CHARACTERISTICS OF CRITICAL INFRASTRUCTURE SITES AS SITE OF TERRORIST THREATS

Hristo A. Desev

National Military University "V. Levski", Artillery, "Air Defense and CIS" Faculty
Shumen, "K. Scorpil"str. № 1

***Abstract**: The report analyzes the approaches of European countries to the identification of critical infrastructure according to the accepted definitions. The criteria for assessing threats to key sectors, light targets and cyber threats to industrial management systems are personalized. The connection of the terrorist attacks to the critical infrastructure on the governance of the states has been revealed. Conclusions and recommendations have been made for adapting the protection system to the common European system for protection and mitigation of the effects of terrorist threats.*

***Key words:** criticality threshold, crisis management, key factor, counter-terrorism strategy*

ХАРАКТЕРИСТИКА НА ОБЕКТИТЕ ОТ КРИТИЧНАТА ИНФРАСТРУКТУРА КАТО ОБЕКТИ НА ТЕРОРИСТИЧНИ ЗАПЛАХИ

Христо А. Десев

Тероризмът създава сериозна заплаха за принципите на върховенството на закона, защитата на правата на човека и тяхното ефективно осъществяване. В контекста на своите задължения по международното право в областта на правата на човека държавите са длъжни да защитават лицата под тяхна юрисдикция, от намеса в правата им от терористични структури. Това задължение е особено важно, като се вземе предвид, че потенциалното въздействие върху критичните важни обекти от инфраструктурата (КВОИ), може да има ефект върху населението, според ролята, която подобна инфраструктура играе в поддържането или прилагането на жизненоважни функции на обществото.

В глобалната стратегия за борба с тероризма в Раздел II "Мерки за борба с тероризма и неговата превенция" държавите-членки решиха да засилят всички усилия за подобряване на безопасността и защитата на особено уязвимите обекти, като например инфраструктура и обществени места, така и отговор на терористични атаки и други бедствия, по-специално в областта на гражданската отбрана, като същевременно признават, че държавите се нуждаят от помощ за тази цел.

На 17 февруари 2017 г. Съветът за сигурност на Обединените нации окончателно приема резолюция 2341 относно защитата на критичните инфраструктурни съоръжения и разширяване на способностите на държавите за предотвратяване на атаки срещу критични инфраструктурни съо-

ръжения и призовават държавите-членки да реагират на опасностите от терористични атаки върху критичната инфраструктура и съоръжения.

Процеса на идентификация на КВОИ, обикновено започва с приемането на всеобхватна дефиниция за това какво следва да се разбира под КВОИ. Това е необходимо за създаване на платформа, върху която да бъде разработена по-голяма политическа и регулаторна рамка. В общи линии, докато определенията в някои страни се подчертава крайност или назначението на инфраструктурата (т.е. критичността е свързана с изпълнението на основните социални функции), то други поставят акцент върху последиците от унищожаване или повреда.

В резолюция 2341 на Съвета по сигурност се фиксира, че "всяка държава сама определя, кои са нейните критични инфраструктурни обекти" при това, тя не препоръчва никакъв специфичен метод за селектиране на КВОИ сред многото инфраструктурни съоръжения, разположени на нейната територия.

По този начин, страните се предоставят голяма свобода на действие при избора на критерии, за да се определи кои инфраструктурни съоръжения, работещи на тяхна територия, съответстват на прага на критичност. Задачата е значително сложна. Разликата между най-важните (значими) обекти на инфраструктурата и тези, които трябва да получат статута "критически важно", е ключов фактор, даващ възможност да разпределят приоритетно ограничени ресурси за защита на огромни активи, системи и процеси. От една страна, включването на твърде много инфраструктури в категорията "критично важни" да се превърне в неуправляема задача (освен, че е и финансово нестабилна). От друга страна, прекалено рестриктивен подход рискува броя на ключови активи и процеси не са защитени с потенциално катастрофални последици в случай на инцидент.

