НЯКОИ КИБЕРЗАПЛАХИ В ДИГИТАЛНОТО ОБЩЕСТВО

Любен Боянов, Златогор Минчев, Кирил Боянов

1. Въведение

През последните години технологиите промениха коренно нашия живот. Широкото им навлизане във всички сфери на обществото доведоха както до рязкото подобряване на условията за съществуване, така и до промени в начините на мислене на хората. Според изследване на CISCO [CISCO, 2011] над 90 процента от Интернет потребителите ползват постоянно уеб технологиите. Голяма част - чрез мобилните комуникации осъществяват достъп до глобалната мрежа, която има вече над два милиарда (стационарни и мобилни) потребители. Факт е, че новите технологии активно променят нашите приоритети и начин на живот в настоящия информационен век [Ackerman & Guizzo, 2011].

2. Дейности в областта на киберсигурността

От 2010 година, проблемът за киберсигурността придоби голяма значимост и стана част от Дигиталния дневен ред за Европа – DAE [Digital Agenda for Europe, 2010]. Изследванията свързани с тази инициатива породиха след себе си и други, насочени към формулиране и провеждане на превантивни политики – напр. между НАТО и страните от БРИКС, инициативата на ЕС за Асамблея по Интернета на бъдещето [FIA Internet Portal, 2008], изграждането на международно сътрудничество в областта на ИКТ и за доверие в глобалните мрежи и услуги [BIC Project Web Page, 2011].

Проблемите с киберсигурността на FIA са адресирани към обема и произхода на данните, мобилните устройства, физическите обекти в мрежата и комерсиалните услуги. Сериозно внимание на киберсигурността се отделя не само от влиятелните политически институции, а и от неправителствени организации [Buckland, Schreier & Winkler, 2010; Ghannam, 2011; Lewis et al, 2011, Schreier, Weekes & Winkler, 2011]. В европейски мащаб правят впечатление проектите за идентифициране на информационна критична инфраструктура FORWARD [Forward Web Page, 2008] и изграждането на Европейска мрежа за управлението на рисковете и заплахите в Интернет в бъдещето [SysSec Web Page, 2010]. [1]

Два важни доклада бяха публикувани във връзка с киберзаплахите - от Sophos [Sophos Security Threat Report, 2011] и от Symantec [Symantec Internet Security Threat Report, 2011]. Тези материали идентифицират някои общи заплахи за

[1] Тук може да се отбележи и факта, че в България, с подкрепата на Фонд „Научни изследвания“ и Министерството на образованието, науката и младежта, през 2011 година, стартира успешно проект за млади учени на тема „Изследване на информационните заплахи и поведенческа динамика на потребителите в социални мрежи от Интернет пространството“ [SnFactor Web Page, 2012].

2010 и 2011 години, които ще продължат да имат съществено влияние и за в бъдеще. *Сред тях са: социалните мрежи, мобилния достъп до Интернет, зловредния софтуер с акцент върху червея Stuxnet, както и ролята на вътрешните агенти (инсайдерите), имащи съществено значение за индустриалните SCADA (Supervisory Control and Data Acquisition) системи и следователно за защитата на критичната инфраструктура. Накрая са отразени и заплахите от типа „атаки в ден нула“ (zero-day attacks), породени от от умишлени и неумишлени софтуерни грешки.*

Изследователската общност в сферата на киберсигурността в Европа, работи успешно в последните години по проекта *SySSec.* Бяха публикувани няколко анализа през 2011 и 2012 години, които адресират киберсигурността в следните области: кибератаки, заплахи за Интернета на бъдещето, зловреден софтуер и измами и сензорни мрежи.

