IT4Sec Reports 108
http://dx.doi.org/10.11610/it4sec.0108

Киберсигурността – стратегически национален проблем

Величка Милина

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, юни 2013 г.

Величка Милина, Киберсигурността – стратегически национален проблем**,** *IT4Sec Reports* 108 (София, Институт по информационни и комуникационни технологии, юни 2013 г.), http://dx.doi.org/10.11610/it4sec.0108.

IT4SecReports 108 „Киберсигурността – стратегически национален проблем“ Съвременната информационна и комуникационна епоха породи сложна взаимозовисимост и взаимообвързаност на всички жизненоважни за съществуването на обществото инфраструктури, което доведе до експоненциално нарастване на уязвимостите и рисковете за тяхното функциониране. Ето защо, сигурността на киберпространството се превърна в едно от най-важните предизвикателства на 21-ви век, а кибернетичната сигурност все повече се разглежда като хоризонтален и стратегически национален проблем, който засяга всички нива на обществото. Националните стратегии за киберсигурност са призвани да дадат отговор на новите предизвикателства и да гарантират сигурността в киберпространството. Анализът и оценката на приети национални киберстратегии позволява да бъдат направени някои общи изводи за добрите практики и да бъдат обособени проблемните сфери. За страните-членки на ЕС е важно да синхронизират националните си стратегии със стратегията на Съюза за кибернетична сигурност.

IT4Sec Reports 108 “Cybersecurity: A National Strategic Issue“ The modern information and communication age brought a complex of interdependencies among infrastructures that are essential for society and led to an exponential growth of vulnerabilities and risks. Hence, security of cyberspace turned into one of the most important challenges of Twenty first century, while cybersecurity is already seen as a cross-cutting, strategic national issue that impacts all societal levels. National cybersecurity strategies are expected to provide answers to the novel challenges and to guarantee security of cyberspace. This report provides analysis available national cyber strategies that allows identification of good practices and remaining gaps. For Member States of the European Union it is important to synchronize their national strategies with the EU strategy for cybersecurity.

Keywords: Cybersecurity, cyberspace, cybersecurity strategy, critical infrastructure, vulnerability, risk

д-р Величка Милина е доцент по политология в катедра „Национална и международна сигурност“ във Военна академия „Г.С.Раковски“. Преподава политически аспекти на националната и международната сигурност, Русия в глобалния свят, енергийна сигурност и геополитика.

ISSN 1314-5614

Управлението на сигурността в киберпространството чрез национална стратегия е необходимост, обща за всички национални правителства през 21-ви век. Причината е, че постмодерната епоха на глобализация и всеобща информатизация направи част от нашия живот едно ново явление – информационната мрежа, която обвърза значителна част от човечеството, неговите жизнени сфери в неразривна система и направи сигурността в киберпространството ключова за сигурността на обществото.

Настоящето изложение анализира и оценява киберсигурността като стратегически проблем на политиката и управлението на националната сигурност.

Средата: Съществуването на съвременния живот - на индивидуално, национално и международно ниво все повече зависи от множество взаимосвързани и взаимозависими инфраструктури. Услуги като храна, вода, здравеопазване и транспорт винаги са били от критично значение за оцеляването на човека, но днес тяхната доставка в по-широк план е вплетена в комуникационната инфраструктура и киберпространството. В основата на всичко това е енергийният сектор, без който никой друг сектор не би могъл мащабно да функционира. В резултат от информатизацията, основните обществени сектори – икономика, енергетика, информация и комуникации, транспорт и т.н са все по-взаимосвързани и взаимозависими. Всеобхватността на информационните технологии породи „сраставе“ на кибернетичния и материалния свят. Днес физически, виртуални и логически мрежи са се увеличили по размер и сложна взаимозависимост до такава степен, че дори малки прекъсвания, повреди и смущения, могат да имат драматични последици за тях („парадокс на уязвимостта“)[1].

Обикновено се приема, че критичната инфраструктура включва особено чувствителни елементи на по-голяма система, обхващаща публичния и частния сектор и обществото като цяло. Това разбиране надхвърля физическата инфраструктура и включва информация (данни) - което може да се счита за форма на логическа инфраструктура или "критична информационна инфраструктура". Киберпространството и взаимосвързаните – информационни и комуникационни технологии са станали основни компоненти на съвременния живот. Въпреки, че киберпространството се категоризира като отделен сектор, на практика то е толкова дълбоко вкоренено в другите сектори, че тази разлика изглежда трудно определима. То може да бъде визуализирано като тънък слой (или нервна система), преминаваща през всички други сектори, като им дава възможност да работят и да взаимодействат. Взаимозависимостта на различните жизнени системи чрез киберпространството значително разширява обхвата на анализа (т.е. по принцип почти всичко вече може да бъде свързано с всичко останало) и е основен фактор за нарастващата комплексност на критичната инфраструктура. Тази сложност се увеличава експоненциално, "чрез разширяване на географското място, разширяване на предоставяните услуги; въвеждане на нови компоненти с богата функционалност заради използването на разнообразни технологии, увеличаването на броя на мрежи, възли, и връзки, и взаимозависимости; чрез наслояване на системи върху системи"[2].

---

[1] Uwe Nerlich, F. Umbach, *European Energy Infrastructure Protection: Addressing the Cyber-warfare Threat*, 10.2009, http://www.ensec.org/index.php?option=com_content&view=article&id=219:european-energy-infrastructure-protectionaddressing-the-cyber-warfare-threat&catid=100:issuecontent&Itemid=352, (30.05.2013)

[2] Myriam Dunn, *Cavelty, Systemic cyber/in/security – from risk to uncertainty management in the digital realm*, Swiss Re Centre for Global Dialogue, 15 September 2011, http://cgd.swissre.com/features/Systemic_Cyber_In_Security.html, (03.06.2013)

В тази нова виртуална реалност става все по-трудно да се идентифицират критичните точки (възли) на системите и самите системи, чиято защита трябва да бъде приоритет. В обществения дебат има склонност отраслите на критичната инфраструктура да бъдат категоризирани в много широк смисъл, до степен, че те да обхванат почти всеки аспект от ежедневния живот. Възможният ефект е, че когато всичко е "критично", нищо не е.

