IT 4 Sec Reports

Нови тенденции в политиката за сигурност на критичната енергийна инфраструктура

Величка Милина

New Trends in the Policies for Security of Critical Energy Infrastructures

Velichka Milina

106

IT4Sec Reports 106
http://dx.doi.org/10.11610/it4sec.0106

Нови тенденции в политиката за сигурност на критичната енергийна инфраструктура

Величка Милина

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

София, януари 2013 г.

Величка Милина, Нови тенденции в политиката за сигурност на критичната енергийна инфраструктура**,** *IT4Sec Reports* 106 (София, Институт по информационни и комуникационни технологии, декември 2012 г.), http://dx.doi.org/10.11610/it4sec.0106.

IT4SecReports 106 „Нови тенденции в политиката за сигурност на критичната енергийна инфраструктура“. Съвременното разбиране за ефективна политика за сигурност на критичната енергийна инфраструктура поставя акцента върху способността да се систематизират уязвимостите, да се предвиждат заплахите и да се неутрализират рисковете от кибератаки върху елементи на сложно взаимообвързаните, интелигентни енергийни инфраструктури. Три са основните нови тенденции в политиката за сигурност на функционирането на критичната енергийна инфраструктура – киберсигурност, публично-частно партньорство и международно сътрудничество във формирането и реализирането на политиката за сигурност на критичната енергийна инфраструктура. Различни страни и международни организации предлагат свои модели на тези политики, чиято ефективност предстои да бъде доказвана.

IT4Sec Reports 106 „New Trends in the Policies for Security of Critical Energy Infrastructures“. The current understanding for effective security policy of the critical energy infrastructure focuses on the ability to systematically assess vulnerabilities, predict threats and neutralize the risks of cyber attacks on the interdependent elements of the complex, intelligent energy infrastructures. There are three major new developments in the security policy concerning the functioning of the critical energy infrastructure – cyber security, public-private partnership and international cooperation in the development and implementation of the policy for security of critical energy infrastructures. Various countries and international organizations offer their own policy models, while their efficiency is yet to be proven.

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

Постмодерното общество, като сложен организъм от мрежи, системи и инфраструктури, от които зависи неговото съществуване, все по-често е дефинирано като уязвимо, рисково (У. Бек). Предизвикателствата, пред които то ни изправя, обуславят необходимостта от ново схващане за неговите жизнено важни/критични системи и подходите за тяхната защита. Днес експерти и политици насочват вниманието си върху задълбочено изследване на новите параметри на уязвимостта на съвременните развити общества. Понятието “soft targets“ (меки цели) отдавна е легализирано и легитимирано, а управлението на сигурността на една от най-уязвимите системи – жизнено важните граждански инфраструктури, започна да става част от политиката за сигурност.

Енергийната сигурност е ключов аспект на националната и глобалната сигурност, а енергийната инфраструктура – една от особено значимите за нормалното функциониране на обществото критични инфраструктури. През последните години рисковете и предизвикателствата пред сигурността на функционирането на тази инфраструктура нараснаха неимоверно заради намаляването на основните въглеводородни ресурси върху които е базирана съвременната икономика (нефт и природен газ), нарастващата конкуренция за достъпа до тях, увеличаването на разстоянието между страните, където те се добиват и страните с най-голямо потребление, както и заради компютъризирането на основните процеси при тяхното производство и транспортиране.

Настоящата статия предлага структуриране на новите тенденции в политиката по управление на сигурността на критичната енергийна инфраструктура (КЕИ) в контекста на анализа на новите уязвимости в нейното функциониране.

* * *

В индустриализираните общества енергийната инфраструктура винаги е била обект на специална защита. Причините днес да търсим нови решения в политиката по управление на нейната сигурност е в появата на няколко фактора, действието на всеки от които усилва въздействието на останалите.[1] Първо, глобализацията и съвременната информационна и комуникационна революция промениха кардинално основни характеристики на енергийната инфрастурктура. Глобализацията води до все по-голяма взаимосвързаност и взаимозависимост на системи от основните обществени сектори – икономика, енергетика, информация и комуникации, транспорт и т.н. 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“).[2]

Второ, непрогнозируемостта и неопределеността на средата за сигурност, в която оперира тази система. *Неизвестността* (кой е противникът (напр. Anonymous) и с какво стои срещу нас, какви са неговите цели и способности) и *непредсказуемостта* (на времето, мястото и характера на евентуалната атака), придават нов характер на заплахите и създават усещане за тотална несигурност.

Трето, осъществената през последния четвърт век значителна приватизация и либерализация (дерегулация) в този сектор, която доведе до свиване на ролята на публичните

[1] Вж: П. Дракалиева, И. Иванов, Съвременната концепция за защита на критичната инфраструктура: генезис, цели, методология, проблемни зони, Защита на критичната инфраструктура в ЕС и България - икономически и организационни аспекти (София, 2010): 12-35.

[2] Uwe Nerlich and Frank Umbach, „European Energy Infrastructure Protection: Addressing the Cyber-warfare Threat*”, Journal of Energy Security*, October 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 (31.10.2012).

институции в оперирането с енергийната инфраструктура. Главната последица е в сложните и засега нерешени проблеми около разпределението на ролите и отговорностите на държавата и частния сектор за сигурността на инфраструктурата.

Това са основните фактори, които днес детерминират кардиналното нарастване на уязвимостта на енергийните 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 бе 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 релевантни заплахи.

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

Този анализ се прави на различни нива: от оператора на конкретната инфраструктура, който отговаря за безопасното и непрекъснатото й функциониране и от публичните институции, отговорни за политиките за сигурност на тази инфраструктура като критично важна за нормалното функциониране на обществото.[5]

Кои са основните нови тенденции в политиката за сигурност на функционирането на критичната енергийна инфраструктура и на кои предзвикателства трябва да отговорят?

