия ЕС.

3. ПРИЗНАВА, че през последните две десетилетия ENISA се доказа като безценна структура в европейската екосистема на киберсигурност, която играе решаваща роля за активната подкрепа на държавите членки и институциите, органите, службите и агенциите на ЕС при прилагането и разработването на политики в областта на киберсигурността, в изграждането на капацитет и подготвеността им, в сътрудничеството им и в насърчаването на осведомеността и сертифицирането в областта на киберсигурността.

ОБЩИ ПРЕПОРЪКИ ПО ПОЛИТИКАТА

4. ПРИКАНВА Комисията да използва **оценката на Акта за киберсигурността** като възможност да проучи как той може да допринесе за опростяването на сложната екосистема на киберсигурност, като по този начин повиши ефективността и ефикасното използване на ресурсите. Поради това ПРИЗОВАВА Комисията да осигури целенасочен и ясно определен мандат на ENISA в подкрепа на държавите членки и институциите, органите, службите и агенциите на ЕС, с конкретни стратегически цели и приоритетни задачи, както и по-прецизно разпределение на задачите и компетентностите по отношение на други участници. Във връзка с това ПРИКАНВА Комисията да проучи и допълнително да засили ролята на ENISA в подкрепа на оперативното сътрудничество на равнището на ЕС и между държавите членки за повишаване на киберустойчивостта, като се вземат предвид компетентностите на държавите членки в тази област. Наред с това ПРИЗОВАВА Комисията да засили консултативната роля на ENISA при предоставянето на експертни и основани на доказателства насоки и препоръки по отношение на изпълнението на настоящите и бъдещите законодателни и незаконодателни инициативи на ЕС, като същевременно гарантира съгласувана рамка на ЕС в областта на киберсигурността.

5. В същия дух НАСЪРЧАВА Комисията да разгледа възможността за рационализиране на ролята на ENISA по отношение на задачите, които не са основополагащи за нейната мисия. ПОДЧЕРТАВА, че **отговорностите на ENISA бяха значително разширени** чрез неотдавнашни законодателни инициативи, включително, наред с другото, МИС 2, Законодателния акт за киберустойчивост и Законодателния акт за киберсолидарност. Като ОТБЕЛЯЗВА, че макар и ENISA да е получила допълнителни ресурси в резултат на някои от тези инициативи, ИЗТЪКВА, че разширяването на отговорностите на ENISA и нарастващата сложност на киберзаплахите и предизвикателствата са довели до значително увеличаване на нейните задачи, което следва да намери отражение в набавянето на **достатъчно ресурси** — човешки, финансови и технически — за да може Агенцията да изпълнява пълноценно всички задачи, които попадат в обхвата на нейната компетентност, без да се засягат преговорите по многогодишната финансова рамка. За тази цел ПРИЗОВАВА Комисията при изготвянето на проекта за общ бюджет на Съюза да даде приоритет на действията и задачите, свързани с подпомагането на държавите членки за повишаване на киберустойчивостта им, оперативното им сътрудничество и разработването и прилагането на правото на Съюза.

ПОДКРЕПА НА ENISA ЗА РАЗРАБОТВАНЕТО И ПРИЛАГАНЕТО НА ПОЛИТИКИ

6. ПРИПОМНЯ, че съгласно настоящата правна рамка в областта на киберсигурността на ENISA са възложени няколко ключови отговорности за подкрепа и консултиране в целия ЕС. ПРИВЕТСТВА ролята на ENISA в това отношение за предоставяне на **помощ на държавите членки** за ефективното прилагане на законодателни и незаконодателни инициативи. ПРИЗОВАВА ENISA, в тясно сътрудничество с групата за сътрудничество за МИС и Комисията, да продължи да предоставя обща информация и анализ относно настоящата правна среда с оглед на киберсигурността. НАСЪРЧАВА ENISA да споделя и активно и редовно да популяризира технически насоки и най-добри практики по структуриран начин, като подпомага държавите членки при прилагането на политиката и законодателството в областта на киберсигурността.