Това е средата, която днес детерминира кардиналното нарастване на уязвимостта във функционирането на жизненоважните за обществото инфраструктури.

Известно е, че „уязвимост“[3] се дефинира като място, обект, връзка в системата, което се характеризира с по-голяма степен на податливост на въздействие на заплахата, поради което там с по-голяма вероятност би се появило смущение/повреда със сериозни последствия. Такива „слаби звена“ в системата обикновено са лесто достъпни за „атака“ от заплахи, но трудни за защитаване. От тях може да стартира разпространение на каскаден ефект или ефект на доминото. Уязвимостта сама по себе си не генерира неблагоприятни последици, тя се реализира само тогава, когато е подложена на въздействието на (експлоатирана е от) релевантни заплахи.

Рискът[4] се представя като комбинация от заплахи, експлоатираща дадена уязвимост на системата/елемента и произтичащите вредни въздействия/последствия за системата/елемента. Ако заплахата и релевантната уязвимост не се срещнат, то вредното последствие няма да възникне. Установяването на риска от срив на критичните инфраструктури е свързано с анализ на заплахите и уязвимостите.

Този анализ днес се прави на много нива: от частните собственици и операторите на критични инфраструктури; от публичните национални институции, от институциите на системите за международна сигурност.

Параметрите на средата, в която трябва да се управлява сигурността в киберпространсвото категорично показват, че нациите са все по-зависими от сложни системи и информационни технологии. В много случаи, информационни и комуникационни технологии, които са от жизненоважно значение за националната и икономическа сигурност са обект на смущения по редица причини, които могат да бъдат с национален или външен за страната произход. Ръководителите на държавни органи, организации и частната индустрия все по често се сблъскват с несигурност относно риска и уязвимостите в кибернетичното пространство.

В този контекст, нарастващата зависимост на обществото от стабилното функциониране на критичните активи става приоритетна тема на националния интерес, а кибернетичната сигурност все повече се разглежда като хоризонтална и като стратегически национален проблем, който засяга всички нива на обществото.

Европейският контекст: Днес, започвайки от 2008 г. с Естония, 25 държави имат приети национални стратегии за сигурност, от тях - 13 членки на Европейския съюз. На

---

[3] П. Дракалиева, И. Иванов, Съвременната концепция за защита на критичната инфраструктура: генезис, цели, методология, проблемни зони, Защита на критичната инфракструктура в ЕС и България - икономически и организационни аспекти, София, 2010, стр. 19

[4] Пак там, стр. 21

7 февруари 2013г. Европейската комисия представи за обсъждане принципи, стратегически приоритети, роли и отговорности, както и директивни изисквания в дългоочакваната Европейска стратегия за киберсигурност[5] подкрепена с Директива „Касаеща мерките за осигуряване на високо общо ниво на мрежовата и информационната сигурност в Съюза"[6]. Тези два документа дефинират параметри и фиксират изисквания (особено в Директивата), с които националните киберстратегии на страните-членки трябва да се синхронизират задължително. Въпреки че стратегията не призовава всички страни-членки да разработят и приемат свои национални стратегии за киберсигурност възможно най-скоро, това е необходимост, произтичаща от записаното в стратегията тристепенно (национално-европейско-международно) разпределение на ролите и отговорностите за кибернетична сигурност. Освен това, за постигането на сигурност в киберпространството е важно да се осигури взаимно допълване между националните стратегии и стратегията на ЕС. Важно е също така действията (политиките) на ЕС да допълват съществуващите структури и най-добри практики в държавите членки.

Каква е философията и кои са ключовите моменти в стратегията и политиката на ЕС за киберсигурност?

Европейската политика на сигурност в кибернетичното пространство, която постепенно се развива през последните години[7], цели да установи минимални стандарти във всички държави-членки на ЕС по отношение на превенцията, устойчивостта и международното сътрудничество. Тя има за цел да укрепи националната сигурност, без да се прави компромис с демократичните принципи или неправомерно да се нарушават индивидуалните свободи. Ключов проблем при формулирането на тази политика е трудността да се намери баланс между така обявените цели и мерките на ЕС, тъй като неизбежно възниква въпросът за демократичните последици от Европейската политика за киберсигурност: дали институционалните структури и инструменти на тази политика са съвместими с критериите на демократичното управление? В този смисъл, най-сериозният въпрос пред общата политика на ЕС за киберсигурност е как тя да бъде включена в институционалната структура на ЕС, защото принципно управлението в областта на кибернетичната сигурност се характеризира с определена двойственост. По отношение на регулацията европейският подход най-общо казано е либерален, което означава, че частните играчи се окуражават да участват в този процес. Но когато става дума за въпроси свързани с националната сигурност, акцентът категорично е върху ролята на държавата.

---

5 Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council,the European Economic and Social Committee and the Committee of the Regions, Brussels, European Commission, 7.2.2013

6 Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, European Commission, 7.2.2013

7 През 2001 г. Комисията приема съобщение, озаглавено „Мрежова и информационна сигурност: предложение за европейски политически подход " (COM (2001) 298);

През 2006 г. тя приема Стратегия за сигурно информационно общество (COM (2006) 251).

От 2009 г. насам Комисията приема също План за действие и съобщение относно защитата на критичната информационна инфраструктура (CIIP) (COM(2009)149, одобрен с решение 2009/C 321/01 на Съвета, и COM(2011)163, одобрен в заключенията от срещата на Съвета 10299/11).