1. КИБЕРСИГУРНОСТ НА КРИТИЧНАТА ЕНЕРГИЙНА ИНФРАСТРУКТУРА

В съвременната енергийна инфраструктура цифровизацията е необходима за гладкото и ефективното й функциониране. Това обаче повишава уязвимостта на елементите на инфраструктурата към заплахи от киберпространството, особено след като те са станали оперативно по-съвместими, дистанционно достъпни и по-икономични, заради използването на отворените софтуерни стандарти и протоколи за постигане на ефективност на разходите.

Днес кибероръжия срещу енергийна инфраструктура не е само епизод от холивудски филм. Едно от първите използвания на “logic bomb” е през юни 1982 г., когато американски спътник за ранно предупреждение отбелязва грандиозен, наподобяващ ядрен, взрив в Сибир. Най-вероятно това е експлозия на съветски газопровод, причинена от повреда в компютърната система за контрол, която съветски шпиони са откраднали от канадска фирма. Повредата не е случайна, а е заложена от специалисти на ЦРУ в компютърната система със забавен ефект на действие.[6]

---

[3] П. Дракалиева, И. Иванов., стр. 19.

[4] Пак там, стр. 21.

[5] Вж. например Todor Tagarev, Venelin Georgiev and Petya Ivanova, "Analytical Support to Critical Infrastructure Protection Policy and Investment Decision-Making," Information & Security: An International Journal 28, no. 1 (2012): 13-20, http://dx.doi.org/10.11610/isij.2801.

[6] “Cyberwar. War in the fifth domain”, The Economist, July 2010, http://www.economist.com/node/16478792 (31.10.2012).

Три десетилетия по-късно честотата на използване на кибероръжията е нараснала експоненциално: поредица от доклади, изготвени от Правителствената служба за отчетност (GAO) от 2009 г. насам, подчертава нарастващите опасения от кибератака на критичната енергийна инфраструктура в САЩ. В доклад от 24 април 2012, "Cybersecurity Threats Impacting the Nation" се отбелязва, че „през последните шест години броят на инцидентите, докладвани от федералните агенции на федералния център за информационна сигурност при инциденти се е увеличил с близо 680%"[7].

За степента на заплахата, която днес кибератаките представляват по отношение на основните граждански критични инфраструктури алармира министърът на отбраната на САЩ Леон Панета предупреждавайки, че е възможно САЩ да станат обект на "кибернетичен Пърл Харбър", като чуждестранни хакери могат да извадят от строя енергийната, финансовата и транспортната система с „атака, която ще парализира и шокира нацията и ще създаде дълбоко, ново чувство на уязвимост"[8].

Сериозността на тази заплаха се споделя и от експертите в енергийния сектор. Изследване на 200 висши мениджъри по сигурността на критичната инфраструктура на електроснабдителни предпрятия от 14 страни установява: 40% считат, че уязвимостта на този индустриален сектор се е увеличила; според почти 30% тяхната компания не е подготвена за кибератака; повече от 40 на сто очакват голяма кибератака в рамките на следващата година.[9]

McAfee и CSIS (Center for Strategic and International Studies) две поредни години правят представително проучване на ефектите от въздействието на кибератаките върху критичната енергийна инфраструктура. Докладът за 2010 г. „In the Crossfire: Critical Infrastructure in the Age of Cyberwar" констатира липсата на адекватна защита на компютърните мрежи при много от критичните инфраструктури в света и разкрива потресаващите размери на въздействието на кибератаките и на необходимите разходи за възстановяването на тези мрежи.

Информацията от доклада за 2011 г. - "In the Dark: Crucial Industries Confront Cyberattacks," доказва тревожния извод на неговите автори: „че докато нивото на заплаха на тези инфраструктури се е увеличило, нивото на отговор не е."[10] „Само през миналата (2010) година, почти половината от анкетираните са заявили, че никога не са били изправени пред мащабна кибератака „отказ на услуга" (denial of service) или мрежови проникванията. От тази (2011) година, тези числа са се променили: 80% са били изправени пред мащабна атака „отказ на услуга" и при 85% има опити за проникване в мрежата. Стряскащ е факта, че почти две трети съобщават за чести опити (поне веднъж месечно) за проникване на зловреден софтуер, проектиран за саботаж на тяхната система."[11]

Именно използването на зловредни вируси за атака срещу критична енергийна (и друга) ифраструктура качествено промениха киберпространството и поставиха системите за сигурност пред много сириозно ново предизвикателство.

---

7 Alic Jen, "US Gas Pipelines under Cyber Attack", *Says DHS*, 09 May 2012, http://oilprice.com/Energy/Energy-General/US-Gas-Pipelines-under-Cyber-Attack-Says-DHS.htm (30.10.2012).

8 Elisabeth Bumiller and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S.", *The New York Times*, 11 October, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all (13.10.2012).

9 "McAfee and CSIS Report Reveals Dramatic Increase in Cyberattacks and Sabotage on Critical Infrastructure Yet Organizations Remain Unprepared", *McAfee,* 19 April, 2011, http://www.mcafee.com/us/about/news/2011/q2/20110419-01.aspx (31.10.2012).

10 Пак там.

11 "In the Dark.Crucial Industries Confront Cyberattacks", McAfee second annual critical infrastructure protection report.Written with the Center for Strategic and International Studies (CSIS), *McAfee Inc.*, 2011, http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf (02.11.2012).

