فصلنامه مطالعات راهبردی فضای سایبر
سال اول، شماره اول، زمستان ۱۴۰۰، صفحات ۲۸-۷

بررسی آثار تهدیدها و حملات سایبری بر امنیت ملی جمهوری اسلامی ایران

محمدرضا حسینی [۱] محمد جداری سلامی [۲]

تاریخ دریافت: ۱۴۰۰/۰۳/۱۸ **تاریخ پذیرش: ۱۴۰۰/۱۰/۲۱**

چکیده

تهدیدها و حملات سایبری مصداق سلاح نوینی است که می‌تواند روش هدایت جنگ مدرن توسط بازیگران دولتی و غیردولتی را دگرگون سازد. سرشت منحصربه‌فرد این تهدیدها و توانمندی مرتکبان حملات سایبری در آسیب رساندن، کشتار و تخریب فیزیکی از طریق فضای سایبر تعاریف سنتی توسل به زور را متحول ساخته است.

مقاله حاضر در پی پاسخ‌گویی به این پرسش است که تهدیدهای سایبری و حملات سایبری چگونه بر امنیت ملی تأثیر می‌گذارند و این اثرگذاری در چه ابعادی خود را نمایان می‌سازد. در پاسخ می‌توان گفت تهدیدها و حملات سایبری به علت برخورداری از ویژگی‌هایی چون قیمت پایین ورود، گمنامی و تأثیرگذاری شگرف، پدیده‌ای به نام انتشار قدرت را به وجود آورده است که نه‌تنها باعث شده دولت‌های کوچک از ظرفیت بیشتری برای اعمال قدرت در این فضا برخوردار شوند، بلکه منجر به ورود بازیگران جدیدی همچون شرکت‌ها، گروه‌های سازمان‌یافته و افراد به معتدلات قدرت جهانی شده است؛ بنابراین، این پدیده امنیت ملی را از ابعاد مفهوم امنیت، دولت‌محوری در امنیت، بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه تحت تأثیر قرار داده است.

کلید واژه‌ها: فضای سایبری، تهدیدهای سایبری، جنگ سایبری، بدافزارها، امنیت ملی

۱.دانشیار دانشگاه عالی دفاع ملی، نویسنده مسئول rezahsn88@gmail.com
۲.گروه حقوق بین‌الملل دانشگاه تهران (پردیس فارابی).

مقدمه

جهان در دهه ۱۹۷۰ میلادی با یک انقلاب فناورانـه جدیـد روبـه‌رو شـده اسـت. ایـن انقلاب جدید به نام «انقلاب اطلاعات» شهرت یافته است و همان‌طور که می‌دانیم، ماهیـت علوم را اطلاعات تشکیل می‌دهد؛ عنصری که به دلیل اهمیت فوق‌العاده‌اش، عصر حاضر به آن نام گرفته است.[۱] نوآوری‌ها و هزینه کم در این زمینـــه باعـــث شده دسترسـی، استفاده و عملکرد اینترنت به میزان قابل توجهـی افزایش یابـــد، بـه‌طـوری کـــه امروزه اینترنـت در سراسر دنیا در حدود دو میلیارد کاربر دارد. اینترنت شبکه وسیع جهانـی را بـه وجود آورده که سالانه میلیاردها دلار برای اقتصاد جهانی سودآوری داشته است.

با وجود این، اینترنت دولت‌ها را در مقابل چـالش‌هـای جدید امنیتـی قرار داده اســت. هزینـه کم ورود، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگـذاری شـگرف و عدم شفافیت عمومـی در فضـای سایبری موجب شده بازیگران قوی و ضـعیف اعم از دولت‌ها، گروه‌های سازمان‌یافتـه و تروریستـی و حتـی افراد به این فضا وارد شده و تهدیـــدهایـــی همچـــون جنگ سایبری، جـــرائم سایبری، تروریسم و سایبری، جاسوسی سایبری و مانند آن‌ها را بـه وجـــود آورند. همـین نکته، تهدیدهای سایبری را از تهدیدهای ســـنتی امنیت ملـــی که تا حدود زیـــادی از ماهیت شفافـــی برخوردارند و بازیگران آن را دولت- ملت‌هایی تشـکیل می‌دهند کـه در یـک قلمرو مشخص جغرافیایـی قابل شناسایـی هستند، متمایز کرده و سبب شده است امنیت ملی بـه مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارآمد به حساب آید.

بنابراین، در مقاله پیش رو، به این مسئله مـی‌پـردازیم کـــه ماهیـــت تهدیـــدات سـایبری جدیـد چگونه بر امنیت ملی تأثیر می‌گذارد و این اثرگذاری، امنیت ملـی را با چه تغییرات مفهومی مواجه می‌کند. برای این منظور، در بخش پایانی پژوهش به سؤال اصلی یعنی چگونگی تأثیرگذاری تهدیـدهای سـایبری جدیـد بـر مفهـوم امنیـت ملـی می‌پردازیم.

---

۱. Electronic Communication.

الف. ماهیت تهدیدات سایبری

تهدیدهای سایبری پدیده‌ای جدید است که در دهه‌های اخیر، هم‌زمان با تحول فناوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان ظهور پیدا کرده است، به‌گونه‌ای که امروزه چالش تهدیدهای سایبری، هم مهم و هم پیچیده به نظر می‌رسد. این اهمیت و پیچیدگی ناشی از ماهیت جدید تهدیدهای سایبری و ویژگی‌ها و نمودهای منحصربه‌فردی است که شناخت از آن را بسیار مهم و ضروری می‌نماید.

۱. تعاریف

در همایشی که در ۲ مارس ۲۰۱۰ میلادی از سوی مؤسسه بین‌المللی CACI و مؤسسه مطالعاتی نیروی دریایی آمریکا با عنوان «تهدیدهای سایبری امنیت ملی و مقابله با چالش‌های پیش روی زنجیره عرضه جهانی» برگزار شد، تهدیدهای سایبری به‌صورت «وقایعی که به‌صورت طبیعی و یا توسط انسان (به‌طور عمدی یا غیرعمدی) بر فضای مجازی تأثیرگذار باشد یا حوادثی که از طریق فضای مجازی عمل کند یا به نحوی به آن مرتبط باشد» تعریف شد (CACI and USNI, 2010).

فضای سایبری نیز از سوی برخی کارشناسان به‌عنوان «تأثیر فضا و جامعه‌ای که توسط رایانه‌ها، اطلاعات و ابزارهای الکترونیکی، شبکه‌های دیجیتالی یا کاربران آن شکل می‌گیرد تعریف شده است (Lord and Sharp, 2011: 10).

