КРИТИЧНА ИНФРАСТРУКТУРА – СТРАТЕГИЧЕСКИ ИЗМЕРЕНИЯ

Десислава Стоева
Университет по библиотекознание и информационни технологии
гр. София

CRITICAL INFRASTRUCTURE - STRATEGIC DIMENSIONS

Desislava Stoeva

Анотация*: В динамичната среда в която живеем би трябвало да помислим за рисковете за информационната сигурност и заплахите от кибернетични атаки срещу стратегически ,граждански и военни комуникационно-информационни системи и обекти от критичната инфраструктура и да имаме ясна цел и законова уредба за прилагане на защитата им.*

Ключови думи*: сигурност, защита на стратегически обекти, законодателство, превенция.*

Abstract: *In the dynamic environment in which we live, we should think about the risks to information security and threats of cyber attacks against strategic, civilian and military communications-information systems and critical infrastructure objects, and have a clear goal and legal framework to enforce their protection.*

Key words: *security, protection of strategic sites, legislation, prevention.*

Стратегическата среда на сигурност е сложна, динамична и с трудно предвидими измерения. Влияние върху формирането й оказват редица фактори като: глобализацията; кризисните явления във финансовата и икономическата сфера; разпространяването на оръжията за масово унищожение и на средства за тяхната доставка; климатичните и здравните проблеми; демографските, екологичните и енергийните проблеми; асиметричните рискове и заплахи; заплахите за информационната сигурност; страните със слаба държавност; вътрешните и регионалните конфликти; европейската и евроатлантическата интеграция; усилията на международната демократична общност за поддържане на мира и стабилността. Процесите на глобализация влияят неоднозначно върху формирането на различните аспекти на средата на сигурност. Те създават условия за развитие на връзките между държавите, но и задълбочават икономическото и социалното неравенство и дисбалансът в развитието на страните и демографските диспропорции. Кризисните финансови и икономически явления в света се отразяват негативно не само върху вътрешната стабилност на държавите и международните отношения, но и върху сектора на сигурност и отбрана. Промените в климата, природните аномалии и бедствия, както и широкото разпространение на опасни болести допълнително усложняват съществуващите проблеми – бедност, социално напрежение, екологична обстановка, като застрашават управлението и стабилността на държавите. Те създават предпоставки за вътрешни конфликти и хуманитарни кризи, които изискват заделяне на сериозни граждански, финансови и военни ресурси за

тяхното разрешаване. Проблемите, свързани с недостига на енергийни и природни ресурси се превръщат във все по-сериозно предизвикателство за всички страни. В този контекст енергийната сигурност придобива нови измерения, а рисковете и заплахите в тази област произтичат от засиленото противоборство на интереси, действията на терористични групи и въоръжени формирования и наличието на нерешени конфликти в районите на добиване и транспортиране на ресурси. Ключово влияние върху стратегическата среда на сигурност оказват асиметричните и другите транснационални рискове и заплахи, особено тероризмът. Терористичните организации децентрализират структурите си, което затруднява локализирането и неутрализирането на отделните им елементи. Увеличават се възможностите терористите да използват радиоактивни материали, химически и биологични агенти. Увеличават се рисковете за информационната сигурност и заплахите от кибернетични атаки срещу стратегически, граждански и военни комуникационно-информационни системи и срещу сили, участващи в мисии и операции извън територията на страната. Те се пораждат от динамичното развитие на технологиите, разширяването на кръга от престъпни и екстремистки организации и хакери, които се опитват да осъществят нерегламентиран достъп до класифицираната информация, създавана, обработвана, съхранявана и пренасяна в автоматизирани информационни системи или мрежи. Анализ на националното законодателство на България по защита на критичната инфраструктура В рамките на МО Гражданска отбрана осъществява дейности по организация и защита на населението и народното стопанство (ОЗННС). Основен акцент е планирането на ЗННС в условия на термоядрен конфликт. Именно в този контекст е разработен единственият действащ подзаконов акт, свързан с устойчивостта на критичната инфраструктура на България, са „Инженерно-техническите правила по Гражданска отбрана" Постановление № 45 на министерския съвет от 1988г. (необнародван.) Радикалните промени в държавното устройство и собствеността в икономиката до голяма степен ликвидират съществуващата система за защита на народното стопанство. Същевременно част от съществувалите ведомствени традиции и понятиен апарат са запазени 17 години след началото на прехода. Терминът „критична инфраструктура" е въведен в българското законодателство едва през 2005 г. с приемането на Закона за управление при кризи. Паралелно с него обаче в българското законодателство се използват още 4 термина, които са близки или дори идентични по значение. Това припокриване на понятия е сериозен недостатък на изграждащата се система за ЗКИ. От юридическа гледна точка е необходимо създаването на единен понятиен апарат, приложим за всички актове, което ще консолидира нормативната база, ще спомогне за преодоляване на противоречията в нея и ще улесни правоприлагането. Исторически погледнато, до съвсем неотдавна политиките на ЕС и САЩ по отношение на сигурността на КИ се фокусираха най-вече върху физическата й защита. ЕС е изправен пред все по-сложна съвкупност от рискове, които са преплетени във всички аспекти на бизнеса, инфраструктурата и общността. Заплахата от природни бедствия, финансова нестабилност, пандемии, престъпления в кибернетичното пространство, социални безредици, терористични актове и други разрушителни събития, произтичащи от процеса на глобализация, вече са част от ежедневието ни.