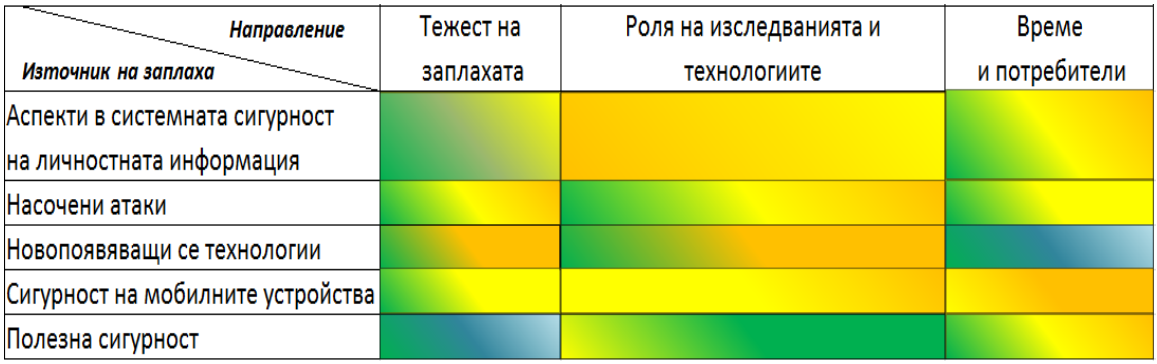
Структурирането на тези изследвания в мрежата SySSec обобщава кибер рисковете и заплахите свързани с тях в три направления: *лично*, *обществено* и *професионално* [Balzarotti, 2011], като негативните влияния са оценени в тристепенна скала: „ниско“ – „зелено“, „средно“ – „жълто“ и „високо“ – „червено“, както следва:

Направление / **Източник на заплаха**	**Лично**				**Обществено**		**Професионално**
	Личностна информация (Човешки права)	Дигитална идентичност	Финансово направление	Здравна сигурност	Критична инфраструктура	ГРИД Облачни технологии	Продажба на данни и др.
Анонимен достъп до Интернет							
Повсеместни мрежи							
Човешки фактор							
Атаки на вътрешни агенти							
Ботнети (външни агенти)							
Програмни грешки							
Мащаб и сложност							
Мобилни устройства							
Свързаност 24/7							
Достъп до повече лична информация							
Смартметри							
Следене							
Интелигентни среди							
Необазопасени устройства							
Социални мрежи							
Киберфизична свързаност за инфраструктури, коли и др.							
Организирана престъпност							
Мобилен зловреден софтуер							
SCADA зловреден софтуер							

Предвид факта, че предложената класификация е статична, през 2012 година, тя бе значително окрупнена и усъвършенствана [Balzarotti, 2012] с използване на идеи от аналитичната работа на Световния икономически форум [Global Risks Report, 2012], оставаики контекстно зависима от експертно дефинираните сценарии и области на интерес.

Оценяват се три направления с времеви хоризонт от пет години - *Тежест на заплахата, Ролята на изследванията и технологиите* и *Време и*

потребители за идентифициране на пет типа източници на киберзаплахи - *Аспекти в системната сигурност на личностната информация, Насочени атаки, Новопоявяващи се технологии, Сигурност на мобилните устройства* и *Полезна сигурност*. Обобщеното представяне на резултатите от това изследване е показано графично с използване на експертни оценки в четиристепенна линейно-градиентна скала: „ниско“ – „зелено“, „средно“ – „жълто“, „високо“ – „оранжево“ и „неопределено“ – „синьо“, както следва:



Така представените приоритетни направления за идентификация на киберзаплахите и киберрискове показват устойчива тенденция по отношение на повишаване на тяхната важност (изразена в преминаване от зелено към жълто-оранжево). Съществуват и тенденции към увеличаване на неопределеността (показани като преминаване от зелено към синьо), касещи *Новопоявяващи се технологии* и *Полезна сигурност*, в направления *Време и потребители* и *Тежест на заплахата*. Обобщението, за съжаление, не дава отговори на какво точно се дължат тези експертни прогнози.

3. Дигитална грамотност

Политическата, икономическата и социалната даденост на съвременното общество се обуславя и от нарастването на информационния поток, усъвършенстване на техническите средства за неговата обработка и все по-активното участие на човека в този процес.

Интернет промени съвременните политическа и социална действителност, предостави нови възможности за комуникации между хората и разшири кръгозора им. Социалните мрежи и електронните медии създадоха предпоставки за изграждане на „дигитално общество”, на по-активни и чуваеми обществени формации. Реализацията на това „дигитално общество” предполага изграждане на нови връзки, нов начин на общуване, нова грамотност. Тази нова грамотност включва способностите за пълноценно участие и общуване. По същество това е комбинация не само от техническите, но и от социалните умения на участниците в това общество. Както традиционните до момента грамотност и различните умения позволяват на хората да участват в трудовите и социални процеси, така и „дигиталната грамотност” и „дигиталните умения” дават определени умения на всеки участник да стане уверен и пълноценен член на това общество. Навлизането в дълбочина в сферата на компютърните и комуникационни технологии

разширява знанията и уменията на хората от тяхната детска възраст, с което подобрява качеството на „дигиталното общество".

