Киберсигурността в енергийния сектор – в търсене на решения

Елизабет Йонева*

Резюме: Обект на статията се явява енергийният сектор, а специфичният предмет е киберсигурността като негово изключително релевантно измерение в съвременната епоха, кореспондиращо и с едно от най-модерните направления на изследване в рамките на проблематиката. През последното десетилетие темата за негативните аспекти на използването на информационните и комуникационните технологии привлича все по-сериозно внимание на глобално ниво с оглед на мащабното разрушително въздействие на кибератаките. Те генерират своите преливащи ефекти и към плоскостта на енергетиката. С оглед на тези тенденции целта на изследването е да се разгледат предизвикателствата по линия на адаптирането и на енергийния сектор към новите реалности. Представени са основните вектори на енергийната киберсигурност с акцент върху заплахите за критичната инфраструктура. Авторът дискутира различни аспекти на планираните и реализирани мерки за оптимизиране на механизмите за противодействие на енергийните кибератаки през перспективата на еволюцията в последните години. Очертана е концептуалната рамка на усилията и на ниво национални политики за справяне с компликациите, породени от тези нови видове заплахи.

Ключови думи: киберсигурност, енергиен сектор, енергийна сигурност, информационни и комуникационни технологии, SCADA.

JEL: F52, O13, O33, Q40.

1. Увод

В съвременните условия енергийната индустрия се изправя пред кардинално нови предизвикателства както с оглед на сътресенията и трансформациите, на които бяха подложени световните пазари през последните години, така и поради компликациите, генерирани в хода на адаптирането на сектора към възможностите и рисковете, породени в резултат на навлизането в дигиталната ера. Имайки предвид, че всяка стъпка в съвременното производство и начин на живот е обвързана по пряк или индиректен начин с енергията, то нейната роля е от колосално значение по отношение на подпомагането на промишлените и търговските процеси, транспорта, комуникациите и др. Достъпът до енергийни ресурси е определящ за социално-икономическото развитие на всяка страна и за жизнения стандарт на населението. Тенденциите в развитието на световната енергетика безспорно връщат днес тази проблематика във фокуса на политическите и обществе-

* Елизабет Йонева е доктор, главен асистент в катедра „Международни отношения“, УНСС, e-mail: yoneva@unwe.bg

ните дискусии. Енергийните въпроси и особено техните модерни аспекти, кореспондиращи със заплахите в сферата на киберсигурността, все повече излизат на преден план в глобалния дневен ред.

Насочвайки се към историческата перспектива, не можем да не забележим незаслуженото игнориране на енергийната тематика в изследователски план за дълги периоди от време. Възходите и спадовете в интереса към енергетиката се предизвикват в течение на XX в. от редица промени в световната икономика, непосредствено свързани с енергийните фактори. Петролните кризи от 70-те години провокират вълна от сериозни изследвания по отношение на рисковете за икономическия растеж и благосъстояние с оглед на евентуален дефицит на енергийни и други ресурси. Академичният интерес към тематиката през 80-те години се определя от инцидентите в областта на ядрената енергетика. Повишеното публично внимание към проблемите, породени от замърсяването на околната среда и по-специално към глобалното затопляне и климатичните промени, предизвиква от своя страна втората голяма вълна в енергийните изследвания в началото на 90-те години. Първото десетилетие на XXI в. пък премина под знака на пиковите концепции за енергийните ресурси, като все повече започнаха да се представят песимистични сценарии в посока на предстоящо изчерпване на ограничените въглеводородни суровини и приближаващ край на ерата на изкопаемите горива. С оглед на актуалните научни тенденции спокойно можем да определим второто десетилетие на настоящия век като такова, което ще бъде белязано от предизвикателствата пред енергийната киберсигурност.

2. Концептуализиране на енергийната сигурност

Киберзаплахите по отношение на този стратегически сектор са неотделима част от по-пространната тема за енергийната сигурност. Несъмнено на фона на осъществените трансформации на световната енергийна карта през изминалите години, извеждането на преден план на въпросите за осигуряването на доставките и за минимизирането на политическите, икономическите и технологичните рискове при обезпечаването на ценните суровини изглежда напълно естествено. С оглед на това релевантната проблематика на енергийната сигурност привлича все по-сериозно внимание на международно равнище и генерира нови импулси за разгръщането на по-пространен дебат, неотменима част от който е посветен на измеренията, свързани с използването на информационните и комуникационните технологии.

