تهدیدات سایبری و تأثیر آن بر امنیت ملی

تاریخ دریافت: ۱۳۹۰/۸/۱۹ تاریخ پذیرش: ۱۳۹۱/۲/۲

علی خلیلی‌پور رکن‌آبادی*

یاسر نورعلی وند*

چکیده

مقاله حاضر در پی پاسخ‌گویی به این پرسش است که تهدیدهای سایبری چگونه بر امنیت ملی تأثیر می‌گذارند و این اثرگذاری در چه ابعادی خود را نمایان می‌سازد. در پاسخ می‌توان گفت این تهدید به علت برخورداری از ویژگی‌هایی چون قیمت پایین ورود، گمنامی و تأثیرگذاری شگرف، پدیده‌ای به نام انتشار قدرت را به وجود آورده است که نه تنها 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 معادلات 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.

کلیدواژه‌ها: فضای سایبری، تهدیدهای سایبری، جنگ سایبری، تروریسم سایبری، جاسوسی سایبری، امنیت ملی

---

* دانشجوی کارشناسی ارشد مطالعات آمریکای شمالی دانشگاه تهران

* کارشناس ارشد مطالعات اروپای دانشگاه تهران

مقدمه

بیش از دو دهه است که اینترنت نقش بسزایی در ارتباطات جهانی ایفا می‌کند و به طور روزافزونی با زندگی مردم جهان عجین شده است. نوآوری‌ها و هزینه کم در این زمینه باعث شده دسترسی، استفاده و عملکرد اینترنت، به میزان قابل توجهی افزایش یابد، به طوری که امروزه اینترنت در سراسر دنیا در حدود ۲ میلیارد کاربر دارد. اینترنت شبکه وسیع جهانی را به وجود آورده که سالانه میلیاردها دلار برای اقتصاد جهانی سودآوری داشته است.

با وجود این، اینترنت دولت‌ها را در مقابل چالش‌های جدید امنیتی قرار داده است. هزینه کم ورود، ناشناس‌بودن، مشخص‌نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان‌یافته و تروریستی و حتی افراد به این فضا وارد شده و تهدیدهایی همچون جنگ سایبری، جرایم سایبری، تروریسم سایبری، جاسوسی سایبری و مانند آنها را به وجود آورند. همین نکته، تهدیدهای سایبری را از تهدیدهای سنتی امنیت ملی که تا حدود زیادی از ماهیت شفافی برخوردارند و بازیگران آن را دولت- ملت‌هایی تشکیل می‌دهند که در یک قلمرو مشخص جغرافیایی قابل شناسایی هستند، متمایز کرده و سبب شده است امنیت ملی به مفهوم سنتی آن در این فضا به چالش کشیده شده و ناکارآمد به حساب آید.

بنابراین، در مقاله پیش رو، به این مسئله می‌پردازیم که ماهیت تهدیدات سایبری جدید چگونه بر امنیت ملی تأثیر می‌گذارد و این اثرگذاری، امنیت ملی را با چه تغییرات مفهومی مواجه می‌کند. برای این منظور، در بخش اول به بررسی ماهیت و چیستی تهدیدهای سایبری، در بخش دوم به مبحث امنیت ملی و برداشت‌های رایج از آن و در بخش سوم و پایانی پژوهش، به سؤال اصلی، یعنی چگونگی تأثیرگذاری تهدیدهای سایبری جدید بر مفهوم امنیت ملی می‌پردازیم.

الف. ماهیت تهدیدات سایبری

تهدیدهای سایبری پدیده‌ای جدید است که در دهه‌های اخیر، همزمان با تحول فن‌آوری اطلاعات و گسترش ارتباطات جهانی از طریق شبکه وسیع اینترنت در سراسر جهان ظهور پیدا کرده است، به گونه‌ای 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 منحصر به فردی است که شناخت از آن را بسیار مهم و ضروری می‌نماید. در این بخش، پس از تعریف تهدیدهای سایبری، ویژگی‌ها و نمودهای آن را به طور مختصر مورد بررسی قرار می‌دهیم.