За въвеждането на нови типове поведение ще се използва информационното /кибер/ пространство с възможностите, които то предлага. Използването на мобилните комуникации и мобилния интернет значително улесняват достъпа на обикновени човек до информацията по всяко време. В съществуващото вече информационно /кибер/ пространство, достъпът до информацията е свързан с два важни аспекта за потребителите.

Първият аспект е поведението на потребителите. Известно е, че ползването на определени инфраструктурни обекти – пътища, обществен транспорт, движение в градски условия и т.н. се извършва като се спазват определени изисквания и норми на поведение. Това предполага изграждане на определена „грамотност" на потребителите. В "дигиталното общество" и в различни негови сфери човек трябва да има изградено поведение, изградени навици. В литературата [Ribble, 2004] се определят важни области на поведение, с които обитателите на „дигиталното" общество трябва да се съобразяват: етикет, комуникация, образование, достъп, търговия, отговорност, права, безопасност и сигурност. Други автори [Yang, 2011] определят четири ключови области: дигитална компетентност, дигитална етика, дигитална чувствителност и дигитално участие.

Вторият аспект са начините за избягване на киберзаплахите и тяхната връзка с поведението на потребителите в дигиталното общество. Експотенциалното разширение на Интернет и приложението му в почти всички области на икономиката, обществения и социалния живот доведе до неимоверно нараствена на атаките и заплахите от тях. Съществуващите „защитни стени" /firewalls/ не винаги дават добри резултати, което обуславя необходимостта от значителни усилия на експертите по сигурността и на обществения контрол по отношение изискванията към „хакерите" за повишаване на тяхната отговорност.

Според Oppliger и Wildhaber [Oppliger, 2012] съществуват погрешни схващания в областта на сигурността, които се разделят на две основни групи. Едната група засяга социалните и поведенчески схващания – на първо място, че хората, като цяло, се интересуват от сигурността, докато всъщност те се интересуват само от определени изисквания към нея. На второ място е схващането, че сигурността е чисто технически въпрос, докато това, в наши дни, е една далеч по-всеобхватна задача, която не може да се реши само с технически средства. На трето място е подхода, че сигурността може да се реши без намесата на потребителя. Другата група засяга техническите и методологически подходи. В тази група се откроява становището, че към сигурността трябва да се подходи с формален анализ на риска, но става ясно, че типичния анализ на риска не е приложим към информационните технологии.

4. Някои киберзаплахи в дигиталното общество

4.1. Използване на пароли

Един от начините за повишаване на сигурността е добра защита на „пароли “ (“passwords”). Увеличаването броя на символите не е приемливо за потребителите, поради което усилията са насочени към постигане на максимална използваемост /секретност/ и лесно запомняне. За тази цел се предлагат различни подходи включително загадки (puzzles). Те включват различни техники използуващи пръстови отпечатъци, последователност от честотни поредици и т.н. [Bianchi, 2012].

Съвременните системи за сигурност обикновенно не изследват съдържанието на информацията разменяна между потребителите в мрежата. Повечето системи удостоверяват потребителското име (username) и паролата (password). Въвеждането на система, следяща най-общо съдържанието, би дала съответна информация – например каква е причината служител на дадена организация да тегли информация в 3 часа през нощта,когато обикновенно той прави това в 9 часа сутрин от работното си място. В [Ortiz, 2012] е описана система, която идентифицира обстоятелствата, при които потребителят се опитва да получи достъп до мрежата и какво възнамерява да прави с данните, които иска да получи. Системите изследващи съдържанието на информацията, за повишаване на сигурността, позволяват да се направят редица статистически наблюдения на навиците на потребителите, връзките които те установяват от гл. т. на интереси и т.н. Това в редица случаи ще подобри сигурността и на организациите и на потребителите, като спомогне и за предотвратяване на феномени от типа на WikiLeaks. Има и други примери в тази насока, като услугата Google mail, която отчита кога потребителят влиза в своята електронна поща от необичайно място, след което изисква потвърждение от неговия мобилен телефон за това, че този достъп не е от някой друг.