Stuxnet е първият образец на зловреден вирус/софтуер[12] (разкрит през юни 2010 г.), специално създаден да поразява реални физически инфраструктури, промишлени обекти (управлявани от SCADA[13] системи). 60 % от заразените компютри са в Иран, но вирусът има наистина глобален обхват: от Испания и Русия, до Индия и Индонезия. Към месец април 2011 г., неактивиран, но напълно работоспособен Stuxnet е открит в повече от половината компютърни системи на германски енергийни компании, а също и при тръбопреносните оператори на комуналното разпределение на газ и вода. Аналогична е степента на заразяване с вируса във Франция, Индия и други страни.[14]

Според характеристиките и поставяните цели, Stuxnet е кибероръжие. Неговото разработване доказва, че правителства възнамеряват да развиват злонамерен софтуер, за да саботират противниците си чрез информационно-технологичните системи и критичната инфраструктура. Съществуването на Stuxnet показва също така, че враждебни правителства могат лесно да застрашат SCADA системите, които масово контролират функционирането на системите за електричество, газ, петрол, вода и канализация в една държава, побеждавайки защитата, на която повечето фирми-оператори на тези критични ифраструктури разчитат.[15]

Вторият известен (от този порядък), зловреден вирус е Flame (разкрит през май 2012 г.). Според експерти, той структурно и функционално многократно превъзхожда всички досега известни зловредни програми. Определят Flame като инструмент на кибершпионажа, който събира множество информация от компютрите-жертви (картинки, натиснат клавиш, пароли и информация за местоположение). Най-пострадалите от него страни са Иран, Израел, Судан, Сирия, Ливан, Саудитска Арабия и Египет.

Компютърни специалисти доказват, че и двата вируса са циркулирали няколко години преди някой да ги забележи. Според тях, създаването на толкова съвършени продукти предполага огромни инвестиции и държавна ангажираност в проекта. През юни 2012 г. вестник Washington Post съобщи, че шпионският вирус Flame е разработен от специалисти

---

[12] Зловредният софтуер (Malware) обикновено се използва, за да се откраднат пароли и други данни, или да се отвори "задна врата" към компютър, така че да може да е открит за външни. Такива "зомби" машини могат да бъдат свързани до хиляди, ако не и милиони с други по целия свят и да се създаде “botnet”. Botnets се използват за изпращане на спам, разпространение на зловреден софтуер или за започване на разпределен отказ на услуги - DDoS атаки (при кибератаката в Естония, 2007), които се опитват да блокират целенасочено компютърната мрежа от претоварване с безброй фалшиви молби.

[13] SCADA е вид система за контрол (ICS) в индустриални обекти. SCADA системите предшестват развитието на интернет. Първоначално те са предвидени основно за контролиране на процесите на едно място и не са предназначени да бъдат свързвани към външния свят. Въпреки това, с появата на евтините персонални компютри, подобрените телекомуникации и интернет, отделните индустриални обекти са били свързвани един с друг, а в много случаи и с външния свят чрез интернет. Освен това, либерализацията на енергийния пазар изисква дружествата за производство на енергия непрекъснато да споделят своите данни за производството и резервен капацитет с пазарните оператори и операторите на преносни системи, директно от техните SCADA системи за контрол. *Виж* Bruce Averill and Eric A.M. Luiijf, “Canvassing the Cyber Security Landscape: Why Energy Companies Need to Pay Attention”, *Journal of Energy Security*, 18 May 2010**,** http://www.ensec.org/index.php?view=article&id=243%3Acanvassing-the-cyber-security-landscapewhy-energy-companies-need-to-pay-attention&option=com_content&Itemid=361 (30.10.2012).

[14] Andrei Korneyev, “Security of energy networks in USA: the problems of combating cybernetic terrorism// США - Канада: экономика, политика, культура.” *Scientific article*, (in Russian), No. 7, 2011, 25-46 http://nemchenko.ru/wind.php?ID=642928 (24.10. 2012).

[15] *McAfee Inc.*, 2011 http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf (02.11.2012).

на САЩ и Израел за получаване на информация, която би могла да бъде полезна за проваляне на иранската ядрена програма.[16]

Примиряването със съществуване на зловредни вируси от такъв порядък е изключително опасно, защото те отварят кутията на Пандора[17] и различни страни по света, позовавайки са на прецедентното право, вече могат да твърдят, че е законно да използват зловреден софтуер превантивно срещу индустриални обекти и критична инфраструктура на враговете си. Друга опасност произтича от възможността зловредните вируси, които вече са заразили хиляди компютри (предполага се, че Stuxnet е заразил около 50 000) да бъдат копирани, адаптирани и използвани от хакерски групи, киберпрестъпници и разузнавателни агенции. Клонингите, обаче могат да не са толкова съвършени (точни) като оригинала, което означава, че те биха могли да заразяват и повреждат обекти извън пределите на своите цели (вирус предназначен за канализационната ситема на един град може да увреди управлението на ядрена електроцентрала, например).

Създаването на такъв тип зловредни вируси и атакуването с тях не оставя съмнение за наличието на надпревара във въоръжаването в киберпространството. Може да се допусне, че в информационното пространство „се разхождат“[18] и други такива вируси, чието създаване е спонсорирано от други държави. До разкриването на Stuxnet и Flame даже говоренето за такива оръжия беше недопустимо. Днес те са част от реалността и става очевидно, че тяхното притежаване и развиване ще бъде неотменен елемент от военния капацитет на държавите и една от основните им цели ще са жизнено важни крититични инфраструктури.

Кибероръжието има безспорни „предимства“[19], които се проявяват и когато се използват срещу критичната енергийна инфраструкура. То е ефективно; значително по-евтино от конвенционалното; сложно е да бъде приписано на конкретен нападател; от него е много трудно да се защитиш; репликира се с нулеви загуби; привидната му безобидност намалява прага за прилагането му. По своята разрушителна сила то е сравнимо с ядреното, химическото и биологичното, но за разлика от тях не се контролира по никакъв начин и се смята, че кибероръжието сериозно превъзхожда останалите оръжия за масово поразяване със своята точност, невидимост, всеобхватност, „безобидност“.