۲. ویژگی‌های تهدیدهای سایبری

تهدیدهای سایبری ویژگی‌های منحصربه‌فردی دارند. از یک‌سو، این تهدیدها گستره وسیعی اعم از موانع قانونی، فنی، سازمانی و فرهنگی را شامل می‌شوند و از سوی دیگر، هزینه کم، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری موجب شده بازیگران زیادی به این عرصه وارد شوند. مهم‌ترین ویژگی‌های تهدیدهای سایبری در مؤلفه‌های زیر خلاصه می‌شوند:

۱. تعدد بازیگران در فضای سایبری: هزینه کم فناوری رایانه‌ای، اتصال گسترده به اینترنت و سهولت ایجاد یا به دست آوردن نرم‌افزارهای مخرب به این معنا است که تقریباً هر کسی می‌تواند به این فضا وارد شود. این بازیگران شامل افراد، گروه‌های سازمان‌یافته جنایی، گروه‌های تروریستی، شرکت‌های خصوصی و دولت – ملت هستند(Charney,2009: 5-6).

۲. هزینه کم ورود، صرف زمان کم و سرعت بالای اقدام: هر فرد برای انجام حمله سایبری تنها به یک رایانه، یک ارتباط اینترنتی و دانش فنی محدود در زمینه فضای سایبری نیاز دارد. در نتیجه، فضای سایبری شرایطی را فراهم کرده است که با هزینه پایین می‌توان اقدامات خطرناکی را در مدت‌زمان کم و با سرعت بالایی انجام داد. البته، انجام حملات پیچیده‌تر سایبری نیازمند صرف هزینه‌های بالاتری است (Lord and Sharp, 2011: 20-28).

۳. ناشناس ماندن بازیگران و عدم قابلیت ردیابی: اینترنت به‌عنوان سیستم نامتمرکز طراحی شده و کاربران آن، اغلب شناخته‌شده نیستند. همین ناشناختگی باعث می‌شود هیچ اثری از برخی از حمله‌های سایبری باقی نماند. افراد فعال در عرصه اینترنت می‌توانند از اقصی نقاط دنیا بدون هشدار و در عرض چند ثانیه و بدون آنکه اثر یا نامی از خود بر جای بگذارند، اهداف دیجیتالی را مورد هدف قرار دهند (Ibid).

۴. تأثیرگذاری شگرف: ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلال یا وقفه می‌تواند تأثیرات و پیامدهای به‌مراتب بیشتری از حادثه اولیه در پی داشته باشد. وقوع حمله‌های سایبری و در نتیجه آن بروز اختلال در شبکه‌ها می‌تواند موجب ایجاد خسارت به اموال، زمان، محصولات و تولیدات، اعتبار، اطلاعات حساس و حتی از دست دادن جان انسان شود، زیرا در این‌گونه مواقع، زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند (Lord and Sharp: 20-28).

۵. کمرنگ شدن نقش جغرافیا: فضای سایبری سرعت انتقال به سراسر جهان را در لحظه کوتاهی فراهم کرده است؛ بنابراین، تهدیدکنندگان قادر به فراتر رفتن از محدوده جغرافیایی خود و رسیدن به اهداف کلیدی‌شان هستند (Starr, 2009: 18).

۶. ساختار فضای اینترنت: اینترنت دامنه مشترک و یکپارچه است. استفاده از این فضا توسط شهروندان، شرکت‌ها و دولت‌ها به شیوه‌ای است که جداسازی آن‌ها بسیار دشوار است. توانایی محدود برای جدا کردن بازیگران و فعالیت‌های آن‌ها، پاسخ مناسب به تهدید را بسیار دشوارتر کرده است (Charney, 2009: 5-6). از سوی دیگر، ساختار اینترنت، دولت‌ها و شرکت‌های خصوصی را با عدم اطمینان در قبال خطرات فضای اینترنتی مواجه کرده است. این عدم قطعیت ناشی از پیچیدگی‌ها و فناوری در حال تکامل برای پشتیبانی از سیستم‌های حیاتی است (Haller and Et al, 2010: ۴).

۷. پایین بودن احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری: احتمال تنبیه یا بازخواست اقدام‌های مجرمانه در فضای سایبری پایین است. در نتیجه، افراد و سازمان‌ها نیز این فضا را در مقایسه با گزینه‌های جایگزین غیرسایبری مطمئن‌تر و دارای خطرات کمتری می‌بینند (Lord and Sharp, 2011).

۳. انواع تهدیدهای سایبری

بازیگران دولتی و غیردولتی از قدرت سایبری استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی خود در فضای سایبری و دنیای واقعی دست یابند. این اهداف در فضای مجازی از شیوه‌های متفاوتی حاصل می‌شوند که مهم‌ترین آن‌ها عبارت‌اند از: جنگ سایبری، تروریسم سایبری، جرائم سایبری، جاسوسی سایبری و آشفتگی سایبری.

۳-۱. جنگ سایبری[1]

اگر با نظر «کلازویتز» موافق باشیم که جنگ عمل صرفاً سیاسی نیست، بلکه ابزار سیاسی برای رسیدن به اهداف سیاسی است، می‌توانیم بگوییم که جنگ در فضای مجازی توسط بازیگرانی صورت می‌گیرد که به دنبال استفاده از فضا برای رسیدن به اهداف سیاسی خود هستند. به‌منظور درک اینکه آیا عمل خصمانه در فضای مجازی جنگ

1. Cyber War.

قلمداد مـی‌شـود یا نه لازم است قصد بازیگر را درک کنیم. بـه‌عنـوان مثال، اگر هدف از یک حملـه اینترنتی سود مالی یا شخصـی از طریق روش‌هـای مجرمانه مانند سرقت، تقلب و اخاذی باشد، باید با آن بـه‌عنـوان عمل مجرمانه برخـورد شود، اما اگر هدف مهاجم با جـاه‌طلبـی‌هـای به‌مراتب بزرگ‌تـر همچون وارد کـردن آسیب جدی به دولت یا شهروندان آن همچون تخریب، تضـعیف و غیرفعال کردن زیرساخت‌های نظامی و غیرنظامی باشـد، چنـین رفتـاری درواقـع چیـزی نزدیک به اقدام جنگی در مفهوم سنتی است (Cornish and Et al,2010: 12 -13).

در سـال ۲۰۰۷ میلادی، استونی به‌عنـوان کشور کوچـک مدرن در مقیاس بزرگ مـورد حمله‌های اینترنتی قـرار گرفت. فناوری بالای این کشور زمینه‌ای مناسب برای حملـه‌هـای اینترنتی با انگیزه‌های سیاسی بود (Tiirma-Klaar, 2011).

