СИГУРНОСТТА В КИБЕРПРОСТРАНСТВОТО – КОЛЕКТИВНА ОТГОВОРНОСТ

Васил Ст. Ризов

гр. София 1505, ул. „Черковна“, № 90, Държавна комисия по сигурността на информацията, ел. поща: dksi@government.bg; vsrizov@abv.bg

SECURITY IN CYBERSPACE - COLLECTIVE RESPONSIBILITY

Vasil St. Rizov

ABSTRACT: *Over the last two decades, the Internet and more broadly cyberspace has had a tremendous impact on all parts of society. Our daily life, fundamental rights, social interactions and economies depend on information and communication technology working seamlessly. An open and free cyberspace has promoted political and social inclusion worldwide; it has broken down barriers between countries, communities and citizens, allowing interaction and sharing of information and ideas across the globe; it has provided a forum for freedom of expression and exercise of fundamental rights, and empowered people in their quest for democratic and more just societies.*

KEY WORDS: *CERT, computer security, critical information infrastructure, critical information infrastructure protection, cyberattack, cybercrime, cyber defense, cybergovernance, cybersecurity, cybersecurity strategy, cybersecurity system, cyberspace, EFMS, ENISA, ICT security, information assurance, information security, internet security, network and information security, network security, personal data protection*

1. Съвременни предизвикателства, заплахи, тенденции

През последните десетилетия интернет и по-общо киберпространството оказва все по-голямо значение върху нашата икономика и на практика върху всички сфери на нашето общество. Наличието на сигурен интернет е важна предпоставка и за създаването на надеждна среда за глобална търговия с услуги. Нашето ежедневие, социалните взаимодействия и икономиките ни зависят от безупречната работа на информационните и комуникационните технологии. Наличието на едно отворено и свободно киберпространство даде тласък на политическото и социалното приобщаване в световен мащаб, то премахна бариерите между държави, общности и граждани, възможността за свободна комуникация в него предостави свобода за взаимодействие и обмен на информация и идеи в световен мащаб, предостави форум за свободно изразяване на мнения и упражняване на основните права и подкрепи хората в стремежа им за демократични и по-справедливи общества.

Информационните и комуникационни технологии (ИКТ) се превърнаха в гръбнак на нашия икономически живот и са ресурс с критично значение за всички икономически сектори. Сега те са в основата на сложните системи, които поддържат функционирането на нашите икономики в ключови сектори като финансите, здравеопазването, енергетиката и транспорта; същевременно много бизнес модели са изградени върху непрекъснатостта на достъпа до интернет и безупречното функциониране на информационните системи.

Някои от тези основаващи се на ИКТ системи, услуги, мрежи и инфраструктури формират жизнено важна част от европейската икономика и общество, като или предоставят съществени продукти и услуги, или представляват основната платформа за други критични инфраструктури. Те се считат обикновено за критични информационни инфраструктури (КИИ)[1] тъй като тяхното разстройване или разрушаване би могло да окаже сериозно въздействие върху жизнено важни обществени функции. Днес ние повече от всякога зависим

от информационната и комуникационна инфраструктура за управлението на нашето общество, извършване на стопанска дейност и упражняване на правата и свободите си като граждани. Тя е важна предпоставка и за създаването на надеждна среда за глобална търговия с услуги.

Информационните системи обаче могат да бъдат засегнати от инциденти по отношение на сигурността, например човешки грешки, природни явления, технически повреди или злонамерени атаки. Тези инциденти стават все по-мащабни, по-чести и по-сложни. От проведената от Европейската комисия обществена онлайн консултация „Подобряване на мрежовата и информационната сигурност в ЕС“[2] става ясно, че през изминалата година 57 % от участниците са имали случаи на инциденти във връзка със сигурността на информационните системи, които са се отразили сериозно на техните дейности. Липсата на мрежова и информационна сигурност може да компрометира основни услуги, които зависят от целостта на мрежовите и информационните системи. Това от своя страна може да стане причина за спиране на стопански дейности, да доведе до значителни финансови загуби за икономиката на ЕС и да се отрази отрицателно на благосъстоянието на обществото.

Като комуникационен инструмент без граници цифровите информационни системи и най-вече интернет са взаимосвързани в различни държави и играят основна роля за улесняването на трансграничното движение на стоки, услуги и хора. Значителните нарушения в дейността на тези системи в една държава могат да засегнат и други държави, както и международната общност като цяло. Затова устойчивостта и стабилността на мрежите и информационните системи е от основно значение за завършването на цифровия единен пазар и за безпроблемното функциониране на вътрешния пазар. Вероятността и честотата на инцидентите и неспособността да се гарантира ефикасна защита вредят и на обществено доверие в мрежовите и информационните услуги. Проведеното през 2012 г. изследване на Евробарометър показва, че 38 % от ползвателите на интернет в ЕС имат притеснения относно сигурността на плащанията онлайн и са променили поведението си поради притеснения във връзка със сигурността - 18 % са по-малко склонни да пазаруват онлайн, а 15 % са по-малко склонни да използват услуги за интернет банкиране[3].

Следните факти илюстрират състоянието на киберсигурността днес:

Всеки ден циркулират около 150 000 компютърни вируса и 148 000 компютъра биват компрометирани.

Немалък дял от инцидентите в киберпространството са причинени от киберпрестъпността; Symantec счита, че жертвите на киберпрестъпленията в световен мащаб губят около 290 млрд. евро всяка година, докато според проучване на McAfee приходите за киберпрестъпността са 750 млрд. евро годишно.

Според Световния икономически форум има 10-процентна вероятност от значителен срив на критична информационна инфраструктура през следващото десетилетие, което би могло да нанесе щети от 250 млрд. щатски долара.

Междувременно, данните на Евростат показват, че от януари 2012 г. само 26 % от предприятията в ЕС са имали официално определена политика за защита на ИКТ[4].

Инцидентите в областта на киберсигурността стават все по-чести, по-значителни и по-комплексни и за тях няма граници. Тези инциденти могат да причинят значителни щети на безопасността и на икономиката.