4.2. Неприкосновенност на личните данни и сигурност на данните

Изискванията за неприкосновенност на личните данни, както и защитата на данните обменяни по мрежата стават очевидна необходимост.

Технологично напредналите страни въвеждат законодателство, отнасящо се до неприкосновеността на личните данни и на данните съдържащи корпоративна информация. Законите за неприкосновеност на личните данни включват регулаторни механизми за събиране, използване, обработка, съхраняване и предоставяне на персонална (лична) информация. В ЕС законите предвиждат специални правила за т.нар. „чувствителна“ информация засягаща расова или етническа принадлежност, религия, политически възгледи и т.н., отразени отчасти в [Digital Agenda for Europe, 2010] и [Schreier, Weekes & Winkler, 2011].

Законите за сигурността на данните третират изискванията за защита на персоналната информация, която се обменя между потребителите. Това е свързано не само със защита на материалните нитереси на потърпевшите, но и с възможните морални последствя за отделния индивид [Gaff, 2012a], [Gaff,

2012b]. Сравнително лесно е да „откраднеш“ информация, особено когато тя е в електронен вид. Последствията, обаче, могат да се окажат непредсказуеми.

4.3. Атаки върху статии и публикации в списания и електронни издания, уеб приложения и потребителска информация

Все по-често се забелязва изопачаване на информацията в някои електронни издания. В края на 2004 година информацията в Wikipedia започна експоненциално да нараства с появата на нови статии. През 2007 година се отчита получаване на 180 материала за една минута. Този информационен поток не може да се следи от редакторите ръчно. Ето защо, бяха създадени средства, които автоматично да филтрират повтарящи се задачи и правописни грешки. Тези „Robots“ и „Cyborgs“, на първо време, бяха „имунната система“ на енциклопедията. Първите средства които следяха за промени в статиите довеждащи до „изкривена информация“ бяха програмите „AntiVandlBot“ и „VandlProff“. AntiVandlBot представлява проста система от правила, позволяващи мониторинг на промени в статиите и автоматично им отхвърляне. VandalProof използва графичен потребителски интерфейс написан на Visual Basic, позволяващ да се следят редактори, нямащи съответното доверие и да се отхвърлят направените от тях корекции. Въвеждането на нови средства, позволяващи стотици пъти по бързо редактиране, се съгласува и с авторите на статии в Wikipedia. За целта е създадена Bot Approvals Group, членовете на която са доброволци. В [Halfaker, 2012] са описани някои особености на създадените системи.

Тук ще отбележим и заплахите насочени както към уеб приложенията, така и към информацията използвана от потребителите при осъществяване на определени процеси в уеб пространството.

Една продължаваща разпространението си заплаха е “cross-site scriping” (XSS). Основната идея на XSS е да се използува специален символ, който вмъкнат заставя Web браузера (с разширител, използващ интерпретатор на уеб език от високо ниво, като Java, PHP, Perl и др.) да превключва от обработка на „данни“ към обработка на „кодове“ [Shar, 2012]. Например, когато HTML страницата се инициализира като „данни“, хакерът може да включи признак (чрез Java script код), което да провокира интерпретатора на Java Script. Ако приложението не филтрира подобни специални символи, XSS вмъкването е успешно и може да доведе до използване профила (account) на потребителя или други негови данни или атрибути.

4.4. Сигурност в домовете на бъдещето

Развитието на домовете на бъдещето като част от по-широката концепция за дигитална урбанизация и въвеждане на нови технологии [Chourabi et al, 2012] става неделима част от съвременното дигитално общество. Според [De Silva et al, 2012] те се класифицират в четири основни категории: (*i*) предоставящи услуги според здравния статус на техните обитатели; (*ii*) събиращи информация за поведението на техните обитатели; (*iii*) с охранителни функции и (*iv*) имащи отношение към повишаване на енергийната ефективност на дома. Редица софтуерни разработки [Dixon et al, 2011] и хардуерни решения [Ding et al, 2011], позволяват превръщането на обикновения дом в дом на бъдещето. С това възникват и опасности, свързани с взаимодействието между технологиите

и техните потребители. В стремежа за осигуряване на повече комфорт се пораждат заплахи, свързани с отдалечения достъп и управление на различни битови уреди и други интелигентни сензорни устройства и системи [Larsson, 2011].