۱. تعاریف

در همایشی که در ۲ مارس ۲۰۱۰ از سوی مؤسسه بین‌المللی CACI و مؤسسه مطالعاتی نیروی دریایی ایالات متحده با عنوان «تهدیدهای سایبری امنیت ملی و مقابله با چالش‌های پیش روی زنجیره عرضه جهانی» برگزار شد، تهدیدهای سایبری به صورت «وقایعی که به صورت طبیعی و یا توسط انسان (به صورت 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 به عنوان «تأثیر فضا و جامعه‌ای که توسط رایانه‌ها، اطلاعات و ابزارهای الکترونیکی، شبکه‌های دیجیتالی و یا کاربران آن شکل می‌گیرد» تعریف شده است (Lord and Sharp, 2011: 10).

۲. ویژگی‌های تهدیدهای سایبری

تهدیدهای سایبری ویژگی‌های منحصر به فردی دارند. از یک سو، 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 می‌شود:

یک. تعدد بازیگران در فضای سایبری: هزینه کم فن‌آوری رایانه‌ای، اتصال گسترده به اینترنت و سهولت ایجاد یا به دست آوردن نرم‌افزارهای مخرب به این معناست 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).

دو. 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 مدت زمان کم و با سرعت بالایی انجام داد. البته، انجام حملات پیچیده‌تر سایبری نیازمند صرف هزینه‌های بالاتری است (Lord and Sharp, 2011: 20-28).

سه. ناشناس‌ماندن بازیگران و عدم قابلیت ردیابی: اینترنت به عنوان سیستم نامتمرکز طراحی شده و کاربران آن، غالباً 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 (Lord and Sharp : 20-28).

چهار. تأثیرگذاری شگرف: ماهیت خاص فضای سایبری شرایطی را به وجود آورده است که بروز هر اختلال یا وقفه می‌تواند تأثیرات و پیامدهای به مراتب 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 انسان‌ها شود، زیرا در این گونه مواقع، زیرساخت‌ها و سامانه‌های مهم دچار آسیب می‌شوند (Lord and Sharp: 20-28).

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

شش. 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 جداکردن 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 فن‌آوری در حال تکامل برای پشتیبانی از سیستم‌های حیاتی است (Haller and Et al, 2010: 4).

هفت. پایین‌بودن 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 عبارتند از: جنگ سایبری، تروریسم سایبری، جرایم 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 این فضا برای رسیدن به اهداف سیاسی خود هستند. به منظور درک اینکه آیا عمل خصمانه در فضای مجازی جنگ قلمداد می‌شود یا نه، لازم است قصد بازیگر را درک کنیم. به عنوان مثال، اگر هدف از یک حمله اینترنتی سود مالی یا شخصی از طریق روش‌های مجرمانه مانند سرقت، تقلب و اخاذی باشد، باید با آن به عنوان عمل مجرمانه برخورد شود، اما اگر هدف مهاجم با جاه‌طلبی‌های به مراتب بزرگتر همچون واردکردن آسیب جدی به دولت یا شهروندان آن همچون تخریب، تضعیف و غیرفعال کردن زیرساخت‌های نظامی و غیرنظامی باشد، چنین رفتاری در واقع چیزی

1. Cyber War

نزدیک به اقدام جنگی در مفهوم سنتی است (Cornish and Et al,2010: 12 -13). در سال ۲۰۰۷، استونی به عنوان کشور کوچک مدرن در مقیاس بزرگ مورد حمله‌های اینترنتی قرار گرفت. فن‌آوری بالای این کشور زمینه‌ای مناسب برای حمله‌های اینترنتی با انگیزه‌های سیاسی بود (Tiirma-Klaar, 2011). همانطور که ریچارد کلارک[1] استدلال می‌کند، جنگ سایبری شکل جدیدی از مبارزه است که ما هنوز نمی‌توانیم آن را به طور کامل درک کنیم. در عین حال، روشن است که در دنیای امروز، میدان جنگ حوزه خود رابه فضای مجازی گسترش داده و باید آن را به عنوان پنجمین عرصه جنگ در کنار عرصه‌های سنتی زمین، هوا، دریا و فضا در نظر 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 صحت یا درستی داده‌هاست که معمولاً از طریق کدهای مخرب و تغییر در منطق برنامه و کنترل داده‌ها که منجر به خروجی‌های اشتباه می‌شود، صورت می‌گیرد (Rodriguez, 2006: 9-10). حمله‌های سایبری شامل چهار حوزه می‌شود:۱- از دست دادن تمامیت، ۲- از دست دادن قابلیت، ۳- از دست دادن اطلاعات محرمانه و ٤- تخریب فیزیکی (Army, 2005: 1-3). آب، برق، بانکداری و حمل‌ونقل هوایی، تنها چند نمونه از خدماتی است که توسط زیرساخت‌های اطلاعات و ارتباطات در حال اجراست. این زیرساخت‌ها به طور فزاینده‌ای به یکدیگر وابسته هستند و هر حمله اینترنتی می‌تواند همانند بازی دومینو در آنها اختلال ایجاد کند. اختلال در یک سیستم مساوی با اختلال در دیگر سیستم‌هاست و ادامه این روند از تأثیرات بالقوه حملات اینترنتی است (Islan and Et al, 2011: 5-6).