Днес концепцията за енергийна сигурност се отличава с пълното единодушие за важността ѝ, но и с липсата на консенсус за нейната същност и съдържание. Налице са десетки определения в теоретичен план по отношение на термина. Енергийната сигурност се счита за стратегически въпрос най-вече за големите потребители, като техният интерес е насочен естествено към обезпечаването на доставките по отношение на вноса. Тя се свързва с наличието на комбинация от необходими условия за дадена държава, при които тя да осигури своето енергийно снабдяване по начин, който да позволи постигането на стабилно и хармонично социално-икономическо и политическо развитие на обществото, както и посрещането на настоящи и бъдещи нужди от качествена и достъпна енергия. Наред с това тя кореспондира с възможностите за опериране на енергийния сектор в критични ситуации, както и със способността на държавата да се справи с налични или потенциални заплахи, произтичащи от негативното въздействие на вътрешни и външни фактори върху него.

Визията за естеството на енергийната сигурност преминава през поредица от

трансформации, като първоначално възниква от опасенията за физическите рискове пред снабдяването, свързани с транспортните и инфраструктурните съображения. Впоследствие обаче тя започва да се фокусира преимуществено върху икономическите условия, които въздействат върху доставките. Понастоящем все по-сериозно внимание започва да се обръща и на политическите фактори в посока на използването на енергийните ресурси като инструмент за натиск върху вносителите от една страна, както и на заплахите, които поражда нестабилният политически климат в страните-износителки – от друга. Така факторите, които могат да генерират заплахи за енергийната сигурност, обхващат вече широк спектър, в който се включват, например, политически интервенции, санкции, инвазии, терористични атаки, саботажи, технически сривове, липса на инвестиции (по отношение на проучване, добив и рафиниране), инфраструктурна недостатъчност, икономически проблеми, природни бедствия и др.

3. Кибератаките и енергийната индустрия

Анализирайки темата за енергийните измерения на предизвикателствата пред сигурността, наред с по-традиционните заплахи като тероризма, се появяват и нови такива, сред които изпъкват кибератаките. Динамичното развитие на информационните и комуникационните технологии през последните десетилетия произвежда както положителни, така и отрицателни ефекти за редица индустрии. От една страна, технологичната революция и взаимосвързаността спомагат за повишаване на ефективността, намаляване на разходите за опериране и поддръжка и позволяват изпълнение на комплексен набор от действия и взаимодействия (Sklar, 2013). От друга страна, те провокират възможности за осъществяване на нов вид престъпления. Кибертероризмът и кибервойните постепенно извървяват пътя от научната фантастика до реалните феномени.

Зачестяващите новини за кибератаки срещу системите на Google, Yahoo и др., срещу социални мрежи (например Фейсбук през август 2009 г. или Twitter през август и декември 2009 г.), както и срещу правителствени страници (например в Естония през април 2007 г., в Грузия през август 2008 г. и в САЩ през юли 2009 г.), все по-убедително свидетелстват за нарастващите умения на хакерите по отношение на проникването в добре защитени сайтове. Разгръщащият се кибершпионаж има значителен икономически ефект. Според изчисленията кражбата на дигитална информация струва стотици милиарди долари на година на американските компании.

Далеч по-опасни обаче се явяват кибератаките над критичната инфраструктура, която е от значение за националната сигурност. Интегралната роля на енергийната индустрия в дебата за новите заплахи е безспорна с оглед на колосалните ефекти, които могат да бъдат произведени от засягане на електрическата мрежа, петролопроводите и газопроводите, и други инфраструктурни компоненти като електроцентрали, рафинерии и др. Активността в това отношение е видна по линия на проект на Deutsche Telekom от 2013 г., позволяващ изготвянето на карта, показваща в реално време броя на кибератаките срещу ключови системи в световен мащаб. Той възлиза на около половин дузина или повече опити на всяка секунда.

Един от емблематичните примери за кибератаки над компютърните системи на енергийни компании е саудитската Aramco. През август 2012 г. 30 000 компютъра от мрежата на компанията са засегнати от зловреден софтуер, обозначен впоследствие от анализаторите с названието “Shamoon”. Несъмнено евентуален успех на атаката щеше да има катастрофични последици, ако

бе причинил срив на производството, който от своя страна би генерирал значително увеличаване на цените на суровия петрол.