Решенията за повишаване на сигурността в тази насока изискват комплексен подход и към момента включват основно въздействие върху комуникационния канал с използване на различни протоколи (*IPv4,6*, *802.11a-y* и *A10*, наследникът на популярния *X10*) и контрол на претоварването поради атаки за отказ на услуги (DDoS).

4.5. Влияние на мултимедията

Изследването на този елемент от дигиталното общество е свързано с необходимостта на потребителите да се забавляват и споделят информация, като използват съвременни аудиовизуални средства. Възможностите за забавление с въвеждането на Web 2.0, HDTV, Dolby Digital и 3D технологиите се увеличиха значително поради включването на интерактивност в реално време и висока доза реализъм в пресъздадената среда. Съвместното използването на решения от типа DES, AES, IPv6, MPEG2,4, DVB и др. при предаването на мултимедийно съдържание позволи реалното трансформиране на мултимедията в „хипермедия“. От това произтичат и редица проблеми свързани с мултимедийното съдържание, неговата защитата и влияние върху потребителите. Пристрастяването към хипермедийни забавленията оказва влияние върху поведението на потребителите във всекидневния им живот, което поставя въпроса и за тяхната полезност и контрол, особено при подрастващите [Bavelier et al, 2011], [Shafi, 2012], [Hazelle, 2012].

Друг проблем около тази тема е авторските права на хипермедийното съдъжание, чието гарантиране в дигиталното общество изисква комбиниране на законодателни и технологични решения, станали напоследък дискусионни около споменатия по-горе Дигиталния дневен ред за Европа и идеите за въвеждане на SOPA, PIPA и ACTA.

4.6. Социален инженеринг

Един сериозен проблем, в съвременното дигитално общество, включва самите потребители – т.нар. „социалния инженеринг“. Подходите използвани в него датират още от първите опитите за създаване и управление на общности от хора, но с развитието на Интернет технологиите, мобилните комуникации и социалните мрежи ескалацията на заплахите породени от този инженеринг придобиват застрашителни мащаби [Platzer, 2012]. Днес потребителите на най-популярните социални мрежи Facebook, Twitter and LinkedIn [Top 15 Most Popular Social Networking Sites, 2012] са над милиард и половина, а възможностите за въздействие върху тях са трудно предвидими и описуеми.

Съществуват значими опасности свързани със социалния инженеринг, ориентирани около социални манипулации, революции [Ghannam, 2011] и негативно въздействие върху подрастващите [Bavelier et al, 2011], [Hazelle, 2012].
Разглеждайки този проблем е важно да се отбележат още два съществени момента: (*i*) ролята на маркетинговите кампании в социалния иженеринг,

събиращи данни за потребителите по опосредставан път, профилиран от техните навици, поведение и начин на използване на различни входни устройства в търсене на икономическа полза и (*ii*) психологичните нагласи и динамика в потребителите на социални мрежи, които също е възможно да бъдат мониторирани и използвани, както директно така и индиректно [SnFactor, 2012], [Platzer, 2012].

4.7. Заплахи към виртуалната среда

Използването на виртуални машини (ВМ) намира все по-голямо приложение. Много организации са инсталирали виртуални операционни системи, което позволява няколко програми да работят върху един сървер и като следствие да се намали броя на компютрите, което е икономически изгодно.

Във виртуалните системи хипервайзор създава чрез емулация компютър (виртуална машина) за всяка една виите на всяка една виртуална операционна система с процесора и периферните устройства.

Този подход е важен за изчислителните центрове, където работят хиляди сървери. Според [Garber, 2012] в индустриалните организации има изградена 80% виртуална инфраструктура на техните сървери. Това излага на сериозни кибер заплахи потребителите на услуги. В случай на атака на хост-сървер, слоят на ОС, осъществяващ виртуализацията, е компроментиран, което излага на опасност всички виртуални машини, съответно данните и приложенията, които изпълняват. Програмните системи за защита не следят трафика между виртуалните машини и не са в състояние да отчетат атаките.