След поредицата природни бедствия и терористични актове през последните години, световната общност вече призна, че не е възможно да се предотвратят всички заплахи за всички активи по всяко време. Няма как да пренасочим ураган, да намалим магнитудата на силно земетресение, да пресечем всяка кибер атака или да предотвратим всяко разрушение. В тази логическа последователност, устойчивостта на критичната инфраструктура се очертава като допълнителна цел – комплекс от дей-

ности, насочени към превенция. Докато политиките за сигурност на критичната инфраструктура са съсредоточени основно върху предотвратяването на терористични актове, аварии и други разрушителни явления, дейностите по създаване на устойчивост на критичната инфраструктура целят засилване на способността й да продължи да предоставя стоки и услуги, дори в случай на разрушение/нарушена функционалност. Приложени заедно, стратегиите за сигурност и устойчивост на критичната инфраструктура осигуряват по-пълен набор от дейности за постигане на по-висока степен на готовност на КИ системите за работа в несигурна среда с множество опасности.

Общоприето определение за устойчивост на критичната инфраструктура до този момент не съществува. Въпреки това има известно припокриване между десетките предлагани дефиниции. Най-разпространената тема във всички дефиниции е, че инфраструктурната система се справя с промени, които могат да повлияят на нейната работа. Много определения предлагат механизми, с които инфраструктурата да реагира на промените и най-често споменаваните са:

- Способности да абсорбира или да устои на въздействието на промяната;
- Способности да се адаптирате в отговор на промяната;
- Способности за бързо възстановяване на системата и системната функционалност.

Ефективността или количеството на ресурсите, необходими за успешно реагиране на системен срив, е по-рядко обсъждан, но но също толкова важен въпрос. Във време на криза работната ръка, оборудването и други критични ресурси за реагиране и възстановяване са с голямо търсене. Следователно, способността на системата да работи по време на разрушителни събития с по-малко потребление на ресурси, отколкото другите системи, би била желана характеристика и ще я направи по-устойчива от системите, изискващи повече ресурси.

Използвана литература:

1. Йончев, Димитър. В търсене на сигурността: Сигурността в концепцията на присъствието / Димитър Йончев. – София: Изток-Запад, 2014. – 416 с.
2. Концепция и стратегия за разработване на Система за ранно реагиране на кибер престъпления // Международна академия за обучение по киберразследвания, София, 2014. – 28 с.
3. Манев, Евгени. Глобална, регионална и национална сигурност / Евгени Манев. – София: Софттрейд, 2012. – 494 с.
4. Организация на системата за национална сигурност. // УНИБИТ, http://iniod.com/wp-content/uploads/2013/11/02-Организация на системата за национална сигурност.doc
5. Проучване на необходимостта от създаване на система за ранно реагиране на кибер престъпления // Международна академия за обучение по киберразследвания, София, 2014. – 40 с.
6. Стратегия за национална сигурност на Република България. // Министерство на отбраната на Република България, 19.03.2011. http://www.md. government. bg/bg/doc/strategicheski/20110319_strategia_za_nacionalna_sigurnost.pdf
7. Закон за защита на класифицираната информация. https://www.lex.bg/laws/ldoc/2135448577

Десислава Стоева
email: desislavap.stoeva@gmail.com
Докторант
Университет по библиотекознание и информационни технологии, гр. София