Рамкова директива за електроните комуникации - Членове 13а и 13б от Директива 2002/21/ЕО

Също така законодателство на ЕС в областта на защита на данните - Член 17 от Директива 95/46/ЕД; член 4 от Директива 20002/85/ЕО

Друга характерна особеност на Европейската политика за сигурност в кибернетичното пространство е множеството на участниците. Това многообразие е и причината за липсата на ясно определени области на отговорност и отчетност между различните институции. В резултат, политиката за киберсигурност функционира като "многостранен" модел[8], където всяка група с опит в съответната област (бизнес) или необходимата политическа власт (членки на ЕС) може да участва в процеса на изготвяне на политиките.

Европейската политика за сигурност в кибернетичното пространство е тясно свързана както с международни, така и с национални регулаторни процеси. Казано по друг начин, Европейската политика за сигурност в кибернетичното пространство се формулира и имплементира в глобална многостепенена и включваща много заинтересовани страни структура. Това поставя три основни проблема на демократичното управление:[9]

Размиване на границите между вътрешните и външните политики: В областта на кибернетичната сигурност е почти невъзможно да се поддържа традиционното разделение между вътрешни и външни политики. Интернет-базирани атаки могат да произхождат от много далечни или съседни страни, но често е трудно, ако не и невъзможно, да се идентифицира източника на атаката. В резултат на това, границите между правосъдието и вътрешните работи от една страна и външната политика от друга страна, стават все по замъглени. Заплахите вече не могат да бъдат ясно определени като принадлежащи към зоната на отговорност на една определена област на политиката.

Видим признак на това развитие е увеличаването на нивото на сътрудничество между органи и институции, отговорни за различни области на политиката. Тази ерозията на традиционните роли е по-проблематична в ЕС, отколкото в национален контекст, но това по никакъв начин не е ново явление. През последните години, развитието на европейската политика за сигурност до голяма степен е задвижвано от интернационализацията на правосъдието и политиките по вътрешните работи на ЕС, а ролята на ОВППС в областта на политиката за киберсигурност е ограничена до действията на пет господстващи в тази сфера държави-членки (Германия , Франция, Великобритания, Холандия и Швеция). В тази нова политическа структура и Европейската комисия, и Европейският парламент получават нови възможности за влияние върху процесите на правене на политики.

Секюритизация: Известно е, че създаването на общо "пространство на свобода, сигурност и правосъдие" е основополагаща цел на ЕС.

С нарастването на новите заплахи, обаче, Комисията и държавите-членки са склонни да подчертават приоритетността на сигурността над свободата, като наблягат на въвеждането на нови мерки в политиката за сигурност. Допълнителна сложност е обстоятелството, че частните охранителни фирми придобиват все повече и повече влияние в тази област на политиката.

Приватизация на управлението: Традиционното разграничаване между частния и обществения сектор все повече избледнява в зараждащите се нови политически структури. Без технологичната експертиза на частни фирми, вече е трудно да се определят съответните заплахи и адекватно да се реагира на тях. Освен това, много частни фирми също

---

8 Вж: Annegret Bendiek, European Cyber Security Policy, German Institute for International and Security Affairs, RP 13, Berlin, October 2012

9 Пак там

носят отговорност за сигурността като собственици или оператори на критичната инфраструктура в енергетиката, здравеопазването, транспорта.

Включването на тези компании в процесите и политиките по оценката на риска, идентифицирането на заплахите и управлението на кризи, става важна част от поддържането на обществената сигурност. От друга страна обаче, не се отменя правилото, че тя трябва да бъде гарантирана от институциите, които имат конституционен мандат за това.

За да се осигури съвместимостта на институционалната структура и на инструментите на европейската политика в областта на кибернетичната сигурност с принципите на демократичното управление, е необходимо да се гарантира приложимостта на следното правило: "Доброто управление" в Европейската политика за киберсигурност трябва да отговаря на такива критерии като прозрачност, върховенство на закона, отчетност и участие.

Философията на *Европейска стратегия за киберсигурност* е базирана на няколко *основополагащи принципа*[10], които подчертават общоевропейските ценности и могат да бъдат крайъгълния камък, около който да се изградят международните регламенти за сигурност в кибернетичното пространство:

- *Основните ценности на ЕС важат в еднаква степен в цифровия и във физическия свят*. Законите и нормите, които се прилагат в други области на нашия всекидневен живот, ще се прилагат също така и в кибернетичното пространство.
- *Защита на основните права, свободата на изразяване на мнение, на личните данни и неприкосновеността на личния живот*. Киберсигурността може да има смисъл и да бъде ефективна, ако се основава на основните права и свободи, залегнали в Хартата на основните права на Европейския съюз и основните европейските ценности.
- *Достъп за всички*. Ограниченият дстъп или липсата на достъп до интернет, както и цифровата неграмотност поставят гражданите в неблагоприятно положение, като се има предвид голямата степен на навлизане на цифовите технологии във всички дейности на обществото. Всеки трябва да има безопасен достъп до Интернет и до безпрепятствен пренос на информация.
- *Демократично и ефективно многостранно управление.* Дигиталният свят не се контролира от един единствен субект. Понастоящем редица заинтересовани страни, сред тях много търговски и неправителствени структури, участват във всекидневното управление на интернет ресурси, протоколи и стандарти, както и в бъдещото развитие на интернет. ЕС потвърждава значението на всички заинтересовани страни и подкрепя този многостранен подход на управление.
- *Споделена отговорност за гарантиране на сигурността.* Нарастващата зависимост от информационните и комуникационните технологии във всички сфери на човешкия живот породи уязвимости, които трябва точно да се определят, подробно да се анализират, да се отстраняват и в последна сметка да намалеят. Всички заинтересовани страни - публичните власти, частният сектор и отделните граждани, трябва да признаят тази споделена отговорност, да предприемат действия, за да защитят себе си и ако е необходимо, да осигурят координиран отговор за засилване на киберсигурността.