Социалните медии, които роди Web 2.0 базирания интернет, също създават нови заплахи за сигурността на КЕИ. Енергийните пазари могат да бъдат манипулирани от слухове (често разпространявани чрез социалните мрежи) за атака, за затваряне на основен тръбопровод за газ/нефт или чрез директна манипулация на цените на спотовите пазари на големи борси за природен газ, като Powernext например. Такива манипулации могат да доведат до неочакван недостиг в електроснабдяването и газопреносните мрежи. За съжа-

---

16 Ellen Nakashima, Greg Miller and Julie Tate, “U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts”, officials say, *The Washington Post*, June 19, 2012, http://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html (22.10. 2012).

17 През август 2012 г., обект на кибератака е държавната компания Saudi Aramco, заразени са повече от 30 000 компютъра. Виж „Нов кибервирус Shamoon атакува компютри в енергийната индустрия”, *Дневник*, 19 август 2012, http://www.dnevnik.bg/sviat/2012/08/19/1890737_nov_kibervirus_shamoon_atakuva_kompjutri_v_energiinata/ (26.10.2012).

18 Експертите периодично разкриват нови образци на зловреден софтуер: Dugu (10.2011); Gauss (08.2012).

19 Eugene Kaspersky, **“**Flame, который изменил мир”, *Nota Bene*, June 14, 2012, http://eugene.kaspersky.ru/2012/06/14/flame-that-changed-the-world/ (26.10.2012).

ление, това не е просто теоретичен проблем: за 2010 година загубите от престъпни манипулации на пазара на въглеродни емисии се оценява на над 5 милиарда евро.[20]

Сериозно предизвикателство пред киберсигурността е и все по-широкото прилагане на технологията „интелигентна мрежа“ (smart grid technology), която е критичен компонент за енергийните системи на 21-ви век. Интелигентните мрежи използват цифрова технология за пестене на енергия, снижаване на разходите, намаляване на емисиите и повишаване на надеждността на системата. За съжаление обаче, нарастването на цифровата свързаност на мрежите, увеличава броя на потенциалните уязвимости[21].

Посочените примери и многобройните съобщения за кибератаки срещу обекти и елементи на енергийната инфраструкура правят *ключов въпроса за реакцията на държавата* и *за умението ѝ да изгражда защитна стена срещу проникване* (независимо дали е с политически или с криминални мотиви). Това е сериозно предизвикателство, защото е изключително сложно да се определи кой в последна сметка е поръчителя на кибератаката – държава, организация или личност. Заразените с вирус машини, реализиращи нападението, могат да се намират на територията на трета или на много други страни (има твърдения, че атаката в Естония е била от IP-адреси в 78 държави по света, включително редица западноевропейски). Използването на компютри „зомби“ при кибератака прави невъзможно посочването на клавиатурата, от която е дадена командата, да не говорим за снемане на отпечатъци от пръстите, натиснали клавишите. Според експерти, главните тенденции при кибератаките са две: засилване ролята на недържавните участници и превръщането на Африка в основна база на атакуващите, главно защото там практически не действат международните правила за регулиране на интернет – сървърите.

В този нов контекст, управлението на сигурността на критичната енергийна инфраструктура се нуждае от принципно преосмисляне на подходите за гарантиране информационнната сигурност на отделните елементи от енергийната система. Експертите посочват като задължителни условия: пълната им изолация от Интернет; смяна на неадекватните на нови предизвикателства, остарели индустриални системи за управление; въвеждане на ешалонирана, многостепенна система за защита от киберзаплахите.

Тези, вече азбучни истини, са известни и общоприети и от експерти, и от оператори на енергийната инфраструктура, и от политици, занимаващи се с управление при кризи. Въпреки това, те си остават пожелателни или са реализирани в много ниска степен, както се вижда в цитирания по-горе доклад на McAfee и CSIS. Причината – проблемите и сложните отношения между държавата и частните собственици и оператори на критична енергийна инфраструктура. Намирането на ефективните формули на тези отношения е втората нова тенденция в политиката за защита на КЕИ.

---

[20] Bruce Averill and Eric A.M. Luiijf, “Canvassing the Cyber Security Landscape: Why Energy Companies Need to Pay Attention”, *Journal of Energy Security*, 18 may 2010, http://www.ensec.org/index.php?view=article&id=243%3Acanvassing-the-cyber-security-landscapewhy-energy-companies-need-to-pay-attention&option=com_content&Itemid=361 (02.11.2012).

[21] Пак там.

2. ПУБЛИЧНО-ЧАСТНО ПАРТНЬОРСТВО ВЪВ ФОРМИРАНЕТО И РЕАЛИЗИРАНЕТО НА ПОЛИТИКАТА ЗА СИГУРНОСТ НА КРИТИЧНАТА ЕНЕРГИЙНА ИНФРАСТРУКТУРА

Високият процент частни собственици и оператори на енергийна инфраструктура е факт, или доминираща тенценция за преобладаващия брой индустриални държави (за САЩ - над 80%[22], за Германия – 90%[23]). Основните проблеми на отношенията между тях и държавата са свързани с разпределението на отговорностите, споделянето на информация и финансиране повишаването на сигурността на функциониране на инфраструктурата.

Традиционно, разпределението на отговорностите по безпроблемното функциониране на енергийната инфраструктура е по правилото: за безопасността (*safety*) отговаря операторът, за сигурността (*security*) – държавата. Днес обаче, в контекста на новите заплахи (главно киберзаплахи) това правило на двулентово разделение не може да бъде ефективно. Работещата формула задължително предполага *консенсус между частния и публичния сектор*, което означава *споделяне на ценности, правила и политики* на всички основни нива на защита на енергийната инфраструктура.