Неслучайно проблемите на сигурността в киберпространството напоследък заемат съществено място в дневните редове на регионални и глобални форуми. Лидерите на водещи организации и държави от цял свят обръщат все по-сериозно внимание на заплахата от това важни обществени, политически и икономически проекти да бъдат компроментирани поради инциденти или преднамерени атаки срещу сигурността или интегритета на развиващите ги мрежови и информационни системи.

2. Политика за киберсигурност на Европейския съюз

В съобщение за медиите от 7 февруари тази година относно Плана на ЕС за киберсигурност за защита на отворения интернет и свободите и възможностите, които той предлага, заместник-председателят на Европейската комисия и комисар по въпросите на цифровите технологии Нели Крус заяви: *„Колкото повече хора разчитат на интернет, толкова повече очакват той да им предложи сигурност. Сигурният интернет защитава нашите права и свободи и способността ни да правим бизнес. Време е да се предприемат координирани действия — цената на бездействието е много по-висока от цената на действието.“* Отбелязано беше, че досегашните усилия на Европейската комисия и отделни държави членки бяха твърде разпокъсани, за да се справят с нарастващото предизвикателство. Трябва да се засилят усилията за предотвратяване, сътрудничество и по-голяма прозрачност по отношение на инцидентите в киберпространството.

Международната политика на ЕС за киберпространството насърчава зачитането на основните ценности на ЕС, определя стандарти за отговорно поведение, защитава прилагането на съществуващите международни закони в киберпространството, като подпомага държави извън ЕС при изграждането на капацитет за киберсигурността и насърчава международното сътрудничество по проблеми в киберпространство.

Безграничният и многопластов интернет се превърна в един от най-мощните инструменти за глобален напредък без правителствен надзор или правителствено регламентиране. Въпреки че частният сектор следва да продължи да играе водеща роля в изграждането и оперативното управление на интернет, необходимостта от изисквания относно прозрачността, отчетността и сигурността става все по-явна.

На 7 февруари тази година, Европейската комисия, заедно с върховния представител на Съюза по въпросите на външните работи и политиката на сигурност, публикува Стратегия за киберсигурност наред с предложение на Комисията за Директива в областта на мрежовата и информационната сигурност (МИС).

Стратегията за киберсигурност „Отворено, безопасно и сигурно киберпространство“[5], представлява цялостната визия на ЕС за това как най-добре да се предотвратяват кибернетични смущения и атаки и да се отговаря на тях. Целта е насърчаване на европейските ценности свобода и демокрация и осигуряване на безопасния растеж на цифровата икономика. Конкретните дейности са насочени към засилване на устойчивостта на информационните системи в киберпространство, намаляване на киберпрестъпността и укрепване на международната политика за киберсигурността и киберотбраната на ЕС.

В стратегията се представя визията на ЕС за кибернетична сигурност по отношение на **пет приоритета**:

- Постигане на устойчивост в киберпространството
- Чувствително намаляване на киберпрестъпността
- Разработване на политика за киберотбрана и способности, свързани с общата политика за сигурност и отбрана (ОПСО)
- Разработване на промишлени и технологични ресурси за киберсигурност
- Създаване на съгласувана международна политика на Европейския съюз за киберпространството и насърчаване на основните ценности на ЕС

В Стратегията за киберсигурност се разясняват принципите, от които следва да се ръководи политиката за киберсигурност както в ЕС, така и в международен план.

Основните ценности на ЕС важат в еднаква степен в цифровия и във физическия свят

Същото законодателство и норми, които се прилагат в другите области на нашия живот, важат и в киберпространството.

Защита на основните права, свободата на изразяване на мнение, личните данни и неприкосновеността на личния живот

Киберсигурността може да бъде надеждна и ефективна само ако се основава на основните права и свободи, залегнали в Хартата на основните права на Европейския съюз, и на основните ценности на ЕС. И обратното, правата на индивида не могат да бъдат обезпечени без сигурни мрежи и системи. За целите на киберсигурността, когато става въпрос за лични данни, всеки обмен на информация следва да е в съответствие със законодателството на ЕС за защита на данните и да отчита в пълна степен правата на личността в тази област.

Достъп за всички

Ограниченият достъп или липсата на достъп до интернет, както и цифровата неграмотност поставят гражданите в неблагоприятно положение, като се има предвид голямата степен на навлизане на цифровите технологии във всички дейности на обществото. Всеки трябва да има възможност за достъп до интернет и за безпрепятствен пренос на информация. Целостта и сигурността на интернет трябва да бъдат гарантирани, за да се предостави безопасен достъп за всички.

Демократично и ефикасно управление с участието на множество заинтересовани страни

Цифровият свят не се контролира от една-единствена организация. Понастоящем редица заинтересовани страни, много от които са търговски и неправителствени организации, участват в оперативното управление на интернет ресурси, протоколи и стандарти, както и в бъдещото развитие на интернет. ЕС потвърждава значението на всички заинтересовани страни в настоящия модел на управление на интернет и подкрепя този управленски подход с участието на множество заинтересовани страни.

Споделена отговорност за гарантирането на сигурността

Нарастващата зависимост от информационните и комуникационните технологии във всички области на човешкия живот доведе до слаби места, които трябва да бъдат правилно определени, внимателно анализирани, отстранени или ограничени. Всички съответни участници, независимо дали са публични органи, представители на частния сектор или отделни граждани, трябва да осъзнаят тази споделена отговорност, да предприемат действия, за да защитят себе си и, ако е необходимо, за да осигурят координиран отговор с цел укрепване на киберсигурността.

ЕС направи важни стъпки напред по отношение на защитата на гражданите от онлайн престъпления, включително като основа Европейския център за борба с киберпрестъпността, предложи законодателство в областта на атаките върху информационни системи и създаде Глобален алианс срещу сексуалното насилие над деца в интернет. Още една цел на стратегията е да разработи и финансира мрежа от национални центрове за високи постижения за борба с киберпрестъпността, за да се улесни обучението и изграждането на капацитет.

Предложението за Директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза[6] е важен елемент от цялостната стратегия и изисква от всички държави членки, основни доставчици на интернет и оператори на критични инфраструктури, като платформи за електронна търговия и социални мрежи, оператори в областта на енергетиката, транспорта, банковото дело и здравните услуги да гарантират сигурна и надеждна цифрова среда в целия ЕС.