---

1. Richard Clarke
2. Cyber Attacks

۳-۳. تروریسم سایبری[1]

آژانس مدیریت فوق‌العاده فدرال[2]، تروریسم سایبری را اینگونه تعریف می‌کند: تهدید و حمله غیرقانونی علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره‌شده در آن، زمانی که برای ترساندن یا مجبورکردن حکومت یا مردم آن در پیشبرد اهداف سیاسی یا اجتماعی صورت می‌گیرد (Congressional Research Service, 2008:4). تروریست‌ها با از دست دادن پایگاه‌های فیزیکی کلیدی (مانند افغانستان)، به عامل کلیدی برای اقدام در فضای سایبری تبدیل شده‌اند. این اقدام‌های می‌تواند شامل افزایش منابع برای حمایت از عملیات‌های خود، برنامه‌ریزی عملیات (استفاده از ابزارهای در دسترس همانند Google earth)، فرماندهی و کنترل عملیات، انجام عملیات‌های نفوذی و آموزش به هواداران خود (استقرار وسایل انفجاری) باشد(Starr, 2009:18).

۳-٤. جرایم سایبری[3]

جرایم اینترنتی می‌تواند نقض حق مالکیت معنوی، نقض حق اختراع، ربودن اسرار تجاری و غیره باشد. این جرایم، همچنین شامل حمله عمدی به رایانه‌ها به منظور مختل‌کردن آنها و یا کپی از اطلاعات طبقه‌بندی‌شده می‌شود (Nagre and Warade, 2008: 5). تحلیل‌گران هزینه جرایم اینترنتی را برای صنعت جهانی بیش از هزار میلیارد دلار در موارد نقض مالکیت فکری و از دست دادن اطلاعات تخمین زده‌اند. برای مثال، شخصی در سال ۲۰۰۹، چندین ترابایت از داده‌های مربوط به سیستم الکترونیکی و طراحی اطلاعات از برنامه جنگنده‌های مشترک ۳۰۰ میلیارد دلاری پنتاگون را به سرقت برد. علاوه بر این، بیشتر مجرمان اینترنتی از مجازات فرار کرده‌اند. بدیهی است این فعالیت پرسود و اغلب بدون مجازات، در واقع تهدیدی برای امنیت ملی است (Peritz and Sechrist, 2010:5-7).

---

1. Cyber Terrorism
2. Federal Emergency Management Agency
3. Cyber Crime

۳-۵. جاسوسی سایبری[1]

جاسوسی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا اطلاعات محرمانه را جمع‌آوری کند. برخلاف جرایم 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 دزدیده‌شده را با اهداف مختلف مورد استفاده قرار می‌دهند که برخی از آنها عبارتند از تهدید، اخاذی و مختل‌کردن اقدامات رقبای سیاسی (Lord and Sharp, 2011: 17).

۳-٦. آشفتگی سایبری[2]

آشفتگی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا هدف مورد نظر خود را ناقص کرده، تحت تأثیر قرار داده و 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 نیهیلیست‌ها از آشفتگی سایبری استفاده می‌کنند. به عنوان مثال، گروهی تحت عنوان «ناشناخته‌ها» در واکنش به دستگیری جولیان آسانژ[3]، مدیر سایت جنجالی ویکی‌لیکس، حمله‌های سایبری گسترده‌ای انجام دادند. برخلاف جرایم 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 و یا تغییر یابد و یا هزینه‌های مادی فراوانی به شبکه‌های هدف وارد شود، اما قصد و نیت اصلی آشفتگی سایبری، آسیب‌رساندن است. بازیگران دولتی و غیردولتی می‌توانند از این ابزار استفاده کنند، ولی تا کنون آشفتگی سایبری توسط افرادی انجام شده که با نام فعالان عرصه هک شناخته شده‌اند (Lord and Sharp: 18).