Традиционните защитни системи (firewalls), инсталирани в мрежата, са между отделните компютри. Тъй като виртуалните машини работят върху един компютър, този подход не може да се приложи. Освен това процесът на виртуализация е единичен, като систематично се създават и изключват виртуални машини към различни хостове, което предполага динамична система за сигурност. Нови виртуални машини се инсталират автоматично, което предполага, че трябва да бъдат защитени.

Съществуват различни средства за защита. Маршрутизацията на трафика до физическия слой определен за защита, който го анализира и изпраща обратно към виртуалната система е неефективен процес. Понастоящем HP, IBM, Juniper, McAfee предлагат виртуална защитна система. Те работят като програмни приложения в операционната система на основния компютър и не е необходимо да пренасочват маршрутизацията до физическия слой за защита.

Заключение

Ограничаването на заплахите в дигиталното общество е неразривно свързано със създаването на правила и култура на поведение и спазването им от това общество. За осъществяването на такива дейности се изисква време и усилия не само от технологичен, но и от социален характер. Важно е да се предложи превантивна политика, като се отчитат възможните заплахи. Обществото следва постоянно да бъде информирано за появата на нови хакерски заплахи, които непрекъснато ще се появяват заедно с технологическите усъвършенствания. Това е задача както за учените, така и за медиите.

Благодарност
Изследванията в тази публикация са подпомогнати от проект „Европейска мрежа от центрове за върхови постижения в сферата на управлението на рисковете и заплахите за Интернета на бъдещето: Европа за света“ - SySSec, 7 РП на ЕС, No. 257007, http://www.syssec-project.eu/

Литература

Ackerman, E., & E. Guizzo, 5 Technologies That Will Shape the Web, 2011, Available at: http://spectrum.ieee.org/telecom/internet/5-technologies-that-will-shape-the-web/0

A Study on IT Threats and Users Behaviour Dynamics in Online Social Networks, DMU03/22, Young Scientists Project Web Page, 2012, Available at: www.snfactor.com

Bavelier, D., Green,C.S., Han, D. H., Renshaw, P.F., Merzenich M. M.and Gentile, D.A., Brains on Video Games, Nature Reviews, Neuroscience, vol. 12, December 2011, 763-768.

Balzarotti, D. (Editor) First Report on Threats on the Future Internet and Research Roadmap, September, 2011, The SySSec Consortia, Available at: http://www.syssec-project.eu/media/page-media/3/syssec-d4.1-future-threats-roadmap.pdf

Balzarotti, D. (Editor) Second Report on Threats on the Future Internet and Research Roadmap, SySSec Consortia, August, 2012, Available at: http://www.syssec-project.eu/media/page-media/3/syssec-d4.2-future-threats-roadmap-2012.pdf

Bianchi A., Oakley I., Kwon D., Open Sesame: Design Guidelines for Invisible Passwords, Computer, IEEE Computer Society Publ, ISSN 0018-9162, April, 2012, 58-65

BIC Project Web Page, 2011, Available at: http://www.bic-trust.eu/

Buckland, B., Schreier, F., & Winkler, T. H. Democratic Governance Challenges of Cyber Security, DCAF Horizon 2015 Working Paper No.1, Geneva: Geneva Centre for the Democratic Control of Armed Forces, 2010, Available at: http://genevasecurityforum.org/files/DCAF-GSF-cyber-Paper.pdf

Chourabi, H. et al, Understanding Smart Cities: An Integrative Framework, System Science (HICSS), 45th Hawaii International Conference on System Sciences, 2012, 2289-2297.
Cisco Connected World Technology Report, September 21, 2011,

Available at:
www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/CCWTR-Chapter1-Report.pdf.

De Silva, L.C., Mirokawa, Ch., Petra M. I., State of the art of smart homes. Eng. Appl. Artif. Intel., 2012, Available at: http://dx.doi.org/10.1016/j.engappai.2012.05.002

Ding, D., Cooper, A.R, Pasquina, F. P., Fici-Pascquina, L., Sensor technology for smart homes, Maturitas 69, 2011, 131-136.