Съгласно регулаторната рамка, залегнала в Директивата на Европейския парламент и на Съвета относно мерките за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза, само предприятията, работещи в сферата на далекосъобщенията, са длъжни да предприемат стъпки за управление на риска и да докладват за инциденти, свързани с МИС. Много други сектори обаче разчитат на ИКТ като на основен за тях фактор, и поради това също следва да проявяват загриженост по отношение на МИС. Някои конкретни доставчици на услуги и оператори на инфраструктура са особено уязвими поради това, че зависят в голяма степен от добре работещите мрежови и информационни системи. Тези отрасли играят основна роля при предоставянето на ключови за нашата икономика и общество услуги и сигурността на техните системи е от особен интерес за функционирането на вътрешния пазар. Сред тези сектори са публичните администрации, банковото дело,

фондовите борси, здравеопазването, производството, преносът и разпределението на енергия, транспортът (въздушен, железопътен, морски), интернет услугите и др.

Поради това е необходима радикална промяна в начина, по който се работи по мрежова и информационна сигурност в ЕС. За да бъдат осигурени еднакви условия, са необходими отговорности, регламентирани в законови норми. За да разреши тези проблеми и да повиши нивото на МИС в Европейския съюз, Директивата на Европейския парламент и на Съвета относно мерките за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза си поставя следните **цели**:

На първо място, поставя се изискването всички държави членки да гарантират, че са постигнали минимално ниво на национален капацитет, като са определили компетентни органи, сформирали са екипи за незабавно реагиране при компютърни инциденти (CERT) и са приели национални стратегии за МИС и национални планове за сътрудничество за МИС.

На второ място, националните компетентни органи следва да си сътрудничат в рамките на мрежа, която дава възможност за сигурна и ефективна координация, включително за координиран обмен на информация, както и за откриване и отговор на равнището на ЕС. Чрез тази мрежа държавите членки следва да обменят информация и да си сътрудничат в борбата срещу заплахите и инцидентите в сферата на МИС съгласно европейски план за сътрудничество за МИС.

На трето място, Директивата се стреми да гарантира развитието на култура на управление на риска и на обмен на информация между частния и публичния сектор. От предприятията в конкретните критични сектори и от публичните администрации ще се изисква да оценяват рисковете, пред които са изправени, и да приемат подходящи и пропорционални мерки за гарантиране на МИС. От тези субекти ще се изисква да докладват на компетентните органи за инцидентите, които компрометират в голяма степен техните мрежи и информационни системи и оказват значително въздействие върху непрекъснатостта на критичните услуги и доставката на стоки.

Предложената директива установява мерки, според които държавите членки трябва да приемат стратегия за киберсигурност и да определят национален компетентен орган по киберсигурност с достатъчни човешки и финансови ресурси, за да предотвратява, управлява и реагира в случай на рискове и инциденти в областта на МИС.

Създава се механизъм за сътрудничество между държавите членки и Комисията за споделяне на ранни предупреждения за рискове и инциденти чрез сигурна инфраструктура, за сътрудничество и за организиране на редовни партньорски оценки. Операторите на критични инфраструктури в някои сектори (финансови услуги, транспорт, енергетика и здравеопазване), доставчиците на услуги за информационното общество (по-специално: платформи за електронна търговия с приложения, плащания по интернет, изчисления в облак, търсачки, социални мрежи) и публичните администрации трябва да въведат практики за управление на

риска и да докладват значителни инциденти, свързани със сигурността на основните им услуги.

Държавите членки трябва да започнат да прилагат директивата в рамките на 18 месеца след приемането ѝ от Съвета и Европейския парламент (което се очаква да стане през 2014 г.).

По искане на Съвета и на Европейския парламент започна дебат за определяне на предизвикателствата и приоритетите за политиката за мрежова и информационна сигурност, както и на най-подходящите инструменти, необходими на нивото на ЕС за справяне с тях, при който ударението се поставя върху предотвратяването, готовността и информираността, като се формулира план за незабавни действия за укрепване на сигурността и устойчивостта на КИИ. Предлаганите действия са и допълнение към мерките за предотвратяване, борба и преследване на престъпни и терористични дейности, насочени срещу КИИ, и са в синергия със сегашните и бъдещите научни изследвания в ЕС в областта на мрежовата и информационната сигурност, както и с международните инициативи в тази област.

Комисията направи оценка на въздействието на три варианта на политиката:

Вариант 1: Запазване на обичайната практика („базисен вариант“); запазване на сегашния подход.

Вариант 2: Регулаторен подход, състоящ се от законодателно предложение, с което се създава обща правна рамка на ЕС за МИС по отношение на капацитета на държавите членки, механизмите за сътрудничество на равнище ЕС и изискванията по отношение на частните участници и публичните администрации, имащи ключова роля.

Вариант 3: Смесен подход, при който се съчетават доброволни инициативи по отношение на капацитета за МИС на държавите членки, механизми за сътрудничество на равнище ЕС и регулаторни изисквания по отношение на частните участници и публичните администрации, имащи ключова роля.

Комисията заключи, че вариант 2 би имал най-голямо положително въздействие, тъй като би подобрил значително защитата на потребителите, предприятията и държавното управление в ЕС срещу инциденти, заплахи и рискове, свързани с МИС. По-специално задълженията, вменени на държавите членки, ще гарантират адекватна готовност на национално равнище и ще допринесат за създаването на климат на взаимно доверие, което е предпоставка за ефективно сътрудничество на равнище ЕС. С изграждането на механизми за сътрудничество на равнище ЕС чрез мрежата ще се постигне последователна и координирана превенция и отговор на трансграничните инциденти и рискове в МИС. Въвеждането на изисквания за управление на риска в областта на МИС за публичните администрации и основните частни участници ще създаде силен стимул за ефективно управление на рисковете, свързани със сигурността.

В становището на Европейския икономически и социален комитет (ЕИСК) от 22 май 2013г., относно „Предложение за директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза“, се

посочва, че Комитетът е изключително разочарован от липсата на напредък от страна на много държави членки по отношение на осигуряването на ефективна МИС на национално равнище. Този неуспех създава повишени рискове за гражданите и оказва отрицателно въздействие върху доизграждането на единния цифров пазар. Всички държави членки трябва незабавно да предприемат действия във връзка с неизпълнените си задължения по отношение на МИС.