---

1. Cyber Espionage
2. Cyber Agitation
3. Julian Assange

تهدیدهای سایبری از ماهیتی متنوع، گسترده و منحصر به فرد 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 بالاست. گستردگی نیز از آن رو که نه تنها بازیگران دولتی، بلکه شرکت‌های خصوصی، گروه‌ها و افراد را نیز درگیر خود کرده است و منحصر به فرد بودن نیز بدین علت است که ماهیت این تهدیدها متمایز از تهدیدهای سنتی و رایج گذشته است که البته، این ویژگی بیشتر دولت‌ها و درک آنها از تهدید را تحت تأثیر قرار داده است.

ب. امنیت ملی: برداشت‌های رایج

همزمان با به وجود آمدن دولت- ملت و گسترش کارویژه‌های آن، امنیت ملی به عنوان یکی از مهم‌ترین این کارویژه‌ها در دستور کار دولت‌ها قرار گرفت، به طوری که اکثریت قریب به اتفاق 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. در این بخش، علاوه بر ارائه تعریف‌های متفاوت از امنیت ملی، به مهمترین رویکردهای نظری رایج در این زمینه می‌پردازیم.

۱. تعاریف و ویژگی‌های امنیت ملی

تعاریف مندرج در فرهنگ‌های لغت درباره مفهوم کلی امنیت، بر روی «احساس آزادی از ترس» یا «احساس ایمنی» که ناظر بر امنیت مادی و روانی است، تأکید دارند (مندل، ۱۳۷۹: ٤٤). چندبعدی‌بودن مفهوم امنیت ملی سبب شده است دیدگاه‌های بسیار متنوعی راجع به آن وجود داشته باشد و هر کسی از زاویه دید خود به تعریف آن بپردازد. در همین راستا، برخی از نظریه‌پردازان، امنیت ملی را معادل با ارزش‌های حیاتی کشور می‌دانند، بدانگونه که آرنولد ولفرز آن را برابر با «نبود تهدید برای ارزش‌های اکتسابی» می‌داند (Wolfers, 1962: 150).

بری بوزان نیز امنیت را «رهایی از تهدید و توانایی دولت و جوامع برای حفظ هویت مستقل و یکپارچگی کارکردی در مقابل نیروی تغییردهنده» تعریف می‌کند (Buzan, 1991: 432) . در عین حال، یکی از کامل‌ترین تعاریف را ریچارد اولمن[1] ارائه کرده است:

«تهدید امنیت ملی اقدام یا سلسله رویدادهایی است که نخست، به شکلی مؤثر و در دوره زمانی کوتاه خطر افت کیفیت زندگی را برای ساکنان کشور پیش آورد و دوم، با خطر جدی کاهش طیف خط مشی‌هایی که حکومت یا واحدهای غیرحکومتی خصوصی موجود در داخل کشور (اشخاص، گروه‌ها، شرکت‌ها) می‌توانند از میان آنها دست به انتخاب زنند، همراه باشد. مسلماً با این تعریف تصور ما از عوامل تهدیدزا دامنه بیشتری می‌یابد» (تریف، ۱۳۸۳: ٤۹).

در مورد خصوصیات و ویژگی‌های امنیت ملی نیز تحلیل‌گران به طور عمده بر روی سه ویژگی تحول‌پذیری، نسبی‌بودن و ذهنی‌بودن مفهوم امنیت ملی تأکید می‌کنند. در مورد ویژگی اول، یعنی تحول‌پذیری مفهوم امنیت ملی باید گفت به دلیل نیاز حکومت به تعریف مشخصی از امنیت ملی، صاحب‌نظران کوشیده‌اند به این مهم دست یابند، اما تا کنون هیچیک از آنان تعریف جامعی از این مفهوم ارائه نداده‌اند. در مورد ویژگی دوم یعنی نسبی‌بودن نیز باید افزود که ادعای دست‌یابی به امنیت مطلق، قابل تصور نیست. کشوری که ممکن است از لحاظ نظامی و اقتصادی دچار ناامنی نباشد، تهدیدهایی با ماهیت فرهنگی و اجتماعی، امنیت آن را در معرض خطر قرار دهد. جنبه دیگر نسبی‌بودن امنیت، توانایی‌های نسبی دولت‌ها برای مقابله با تهدیدهاست (درویشی سه‌تلانی، ۱۳۷٦: ۲۳).