7. ОТЧИТА жизненоважната роля на ENISA в разработването на **европейски схеми за сертифициране на киберсигурността**, които са в основата на доверието в продуктите, услугите и процесите в областта на ИКТ, както и в управляваните услуги за сигурност, с оглед на предстоящото целево изменение на Акта за киберсигурността. ИЗТЪКВА, че държавите членки и секторът са загрижени във връзка с продължителния процес на подбор, разработване и приемане на схеми за сертифициране на киберсигурността; поради това НАСТОЙЧИВО ПРИКАНВА Комисията да използва оценката на Акта за киберсигурността, за да намери начини за по-опростен, основан на риска, както и по-прозрачен и по-бърз подход към разработването на схеми на ЕС за сертифициране на киберсигурността, като същевременно ИЗТЪКВА важната роля на държавите членки в процеса. Наред с това ПОДЧЕРТАВА значението на изричното възлагане на отговорност за поддръжката на всяка схема за сертифициране. Освен това ПРИПОМНЯ, че ENISA следва да се консултира своевременно с всички съответни заинтересовани страни чрез официален, открит, прозрачен и приобщаващ процес при изготвянето на проекти за схеми и че Комисията следва да се консултира по открит, прозрачен и приобщаващ начин при оценката на ефективността и използването на приетите схеми. НАСЪРЧАВА ENISA да засили допълнително сътрудничеството с общността в областта на защитата на данните, по-специално с Европейския комитет по защита на данните, при целесъобразност, и с националните компетентни органи, като се обърне специално внимание на насърчаването на полезните взаимодействия в контекста на разработването на бъдещи европейски схеми за сертифициране на киберсигурността.

8. За да се предотврати ненужната административна тежест, която би могла да възникне поради сложната рамка за докладване, ПРИЗОВАВА ENISA, в сътрудничество с Комисията, да продължи да обменя информация с държавите членки относно практическите аспекти, опростяването и рационализирането на процедурата за докладване. Освен това ПРИПОМНЯ призива си към Комисията да изготви, с подкрепата на ENISA и други имащи отношение структури на ЕС, опис на съответните задължения за докладване, съдържащи се в приложимите законодателни актове на ЕС по въпросите на киберсигурността и цифровите технологии. ПРИПОМНЯ, че обменът на информация между ENISA и държавите членки се основава на отношения на доверие, при които сигурността и поверителността са гарантирани в съответствие с Акта за киберсигурността и приложимите правила и протоколи, и следва да бъде ограничен до това, което е уместно и пропорционално спрямо целта му. ПОДЧЕРТАВА необходимостта от надлежно третиране на данните и информацията.

9. ИЗТЪКВА, че ENISA отговаря за създаването и поддържането на **единната платформа за докладване съгласно Законодателния акт за киберустойчивост**, която ще има конкретна оперативна добавена стойност, особено за активно използвани уязвимости и сериозни инциденти, засягащи сигурността на продукти с цифрови елементи. Предвид широкия обхват на това хоризонтално законодателство единната платформа за докладване следва да бъде ефективен и сигурен инструмент за улесняване на обмена на информация между националните ЕРИКС и ENISA. Поради това НАСТОЙЧИВО ПРИКАНВА ENISA да ускори създаването на платформата като основен приоритет, както и да осигури достатъчно човешки ресурси, за да се гарантира, че ще бъде готова до края на срока, определен в Законодателния акт за киберустойчивост.

10. ОТЧИТА ролята на ENISA за създаването на **европейска база данни за уязвимости**, която има за цел да осигури по-голяма прозрачност по отношение на оповестяването на уязвимости, като същевременно гарантира подходящо обработване на чувствителните данни. Като се има предвид краят на срока за транспониране на Директивата за МИС 2, НАСТОЙЧИВО ПРИКАНВА ENISA да ускори всички действия, необходими за осигуряване на гладкото функциониране на тази база данни. Наред с това ПРИКАНВА групата за сътрудничество за МИС да продължи, с помощта на ENISA, да публикува насоки, политики и процедури относно оповестяването на уязвимости.

11. ПРИЗНАВА ползите от **действието за подкрепа на киберсигурността**, изпълнявано от ENISA, което функционира като набор от услуги в областта на киберсигурността, предоставяни на държавите членки за допълване на техните усилия, както и опита на ENISA, натрупан в хода на неговото изпълнение. Във връзка с това ИЗТЪКВА, че ENISA следва да играе централна роля в управлението и функционирането на резерва за киберсигурност на ЕС. ПРИКАНВА ENISA да започне да набелязва необходимите услуги и тяхната наличност веднага след влизането в сила на Законодателния акт за киберсолидарност, за да направи резерва за киберсигурност на ЕС възможно най-полезен и съобразен с нуждите на потребителите във всички държави членки. ПРИКАНВА ENISA, след като ѝ бъде възложено, да включи държавите членки, по-специално чрез събиране на информация относно необходимите критерии и информиране за предстоящите обществени поръчки, на ранен етап от процеса на създаване на резерва за киберсигурност на ЕС. Приканва ENISA, след като ѝ бъде възложено, да гарантира, че процесът на подбор на надеждни доставчици на управлявани услуги за сигурност е прозрачен, открит, справедлив и позволява участието на доставчици от всички държави членки, независимо от размера им. Освен това ПРИПОМНЯ, че от ENISA се изисква да представи без ненужно забавяне насоки за оперативна съвместимост на трансграничните киберцентрове.