همان‌طور که ریچارد کلارک[1] استدلال می‌کنـد، جنـگ سایبری شکل جدیدی از مبارزه است که ما هنوز نمی‌توانیم آن را به‌طـور کامل درک کنـیم. در عـین حال، روشن است که در دنیای امروز، میدان جنـگ حوزه خود را به فضـای مجـازی گسترش داده و باید آن را به‌عنوان پنجمین عرصه جنگ در کنار عرصـه‌هـای سـنتی زمـین، هوا، دریا و فضا در نظـر گرفت (Cornish and Et al, 2010: 12-13).

۳-۲. حمله‌های سایبری[2]

حمله سایبری چیزی متفاوت از جنگ سایبری است. حمله سایبری اختلال در صـحت یـا درستی داده‌ها است که اغلـب از طریق کدهای مخرب و تغییر در منطق برنامه و کنتـرل داده‌هـا است که منجر بـه خروجی‌های اشـتباه می‌شود، صـورت می‌گیرد(Rodriguez, 2006: 9-10).

حمله‌های سایبری شامل چهار حوزه می‌شود: ۱- از دسـت دادن تمامیـت، ۲- از دسـت دادن قابلیت، ۳- از دست دادن اطلاعات محرمانه و ۴- تخریـب فیزیکـی (Army, 2005: 1-3). آب، برق، بانکداری و حمـل‌ونقـل هوایـی تنها چند نمونه از خدماتـی است که توسط زیرساخت‌های اطلاعات و ارتباطات در حال اجرا است. این زیرساخت‌ها به‌طـور فزاینـده‌ای به یکدیگر وابسـته هستند و هر حمله اینترنتی می‌تواند همانند بازی دومینـو در آن‌هـا اختلال ایجاد

---

۱. Richard Clarke.
۲. Cyber Attacks.

کنـد. اخـتلال در یک سیستم مساوی با اختلال در دیگر سیستم‌ها است و ادامـه ایـن رونـد از تـأثیرات بـالقوه حملات اینترنتی است (Islan and Et al, 2011: 5-6).

۳-۳. تروریسم سایبری[1]

آژانس مدیریت فـوق‌العـاده فدرال[2] تروریسم سایبری را ایـن‌گونـه تعریف مـی‌کنـد: تهدیـد و حمله غیرقانونی بر ضد رایانه‌ها، شبکه‌ها و اطلاعـات ذخیره‌شده در آن، زمـانـی کـه بـرای ترساندن یا مجبـور کـردن حکومت یا مردم آن در پیشبرد اهداف سیاسـی یا اجتمـاعی صـورت می‌گیرد (Congressional Research Service, 2008:4). تروریست‌هـا بـا از دسـت دادن پایگاه‌های کلیدی (مانند افغانسـتان)، به عامل کلیدی برای اقدام در فضـای سـایبری تبدیل شده‌اند. این اقدام‌ها می‌تواند شامل افزایش منابع بـرای حمایت از عملیـات خود، برنامـه‌ریـزی عملیات (استفاده از ابزارهای در دسترس هماننـد (Google earth) فرمانـدهـی و کنترل عملیات، انجام عملیات نفوذی و آمـوزش بـه هـواداران خـود (اسـتقرار وسـایل انفجاری) باشد (Starr, 2009:18).

۳-۴. جرائم سایبری[3]

جرائم اینترنتـی مـی‌توانـد نقض حـق مالکیت معنوی، نقض حق اختـراع، ربودن اسرار تجـاری و ... را شامل شود و همچنین شامل حمله عمدی به رایانه‌ها به‌منظـور مختل کردن آن‌ها یا کپی از اطلاعات طبقه‌بندی شده می‌شود (Nagre and Warade, 2008: 5). تحلیلگـران هزینـه جـرائم اینترنتـی را برای صنعت جهانـی بیش از هزار میلیارد دلار در موارد نقض مالکیت فکـری و از دست دادن اطلاعات تخمین زده‌انـد. برای مثال، شخصـی در سـال ۲۰۰۹ میلادی چندین ترابایت از داده‌های مربوط به سیستم الکترونیکی و طراحی اطلاعات از برنامه جنگنده‌هـای مشـترک ۳۰۰ میلیارد دلاری پنتاگون را به سرقت برد. علاوه بر این، بیشتر مجرمان اینترنتی از مجـازات فـرار کرده‌اند. بـدیهی است این فعالیت پـرسود و اغلب بدون مجازات، درواقع تهدیدی برای امنیـت ملی است(Peritz and Sechrist, 2010:5-7).

---

۱. Cyber Terrorism.
۲. Federal Emergency Management Agency.
۳. Cyber Crime.

۳-۵. جاسوسی سایبری[۱]

جاسوسی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا اطلاعات محرمانه را جمع‌آوری کند. برخلاف جرائم سایبری که مسائل مالی و اقتصادی محرک اصلی مجرمان است، جاسوسی سایبری بیشتر تأثیرات سیاسی داشته و جامعه را تهدید می‌کند. محرک‌های اصلی جاسوسی سایبری متفاوت است، اما شامل کسب منافع نظامی، صنعتی، سیاسی و فنی است. جاسوسان سایبری اطلاعات دزدیده شده را با اهداف مختلف مورد استفاده قرار می‌دهند که برخی از آن‌ها عبارت‌اند از تهدید، اخاذی و مختل کردن اقدامات رقبای سیاسی (Lord and Sharp, 2011: 17).

۳-۶. آشفتگی سایبری[۲]

آشفتگی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا هدف مورد نظر خود را ناقص کرده، تحت تأثیر قرار داده یا آن را آزار دهد. اهداف سیاسی و ایدئولوژیکی در پشت این اقدامات وجود دارد و افراد از ابزاری استفاده می‌کنند که غیرقانونی هستند. گروه‌های هکری آنارشیستی و نهیلیست‌ها از آشفتگی سایبری استفاده می‌کنند. به‌عنوان مثال، گروهی تحت عنوان «ناشناخته‌ها» در واکنش به دستگیری جولیان آسانژ[۳] مدیر سایت جنجالی ویکی لیکس، حمله‌های سایبری گسترده‌ای انجام دادند. برخلاف جرائم سایبری و جاسوسی سایبری که هدفشان دزدی یا تغییر اطلاعات است، آشفتگی سایبری سعی در مجازات یا تأثیرگذاری بر عقاید و رفتار هدف‌های خود دارد. ممکن است طی این مرحله، اطلاعات زیادی دزدیده شده یا تغییر یابد یا هزینه‌های مادی فراوانی به شبکه‌های هدف وارد شود، اما قصد و نیت اصلی آشفتگی سایبری، آسیب رساندن است. بازیگران دولتی و غیردولتی می‌توانند از این ابزار استفاده کنند، ولی تاکنون آشفتگی سایبری توسط افرادی انجام شده که با نام فعالان عرصه هک شناخته شده‌اند (Lord and Sharp: 18).