Частният сектор трябва да участва в споделянето на информация за новите рискове и заплахи, да поема своите отговорности за непрекъснатостта на производството и доставките на услуги в енергийния сектор, да инвестира в нови системи за управление и контрол, адекватни на новите нива на заплахи от киберпространството, да участва на всички етапи във формулирането на националната политика за сигурност на КЕИ и реакциите при кризи.

Публичният сектор има своята част от отговорности, които нарастват и стават все по-многообразни в новата среда за сигурност.

През 2010 г. САЩ демонстрираха една възможна държавна реакция на нарастващите киберзаплахи, като *обявиха киберпространството за пета отбранителна сфера* наред със земя, въздух, вода, космос. Обама нарече цифровата инфраструктура на страната „стратегически национален актив“ и създаде отделно киберкомандване.[24] Неотдавна, Секретарят по отбраната Леон Панета заяви, че е необходимо да се повиши нивото на обществен дебат за развиване капацитета на Министерството на отбраната не само да се защитава, но също така да извършва нападения над компютърни мрежи.[25] Политики за киберсигурност развиват и Великобритания, Русия, Израел, Северна Корея, Иран. Официално киберармии имат САЩ, Китай, Англия, Франция, Германия.

Днес, когато става дума за кибератаки, най-често се споменава новата „ос на злото“: Китай – Русия - КНДР, от която произтичат преобладаващите кибератаки върху информационнната структура на САЩ и неговите съюзници. Най-многочислените обвинения са към Китай. В действителност, през последните пет години в страната се акцентира върху подготовката на кадри и нарастването на капацитета по активна защита на киберпространството. През 2011 г. официално е обявено създаването в Народно-освободителната армия на „сини интернет-войски“. Като се има пред вид традиционната закритост на информацията за въоръжените сили, това признание е доказателство за невъзможността да се скрият мащабите на тази дейност. Според открити източници (доктрини) към 2020 година китайска-

---

22 “Energy Sector: Critical Infrastructure”, Sector Overview, *Homeland Security*, 2012, http://www.dhs.gov/energy-sector (03.11.2012).

23 П. Дракалиева, , И.Иванов, стр. 31.

24 “Cyberwar.War in the fifth domain”, *The Economist*, Luly 2010, http://www.economist.com/node/16478792 (26.10.2012).

25 Elisabeth Bumiller and Thom Shanker, “Panetta Warns of Dire Threat of Cyberattack on U.S.”, *The New York Times*, 11 October, 2012, http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all (01.11.2011).

та армия трябва да бъде с най-голям капацитет в киберпространството.[26] Към „лошите“ в киберпространството напоследък са присъединявани също Иран и Украйна.

Нарастването значимостта на сигурността на енергийната критична инфраструктура и на публично-частното парньорство за нейното гарантиране намира израз и в започналото създаване на *специализирани администрации* по този проблем.

Азербайджан и Грузия имат специални отдели за сигурност, структури в рамките на техните национални администрации, създадени за защита на енергийната инфраструктура и съоръжения: „Специална служба за държавна защита“ (Special State Protection Service - SSPS) в Азербайджан и „Стратегически отдел за защита на тръбопроводите“ (Strategic Pipeline Protection Department - SPPD) в Грузия.

В Австралия е създадена „Мрежа на доверието за обмен на информация за издържливост на критичната инфраструктура“ (Trusted Information Sharing Network for Critical Infrastructure Resilience – TISN). Тя осигурява среда, в която бизнесът и правителството могат да споделят важна информация по въпросите на сигурността, отнасящи се до защитата на критичната инфраструктура и непрекъсваемостта на основните услуги пред лицето на всички опасности.[27]

В Турция, заради превръщането ѝ в хъб на Южния енергиен коридор и изключителните отговорности по защита на международните енергийни трасета през нейната територия, експерти предлагат създаването на нова институционална/организационна единица в Министерството на енергетиката и природните ресурси (като е в САЩ) или в рамките на въоръжените сили, която да се занимава специално със сигурността на енергийната инфраструктура.[28]

В САЩ, през септември 2012 г., във Федералната комисия за енергийно регулиране (Federal Energy Regulatory Commission - FERC) е създаден „Отдел по сигурността на енергийната инфраструктура“ (Office of Energy Infrastructure Security - OEIS). В мотивите за институционализирането му се казва, че Федералната комисия за енергийно регулиране (FERC) създава нова служба за справяне с кибер и физическите рискове за сигурност на съоръженията, които са отговорност на FERC: електрически съоръжения за производство и пренос, тръбопроводи за нефт и природен газ и терминалите за втечнен природен газ.[29]

Една от най-важните задачи на новата държавна структура е да съдейства за преодоляването на пропастта между частната индустрия и федерални правителствени агенции, чрез:[30]

- координация и сътрудничество между съответните федерални и държавни агенции и представителите на промишлеността по въпроси на физическата и кибернетична-

---

[26] Андрей Новацкий, “Кибербезопасность: новые угрозы, новые возможности”, *Фонд Стратегической Культуры,* 23.03.2012, http://www.fondsk.ru/news/2012/03/23/kiberbezopasnost-novye-ugrozy-novye-vozmozhnosti.html (26.10.2012).

[27] “Critical energy infrastructure protection and resilience”, *Australian Government*, 17 April 2012, http://www.ret.gov.au/energy/energy_security/critical_infrastructure_protection_and_resilience/Pages/CriticalInfrastructureProtectionandResilience.aspx (26.10.2012).

[28] Hasan Alsancak, “The Role of Turkey in Global Energy: Bolstering Energy Infrastructure Security”, *Journal of Energy Security* 18 May 2010, http://www.ensec.org/index.php?option=com_content&view=article&id=247:the-role-of-turkey-in-the-global-energy-bolstering-energy-infrastructure-security&catid=106:energysecuritycontent0510&Itemid=361 (20.10.2012).