[10] Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council,the European Economic and Social Committee and the Committee of the Regions, Brussels, European Commission, 7.2.2013, p. 3-4

В документа на Европейската комисия са формулирани *пет стратегически приоритета*[11], които трябва да дадат адекватен отговор на предизвикателствата пред сигурността в киберпространството. Тяхното реализиране предвижда действия, както в краткосрочен, така и в дългосрочен план. Те съдържат разнообразие от политически инструменти и включват различни видове участници - на ниво институции на ЕС, държавите-членки на ЕС или бизнеса. Тези стратегически приоритети и действия са:

- Постигане на устойчивост на киберпространството.
- Драстично намаляване на престъпленията в кибернетичното пространство.
- Разработване на политика за киберотбрана и изграждане на капацитет във връзка с общата политика за сигурност и отбрана (ОПСО).
- Развитие на индустриални и технологични ресурси за киберсигурност.
- Създаване на последователна международна политика на Европейския съюз за киберпространството и насърчаване на на основните ценности на ЕС.

Третият основен акцент в европейската стратегия за киберсигурност е *изясняване на ролите и отговорностите*[12] на множеството участници, отговарящи за сигурността в дигиталното пространство. Най-сериозното предизвикателство е как те да бъдат включени в системата на общата отговорност за сигурност при наличието на различни правни рамки и юрисдикции.

Решението, което предлага стратегията е това да става на три нива, тъй като предвид сложността на въпроса и широкия спектър от участници, очевидно, централизиран европейски надзор не може да бъде ефективен.

Първото е нивото на националните правителства, които могат най-добре да организират превенцията и реагирането на инциденти и атаки в кибернетичното пространство, както и да установят контакти с частния сектор и широката общественост в контекста на съществуващите политически правила и правни рамки. Въпреки че интернет е неограничено пространство, правната регламентация и отговорността за сигурността в тази сфера си остават под юрисдикцията на държавата-нация.

В същото време, поради специфичния характер на киберрисковете, където потенциално или действително границите отсъстват, ефективният национален отговор често би изисквал и участие на равнище ЕС. За да се постигне широка киберсигурност дейностите трябва да се опират на три ключови стълба – мрежова и информационна сигурност (Network and Iinformation Security - NIS), прилагане на закона и отбрана (защита). На това второ ниво на отговорност на ЕС има няколко институционални субекта, занимаващи се специално с киберсигурност - ENISA[13], Europol/EC3[14] и EDA[15]. Това са три агенции, активно работещи от гледна точка и на трите стълба: на NIS, на прилагане на закона и на съответната защита. Тези агенции предлагат платформи за координация на равнище ЕС и имат управителни съвети, в които са представени държавите-членки.

---

11 Пак там, с. 4-17.

12 Пак там, с. 17-19

13 ENISA - European Network and Information Security Agency, основана 2004 г.

14 European CyberCrime Centre (EC3) е агенция открита през януари 2013 г. към Europol

15 EDA – Европейска агенция за отбрана

Третото, е международното ниво. Тук Комисията и Върховният Представител, заедно с държавите-членки гарантират координирани международни действия в областта на киберсигурността. Те работят за установяване на основните ценности и за насърчаване на мирно, открито и прозрачно използване на кибертехнологиите. Комисията, Върховният Представител и държавите-членки участват в политическия диалог с международните партньори и с международни организации като Съвета на Европа, ОИСР, ОССЕ, НАТО и ООН по проблемите на международната киберсигурност.

За да се гарантира ефективното реализиране на стратегията, тя е подкрепена с Директива „Касаеща мерките за осигуряване на високо общо ниво на мрежовата и информационната сигурност в Съюза".

По принцип, Директивите са инструкции за страните-членки относно това, какво трябва да бъде постигнато от законодателството, като на всяка страна се предоставя правото да изпълнява това законодателство по начин, който е най- подходящ за нея. По тази логика, новата директива на ЕК за мрежова и информационна сигурност (NIS) се опитва да определи стандартизирано минимално ниво за сигурност в ЕС без да възпрепятства никоя от членките да вдигне летвата дори по-високо.

Трите ключови предложения в директивата за NIS са:[16]

1. Всяка страна-членка трябва да възприеме стратегия за NIS и да прилага компетентно законодателство.
2. Всяка страна-членка трябва да създаде "Механизъм за сътрудничество", за да споделя информационната сигурност в ЕС.
3. Операторите на критичните инфраструктури, като енергетика, транспорт, и ключовите доставчици на информационни социални услуги (е-комерсиални платформи, социални мрежи и други), както и публичните администратори, трябва да изработят подходящи стъпки за управление на рисковете за сигурността и да докладват сериозните инциденти към компетентните национални власти.

Ключовото изискване в Директивата - да се докладват сериозни инциденти, е допълнено с необичайната стъпка да бъде публикуван списък на дружествата, които трябва да докладват за значителни инциденти, свързани със сигурността на основните им услуги като Google или търговецът на дребно Amazon. Основно в списъка присъстват операторите на критични инфраструктури в някои сектори (финансови услуги, транспорт, енергетика и здравеопазване), доставчиците на услуги за информационното общество (платформи за електронна търговия с приложения, плащания по интернет, изчисления в облак, търсачки, социални мрежи), както и публичните администрации. Около 42 хил. компании в Европейския съюз, включително летища, банки и болници, ще трябва да докладват за хакерски атаки.

Ефективото прилагане на това изискване, обаче се нуждае от допълнителна европейска регулация. Необходима е по-подробна информация за това как държавите членки да докладват и събират данни за киберпрестъпността, както и допълнителни указания за начина, по който да се прилагат мерките. За да се избегне несигурност и несъгласуваност по

[16] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, European Commission, 7.2.2013

въпроса как националният компетентен орган за NIS определя и измерва киберинцидентите със „сериозно въздействие“, ще трябва да се въведат общи системи за докладване и да се внесе допълнителна яснота относно изискванията за нотифициране. Наложително е също така при създаването на националния компетентен орган за NIS да се вземе предвид разпределението на правомощията в рамките на държавите членки, особено в онези със силно федерализирани или децентрализирани структури.