Като най-парализираща обаче бива отчитана потенциална атака върху електроенергийната система. Експертите описват следната бедствена картина: „Светът, какъвто го познаваме, ще спре да съществува, когато се прекъсне електричеството; няма да може да се изпомпва бензин, климатичните и всички останали домакински уреди няма да могат да се използват, потапяйки ни в тъмната ера без наличие на нейните оръдия – свещите, дървата за огрев, конете и каруците“ (King, 2012). Доказателство за уязвимостта на електрическата мрежа се явяват мащабните прекъсвания на енергоснабдяването в североизточната част на САЩ и в Западна Европа в края на лятото и началото на пролетта на 2003 г., демонстриращи възможността за лавинообразен срив заради проблеми с хардуера или софтуера на контролните системи. Разследвания за серията от смущения в електрическата мрежа на Бразилия през 2005, 2007 и 2009 г. също насочват към идеята за киберпрестъпления. Докладите за специфичните инциденти, дължащи се на кибератаки, регистрират редица успешни опити, при които хакери проникват в критични надзорни системи в мрежите на Австралия, Европа и САЩ. При по-смущаващите примери се стига дори до изключване на електроцентрали заради киберсривове.

Същевременно тези действия далеч не се оказват някакъв рядък феномен. Осъществено през 2008 г. проучване сред висшия мениджмънт и мрежовите инженери и администратори в различни индустрии, показва, че над половината от тях са преживели кибератака, изтичане на данни или вътрешни пробиви. Тук трябва да се отбележи, обаче, че в повечето случаи разкриването на инциденти се осъществява не от самите енергийни компании, а от разузнавателните служби.

Защо обаче кибератаките се оказват относително лесни за извършване днес? Съвременната технологична уязвимост на обществата се определя от устройство, явяващо се важна част от модерната инфраструктура. Това е т.нар. програмируем логически контролер (PLC), чието изобретяване датира още от 60-те години на XX в. Постепенно той заменя различните релета и човешки команди, допринасяйки за автоматизацията. Благодарение на последвалата му компютъризация, обаче, днес той отговаря за почти всяка индустриална или търговска операция, явявайки се „мозъка“ за ръководене на всякакви важни системи – от въздушния трафик до железопътния транспорт.

Обект на кибератаки се явяват т.нар. SQL сървъри (от Structured Query Language, т.е. „Език за структурирани запитвания“). Целта е проникването през Интернет в компютърно управляваните индустриални контролни системи, които наблюдават и ръководят промишлените процеси. Най-важната им разновидност са системите SCADA (Supervisory Control and Data Acquisition), обхващащи понастоящем мащабни процеси, които включват разпръснати съоръжения и устройства на големи дистанции. Този тип системи, чието създаване предшества развитието на Интернет, днес се оказват благодарение на него свързани с външния свят. От една страна, това им позволява да изпълнят предписанията на либерализацията на енергийния сектор, изискващи от компаниите непрекъснато да споделят данни за производството и резервния си капацитет с пазарни оператори и с оператори на преносни мрежи. От друга страна, обаче, се появяват проблеми в случаите, когато компаниите, с цел съкращаване на разходи, ползват едни и същи компютри и мрежи както за контрол над вътрешните операции, така и за бизнес, който изисква контакт с външния свят. Това прави контролните системи особено уязвими за кибератаки.

Нападенията често са насочени към конзолите на SCADA оператори в рафинерии и химически заводи. Зловреден софтуер, вкаран в контролните системи на морски петролни и газови платформи, резултира от своя страна пък в риск от неконтролирано изпускане на суровини и потенциална екологична катастрофа, както и възможни експлозии и унищожаване на съоръженията. В тази връзка трябва да бъде споменат и т.нар. „Ефект Аврора" по името на демонстрационния проект на Американския департамент по енергетика, показващ как кибермanипулациите на SCADA системата на електроцентрала може не само да прекъсне електричеството, но и да произведе разрушителни повреди върху съоръженията (Averill, 2010). Другата голяма заплаха за контролните мрежи се явява т.нар. „буря от данни", при която генерирането на прекомерно много данни претоварва устройството, като блокира способността да се мониторират и контролират процесите по управление. Подобен ефект се получава при наличие на дефектни механизми, но той спокойно може да се постигне и дистанционно през Интернет.