Тази липса на напредък създава друга цифрова пропаст между елитната група от десет държави членки, които са силно напреднали по отношение на МИС и онези, които са по-слабо развити в това отношение. Тези десет държави членки създадоха Групата на европейските правителствени CERT (EGC), чиито членове си поставиха за задача да работят в тясно сътрудничество по въпросите на МИС и реагирането на инциденти. Понастоящем не се приемат нови членове в EGC: засега останалите по-слабо развити 17 държави членки и новосформираният CERT-EC[7] са изключени от тази елитна група. Между държавите членки, които са силно напреднали в областта на МИС, и останалите се разкрива нова цифрова пропаст.

Тази пропаст пречи на доверието и сътрудничество в областта на МИС на равнището на ЕС и, ако не ѝ бъде обърнато спешно внимание, има вероятност да предизвика неуспехи на вътрешния пазар, свързани с различията в способностите на отделните държави членки. Ако тази пропаст по отношение на МИС не бъде преодоляна, ще бъдат отслабени основите на единния цифров пазар, което ще ограничи изграждането на доверие, хармонизирането и оперативната съвместимост. Освен това без решителни действия, пропастта между силно напредналите и по-малко напредналите държави членки вероятно ще се увеличи, а оттук ще се увеличат и неуспехите на вътрешния пазар, свързани с различията между държавите членки по отношение на техния капацитет.

Анализът на процесите в тази област до момента показва недвусмислено, че мерките с ориентировъчен и доброволен характер не вършат работа и че на държавите членки трябва да се наложат силни регулаторни задължения, за да се осигури хармонизирането, управлението и осъществяването на мрежовата и информационната сигурност в Европа. Някои водещи експерти по управление на МИС смятат, че настоящото предложение за директива не предоставя необходимото ясно и решително законодателство. За да се осигури необходимото високо общо равнище на МИС, вероятно ще бъде необходими по-строги мерки – регламент, с ясно определени обвързващи държавите членки задължения, би бил по-ефективен, отколкото директива.

Независимо от намерението на Европейската комисия да приеме делегирани актове с цел да осигури определени еднакви условия за изпълнение на части от директивата, в предложения акт има недостиг на стандарти, на ясни определения и на категорични задължения, което дава прекалено много свобода на държавите членки по отношение на тълкуването и транспонирането на критично важните му елементи. В този акт трябва да бъдат включени

много по-ясни определения на стандартите, изискванията и процедурите, касаещи държавите членки, публичните органи, пазарните оператори и лицата, които изпълняват ключова роля за предоставянето на интернет услуги.

Като се има предвид колко е важно всички държави членки да спазват изискванията за МИС в целия ЕС, Европейския икономически и социален комитет призова Комисията да обмисли какви средства от многогодишната финансова рамка (МФР) биха могли да бъдат насочени за подпомагане на онези държави членки, които се нуждаят от финансова помощ във връзка със спазването на изискванията за МИС.

Разходите за научни изследвания, развойна дейност и иновации за технологии, свързани с МИС, се очаква да бъдат основен приоритет в Рамковата програма на ЕС за научни изследвания и иновации „Хоризонт 2020“, така че Европа да върви в крак с бързо променящия се пейзаж на киберзаплахите.

За да се осигури яснота относно това кои предприятия имат правни задължения съгласно предложения акт, ЕИСК би желал всяка държава членка да бъде задължена да публикува онлайн директория на всички лица, за които се отнасят изискванията на директивата по отношение на управлението на риска и докладването. Тази прозрачност и обществена отчетност ще изградят доверие и ще осигурят подкрепа за спазването на законовите изисквания.

Успехът на Стратегията за киберсигурността и ефективността на предложената директива за МИС ще зависят от наличието на силна индустрия за МИС в Европа и достатъчно служители със специализирани умения в сферата на МИС. В този смисъл е положително, че в предложената директива е посочена необходимостта държавите членки да инвестират в образование, информираност и обучение по МИС. От съществено значение е също така всяка държава членка да положи специални усилия, за да информира, образова и подпомага сектора на малките и средни предприятия по отношение на киберсигурността. Големите предприятия могат лесно да придобият знанията, от които се нуждаят, но малките и средни предприятия имат нужда от подкрепа.

Пътят напред: увеличаване на координацията и сътрудничеството в ЕС

Понеже проблемът има общностно и международно измерение, единният подход на ЕС за повишаване на сигурността и устойчивостта на КИИ би допълнил и обогатил националните програми, както и съществуващите двустранни и многостранни схеми за сътрудничество между държавите-членки.

Обществените политически дискусии след събитията в Естония подсказват, че последиците от подобни атаки могат да бъдат ограничени чрез превантивни мерки и координирани действия по време на кризата. По-структуриран обмен на информация и добри практики в рамките на ЕС би улеснил значително борбата с трансгранични заплахи.

Необходимо е укрепване на съществуващите инструменти за сътрудничество, включително ENISA, и създаване при нужда на нови инструменти. От съществено значение е подход,

обхващащ различните участници и нива, осъществяван на европейско равнище, но същевременно изцяло зачитащ и допълващ националните компетенции. От значение е и времевият хоризонт. Налице е очевидна потребност да се действа сега и бързо да се въведат необходимите елементи за изграждане на рамка, която ще ни позволи да отговорим на сегашните предизвикателства и която ще може да се пренесе в бъдещата стратегия за мрежова и информационна сигурност.

За справяне с тези предизвикателства се предлагат **пет направления на действие**:

- Готовност и предотвратяване: за осигуряване на подготвеност на всички нива;
- Откриване и реагиране: за предоставяне на адекватни механизми за ранно предупреждение;
- Смекчаване на последиците и възстановяване: за укрепване на отбранителните механизми на ЕС за КИИ;
- Международно сътрудничество за утвърждаване в международен мащаб на приоритетите на ЕС;
- Критерии за сектора на ИКТ: да се подпомогне прилагането на Директивата относно установяването и означаването на европейските критични инфраструктури[8].

