امنیت سایبری در اینترنت اشیاء :

جنبه های قانونی

چکیده

رشد تعدادی از دستگاه های هوشمند، بهم پیوسته و ذاتا ناامن باعث تغییر در پارادیم امنیتی شده است. در حالی که تکنولوژی اینترنت اشیاء نیاز به تغییری در چارچوب قانونی دارد، روش های جایگزین نیز نیاز به توسعه دارند. این مقاله به بررسی تغییر محیط امنیت سایبری قانونی در زمینه اینترنت اشیاء می پردازد. این بحث های مقرراتی بین المللی قابل اجرا و همچنین روش های جایگزین برای پرداختن به مسائل ناشی از اینترنت اشیاء انتخاب شده اند.

ما می دانیم که تقریبا هر چیزی می تواند به اینترنت وصل شود، پس باید تمام حالات را در نظر بگیریم : هر چیزی که می تواند به اینترنت وصل شود می تواند هک شود[1و2].

کلید واژه ها: امنیت سایبری اینترنت اشیا چالش های امنیتی ابزار حقوقی

1. مقدمه

اگر چه در حال حاضر ، تعداد حملات سایبری [3] در سال های اخیر، زیاد شده است و قربانیان آنان افراد و شرکت ها می باشند، از این رو سازمان های اجرای قانونی و دولت ها در سراسر جهان، به هشدارها ادامه می دهند [4]. سال 2014، سال نفوذ [5] برچسبدار کردن بود و سال2015، سال اصلاح شدن بود که توسط برخی از مفسران صنعتی

به عنوان سال نفوذ .2.0 [6] لقب گرفته است درحالی که ممکن بود این برچسب ها بیش از حد کلی باشند، بطور کلی (و ترسناکی) تصویری که این برچسب ها دارند یکی از مکررترین، پیچیده ترین و شدیدترین حملات سایبری می باشد. علاوه براین، بنا به گزارشی تغییرات تدریجی برای تخریب بیشتر و حملات شخصی تر [7] بوده است[8].

تعداد نیروهای مسئول در برابر نفوذهای سایبری خصمانه و رخنه در شبکه های غیر مجاز افزایشی شدید داشته است. رشد فن آوری های جدید و رشد وابستگی های اجتماعی به فن آوری ها در سطح جهانی، همراه با اتوماسیون ابزارهای حملات سایبری [9]، پیچیدگی حمله های سایبری، و موانع ورود به بازار جرایم اینترنتی [10] بدون شک المان های کلیدی امنیت سایبری می باشند[11].

ظهور اینترنت اشیاء بطور چشم گیری چشم انداز تهدیدهای سایبری را تغییر داده است [12]. همانطور که در جزئیات زیر بحث شده است، پدیده اینترنت اشیاء مستلزم یکپارچه سازی همیشگی (بطور کلی) دستگاه های محافظتی ضعیف (اشیاء) در شبکه از طریق اتصال به اینترنت و به یکدیگر می باشد [13]. گسترش انبوه چنین دستگاه هایی که بطور ذاتی آسیب پذیر هستند باعث ایجاد مسیری برای حمله می شوند [14]، که به نوبه خود، خطرات امنیتی را زیاد می کنند [15]. در نتیجه، تغییر پارادایم مورد نظر توسط اینترنت اشیاء که بنظر می رسد طوفانی امنیتی کامل را ایجاد کرده است، تشکیل می شود [16]، اعتبارسنجی روش های امنیت سایبری حقوقی مرسوم به پرسشی در سطوح متعدد و عمیق تبدیل شده است [17].

در پاسخ به این چالش، این مقاله به دنبال بررسی تغییر چهره امنیت سایبری در اینترنت اشیاء می باشد- که به عنوان یکی از بزرگترین چالش های امنیتی در کوتاه مدت- از نظر قانونی می باشد [18].

این مقاله به شرح زیر سازماندهی شده است. بخش 2 مجموعه مرحله ها را با کاوش در مفاهیم امنیت سایبری و اینترنت اشیاء بیان می کند. بخش 3 به بررسی چالش های امنیتی بدست آمده با توجه به دینامیک اینترنت اشیاء می پردازد. بخش 4 به تحلیل مقررات بین المللی که مرتبط با امنیت سایبری هستند، می پردازد. در نهایت، بخش 5 بطور خلاصه به بحث در مورد روش های نظارتی جایگزین برای پرداختن به چالش های امنیتی در اینترنت اشیاء می پردازد.

2 . مفاهیم پایه ای و اصطلاحات

2.1 امنیت سایبری

2.1.1 (نبودن) تعریف

مرحله اول برای چارچوب موضوع امنیت سایبری در فضای مجازی درک معنای اصطلاح " امنیت سایبری " می باشد. به نظر می رسد تلاش برای برای به چالش کشاندن این موضوع از گذشته تا به امروز ادامه دارد و هیچ تعریف استاندارد و یا مورد پذیرش جهانی برای این اصطلاح وجود ندارد [19]. برای اینکه همه چیز پیچیده تر می باشد، هیچ اتفاق نظری در مورد معنای دقیق این اصطلاح و حتی املای آن وجود ندارد[20]. در رابطه با این موضوع، جامعه اینترنتی اظهار دارد که " به عنوان کلمه ای راهنما، امنیت سایبری کلمه ای اشتباه می باشد و می توان برای ایجاد لیستی بی پایان از نگرانی های مختلف امنیتی، چالش های فنی و " راه حل ها" اعم از فنی تا قانونی را برای آن در نظر گرفت[21].

برای هدف این مقاله، تعریف اتحادیه بین المللی مخابرات (ITU) استفاده خواهد شد[22]. ITU امنیت سایبری را به عنوان " مجموعه ای از ابزارها، سیاست ها، مفاهیم امنیتی، محافظین امنیتی، دستوالعمل ها، روش های مدیریت ریسک، اقدامات، آموزش، بهترین شیوه، اطمینان و فن آوری تعریف می کند که می توانند برای حفاظت محیط سایبری و سازماندهی و دارایی های کابران استفاده شوند [23]. سازمان و دارایی کاربران بویژه " دستگاه های محاسبه کننده متصل" [24]، مانند دستگاه های اینترنت اشیاء می باشد.

با توجه به ITU، هدف نهایی امنیت سایبری، اطمینان از ویژگی های سازمان و دارایی های کاربران می باشد و همچنین حفاظت آنها در برابر ریسک های امنیتی در محیط سایبری می باشد[25]. اهداف امنیتی عمومی عبارتند از (i) محرمانه بودن، (ii) بی نقص بودن و (iii) در دسترس بودن (همچنین به عنوان مجموعه سه گانه CIA در صنعت امنیت اطلاعاتی شناخته می شود [26]) می باشد[27]. محرمانه بودن بدین معنی است که اطلاعات را بطور نادرست در اختیار افراد غیر مجاز، فرآیندها و یا دستگاه ها قرار ندهیم [28]. بی نقصی اشاره به محافظت اطلاعات در برابر تغییرات غیرمجاز یا تخریب بدون مجوز دارد[29] . در دسترس بودن اشاره به دسترسی قابل اطمینان و به

موقع اطلاعات و داده ها برای کاربران مجاز دارد [30].

2 . 1 . 2 چشم انداز تهدید سایبری

2.1.2.1 طبقه بندی امکان پذیر. یکی از راه های شروع یک بحث در مورد امنیت شناسایی تهدیدات می باشد [31] که باعث چالش آن می شود. این بخش بصورت خلاصه چشم انداز تهدید سایبری معاصر را با استفاده از روش خطی که شامل تهدیداتی از قبیل (i) عوامل تهدید، (ii) ابزارهای تهدید و (iii) نوع تهدید می باشد را شرح می دهد [32]. لازم به ذکر است که، در حالی که چنین طبقه بندی به منظور بحث زیر مفید است، (هدفی) الگویی جامع از ماهیت بسیار پیچیده و ویژگی های تهدیدات سایبری وجود ندارد.

2.1.2.2 عوامل تهدید. طیف گسترده ای از عوامل خارجی و داخلی امنیت سایبری را تهدید می کنند. عوامل تهدید می توانند پیچیده یا ساده باشند. که عبارتند از دولت های ملی، مجرمان اینترنتی سودجو، سازمان های جنایی، هکر ها (کلاه سیاه، خاکستری یا سفید [33])، فعالین هکری، افراط گرایان و گروه های داخلی می باشند. این دسته بندی ها متقابلا منحصر به فرد یا انحصاری نیستند [34].

انگیزه های عوامل تهدید بطور قابل توجه ای متفاوت است. عواملی که به دلایل سیاسی می باشند (برای مثال، تخریب، آسیب رساندن، اختلال و یا به دست گرفتن کنترل اهداف، درگیر شدن در جاسوسی سایبری و یا اعتراض سیاسی) [35]. آنها علاوه براین ممکن است، انگیزه های مالی (برای مثال، سرقت اطلاعات با ارزش شخصی و یا مالی، مانند شماره امنیت اجتماعی و شماره کارت اعتباری که می تواند برای سرقت هویت و غیره استفاده شود [36]) و همچنین انگیزه های فرهنگی و اجتماعی (برای مثال، درگیر شدن در حملات با داشتن اهداف فلسفی یا اهداف تبلیغاتی، کنجکاوی و غیره) داشته باشند [37].

2.1.2.3 ابزارهای تهدید. عوامل تهدید معمولا استفاده از ابزارهای تهدید مشابه می باشد. ابزارهای امنیتی اصلی

شامل نرم افزارهای مخرب [38] و انواع آن (باج افزارها [39]، ویروس ها، کرم ها، اسب های تروجان و غیره) و بات نت ها می باشند [40].

نرم افزارهای مخرب در رده بندی کلی، بطور کلی اشاره به هر کد یا نرم افزاری دارند که بطور مخفیانه در یک دستگاه بدون اجازه نصب شده باشند. که این مورد شامل کدهای مخرب طراحی شده برای اهدافی مانند آسیب رساندن، اختلال، یا بطور کلی وارد کردن ضربه ای به برخی از انواع داده ها و سیستم و یا شبکه می باشد [41]. باج افزارها، نوعی از نرم افزارهای مخرب می باشند که دسترسی به دستگاه های آلوده و یا سیستم را محدود می کنند [42]. در صورت حمله باج افزار، باج افزار سیستم در حال کار با تمام داده ها یا فایل های خاص را از دسترسی خارج می کند[43]. سپس حمله کننده سایبری درخواست باج، یا بطور کلی بیت کوین، برای بازگرداندن سیستم به حالت اول خود می کند[44]. بات نت ها، معمولا شامل سرورهای کنترل و فرمان (C&C) و شبکه های کامپیوتری آلوده شده توسط نرم افزارهای مخرب می باشند که می توانند از راه دور کنترل شوند[45].

با توجه به گزارش چشم اندازه تهدید سال ENISA 2015، نرم افزارهای مخرب در سال 2015 تهدیدهای شماره یک به حساب آمدند [46]. باج افزار، با توجه به گفته کارشناسان صنعت، یک تهدید اصلی می باشد و بسرعت در حال افزایش می باشد [47]. بات نت ها به عنوان عنصر اصلی در " مصرف سازی جرم سایبری" (مدل تجاری " استخدام بات نتر"، که می تواند در حملات بر طبق گزارشات برای USD 38/ بطور ماهانه، بر عدم تناسب مهم بین هزینه های حمله و آسیب های بالقوه تاکید کنند [48]) پرچم دار می باشند [49]. به تازگی، بات نت هایی به مهمترین سلاح های برای مجرمان سایبری تبدیل شده اند [50]. با توجه به تهدیدات، بطور خاص برای اینترنت اشیاء، هر دو برنامه های مخرب و بات نت ها به عنوان تهدیدات در حل ظهور در گزارشات ENISA مطرح شده اند[51].

2.1.2.4 انواع تهدید. تهدید به امنیت سایبری شامل تهدیدات مربوط به اصلاح اطلاعات یا سوءاستفاده، تخریب اطلاعات، دسترسی غیرمجاز، نقض داده، سرقت اطلاعات و محروم سازی- سرویس (DoS) می باشد [52].

اگر چه تمام جنبه های سه گانه سازمان CIA (بخش 2. 1. 1) با حملات سایبری تهدید شده است، آزمایشگاه McAfee پیش بینی کرده است که تهدید به یکپارچگی سیستم ها و داده ها یکی از مسیرهای جدید حملات سایبری در سال 2016 را تشکیل می دهد [53]. به این دلیل که، توسط آزمایشگاه McAfee توصیف شده است، " قابلیت اعتماد و در دسترس بودن حملات، واضح و روشن است. آنها همه چیز را نقض و داده ها را افشاء کردند- که باعث شرمساری، ناراحتی و برخی ضررها شده است. یکپارچگی حملات مخفی، (و) انتخابی، (. . .) می باشد. به جای آسیب و یا تخریب به داده های حساس زیاد، بر عناصر خاص در حال تغییر در معاملات (تراکنش ها)، ارتباطات، یا داده هایی برای بدست آوردن سود قابل توجه متمرکز شدند[54].