В специално изследване на Rice University от 2012 г., посветено на въпросите на киберсигурността в американската енергийна индустрия (Cybersecurity Issues and Policy Options for the U.S. Energy Industry, 2012), във връзка с нарастващите заплахи за контролните системи се препоръчва ориентирането от реактивна към по-стратегическа позиция по темата. Това предполага излизане извън схващането за въпроса като проблем от областта на информационните и комуникационните технологии. Според един от основните автори на доклада – Кристофър Бронк, „за енергийната индустрия киберсигурността не е просто технологичен проблем, а по-скоро е такъв, обхващащ по-широката динамика на информацията и операциите" (Falk, 2012). Наред с теоретичните постановки, коментираното изследване предоставя достатъчно детайлни примери за големи петролни и газови компании, които са претърпели пробив в системите си.

4. В търсене на решения

Извън усилията на академичната общност, политическият сектор също се опитва да потърси адекватен отговор с цел адаптиране към новите реалности. През 2013 г. САЩ направиха значителна стъпка по отношение на извеждането на преден план на въпросите на киберсигурността. За първи път след 11 септември 2001 г. терористичните удари отстъпиха лидерската си позиция в списъка на заплахите за националната сигурност на страната (US Intelligence Community, 2013). Кибератаките заеха челното място в специализирания доклад, представян всяка година пред сенатския комитет, ангажиран с въпросите на разузнаването (Martinez, 2013). Високопоставени служители от сектора констатират, че киберзаплахите се превръщат в оръжие, което се използва срещу САЩ и което спомага за дефинирането на нов „мек" начин на война. Според Джеймс Клапър, директор на американското разузнаване, различни държавни и недържавни актьори все повече придобиват експертни киберзнания, които използват за постигане на стратегически цели чрез събиране на тайна информация от единици от публичния и частния сектор и чрез осъществяване на контрол над съдържанието и потока от данни. Това поставя на риск всички национални сектори – от държавните до частните мрежи и особено критичната инфраструктура.

Зачестяването на кибератаките срещу критична инфраструктура демонстрира по категоричен начин необходимостта от подобряване на сигурността в тази сфера. То е тясно свързано от своя стана с въпроса за прилагането на мерки за защита на стратегическите инфраструктурни компоненти. Темата за предприемане на законодателни действия по въпросите на

киберсигурността е особено актуална през последните няколко години в САЩ (Harder, 2013). Мерките, предприети от президента Барак Обама през февруари 2012 г., бяха насочени към позволяване на събирането на разузнавателни данни за кибератаки и киберзаплахи по отношение на критичната инфраструктура (The White House, 2013). Целта бе да се подобри споделянето на информация по тези въпроси между правителството и индустрията и да се създаде набор от добри практики за компании, които оперират с критична инфраструктура като водни системи, електроцентрали и телекомуникационни мрежи. Същевременно президентската администрация и Конгресът не успяха да се споразумеят за законодателни действия, отчасти заради спорове коя агенция трябва да е водеща в прилагането на регулациите. Редица анализатори побързаха да подложат на сериозна критика създалата се ситуация. Според Уилям О'Кийф „тази бюрократична схватка е аналогична на преподреждането на креслата на палубата на Титаник" (O'Keefe, 2013). Конгресът обаче изтъква като сериозна пречка пред приемането на законодателни мерки в сферата на киберсигурността проблемът с боравенето с персонална информация и лични данни в нарушение на основните права на гражданите.

Очевидно е, обаче, че съществуващите институции и стандарти се оказват неадекватни в борбата с новите заплахи. Подобряването на ситуацията по отношение на споделянето на информация за кибератаките несъмнено се явява от ключово значение не само за енергийния, но и за редица други стратегически сектори. В тази връзка не може да не се отбележи нуждата от разгръщане на мащабно публично-частно партньорство по тези въпроси, опиращо се на сътрудничество между индустрията и държавните институции. Обосновката за неговата необходимост се опира на няколко причини. От една страна, частният сектор разполага със скромни средства и недостатъчни възможности да идентифицира, разкрива и противодейства на киберзаплахите заради ограничения си капацитет в областта на разузнаването. Правителството, от своя страна, е ангажирано с проблемите на националната сигурност и работи със специализираните агенции, опериращи в тази сфера. Най-важният източник по отношение на информация, успешни практики и техническа подкрепа са именно публичните институции. От друга страна, обаче, компаниите са тези, които разполагат с експертните знания за схемите, съобразно които са изградени и функционират техните сложни контролни системи (Brown, 2013).