12. ПОДЧЕРТАВА, че **наблюдението на тенденциите при нововъзникващите технологии** в бързо развиваща се област като киберпространството е от съществено значение за поддържането и по-нататъшното укрепване на състоянието на киберсигурността ни. ОТЧИТА работата, извършена от ENISA, за привличане на вниманието на обществеността към рисковете и възможностите на технологии като изкуствения интелект и квантовите изчислителни технологии, което способства за по-доброто разбиране на настоящите предизвикателства. НАСЪРЧАВА ENISA да продължи да допринася за изпълнението на тези задачи, да се застъпва активно за изпълнението на препоръките ѝ и при целесъобразност да предоставя консултации и да си сътрудничи с Европейски център за експертни познания в областта на киберсигурността.

ПОДКРЕПА НА ENISA ЗА ДЪРЖАВИТЕ ЧЛЕНКИ ЗА ПОВИШАВАНЕ НА КИБЕРУСТОЙЧИВОСТТА И ОПЕРАТИВНОТО СЪТРУДНИЧЕСТВО

13. ПОДЧЕРТАВА, че ENISA изпълнява важна роля като **секретариат на двете ръководени от държавите членки мрежи за киберсътрудничество на равнище ЕС, а именно мрежата на ЕРИКС и EU-CyCLONe**. ИЗТЪКВА ценното участие на ENISA в групата за сътрудничество за МИС, по-специално чрез активното ѝ участие и техническия ѝ принос в различните работни направления. НАСЪРЧАВА ENISA да продължи да подкрепя функционирането и сътрудничеството на тези мрежи в бъдеще, тъй като те осигуряват основни канали за сътрудничество на държавите членки на различни равнища.

14. ИЗТЪКВА ОТНОВО необходимостта от повишаване на **общата ситуационна осведоменост** на равнището на ЕС, която допринася за състоянието на киберсигурността на ЕС, във връзка с откриването, предотвратяването и реагирането на киберинциденти. Във връзка с това ПОДЧЕРТАВА значението на дейностите по прогнозиране на ENISA, редовните доклади и оценките на заплахите, всички от които допринасят за подобряване на ситуационната осведоменост. НАСЪРЧАВА ENISA да работи в тясно сътрудничество с държавите членки, за да допринася за развитието на ситуационната осведоменост на равнище ЕС. Във връзка с това ОТЧИТА важната роля на ENISA заедно със CERT-EU и Европол за подкрепа на Съвета чрез ситуационни брифинги в контекста на инструментариума за кибердипломация, допълващи ситуационната осведоменост, осигурявана от единното звено за анализ на разузнавателна информация (SIAC), и ИЗТЪКВА необходимостта от изграждане на цялостна картина на заплахите от различни източници, включително частния сектор. Във връзка с това НАСЪРЧАВА по-нататъшното развитие на сътрудничеството на ENISA с ЕСВД, и по-специално с Центъра на ЕС за анализ на информация (INTCEN), при пълно зачитане на съответните им мандати.

15. ИЗТЪКВА, че Центърът за киберситуация и анализ на Комисията изпълнява вътрешна функция в рамките на Комисията и се подпомага чрез сътрудничеството си с ENISA и CERT-EU. С цел да се създаде максимален потенциал за полезни взаимодействия и да се намали сложността в рамките на екосистемата на киберсигурност на ЕС, ПРИКАНВА Комисията да вземе предвид резултатите от оценката на Акта за киберсигурността, както и обсъжданията на оценката на подробния план в областта на киберсигурността, за да оптимизира задачите на Центъра за киберситуация и анализ на Комисията и произтичащите от тях задачи на ENISA. НАСЪРЧАВА Комисията да избягва ненужното дублиране на задачи, като същевременно запази централната роля на ENISA в приноса за развитието на общата ситуационна осведоменост на равнището на Съюза в подкрепа на държавите членки, при надлежно зачитане на националните им компетентности.