Dixon, C., Mahajan, R., Agarwal, S., Brush, A.J., Lee, B., Saroiu, S., Bahl, P., An Operating System for the Home, 2011, Available at: http://research.microsoft.com/pubs/157701/homeos.pdf
FIA Internet Portal, 2008, Available at: www.future-internet.eu

Ghannam, J.Social Media in the Arab World: Leading up to the Uprisings of 2011. Washington, D.C.: Center for International Media Assistance, Available at: http://cima.ned.org/sites/default/files/CIMA-Arab_Social_Media-Report%20-%2010-25-11.pdf

Global Risks Report 2012, Seventh Edition, World Economic Forum, Available at: http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2012.pdf

Larsson, A. (Editor), Report on the State of the Art of Security in Sensor Networks, SysSec Consortia, September, 2011, Available at: http://www.syssec-project.eu/media/page-media/3/syssec-d6.1-SoA-SecurityInSensorNetworks.pdf

Digital Agenda for Europe, Brussels, COM(2010), Available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF

Forward Project Web Page, 2008, Available at: http://www.ict-forward.eu/

Gaff B., Smedinghoff T., Sor S., Privacy and Data Security, Computer, IEEE Computer Society Publ, March 2012a, 8-10

Gaff B., Loren R, Spinney E., Intellectual Property, Part II, Computer, IEEE Computer Society Publ, February, 2012b, 9-11

Garber L, The Challenges of Securing the Virtualized Environment, Computer, IEEE Computer Society Publ, ISSN 0018-9162, January 2012, 17-20.

Halfaker A, Riedl J., Bots and Cyborgs: Wikipedia's Immune System, Computer, IEEE Computer Society Publ, March 2012, 79-82

Hazelle R, Effects of Technology on Younger Generations – Children, October 10, 2012, Available at: http://scienceray.com/earth-sciences/effects-of-technology-on-younger-generations-children/

IFIP Technical Committee 14: Entertainment Computing Web Page, 2006, Available at: http://www.org.id.tue.nl/ifip-tc14/index.html
Lewis, J.A., Timlin, K., Deitz, S., Kempf, A., Rifkind, J., McGee, J., and Lukich, A. Cybersecurity and Cyberwarfare 2011, Preliminary Assessment of National Doctrine and Organization, Center for Strategic and International Studies, UN Institute for

Disarmerment Research, 2011, Available at: http://www.unidir.org/pdf/ouvrages/pdf-1-92-9045-011-J-en.pdf

Oppliger R, Wildhaber B.,Common Misconceptions in Computer and Information Security, Computer, June 2012, IEEE Computer Society, Vol 45, No 6, 102-104

Ortiz S. Jr, New Approach Keeps security in Context, Computer, IEEE Computer Society Publ, ISSN 0018-9162, April, 2012, 15-17.

Platzer, Ch. (Editor) Preliminary Report on Social Networks Security, The SySSec Consortia, March, 2012,
Available at: http://www.syssec-project.eu/media/page-media/3/syssec-d5.2-SoASocialNetworkSecurity.pdf

Ribble M, Bailey G., Ross T., Digital Citizenship-Addressing Appropriate Technology Behavior, Learning & Leading with Technology, September 2004, vol. 32, No 1, 6-11.

Shafi, S. Positive and Negative Influence of Media Among Young People, Youth World, Available at: http://uthmag.com/media-influence-on-youth/

Shar, L., Tan H., Defending against Cross-Site Scripting Attacks, Computer, IEEE Computer Society Publ, ISSN 0018-9162, March 2012, 55-62.

Schreier, F., Weekes, B., & Winkler, T. H. (2011). Cyber Security: The Road Ahead, DCAF Horizon 2015 Working Paper No.4. Geneva: Geneva Centre for the Democratic Control of Armed Forces, Available at:
http://www.dcaf.ch/content/download/35863/526943/file/Cyber2.pdf

Symantec Internet Security Threat Report, *Trends for 2010*, Volume 16,

Available at:
http://msisac.cisecurity.org/resources/reports/documents/SymantecInternetSecurityThreatReport2010.pdf

SySSec Project Web Page, 2010, Available at: www.syssec-project.eu

Top 15 Most Popular Social Networking Sites, September 2012,
Available at:
http://www.ebizmba.com/articles/social-networking-websites

Yang H, Oh K., A Study of the Digital Citizenship. The international Journal of Policy Studies, Korean Association for Public Studies, 2011.