Същевременно при осъществяването на кибератака засегнатите трябва да споделят информация и с други компании, тъй като те също могат да се окажат изложени на идентичен риск. От тази гледна точка вътрешната междуфирмена комуникация също не бива да се пренебрегва. И двете нива на партньорство (и на компаниите с държавните институции, и помежду им) трябва да бъдат развивани успоредно, тъй като единствено активният обмен на данни за източниците и естеството на кибератаките ще спомогне за осъществяването на ефективно противодействие (Kuhn, 2013).

Разглеждайки тази тема, не можем да не споменем и въпроса за прилагането на стандарти за киберсигурност за предпазване на критичната инфраструктура. От особена важност е и прилагането на мерки за предотвратяване на деструктивното въздействие от кибератаките върху енергийната инфраструктура. Така например чрез внедряването на механични предпазители става невъзможно взривяването на газопровод чрез увеличаване на налягането от страна на кибертерористи (Santa, 2013). Енергийната индустрия започва да полага все повече усилия за защита на системите си, осъществявайки стратегически инвестиции в киберсигурността. Редица частни компании се насочват към

влагане на ресурси за противодействие на хакерите, но това провокира поставянето на въпроса, кой в крайна сметка ще плати цената за допълнителните мерки – бизнесът или обикновените потребители.

От тази гледна точка това, че киберзаплахите непрекъснато се променят и еволюират, подготвеността за ответна реакция е от императивно значение. За да се реализира тя обаче, е необходимо да не се пренебрегват или укриват инциденти от подобно естество, а както препоръчват експертите, да се развият уведомителни механизми по модела на съществуващите в авиационната индустрия. Наред с това сред ефективните мерки се изтъква и потенциалът на изготвянето на национални планове за междусекторно сътрудничество за подобряване на киберсигурността. Като цяло националните регулаторни системи реагират относително бавно на бързо развиващите се заплахи. Успешното им атакуване, обаче, е от интерес както за правителствата и енергийната индустрия, така и за потребителите, но за да може да се осъществи противодействие, първо трябва да е налице осъзнаване и сериозно възприемане на проблемите.

Анализаторите изтъкват и необходимостта от международно сътрудничество по въпросите на енергийната киберсигурност. Посочвайки като пример свързаността на американската електрическа мрежа с тази на Канада и Мексико, експерти наблягат на адекватността на по-мащабното трансгранично партньорство (Kruger, 2013). От друга страна често пъти зад атаките се крият чуждестранни правителства, стремящи се към реализация на собствените си национални интереси. Конфронтацията в такива случаи е неизбежна. Един от емблематичните примери в тази посока са американско-китайските отношения с оглед на призивите на Белия дом към Пекин да вземе „сериозни мерки" за възпиране на хакери при проникване в компютърни мрежи на американски фирми (Weinstein, 2013). Според Ричард Кларк, бивш национален координатор на САЩ по сигурността, защитата на инфраструктурата и борбата с тероризма, редица американски компании са били обект на успешни пробиви, инспирирани от Китай (Franks, 2013).

Във връзка с темата за защитата на критичната инфраструктура се дискутира и ролята на НАТО в тази област. Привържениците на потенциалната милитаризация на задачите на енергийната сигурност се опират на нейното интерпретиране не от икономическа перспектива, а през призмата на политически и стратегически съображения. Засилването на военния контрол според тях е оправдано и с оглед на новите заплахи пред сигурността като кибератаките срещу енергийна инфраструктура (Behrens, 2012, с. 4).