КВОИ, могат да се характеризират, като се има предвид тяхната роля в ежедневието и защитата на правата на човека (например инфраструктура, която е от жизненоважно значение за функционирането на системата за медицинска помощ; системите за аварийно обслужване, водоснабдителните и канализационните системи и др.), както и на въздействието върху правата на човека, което може да се случи поради повреда, нарушения или унищожаване на инфраструктурни съоръжения (например, невъзможността да се осигурят подходящи или дори жизненоважни медицински услуги, екологични щети, които могат да доведат до смъртта на хора, здравеопазване и т.н.). Този подход съответства на духа на съществуващите дефиниции в Европейския съюз "…критични инфраструктурни обекти" като "активи от система или част от нея", която "е необходимо за поддържане на жизнените функции на обществото, здравеопазването, безопасността, опазването, икономическо или социално благополучие на хората ", нарушаването или унищожаването на която ще има значително влияние" в резултат на неспазване на тези функции ".

В процеса на създаване и експлоатация КВОИ непрекъснато са обект на най-различни опасности, включително природни явления, човешки грешки, технически повреди и престъпни действия в широк смисъл, зараждането на идеята за тяхната защитата като специална област на политиката за национална сигурност е пряко следствие от събития от 11Септември 2001 година.

През последните няколко десетилетия, терористите несъмнено засилиха интереса към КВОИ като потенциални обекти за постигане на своите цели. Още през 2002 година са открити явни признаци, че Ал-Кайда се стремят да използват факторите на уязвимост в обществени и частни комунални услуги в САЩ. Откриването в Афганистан на компютър, съдържащ структурна програма за анализ на характеристиките на язовирните стени, което предизвика Националния център за сигурност за Център за защита на САЩ инфраструктура, да разпространи предупредителен бюлетин (NIPC 2002).

Важно е да се отбележи, че едва ли всеки сектор е избегнал последиците от терористични дейности или най-малкото не е бил на вниманието на терористични групи. Примери изобилстват. В транспортния сектор, последните събития включват едновременни атаки през 2016 г. до летище Брюксел и метрополитена. Като цяло, 32 души загинаха, а около 300 са ранени.

Енергийният сектор е чест обект на терористична дейност, в резултат на атаки, извършени от Ал-Кайда и нейните клонове за съоръженията и персонала на петролните компании в Алжир, Ирак, Кувейт, Пакистан, Саудитска Арабия и Йемен.

Ключови водни инфраструктури са били обект на специално внимание от ИДИЛ. За периода 2013-2015 г., ИДИЛ ангажира около 20 големи атаки срещу сирийски и иракски обекти. В допълнение към унищожаване на тръбопроводи, санитарни съоръжения и мостове, ИДИЛ стратегически използва водната инфраструктура, като например изключване на подаването на вода (Vishwanath 2015 г.).

В редица случаи съществуват опити да се атакуват обекти от инфраструктурата, съдържаща опасни материали. На 26 юни 2015 г. самоубийствена кола-бомба се блъска в химически завод близо до Лион, като провокира експлозия в газови цистерни,. През 2016 г. две атомни електроцентрали в Белгия бяха блокирани по подозрение за опит на ИДИЛ за нападение, проникване или провеждане на саботаж в съоръженията, с цел да се добият ядрени радиоактивни материали.

Паралелно с основните сектори и обекти от КВОИ съществуват като цели на терористична дейност и „леки цели“. Концепцията за "леки цели" обикновено се свързва с места, където хората се събират в големи количества, като музеи, кина, религиозни обекти, търговски центрове и др. Леките цели са противовес на така наречените "трудни цели", които са местата с високо ниво на защита се осигурява от често въоръжени хора и/или където достъпът на обществеността се ограничава или подложени на строг контрол (например, военни съоръжения, посолства, летища).

Според последните атаки в зоните за пешеходци в Ница и Барселона, на Коледния пазар в Берлин и на други места, отворена среда и висока степен на достъпност до леките цели ги направи особено уязвими по отношение на терористични атаки. В същото време, леките цели предоставят на терористите перфектната платформа за нанасяне на удари с малки организационни усилия и водят до масови жертви.