[29] “FERC Launches New Cybersecurity Office”, *Sutherland Asbill & Brennan LLP*, 21 September, 2012, http://www.sutherland.com/files/upload/FERCLaunchesNewCybersecurityOffice.pdf (02.11.2012).

[30] “New FERC Office to Focus on Cyber Security”, *Security Magazine,* 26 September, 2012, http://www.securitymagazine.com/articles/83526-new-ferc-office-to-focus-on-cyber-security (02.11.2012).

та сигурност, както и съвместното им участие в конференции, семинари и класифицирани брифинги по проблемите на енергийната инфраструктура;

- направляване на съвместната работа с частния сектор, собствениците, ползвателите и операторите на системи за доставка на енергия, по идентифициране, комуникация и снижаване на риска от физически и киберзаплахи към енергийните съоръжения под юрисдикцията на FERC.

Доказателство за това, колко наистина сложно е да се постигне ефективно, консенсусно публично-частно партньорство в защитата на КЕИ, дори при споделено рабиране за високата степен и нетрадиционност на заплахите[31], е отхвърлянето през август 2012 г. на законопроекта за киберсигурност (Cybersecurity Act of 2012) в американския Сенат. Целта на законопроекта е да подобри сигурността и издръжливостта на кибернетичното пространство и комуникационната инфраструктура на САЩ, чрез налагане на минимални стандарти за сигурност на компютърните системи, работещи в критична инфраструктура. Въпреки че законопроектът предвижда държавен надзор изцяло на доброволен принцип, бизнес лобито категорично се противопоставя на тази идея. Неговите основни контрааргументи са два: 1) на бизнеса несправедливо се налагат високи разходи и 2) частният сектор може сам да се справи с проблема, държавната регулация само ще пречи.[32]

Дебатът дали и колко държавата трябва да се намесва в предотвратяването на киберзаплахите, има много широка основа. Сериозни аргументи и немалобройни привърженици, главно киберексперти, стоят зад тезата, че намесата на държавата ще доведе до силно милитаризиране на киберпространството. Експертите са тези, които в своята общност могат да споделят и решават проблемите с киберзаплахите. Обратната теза е, че проблемът (киберсигурност) вече е толкова мащабен и с такъв ефект върху националната и глобална сигурност, че никой няма право да играе на това поле „игри на късмета“.

Публично-частното партньорство в защитата на КЕИ няма само национални измерения. Пример за сътрудничество между военния, невоенния и частния сектор за постигане на общите стратегически цели е Caspian Guard, инициатива на Програмата за регионална сигурност на Департамента за отбрана на САЩ. Идеята е чрез регионални мултинационални усилия, заедно с местни военни и невоенни агенции от страната домакин и с усилията на частните енергийни фирми, работещи в страните с излаз на Каспийско море, да се създаде интегриран режим за граничен контрол на въздушното и морското пространство.[33] Програмата предвижда да координира дейностите в Азербайджан и Казахстан с тези на Централното командване на САЩ и на други американски правителствени агенции за подобряване сигурността в региона на Каспийско море. Основната цел е колективна защита на взривно нарастващата енергийна инфраструктура в региона на Каспийско море.

Друг пример за публично-частно партньорство е създадената от американското правителство през 2006 г. „Глобална стратегия за сигурност на критичната енергийна инфраструктура“ (Global Critical Energy Infrastructure Protection - GCEIP). Тази стратегия е насочена към страни-донори на енергийни ресурси с повишен риск от терористични заплахи. Дори класическите терористични атаки на инфраструктурни обекти, нарушаващи физическите им параметри, са с много висока ефективност. Например, "Една неголяма атака срещу петролопровод в югоизточната част на Ирак, за която са вложени около $ 2 000, струва на

[31] According the National Security Agency's Gen. Keith Alexander cyber attacks against infrastructure are up 1,700% since 2009, виж Dave Aitel, “The Cybersecurity Act of 2012: Are We Smarter Than a Fifth Grader?”, *Huff Post Tech*, 08 March, 2012, http://www.huffingtonpost.com/dave-aitel/the-cybersecurity-act-of-_b_1737129.html (03.11.2012).

[32] Dave Aitel, “The Cybersecurity Act of 2012: Are We Smarter Than a Fifth Grader?”, *Huff Post Tech*, 08 March, 2012, http://www.huffingtonpost.com/dave-aitel/the-cybersecurity-act-of-_b_1737129.html (02.11.2012)

[33] “Military: Caspian Guard”, *GlobalSecurity.org,* 5 July 2011, http://www.globalsecurity.org/military/ops/ caspian-guard.htm (07.12.2012).

иракското правителство повече от $ 500 млн. загубени приходи от петрол. Това е връщане на инвестициите на 25 000 000%".[34]

Стратегията може да бъде потенциален модел за развитие на публично-частни партньорства и цели да запълни празнината между частните и обществените сили за сигурност при защитата на енергийни обекти, които си остават привлекателна цел за атака в редица страни.

Тази стратегия[35] е базирана на междуправителствено сътрудничество, целящо да се окуражават усилията на страната домакин на критична енергийна инфраструктура да подобрява взаимодействието си с местните оператори. Американското правителство участва с техническа помощ и съвети и така увеличава гаранциите, че направените разходи и усилия действително ще доведат до подобряване на сигурността на инфраструктурата. Основният аргумент за това сътрудничество е, че нито страната домакин, нито САЩ имат интерес евентуално крупни енергийни съоръжения да не работят за продължителен период от време. Инвестирането от правителството-домакин на една малка част от приходите от енергийни ресурси в подобряване сигурността на инфраструктурата е действителна застрахователна полица за минимизиране на риска от загуби. Като правило, местното правителство нарежда на оператора на съоръжението да отговаря за физическите подобрения на охраната и сигурността в рамките на периметъра на неговата дейност, докато правителството на приемащата страна е отговорно за сигурността извън периметъра, включително ако се налага и чрез въоръжени сили, които да осигуряват защита.