2 . 2 اینترنت اشیاء

2.2.1 تعریف و مفهوم

اصطلاح اینترنت اشیاء (IoT) برای اولین بار توسط پیسگام تکنولوژی بریتانیا کوین اشتون در سال 1999 برای توصیف سیستمی که در آن اهداف فیزیکی را می توان از طریق سنسورهایی به اینترنت متصل، نمود ابداع شد[55]. اگر چه هیچ استاندارد یا تعریف جهانی در موردIoT وجود ندارد، برخلاف امنیت سایبری که تعاریف مختلفی دارد (بخش 2 . 1. 1)، اما اتفاق نظری در مورد مفهوم آن وجود دارد [56]. به این ترتیب، IoT به " اصطلاح محبوبی برای توصیف سناریوی هایی که در آن اتصال به اینترنت و قابلیت محاسبه برای انوع مختلفی از اهداف، دستگاه ها، سنسورها و اقلام روزمره " [57] شامل اتومبیل ها، یخچال ها و فریزرها، ترموستات ها، مانیتورهای سلامت و جاده ها تبدیل شده است. بدین ترتیب، اینترنت اشیاء ابعادی از " هرچیز" را برای اطلاعات و فن آوری های ارتباطات (ICT) جمع آوری می کند، که در حال حاضر ویژگی " هر زمانی" و " هر مکانی" به جنبه های عملی [58] و به اهدافی مرسوم در " هوشمند سازی" تبدیل شده است[59].

تعاریف مختلفی از IoT در حال حاضر به وجود آمده است. تفاوت های مهم میان تعاریف ظاهر شده وابسته به دیدگاه مورد نظر برای بررسی IoT می باشد. با توجه به تعاریفی که اغلب در مورد IoT ذکر شده، IoT " زیرساخت

هایی جهانی را برای جامعه اطلاعاتی در نظر می گیرد و خدمات پیشرفته ای را توسط ارتباط (فیزیکی و مجازی) اشیاء براساس فن آوری های ارتباطی و اطلاعات سازگار در حال تحول و موجود " اجرا می کند[60] (تاکید اضافه شده). به این ترتیب، تعریف ITU عمدتا بر ویژگی اتصال IoT بدون هیچ گونه اشاره به اینترنتی متمرکز شده است [61].

از نظر اهمیتی، استدلال کوچکی با این واقعیت وجود دارد که تغییر در فن آوری IoT دارای پیامدهای گسترده و مخربی است. انواع مختلف برنامه های کاربردی در حال ظهور در زمینه IoT، بطور فزاینده ای از کارهای روزمره ما به وجود آمده اند[62]. به این ترتیب، صنایع گسترده IoT، حوزه هایی مانند بهداشت هوشمند (برای مثال، نظارت بر بیماران)، حمل و نقل هوشمند (برای مثال، اتومبیل های بدون راننده)، زندگی هوشمند (برای مثال، نظارت بر کودک)، ساختمان های هوشمند (برای مثال ترموستات هوشمند)، مواد غذایی هوشمند (برای مثال، کنترل/ مدیریت زنجره غذایی)، انرژی هوشمند (برای مثال شبکه هوشمند)، صنعت هوشمند (برای مثال، سسنور دما) و حتی شهرهای هوشمند (برای مثال نظارت بر ترافیک) را در بر می گیرد[63].

2 . 2 . 2 (مختصر) زمینه های فنی

IoT در حال حاضر به تعدادی از فناوری های مختلف وابسته است[64]. که شامل سیستم های شناسایی فرکانس های رادیویی (RFID) و همچنین شبکه های حسگر بی سیم (WSN)، سیستم های ماشین به ماشین (M2M)، داده های بزرگ، خدمات ابر و برنامه های هوشمندمی باشد[65].

توپولوژی RFID یکی از بلوک های کلیدی IoT می باشد[66]. این تکنولوژی بطوری منحصربفرد، با دقت و با تشخیصی بطور خودکار، ردیابی و تعیین محل دارایی ها را از طریق امواج بی سیم (مغایر با بارکد نوری) انجام می دهد [67]. سیستم RFID از دو بخش : (i) فرستنده (برچسب RFID)، که به " اشیاء" متصل است (که می تواند عملا هر دستگاه محاسباتی را به محصول غذایی، حتی حیوان یا انسان متصل کند [68]) و سرورها را به عنوان انتقال دهد، و (ii) دستگاه ثبت یا خواننده، که داده ها را از دستگاه فرستنده بخواند[69]. از دیدگاه امنیتی، RFID

یک بخش بسیار آسیب پذیر است، که هیچ سطح بالاتری از هوش نمی تواند آن را فعال کند[70].

طرح پیشنهادی صنایع محبوب برای زیرساخت های IoT، کد محصول الکتریکی (EPC) می باشد[71]. در چنین زیر ساخت هایی، " اشیاء" اهدافی هستند که برچسب های RFID را با EPC منحصر بفرد حمل می کنند[72]. زیرساخت ها می توانند سرویس های اطلاعاتی EPC (EPCIS) را بصورت محلی و از راه دور به مشترکین ارائه دهند[73]. بجای ذخیره اطلاعات بر روی یک برچسب RFID، سرور توزیع در اینترنت، می تواند اطلاعات را از طریق ارتباط و ارتباط-متقابل با کمک یک سرویس نام گذاری اشیاء (ONS) تامین کند[74].

3. پیامدهای امنیتی اینترنت اشیاء

3.1 چالش های ایجاد شده توسط اینترنت اشیاء

برای ادامه توسعه و استقرار سیستم های IoT به یک فاکتور بسیار مهم که امنیت می باشد نیاز است[75].

در حالی که موضوع امنیت در زمینه فن آوری اطلاعات که البته جدید نیست، IoT را با چالش های جدیدی روبرو می کند[76]. همانطور که توسط کارشناسان صنعت [77] در قیاس های زیر خلاصه شده است: " هر چیزی که به اینترنت متصل شود می تواند هک شود. هر چیزی می تواند به اینترنت متصل شود. (در نتیجه) هر چیزی می تواند آسیب پذیر باشد(. . .)" [78]. از این رو، به نظر می رسد که هر دستگاه با وصل شدن به اینترنت [79] به ناچار در برخی از نقاط به خطر خواهد افتاد. با توجه به این دیدگاه، سوال این است که آیا زمان زیادی طول می کشد این اشیاء هک شوند؟

یک چالش امنیتی کلیدی در زمینه IoT افزایش سطح حمله کلی [80] برای حملات مخرب، [81]، نسبت به سیستم های جدا (به معنی بدون اتصال) می باشد. این ممکن است بطور خاص به عوامل زیر مرتبط باشد:

اولا، با توجه به سهولت و هزینه (نسبتا کم) توسعه دستگاه های IoT و همچنین با توجه به میزان پذیرش بالای اشیاء متصل شده هوشمند، رشد سیستم IoT بطور پیوسته در تنوع و اندازه های مختلف در سال های آینده ادامه خواهد داشت[82]. شرکت ها و سازمان های مختلف در مورد تعدادی از اشیائی که در آینده به اینترنت متصل می

شوند پیش بینی هایی کرده اند. پیش بینی محافظه کارانه توسط Gartner، برای مثال، این است که، تعداد دستگاه های شبکه شده که در سراسر جهان استفاده می شود تقریبا برابر با 20.8 میلیارد در سال 2020 خواهد شد[83]. Cisco تخمین می زند که در سال 2020 اتصالات IoT برابر با 50 میلیارد خواهد شد[84]. پروژه های Huawei، چنین ارتباطاتی را حدود 100 میلیارد در سال 2025 برآورد می کند[85]. در حای که تفاوت در این پیش بینی به هر شکلی سوال برانگیز می باشد[86]. نتیجه مستقیم از این موضوع این است که به زودی مقداری عظیم از دستگاه های فعال اینترنتی بصورتی پویا به حفاظت نیاز دارند.

دوما، با توجه به رشد سریع IoT که بدون در نظر گرفتن مناسب مسائل امنیتی رخ داده است، دستگاه های هوشمند بطور کلی ذاتا نا امن می باشند[87]. مطالعات سال 2015 توسط Hewlett Packard نشان می دهد که 70 درصد دستگاه های IoT بطور جدی آسیب پذیر می باشند[88]. این آسیب پذیری بخصوص ناشی از دلایل زیر است[89]:

عدم انتقال رمز : بسیاری از دستگاه های IoT " واحد- انجام دهنده" ساده هستند، و تمام دستگاه ها دارای هزینه، اندازه و محدودیت های پردازشی (هزینه قدرت پردازش اضافی) می باشند[90]. این به معنی این است که اکثر دستگا ها قدرت پردازشی مورد نیاز برای اقدامات امنیتی قوی و ارتباطی امن ندارند، مانند رمزگذاری (برای مثال، میکروکنترلر 8 بیتی، تابعی که صرفا برای چراغ روشن و خاموش است، نمی تواند از استاندارد صنعتی SSL برای رمزگذاری ارتباطات استفاده کند[91]) و ممکن است داده ها را در متنی واضح انتقال دهد[92]. البته، بخصوص در زمینه IoT این مسئله گیج کننده می باشد، با توجه به حجم انبوهی از داده ها که در حال حاضر بین دستگاه های هوشمند، ابر و برنامه های کاربردی منتقل می شود[93].

تشخیص هویت و تاییدیه ناکافی : تشخیص هویت / تاییدیه می توانند با توجه به الزامات رمز عبور، استفاده بدون دقت از رمز عبور (میوه ای حلق آویز برای هکرها)، عدم بازنشانی رمز عبور دوره ای و عدم نیاز به تشخیص هویت دوباره برای داده های حساس ضعیف باشند[94]. تشخیص هویت ضعیف و تاییدیه کل سیستم IoT را به خطر می اندازد [95].

ارتباط وب نا امن : موضوع امنیت با ارتباط وب شامل تهیه فایل آغازگر سایت – عبور مداوم، مدیریت دوره ای ضعیف و اعتبار بطور پیش فرض ضعیف یا ساده (که می تواند توسط حساب های مورد نظر سوءاستفاده شود تا دسترسی برقرار شود) می باشد[96].

نرم افزار نا امن و سیستم عامل : با توجه به محدودیت های منابع، بسیاری از دستگاه های IoT بدون توانایی برای نرم افزارهای تطبیقی یا بروز رسانی های سیستم عامل (که هزینه ای اضافه دارد) طراحی شده اند. در نتیجه، سرهم بندی آسیب پذیری دشوار (اگر غیر ممکن نباشد) است[97]. این به معنی، البته، مشکل از آنجایی است که " تقریبا غیرممکن " [98] برای طراحی برنامه آسیب پذیر- رایگان می باشد[99]. علاوه براین، بروز رسانی ها در دسترس هستند، بسیاری از دستگاه ها به نظر نمی رسند که از رمزگذاری برای دانلود بروزرسانی های نرم افزاری استفاده کنند[100].

از این رو، انفجار در دستگاه های متصل، همراه با کمبود امنیتی متعدد اینترنت اشیاء باعث تغییر پارادایم امنیتی از سخت افزار به شبکه هایی می شود که دستگاه ها را پردازش می کنند. از لحاظ امنیتی، هر چیزی که نقطه ضعف برای حمله دارد، که عدم تعادلی بزرگ در رقابت تسلیحاتی امنیت سایبری ایجاد کرده است: در حالی که مدافعان باید امنیت هر قسمت از سیستم را بصورت تک به تک فراهم کنند، چون برای یک مهاجم تنها یک راه ورودی به شبکه کافی است. به این ترتیب، " هر شئ شبکه شده دارای زنجیره ارتباطی طولانی است که تنها یک ارتباط ضعیف منجر به ورود مهاجم می شود[101].

3.2 آسیب پذیری و عناصر ریسک

ریسک مربوط به دستگاه های IoT متعدد و متنوع می باشند. به این ترتیب، IoT ریسکی ایجاد می کنند که ممکن است از اطلاعات سوء استفاده شود، و دسترسی غیرمجاز به دستگاه ها بدست بیاید و دستگاه ها کنترل مشوند و یا آسیب بینند و حمله به دیگر سیستم ها آسان شود[102]. در حالی که این ریسک ها در کامپیوترهای مرسوم و شبکه های کامپیوتری (بخش 2 . 1. 2) وجود دارد، که باعث می شود نگرانی های منحصربفرد در زمینه اینترنت

اشیاء زیاد شود [103 و 104].

حملات دیجیتالی به دستگاه های متصل نه تنها ریسک هایی را در دنیای دیجیتال نشان می دهد بلکه ریسک های فیزیکی برای دستگاه ها (صدمه به اموال) و همچنین، حتی ریسک های ایمنی برای کاربران IoT (یعنی خطر آسیب فیزیکی و حتی مرگ) ایجاد می کند[105]. برای درک بهتر، اگر کسی در نظر بگیرد که حدود 10 میلیون خودرو در جاده بدون راننده در چند سال آینده وجود خواهد داشت[106]. اگر آسیب پذیری در چنین دستگاه هایی پیدا شود و توسط مجرمان سایبری از آن سوء استفاده شود؛ نه تنها ایمنی جاده بلکه زندگی افراد نیز به خطر می افتد[107]. ضربان ساز قلب یکی دیگر از مثال های خوب از تهدیدات فیزیکی می باشد که توسط دستگاه های متصل نا امن می شود[108].

ریسک نه تنها ممکن است باعث شود مهاجمان کنترل دستگاه ها را به دست گیرند بلکه ممکن است اطلاعات موجود در اشیاء هوشمند را در اختیار مهاجمان قرار دهد. در واقع، دستگاه های با قابلیت جمع آوری داده که بطور فزاینده ای در فضاهای معمولی خصوصی، حتی فضاهای خودمانی معرفی شده اند (برای مثال، سازمان ها، خانه ها، ماشین، و . . . ، از طریق فن آوری های پوشیدنی و خوردنی، حتی جسمی) در نظر گرفته می شود[109]. در نتیجه مقدار زیاد داده ها، شامل داده های مهم تجاری یا داده های شخصی، تولید شده، جمع آوری شده و ذخیره شده می باشد[110]. به ناچار، بویژه برای مقدار زیاد داده ها،[111] که باعث ایجاد پتانسیل زیاد برای سوءاستفاده می شود. [112].