---

۱. Cyber Espionage.
۲. Cyber Agitation.
۳. Julian Assange.

تهدیدهای سایبری از ماهیتی متنوع، گسترده و منحصربه‌فرد برخوردارند. متنوع از آن رو که این تهدیدها تمام حوزه‌های زندگی بشر را تحت تأثیر قرار داده‌اند و در نتیجه عدم امنیت در فضای سایبری بسیار بالا است. گستردگی نیز از آن رو که نه‌تنها بازیگران دولتی، بلکه شرکت‌های خصوصی، گروه‌ها و افراد را نیز درگیر خود کرده است و منحصربه‌فرد بودن نیز به این علت است که ماهیت این تهدیدها متمایز از تهدیدات سنتی و رایج گذشته است که البته این ویژگی بیشتر دولت‌ها و درک آن‌ها از تهدید را تحت تأثیر قرار داده است.

تأثیر تهدیدهای سایبری بر امنیت ملی

بسیاری از کارشناسان و تحلیلگران حوزه امنیت، بر این باورند که پایان یافتن دوران جنگ سرد نه‌تنها منجر به امن‌تر شدن جهان نشده است، بلکه باعث به وجود آمدن چالش‌های امنیتی غیرنظامی جدیدی همچون تخریب محیط زیست، رفاه اقتصادی، سازمان‌های جنایی بین‌المللی و مهاجرت گسترده افراد، امنیت جهانی را با چالش‌های جدی‌تری نسبت به گذشته مواجه ساخته است. تحلیلگران بر این باورند که اهمیت این مسائل «جدید» نه‌تنها بازاندیشی در تهدیدهای امنیتی، بلکه تجدیدنظر درباره خود مفهوم امنیت را ضروری می‌سازد.

در عین حال، انتقادی که بر ادبیات موجود امنیت وارد است، این است که اغلب این متون به تهدیدهای سایبری به‌عنوان یکی از همین چالش‌های امنیتی جدید که در این زمینه بسیار هم پراهمیت به نظر می‌رسد، توجه اندکی داشته‌اند. همان‌طور که در بخش‌های پیشین اشاره شد، آنچه در مورد این تهدیدهای جدید قابل توجه است، این است که ویروس‌ها، کرم‌ها، جرم‌ها، هکرها و حملات اینترنتی، امروزه واقعیت مسلم و روزمره هستند.

حملات مخرب مهم با تأثیرات گسترده، تهدیدهای سایبری را به‌عنوان یکی از بدترین تهدیدهای منافع ملی به تصویر کشیده است تا جایی که آمریکا اعلام کرده است که این حملات را به‌عنوان جنگ تلقی کرده و با آن برخورد فیزیکی خواهد کرد. از طرف

دیگر، بحث و گفتگـو دربـاره ایـن تهدیـدات متـأثر از انقلاب مداوم اطلاعات و رسوخ آن به تمام جنبه‌های زندگی بشر امروز است.

مطابق آنچه که در مورد تهدیدات در فضای سایبر بیان شد، در ایـن بخـش بـه بررسـی «حملات سایبری» و روش‌های گوناگون آن می‌پردازیم و با بررسی تأثیر آن بر امنیـت ملـی نتیجه‌گیری ارائه خواهد شد.

ب. ماهیت حملات سایبری

«حملات سایبری» در چارچوب طیف گسترده‌تری از آنچه «عملیات اطلاعـاتی» نامیـده می‌شود قرار می‌گیرند. عملیات اطلاعاتی کـه «جنـگ اطلاعـاتی» نیـز زیرمجموعـه‌ای از آن اسـت و هنگـام مخاصـمه مسـلحانه بـه آن توسـل مـی‌شـود (Schmitt, 1998: 890-891)، به‌کارگیری منسجم توانمندی‌های جنگ الکترونیکی، عملیات شـبکه‌ای رایانـه‌ای، عملیـات روانی، حیله‌های نظامی و عملیات هماهنگ با قابلیـت‌هـای پشـتیبانی اسـت کـه بـه‌منظـور تأثیرگذاری، متوقف نمودن، تخریب یا سرقت اطلاعات دشمن و در عین حال پشـتیبانی از فرایندهای تصمیم‌گیری نهادهای ملی صورت می‌گیرد.[1]

امروزه به‌هم‌پیوستگی زیرساخت‌های دیجیتالی نهادهـای مختلـف از قبیـل سـازمان‌هـا، کسب‌وکارها، دولت‌ها، افراد و ... باعث شده است که این فضا با چالشـی جهـانی از سـوی حملات سایبری روبه‌رو شود. دامنه و گستردگی این حملات که از یک بدافزار ساده گرفته تا حملات مـداوم پیشـرفته و هدفمنـد بـه‌گونـه‌ای اسـت کـه اطلاعـات حسـاس افـراد و زیرساخت‌های حیاتی سازمان‌ها و کشورها را با تهدید جدی مواجه کرده اسـت. بـه علـت همبستگی بین نهادها و موجودیت‌های مختلف در جهان این تهدیدات به‌طـور قـراردادی و فنی به‌عنوان «تهدیدات سایبری جهانی» شناخته می‌شوند. ایـن تهدیـدات دامنـه وسـیعی از جرائم سایبری را در برمی‌گیرد و همواره خسـارات جـدی را بـه سـازمان‌هـا و افـراد وارد می‌کند. تهدیدات در بیشتر مواقع به‌طور ذاتی مخرب و تهاجمی است. قربانیان ممکن است دارایی‌های فکری و مالکیت معنوی خود را از دست بدهند یا حساب‌های بانکی آن‌ها افشا

---

1. www.dod.gov.

شود، یا به‌طور ناخواسته باعث انتشار ویروس به رایانه‌های دیگر شبکه شوند. در سطح بالاتر هکرها اطلاعات محرمانه کسب‌وکارها را به دست آورده و حتی زیرساخت‌های حیاتی کشورها را تهدید و از کار می‌اندازند.

روش‌های متداول حمله[1]

در زیر فهرست و خلاصه‌ای از روش‌های حمله سایبری ارائه شده است که در سال‌های اخیر متداول و فراگیر شده و به‌طور حتمی این تهدیدات برای سازمان‌هایی که در بخش‌های مختلف نظامی، دولتی، عمومی و خصوصی فعالیت می‌کنند، قابل وقوع است.