В този контекст, резолюцията на Съвета за сигурност 2396 (2017) специфично признава опасността, за планирани нападения от чуждестранни бойци-терористи, свързани с ИДИЛ срещу леки цели след завръщането им от зоните на реалните бойни действия. Леките цели не винаги имат характеристиките на критични обекти предоставящи основни услуги, но се превръщат в такива при масови мероприятия (концерти, спортни прояви). В различието си двата вида обекти на КВОИ не трябва да се разглеждат самостоятелно, а в синергично единство, което съдейства за създаване на общи политики за защита и противодействие

Свързаните с тероризма заплахи за КВОИ са многоаспектни и могат да се класифицират по произход, количество, и според своя характер. Еднаквото разбиране за заплахите е основната стъпка за изграждане на обща система за противодействие.

Физическите заплахи са най-често срещаните и са свързани с физическо въздействие върху КВОИ със запалителни устройства, транспортни средства, взривни материали и др. С тях се постига пълен или частичен колапс, или унищожаване на инфраструктурата. Атаките могат да включват също умишлена модификация или манипулиране на системи и процеси в КВОИ (например, включване и изключване, отваряне и затваряне на обтураторите на тръбопроводи, потискане на технологичните сигнали, изпращане на сигнали за грешки или аларми).

Кибер заплахите са новост в терористичните действия и се различават съществено от физическите заплахи по своя характер, но крайният резултат може да бъде същият. Кибер заплахите могат да се групират в няколко направления:

- манипулиране на системи или данни - като злонамерени програми, които използват уязвимости в софтуерните и хардуерните компоненти на компютрите, които управляват работните процеси в КВОИ;
- изключване на критични системи, като например "отказ от поддържа";
- ограничават достъпа до критично важни системи или информация - с помощта на атаки за изнудване и откуп.

Въздействието върху съвременните интегрирани автоматизирани системи за управление на КВОИ бележат рязко увеличаване на инцидентите. През 2010г. близо половината от предприятията в сектор енергетика от 14 държави не са се срещали със заплахи в мрежите и сериозни откази на оборудването. За 2011г. 80% от същите предприятия са се сблъскали с мащабни откази, а 85% са разкрили проникване в мрежовите структури. В таблица 1 са обобщени основните заплахи за промишлените системи за управление.

Таблица 1

№	Заплаха	Обяснение
1.	Несанкционирано използване на точки за достъп с отдалечено използване	Точки за достъп до техническо обслужване-специални външни входове в ИКТ с недостатъчна защита.
2.	Мрежови атаки в корпоративните мрежи	Офисните връзки които са изградени позволяват несанкциониран достъп.
3.	Атаки срещу стандартните ИКТ компоненти.	Стандартните IT компоненти (готови продукти COTS), сървъри, база данни, които имат програмни недостатъци и се използват за атаки
4.	Атака от типа отказ от обслужване	Този тип атаки разконцентрират мрежовите връзки.
5.	Човешка грешка и саботаж.	Предните мерени действия от аут и инсайдъри и прояви на небрежност от служителите застрашават конфиденциалността и целите на защитата.
6.	Внедряване на вредоносно програмно осигуряване	Използване на мобилни IT компоненти за заразяване с вредоносно програмно осигуряване
7.	Публикуване на новости по мрежовите връзки на ИКТ	Позволява разкриването и четенето на командите за управление и въздействие върху тях.
8.	Несанкциониран достъп	Използване на необезопасени връзки поради не прилагане на аутефикационни и авторизационни методи.
9.	Атаки срещу мрежовите компоненти.	Злоумишлено манипулиране на мрежовите компоненти.
10.	Технически неизправности	Увреждания от екстремална природна среда, технически откази.

Заплахите за КВОИ традиционно са насочени към отделни обекти, но често имат и широк план за въздействие върху цял сектор от КВОИ или търсене на каскадни ефекти и блокиране на няколко сектора в една и съща географска зона. Така атаките започват като цели кампании или серийни атаки и се разпространяват върху множество институции с мултипликационен ефект, през 2011г. серията от атаки LURID начално насочена към ИКТ на редица дипломатически мисии и с едновременното въздействие върху работещи по изследване на Космоса институции. Не по-маловажен е факта, че за голяма част от секторите информация за получени инциденти в ИКТ не се публикува.