اخیرا موجی از هک ها و نفوذ ها باعث نگرانی های زیادی شده که مرتبط با دستگاه های متصل شده به اینترنت می باشد. با این ترتیب، برای مثال، در زمینه بهداشت هوشمند (که " شاید مستعد پیادمدهای امنیتی IoT " می باشد [113])، محققی امنیتی، ایرادی در پمپ های بیمارستان کشف کرده است که می تواند به هکرها اجازه دهد به داروها و بیماران از طریق اینترنت دسترسی پیدا کنند[114]. یکی دیگر از حوادث بسیار علنی آسیب پذیری های بحرانی در تعداد زیادی از مانیتورهای کودکان متصل به اینترنت می باشد. این آسیب پذیری می تواند توسط هکر برای انجام فعالیت های مخرب (شامل فریاد نوزاد، و والدین اش، یا قطع مانیتور و یا تغییر تنظیمات دوربین آن برای

جاسوسی) مورد استفاده قرار گیرد[115]. در یک مورد، مهاجمی با بدست گرفتن کنترل مانیتورهای کودکان، تصویر آنها را بر روی یک وب سایت به نام " بردار بزرگ در حال تماشای شماست" پخش کرده است[116]. همانطور که ذکر شده، اتومبیل های متصل به اینترنت نیز در معرض هک می باشند. درجولای سال 2015، Fiat Chrysler اعلام کرد که 1.4 میلیون ماشین Jeep شناسایی شده اند که بعد از اتصال به اینترنت (عملکرد داشبورد، فرمان، انتقال و سیستم ترمز) می توانستند توسط یک لپ تاپ از راه دور هک شوند و مهاجمان می توانستند هر کاری شامل قفل در باز کردن در و یا خاموش کردن خودروی در حال حرکت انجام دهند [117]. علاوه بر این، کودکان نیز در معرض خط در IoT می باشند از آنجایی که اسباب بازی هایی ممکن است به اینترنت متصل شوند. شرکت سازنده الکترونیکی اسباب بازی Vtech اعلام کرده است که " هکر اخلاقی " اعتراف کرده است که با هک اساب بازی ها ، 6.3 میلیون کودک را مورد آزار قرار داده است[118]. هکر نام کودکان، آدرس منزل، تصاویر و چت های شخصی آنها را به دست آورده است، از این رو شرکت اسباب بازی در حال رفع نقض امنیتی می باشد[119].

با توجه به موارد ذکر شده، افزایش و تامین امنیت قوی در شبکه های IoT و سیستم ها موضوع مهمی می باشد.

4 . چارچوب قانونی

4.1 ملاحضات مقدماتی

در حقیقت در برخورد با این طوفان امنیتی کامل، چشم انداز قانونی و نظارتی سایبری بطور مداوم و به سرعت در تلاش برای حل چنین نگرانی هایی که در معرض تهدید می باشد است.

سیاست گذاران بطور معمول در مورد امنیت سایبری اظهار نظرهایی می کنند و بطور مداوم آن را در اولویت های سیاسی خود قرار می دهد. دولت ها در سراسر جهان برای (حداقل، رسما) تامین امنیت فضای مجازی و سیستم ها تلاش هایی انجام می دهند [120]. آنها روش های مختلفی برای امنیت سایبری به تصویب رساندند[121]. علاوه بر این، آنها تلاش هایی را برای اجرای قوانین سایبری جدید و یا بهبود مقررات قبلی انجام می دهند و در تلاش برای

انظباق آن با محیط زیست در سطح جهانی می باشند[122].

با وجود سراسیمگی فعالیت ها و طرح های مربوط به امنیت سایبری می توان گفت، سند جامع ای در این زمینه وجود دارد. و اسناد حقوقی گسترد ای برای رسیدگی به جرایم اینترنتی و امنیت فضای مجازی به تصویب رسیده است.

بخش های زیر تحیلی دو کلمه ابزارهای قانونی می باشد، یعنی، شورای کنوانسیون اروپا در جرایم اینترنتی (کنوانسیون بوداپست)، به عنوان اولین سازنده معاهده قانونی بین المللی برای تنظیم جرایم اینترنتی (بخش 4 .1) می باشد که اخیرا در دستوالعمل امنیت اطلاعات و شبکه (NIS) تصویب رسیده است، و به عنوان اولین متصل کننده ابزار قانونی گسترده EU برای تنظیم میدان وسیع تری از " شبکه و امنیت اطلاعات " می باشد(بخش 4 . 3).

4.2 کنوانسیون بوداپست

4.2.1 زمینه

کنواسیون بوداپست [123] در سال 2001 به تصویب رسید و سال 2004 اجرا شد[124]. در نظر گرفته شده که قوانین لازم به اجرا در زمینه جرایم اینترنتی به تصویب برسد [125].

درهای کنوانسیون بوداپست بروی همه باز است. تا به امروز، 48 دولت عضو این کنوانسیون شده اند، که از جمله، مشورهای عضو اتحادیه اروپا، و استرالیا و کانادا و ژاپن می باشند[126]. علاوه بر این، شش ایالت حق امضاء دارند، و 12 ایالت برای به رای آوردن قانون نیاز می باشد [127]. با وجود این گستردگی، کنوانسیون هنوز جهانی نشده است. بطور قابل ملاحضه ای، بخشی از کشورهای بزرگ[128]، فاقد کاربران اینترنتی می باشند که باعث می شود آنها در کنوانسیون شرکت نکنند[129].

4.2.2 هداف و محتوا

همانگونه که در مقدمه ذکر شده، هدف اصلی کنواسیون بوداپست دنبال کردن " سیاست مشترک در قبال جرم "

در برابر مجرم اینترنتی توسط اتخاذ " قوانین مناسب و همکاری بین المللی " است[130]. هدف از کنواسیون " جلوگیری از اقدام مستقیم علیه قابلیت اعتماد، یکپارچگی، و در دسترس بودن سیستم های کامپیوتری، شبکه ها و اطلاعات کامپبوتر و همچنین سوء استفاد از سیستم هایی مانند شبکه و داده ها " توسط مجرم شناختن چنین رفتاری و با تسهیل تشخیص، تحقیق، و پیگرد قانونی در سطح بین المللی و داخلی است.

طبق یادداشت توضیحی کوانسیون بوداپست، منطق در قبال جرم این است، در حالی که " موثر ترین" راه برای جلوگیری از دسترسی های غیر مجاز " اقدامات موثر امنیتی" است، پاسخ جامع باید همچنان شامل بازدارندگی باشد، یعنی " تهدید و استفاده از قوانین کیفری باشد[131].

کنواسیون بوداپست برای چهار دسته از جرایم اساسی، قوانینی را ارائه می دهد که از جمله (i) محرمانگی، یکپارچگی و در دسترس بودن اطلاعات در سیستم ها و کامپیوترها (ماده. 6-2) و (ii) جرایم مربوط به کامپیوتر ها (ماده8-7) می باشد. در این گزارش توضیحی مشخص می کند که جرایم تعریف شده براساس ماد 6-2، که شامل هک و نفوذ های کامپیوتری (تحت مفهوم کلی " نفوذ غیرمجاز")[132]، برای محافظت از محرمانگی و یکپارچگی و در دسترس بودن سیستم های کامپیوتری در نظر گرفته شده است[133]. به این ترتیب، اهمیت (محافظت) سه گانه CIA به وضوح در کنوانسیون بوداپست منعکس شده است[134]. اصطلاح " سیستم های کامپیوتری" در تعریف کنواسیون بوداپست " هر دستگاه یا گروهی از دستگاه های متصل و یا مرتبط با آن، یکی یا بیشتر از آن که، دنبال کننده برنامه، پردازش خودکار داده ها را انجام می دهد " می باشد (ماده 1). چنین تعریف گسترده ای نزدیک به دستگاه های دیجیتال [135]، شامل دستگاه های IoT بطور خاص می باشد.

از لحاظ دامنه،دسته های جرم در کنواسیون بوداپست طیف گسترده ای از جرم های سایبری (که به عنوان جرایمی در کشورهای عضو تعریف شده اند) را در نظر نمی گیرد[136]. این ممکن است ناشی از این واقعیت باشد که جرایم خاص به احتمال زیاد پیش بینی نشده اند (که جای تعجبی نیست زیرا کنواسیون از یک دهه پیش کار خود را آغاز کرده است) اما ممکن است نشان دهد که اجماع بین المللی نتواند با توجه به جرایم به آنها رسیدگی کند[137]. یا این حال، کنواسیون بوداپست برای امکان، مکمل یا اصطلاح برای این مشکل دارد (ماده 46). علاوه بر این، اشخاص

و سازمان های دیگر می توانند به جرایم اساسی کنواسیون بوداپست رسیدگی کنند به شرطی که چنین فعالیتی با کنواسیون در تضاد نباشد[138]. در عمل، این کار انجام می شود، یعنی کشورهای عضو، قوانین جرایم اینترنتی خود را بروز رسانی می کنند، با وجود این وافعیت که در کنواسیون بوداپست این قوانین تغییر نمی کند[139].

با توجه به موضوع گسترده همکاری های مرزی، کنواسیون بوداپست نیاز به احزابی برای همکاری با یکدیگر " با وسیع ترین حد ممکن" برای اهداف تحقیقاتی و یا دادرسی مربوطه به جرایم جنایی مرتبط با سیستم های کامپیوتری و داده ها یا برای جمع آروی شواهد الکترونیکی دارد (ماده23). هدف از همکاری های مرزی موثر برای " به حداقل رساندن موانع جریانی تندرو و اطلاعات و شواهد " [140] در سطح بین المللی می باشد. این تعهد بطور کلی به همکاری بیشتر در مقررات منجر می شود، که اصول استرداد مجدد (ماده 24)، کمک متقابل (ماده 25) و اطلاعات بدون دسترسی (ماده 26) را تنظیم می کند، که به احزاب حق می دهد به اطلاعات مربوطه بدون درخواست های قبلی دسترسی داشته باشند.

4.2.3 ارزیابی بحرانی

کنواسیون بوداپست اولین (بلند پروازی) تلاش خود را برای هماهنگ کردن چارچوب های قانونی به منظور مبارزه با جرایم سایبری آغاز کرده بود[140].

با وجود نقش خود در ارائه چارچوب شناخته شده بین المللی برای هماهنگ سازی بین المللی و تاثیر آن بر مقدار زیادی از قوانین جرایم سایبری EU، [142] بیش از یک دهه پس از تاسیس کنواسیون، کنواسیون بوداپست توسط منتقدان منسوخ شد. دلایل مختلفی برای ادعای منسوخ شدن ذکر شده، از جمله این واقعیت که، کنواسیون مبتنی بر جرایمی می باشد که در گذشته انجام شده (یعنی اواخر 1990) و در نتیجه (بطور طبیعی) ابزار حمله ای جدید را مدنظر قرار نمی دهد (مانند بات نت ها و نرم افزارهای مخرب)[143]. علاوه بر این، کنواسیون بطور ویژه درباره جرایم اقتصادی مجازی قانونی ارائه نمی دهد[144]. در نتیجه، باید راه کاری جدید برای تجدید نظر کلی کنواسیون بوداپست و یا حتی تصویب قانونی جدید در رابطه با جرایم سایبری، به عنوان مثال در سطح UN استفاده شود.

[145]

4.3 بخشنامه NIS

4.3.1 ملاحضات مقدماتی

EU به مبارزه با جرایم سایبری و تقویت امنیت سایبری از طریق اقداماتی پرداخته است. در این زمینه، EU تصمیماتی اتخاذ کرده است : (i) دستورالعمل های NIS، (ii) مقررات حفاظت اطلاعات عمومی (GDPR) و (iii) استراتژی بازار واحد دیجیتال EU (DSM) (که سنتز اولیه ای بر روی امنیت و حفاظت داده بطور خاص انجام می دهد) [147]، طرح های EU برای راه اندازی مشارکت خصوصی-عمومی در امنیت سایبری در سال 2016، همانطور که در DSM در سال 2015 انجام داده، می باشد[148]. بخش های زیر برروی دستوالعمل NIS متمرکز شده است.

4.3.2 زمینه سیاسی

در حال حاضر در سال 2001، کمیسیون اروپایی افزایش اهمیت شبکه و امنیت اطلاعات (NIS) در شبکه های ارتباطی و امنیت اطلاعات خود را برجسته کرده است: که پیشنهاد برای روش سیاسی اورپایی است[149].

در سال 2004، شبکه اروپایی و امنیت اطلاعات (ENISA) با هدف ترویج " فرهنگ شبکه و امنیت اطلاعات به نفع سازمان ها، شهروندان، مصرف کنندگان، تاجران و بخش عمومی در اتحادیه اروپا " بوجود آمد[150]. ENISA بطور عمده با ردیابی خطرات امنیتی اطلاعات، تسهیل همکاری و اشتراک گذاری اطلاعات بین نهادهای بخش دولتی و خصوصی، و کمک به کشورهای عضو در توسعه آنها از استراتژی امنیت سایبری صنعت خاص استفاده می کند [151].

دو سال بعد، در سال 2006، کمیسیون اروپا اروپا با هدف توسعه فرهنگ NIS در اروپا استراتژی ای برای جامعه اطلاعاتی امن اتخاذ کرده است[152]. عناصر اصلی استراتژی سال 2006، شامل امنیت و انعطاف پذیری در

زیرساخت های ICT بود که در قطعنامه شورای اروپا تایید شد[153].

در مسیر استراتژی سال 2006، در سال 2009، کمیسیون اروپا ارتباطات حفاظتی در زیرساخت های اطلاعاتی مهم را تصویب کرد، که در اروپا برای حفاظت از اختلال سایبری با افزایش امنیت و انعطاف پذیری متمرکز شده است[154].