ویژگی آخر یعنی ذهنی‌بودن امنیت به برداشت‌ها از احساس امنیت یا عدم امنیت مربوط می‌شود و ممکن است افراد و گروه‌های مختلف نسبت به آن نظر واحدی نداشته باشند (روشندل، ۱۳۷٤: ۱٤).

---

1. Richard Ullman

۲. 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 بین‌الملل نیست و در این راستا ناامنی ویژگی بارز نظام بین‌الملل است (عبدالله‌خانی،۱۳۸۲:۷۰). از نظر واقع‌گرایان، عدم امنیت اصلی‌ترین مسأله، قدرت مهم‌ترین ابزار، دولت مهم‌ترین بازیگر و جنگ، بارزترین جلوه بروز ناامنی در عرصه بین‌المللی است (یزدان‌فام، ۱۳۸٦: ۷۳۱). 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 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 (عبدالله‌خانی،۱۳۸۲: ۸۳).

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 به عنوان 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، راه حل متفاوتی دارد. صاحب‌نظران این نظریه بر این باورند که برای

---

1. Stephen Walt

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 (یزدان‌فام، ١٣٨٦: ٧٣٢).

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، ١٣٧٨: ٨). از نظر مکتب کپنهاگ، اگرچه امنیت فردی گویای سطح مشخص و مهمی از تحلیل است، اما افراد نمی‌توانند به عنوان مرجع امنیت شناخته شوند، چرا که اصولاً تابع ساختارهای سیاسی عالی‌تر دولتی و بین‌المللی می‌باشند. بنابراین، مکتب کپنهاک نیز با رد فردمحوری در مرجع امنیت، تمرکز خود را بر دولت به عنوان محور امنیت قرار می‌دهد (عبدالله‌خانی،١٣٨٢). بوزان در یکی از نوشته‌های خود با عنوان «الگوی جدید مطالعه امنیتی در قرن ٢١»، 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 به عنوان دستورالعمل، وارد بررسی‌های امنیتی و سیاست خارجی دولت‌ها کرد. در این چارچوب، دولت‌ها بر اساس هویت‌شان، دشمنان، رقبا و دوستان خود را درک می‌کنند و در این فرایند، هویت خود را تعریف و بازتعریف می‌نمایند. امنیت بر وضعیت مادی بیرونی دلالت ندارد، بلکه مفهومی است اجتماعی، بیناذهنی و معنایی که در فرایند اجتماعی برساخته‌شده و قوام می‌یابد. توجه به امنیت انسانی، به عنوان مرجع نهایی امنیت و گرایش به مفاهیم جهان‌شمول در امنیت جهانی، از ویژگی‌های نظریه سازه‌انگاری است (یزدان‌فام، ١٣٨٦: ٧٣٧).البته، باید اضافه کرد که برخی نویسندگان همچون جسیکا تاچمن به دنبال برخی تحولات جهانی بر گسترش مطالعات امنیتی به مسائلی همچون تهدیدهای زیست‌محیطی، رفاه اقتصادی و رشد جمعیت تأکید کرده‌اند (Tuchman, 1989: 162-177).

بنابراین، با این بررسی هر چند اجمالی، در پایان این بخش به همان نتیجه‌ای می‌رسیم که بری بوزان در مطالعات امنیتی خود رسیده است. وی تشریح می‌کند که «امنیت ملی از لحاظ مفهومی ضعیف، از نظر تعریف مبهم، ولی از نظر سیاسی مفهومی قدرتمند باقی مانده است» (مندل، ١٣٧٩: ٥٥). در نتیجه، هیچ‌یک از تعاریف و رویکردهای مربوطه نتوانسته‌اند به خوبی و

همه‌جانبه از پس تحلیل موضوع امنیت ملی برآمده و هر یک از ظن خود به این مقوله نگریسته و تنها بخشی از واقعیت‌های موجود آن را تشریح کرده‌اند. این پیچیدگی مفهوم امنیت با واردشدن مباحث مربوط به فضای سایبری و تهدیدهای مرتبط با آن در دو سه دهه گذشته، دوچندان شده است. اگر تا پیش از این، فضای مفهومی و تحلیلی امنیت بر مبنای درک مشخصی از مرزهای جغرافیایی تهدید و منابع تهدیدکننده استوار بود، در عصر اطلاعات و با کشیده‌شدن مفهوم امنیت به فضای مجازی، نه تنها درک روشنی از فضای جغرافیایی تهدید وجود ندارد، بلکه با گستردگی منابع تهدیدکننده امنیت نیز مواجه هستیم.