5. Заключение

В съвременната дигитална епоха ставаме свидетели на все повече „чудеса", превръщащи се в реалност в резултат на технологичния напредък. Не трябва обаче да се забравя, че тези „магически" нововъведения могат да имат и своето негативно въздействие върху обществата и стопанския живот. Модерните енергийни технологии стават във все по-прогресираща степен податливи на кибератаки, докато паралелно с това нараства и зависимостта на хората от тези системи, явяващи се определящи за редица аспекти на техния живот. Ключовият проблем днес обаче се явява не обвързаността ни с дигиталните системи, а въпросът как тя да кореспондира с адекватни способности да ги защитим. Революцията, провокирана от съвременните устройства, не може да се възпрепятства, тъй като тя е част от историята на технологичния прогрес. В настоящите условия, обаче, тя създава възможности да се причиняват катастрофални по размерите си опустошения дори без изстрелването на един куршум, а посредством

използването единствено на компютърна клавиатура. Елиминирането на негативните ефекти от новите технологични опции ще бъде възможно единствено при реализиране на съвместни усилия от страна на академичните среди, политическите лидери и представителите на бизнеса.

Цитирани източници:

Averill, Bruce, Eric Luiijf, 2010. Canvassing the Cyber Security Landscape: Why Energy Companies Need to Pay Attention. IAGS, *Journal of Energy Security*, 18 May 2010.

Behrens, Arno, Philip Bohler, 2012. A European Take on NATO's Emerging Role in Securing Energy Supplies. *Quarterly Journal*, Vol. 5, July 2012, Energy Security Forum, pp.4-5, Available at: < www.esc.mfa.lt [Accessed 15 June 2017].

Brown, David, 2013. Without Information Sharing, We're in the Dark. *National Journal*, Energy Experts Blog, 21 March 2013, Available at: < http://energy.nationaljournal.com [Accessed 15 June 2017].

Cybersecurity Issues and Policy Options for the U.S. Energy Industry, 2012. Baker Institute Policy Report, Rice University, September 2012, Available at: < https://www.bakerinstitute.org/media/files/Research/ba7df664/IT-pub-PolicyReport53.pdf [Accessed 15 June 2017].

Falk, Jeff, 2012. Energy firms must acknowledge cybersecurity as more than an IT problem, according to new Rice University paper. Rice University, 17 September 2012, Available at: < http://news.rice.edu [Accessed 15 June 2017].

Franks, Trent, 2013. The True Threat of Cyber Hackers. *National Journal*, Energy Experts Blog, 21 March 2013, Available at: < http://energy.nationaljournal.com [Accessed 15 June 2017].

Harder, Amy, 2013. Risky Energy: Cybersecurity and the Nation's Infrastructure. *National Journal*, Energy Experts Blog, 18 March 2013, Available at: < http://energy.nationaljournal.com [Accessed 15 June 2017].

King, Lewellyn, 2012. The Devastating Effects of a Cyber-Attack Against a Country's Energy Grid. Oilprise.com, 10 July 2012, Available at: < http://oilprice.com [Accessed 15 June 2017].

Kruger, Joe and Lemack, Carie, 2013. How Should Government and Industry Secure the Electric Grid from Cyber Attacks? Bipartisan Policy Center, 11 June 2013, Available at: < http://bipartisanpolicy.org [Accessed 15 June 2017].

Kuhn, Tom, 2013. Coordination and Cooperation are Best Defense. National Journal, Energy Experts Blog, 18 March 2013, Available at: < http://energy.nationaljournal.com [Accessed 15 June 2017].

Martinez, Luis, 2013. Intel Heads Now Fear Cyber Attack More Than Terror. ABC News, 13 March 2013, Available at: < http://abcnews.go.com [Accessed 15 June 2017].

Santa, Don, 2013. Collaborative, Voluntary Program Needed. *National Journal*, Energy Experts Blog, 18 March 2013, Available at: < http://energy.nationaljournal.com [Accessed 15 June 2017].

Sklar, Scott, 2013. Cybersecurity is 'Hit-or-Miss' Game. *National Journal*, Energy Experts Blog, 18 March 2013, Available at: < http://energy.nationaljournal.com [Accessed 15 June 2017].

O'Keefe. William, 2013. Collaboration, No Government Mandate. *National Journal*, Energy Experts Blog, 19 March 2013, Available at: < http://energy.nationaljournal.com [Accessed 15 June 2017].

The White House, 2013. Executive Order: Improving Critical Infrastructure Cybersecurity. 12 February 2013, Available at: < http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity [Accessed 15 June 2017].

US Intelligence Community, 2013. Worldwide Threat Assessment, 12 March 2013.

Weinstein, Bernard, 2013. In Cybersecurity Best Offense is Defense. National Journal, Energy Experts Blog, 19 March 2013, Available at: < http://energy.nationaljournal.com [Accessed 15 June 2017].