در سال 2012، کمیسیون اروپایی مشاوره ای عمومی و آنلاین برای بهبود NIS در اتحادیه اروپا برگزار می کند[155]. نتیجه کلیدی از مشاوره نمایش داده شده، حمایت گسترده از ذینفعان برای بهبود NIS در سراسر EU بود[156]. نتایج (منتشر شده) حاصل از مشاوره برای کمک به اصلاح طرح ها در سال 2013، در بخشنامه امنیت اطلاعاتی و شبکه به تصویب رسیده است[157].

در سال 2013، کمیسیون اروپا استراتژی امنیت سایبری اتحادیه اروپا را منتشر کرد: که فضایی سایبری باز، امن و مطمئن [158] (استراتژی) می باشد. چهار مجموعه استراتژی در روش EU برای بهترین پیشگیری و پاسخ به اختلالات سایبری و حملات ارائه شده است. نظارت متمرکزی در آن وجود ندارد، اما کشورها را به سازماندهی و پاسخ به تهدیدات سایبری در سطح ملی تشویق می کند [159]. چهار مجموعه استراتژی از یک سری اقدامات با هدف انعطاف پذیری سایبری و کاهش جرایم اینترنتی در میان اشیاء استفاده می کند[160]. همچنین ENISA، قدرتی برای همکاری با بخش های دولتی و خصوصی به منظور پیشبرد تصویب استانداردهای NIS و پشتیبانی با توسعه دستوالعمل ها که منعکس کننده بهترین شیوه صنعتی است، اعطا می کنند [161].

در رابطه با این استراتژی، پارلمان اروپا و شورای اروپا دستورالعمل شبکه و امنیت اطلاعات را برای " اطمینان از سطح مشترک بالای شبکه و استاندارد امنیتی اطلاعاتی در میان کشورهای عضو " (طرح پیشنهادی NIS) پیشنهاد داده است [162]. طرح پیشنهادی با هدف امنیت اینترنت و سیستم های اطلاعاتی و شبکه های خصوصی که به جامعه دیجیتال وابسته است، مطرح شده است. قبل از معرفی دستورالعمل طرح پیشنهادی NIS، کمیسیون اروپا بر عدم وجود هر گونه مکانیزم موثری را در سطح EU برای همکاری موثر و برای تسهیل به اشتراگ گذاری در حوادث NIS و خطرات در میان کشورهای عضو اشاره کرده است. این، کمیسیون اروپایی هشدار داده بود، خطر مداخلات

نظارتی ناهماهنگ، استراتژی نامنظم و استانداردهای متفاوت و در نتیجه حفاظت ناکافی در سراسر EU وجود دارد[163].

دو سال بعد، در 7 دسامبر 2015، پارلمان اروپا و شورای اروپا به یک توافق سیاسی در اقدامات پیشنهادی کمیسیون اروپا برای افزایش امنیت آنلاین در EU رسیدند[164].

در 18 دسامبر 2015، پیش نویس سازش نهایی دستوالعمل NIS (پیش نویش طرح NIS) منتشر شد[165]. در می سال 2016، بطور رسمی سورای اروپا دستوالعمل NID را به تصویب رساند[166]. پس از انتشار متن به تصویب رسیده در مجلات رسمی اتحادیه اروپا و لازمالاجرا شده آن (که انتظار می رفت در آگوست سال 2016 این اتفاق رخ دهد)، کشورهای عضو، 21 ماه برای تغییر در دستورالعمل NIS در قوانین ملی (ماده 21، پیش نویس دستوالعمل NIS) وقت داشتند[167]. پس از این دوره، آنها شش ماه دیگر برای شناسایی و ایجاد لیستی از ارائه دهندگان خدمات ضروری در کشور خود که در حوزه دستوالعمل می باشد (ماده 3a پیش نویش دستوالعمل NIS) (بخش 4 . 3 . 3) وقت داشتند[168].

4.3.3 اهداف و محتوا

همانطور که ذکر شده، دستورالعمل NIS اولین قانون اتحادیه اروپا در مورد امنیت سایبری بود که بطور گسترده اجرا شد[169]. اهداف اصلی برای رسیدن به هماهنگی حداقل منطقه ای (EU) و برای ایجاد محیطی آنلاین قابل اعتماد، [170] که در نهایت برای پستیبانی از DSM می باشد[171].

دستورالعمل NIS به صراحت به مجموعه سه گانه CIA در تعریف امنیت NIS ، که " توانایی شبکه ها و سیستم های اطلاعاتی را برای مقاومت در سطح مشخصی از اعتماد، هر اقدامی که با موافقت در دسترس بوده، اعتبار، صحت و محرمانه بودن داده های ذخیره شده یا انتقال و پردازش داده های خدمات مربوطه ارائه شده قابل دسترس توسط شبکه و سیستم های اطلاعاتی (ماده 3 پیش نویس دستوالعمل NIS) (تاکیده اضافه شده) اشاره دارد.

دستوالعمل چهارگانه با اهداف اصلی و اقدامت لازم در مورد سطح مشترک بالایی از NIS در اروپا (ماده 1 پیش

نویس دستوالعمل NIS) بصورت زیر می باشد[172].

i . بهبود قابلیت های امنیت سایبری ملی: کشورهای عضو ملزم به اتخاذ یک استراتژی امنیت سایبری ملی (ماده 5 . پیش نویس دستوالعمل NIS) (استراتژی NIS) می باشند. این شامل ایجاد یک سیاست و یک محیط قانونی برای امنیت اطلاعات می باشد. دستورالعمل NIS بیشتر نیاز به کشورهای عضو برای ایجاد ظرفیت های سازمانی دارد. به این ترتیب، کشورهای عضو باید مقامات ذیصلاح ملی را برای اجرا و اعمال دستوالعمل NIS (ماده 6 پیش نویس دستوالعمل NIS) معین کنند و همچنین تیم های امنیت کامپیوتری برای واکنش سریع به حوادث (CSIRT) [173]، مسولیت کنترل حوادث و خطرات (ماده 7، پیش نویس دستوالعمل NIS) را بر عهده دارند.

ii . بهبود همکاری در سطح- EU : دستوالعمل NIS یک گروه همکاری با هدف حمایت و تسهیل همکاری های استراتژیک و تبادل اطلاعاتی بین کشورهای عضو (ماده 8a ، پیش نویس دستورالعمل NIS) ایجاد می کند.

iii . امنیت و الزامات هشداری حوادث: به منظور ترویج فرهنگ مدیریت ریسک باید اطمینان حاصل شود که حوادث جدی تری گزارش شده است (شرح پیش نویس دستورالعمل NIS)، دستوالعمل NIS الزاماتی هشدار دهنده حوادث و امنیت را در دو گروه از اشخاص نشان می دهد، برای مثال، (A) اپراتورها از خدمات ضروری و (B) ارائه دهندگان از خدمات دیجیتال استفاده می کنند. سند مربوطه توضیح می دهد که این تمایز و رفتار متفاوت با توجه به تفاوت های بین اپراتورهای خدمات ضروری (که دارای لینکی مستقیم با زیرساخت های فیزیکی) و ارائه دهندگان خدمات دیجیتال (گه دارای طبیعت عبور مرزی هستند) (سند اصلاح مربوط به فصل IVa) بوجود آمده است.

یک اپراتور خدمات ضروری یک‌نهاد عمومی یا خصوصی است که یک خدمت ضروری را ارائه می‌کند.(a) و برای نگه‌داری و حفظ فعالیت‌های اجتماعی و اقتصادی ضروری است. (b) اطلاعات سیستم و شبکه وابسته است.(c) به‌گونه‌ای است که یک حادثه در اطلاعات و شبکه سیستم اثرات مخرب قابل‌توجهی را در این سرویس‌ها ارائه می‌کنند(ماده 3A پیش‌نویس دستوالعمل NIS). دستورالعمل NIS شامل ضمیمه‌ای می‌شود که شامل نوع چهارم مجموعه‌هاست و می‌توان با آن مانند خدمات ضروری رفتار کرد (ضمیمه / پیش‌نویس دستوالعمل NIS). جای

تعجب ندارد که ضمیمه شامل صنایعی مانند تأمین‌کنندگان انرژی، ارائه‌دهندگان خدمات حمل‌ونقل، مؤسسات بزرگ مالی، خدمات شهری ، ارائه‌دهندگان خدمات بهداشتی و زیرساخت دیجیتال می‌باشد[174].

ضمیمه 3 دستورالعمل NIS سه دسته از ارائه‌دهندگان خدمات دیجیتال را شناسایی می‌کند به‌عنوان‌مثال ارائه‌دهندگان بازار آنلاین، موتورهای جستجوی آنلاین و خدمات محاسبات ابری. برخلاف نیاز به شناسایی اپراتورهای خدمات ضروری (در بال ذکر شد)، کشورها نیازی ندارند که عضو شوند و لیست اشخاصی را که خدمات دیجیتال ارائه می‌کنند را منتشر کنند. شرکت‌ها به این نتیجه رسیده‌اند که باید برای خود تعیین کنند که آیا می‌خواهند که در محدوده‌ی دستورالعمل‌های NIS باشند و مشمول الزامات آن باشند. باید اشاره کرد که به نظر می‌رسد سه دسته تفسیر خواهد شد اما نه به‌طور گسترده‌ای، NIS به شرکت‌های کوچک را از الزامات آن به‌منظور جلوگیری از تحمیل فشار مضاعف مالی و اداری معاف می‌کند[175]. بنابراین، دستورالعمل برای ارائه‌دهندگان خدمات دیجیتال با تعداد کارمند کمتر از 50 و ترازنامه کل کمتر از 10 میلیون یورو در سال اجرا نمی‌شود[176]. علاوه بر این طبق یک رسیتال، تولیدکنندگان سخت‌افزار و توسعه‌دهندگان نرم‌افزار به‌عنوان ارائه‌دهندگان خدمات دیجیتال در نظر گرفته نمی‌شوند (و نه اپراتور خدمات ضروری)[177]. مهم‌تر از همه اینکه ارائه‌دهندگان خدمت مبتنی بر اساس‌نامه اتحادیه اروپا که خدمات ارائه در اتحادیه اروپا را پیشنهاد داده‌اند تحت دامنه دستورالعمل قرار می‌گیرند.

A . ارائه‌دهندگان خدمات مشمول (1) الزامات امنیت (2) الزامات اطلاع‌رسانی نقض اجباری خواهند بود. اقدامات امنیتی و سازمانی باید از اقدامات صنعتی دولت پیروی کند که سطحی از امنیت شبکه و اطلاعات سیستم را مهیا می‌کند و ما را در مقابل تهدید مطمئن می‌سازد (ماده 14 دستورالعمل پیش نویس NIS). با توجه به نیازمندی برای ارائه آگهی، کشورهای عضو باید اپراتورهای خدمات ضروری مطمئن باشند و مقامات امنیتی را از شکافی که به یک آستانه مشخصی از آسیب‌رسیده است مطلع سازند، به‌عنوان‌مثال نقض در داشتن"تأثیر قابل‌توجهی در تداوم ارائه خدمات ضروری" (ماده 14 پیش‌نویس دستوالعمل NIS).

برای تعین یک رویداد، اپراتورها باید حداقل پارامترهای زیر را در نظر بگیرند(ماده 14 پیش‌نویس دستورالعمل NIS): (الف) تعداد کاربران به خدمات ارائه‌شده نهاد وابسته است. (ب) وابستگی سایر بخش‌ها در ارائه خدمات به

نهاد ارائه‌دهنده وابسته است (ج)تأثیری که حوادث می‌توانند داشته باشند، به لحاظ اندازه و مدت‌زمان در فعالیت‌های اقتصادی و اجتماعی و یا امنیت عمومی (د) سهم بازار از نهاد (ه) گسترش جغرافیایی با توجه به منطقه‌ای که می‌تواند تحت تأثیر یک حادثه باشد و (ی) اهمیت دادن نهاد برای حفظ یک سطح کافی از خدمات با توجه به گزینه‌های در دسترس ارائه خدمات(ماده 15a، پیش نویس دستوالعمل NIS).

B . ارائه‌دهندگان خدمات دیجیتال نیز شامل امنیت و الزامات اطلاع‌رسانی نقض اجباری خواهند بود اگرچه که اپراتورهای ارائه خدمات ضروری به‌مراتب کمتر با اقدامات سختگیرانه مواجه شده‌اند. کشورهای عضو باید اطمینان حاصل کنند که ارائه‌دهندگان خدمات ضروری نیازمند آن هستند که حوادث امنیتی را گزارش دهند که " تأثیر قابل‌توجهی را در ارائه یک خدمت دارد... آن را در اتحادیه ارائه دهند". (ماده 15A پیش‌نویس دستوالعمل NIS).

برای تعیین کردن اینکه آیا آستانه آسیب را به دست آورده‌ایم ارائه‌دهندگان خدمات دیجیتال نیازمند ان هستند که عوامل زیر را در نظر بگیرند (ماده 15A پیش‌نویس NIS): (1) تعداد کاربران تحت تأثیر حادثه (بعضی از کاربران خاص برای ارائه خدمات خودشان به سرویس وابستگی دارند). (2) مدت‌زمان حادثه (3) گسترش جغرافیایی با توجه به منطقه تحت تأثیر (4) اینکه وسعت اختلال تا چه حد در عملکرد این سرویس اثر دارد (5) آیا تعداد زیادی از کاربران تحت تأثیر اختلال در ارائه خدمت هستند به‌خصوص کاربران خاصی که به ارائه‌ی خدمت خودشان به سرویس وابسته است و (6) میزان تأثیر در فعالیت‌های اقتصادی و اجتماعی.