Големите потребители на енергийни ресурси – САЩ, ЕС, могат и трябва да инвестират и да споделят отговорностите за сигурността на КЕИ в рискови страни-донори (Ирак, Либия), разбира се, ако има правителство готово за кооперирание. Моделът GCEIP е възможно решение.

Съвременната енергийна сигурност и критичната енергийна инфраструктура са интернационални понятия, което предпоставя и третата основна тенденция в защитата на КЕИ.

3. МЕЖДУНАРОДНО СЪТРУДНИЧЕСТВО В ПОЛИТИКАТА ЗА СИГУРНОСТ НА КРИТИЧНАТА ЕНЕРГИЙНА ИНФРАСТРУКТУРА

Днес енергийната сигурност е състояние на сложна взаимозависимост и взаимообвързаност. Сигурността на всяка една страна – донор, транзитна или потребител на енергийни ресурси, пряко зависи от сигурността на функционирането на енергийния сектор във всички останали по енергийното трасе. В този смисъл, енергийната инфраструктура все повече се превръща в многонационална мрежа, сигурноста на функционирането на която е равна на уязвимостта на най-слабото звено.

Интернационализирането на енергийните инфраструктури закономерно води до интернационализиране на тяхната защита в различни формати.

Европейският съюз предлага един такъв формат. От 2004 г., се работи за общ европейски подход при защита на енергийната инфраструктура, така както е определено в Европейската програма за защита на критичната инфраструктура. Общата политика на

[34] Bruce Averill, “Using Public-Private Partnerships to Improve International Energy Infrastructure Security”, *Ensec.org*, 27 October 2009, http://www.ensec.org/index.php?view=article&catid=100%3_Aissuecontent&id=217%3Aqusing-public-private-partnershipsq-to-improve-international-energy-infrastructure-security&tmpl=component&print=1&page=&option=com_content&Itemid=352 (30.10.2012).

[35] Пак там.

съюза цели ефективен отговор на новите предизвикателства пред сигурността на КЕИ, към които се прибавя и високата степен на взаимообвързаност и взаимозависимост на европейските енергийни мрежи, която в контекста на директивите за свързване и на газовите трасета, ще нарасне още повече.

Ключовите задачи[36] са:

- Създаване на правни инструменти за прилагане на Европейската програма за защита на критичните инфраструктури със секторно измерение.
- Идентификация на европейските критични инфраструктури в различни сектори на енергетиката: нефт, газ, електричество.
- Препоръки и техническа помощ на държавите-членки.
- Проследяване на националните програми, отнасящи се до критични инфраструктури.
- Насърчаване на мрежи между ЕС, държавите-членки, технологичните компании за сигурност, собствениците и операторите на енергийна инфраструктура.
- Координация със съответните международни организации.

Първото сериозно постижение в изпълнението на ключовите задачи е изготвянето на Директива 2008/114/ЕС от 08.12.2008 г. относно установяването и означаването на европейските критични инфраструктури и оценка на необходимостта от подобряване на тяхната защита. През 2010 г. Генерална дирекция „Енергетика“ на Европейската комисия създава мрежа (Network TNCEIP) на операторите на критични енергийни инфраструктури от секторите електроенергия, газ и петрол, за да обменят опит по въпроси, свързани със сигурността. Мрежата е отворена за членство на европейските компании, операторите на енергийни съоръжения и инфраструктури. На тримесечни срещи те могат да обсъждат важни за сигурността на енергийната инфраструктура теми като "Оценка на заплахата", "Управление на риска", "Киберсигурност", и др.

Както и при други общи политики в ЕС обаче, и тук има повече декларативност, отколкото ефективност. Това е особено тревожно на фона на нарастващите заплахи от кибератаки.

НАТО е друг международен формат, който предлага политики за сигурност и участие в гарантирането на защитата на КЕИ.

Включването на НАТО в политиката за гарантиране на енергийната сигурност (главно чрез защита на КЕИ) беше и е съпътствано от сериозни дебати. Първият от тях произтича от обстоятелството, че енергийната сигурност често се определя като приоритет и изключителна отговорност на националната политика. Доказателство в тази посока е ниската ефективност на общата енергийна политика на ЕС, фактът, че страни като Германия, Италия, Франция поставят на преден план националните си енергийни интереси пред тези на общността - по отношение на политиката спрямо Газпром, например. От друга страна, държави като Белгия, с нейните 5 % зависимост, не споделят тревогата на балтийските държави, които са 100 % зависими от вноса на руски природен газ.

Вторият дебат е за това, дали военнополитическа организация трябва да навлиза в сфера, в която решенията са предимно политически. Досегашният опит показва, че НАТО успешно се справя с военни проблеми, но когато е необходимо да се вземат политически решения, механизмът не е толкова ефективен. Заради разнопосочните интереси, хармонизирането на позициите между съюзническите държави по енергийната сигурност може да се окаже трудна битка.

[36] “Energy Infrastructure. Critical Infrastructure Protection”, *European Commission*, 2012 http://ec.europa.eu/energy/infrastructure/critical_en.htm (03.11.2012).

На трето място, страните-членки участват в редица международни организации, които вече имат ангажименти и отговорности за енергийната сигурност, като се започне от ЕС, Международната агенция по енергетика, МААЕ и се завърши с ОССЕ. Усилията на НАТО да поеме допълнителни отговорности, често се разглеждат от тези организации като опит за изземване на техни функции и роли.

И на четвърто, но много важно място е дебатът, свързан с опасението, че по-активна роля на НАТО може да доведе до милитаризиране на политиката за енергийна сигурност в глобален мащаб.