ج. تأثیر تهدیدهای سایبری بر امنیت ملی

بسیاری از کارشناسان و تحلیل‌گران حوزه امنیت، بر این باورند که پایان‌یافتن دوران جنگ سرد نه تنها منجر به امن‌ترشدن جهان نشده است، بلکه 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" نه تنها بازاندیشی در تهدیدهای امنیتی، بلکه تجدید نظر 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 به عنوان 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 به عنوان یکی از بدترین تهدیدهای منافع ملی به تصویر کشیده است تا جایی که ایالات متحده آمریکا اعلام کرده است که این حملات را به عنوان جنگ تلقی کرده و با آن برخورد فیزیکی خواهد کرد. از طرف دیگر، بحث و گفتگو درباره این تهدیدات متأثر از انقلاب مداوم اطلاعات و رسوخ آن به تمام جنبه‌های زندگی بشر امروز است. بنابراین، در بخش پیش رو، ابتدا به انقلاب اطلاعات و تأثیر شگرفی که بر روی قدرت و منابع آن خواهد داشت

پرداخته و سپس از این رهگذر، تهدیدهای سایبری وابسته به آن و تأثیری که می‌تواند بر امنیت ملی داشته باشد، مورد بررسی قرار خواهد گرفت.

۱. قدرت در عصر جدید

در علوم سیاسی، قدرت و امنیت دو مفهوم کاملاً وابسته به هم می‌باشند و به جرأت می‌توان گفت شاید نتوان اندیشمندی را در این حوزه یافت که وابستگی این مفاهیم را به یکدیگر رد کند. در طول سده‌های اخیر، تحول در مفهوم قدرت و منابع وابسته به آن، تغییر در مفهوم امنیت و تحولات وابسته به آن را به دنبال داشته است. در عصر جدید و به دنبال انقلابی که در اطلاعات رخ داده است، به نظر می‌رسد بار دیگر منابع قدرت در کشورها با دگرگونی عمیقی مواجه شده که به تبع خود، مفهوم امنیت را نیز با تحولاتی مواجه نموده است.

همانگونه که فرانسیس بیکن[1] چهارصد سال پیش نوشت، اطلاعات قدرت است. انقلاب اطلاعات را به معنی پیشرفت‌های سریع فناوری در عرصه رایانه‌ها، ارتباطات و نرم‌افزار می‌دانیم که با خود کاهش چشمگیر هزینه پردازش و انتقال اطلاعات را به همراه آورده است (روزنا و دیگران، ۱۳۹۰: ۳٦۲). جهان در حال حاضر به عصر جدیدی وارد شده که ویژگی‌های خاص خود را دارد. تجارت الکترونیک، فعالیت‌های اقتصادی شبکه‌ای و جهانی مبتنی بر اطلاعات، از ویژگی‌های این عصر است. غالب مبادلات و معاملات اقتصاد کنونی از نوع اطلاعات است تا کالاهای فیزیکی (میرمحمدی و محمدی لرد، ۱۳۸۷: ۵۲).

می‌توان میان قدرت رفتاری،[2] یعنی توانایی به دست آوردن نتایج مطلوبمان و قدرت منابع[3]، یعنی در اختیار داشتن منابعی که معمولاً با توانایی به دست آوردن نتایج مطلوب مرتبط شناخته می‌شوند، تمایزی اساسی قائل شد. انقلاب اطلاعات، گذشته از قدرت رفتاری، بر قدرتی هم که بر حسب منابع سنجیده می‌شود، تأثیر می‌گذارد (روزنا و دیگران، ۱۳۹۰:۳٦۷). در همین رابطه، برخی ناظران معتقدند منابع قدرت عموماً در حال تغییرند؛ بدین صورت که به تدریج تأکید کمتری روی نیروی نظامی به عنوان منبع قدرت صورت می‌گیرد. امروزه در ارزیابی قدرت