با توجه به داده‌های شخصی در زمینه‌ی نقض سایبری، دستورالعمل NIS اطلاعاتی را ارائه می‌کند که نقض اطلاعات شخصی ناشی از حوادث در بسیاری از موارد در معرض خطر به‌عنوان نتیجه حوادث، همکاری بین مقامات ذیصلاح و مقامات حفاظت از اطلاعات تشویق شده است (اصلاح سند 31 پیش‌نویس دستورالعمل NIS)[178].

عدم تطابق با مقررات ملی و متعاقب آن دستورالعمل NIS ، در موارد خاص رخنه‌ها و عواقب بالقوه خشن آن را اطلاع‌رسانی می‌کند. اگر چه محاسبه دقیق هنوز مشخص نیست، دستورالعمل NID به وضوح نشان میی دهد که مجازات باید " موثر، متناسب و بازدارنده " (ماده 17 پیش نویس دستوالعمل NIS) باشد.

4.3.4 ارزیابی بحرانی

شکی نیست که از لازم الاجرا شدن از دستورالعمل NIS چشم انداز نظارتی اتحادیه اروپا تغییر خواهد کرد و طیف گسترده ای از لوازم و بازیکنان، از جمله اپراتورهای جهانی تحت تاثیر قرار خواهد داد[179]. با این حال، باقی مانده آن خواه ناخواه رهنمود خواهد شد و تعویض بازی وعده داده شده در عرصه امنیت سایبری اتحادیه اروپا اجرا می شود[180].

منتقدان دستورالعمل NIS ادعا کرده اند که هنوز هم جای زیادی برای پیشرفت وجود دارد[181]. اول، دستورالعمل NIS با هدف دستیابی به "حداقل" سازگاری (ماده 2 پیش نویس دستورالعمل NIS). به این ترتیب به ویژه اجازه می دهد تا کشورهای عضو قوانینی که ممکن است بر اپراتورهای در صلاحیت این حوزه تصویب کنند سختگیرانه تر از آن است که در دستورالعمل مندرج شود. این، با این حال، همراه با درجه های مختلف بلوغ امنیت سایبری میان کشورهای عضو، خطر برچیده شدن قانونی وجود دارد. بنابراین، اپراتورهای بازار فعال در حوزه های قضایی متعدد به طور بالقوه هزینه انطباق بالاتر در تمام اتحادیه را با مقرراتی که در محل وجو دارد پرداخت می کنند. با این حال، در برخی موارد، ممکن است بهترین راه حل برای چنین شرکت هایی داشتن سطح یکنواختی از پذیرش آن در همه حوزه های قضایی باشد، به عنوان مثال برای تمام بخش ها به بالاترین استاندارد های موجود پایبند باشند. پس از آن بی ربط می شود اگر حوزه های قضایی طبق هیچ استانداردی تحمیل نشوند. در همین راستا، نیاز اطلاع رسانی دستورالعمل NIS به طور بالقوه با سایر مقررات گزارش نقض موجود تحت دیگر قانون EU، که همچنین به برچیده شدن آن کمک می کند، همپوشانی دارد[182].

دوما، تعدادی از الزامات، مانند، برای مثال، الزام در اپراتوها از خدمات ضروری برای " اقدامات فنی و سازمانی مناسب و متناسب"، در معرض تفسیر است. تنوع تفسیر در میان کشورهای عضو می تواند به یک میدان بازی بدون سطح در زمینه تجارت تبدیل شود و مانعی برای عملکردهای بطور همزمان در کشورهای عضو مختلف تشکیل دهد[183].

علاوه بر این، نگرانی های با توجه به معافیت شرکت های کوچک و متوسط از دستورالعمل و همچنین معافیت تولید کنندگان سخت افزار و توسعه دهندگان نرم افزار (که به تشکیل دهندگان ارائه دهندگان خدمات دیجیتال تلقی شده

است، و بخش بالای 4. 3 . 3). وجود دارد. معافیت چنین شرکت هایی از انجام حداقل اقدامات امنیتی یا تعهدات گزارش طبق دستورالعمل ممکن است خود را به ضعیف ترین حلقه در زنجیره امنیت تبدیل کنند و به اهداف آسان برای جرایم اینترنتی تبدیل شوند[184]. این روند برای کسب و کارهای کوچک و متوسط مشکل ساز است که بزرگترین درصد شرکت هایی که از زیرساخت های NIS استفاده می کنند[185].

با توجه به این مسئله به طور خاص گزارش دهی نقض اجباری ، این مسئله باقی می ماند که این نیاز چگونه به خوبی دیده می شود، که باعث جنجال قابل توجه است، موافقت و اجرا خواهد شد. در واقع، همه سهامداران از تصویب آن استقبال نکردند. صنعت می ترسید که، با وجود مرجع درست اطلاعات و یا CSIRT در مورد حوادث فردی اگر به اطلاع عموم مردم برسد (که آگاهی عمومی در آن ضروری است)، نیاز به گزارش نقض شدگی قابل توجهی است که خطر بالقوه آسیب رسیدن به شهرت آنها و در نتیجه از دست دادن اعتماد مصرف کننده را در پی دارد[186]. چالش دیگری که در این زمینه مطرح می شود این است که برای ایجاد یک سطح افشای به اندازه کافی بالا، متقاعد کردن کاربران برای نصب پچ (Patch) است، که باعث می شود، سطح پایینی از هکرها توانایی مهندسی معکوس برای بهره برداری بر اساس افشای عمومی اطلاعاتی انجام دهند[187].

5. مقررات و جایگزین آن برای روش های خاص

5.1 نکات کلی

دنیای دیجیتال، که در آن IoT نصب شده است، توسط هیچ شخصی کنترل و اداره نشده است[188]. هزاران مورد، از جمله شرکت ها، سازمان های بین دولتی و دولتی برخی کنترل های اضافی را در اینترنت و فضای مجازی دارند[189]. علاوه بر این، دنیای دیجیتال پیچیده و بسیار پویا است. از این منظر، مقرراتی که مدعی سروکار داشتن با حالت سایبری هستند باید به اندازه کافی انعطاف پذیر و آینده گرا [190] ساخته شوند که برای جلو ماندن منحنی تهدید سایبری در حال تحول، مطمئنا کار دشواری (اگر نگوییم غیر ممکن) خواهد بود.

بخش 5 .2 به بررسی این مسئله می پردازد که آیا مقررات IoT مورد نظر، ممکن است در این مرحله از توسعه

IoT مورد نیاز باشد. بخش 5 . 3 به بررسی یک جایگزین ممکن برای روش های سنتی نظارتی بر اساس تئوری مقررات چند مرکزی می پردازد.

5.2 زیست پذیری یک قانون اینترنت اشیا خاص

درحالیکه فعالیت های منظم همچون دستور دهنده NIS (بخش 4 . 3) روی اهمیت امنیت در ابزارهای متصل و سیستم ها تاثیر خواهد گذاشت [191]، سوالی که موضوع قالب توجه بحث است این است که آیا قانون IoT –خاص در این زمان ضروری و مناسب است.

در سال 2012 کمیسیون مشاوره عمومی اروپا، که توجه زیادی به خود جلب کرد، [192]، دیدگاه متفاوتی در این مورد دریافت کرده است[193]. با توجه به امنیت و ایمنی شخصی در IoT چند نقش آفرین صنعتی ادعا کرده اند که قوانین اضافه مورد نیاز نیست و باید در هر رویداد خاص باشد[194]. به طور خاص این پاسخ دهندگان در برابر مقررات بیش از حد و ایجاد موانع منظم غیر ضروری در یک محیط متشنج سریع اخطار داده اند[195]. برعکس، اکثریت بزرگی از پاسخ دهندگان نیازهای خود را برای دستور العمل ها و استانداردها مطرح می کنند، چندین تن از آنها بر ضرورت همکاری های بین المللی در"اینترنت در سطح جهان عامل" تاکید می کنند[196]. اکثریت پاسخ دهندگان بیشتر پذیرفته اند که دستورالعمل ها و استانداردها باید برای حفاظت از سه گانه سازمان سیا در زمینه اینترنت اشیا ایجاد شده باشند[197].

به علاوه تعداد زیادی از پاسخ دهندگان اظهار دارند که دستورالعمل ها و استانداردها باید توسعه یافته باشند "در چارچوب نگهدارند چندگانه با مشارکت سازمان های مصرف کننده جامعه مدنی و مقامات نظارتی علاوه بر مقامات دولتی و سهامداران خصوصی"[198]. مشاوره همچنین، سازمان و امکان اجرای روشهای یک چارچوب نظارتی IoT ممکن را بررسی می کند[199]. بعنوان یک موضوع عمومی یک حوزه قابل توجهی بین صنعت و دانشگاهیان مشروعیت مداخله دولت در یک میدان که هنوز در مراحل اولیه اش است را مورد سوال قرار می دهد[200].

در همین حال، در گزارش کارکنان سال 2015 [201] در رابطه با این موضوع، کارکنان کمیسیون تجارت فدرال

آمریکا اعلام کردند که قانون IoT – خاص در این زمان " زودرس" خواهد بود و در عوض باید به تشویق توسعه خود نظارتی برای بخش صنعت، به منظور بهبود امنیت (و حفظ حریم خصوصی) پرداخت[202].

در مارس سال 2015، کمیسیون اروپا اتحاد لازم برای نوآوری در اینترنت اشیاء (AIOTI) را ارائه داد، که هدف آن ارائه یک نقشه راه برای IoT در سال 2020 بود[203]. در اکتبر سال 2015، AIOTI ، 12 گزارش منتشر کرده [204]، که تعیین و تنظیم مجموعه چهار گانه به منظور " توصیه برای کار مشترک آینده در زمینه اینترنت اشیاء در افق سال 2020 " و پوشش مناطق اصلی با تمرکز بر برنامه IoT در سال 2016- 2017 بود که شامل، " مسائل مرتبط با سیاست" برای گزارش[205]، (AIOTI WG04 : گزارش در مورد مسائل سیاسی)کار آنها می باشد. این سوال مطرح می شود که آیا ظهرو IoT مستلزم مقررات جدید AIOTI WG04 در نتیجه منفی می باشد، با این استدلال که هر پیشنهاد نظارتی با هدف قرار دادن IoT باید در بازارهای تعریف شده منجر به شکست شود و نتواند از طریق معیارهای قانونی رسیدگی شود[206]. AIOTI همچنین به خطر خطای نظارتی در یک محیط پیچیده و سریع، مانند IoT می تواند منجر شود[207].

5.3 آیا مقررات چند مرکزی می تواند به عنوان یک مدل در نظر گرفته شود؟

همانطور که در بالا گفته شده، برای تعدادی از سهامداران، از جمله EU [208] آشکار است، برای حمایت، ازس روش سهامداران چندگانه شامل بخش عمومی و خصوصی، به منظور رسیدگی به مشکل جهانی و جمعی از امنیت سایبری [209]،در زمینه IoT استفاده می شود.

یک روش برای مقابله با چالش های امنیتی در حال انجام در IoT می تواند استفاده از قانون چند مرکزی باشد[210].

مقررات چند مرکزی می تواند بصورت " شرکتی از پیش تعیین شده که در معرض رفتار انسانی برای حکومت خارجی، چه دولتی و چه غیر دولتی، در نظر گرفته شده و یا ناخواسته است" تعریف شده است[211]. نظریه مقررات چند مرکزی متمایز از نظریه های نظارتی است[212]. بطور خاص، در تضاد با روش های دولت محور با توجه به

حاکمیت اینترنت و امنیت فضای مجازی است که توسط تعدادی کشورها اجرا می شود[213]. در واقع، مقررات چند مرکزی بر حکومت ذینفعان و بر خود قانونی متمرکز است[214].

در یک سیستم چند مرکزی (سایبری) حکومت سهامداران (ذینفعان) قادر خواهد بود بیشترین آشنایی با این موضوع را برای تعیین قوانین پس از آن وضع کند[215]. برخی از سهامداران موقعیت خوبی در این زمینه در بخش خصوصی دارند، که هر دو زمینه توسعه فن آوری و سهام دارانی که مالک آنها هستند را به کنترل (بخش مهمی از) فضای سایبری وا می دارد[216]. حاکمیت چندمرکزی موثر با هدف افزایش امنیت سایبری با " قوانین و هنجارها؛ مشوق های مبتنی بر بازار، کد، خود تنظیمی؛ مشارکت دولتی و خصوصی و همکاری های دو جانبه منطقه ای و چند جانبه ترکیب شده است [217].

مقررات چند مرکزی به طراحی فعالیت های قانون سازی که به روش مسائل حقوقی احتمالی در فضای مجازی نیاز نباشد کمک می کند. علاوه بر این، تمایز کارکردی با توجه به نیاز داشتن به داده ها می باشد[218]. چنین رویکردی مدل هندسه متغییر است که با توجه به شرایط ضمنی تنظیم شده اعمال می شود.

با این حال، در حالی که می دانیم مدل چند مرکزی دارای مزایایی منحصربفردی است، اما هیچ سیستمی کامل نیست و سیستم چندمرکزی مستثنی از این معیار نمی باشد. نقاط صعفی که در روش چند مرکزی وجود دارد شامل، این واقعیت است که این روش مسائل مربوط به قانون سازی و چند وجهی شدن قانون را در نظر نمی گیرد (و می تواند در نتیجه بطور بالقوه منجر به مجموعه قوانین ناهماهنگ می شود) [219]. علاوه بر این، این روش مسائل مربوط به مشروعیت و نبود دموکراسی را افزایش می دهد[220]، و همچنین مسائل ناشی از عدم وجود یک سلسله مراتب تعریف شده که باعث می شود اقدامات هماهنگ دشوار شود[221].