16. ИЗТЪКВА, че развитието на общата ситуационна осведоменост е предпоставка за навременното и ефективно управление на кризи в Съюза като цяло. ПОДЧЕРТАВА, че на равнището на ЕС **в реагирането на мащабни киберинциденти** участват различни ключови участници и че в случай на такива инциденти ефективното сътрудничество между държавите членки се основава главно на мрежата на ЕРИКС и EU-CyCLONe. ENISA играе важна роля в управлението на киберкризи като секретариат на мрежата на ЕРИКС и EU-CyCLONe. ПРИКАНВА Комисията да използва оценката на подробния план в областта на киберсигурността, за да отрази по подходящ начин допълнителните задачи и отговорности, допринасящи за разработването на съвместна реакция при мащабни трансгранични киберинциденти или кризи, както и ролята, отредена на ENISA като секретариат на мрежата на ЕРИКС и EU-CyCLONe и от неотдавнашното законодателство в областта на киберсигурността.

17. ПОДЧЕРТАВА, че е важно да се организират редовни **учения в областта на киберсигурността**, които значително повишават готовността на ЕС за реагиране при инциденти и кризи. ОТЧИТА, че ENISA е натрупала ценен и богат опит в тази област чрез подкрепата си за държавите членки. ОТЧИТА важната роля на ENISA в етапите на планиране, подготовка, изпълнение и оценка на ученията в областта на киберсигурността и ИЗТЪКВА, че тя следва да продължи да бъде един от централните участници на равнището на ЕС, като се има предвид, че провеждането на тези учения следва да се основава на структурирани рамки и общи терминологии. ПРИКАНВА ENISA, мрежата на ЕРИКС и EU-CyCLONe да използват по най-ефективен начин съществуващите редовни учения за изпитване и подобряване на рамката на ЕС за реакция при кризи и да гарантират, че извлечените поуки се използват възможно най-пълноценно.

СЪТРУДНИЧЕСТВО НА ENISA С ДРУГИ УЧАСТНИЦИ В ЕКОСИСТЕМАТА НА КИБЕРСИГУРНОСТ

18. ИЗТЪКВА ОТНОВО, че поради хоризонталния характер на киберсигурността **сътрудничеството между всички участници на равнището на държавите членки и на равнището на Съюза**е от жизненоважно значение, и поради това ПОДЧЕРТАВА, че повишаването на цялостната киберустойчивост на европейско равнище изисква също съвместна работа между ENISA и други имащи отношение структури в областта на киберпространството.

19. ПОДЧЕРТАВА, че способността на институциите, органите, службите и агенциите на ЕС за поддържане на киберсигурност е от значение за цялостната киберустойчивост на равнището на ЕС, за което ролята на CERT-EU е безценна. Във връзка с това ПРИВЕТСТВА установеното структурирано сътрудничество между CERT-EU и ENISA и ги НАСЪРЧАВА да продължат тясното си сътрудничество в бъдеще.

20. С постигнатата финансова автономност Европейският център за експертни познания в областта на киберсигурността ще допринесе значително за развиването на силна европейска екосистема за научни изследвания, промишленост и технологии в киберпространството, включително умения за развитие на работната сила, в съответствие със своя мандат. НАСЪРЧАВА ENISA и Европейския център за експертни познания в областта на киберсигурността да продължат тясното си сътрудничество, особено във връзка с нуждите и приоритетите в областта на научните изследвания и иновациите, както и с уменията в областта на киберсигурността, за да се повиши конкурентоспособността на сектора на киберсигурността на Съюза. ПРИКАНВА Комисията да проучи как полезните взаимодействия в работата на ENISA и Европейския център за експертни познания в областта на киберсигурността могат да бъдат допълнително оптимизирани и как по-добре да се рационализират дейностите съгласно съответните им мандати.

21. ПОДЧЕРТАВА, че предоставянето на редовна актуална информация за картината на заплахите допринася за по-успешното определяне на мерките и инструментите, необходими за ефективна борба с киберпрестъпността. ПОДЧЕРТАВА добавената стойност на докладите на ЕС за съвместна оценка на киберсигурността (J-CAR), които са резултат от съвместното сътрудничество между ENISA, EC3 на Европол и CERT-EU, и вече са предоставили ценен принос за справяне с различните предизвикателства, включително борбата с киберпрестъпността. ПРИКАНВА ENISA и Европол да продължат да си сътрудничат по структуриран начин и в бъдеще.