3. Политика и план за действие за киберотбрана на НАТО

По време на Косовската криза НАТО за първи път се сблъска с атаки в киберпространството. Наред с редица други проблеми в продължение на няколко дни бе блокирана и електронната поща на Алианса за външни посетители и на няколко пъти имаше поражения в уебсайта на организацията. Но тогава кибернетичното измерение на конфликта се възприе преди всичко като пречка за информационната кампания на НАТО. Кибератаките се приемаха за риск, но с ограничен обхват и малък потенциал за вреди, изискващ лека техническа намеса, придружена с дозирана информация за обществеността.

Събитията от 11 септември 2001 г. промениха тази представа. Като част от Пражкия ангажимент в областта на военните способности, приет през ноември 2002 г., НАТО отправи призив за подобряване на "способностите си за защита от кибератаки".

Същата година НАТО одобри триетапна Програма за киберотбрана. Първият етап включва Съюзна способност за отговор на компютърни инциденти (NCIRC). Вторият предвижда достигане на пълни оперативни способности на Центъра на NCIRC, а третият етап – елиминиране/намаляване на слаби места в киберотбраната и използване на нови технологии за намаляване на киберрисковете. Сред функциите на Съюзна способност за отговор на компютърни инциденти са: да отговаря на заплахи и уязвимости на компютърната сигурност; да обработва и докладва инцидентите и разпространява свързаната с тях информация; да концентрира управлението на инцидентите чрез едно централизирано и координирано усилие; и да смекчава ефектите от проблемите, свързани с компютърната сигурност.

Също така, NCIRC предоставя различни услуги като изпращане на специализирани бюлетини и доклади; управление на анти–злонамерен софтуер, включително предоставяне обновени антивирусни програми, управление на антивирусна поддръжка и заявки и визити за полева поддръжка на компютърни системи; мониторинг на съдържанието на съобщения; и защита на уеб-сайтове.

През следващите години обаче Алиансът се съсредоточи главно върху мерките за пасивна защита, изисквани от военните. Трябваше да се случат инцидентите в Естония и Грузия, съответно през 2007 и 2008 г., за да се насочи вниманието на политиците към тази нарастваща заплаха за обществената безопасност и държавната стабилност. Като следствие от кибератаките НАТО осъзна, че киберсигурността трябва да бъде поставена начело в списъка на новите предизвикателства към сигурността, с които Алиансът трябва да се справи в предстоящите години. Триседмичната вълна от масирани кибератаки показа, че обществата в държавите членки на НАТО са крайно уязвими на кибернетичния фронт. Тези събития подтикнаха Алианса радикално да преосмисли нуждата си от политика за киберзащита и да отдаде по-голямо значение на контрамерките. Инцидентите през следващите години помогнаха да се осъзнае още по-пълно колко е сериозна заплахата и НАТО започна да се адаптира към този нов вид предизвикателство в областта на сигурността.

През 2008 г. бяха одобрени официална политика на НАТО по киберсигурността и съвместна съюзна концепция за киберзащита, както и е сертифициран Кооперативен център за високи постижения по киберотбраната на НАТО (COE CCD). Същата година е създаден и нов орган за ръководство на киберотбраната (NATO Cyber Defence Management Authority – NCDMA) с борд. През 2010 г. заработи и нова дирекция в Международния секретариат на НАТО (Emerging Security Challenges Division), която фокусира дейността си върху тероризма, енергийната сигурност и киберотбраната.

В израз на общата загриженост в тази област, на срещата на върха 2010 Лисабон, държавните глави възложиха на Северноатлантическия съвет да разработи ревизирана политика на НАТО за кибер отбрана. Първоначално, през март 2011 г., за министрите на отбраната беше очертана Концепция за киберотбрана на НАТО, която формира концептуалната основа на ревизираната политика на НАТО за киберотбрана.

„Кибератака може да постави на колене една страна, без нито един войник да трябва да прекоси границата й, и не е никак преувеличено да се заяви, че кибератаките се превърнаха в нова форма на постоянна война на ниско равнище” – Думите на генералният секретар на НАТО Андерс Фог Расмусен илюстрират съвременното виждане на НАТО по въпроса за заплахите в киберпространството.

Това ново предизвикателство беше включено в дневния ред на срещата на министрите на отбраната от НАТО през юни 2011 г. в Брюксел. Министрите се договориха за ревизирана Политика за кибер отбрана, която не само ще гарантира по-бърза и по-ефективна защита на собствената мрежа на НАТО, но ще предостави на съюзниците и на партньорите по-голяма

помощ за предотвратяване на кибер атаките, справянето с тях и ограничаването на последствията от тях.

Тази ревизирана Политика за кибер отбрана на НАТО е фокусирана върху виждането, че за да изпълнява основните задачи на Алианса за колективна отбрана и управление на кризи, НАТО трябва да гарантира интегритета и непрекъснатото функциониране на информационните си системи. Следователно основна задача на НАТО е защитата на собствените комуникационни и информационни системи. При това, за по-добра защита на своите информационни системи и мрежи, НАТО трябва да увеличи капацитета си за справяне с широкия спектър от кибернетични заплахи, пред които понастоящем е изправен. Един по-задълбочен преглед на ролята на НАТО в кибернетичната отбрана показва обаче, че в основният фокус на политиката на НАТО по кибер отбрана се намира не само защитата на собствените мрежи на НАТО, но са поставени и изисквания към кибер отбраната, свързани с националните мрежи, на които НАТО разчита за изпълнение на своите основни задачи: колективна защита и управление на кризи. Този подход е приложен и при формулиране на **основните цели** на Политиката на НАТО за кибер отбрана.

• Интегриране на вижданията за кибер отбрана в структурите и процеса на планиране на НАТО, с оглед изпълнение основните задачи на НАТО за колективна защита и управление на кризи.

• Фокусиране върху превенцията, устойчивост и защита на критичните кибер активи на НАТО и съюзниците.

• Разработване на надеждни способности за кибер отбрана и централизиране защитата на собствените мрежи на НАТО.

• Разработване на минималните изисквания за кибер защита на националните мрежи, критични за основните задачи на НАТО.