با وجود این نقاط ضعف، دخالت تمام سهامداران در روش قانون سازی که مرتبط با IoT است می تواند به ایجاد افزایش اعتبار با توجه به اقداماتی که صورت می گیرد، کمک می کند. علاوه بر این، واضح است که مشارکت بخش خصوصی برای یک عامل مهم به منظور رسیدگی کافی به مسائل و مشکلات مواجه شده در حال ظهور سیستم IoT است.

6 . چشم انداز

ثابت در حال تغییر (در امنیت سایبری) : چشم انداز سایبری به دلیل سرعت فوق العاده خطرناک تغییرات فناوری، پیچیدگی حمله، ارزش اهداف بالقوه و اثرات ناشی از حملات، در میان چیزهای دیگر به طور مداوم در حال تغییر و تکامل است[222].

با توجه به ویژگی های آن IoT چالش های منحصر به فرد را پیش رو قرار می دهد و نیازمند روش های نوین برای امن کردن داده و عملکرد آن است[223] . هر ابزاری که به اینترنت وصل می شود با "تهدید هایی با تمام قوا" مواجه می شود[224]. در دنیای که حمله کردن از دفاع کردن بینهایت آسان تر و از لحاظ پتانسیل شدید هستند. با توجه به انفجارهای اخیر در استفاده از وسایل به هم مرتبط آسیب پذیر، بهبود امنیت در IoT یک مسئله ی بحرانی، فوری و مانند هر شئ سایبری، جهانی است.

جابجایی تکنولوژیکی IoT نیازمند چارچوب قانونی شفاف است [225] . سختی کار بر روی توانایی انعطاف چارچوب ها قرار میگیرد که به اندازه کافی مبتکرانه و انعطاف پذیر باشد تا بتواند با به سرعت با محسط تهدید کننده ذاتی تکنولوژی توسعه پیدا کند[226]. در حالی که در این عرصه پیشرفت هایی نیز بدست آمده است، یعنی در درون EU(حداقل بر روی کاغذ)، اما هنوز سوال باقی مانده این است که چگونه اسناد حقوقی اخیرا به تصویب رسیده است.

تقویت امنیت سایبری بطور کلی و در زمینه IoT باید وجو داشته باشد، با این حال، محدود به قانون و یا روش های نظارتی نمی باشد. در عوض، مقررات ایجاد شده در این زمینه باید اجزای مختلفی را به دور هم جکع کند (در حال حاضر در حال انجام است)، که از جمله، حکومت پایین و بالا و پویا، مقررات سهامداران چندگانه می باشد که باید بطور بالقوه از طریق یک رویکردچند مرکزی انجام شود[227].

منبع

1. سو پورمبا – اینترنت اشیا که دارای تعداد زیادی از مشکلات سایبری است (ژانویه 2015) http://www.forbes.com/sites/sungardas/2015/01/29/the-internet-of-things-has-a-growing-number-of-cyber-security-problems/#1c56d59c4a47.

2 . همه وب سایت ها در 25 مه 2016 دیده شد.

3 . با توجه به ITU، یک حمله سایبری زمانی رخ می دهد که " تهدید نقض کنترل های امنیتی در اطراف ساختار فیزیکی یا دارایی اطلاعات رخ دهد" (ITU امنیت سایبری راهنمای استراتژی ملی) (سپتامبر 2011)، ص16، http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

4 . خیاتی جین- این صفحه 7 حملات سایبری وحشیانه ثابت که هیچ کس در برابر هک ایمن نیست - بخش اول (سپتامبر 2015)، , http://thehackernews.com/ 2015/09/top-cyber-attacks-1.html. همچنین نگاه کنید به زمان واقعی نقشه حمله سایبری از نورس پارسیان (یمستقر در کالیفرنیا امنیت سایبری فیرم) در http:// map.norsecorp.com/.

5 . تارا سیلز - 2014 تا کنون: سال نقض داده ها (اوت 2014)، http://www.infosecurity-magazine.com/news/2014-the-year-the-data-breach/; Ponemon of موسسه نظر سنجی، 2014: یک سال از نقض مگا (ژانویه 2015)، http://www.ponemon.org/blog/2014-a-year -of-mega-breachesچاد همنوی، نگاهی به سال 2014: در سال نقض داده ها (ژانویه 2015)،. http://www.cyberrisknetwork.com/ 2015/01/01/look-back-2014-year-of-the-breach/

7 . دن لورمن، 2015: نقش داده ها (دسامبر 2015)، http://www.govtech.com/blogs/lohrmann-oncybersecurity/2015-the-year-data-breaches-became-intimate.html.

8 . برای به دست آوردن یک حس تنوع و تعداد حملات در حال حاضر و، به عنوان مثال، گزارش اخیر آژانس اتحادیه اروپا برای شبکه و امنیت اطلاعات "ENISA تهدید چشم انداز 2015" (ژانویه 2016)، ص. 5، https://www.enisa.europa.eu/

9 . ENISA، چشم انداز تهدید 2015 ((8 .N، ص. 6 و ص 54.

10 . کاساندرا کیروش، هکر کلا خاکستری: آشتی فضای مجازی، واقعیت و قانون، شمال کنتاکی بررسی قانون (2014)، P.383 ff، P.385 http://www.academia.edu/4721959/Grey_Hat_Hacking _Reconciling_Law_with_Cyber_Reality; AnthonyWing Kosner, Target Breach Of 70 Million Customers' Data Used Bargain Basement Malware (January 2014), http://www.forbes.com/sites/anthonykosner/2014/ 01/15/blackpos-malware-used-in-target-attack-on-70-million-customers-retails-for-1800/#402f5612530d; همچنین وبلاگ موسسه INFISEC : 25 روش برای تبدیل نهایی سند دارد (آکوست 2015)، http://resources.infosecinstitute.com/25 -ways-to-become-the-ultimate-script-kiddie/.

11 . سامانتا بردشاو، مبارزه با تهدیدهای سایبری: CSIRTها و همکاری بین المللی در امنیت سایبری، کمیسیون حاکمیت اینترنتی (دسامبر 2015)، P.6 https://www.cigionline.org/publications/combatting-cyber threatscsirts- and-fostering- international-cooperation-cybersecurity; همچنین گزارش اخیر آزمایشگاه McAfee " پیش بینی تهدیدات 2016" (2015)، . p 21، گزارش آزمایشگاه McAfee در سال 2016 پیش بینی تهدیدات.

12. دبرا دانستون-میلر، اینترنت اشیاء، چالش های امنیتی جدید(فوریه 2014)، , http://www.forbes.com/sites/sungardas/2014/02/25/the-internet-of-things-poses-new-security -challenges/#30b9afde2696; اومنر براجانس، چگونگی تغییر اینترنت اشیاء (IoT) در چشم انداز امنیت سایبری (سپتامبر 2014)، https:// securityintelligence.com/how-the-internet-of-things-iot-is-changingthe- cybersecurity-landscape/; جاناتان کاملی؛ دستگاه های IoT آسیب پذیر در حال تغییر در چشم انداز امنیت سایبری (فوریه 2016)، http:// uk.businessinsider.com/iot-devices-are-changingcybersecurity?r=US&IR=T.

13 .گزارش اخیر از هیولت پاکارد، تحقیقات در مورد اینترنت اشیاء ، گزارش 2015، P.3، http:// www.hp.com/h20195/V2/GetPDF.aspx/4AA5-4759ENW.pdf; همچنین، جامعه اینترنتی ، اینترنت اشیاء: مرورکلی سال 2015، P.2، https://www.internetsociety.org/ sites/default/files/ISOC-IoT-Overview 20151014_0.pdf.

14 . کریستوفر رنندز و دبلیو دیوید استفنسون، امنیت مجازی در اینترنت اشیا(ژوئن 2013)، https://hbr.org/2013/06/cyber -security-in-the-internet/

15 . هیولت پاکارد، اینترنت اشیا مطالعه تحقیقاتی ((n.13)، ص. 3؛ انجمن اینترنت، اینترنت اشیا بررسی اجمالی (. (N 13)، ص. 2.

16 . گری دیویس، مراقب باشین : ' طوفان کامل امنیتی " به زودی (سپتامبر 2015)، https://blogs.mcafee.com/consumer/ august-threats-report-2015/.

17 . کریستوفر جی. رزند و دیوید دبیلو. استفنسون، امنیت سایبری در اینترنت اشیاء (ژوئن 2013)، https://hbr.org/2013/06/cyber - security-in-the-internet; ENISA, Threat Landscape 2015 (n. 8), P.68 ؛ آزمایشگاه ،McAfee ، پیش بینی تهدیدات سال 2016 (n.11)، P.7.

18 . این مقاله به بررسی مسائل سیاسی نپرداخته است که در ارتباط با اینترنت اشیاء می باشد. برای مرور کلی انی موضوع، مرجع رولف اچ. وبر را مشاهده کنید، اینترنت اشیاء : مسائل حریم خصوصی، قانون رایانه ها و نقد و بررسی امنیت (2015) 627-18 .P

19 . در این موضوع، و به عنوان مثال، نازلی چوسری، البات گیهان داو، مدنیک استوارت، چرا امنیت سایبری؟ اکنتشاف در تولید دانش خودکار، (2012) http://ecir.mit.edu/images/stories/Madnick%20et %20al%20Comparison%20Paper%20for%20ECIR%20workshop%20%20Fig%201%20also%20FIXED%20v 2.pdf ، تیم مورر و رابرت مورگان، امنیت سایبری و تعریف چرایی ریسک (نوامبر 2014)، http://isnblog.ethz.ch/intelligence/cybersecurity-and-the -problem-of-definitions; تری هر و آلن فرید من، تعریف دوباره امنیت سایبری، شورای آمریکایی سیاست خارجی ، (ژانویه 2015) http://www.afpc.org/publication_listings/viewPolicyPaper/2664.

20 . چوکری و گیهان داو و استوارت (19 .n)

21 . انجمن اینترنت، چند دیدگاه در امنیت سایبری: 2012 (2012)، ص. 1 http://www.internetsociety.org/doc/some- perspectives -cybersecurity-2012.

23 . ITU تعریف امنیت سایبری

24 . در همان منیع

25 . در همان منیع

26. توماس جی. شاو، امنیت اطلاعات و حریم خصوصی: راهنمای عملی مدیران، وکلا و کارشناسان فن آوری (2011)f P.18 ، اکسل ام. آرن باک، ارتباط خصوصی امنیتی : حفاظت امنیت ارتباطات خصوصی در قانون EU: حقوق اساسی، زنجیره ارزش کاربردی و مشوق های بازار، آمستردام (2015)، P.30 و f 155 .

27 . ITU تعریف امنیت سایبری

28 . شاو (26 N)، ص 18

29 . در همان منیع

30 . در همان منیع

31 . یک تهدید در این زمینه عبارت است از پتانسیلی در هر نهاد برای استفاده از آسیب پذیری و یا به عبارت دیگر دلیل آسیب پذیری (شاو (n.26)، .(p.161).

32. گزارش پارلمان اروپا، امنیت سایبری در اتحادیه اروپا و فراتر: بررسی تهدیدات و واکنش های سیاسی، مطالعه کمیته LIBE، 2015)، P .26 ff، http:// .www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU%282015%29536470_EN.pdf

34 . در همان منبع

35 . در همان منبع

36 . شاو (n.26)، .(p.162).

37 . در همان منبع

38 . این بدافزاری کوتاه مدت برای نرم افزار های مخرب است.

39 . سوزان دبلیو برنر، جرایم اینترنتی و قانون: چالش ها، مسائل، و نتایج (دانشگاه شمال شرقی 2012)، FF p.36؛ ;کیسان و مولینز هیز (N 33)، ص. 3.

40 . باتنت ترکیبی از ربات شرایط و شبکه است.

41 . تعریف تروجان: پرسش و پاسخ ;https://technet.microsoft.com/en -us/library/dd632948.aspx

42 .گزارش آزمایشگاه های مک کافی، 2016 پیش بینی تهدید (N 11)، ص. 35.

43 . در همان منبع

44 . کیم زتر، واژه نامه هکر: راهنمای بد افزار-هک که در حال افزایش است (سپتامبر 2015)، https:// www.wired.com/2015/09/hacker-lexicon-guide-ransomware -scary-hack-thats-rise/.

45 . ENISA، تهدید چشم انداز 2015 (N. 8)، ص. 25-26؛ همچنین پست توسط نورتون، رباتها و بات نت را ببینید - تهدید در حال رشد، http://us .norton.com/botnet/.

46 . ENISA، تهدید چشم انداز 2015 (N. 8)، .p.19

48 . نورین سیبچر، شما می توانید یک وب سایت را برای $ 38 پایین بیاورید (ژوئن 2015)، http://www.cmswire.com/information- management/you -can-bring-down-a-website-for-38/.

49 . ENISA، تهدید چشم انداز 2015 (N. 8)، ص. 26.

50 . دیو مک میلن، چرا بات نت به عنوان یک سلاح برای مجرمان سایبری باقی میماند (مارس 2016) https://securityintelligence.com/why -botnets-remain-the-go-to-weapon-for-cybercriminals/.

51 . ENISA، تهدید چشم انداز 2015 (N. 8)، ص. 75

52 . جی پی کیسان و کارول مولینز هیز (n. 33) ص3

53 . گزارش آزمایشگاههای مک کافی 2016 پیش بینی تهدید (N 11)، ص. 34.

54 . در همان منبع

55 . کوین اشتون – اینترنت اشیا ژورنال RFID (n. 11) ص 34 http://www.itrco.jp/libraries/RFIDjournal-That%20Internet %20of%20Things%20Thing.pdf.