Сериозен е и акцентът върху е постигането на високо ниво на защита на личните данни. Регламентът е, че съответните национални органи отговарят за безопасността на данните на гражданите на ЕС, независимо от тяхното местонахождение. Реализирането на това изискване, очевидно ще Бъде съпроводено с доста сложности. На практика прилаганито му означава, правилата на ЕС да бъдат „изнесени“ в други части на света, което би могло да доведе до спорове относно юрисдикцията с други държави. Мотивът да се защитят данните на гражданите е похвален, но има съмнения как това ще се осъществява на практика, особено предвид сложността на трансграничните правни и регулаторни въпроси.

Националната стратегия: Европейската агенция за информационна сигурност (European Network and Information Security Agency - ENISA) публикува „Национална стратегия за киберсигурност. Практическо ръководство за развитие и изпълнение“ (National Cyber Security Strategies. Practical Guide on Development and Execution)[17], в което се представят добри практики и препоръки за това как да се развива, прилага и поддържа стратегия за киберсигурност.

В ръководството, националната киберстратегия за сигурност се определя като инструмент за подобряване на сигурността и устойчивостта на националните информационни инфраструктури и услуги. Тя създава редица национални цели и приоритети, които трябва да бъдат постигнати в определен период от време. Като такава, тя осигурява стратегическа рамка за подхода на една нация към кибернетичната сигурност.

Жизненият цикъл на националната стратегия за кибернетична сигурност има две ключови фази:

1. Разработване и изпълнение на стратегията.
2. Оценка и адаптиране на стратегията.

На фазата на разработване и изпълнение на стратегията трябва да се реализират следните основни задачи:

- установяване на визията, обхвата, целите и приоритетите;
- национална оценка за риска, с конкретен акцент върху критичните информационни инфраструктури;
- преглед на състоянието на основните елементи на стратегията на национално равнище;
- разработване на ясна рамка за управление на място, която да определя ролите и отговорностите на всички заинтересовани страни. Тя осигурява рамка за диалог и координация на различните дейности, предприемани в жизнения цикъл на стратегията

[17] Вж: *National Cyber Security Strategies. Practical Guide on Development and Execution*, European Network and Information Security Agency (ENISA), December 2012

- ефективно сътрудничество между публичния и частния сектор;
- установяване на надеждни механизми за обмен на информация между частните и публичните заинтересовани страни;
- разработване на национални киберпланове за реагиране;
- упражнения за проверка на съществуващите планове за извънредни ситуации;
- установяване на минимални изисквания за сигурност за даден сектор;
- създаване на механизми за докладване на инциденти;
- осведомяване на потребителите относно киберзаплахи за сигурността и слабите места;
- насърчаване на научноизследователската и развойната дейност;
- засилване на обучението и образователните програми в областта на киберсигурността;
- създаване на възможност за реагиране при инциденти;
- да се подготви съгласувана и координирана реакция срещу престъпленията в кибернетичното пространство;
- международно сътрудничество и обмен на информация;
- създаване на публично-частно партньорство;
- баланс между сигурността и неприкосновеността на личния живот.

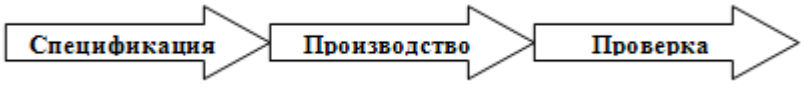
След като стратегията е разработена и се изпълнява в съответствие с изброените основни задачи, периодично трябва да бъде оценявана степента до която се постигат целите. Така ще е възможно да се предприемат всички необходими коригиращи и превантивни действия, които да доведат до съответствие или с настъпили промени, или с целите на стратегията. На тази втора фаза от жизнения цикъл на киберстратегията - оценка и адаптиране, основна задача, освен получаване на данни за състоянието на съществуващите политики, е да се определят бъдещите цели и стратегията да се коригира в съответствие с тях.

Методологията: Препоръчваната от ENISA методология за изработване и адаптиране на стратегия за киберсигурност е базирана на модела на Деминг „Plan-Do-Check-Act" (PDCA)[18], който се използва за контрол и непрекъснато подобряване на стратегии, политики, процеси и продукти.

Този модел е известен е още като "Цикъл на Шухарт", "PDCA цикъл", "PDSA цикъл" или “SDCA цикъл”. Съществуват и редица други модификации на цикъла, които доказват приложимостта му в много области и ситуации.

[18] Вж: http://qmconsult.eu/free_books/model-PDCA.pdf и http://tuj.asenevtsi.com/TQM2009/TQM041.htm (30.05.2013)

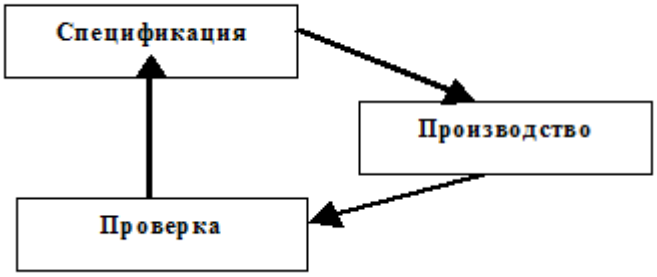
Деминг, всъщност, развива идеята на Шухарт (1939 г.), която е свързана с цикличността на производствания процес. Разбирането, което той променя се отнася до процеса на управление на качеството във вид на линия, с три етапа



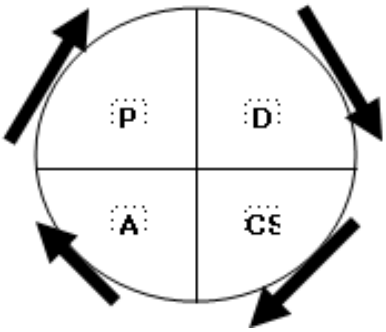
1. Разработка на спецификация (техническо задание, технически условия).
2. Производство на продукция, удовлетворяваща спецификацията.
3. Проверка (контрол) на произведената продукция за оценка нейното съответствие на спецификацията.