الف- تهدید مداوم پیشرفته[2]

تهدید مداوم پیشرفته که به اختصار APT نامیده می‌شود، شامل تلاش‌های پیچیده‌تر و متمرکزی است که به‌وسیله گروهی از هکرهای هماهنگ اجرا می‌شود و بر روی هدف واحدی تمرکز دارند. هدف آن نفوذ به سامانه‌های حساس تا حد امکان غیرقابل کشف بودن برای مدت طولانی و پایین‌ترین سطح از ردیابی موفق است. به این منظور APT ها به یک رویکرد مطلوب برای سازمان‌هایی تبدیل شده است که به دنبال اجرای جاسوسی هوشمند و هماهنگ سایبری هستند. حملات APT عموماً برای کسب اطلاعات حساس و طبقه‌بندی‌شده از شرکت‌ها و سازمان‌های صاحب فناوری و مهم که دارایی‌های اطلاعاتی ارزشمندی دارند، صورت می‌گیرد.

به‌منظور مقابله با این حملات باید دانست که یک فناوری یا فرایند واحد نمی‌تواند آن را متوقف کند و روش‌های امنیتی سنتی نیز توان مقابله با آن‌ها را نیز ندارد.

این در حالی است که بسیاری از سازمان‌ها نسبت به این تهدید آسیب‌پذیرند؛ زیرا آن‌ها در گذشته نتوانسته‌اند به میزان کافی در خصوص امنیت سرمایه‌گذاری نمایند و امنیت موجود قدرت دفاعی کافی و مناسب را ندارد؛ بنابراین روش‌های جدید و مراقبتی بالاتری نیاز است.

---

۱. Mukaram, A. (2014, June 3). Retrieved from Recorded Future: https://www.recordedfuture.com/cyber-threat-landscape-basics

۲. Advanced Persistent Threat.

به‌منظور دفاع در مقابل APT لایه‌های دفاعی مختلف، دانشی از تهدید، مهارت‌های پیشرفته برای کشف و واکنش در مقابل آن نیاز است. به این منظور روش‌های دفاعی سایبری جدید ازجمله مانیتورینگ پایدار مداوم[1] پدید آمدند. در اجرای این روش، سامانه‌های مانیتورینگ کارا و اثربخش در هسته دفاع سایبری قرار دارد.

ب- انکار سرویس توزیع‌شده[2]

حملات انکار سرویس توزیع‌شده یا به اختصار DDoS، حملاتی است که شامل حجم انبوهی از بسته‌های شبکه با مقدار داده‌ای بالا بوده و منظور از آن از کار انداختن خدمات ارائه‌شده توسط سیستم هدف است. در این حمله، ازکارافتادن سرویس بیش از سرقت اطلاعات مدنظر است. اگرچه این حمله نسبت به سایر حملات از چالش‌های فنی کمتری برخوردار است، اما نمی‌توان اثربخشی آن را در ضرر و زیان رساندن دست‌کم گرفت. این حمله باعث می‌شود که درخواست‌های مشروع و مجاز از دست برود یا حداقل، خدمات بسیار آهسته و کند به درخواست‌کننده برسد.

به‌عنوان نمونه یک حمله DDoS موفق دسترسی به اینترنت را قطع می‌کند، اما تأثیری بر روی سیستم‌های رایانه‌ای داخل سازمان ندارد. اگر یک سازمان از روش‌های بهینه امنیتی پیروی کند، شبکه‌ها و سامانه‌های پرداخت مالی و تجاری خود را به‌سادگی در معرض اینترنت و آسیب‌پذیر رها نمی‌کند.

بر اساس آمار منتشره مؤسسه Verizon حملات DDoS از سال ۲۰۱۰ تا ۲۰۱۴ میلادی به‌طور چشم‌گیری رشد داشته است. به‌منظور مقابله با این حملات باید سرورها و خدمات را برای افراد و IP هایی که به آن نیاز دارند، فعال و در دسترس قرار داد و فضای IP مشخصی را برای دسترسی به سرورها در نظر گرفت. باید از تیم عملیاتی باتجربه و قوی برای شناسایی و مقابله با این حملات استفاده کرد. داشتن طرح مقابله با DDoS، حسگرهای شناسایی و لینک‌های موازی بسیار ضروری است. سامانه مانیتورینگ، تشخیص نفوذ و فایروال ازجمله سامانه‌های پرکاربرد در جلوگیری از این تهدید است.

---

1. Continuous Persistent Monitoring.
2. Distributed Denial of Service.

پ- بدافزار چند پلتفرمی[1]

باید بدانیم که بدافزارها فقط به سیستم‌عامل ویندوز منحصر نمی‌شود. انگیزه‌های اقتصادی که امروزه موجب ایجاد بدافزارهای چند پلتفرمی برای جرائم سایبری شده، رو به افزایش است و باعث شده بدافزارها بتوانند روی چندین سیستم‌عامل مختلف ازجمله ویندوز، لینوکس، IOS و ... کار کنند. این مسئله حملات بدافزارهای چند پلتفرمی را افزایش داده است.

برای مقابله با این حملات استفاده از مکانیزم‌های مقابله با بدافزارها ازجمله آنتی‌ویروس روی تمامی رایانه‌ها، ابزارهای دیجیتالی و موبایل و استفاده نکردن از منابع ناامن و کم‌اعتبار ازجمله مشاهده سایت‌های نامعتبر، غیرفعال کردن Java در مرورگرها، باز نکردن ایمیل‌های ناشناخته، متصل نکردن فلش‌های با خطر بالا به رایانه سازمانی بسیار ضروری است.

ت- بدافزار دگرگون‌شده و چندریختی[2]

این نوع از بدافزارها دائماً در حال تغییر هستند و بنابراین هر نسخه‌ای از آن با قبلی متفاوت است. بدافزارهای دگرگون‌شده و چندریختی یکی از خطرناک‌ترین و بزرگ‌ترین تهدیدات برای سازمان‌ها در جهان محسوب می‌شوند؛ زیرا به‌راحتی می‌توانند مکانیزم‌های شناسایی و برنامه‌های آنتی‌ویروس را فریب دهند و از آن‌ها عبور کنند. شایان ذکر است که نوشتن و تولید بدافزارهای دگرگون‌شده چندریختی بسیار مشکل و سخت است؛ زیرا نیازمند فن‌های پیچیده‌ای مانند تغییر نام، تغییر کد، توسعه کد، کاهش کد و درج کد اضافی و زائد است. این مسئله باعث شده که هکرهای کمتری در حوزه پشتیبانی و توسعه این بدافزارها فعالیت کنند.

طبق آمار منتشره توسط مؤسسه Verizon در سال ۲۰۱۴ میلادی، ۶۷٪ از بدافزارها در ساعات اولیه انتشار شناسایی می‌شوند، ۳۰٪ از آن‌ها بین چندین روز یا چند هفته ولی ۱۳٪ پیچیده و خطرناک آن بیش از چندین ماه طول می‌کشد تا کشف و شناسایی شوند.