56 . جامعه اینترنت اینترنت اشیا (n. 13) ص 11

57 . در همان منبع ص 7

58 . ITU-T توصیه Y.2060، بررسی اجمالی از اینترنت اشیا (2012/06)، ص 2

59. آلاآل- فقها، محین گویزانی، مهدی محمدی، محمد آلدهاری و موسی آیش، اینترنت اشیاء: بررسی تکنولوژی های فعال، پروتکل ها و برنامه ها، IEEE ، بررسی ارتباط و آموزش، (2015)، P.2347، http://www ..comsoc.org/files/Publications/Tech%20Focus/2016/iot/3.pdf

60 . پیشنهادی از (N 58) (06/2012) ITU-T Y.2060، ص. 1.

61 . جامعه اینترنت اینترنت اشیا (n. 13) ص 11

62 . اویدیو ورمسان و همکاران، اینترنت اشیاء و تحقیقان استراتژیک و نوآوری، در اینترنت اشیاء –از تحقیق و نوآوری بازار، او. ورمسان و پی. فریس (eds)، ناشر، رودخانه ناشران سری، P.30 ff، http://www .internet-of-things- research.eu/pdf/IERC_Cluster_Book_2014_Ch.3_SRIA_WEB.pdf; استن اشنایدر، درک پروتکل پست اینترنت اشیاء (اکتبر 2013)، http://electronicdesign.com/iot/understanding-protocols-behind-internet-things.

63 .اسکات شاکل فورد، آنجنتا ریموند، راکشانا بلککیرشن، پارکر دیکسیت، جولیانا گژاآنگج و راکتیج کاوی، زماین که توستر حمله می کند، ؛ روش چند مرکزی برای بهبود اینترنت اشیاء، مدرسه کلی، (ژانویه 2016)P.9؛

64 . بنجامین خو، RFIDبه عنوان یک توانمند یاز اینترنت اشیاء : مسائل حریم خصوصی و امنیتی، کنفرانس جهانی 2011 در مورد اینترنت اشیاء، p.709، http://ieeexplore.ieee.org/ stamp/stamp.jsp?arnumber=6142169;

65 . د لی یانگ فنگ لیو و یی دیو لیانگ، بررسی اینترنت اشیا ، مجموعه مقالات. 1 (2010) ICEBI، ص. 358؛ گوارزو(N 64) ،ص. 1.

66 . متیو تروتر، RFID اینترنت اشیا را برای زندگی می سازد، طراحی ماشین آلات (مه 2014) http://machinedesign.com/iot/rfid -makes-internet-things-come-life.

67 . برای اطلاعات بیشتر نگاه کنید به رولف اچ وبر و رومانا وبر، اینترنت اشیا، دیدگاه حقوقی (2010)، ص. 2 F؛ گوارزو(N 64) ، ص. 3.

68 . گوارزو (n. 64) ص 3

69 . در همان منبع

70. آلیسو بوتا، والتر دی دوناتو، والریو پرسیکو و آنتونیو پس کیب، یکپارچه سازی رایانش ابری و اینترنت اشیاء، کنفرانس بین المللی سال 2014- آینده اینترنت اشیاء، P.29

71 . رولف اچ وبر، اینترنت اشیا - نیاز به یک محیط قانونی جدید؟، کامپیوتر و نقد و بررسی قانون و امنیت (2009)، ص. 522 .F

72 . در همان منبع

73 . در همان منبع

74 . در همان منبع

75 . گزارش Capgemini مشاور "ایمنی اینترنت اشیا : قرار دادن امنیت سایبری در قلب اینترنت اشیا» (2015)، ص. 3 https://www.capgemini-consulting.com/ resource-file-access/resource/pdf/securing_the_internet_of _things.pdf.

76 . گزارش سیسکو "ایمنی اینترنت اشیا: یک چارچوب پیشنهادی" - http://www.cisco.com/c/en/us/about/security center/secure-iot-proposed-framework.html.

78 . سخنرانی راد بکستورم در کنفرانس لندن در فضای مجازی (نوامبر 2011)، https://www.icann.org/en/system/files/ files/beckstrom-speech-cybersecurity-london-02nov11-en.pdf.

79 . با توجه به اینترنت اشیاء ، اینترنت اشیاء در تیم باجارین، (ژانویه 2014) http://time.com/539/the-next-big-thing -for-tech- the-internet-of-everything/.

80. سیستم حمله می تواند بصورت زیر مجموعه ای از تعریف منابع مهاجم برای حمله به سیستم استفاده کند(پرات یاسا ک. مانادهاتا و جنتل دبیلو و وینگ، سطح حمله متریک، در IEEE،)

81. بنوا برادشاو (n.11)، P.8، همچنین گزارش EY در امنیت سایبری و اینترنت اشیاء، p.8 ff، http:// www.ey.com/Publication/vwLUAssets/EY-cybersecurity-and-the -internet-of-things/$FILE/EY- cybersecurity-and-the-internet-of -things.pdf;

82 . گزارش آزمایشگاه های مک کافی 2016 تهدید پیش بینی ها (n. 11) ص 13

83 . گارتنر آزادی مطبوعات "گارتنر می گوید 6.4 میلیارد اشیا متصل شده از 2015 تا سال 2016 تا 30 درصد افزایش میابد " (نوامبر 2015)، http://www.gartner.com/newsroom/id/3165317

84 مقاله سیسکو سفید "اینترنت اشیا سیستم های امنیتی: کاهش ریسک، ساده پذیرش و ایجاد اعتماد" (2015)، ص. 1، http:// www.cisco.com/c/dam/en/us/products/collateral/se/internet-of -things/iot-system-security-wp.pdf.

85 . مقاله های هواوی سفید "صفحه اول اتصال 2016" (2016)، ص. 43، http://www.huawei.com/minisite/gci/pdfs/Global_Connectivity_Index_2016_whitepaper.pdf

86 . انجمن اینترنت، اینترنت اشیا: بررسی اجمالی (n.13)، ص. 4.

87 . گوارزو(n.64) ، ص. 3؛ هیولت پاکارد، مطالعه تحقیقات اینترنت اشیا(.N 13)

88 . هیولت پاکارد، بررسی اینترنت اشیا (n.13)

89 . همچنین در همان منبع نگاه کنید به سیمانتک کاغذ سفید "ناامنی در اینترنت اشیا" (مارس 2015) https://www.symantec.com/content/ dam/symantec/docs/white-papers/insecurity-in-the-internet-of -things.pdf

90 . گزارش ورایزون "2015 گزارش داده تحقیقات " (2015)، ص. 63، http://www.verizonenterprise.com/DBIR/2015/

91 . در همان منبع

92 . شکلفورد، ریموند، بالاکریشناند در، دیکسیت، گوناج و از کاوی(n.63) ، ص. 14؛ گوارزو(n.64)، ص. 2؛ هیولت پاکارد، اینترنت اشیاء از مطالعه تحقیقاتی (n.13)؛ انجمن اینترنت، این اینترنت اشیا: بررسی اجمالی (N 13)، ص. 25

93 . گوارزو (n. 64) ص 3

94 . لیست های باز وب سایت برنامه پروژه امنیت (OWASP)از صفحه 10 کافی اعتبار / مجوز، https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient _Authentication/Authorization.

95 . گوارزو (n. 64) ص 3

96 . براد راسل، تهدید امنیت داده ها به اینترنت اشیا (نوامبر 2015) https://www.parksassociates.com/blog/article/data - security-threats-to-the-internet-of-things

97 . هیولت پاکارد، اینترنت اشیا مطالعه تحقیقات (n.13)؛ انجمن اینترنت، اینترنت اشیا: بررسی اجمالی (N 13)، ص. 23.

98 . جی پیل چوی، خایم فرشتمن و نیل گاندال امنیت شبکه: آسیب پذیری و سیاست افشا، 58 مجله اقتصاد صنعتی (2010)، ص. 869.

99 . چوی فرشتمن و گاندال (n. 98) ص 869

100 . گوارزو (n. 64) ص 3

101 . شاکلفورد – ریموند- بالاکریشناند – دیخیت – گوناج و کاوی (n. 63) ص 14

102 . گوارزو (n. 64) ص 1

103 . رحوع کنید به جان اولتیسک، اینترنت اشیاء: CISO و دیدگاه امنیتی شبکه (2014)f P.4، .pdf ;http://www.cisco.com/c/dam/en_us/ solutions/industries/docs/energy/network-security-perspective

104 . شاکلفورد – ریموند- بالاکریشناند – دیخیت – گوناج و کاوی (n. 63) ص 13

105 . جان گرینوف، 10 میلیون اتومبیل خود ران در جاده ها تا سال 2020 خواهد بود (جولای 2015)، http://www.businessinsider.com/report-10 -million-self-driving-cars-will-be-on-the-road-by-2020-2015-5 - 6?IR=T.

106 . گزارش آزمایشگاه های مک کافی- 2016 پیشبینی های تهدید(n. 11) ص 33

107. FTC گزارش کارکنان 2015 (N 103)، ص. هشتم

108. در همان منبع ص 55

109 . پست های ارسال شده توسط بروس اشنایر، داده یک دارایی مضر (مارس 2016) https://www.schneier.com/blog/archives/2016/03/data _is_a_toxic.html

110 . گزارش آزمایشگاه McAfee، 2016، پیش بینی های تهدیدات (n.11)، P.7 توسط برآورد، دیجیتال جهانی، http:// www.emc.com/leadership/digital-universe/2012iview/executive -summary-a-universe-of.htm.

111 . PersonalDataNewAsset_Report_2011.pdf_http://www3.weforum.org/docs/WEF_ITTC.

112 . پست های ارسال شده بروس اشنایدر، داده های رسمی ، is_a_toxic.html_https://www.schneier.com/blog/archives/2016/03/data.

113 . شاکلفورد – ریموند- بالاکریشناند – دیخیت – گوناج و کاوی (n. 63) ص 21

114 . فرگال گالاگر، هکرها از راه دور می توانند دوزهای کشنده را به بیماران از طریق ناقص پمپهای بیمارستان ارسال کنند (ژوئن 2015)، http://www .techtimes.com/articles/59180/20150609/hackers-remotely-send -fatal-doses-patients-via-flawed-hospital-pumps.htm.

115 . کونور گفی، وب ناامنی: کنترل نظارت بر کودک (هک شده) خطرات برجسته ای از اینترنت اشیا است (سپتامبر 2015) http://europe .newsweek.com/web-insecurity-hacked-baby-monitors-highlight -perils-internet-things-332464.

116 . کشمیر هیل، سازمان دیده بان، حقوق فرزند - مانیتور کودک متصل به اینترنت برای هک بسیار آسان است (سپتامبر 2015) http://fusion.net/story/ 192189/internet-connected-baby-monitors-trivial-to-hack/

117 . مایک اسپکتور و دنی یاردون، رگولاتور بررسی فیات کرایسلر امنیت سایبری را به یاد بیاورید (جولای 2015) http://www.wsj.com/articles/ fiat-chrysler-recalls-1-4-million-vehicles-amid-hacking-concerns -1437751526.

118 . آندریا استروپا, آیا ابزارهای مجهز به وب بی خطر است؟ (دسامبر 2015)، http://www.weforum.org/agenda/2015/12/are- web-enabled-toys -safe.

119 . در همان منبع

120 . برادشو (n. 11) ص 6

121 . همانطور که در مه 25 2016 72 عضو از 193 کشور ITU یک استراتژی امنیت سایبری ملی عمومی در دسترس داشتند http://www.itu.int/ en/ITU-D/Cybersecurity/Pages/National-Strategies-Repository .aspx.

122 . ENISA، تهدید چشم انداز 2015 (N. 8)، ص. 5.

123 . کنوانسیون جرایم اینترنتی – شورای کنوانسیون اروپا در جرایم اینترنتی، CETS 185، بوداپست نوامبر 2001 http:// www.coe.int/fr/web/conventions/full-list/-/conventions/rms/ 0900001680081561.

124 . برای بحث دقیق در مورد کنواسیون بوداپست، گزارش کنواسیون در مورد جرایم سایبری، https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?

http://www.coe.int/en/web/conventions/full-list/-.documentId=09000016800cce5b (cited Explanatory Report)

;treaty/185//conventions

125. http://www.coe.int/en/web/conventions/full-list/-/conventions / treaty/ ، برای جزییات دقیق در کنواسیون بوداپست، جهانی متفاوت: کنواسیون بوداپستدر امنیت سایبری و چالش های هماهنگ سازی، دانشگاه موناش(2014)P.698

126. http://www.coe.int/en/web/conventions/full-list/-/conventions/ treaty/185/signatures?p_auth=jnOd8Vj5.

127 . در همان منبع

128 . در همان منبع

129 . ژیون هانگ لیو، بیل هبنتون، سوسیان جو، هندبوک آسیایی جرم شناسی (2012)، ص. 58.

130. http://www.coe.int/en/web/conventions/full-list/-/conventions/ rms/0900001680081561

131 . توضیح گزارش (124 N)، ص. 9؛ همچنین (26 N) ،آرنباک ص. 61.

132 . توضیح گزارش (124 N)، ص. 9

133 . در همان منبع ص 8

134 . در مقدمه کنوانسیون بوداپست نیز به صراحت به مجموعه سه گانه سازمان سیا اشاره دارد.

135 . آرنباک (n. 26) ص 62

136 . کلاف (n. 125) ص702

137 . توضیحی گزارش (124 N)، ص. 7؛ کلاف (125 N)، ص. 703.

138 . توضیحی گزارش (124 N)، ص. 57؛

139 . کلاف (125 N)، ص. 703.

140 . توضیحی گزارش (124 N)، ص. 42؛

141 . کلاف (125 N)، ص. 701 ؛

142 . در همان منبع ص 732 و 736 . آرنباک (125 N) ص. 62.

143 . لیو، هبنتون و جو (129 N) ص. 60.

144 . جونز چمبر کلر، اقتصاد مجازی و جرم مالی: پولشویی در فضای مجازی (2012) ص. 202.