Това, което Шухарт прави, е да преобразува линията в кръг, който той отъждествява с "динамически процес на обогатяване на знанията".

След първия кръг се получават нови знания от резултатите от проверката. Тези знания дават възможност да се подобри спецификацията, което пък подобрява произведения продукт и така цикълът на подобрения продължава.



Деминг стъпва върху тази идея на Шухарт и я развива **в** в т.нар. PDCA (Plan-Do-Check-Act) цикъл, като дава по-общи названия на всеки от етапите. През 20-те години на XX век, Деминг развива PDCA (Plan-Do-Check-Act) цикъла, като добавя още един етап - Изучи (Study). Така е формулиран цикълът PDSA (Plan-Do-Study-Act). Той се използва за анализ на получената на втория етап (изпълнение) информация и е насочен към постоянни подобрения.



Първи етап - Планиране (Plan)

На него трябва да дадат отговори на следните шест въпроса:

- какво? (what?) – дефиниране на целите и задачите;
- защо? (why?) – обосноваване на необходимостта;
- кой? (who?) – определяне на отговорностите;
- как? (how?) – определяне на метода (методите) на извършване;
- къде? (where?) – ограничаване на полето на действие;
- кога? (when?) – разработване на план (график).

Втори етап - Изпълнение (Do)

В началото на този етап се извършва необходимото обучение и квалификация След обучението (или паралелно с него) се изпълнява и внедрява планираното.

Трети етап - Проверка (Check)

На този етап се проверява как е изпълнено и внедрено планираното действие и се оценяват постиженията.

Изучи (Study) **–** използва се при PDSA цикъла

Като част от този етап - изучаване и анализ на постигнатите резултати, с цел уточняване на по-нататъшните действия.

Четвърти етап - Действие (Act)

В зависимост от резултатите на проверката, на този етап са възможни два вида действия:

- въвеждане на постигнатото по-високо ниво като нов стандарт (формализиране) в организацията;
- извършване на коригиращи и/или превантивни действия за подобряване на постигнатото и за постигане в следващия цикъл още по-високо ниво.

Идеологията на цикъла на Деминг е да показва пътя на подобрения. Четирите фази на цикъла са описани в жизнения цикъл на стратегията за киберсигурност: разработване, изпълнение, оценка и корекция. Ефективната стратегия за сигурност в киберпространството, което е една изключително динамична и иновативна среда, трябва да бъде изградена именно върху такава методология, която позволява адекватно адаптиране и успешно развитие.

Практики: Анализът на съществуващи национални стратегии за киберсигуност (NCSS) показва съществени общи характеристики и някои различия, породени от националната политическа специфика.

Една от съществените общи характеристики е интегрирането на проблема киберсигурност в националната сигурност. Повечето стратегии за национална сигурност в една или друга степен отделят внимание на проблемите за сигурността в кибернетичното пространство. Теденцията е, включително и заради засиленото акцентиране от страна на

значими международни организации, да се засилва значението на сигурността в кибернетичното пространство, особено по отношение на защитата на критичната информационна инфраструктура, заради което в перспектива измеренията на киберсигурността все повече ще бъдат обхванати в самостоятелни национални стратегии за киберсигурност (NCS).

Четири са главните, повтарящи се теми в стратегиите за киберсигурност:[19]

- Поддържане на сигурна, устойчива и надеждна електронна работна среда.
- Насърчаване на икономическия и социален просперитет/ насърчаване на доверието и създаване на условия за бизнеса и за икономически растеж.
- Преодоляване на риска при използване на информационни и комуникационни технологии.
- Укрепване устойчивостта на инфраструктурите.

Тези основни теми като правило се формулират като стратегически цели, които по-нататък се разграждат в голямо разнообразие от приоритети.

Допълнителни съществени теми в стратегиите по отношение на визията за поддържане на сигурно киберпространство са изразяваната от някои страни необходимост да се повиши информираността в обществото относно риска в кибернетичното пространство, подчертаването на необходимостта от изграждане на ефективни държавни системи, от приемане на подходяща регулаторна рамка, от модернизиране на правната рамка, от справяне с престъпленията в кибернетичното пространство, от укрепване на критичните инфраструктури. Смята се, че тези и подобни цели също така допринасят за икономическия просперитет чрез насърчаване на доверие и гъвкавост.

Различното приоритизиране на целите се предопределя от различаващите се разбирания за понятието „киберпространство“. Някои страни влагат в него по-широко разбиране, което включва инфраструктури, а други имат по-тясно тълкувание, приравнявайки го с интернет. Съединените щати са в единия край на спектъра с широко определение на киберпространството, което имплицитно включва дори и социалните мрежи. Там е и Холандия, която в своята стратегия включва в киберпространството и чип картите, и електронните системи на автомобилите. На другия край на спектъра, са страни като Австралия, Канада, Германия, Нова Зеландия и Испания, които поставят акцент върху интернет и свързаните с интернет информационни технологии.[20]

Едно от откритията на Luiijf и др.[21], в изучаването на 19 NCSS е, че в по-малко от половината от тях има изрично определяне на понятието "кибернетична сигурност". В някои стратегии то е обяснено описателно. В останалите, обаче, сигурността в кибернетичното пространство се обсъжда без да се определя какъв смисъл се влага в понятието. Европейската агенция за мрежова и информационна сигурност (ENISA) също отчита липсата на определения и дава препоръки за решаване на ситуацията в държавите-членки на Европейския съюз.[22]

---

19 Вж: Eric Luiijf, Kim Besseling, „Graaf, Patrick De, Nineteen national cyber security strategies“, *International Journal of Critical Infrastructures*, Volume 9, Numbers 1-2, January 2013 , pp. 3-31

20 Пак там

21 Пак там

22 ENISA, National Cyber Security Strategies. Setting the course for national efforts to strengthen security in cyberspace, (Heraklion: ENISA, 2012)

В началото на 2011 г. руско-американска двустранна работна група, от East West Institute (EWI) и Московския университет, изготвя международна кибертерминологична рамка. Тя определя кибернетичната сигурност като "свойство на киберпространството (киберсистемата) да противостои на преднамерени и/или непреднамерени заплахи, а също да реагира на тях и да се възстановява след въздействието на тези заплахи"[23].