22. ПОДЧЕРТАВА, че киберотбраната представлява важна и постоянно развиваща се част от борбата със заплахите, произтичащи от киберпространството. ИЗТЪКВА необходимостта ENISA да работи с ЕСВД и Комисията в случаите, когато играе роля в подкрепа на изпълнението на политиката на ЕС в областта на киберотбраната, в тясно сътрудничество с EDA, Европейския център за експертни познания в областта на киберсигурността и общността за киберотбрана. ПОДЧЕРТАВА ролята на ENISA като гражданска агенция. НАБЛЯГА НА ЗНАЧЕНИЕТО на задълбочаването и оптимизирането на гражданско-военното сътрудничество в областта на киберпространството в рамките на ЕС, включително ясно разделение на ролите и отговорностите между двете общности и между ЕС и НАТО, при пълно зачитане на принципите на приобщаване, реципрочност, взаимна откритост и прозрачност, както и автономността на двете организации при вземането на решения. НАСЪРЧАВА ENISA да продължи да работи за постигането на работни договорености с Агенцията на НАТО за комуникация и информация.

23. НАСЪРЧАВА ЕС да продължи да утвърждава нашите общи ценности и съвместни усилия в рамките на световните форуми, за да се гарантира свободно, глобално, отворено и сигурно киберпространство. ПОДЧЕРТАВА, че трансграничният характер на киберзаплахите и инцидентите изисква силно и ефективно сътрудничество не само на равнището на ЕС, но и **с международни организации и партньори**. ОТБЕЛЯЗВА, че международната ангажираност на ENISA следва да се съсредоточи върху стратегическите партньори и държавите — кандидатки за членство в ЕС, в съответствие с общата външна политика и политика на сигурност на ЕС. ПОДЧЕРТАВА, че в рамките на международната си ангажираност ENISA следва да действа в съответствие със своя мандат и съответните разпоредби на Акта за киберсигурността. ОТЧИТА необходимостта от изясняване, в съответствие с приложимите процедури, на международната ангажираност на ENISA, като се гарантира по-специално, че нейният управителен съвет е надлежно и своевременно информиран за свързаните с това дейности. НАСЪРЧАВА участието на ENISA в съответните международни рамки за сътрудничество в областта на киберсигурността, включително организации като НАТО и ОССЕ.

24. ОТНОВО ИЗТЪКВА, че ЕС и неговите държави членки често са откроявали пропуски в **уменията в областта на киберсигурността**. ПРИПОМНЯ, че Комисията и ENISA са въвели широка и всеобхватна рамка за предоставяне на насоки на всички заинтересовани страни като Европейската рамка за умения в областта на киберсигурността, съобщението относно Академията за умения в областта на киберсигурността и ежегодно организираната Европейска конференция за умения в областта на киберсигурността, и НАСЪРЧАВА Комисията и ENISA да се опират на тези инициативи, като специално вземат под внимание текущата дискусия относно консорциума за европейска цифрова инфраструктура (КЕЦИ). За тази цел ПРИКАНВА Комисията да поддържа връзка с държавите членки, заинтересовани от създаването на КЕЦИ. ОТЧИТА, че както ENISA, така и Европейският център за експертни познания в областта на киберсигурността носят отговорност за насърчаване на уменията в целия Съюз. ПРИКАНВА ENISA да даде приоритет на подкрепата на усилията на държавите членки в областта на уменията и образованието, повишаването на осведомеността на широката общественост и при целесъобразност да си сътрудничи с Европейския център за експертни познания в областта на киберсигурността.

25. ОТЧИТА, че през последните години ENISA е развила **сътрудничество с частния сектор**. ПРИПОМНЯ, че тъй като частният сектор непрекъснато следи картината на киберзаплахите, събраната от промишлеността информация би могла да спомогне за подобряване на общата ситуационна осведоменост. Поради това НАСЪРЧАВА ENISA, в тясно сътрудничество с държавите членки и всички структури на ЕС, да засили сътрудничеството с частния сектор.

26. ПРИЗОВАВА Комисията и ENISA да обмислят начини за засилване на сътрудничеството между ENISA и европейските органи по **стандартизация**. ПОДЧЕРТАВА необходимостта ENISA да увеличи експертния си опит в европейската стандартизация в областта на киберсигурността, наред с другото, чрез последващи действия и участие в дейности по стандартизация.

27. НАСТОЯТЕЛНО ПРИЗОВАВА Комисията и ENISA да проучат начините за допълнително оптимизиране на функционирането на рамката на ЕС за киберсигурност, като вземат предвид препоръките и предложенията, направени в настоящите заключения. Постоянното сътрудничество, приоритизирането на задачите и ресурсите, както и опростяването на сложната ситуация, свързана с киберсигурността, ще са ключови елементи за справянето с настоящите и бъдещите предизвикателства.