• Оказване съдействие на съюзниците за достигане на минималното ниво на кибер отбрана и намаляване уязвимостта на националните критични инфраструктури.

• Ангажиране с партньори, международни организации, частния сектор и академичните среди.

Политиката за кибер отбрана беше предложена и одобрена с инструмент за нейното прилагане – План за действие, който представлява подробен документ с конкретни задачи и дейности за собствените структури на НАТО и на отбранителните сили на съюзниците.

Какво всъщност представлява приетият План за действие? Това е един отворен документ, който непрекъснато ще се актуализира, за да се гарантира, че НАТО е в челните редици на развитието на киберпространството и поддържа необходимата гъвкавост, за да отговори на предизвикателствата, породени от кибер заплахите. Ако политиката определя "какво" трябва да бъде направено в контекста на кибернетична отбрана на НАТО, то Плана за действие конкретизира "как" НАТО ще го постигне.

Провеждането на политиката на НАТО за кибер отбрана се опира на т**ри основни стълба на способностите** на организацията в киберпространството.

Субсидиарност - предоставяне на помощ само при поискване; в останалите случаи се прилага принципът на отговорността на суверенните държави;

Избягване на дублирането - да няма излишни двойни структури или способности на международно, регионално и национално равнище.

Сигурност - сътрудничество, основано на доверието, отчитащо чувствителността на свързаната със системи информация, до която трябва да се даде достъп и уязвимите места.

Заложени са практическите стъпки, които ще бъдат предприети за достигане на предвидените в Политиката способности.

• НАТО ще разработи минималните изисквания за тези национални информационни системи, които са от решаващо значение за извършване на основните задачи на НАТО.

• НАТО ще подпомага съюзниците в постигането на минимално ниво на кибернетичната отбрана, за да се намали уязвимостта на националната критична инфраструктура.

• Съюзниците също могат да предложат помощта си на съюзник или Алианса в случай на кибератака.

• Кибер отбраната ще бъде напълно интегрирана в Процеса за планиране отбраната на НАТО. Подходящите изисквания на кибер отбраната ще бъдат идентифицирани и приоритизирани чрез NDPP.

• Военното ръководство на НАТО ще оцени как кибернетичната отбрана подкрепя изпълнението на основните задачи на НАТО, планиране за военни мисии и провеждане на мисии.

• Ще бъдат определени също изискванията за кибернетична отбрана на държави извън НАТО, участващи с войски.

• Ще се прилагат строги изисквания за удостоверяване. Изискванията за управление на риска на процеса за придобиване и веригата за снабдяване ще бъдат опростени.

• НАТО ще засили възможностите си за ранно предупреждение, ситуационна осведоменост и анализ.

• НАТО ще разработи информационни програми, както и ще продължи да развива кибер компонента в ученията на НАТО.

• НАТО и съюзниците се насърчават да черпят експертни познания и подкрепа от Кооперативен център за високи постижения по киберотбраната на НАТО в Талин.

Запазването и укрепването на водещата роля на НАТО в политиката за кибер отбрана изисква укрепване на възможностите на Алианса в сферата на киберотбраната, тъй като заплахите търпят развитие и стават все по-усъвършенствани, потенциално подкопаващи критично важни системи и инфраструктура. За адекватен и своевременен отговор на тези заплахи, новата стратегия изисква всички структури на НАТО да бъдат включени в централизирана система за защита и всички нейни мрежи да бъдат наблюдавани денонощно.

В израз на идеята за колективни усилия, през февруари 2011 г., Агенцията на НАТО за консултации, командване и контрол NC3A (сега NCIA), стартира инициатива за кооперииране и обединяване на усилията за киберзащита на НАТО и предложи на страните-членки да се включат в разработването и финансирането на многонационален проект за придобиване на способности за киберсигурност – Multinational Cyber Defense Capability Development (MN CD2) Project. Визията за обхват на проекта включва изграждане на способности за киберзащита на публични, некласифицирани КИС, както и такива за класифицирана информация на НАТО. До края на годината желание за присъединяване изявиха 8 държави – Канада, Федерална Република Германия, Република Литва, Великобритания, Кралство Холандия, Словакия, Турция и Република България. След срещата на върха на НАТО, проведена в Чикаго – САЩ, проектът MN CD2 е включен в списъка от проекти за Интелигентна отбрана (Smart Defense).

Проектът MN CD2 обхваща 3 пакета:

1 . Изграждане на способности за споделяне на техническа информация (Cyber Defense Technical Information Sharing).

2. Изграждане на инфраструктура за непрекъснат мониторинг и анализ на събития (Cyber Defense Situational Awareness).

3. Изграждане на инфраструктура за събиране, корелиране и дистрибутиране на информация за събития и инциденти в областта на кибер защитата (Cyber Defense Distributed Multi-Sensor Collection and Correlation Infrastructure).

Основанието за включване в проекта и правната и финансова рамка за участие е подписването на Меморандум за разбирателство с Агенцията за комуникации и информация на НАТО (NCIA). Реализирането на проекта стартира на 14 март 2013 г. с участието на 5 страни, подписали меморандума - Канада, Дания, Кралство Холандия, Норвегия и Румъния. С писмо от 19 март 2013 г., NCIA покани останалите страни-членки, включително и Република България. Проектът MN CD2 е с обща продължителност 5 години (2013 – 2017 г.) Финансирането на проекта е на принципа на споделянето на разходите (cost-sharing).

На срещата през юни 2011 г. в Брюксел, НАТО взе решение да се започне сътрудничество с ЕС в областта на киберотбраната, но европейският подход към този въпрос е все още ограничен в рамките на сигурността на компютрите поради съсредоточаването единствено върху екипите за действие при инциденти в информационната сигурност (CERT).

4. Дейности в Република България в областта на киберсигурността

Както беше посочено по-горе, по въпросите за сигурността в киберпространството, в Европейския съюз, говорим за политика за киберсигурност, включваща Стратегия за киберсигурност и предложение на Комисията за Директива в областта на мрежовата и информационната сигурност (МИС), в НАТО има приета Политика за кибер отбрана с План за действие за нейното прилагане, т.е. конкретни документи, израз на последователна и

целенасочена политика. В същото това време, в нашата страна не можем да посочим не само действащ нормативен документ, но и последователни действия за формиране на политика и стратегия по въпросите за сигурността в киберпространството.