145 . لیو، هبنتون و جو (129 N) ص. 58؛ مارتین جیل، کتاب جیبی از امنیت (2014) ص. 334.

146 . انتشار کمیسیون اروپا (می 2015)

http://europa.eu/rapid/press-release_IP-15-4919_en.htm.

147.دستورالعمل پیش نویس در شبکه و امنیت اطلاعات (آزمون از متن سازش بسته به شرایط) اصلاح رسیتال 15

http://www.consilium.europa.eu/en/press/press-releases/2015/12/pdf/st15229-re02_en15_pdf/.

148 . انتشار کمیسیون اروپا (146 N)

149 . ارتباطات از کمیسیون به شورا، مجلس اروپا، اقتصاد اروپا، کمیته اجتماعی و کمیته مناطق، شبکه و امنیت اطلاعات: یک رویکرد برای یک پیشنهاد پلیسی اروپا (2001)

europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298. http://eurlex.

150 . مقررات (EC) شماره 2004/460 پارلمان اروپا و شورای 10 مارس 2004 ایجاد شبکه اروپایی و آژانس امنیت اطلاعات (2004)،

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML.

151 . در همان منبع

152 . شبکه ارتباطات و امنیت اطلاعات: یک رویکرد برای یک پیشنهاد پلیسی اروپا (149 N)

153 . قطع نامه شورا 2007/068/01

154 . ارتباطات از کمیسیون به پارلمان اروپا، شورای، کمیته اجتماعی و اقتصادی اروپا و کمیته مناطق انتقادی حفاظت اطلاعات زیرساخت (2009)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.

155 . مشاوره بر شبکه و امنیت اطلاعات – انتشار پاسخ فردی (جون 2013)

https://ec.europa.eu/digital-single-market/news/consultation-network-and-information-security-publication-

individual-responses.

156 . پیشنهاد برای یک دستورالعمل پارلمان اروپا و شورای باره اقدامات برای اطمینان از سطح مشترک بالایی از امنیت شبکه و اطلاعات در سراسر اتحادیه (2013)

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013PC0048.

157. مشاوره بر شبکه و امنیت اطلاعات – انتشار پاسخ فردی (N 155)

158. ارتباط مشترک به پارلمان اروپا، شورای، کمیته اجتماعی و اقتصادی اروپا و کمیته مناطق، استراتژی امنیت سایبری اتحادیه اروپا: باز، امن و مطمئن فضای مجازی (2013)،

http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667.

159. اسکات ج.شاکلفورد، اسکات روسل و جفری هویت، باسن بالا: مقایسه داوطلبانه قاب امنیت سایبری، دانشگاه دیویس مجله کسب و کار (2016)، ص. 20.

160. http://www.consilium.europa.eu/en/policies/cyber-security/.

161. شاکلفورد، روسل و هویت (N 159) ص. 20.

162.دستورالعمل پیشنهادی (N 156)

163. در همان منبع.

164. دستورالعمل پست کمیسیون اروپا، شبکه و امنیت اطلاعات: قانون گذاران شرکت موافق بودن بر اولین قانون اتحادیه اروپا در امنیت سایبری (دسامبر 2015)

https://ec.europa.eu/digital-single-market/news/network-and-information-security-directive-co-legislators-agree-first-eu-wide-legislation.

165. آزادی مطبوعات شورای اروپا، اقدامات اتحادیه اروپا امنیت سایبری: کشورهای عضو تصویب شرایط (دسامبر 2015)

http://www.consilium.europa.eu/fr/press/press-releases/2015/12/18-cybersecurity-agreement/.

166. شورای اروپا آزادی مطبوعات، قوانین امنیت سایبری اتحادیه اروپا پذیرفته شده توسط شورای (می 2016)

http://www.consilium europa.eu/en/press/press-releases/2016/05/17-wide-cybersecurityrule-adopted/.

167. پست کمیته اروپا (N 164)

168. شورای اروپا آزادی مطبوعات (N 165)، همچنین آزادی مطبوعات کمیسیون اروپا را ببینید، استقبال کمیسیون شرایط به محیط امن تر آنلاین اتحادیه اروپا (دسامبر 2015)

http://europa.eu/rapid/press-release_IP-15-6270_en.htm.

169. پست کمیته اروپا (N 164)

170. اعتماد به خدمات آنلاین پیش شرط برای بازار تنها اتحادیه اروپا دیجیتال است. فقدان یک استراتژی امنیت سایبری قوی (در میان چیزهای دیگر)، می تواند اعتماد وجود نداشته باشد. (http://www.consilium.europa.eu/en/policies/digital-single-market-strategy) اگر اعتماد را تضعیف است، صنعت فن آوری رنج می برد موانع و فن آوری می تواند به پتانسیل کامل خود برسد (نگاه کنید به شاکلفورد، رایموند، بالاکریشنان، دیکسیت، جوناج و کاوی (N 63)، ص.25)

171. پست کمیته اروپا (N 164)

172. انتشار مطبوعات کمیته اروپا (N 168) و همچنین پست کمیته اروپا در سایبری (آپریل 2016)

https://ec.europa.eu/digital-single-market/en/cybersecurity.

173.CSIRT ها اغلب به عنوان "آتش نشان" از فضای مجازی دیده شود (نگاه کنید به بنوا (N 11) ، ص 6، با استناد به عاطف احمد، جاستین هادکیس و AB رویگاور و، تیم واکنش حادثه - چالش ها در حمایت از عملکرد امنیت سازمانی، قانون رایانه ها و امنیت مرور (2012) ص.643،

http://www.sciencedirect.com/science/article/pii/S0167404812000624

174. دستورالعمل پیش نویس NIS ، ضمیمه 2

175. دستورالعمل پیش نویس NIS، اصلاح خوانی 27

176. توصیه های کمیسیون اتحادیه اروپا در رابطه با تعریف میکرو، شرکت های کوچک و متوسط (می 2003)

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:124:0036:0041:en:PDF.

177. دستورالعمل پیش نویس NIS، اصلاح خوانی 24(a)

178. اگر چه این مقاله به دستورالعمل عمومی حفاظت از اطلاعات (GDPR)، در سال 2018 مورد بحث نیست. باید توجه داشت این است که برخی همپوشانی بین GDPR و دستور NIS وجود دارد. هر دو ابزار نیاز به اپراتورهای / ارائه دهندگان به اجرای اقدامات امنیتی و هر دو پیش بینی مورد نیاز اطلاع رسانی در صورت حادثه. با این حال، منافع است که با هدف راهنماها برای محافظت های مختلف (اطلاعات شخصی در مقابل امنیت شبکه) و انواع حوادث است که تحت دامنه خود را قرار می گیرند ممکن است متفاوت باشد (نگاه کنید به گیب مالداف، NIS + GDPR = یک رژیم نقض جدید در اتحادیه اروپا (دیسامبر 2015) https://iapp.org/news/a/nis-gdpr-a-new-breach-regime-in-the-eu/ بعلاوه برخی از تنش بین GDPR و دستور NIS اگر آنها را تحت امنیت در مقابل پارادایم حریم خصوصی در نظر دارد. تا به امروز هیچ راهنمایی در مورد چنین همپوشانی / تنش وجود ندارد.

179. https://ec.europa.eu/digital-single-market/en/news/presentation-ncsc-one-conference-2016.

180. مارکو گریک، دیر انتاراف فور ایین اتحادیه اروپا ریچتیلینی عابر نتز – عاند اطلاعات سیچرهیت (NIS) کامپیوتر و ریچ (جانیوری 2016)، ص. 30

181 . برای مثال، موقعیت Euractiv در آزادی مطبوعات خود، پاسخ به استراتژی امنیت سایبری اتحادیه اروپا و دستورالعمل ازائه شده در شبکه و امنیت اطلاعات (NIS)(فوریه 2013)/http://pr.euractiv.com/pr/ response-eu-cybersecurity-strategy-and-proposed-directive-network-and-information-security-nis.

182 . جیمز هارون و ژان دونت، حریم خصوصی و امنیت داده: حتی بیشتر مقررات داده های EU . دستورالعمل امنیتی اطلاعات شبکه (مارس 2016) http://www.alstonprivacy.com/alston-birdissues- cyber-alert-network-information-security-directive/.

183 . گزارش چشم انداز اقتصادی دیجیتال از BBVA، " دستورالعمل شبکه و امنیت اطلاعات (NIS): بخش 2 از 2 (مه 2016)P.9 https://www.bbvaresearch.com/wp-content/uploads/2016/05/ DEO_May16_Cap3.pdf.

184 . BBVA،" دستورالعمل شبکه و امنیت اطلاعات (NIS): بخش 2 از 2 (مه 2016)P.9

185 . همان منبع

186 . گزارش صنعت و پارلمان " امنیت سایبری 2.0 " ، P.11، http://www.ipt.org.uk/Portals/0/Cyber %20Security%20Commission2%20%282%29%20for%20website.pdf.

187. کسان و مولینز هیز (n.33) p.39

189 . اسکات جی. شاکل فورد، به سوی فضای سایبری : مدیریت سایبری از طریق حکومت، نقد و بررسی از دانشگاه های آمریکا (سال 2013) http://digitalcommons.wcl.american.edu/cgi/ viewcontent.cgi?article=1888&context=aulr،p.1303.

189 . شاکل فورد (N.188)، p.1285.

190 . برای مروری کلی، رولف اچ. وبر، تحقق یک چارچوب فضای سایبری جدید ، مبانی هنجارها و اصول راهنما (2014)، p158-159

191 . گزارش از AIOTI WG04 " گزارشی در مورد مسائل سیاسی" (اکتبر 2015)، P.16 https://ec.europa.eu/digital-single-market/ en/news/aioti-recommendations-future-collaborative-work -context-internet-things-focus-area-horizon-2020.

192 . بیش از 600 پاسخ دهنده، از جمله سازمان های جامعه معدنی، دانشگاهیان و بازیگران صنعت در مشاوره شرکت کرده اند

193 . گزارش کمیسیون اروپا در مشاوره عمومی در مورد حاکمیت IoT، P.3، https://ec.europa.eu/digital -single-market/en/news/conclusions-internet-things-public -consultation.

194 . در همان منبع. P.5

195 . در همان منبع

196 . در همان منبع

197. در همان منبع، P.5-6

198 . در همان منبع، P.6

199 . در همان منبع، P.13

200 . در همان منبع، P.15؛ همچنین رولف. اچ. وبر، اینترنت اشیاء – حاکمیت موجود ؟ قاونو رایانه ها و نقد و بررسی امنیت (2013)، f P.314،

201 . خلاصه ای از گزارش با عنوان " اینترنت اشیاء : حفظ حریم خصوصی و امنیت در جهان متصل " (برگزار شده در نوامبر 2013) و مجموعه چهارگانه توصیه کارکنان در این منطقه

202 . گزارش کارکنان FTC 2015 (n.103)، P.vii،

203 . https://ec.europa.eu/digital-single-market/alliance-internet -things-innovation-aioti.

204 . https://ec.europa.eu/digital-single-market/en/news/aioti -recommendations-future-collaborative-work-context-internet -things-focus-area-horizon-2020.

205 . http://ec.europa.eu/newsroom/dae/ document.cfm?action=display&doc_id=11815.

206 . AIOTI WG04 : گزارش در مورد مسائل سیاسی (191. n)، P.4

207 . AIOTI WG04 : گزارش در مورد مسائل سیاسی (191. n)، P.4

208 . استراتژی امنیت سایبری اتحادیه اروپا: فضای سایبری باز، امن و مطمئن (n.158)

209 . شاکل فورد، راسل و هات (N. 159)، P.1

210 . ساکل فورد (188 .n)، P.1360. برای جزئیات بیشتر، وبر را مشاهده کنید (190 .n)، P.90-91

211. وبر را مشاهده کنید (190 .n)، p.91 (به نقل از د. موری، مقررات فضای مجازی: کنترل در محیط آنلاین، میلتون پارک (2007)، P.47 و p.234-235).

212 . ساکل فورد را مشاهده کنید (n.188)، P.1348

213. در همان منبع. P.1333

214 . در همان منبع. P.1350، با این حال، هرچند جنبه های مهم چند مرکزی حاکمیت، خود تنظیمی به منزله جزئی از نظریه چند مرکزی می باشد (شاکل فورد، ریموند، بلکریشاین، دیکسیت، گژاآنج و کاوی (63. n)، P.23-24)

215 . شاکل فورد را مشاهده کنید (n.188)، P.1353؛ رولف. اچ .وبر، حاکمیت در اینترنت اشیاء – از دوران کودکی و تلاش برای اجرا؟ قوانین (آینده)

216 . شاکل فورد را مشاهده کنید (188 .n) ، P.1285 و P.1362؛ همچنین داشبورد امنیت سایبری BSA EU (2015) ، P.6، http://cybersecurity.bsa.org/ assets/PDFs/study_eucybersecurity_en.pdf.

217 . شاکل فورد را مشاهده کنید (188 . n)، P. 1285

218 . وبر را مشاهده کنید (n.190)، P.92

219 . در همان منبع ، P.91

220 . در همان منبع ، p.91

221 . شاکل فورد، ریموند، بلکریشان، ریکسیت، گژاآنگ و کاوی (n.63)، p.5 و p.36

222. گزارش McAfee، 2016، پیش بینی تهدید(11 . n)، p.34-

223 . ENISA، چشم انداز تهدید 2015، (n.8) P.68

224 . گزارش McAfee، 2016، پیش بینی تهدید(11 . n)، p.21-

225. داشبورد امنیت سایبری BSA EU (216. n)

226 . در همان منبع

227 . شاکل فورد را مشاهده کنید (n.188)، P.1360