Идентифицирането на модели в такива сценарии често изисква силни аналитични инструменти и обработка на информация от обширни и разнородни източници. За да се усложни ситуацията, като ОССЕ подчертава, по отношение на енергийния сектор, информация за повечето кибератаки не са публикувани, тъй като съответните оператори не искат да докладват тези инциденти. Въпреки това, способността да разпознават основните динамиката и методите възможно най-рано е ключов фактор, който позволява на властите да обменят оперативна информация. Той повишава способността за по-ефективно отговарят на настоящите атаки и предотвратяване на неизбежните нападения срещу вероятните жертви (ОССЕ, 2013 г.).

В някои случаи, това, което изглежда като отделна атака, насочена към относително "маловажни" цели, в действителност, всъщност може да бъде част от по-амбициозна и постепенно разрастваща се атака.

В рамките на едно ограничено емпиричното проучване, проведено в тази област (Акерман, 2007 г.), се оказва, че КВОИ са привлекателни като обекти за атака по редица причини. На първо място, те могат да бъдат важна цел поради стратегическото си стойност за обществото, особено в високо индустриалните общества. Интервенцията в областта на функционирането на КВОИ, е с възможност за генериране на каскадни ефекти и позволява на терористите да максимизират щетите и само с един изстрел да генерират щети до нивата, които не могат да бъдат постигнати с атака срещу "обикновените" цели. Разузнавателните централи обобщават, че членове на Ал Кайда са прекарали значителен период от време на наблюдение, за седалищата на различни американски финансови компании и международни организации.

Други атаки към КВОИ могат да бъдат насочени за демонстриране на безсилието на правителствените институции. Например, терористичните организации могат да атакуват енергийни съоръжения, нефтопроводи и т.н., за да преустановят доставката на основни услуги за населението и да демонстрират уязвимостта на държавни органи и свързаните с политиката на правителството (Акерман 2007 г.).

Третият възможен мотив, свързан с предходните два, и е желанието да се получи по-висока степен на обществена разгласеност, отколкото би било възможно, като се фокусират върху "нископрофилни" цели.

Най-вероятно в редица случаи ще бъде налице комбинация от фактори, които насърчават терористични групи да извършат атаки върху КВОИ. Окончателното решение атаката по целевата инфраструктурата ще зависи от оперативните способности на групата да започне конкретна атака. Защитните мерки, взети на определена категория КВОИ естествено ще окаже влияние върху това решение. Това не означава, че терористите ще атакуват обекта, само когато те са сигурни, че може да успеят. Всеки опит, дори и неуспешен, когато предизвиква ограничени щети, може да осигури желаното ниво на резонанс в обществото, особено когато избраната цел е със символична стойност.

Въпреки че в повечето контра-терористични стратегии конкретно не се визира КВОИ, редица цели и институционални механизми, посочени в тях, допринасят за запазването на целостта им и жизнените социални функции, изпълнявани от тях. Например, терористичните стратегии косвено засягат проблемите на защитата на КВОИ, когато се установяват процедури за общо антикризисно управление след терористична атака.

Глобалната стратегия за борба с тероризма на Интерпол включва областта на КВОИ в своите процедури от действие 4.6 "Оръжия и материали", като определя на мандата на организациите от гледна точка на възможността "увеличаване на способността на държавите-членки да защитават своята критична инфраструктура и уязвими цели от физически и кибер атаки ". Стратегиите на защита на КВОИ трябва да съчетават концепциите и процедурите, определени в основите на борбата срещу тероризма, като се адаптират към специфични особенности и условия на защита на КВОИ.

Швеция формулира своята контра-терористичната стратегия в три направления: предотвратяване, предпазване и защита. По-специално, в рамките на "защита", целта е да се гарантира надеждна защита на хората, информацията, функциите и средствата - хората трябва да се чувстват сигурни, защитени и свободни в обществото. "

Законът в Белгия от 1 юли 2011 г. за защита на критична инфраструктура съдържа концепцията за федералната стойност "Points d'Interet Federal". Те се дефинират като "места, които не са маркирани като критична инфраструктура, но от особен интерес за обществения ред, за специална защита на хората и имуществото, да управляват извънредни ситуации или за военни интереси и които могат да изискват защитни мерки, предприети от Генералната дирекция на Главна дирекция. Антикризисен център.