В лекция в УНСС през месец април т.г., на въпроса на студенти „Кой отговаря за това (киберсигурността, б.а.)?", тогавашният министър на отбраната Тодор Тагарев отговори така*: „Не можем да кажем, че за киберсигурността отговаря армията или ГДБОП, само МВР или някоя друга служба в МВР, или ДАНС. Отговорността е споделена."*

И все пак въпросът „Кой отговаря за това?" остава без отговор. Не става неясно как точно е споделена, както и между кои субекти е разпределена отговорността по въпросите на киберсигурността у нас.

Дори и един бърз преглед на състоянието на дейностите в киберпространството у нас показва, че до момента не можем да говорим за цялостна визия в обществения живот по въпросите за киберсигурността. Налице са отделни действия, по-скоро в отговор на конкретни процедури в ЕС или НАТО, отколкото последователни действия, насочени към постигането на ясно формулирана цел. В същото време, като пълноправен член на НАТО и ЕС, Република България има своите ангажименти към общата политика за сигурност и защита, която включва елементи от съвместни действия в областта на киберсигурността и защитата.

На 28.09.2010 г. в Централния военен клуб в София се проведе кръгла маса на тема „Състояние и проблеми на сигурността в киберпространството на България". По време на дискусиите беше споделено, че в областта на киберсигурността все повече се работи, но в същото време беше отбелязано, че се изискват още по-интензивни действия от една страна на държавните институции и от друга на частния бизнес и научните институции, работещи в тази област. Направен беше извода, че е необходимо изграждането на добро сътрудничество и координиране на усилията на всички заинтересовани страни в областта на киберсигурността.

Със свое решение от същата година, Държавната комисия по сигурността на информацията (ДКСИ) е определила точка за контакт за Република България към проекта на ЕС „Механизъм за известяване при инциденти в сигурността на мрежите."

На заседание на 25 май 2011 г. правителството одобри Меморандум за разбирателство за бъдещо сътрудничество в областта на киберсигурността между Органа за управление на киберзащитата към НАТО (NATO Cyber Defence Management Authority - NCDMA) и националните органи за киберзащита Министърът на транспорта, информационните технологии и съобщенията и председателят на Държавната агенция „Национална сигурност" (ДАНС) са упълномощени да проведат преговорите и да подпишат документа. Проектът на меморандум е обща рамка за бъдещо сътрудничество между България и НАТО в областта на киберсигурността. С него се цели при необходимост да бъде оказвана експертна помощ на България в тази област. Той се отнася за информационните системи на административните органи и мрежите за класифицирана информация, поради което от българска страна ще бъде подписан от министъра на транспорта, информационните технологии и съобщенията, като

отговарящ за обществените мрежи (информационни системи на административните органи) и от председателя на ДАНС, като отговарящ за мрежите за класифицирана информация. Експерти от ДКСИ участваха в работата на междуведомствената работна група, сформирана с цел да подготви текста на меморандума. Целта на този Меморандум за разбирателство е да формализира споделянето на информация за киберзащита, обмена на услуги за киберзащита и участието в свързани с тях дейности. Меморандумът урежда въпросите за целите и обхвата, приложимото законодателство, финансовите условия по приложението му, правилата за използване на взаимно обменяната информация, начините за разрешаване на спорове, начините за неговото изменяне и прекратяване. Договарящите страни се ангажират да провеждат двустранни дейности и споделяне на информация, свързани с киберзащитата, с което да допринасят за общите цели за защита на техните съответни информационни мрежи. През месец ноември 2011 г. Меморандумът беше подписан.

През месец септември 2011 г. е създадена Междуведомствена работна група по проблемите на кибернетичната защита със задача да изготви предложение за състав, правомощия, мисия, функции и задачи на Национален орган по кибернетична сигурност в Република България и да подготви проект на Решение на Министерски съвет за неговото ситуиране. Председател на групата е секретар на Съвета по сигурността при Министерски съвет, а функциите на Секретариат на Междуведомствената работна група са възложени на отдел „Информационна сигурност“ в дирекция „Сигурност на информацията“ на Министерството на отбраната. В състава на групата са включени представители на МО, ДАНС, Държавната комисия по сигурността на информацията, ГД „БОП“, МТИТС, ИА „ЕСМИС“, МПр, МВнР и БАН.

В доклада на групата от януари 2012 г. се прави анализ на съществуващото състояние на киберсигурността, като се правят следните констатации:

- липсата на правно – нормативно регламентиране на въпросите за киберсигурността на критичната комуникационна и информационна инфраструктура, както и липсата на национална политика и национална стратегия за киберсигурност; ЗЗКИ регулира обществените отношения само в областта на класифицираната информация, а Закона за електронната управление обхваща ограничена област от информационната сигурност;

- отговорностите за разработване и осъществяване на политиката за оперативна съвместимост и информационна сигурност на КИС на държавната администрация за некласифицирана информация са възложени на МТИТС, където е ситуиран и правителствения център за инциденти в информационната сигурност. ДКСИ и ДАНС осъществяват законовите си правомощия за защита на класифицираната информация. Липсва законова норма за създаване на единна координация за защита на информацията.

Групата предложи да бъде създадена Държавна агенция за киберсигурност, която да изпълнява функциите на национален орган и да подпомага премиера по въпросите на киберсигурността. Структурата да има две направления на дейност. Първото – координация и управление на националната система за бързо реагиране при инциденти, свързани с

кибератаки, като в състава й да функционира национален център за реагиране на компютърни инциденти, който да взаимодейства с центровете в мрежата, както и с аналогичните структури на НАТО и ЕС. Второто направление – разработване и осъществяване на политиката на страната в областта на киберсигурността, като се взаимодейства с местната власт, НПО, академичния сектор и международни организации. Проектът обаче не получи одобрение и работата на междуведомствената работна група продължи.