---

1. Cross-Platform Malware.
2. Metamorphic and Polymorphic Malware.

مقابله با این کدها بسیار سخت بوده؛ چراکه آنتی‌ویروس‌های مبتنی بر امضا در شناسایی آن عاجزند؛ اما آنتی‌ویروس‌های قوی و دارای موتورهای ویروس‌یابی هوشمند می‌توانند تا حدودی کمک‌کننده باشند. استفاده از مرورگرهای به‌روز، رعایت ملاحظات امنیتی در هنگام استفاده از اینترنت و انتقال فایل‌ها در جلوگیری از انتشار و آلوده شدن به آن بسیار تأثیرگذار است.

ث- فیشینگ[1]

این روش عموماً از طریق ایمیل انجام می‌شود و ایده ایمیل به این دلیل است که در حقیقت ایمیل یک ابزار ارتباطی غیرانحصاری است به این معنی که بین دو عاملی که حتی همدیگر را نمی‌شناسند و از هویت همدیگر با اطلاع نیستند، می‌تواند منتقل شود. این در حالی است که افراد عموماً انتظار دارند افرادی با آن‌ها تماس داشته باشند که آن‌ها را می‌شناسند ولی بیشتر آن‌ها دوست ندارند که ارتباطات خود را فیلتر کنند؛ چراکه ماهیت ذاتی ایمیل از بین می‌رود.

این مسئله باعث می‌شود که روزنه‌ای به وجود آید تا هکرها بتوانند از همین خصوصیت غیرانحصاری بودن ارتباطات سوءاستفاده کنند. پروتکل ایمیل هیچ عامل مجازشناسی برای آدرس‌های ارسال‌کننده را ندارد و همین روزنه به هکرها کمک می‌کند تا از هر آدرس ایمیلی به قربانیان خود ایمیل ارسال کنند.

اگرچه ابزارهایی مانند پی جی پی[2]جهت رمزنگاری ایمیل یا چارچوب سیاست فرستنده[3]به‌منظور اعتبارسنجی ایمیل، برای مهار این تهدید تلاش می‌کنند، اما اثربخشی لازم به خاطر اضافه شدن مراحل انجام کار و کاهش مقبولیت و سادگی را در بین کاربران عادی ندارد؛ بنابراین برای مقابله با این تهدیدات علاوه بر ابزارها و فناوری‌های شناسایی کننده و مقابله با فیشینگ و هشداردهنده سایت‌های جعلی، آموزش و آگاهی افراد، باز نکردن ایمیل‌های ناشناخته و فریب نخوردن در مقابل مطالب گمراه‌کننده و وسوسه‌انگیز و باز نکردن مستقیم سایت‌هایی که لینک آن‌ها در ایمیل آمده است، می‌تواند مؤثر باشد.

---

۱. Phishing.
۲. Pretty Good Privacy.
۳. Sender Policy Framework.

ج. امنیت ملی: برداشت‌های رایج

هم‌زمان با به وجود آمدن دولت – ملت و گسترش آن، امنیت ملی به‌عنوان یکی از مهم‌ترین کار ویژه دولت‌ها در دستور کار قرار گرفت، به‌طوری که اکثریت قریب به‌اتفاق تحلیلگران بر این باورند که ماهیت وجودی دولت‌ها به تأمین امنیت داخلی و خارجی آن‌ها و چگونگی تعریف، بسط و گسترش مفهوم امنیت ملی گره خورده است. در این راستا، دیدگاه‌های متفاوتی راجع به بحث امنیت ملی و چگونگی تأمین آن در میان دولت‌ها و محافل دانشگاهی وجود دارد.

رویکردهای نظری متفاوت به امنیت ملی

مقوله امنیت ملی مورد توجه رویکردهای مختلفی در روابط بین‌الملل قرار گرفته است. هر یک از این رویکردها بر اساس نگاه خاص خود به مسائلی همچون قدرت، منافع ملی، ساختار نظام بین‌الملل و مانند آن‌ها به امنیت ملی پرداخته‌اند. در این بخش به مفهوم امنیت ملی از نگاه مهم‌ترین این رویکردها می‌پردازیم.

واقع‌گرایان معتقدند در سطح سیاست داخلی، مسئله‌ای به نام امنیت وجود نداشته و امنیت صرفاً در سطح بین‌المللی معنا می‌یابد. به بیان دیگر، امنیت ملی نزد آنان چیزی جز امنیت بین‌المللی نیست و در این راستا ناامنی ویژگی بارز نظام بین‌الملل است(عبدالله خانی، ۷۰:۱۳۸۲). از نظر واقع‌گرایان، عدم امنیت اصلی‌ترین مسئله، قدرت مهم‌ترین ابزار، دولت مهم‌ترین بازیگر و جنگ، بارزترین جلوه بروز ناامنی در عرصه بین‌المللی است(یزدان فام، ۷۳۱:۱۳۸۶). بنابراین، محور تمرکز واقع‌گرایی در موضوع امنیت، نظامی است.

همان‌طور که استفن والت[1] تعریف می‌کند، مطالعات امنیتی، مطالعه تهدید، استفاده و کنترل نیروی نظامی است (Williams and Krause, 1996: 230).

جدای از مسائل نظامی، سایر عوامل هم در بحث امنیت می‌توانند مهم باشند، اما واقع‌گرایان و نوواقع‌گرایان معمولاً تنها تا جایی آن‌ها را مهم می‌شمارند که به توسعه توانایی‌های نظامی کمک کند (تریف، ۱۳۸۳). از نظر واقع‌گرایان، هر چیزی ممکن است بر

---

۱. Stephen Walt.

امنیت تأثیرگذار باشد، اما موضوع امنیت هر چیزی نمی‌تواند باشد. به باور واقع‌گرایان، چون دولت‌ها بازیگران اصلی در نظام بین‌الملل می‌باشند، بنابراین آنان مرجع امنیت قرار خواهند گرفت (عبدالله خانی، ۸۳:۱۳۸۲).

در نقطه مقابل، لیبرالیسم کلاسیک ضمن قبول وجود آنارشی در عرصه بین‌المللی، با انتقاد از سیاست قدرتمندانه واقع‌گرایی معتقد است صلح نه با موازنه قدرت و تسلیح هر چه بیشتر کشورها، بلکه از طریق گسترش حکومت‌های دموکراتیک در جهان میسر است. نئولیبرالیسم نهادگرا به‌عنوان یکی از گرایش‌های مهم لیبرالیسم نیز همانند واقع‌گرایی قبول دارد که عرصه بین‌المللی، عرصه آنارشی است و چنین فضایی امنیت ملی و بین‌المللی را به خطر می‌اندازد، اما برای حفظ امنیت، راه‌حل متفاوتی دارد.

صاحب‌نظران این نظریه بر این باورند که برای ایجاد امنیت و حفظ صلح باید رفتار دولت‌ها مهار و به آن‌ها لگام زده شود و این کار با ایجاد سازمان‌ها و رژیم‌های بین‌المللی میسر است (یزدان فام، ۷۳۲:۱۳۸۶).