Опасенията са, че ако Алиансът разшири програмата си в полето на енергийната сигурност, ще даде аргументи на други играчи открито да милитаризират и допълнително да политизират отношенията в областта на енергетиката, да ги обвържат с по-широки стратегически въпроси. Също така, тъй като повечето страни-членки на НАТО са и членки на ЕС, това би могло да делегитимира усилията на съюза за налагане на маркетизиран, основан на правила, интегриран европейски енергиен пазар. Не трябва да се забравя и Русия, която е не само ключов производител и доставчик на енергия, но и голяма военна сила. Нейната подкрепа за редица жизнено важни резолюции и действия на страните-членки на НАТО, отнасящи се до конфликтни райони в света, не трябва да бъде рискувана. Възможно е и легитимирано (с аргумента НАТО) прилагане на военни инструменти за разрешаване на конкурентни и конфликтни междудържавни интереси в регионите на добив и транспортиране на енергийни ресурси.

Всичко това показава, че някои от притесненията от повишената активност на НАТО по въпросите на енергийната сигурност могат да бъдат добре обосновани. Ето защо, при изработването на параметрите на ангажиментите и отговорностите, страните-членки максимално отчитат тези аргументи и разписват приоритетите на задачите на Алианса така, че той да допринася както за енергийната, така и за глобалната сигурност, а не да създава прецеденти и поводи за конфликти.

В Декларацията от срещата на върха в Букурещ (април 2008 г.) [37] за първи път се разписват параметрите на ангажиментите на НАТО в полето на енергийната сигурност. НАТО фиксира участие в следните области: споделяне на информация и разузнавателни данни, разпространяване на стабилност, развитие на международното и регионалното сътрудничество, управление на последиците, както и преди всичко *подкрепа на защитата на критичната енергийна инфраструктура*. Подчертано е, че усилията на НАТО ще добавят стойност и ще са напълно координирани и вградени в тези на международната общност, която разполага с редица организации специализирани в областта на енергийната сигурност.

Темата за киберсигурността е основна на срещата на върха в Букурещ през 2008 г. Като виден международен военен съюз НАТО смята, че притежава достатъчна легитимност за да започне да артикулира глобална визия за конституционния ред в кибернетичното пространство.[38] Новата стратегическа концепция на НАТО разглежда киберзаплахите като възможни основни заплахи за страните членки.[39]

След срещата на върха в Чикаго, НАТО продължава да развива капацитет по отразяване и на двете нови предизвикателства – енергийната сигурност и киберсигурността. На полето на защитата на критична енергийна инфраструктура те се срещат и наслагват.

---

[37] "Bucharest Summit Declaration" *meeting of the North Atlantic Council in Bucharest* on 3 April 2008, http://www.nato.int/cps/en/natolive/official_texts8443.htm

[38] Rex B. Hughes, "NATO and CyberDefence- Mission Accomplished?", no. 1 (April 2009), http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf

[39] Defending against cyber attacks, NATO, 2012, http://www.nato.int/cps/en/natolive/topics49193.htm (27.102012).

Международното сътрудничество в политиката за киберсигурност на КЕИ среща засега непреодолимо препятствие - отсъствието на общоприета международна конвенция за сигурност в кибернетичното пространство.

Отсъстват споделени договорености по правилата за разработване, разпространение и използване на кибероръжия. В правния вакуум, водещ до липса на механизми и процедури за споделяне на критична информация, за координация и съвместно противодействие, става много реална ситуацията, при която особено опасен зловреден вирус, може да атакува обекти на критичната енергийна инфраструктура, което да провокира регионална/глобална социално-икономическа/екологична катастрофа.

Всички релевантни участници в киберпространството изразяват убеденост в неотложното изработване на международно-правен документ регулиращ тази сфера, гарантиращ сигурност и ефективно противодействие на кибертероризма, киберпрестъпноста и недопускане на кибервойна. Позициите на основните играчи засега обаче, са принципно трудно съвместими. Това е тревожен факт, защото „мрежата“ всъщност е една и сигурността в нея е възможна само като споделена сигурност.

В тази ситуация, в която не само, че няма общо разбиране за правилата в киберпространството, но даже няма международна система за оповестяване на кризисни събития, свързани със сигурността на КЕИ, Обединеното кралство предлага възможна прагматична политика. То активно работи за *сключване на двустранни договори/споразумения за кризисни комуникации* между държави, които най-често са обект на кибератаки. През 2012 г. Великобритания развива такава двустранна политика с Китай и Русия. Идеята е, в случай на криза, предизвикана от зловредни действия в киберсферата, държавите да споделят информация *по механизма, по който това се прави в областта на контрола на въоръженията*.[40]

* * *

Съвременното разбиране за ефективна политика за сигурност на КЕИ поставя акцента върху способността да се систематизират уязвимостите, да се предвиждат заплахите и да се неутрализират рисковете от кибератаки върху елементи на сложно взаимообвързаните, интелигентни енергийни инфраструктури. Тези задачи изглеждат нерешими в контекста на отсъствието не само на общоприети правила за киберсигурност, но и на консесус по съдържанието на основните понятия. Всички значими участници на енергийните пазари осъзнават рисковете и отговорностите си за сигурността на енергийната инфраструктура в епохата на тоталната зависимост от информациннните и комуникационни технологии, която поражда и изключително високата уязвимост на тази критична инфраструктура.

Новите тенденци в политиките за сигурност на КЕИ – киберсигурност, публично-частно-партньорство и международно сътрудничество, създават нови възможности за ефективност на нейната защита. Дали те ще станат реалност, зависи от осъзнаването на необходимостта от споделени усилия на оператори и собственици на енергийна инфраструктура, на националните и международни публични институции.

[40] James Blitz, “UK seeks deals to counter cyber attacks”, *Financial Times*, 2 October, 2012, http://www.ft.com/intl/cms/s/0/c1296d92-0cb1-11e2-a73c-00144feabdc0.html#axzz29Hf1X4xR (27.10.2012).