Какво би се случило, ако бъде създадена агенция по киберсигурност? Ще се реши ли въпросът? Най-вероятно не. Дори и да бъде създадена такава агенция по киберсигурност, пак трябва всички други, които имат отношение към тези въпроси, да работят заедно.

През месец май т.г., само два дни преди изтичане на мандата на служебното правителство, министър-председателят издаде заповед, с която създаде Междуведомствена работна група за изготвяне на проект на стратегия за киберсигурност на Република България. За председател на работната група беше определен министърът за развитие на електронното правителство, а контролът по изпълнението на заповедта беше възложен на министъра на отбраната, без при това в състава на работната група да е включен представител на Министерството на отбраната. В тази, т. нар. „Междуведомствена“ работна група всъщност са включени само представители на ДАНС и ИА „ЕСМИС“ към МТИС.

В контекста на политиката на НАТО и ЕС, както и всичко, написано по въпроса на киберсигурността, би следвало в обсъждането и решаването на този въпрос да се включат всички структури, работещи по или имащи отношение към проблемите на сигурността в киберпространството. Това са както правителствени органи, така и академичната общност и разбира се, частният сектор, който изпълнява ключова роля за управлението и предоставянето на интернет услуги.

5. Заключение

Необходимо е задълбочено разбиране на околната среда и ограниченията. Разпределеният характер на интернет поражда загриженост, тъй като периферни възли могат да бъдат използвани за осъществяване на атаки — примерно чрез ботмрежи. Този разпределен характер обаче е от ключово значение за стабилността и устойчивостта и може да спомогне за по-бързо възстановяване, отколкото обикновено е постижимо с прекомерно формализирани процедури, осъществявани в йерархичен порядък. Това изисква внимателен анализ поотделно за всеки един случай на обществените политики и на оперативните процедури, които да се въведат.

От значение е и времевото ограничение. Налице е очевидна потребност да се действа сега и бързо да се въведат необходимите елементи за изграждане на рамка, която ще ни позволи да отговорим на сегашните предизвикателства и която ще може да се пренесе в бъдещата стратегия за мрежова и информационна сигурност.

Въпросът за стратегия за киберсигурност е не само изключително наболял и важен, но при неговото решаване следва да се имат предвид някои съществени особености. Стратегията

трябва да обхване както обществените (публични) мрежи, така и мрежите за класифицирана информация и да съответства на политиките на НАТО/ЕС в тази област.

Независимо от голямото забавяне, по темата трябва да се работи внимателно, с отчитане както на международните изисквания и реалности, така и специфичните функции и предпоставки по отношение на националната правната рамка, исторически и политически контекст, държавна структура, организационни структури, процеси за управление на кризи, както и национален манталитет.

В същото време, в контекста на членството на нашата страна в ЕС и НАТО, следва да се вземат под внимание както поетите ангажименти произтичащи от приетите политически и стратегически документи в двата съюза, така и обстоятелството, че голяма част от държавите – членки имат вече приети национални стратегии за киберсигурност, определили са своите национални органи и развиват активна дейност в тази област.

Сериозно внимание трябва да се обърне на засилване обмена на информация както между различните правителствени структури, както и с частния сектор, за да се даде възможност на държавата и частния сектор да поддържат общо виждане за различните заплахи, с цел по-доброто разбиране на новите тенденции и техники - както на използваните за осъществяване на кибератаки, така и на тези, използвани за ускоряване на ответните действия.

Следва да бъдат определени и изградени както Национален орган по кибернетична сигурност, така и структури за работа по въпроси на устойчивостта на киберпространството, киберпрестъпността и отбраната на четирите нива на управление - политическо, стратегическо, оперативно и тактическо (техническо), техния капацитет за справяне с инциденти в киберпространството следва да достигне необходимото равнище. Въпреки това предвид факта, че редица субекти могат да имат оперативни отговорности за различни аспекти на киберсигурността, и като се има предвид важността на участието на частния сектор, координацията между държавните органи на национално равнище следва да бъде оптимизирана. В националната стратегия за киберсигурност следва да се определят ролите и отговорностите на различните национални структури.

За практическото изпълнение на стратегията е необходимо да бъде разработен и национален план за сътрудничество в сферата на МИС, който да се задейства в случай на инциденти в киберпространството, като ангажираните субекти да бъдат в състояние да разпределят ясно формулирани роли и отговорности и да оптимизират ответните си действия.

Тази задача може да бъде решена успешно единствено чрез истинско партньорство с участието на всички заинтересовани страни при поемането на отговорност и справяне с бъдещите предизвикателства.

Използвана литература

1. Слатински, Николай. Измерения на сигурността, София, 2000, 185 с.
2. Семерджиев, Цветан, Сигурност и защита на инфомацията, София, 2012, 79 с.
3. Европейска комисия, Предложение за директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза, COM(2013) 48 final, Брюксел, 2013
4. Европейския икономически и социален комитет, Становище на ЕИСК относно „Предложение за директива на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза“, COM(2013) 48 final – 2013/0027 (COD), Брюксел, 2013
5. Върховен представител на Европейския съюз по въпросите на външните работи и политиката на сигурност, Съвместно съобщение до Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите, JOIN(2013) 1 final, Брюксел, 2013
6. Klimburg, Alexander (ed.). National Cyber Security Framework Manual, NATO CCD COE Publication. Tallin, 2012, PDF
7. NATO Public Diplomacy Division (ed.). Defending the networks, The NATO Policy on Cyber Defence. Brussels, www.nato.int, 2011, PDF

Библиографски бележки

[1] Определение за КИИ беше предложено в Зелена книга относно Европейска програма за защита на критичната инфраструктура COM(2005) 576 final

[2] Обществена консултация онлайн на тема „Подобряване на МИС в ЕС“, проведена от 23 юли до 15 октомври 2012 г.

[3] Евробарометър 390/2012.

[4] IP-13-94

[5] Стратегия на Европейския съюз за киберсигурност „Отворено, безопасно и сигурно киберпространство“, JOIN (2013) final.

[6] COM(2013) 48 final – 2013/0027 (COD).

[7] CERT-EC е постоянният екип за незабавно реагиране при компютърни инциденти (CERT-EU) за институциите, агенциите и органите на ЕС.

[8] Директива 2008/114/ЕО на Съвета.