از سوی دیگر، مکتب کپنهاگ نیز مخالف دیدگاهی است که هسته اصلی مطالعات امنیتی را جنگ و زور می‌داند. «بوزان » معتقد است در دیدگاه واقع‌گرایان مفهوم پیچیده امنیت به مفهومی مترادف با قدرت کاهش پیدا کرده است (بوزان، ۸:۱۳۷۸). از نظر مکتب کپنهاگ، اگرچه امنیت فردی گویای سطح مشخص و مهمی از تحلیل است، اما افراد نمی‌توانند به‌عنوان مرجع امنیت شناخته شوند، چراکه اصولاً تابع ساختارهای سیاسی عالی‌تر دولتی و بین‌المللی می‌باشند؛ بنابراین، مکتب کپنهاک نیز با رد فردمحوری در مرجع امنیت، تمرکز خود را بر دولت به‌عنوان محور امنیت قرار می‌دهد (عبدالله خانی، ۱۳۸۲).

بوزان در یکی از نوشته‌های خود با عنوان «الگوی جدید مطالعه امنیتی در قرن ۲۱»، الگوی جدید مطالعات امنیتی را بر اساس مؤلفه‌های پنج‌گانه سیاسی، نظامی، اقتصادی، اجتماعی و زیست‌محیطی می‌داند (Buzan,1991: 433).

رویکرد سازه‌انگاری نیز ضمن رد ماهیت آنارشیک نظام بین‌الملل، هویت را به‌عنوان دستورالعمل، وارد بررسی‌های امنیتی و سیاست خارجی دولت‌ها کرد.

در ایـن چـارچوب، دولـت‌هـا بر اساس هویتشـان، دشمنان، رقبا و دوستان خود را درک می‌کنند و در ایـن فراینـد، هویت خود را تعریف و بازتعریف می‌نمایند. امنیت بر وضعیت مادی بیرونی دلالـت نـدارد، بلکه مفهومـی است اجتماعـی و معنایـی که در فرایند اجتمـاعی ساخته شده و قـوام می‌یابد. توجه به امنیت انسانـی، بـه‌عنـوان مرجع نهایی امنیت و گرایش به مفاهیم جهان‌شمول در امنیت جهانـی، از ویژگـی‌هـای نظریه سازه‌انگاری است (یـزدان فام ۱۳۸۶:۷۳۷).

البتـه، بایـد اضافه کرد که برخـی نویسندگان همچون جسیکا تـاچمن بـه دنبال برخـی تحـولات جهـانی بـر گسترش مطالعات امنیتی به مسائلـی همچون زیسـت‌محیطـی، رفـاه اقتصادی و رشـد جمعیت تأکید کرده‌اند (Tuchman, 1989: 162-177).

بنابراین، با این بررسی هرچند اجمالی، در پایان این بخش به همان نتیجه‌ای می‌رسـیم کـه بری بوزان در مطالعات امنیتی خود رسیده است. وی تشریح می‌کند که: «امنیـت ملی از لحاظ مفهومـی ضعیف، از نظر تعریف مبهم، ولـی از نظر سیاسـی مفهومـی قدرتمند باقـی مانـده اسـت» (مندل، ۱۳۷۹:۵۵).

در نتیجه، هیچ یک از تعاریف و رویکردهای مربوطه نتوانسته‌اند به‌خوبی و همه‌جانبه از پس تحلیل موضوع امنیت ملی برآمـده و هـر یک از ظـن خـود بـه ایـن مقوله نگریسته و تنها بخشی از واقعیت‌های موجود آن را تشریح کرده‌اند. این پیچیدگـی مفهوم امنیت با وارد شدن مباحث مربوط به فضای سایبری و تهدیدهای مرتبط بـا آن در دو سه دهه گذشـته، دوچندان شده است. اگر تا پیش از این، فضـای مفهـومـی و تحلیلـی امنیـت بـر مبنـای درک مشخصـی از مرزهای جغرافیایـی تهدید و منابع تهدیدکننـده استوار بود، در عصر اطلاعـات و بـا کشیده شدن مفهوم امنیت به فضای مجازی، نه‌تنها درک روشنی از فضـای جغرافیایـی تهدیـد وجود ندارد، بلکه با گستردگـی منابع تهدیدکننـده امنیت نیز مواجه هستیم.

نتیجه‌گیری و پیشنهاد

فضای سایبری و فناوری‌های وابسته به آن، یکی از مهم‌ترین منابع قدرت در هزاره سوم هستند. ویژگی‌های فضای سایبری همچون قیمت پایین ورود، گمنامی، آسیب‌پذیری و نامتقارن بودن، پدیده انتشار قدرت را به وجود آورده است، به این معنی که اگر تاکنون دولت‌ها بازی قدرت را تنها میان خود تقسیم کرده بودند، از این پس باید آن را با بازیگران دیگری همچون شرکت‌های خصوصی، گروه‌های سازمان‌یافته تروریستی و جنایی و افراد تقسیم نمایند، اگرچه هنوز این دولت‌ها هستند که در این عرصه نقش مهمی را بازی می‌کنند. به‌تبع، این پدیده امنیت ملی دولت‌ها را از تأثیرگذاری خود بی‌نصیب نخواهد گذاشت. این تأثیرگذاری را از چند جهت می‌توان مورد ارزیابی قرار داد.

نخست، مفهوم امنیت است. دیگر نمی‌توان امنیت ملی را همانند گذشته در ارتباط با مسائل نظامی و مرزهای داخلی و خارجی تعریف کرد، بلکه امروزه، خطر افت کیفیت زندگی شهروندان نیز نوعی تهدید برای امنیت ملی محسوب می‌شود.

دوم، از میان رفتن بعد جغرافیایی در تهدیدهای سایبری است. در گذشته، تهدیدهای نظامی از محل جغرافیایی خاصی برخوردار بودند. در نتیجه، مقابله با آن دست‌کم از جهت شناسایی کار چندان دشواری نبود.

سوم، گستردگی آسیب‌پذیری‌های ناشی از تهدیدهای سایبری است. این تهدیدها پراکنده، چندبُعدی و چند سویه‌اند و چون در ارتباط با شبکه‌های ارتباطی و زیرساخت‌های حساس می‌باشند، سطح آسیب‌رسانی آن‌ها بسیار بالا است.

چهارم، این تهدیدها را صرفاً شیوه‌های سنتی همانند به‌کارگیری ارتش و نیروی پلیسی نمی‌توان مهار کرد و برای مقابله با آن‌ها تلاش دولت‌ها به‌تنهایی کافی نیست و همکاری مؤثر و دوجانبه دولت‌ها و بخش خصوصی را که دارای منافع مشترکی در برخورد با این‌گونه تهدیدها هستند، می‌طلبد.