В предложената от ЕК, през февруари 2013 г., Европейска стратегия за кибер-сигурност се съдържа едно доста по-разширено тълкуване на понятието „кибернетична сигурност“: „Под киберсигурност обикновено се разбират предпазните мерки и действия, които могат да бъдат приложени за предпазване на киберпространството както в гражданската, така и във военната област, от заплахи, които са свързани с неговите независими мрежи и информационна инфраструктура или могат да нарушат работата им. Целта на киберсигурността е да се съхрани наличността и целостта на мрежите и инфраструктурата, както и поверителността на информацията, която се съдържа в тях“[24].

Терминът „престъпление в кибернетичното пространство“ се определя само в три от 19 NCSS проучени от Luiijf и др. В цитираното руско-американско изследване опреде-лението на този термин е: „използване на киберпространството, за престъпни цели, които се определят като такива от националното или международното законодателство“[25], а в предложението за Европейска стратегия за киберсигурност, отново има по-описателно тълкуване - „широк набор от различни престъпни деяния, в които компютри и информа-ционни системи са или основен инструмент, или основна цел. Киберпрестъпността обхваща традиционни престъпления (например измами, фалшифициране и кражба на самоличност), престъпления свързани със съдържанието (например онлайн разпространение на детска порнография или подбуждане към расова омраза), и престъпления, които са възможни само при компютри и информационни системи (например атаки срещу информационни системи, предизвикване на отказ от услуга и зловреден софтуер).[26]

Отсъствието на еднозначни и общопрети дефиниции на основните понятия, използвани в стратегиите за киберсигурност, може да доведе до значително ниво на объркване в собствената страна. Освен това, тъй като киберзаплахите са глобални, еднозначните определения ще помогнат в разбирането на подхода към кибернетичната сигурност от други народи, съюзи и международни организации, както и обратното. Поради тази причина, без дефинирана и международно хармонизирана кибертерминологична рамка, националните стратегии за киберсигурност трудно ще могат ефективно да постигат целите си. В този дух, като положителна може да бъде оценена практиката повечето нации да обнародват онлайн версия на своите NCSS, включително и на английски език.

---

23 EastWest Institute and Moscow State University, Russia-U.S., *Bilateral on Cybersecurity: Critical Terminology Foundations*, (Brussels and Moscow: EastWest Institute and Moscow State University, 2011)

24 Вж: Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council,the European Economic and Social Committee and the Committee of the Regions, Brussels, European Commission, 7.2.2013

25 EastWest Institute and Moscow State University, Russia-U.S. Bilateral on Cybersecurity: *Critical Terminology Foundations*, (Brussels and Moscow: EastWest Institute and Moscow State University, 2011)

26 Вж: Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council,the European Economic and Social Committee and the Committee of the Regions, Brussels, European Commission, 7.2.2013

Освен нееднаквото разбиране за ключови понятия като киберпространство, съществуващите NCSS се различават и когато дефинират най-значимите киберзаплахи. Повтарящите се категории киберзаплахи, идентифицирани в съществуващите NCSS[27] са заплахите за:

- критичните инфраструктури;
- икономическия просперитет;
- националната сигурност;
- общественото благосъстояние;
- общественото доверие в информационните и комуникационни технологии;
- глобализацията.

Докато някои от тези категории са признати във всички или в повечето NCSS (например, кибер заплахи за критичната инфраструктура) други, като например заплахите на глобализацията или общественото благосъстояние, са описани пряко или косвено в само в няколко стратегии.

В съществуващите NCSS се идентифицират и източниците на киберзаплахи. Сред главните са: кибернетични заплахи чрез широкомащабни атаки, терористи, чужди народи; шпионаж, организираната престъпност; политически активизъм (hacktivism) срещу услуги базирани върху информационно-комуникационни технологии. Някои категории заплахи, като киберзаплахите от организирана престъпност, са подчертани в повечето NCSS. Други видове, като заплахи от активисти (hacktivism) или екстремисти, фигурират в няколко NCSS. Четирите категории източници, споменавани най-често в NCSS са: организирана престъпност; кибернетични заплахи от чужди държави (кибервойна); киберзаплахи, свързани с терористи; кибершпионаж.

Анализът на досегашната практика на изработване на киберстратегии е позволила на авторите на Наръчник за рамките на националната киберсигурност, да формулират някои основни правила и препоръки за политиците, занимаващи се с тази материя, към които се присъединяваме: [28]

Приемане на "един размер за всички (one size fits all) " стратегия: при формулиране на национални стратегии за сигурност или на NCSS, политиците могат да се изкушат да се консултират със съществуващите стратегии на други страни. Въпреки, че това може да бъде полезно, за да се видят възможните формати на стратегии и да се обособят националните интереси, политиците трябва да бъдат внимателни и да не прехвърлят съдържание, което е в противоречие с националните изисквания. Копирането на заплахи и рискове от чужди стратегии, които не са уместни за страната може да донесе повече вреда, отколкото полза, заради отклоняване на национални ресурси. При желание да има съгласуваност със стратегиите на съседите и/или съюзници, политиците могат да смекчат риска "one size fits al", чрез приоритизиране на възприеманите заплахи или определени политически отговори. Например, в стратегията на Обединеното кралство за четирите най-приоритетни риска през

---

27 Вж: Eric Luiijf, Kim Besseling, Patrick De Graaf, „Nineteen national cyber security strategies“, *International Journal of Critical Infrastructures*, Volume 9, Numbers 1-2, January 2013 , pp. 3-31

28 Alexander Klimburg, *National Cyber Security Framework Manual*, NATO Publication, 2012

седващите пет години са определени: международният тероризъм, кибератаките, международните военни кризи и големите аварии или природни бедствия[29].