Политиките за киберсигурност заемат централно място в защитата на КВОИ, тъй като те осигуряват основата, в която страните определят целите и средствата за защита на критичните информационни инфраструктури.

В САЩ, Департамента по национални инициативи за сигурност ръководи усилията на федералното правителство за осигуряване на безопасността на най-важните обекти на инфраструктурата на страната.[1] За да се предотврати всяка заплаха, смекчаване на последствията от тях и в отговор на тях, инициативите включват:

- развитие на технологично неутрална структура на доброволна киберсигурност;
- насърчаване и стимулиране на прилагането на практики за киберсигурността;
- увеличаване на обема, сроковете и качеството на информационния обмен за киберзаплахите;
- въвеждане на строга защита на неприкосновеността на личния живот и гражданските свободи във всяка инициатива за осигуряване на безопасността на критични инфраструктурни обекти;
- разработване на осведоменост за ситуацията, която взема под внимание както на физическите аспекти и кибер аспектите за това как функционират инфраструктурни структури в реално време;
- разбиране за каскаден принцип на въздействието при пробив в обекти от инфраструктурните съоръжения;
- оценка и развитие на публично-частно партньорство;
- актуализиране на План за защита на националната инфраструктура;
- разработване на интегриран план за научни изследвания и развойна дейност.

Департамента насърчава приемането на системата за киберсигурността на Националния институт за стандарти и технологии, за да се подобри киберсигурността на критични важни инфраструктурни обекти.[3] Структурата на подхода е ревизирана през април 2018 г. съдържа указания няколко ключови функции, които подобряват управлението на риска за киберсигурността:

идентификация – разработване на организационно разбиране на управлението на риск за киберсигурността относно системи, хора, активи, данни и потенциал;

защита - разработка и реализиране на съответните мерки за сигурност, за да се гарантират предоставянето на критични услуги;

откриване - разработване и прилагане на действия, за идентифицират случаите киберзаплахи;

отговор - разработване и прилагане на подходящи действия и предприемане на мерки при откриване на инцидент за киберсигурността;

възстановяване - разработване и прилагане на подходящи действия за поддържане на планове за устойчиво развитие и възстановяване на услугите, които са били повредени в резултат на инцидент в киберсигурността.

Анализа на разгледаните характеристики на обектите и подходите на отделните държави за ЗКВОИ категорично показват разрастващите се възможности за въздействие от страна на терористичните организации към секторите, които представляват основната инфраструктура на държавите. Показателна е устойчивата промяна към използване все по-често на киберсредата за осъществяване на терористичните актове. Общите категории в процеса на идентификация на обектите и оценката на стойността им за икономиката на отделните държави са основата за осъществяване на системна защита и дават възможност да се интегрират действията за защита. Персонализирането на факторите които характеризират вида на атаките е подход с който се позволява да се разкрият крайните цели на терористичния акт и да се насочат усилията за неговото неутрализиране или намаляване на ефекта от въздействието му. В международен аспект е необходимо да се подобри взаимодействието в определянето на стандартите за критичност на киберсредата за да се усъвършенства управлението на риска за киберсигурността.

References:

1. Министерство на националната сигурност, Бюлетин: ЕО 13636 "Подобряване на киберсигурността на критичната инфраструктура, безопасност и стабилност на критични инфраструктурни обекти PPD-21", на адрес: www.dhs.gov/sites/default/files/publications/eo-13636- PPD- 2F-FACT-ЛИСТ-508.PDF;

2. Министерство на националната сигурност, доброволно подпомагане на програмата Cyber Общността на критичната инфраструктура на обекти, в WWW.US-CERT.GOV/ccubedvp https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.041620t8.pdf;

3. Каранешев С, Копроративно управление на киберсигурността, София,2020г.;

4. Концепция и стратегия за разработване на Система за ранно реагиране на киберпрестъпления”, проект HOME/2011/ISEC/AG/ 40000002481 на Български кибер център по компетентност за обучение и изследвания, който се изпълнява от Международна академия за обучение по киберразследвания, 2014, София, 5с.