پنجم، همان‌گونه که از نکته قبلی برمی‌آید، تهدیدهای سایبری صرفاً متوجه دولت‌ها نیست، بلکه افراد و شرکت‌ها نیز از آسیب‌های این تهدیدها بی‌نصیب نخواهند بود.

ششـم، چـون امنیت در عصـر اطلاعات صرفاً دولت‌محور نیست، بنابراین رویکردهای مختلف نظری در روابط بین‌الملل کـه به‌طور عمده بر مبنای دولت‌محوری به سـاختاربندی نظریات خود پرداخته‌اند، یا به‌راحتی از کنار این تهدیدها گذشته‌اند یا در تحلیل‌هـای خـود با سردرگمی مواجه شده‌اند.

در پایـــان، ذکـــر ایـــن نکتـــه ضروری است که مجموعه عوامل بالا سبب خواهد شد دولت‌ها و محافل دانشگاهی دیر یا زود در برداشت‌هـای خود نسبت به منافع، پایگـاه‌هـای قدرت و امنیتشان تجدیدنظر کنند.

فهرست منابع و مآخذ

الف. منابع فارسی

- ابراهیمی، شهروز، «حاکمیت فراوستفالیا: جهانی شدن و تعامل حاکمیت ملی با حاکمیت بین‌المللی با تأکید بر جمهوری اسلامی ایران»، دانش سیاسی، ۴، ۱۳۸۵.
- اردبیلی، محمدعلی، حقوق جزای عمومی، ج ۱، انتشارات میزان، چاپ بیست‌وسوم، تابستان ۱۳۸۹.
- اسکات جی شاکل فورد، از جنگ هسته‌ای تا جنگ اینترنتی، مشابهت‌سازی حملات سایبری در حقوق بین‌الملل، ترجمه و تلخیص یاسر ضیایی، قابل دسترسی در: http:/// www. Yaserziacee, blogfa. Com/ post. 7. aspx. Visited 2017
- اسماعیل‌زاده ملاباشی، پرستو؛ عبداللهی، محسن و زمانی، سید قاسم، حملات سایبری و اصول حقوق بین‌الملل بشردوستانه (مطالعه موردی: حملات سایبری به گرجستان)، فصلنامه مطالعات حقوق عمومی، دوره ۷۴، شماره ۲، تابستان ۱۳۹۶.
- اسماعیلی فلاح، مرضیه، دادگاه صالح در رسیدگی به جرائم سایبر، خبرنامه کانون وکلای دادگستری استان اصفهان، شماره ۶۰، تیر ۱۳۹۰.
- اصلانی، جبار، «حملات سایبری از منظر حقوق بشردوستانه با نگاهی به قضیه‌ی استاکس نت و ایران»، فصلنامهٔ مطالعات بین‌المللی، سال دهم، شمارهٔ ۴، ۱۳۹۳.
- افضلی، رسول؛ قالیباف، محمدباقر و احمدی فیروزجانی، میثم، «تبیین تحولات مفهوم مرز در فضای سیاسی مجازی»، پژوهش‌های جغرافیایی انسانی، ۴۵، ۱۳۹۲.
- افق یک، اطلاعات فناوری قضا، تهران: دفتر همکاری‌های فناوری ریاست جمهوری. ۱۳۸۱.
- ایازی، رضا، قوانین و جرائم رایانه‌ای، فصلنامه مطالعات بین‌المللی پلیس، سال اول، شماره ۳، پاییز ۱۳۸۹.
- باستانی، برومند، جرائم کامپیوتری و اینترنتی جلوه‌ای نوین از بزهکاری، انتشارات تهران بهنامی، چاپ سوم، ۱۳۹۰.
- بای، حسینعلی و پورقهرمانی، بابک، بررسی فقهی حقوقی جرائم رایانه‌ای، تهران: پژوهشگاه علوم و فرهنگ اسلامی، ۱۳۸۸.
- خلف رضایی، حسین، «حملات سایبری از منظر حقوق بین‌الملل» (مطالعه موردی: استاکس نت)، فصلنامهٔ مجلس و راهبرد، سال بیستم، شمارهٔ ۷۳، ۱۳۹۲.
- خلیلی‌پور رکن‌آبادی، علی و نورعلی‌وند، یاسر، تهدیدات سایبری و تأثیر آن بر امنیت ملی، فصلنامه مطالعات راهبردی، سال پانزدهم، شماره ۵۶، ۱۳۹۱.
- خواجه نائینی، علی، درآمدی بر مفهوم حاکمیت شبکه‌ای، رهیافت‌های سیاسی و بین‌المللی، شماره ۳۹، ۱۳۹۳.

ب. منابع انگلیسی

- Addendum to Summary Report of Twelfth Meeting of Committee I/’Doc. 866, I/1/30(a), (8 June 1945) 6 UNCIO (1945) 356.
- Albercht Randelzhofer, Article 2(4)’ in B.Simma(ed.), The Charter of United nations: A Commentary (2nd, Oxford University Press, 2002), 118.
- American Institute for Contemporary German Studies, Governing Beyond the Nation – state Global Public Policy: Regionalism or Going Local? AICGS Research Report, No. 11, 1999, p.42.
- An assessment of international legal issues in information operation, United States Department of Defense of the General Council, (DOD OGC),1999,P.15. Availiable at: Http//:www.au.af.mil/an/awc/awcgate/army/jaoac-io.pdf.
- Andrew Linklater, “Citizenship and sovereignty in the post – Westphalian state”, European journal of international Relations, vol.2, 1996, p.77
- Annex of the agreement between the government of the member states of the Shanghai cooperation organization in the field of the international information security of 16 June. 2009.
- Anthony Aust, Handbook of International law, New York: Cambridge University Press. 2010.p.3
- Antonio Cassese, Internationl Law, Oxford University Press,2nd edition, ٢٠٠٥,P.٤٨٤.
- Anupam Chander & Madhavi Sunder, The Romance of the Public Domain, California law Review. Vol. 92, Issue 5, 2004, p.1331.
- Armed activities on territory of Congo (Congo v. uganda) ICJ reports 2005, P.248.
- Beaumont, P. “US Appoints First Cyber warfare General”, the Observer, 10. 23 May 2010, p.10.
- Brenner, S.W., “At Light speed: Attribution and Response to Cyber Crime/ Terrorism/ warfare”, Journal of Criminal Law and Criminology, No, 97, 2006 – ٢٠٠٧, p.٤٢٤.
- Brenner, Susan W. & Clarke, Leo L (2010). "Civilians in Cyberwarfare: conscripts", Vanderbilt Journal of Transnational Law, Vol. 43: 1011-1076.,p1028