Пренебрегване на връзки с други национални/международни стратегии: за ефективността на стратегията за национална сигурност (или NCSS) е важно тя да съответства на съществуващите или бъдещи самостоятелни подстратегии, особено на такива, които предоставят по-големи подробности за това как определена заплаха или предизвикателство ще се управлява (напр. борба с тероризма). Такава практика съдейства за рационалното разпределение на ресурсите за постигането на основните стратегическите цели и подцелите от специализираните стратегии за сигурност. Около половината от съществуващите NCSS нямат пряка връзка със съответните национални стратегии за сигурност.

Липса на актуализация/механизъм за преглед: някои страни, като например САЩ, имат закони или други механизми за преразглеждане или актуализиране на съществуващи стратегия за национална сигурност (NSS) и други документи от стратегическо естество. За страните, които не разполагат с такива механизми, преформулирането на NSS или NCSS може да става с еднократен акт, ако има политическата воля за това. В противен случай, има значителен риск тези стратегии да останат просто един документ с течение на времето. Това важи с особена сила за стратегиите, за които развитието на технологиите може бързо на направи „стари“ отделни части от тях. Например, последиците (рисковете) за сигурността от сравнително неотдавна появили се технологии като изчислителни облаци и 3D (триизмерен) печат, няма как да е отчетено напълно в NCSS, които се появиха около 2008 г.

Липса на група за междуведомствена координация на средно ниво: формулирането на NSS или NCSS изисква информация от различни държавни ведомства и агенции. В подкрепа на този процес, създаването на междуведомствена координационната група на средно ниво, може да бъде полезно за хармонизиране на различните изисквания на всички правителствени отдели.

Неуспех при идентифицирането на критичните услуги: защита на критичните инфраструктури е общо изискване, присъстващо в NCSS. Заради общопризнатата значимост на проблема със защитата на критичните инфраструктури, политиците трябва предварително да дефинират кои услуги са най-критични за благосъстоянието на обществото. Определянето им като приоритетни, в NSS или в самостоятелна стратегия - може да бъде от полза при формулирането на бърза реакция в случай на извънредна ситуация. Положителен пример в тази насока е естонското правителство, което предварително е идинтифицирало 42 критични услуги, вариращи от сигурност на доставките за производство на електроенергия до поддържане пристанището на Талин свободно от лед през зимните месеци, за да се улесни транспортирането на стоки и хора.

Липса на информираност - особено между политиците: формулирането на Стратегията е средство към целта. Една добре развита стратегия следва бъде ръководството за създателите на политики относно ключовите цели, необходимите ресурси и как те могат да се използват най-ефективно. В случай на самостоятелна стратегия, която обхваща специфична област, повишаването на нивото на осведоменост сред правещите политики и вземащите политически решения може да е особено важно, за да се улесни изпълнението на стратегията. Например, по отношение NCSS, стратегиите могат да страдат от ограничена осведоменост на висшите политиците по киберпроблемите и техните последици, особено

[29] UK Cabinet Office, *The National Security Strategy: A Strong Britain in an Age of Uncertainty, 2010*

ако съществува усещането, че частният сектор трябва да играе основната роля за гарантиране на сигурността в киберпространството.

Появата на "петата област" - на киберпространството като поле на човешката дейност - със сигурност е едно от най-значимите събития в историята. Социално-политическите отговори на въпросите, поставени от възхода на киберпространството, като цяло значително изостават от скоростта на технологичните промени. Заради това, националните стратегии за киберсигурност по принцип са под вечната заплаха да остаряват много бързо. Според някои експерти самото понятие "национална киберсигурност" е илюзия „три в едно“: всеки създава концепцията за киберпространството по свое собствено усмотрение, то не може да се регулира в национален контекст и поне в настоящия му вид, по своята същност то е вечно несигурно.

В този контекст създаването на ефективно работещата национална стратегия за киберсигурност е огромно предизвикателство пред политиците, защото цената на техния неуспех ще е много висока.

БИБЛИОГРАФИЯ

Bendiek, Annegret. „European Cyber Security Policy.“ *RP 13* (Berlin: German Institute for International and Security Affairs, October 2012).

Cybersecurity Strategy of the European Union:An Open, Safe and Secure Cyberspace. Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions (Brussels, European Commission, 7.2.2013).

Dunn-Cavelty, Myriam. „Systemic cyber/in/security – from risk to uncertainty management in the digital realm.“ (Swiss Re Centre for Global Dialogue, 15 September 2011), http://cgd.swissre.com/features/Systemic_Cyber_In_Security.html.

Klimburg, Alexander. „National Cyber Security Framework Manual.“ NATO Publication (2012).

Luiijf, Eric, Kim Besseling, Patrick De Graaf. „Nineteen national cyber security strategies.“ *International Journal of Critical Infrastructures* 9, no. 1-2 (January 2013): 3-31.

„National Cyber Security Strategies.“ Practical Guide on Development and Execution (European Network and Information Security Agency (ENISA), December 2012).

Nerlich, Uwe, F. Umbach. „European Energy Infrastructure Protection: Addressing the Cyber-warfare Threat.“ (2009), http://www.ensec.org/index.php?option=com_content&view=article&id=219:european-energy-infrastructure-protectionaddressing-the-cyber-warfare-threat&catid=100:issuecontent&Itemid=352.

UK Cabinet Office. “The National Security Strategy: A Strong Britain in an Age of Uncertainty.” (2010).

Дракалиева, П., И. Иванов. „Съвременната концепция за защита на критичната инфраструктура: генезис, цели, методология, проблемни зони, Защита на критичната инфракструктура в ЕС и България - икономически и организационни аспекти.“ (София, 2010: 19).