---

1. Francis Bacon
2. Behavioral Power
3. Resource Power

بین‌المللی، عواملی همچون فن‌آوری، آموزش و رشد اقتصادی اهمیت بیشتری یافته‌اند و در همین حال، اهمیت جغرافیا و مواد خام کاهش یافته است. با نگاهی به قرون گذشته روشن می‌شود که در هر دوره، منابع متفاوتی از قدرت نقش بیشتری ایفا کرده‌اند. منابع قدرت هیچگاه حالت ایستا ندارد و در دنیای امروز نیز همچنان تغییرات را تجربه می‌کند (نای، ۱۳۸۷: ۹۸).

در سده هجدهم، سرزمین، جمعیت و کشاورزی منبع قدرت تعیین‌کننده بود. در سده نوزدهم، ظرفیت صنعتی، در میانه سده بیستم نیز علم و به ویژه فیزیک هسته‌ای، منابع قدرت تعیین‌کننده‌ای در اختیار قدرت‌ها قرار داده بود. در سده حاضر، توانایی اطلاعاتی در تعریف وسیع خود، احتمالاً تعیین‌کننده‌ترین منبع قدرت است (روزنا و دیگران، ۱۳۹۰ :۳۶۹). (ر.ک. جدول ۱) در همین ارتباط، می‌توان به نظریه‌های مختلفی در زمینه منابع قدرت اشاره کرد که بر دیدگاه قدرت‌ها و راهبرد آنها در حوزه قدرت تأثیر شگرفی داشته است، نظریه‌هایی همانند قدرت زمین از مکیندر، نیروی دریایی از ماهان و نیروی هوایی از دوهه از این جمله‌اند (Starr, 2009: 13).

جدول شماره ۱- منابع عمده قدرت در سده‌های گذشته

دوره	منبع عمده قدرت
قرن ١٦	شمش طلا، تجارت استعماری، ارتش‌های متشکل از سربازان مزدور، پیوند میان سلسله‌های پادشاهی
قرن ١٧	تجارت، بازارهای سرمایه، حمل و نقل و نیروی دریایی
قرن ١٨	جمعیت، کشاورزی، صنعت مناطق روستایی، دستگاه دولتی، ارتش
قرن ١٩	ظرفیت صنعتی، همبستگی سیاسی، امور مالی و اعتباری، نیروی دریایی، هنجارهای لیبرالی، جغرافیا
قرن ٢٠	بزرگی اقتصاد ملی، پیشتازی در حوزه علمی و تکنیکی خصوصاً فیزیک هسته‌ای، نیروی نظامی و ائتلاف‌ها، رژیم‌های بین‌المللی
قرن ٢١	فناوری اطلاعات و توانایی اطلاعاتی، شبکه‌های جهانی، ارتباطات، شرکت‌های بزرگ چندملیتی

منبع: جیمزروزنا و دیگران، انقلاب اطلاعات، امنیت و فناوری‌های جدید، ۱۳۹۰

توانایی استفاده از فضای سایبری، یکی از مهم‌ترین منابع قدرت در قرن ۲۱ به حساب می‌آید. بازیگران دولتی و غیردولتی از این قدرت استفاده می‌کنند تا به اهداف اجتماعی، ایدئولوژیکی، سیاسی، نظامی و مالی خود در فضای سایبری و دنیای واقعی دست یابند. افزایش سرعت فرایندها و ساختارهای پیشرفته، وابستگی بیشتر به اینترنت را به همراه داشته و باعث شده سالانه میلیاردها دلار به اقتصاد جهانی اضافه شود. تجارت اینترنتی در سطح جهان در سال ۲۰۱۰، در حدود ۱۰ تریلیون دلار بوده و تخمین زده می‌شود این آمار در سال ۲۰۲۰، به ٢٤ تریلیون دلار برسد. شرکت‌های اینترنتی تازه‌تأسیس، کارآفرینی زیادی در اقتصاد جهانی ایجاد کرده و در حالی که کسب و کارهای قدیمی را به چالش می‌کشد، محصولات بهتر و جدیدتری به مشتریان ارائه می‌کند (Lord and Sharp, 2011: 22).

از این رو، قدرت اطلاعات در عصر کنونی نقش مهمی در معادلات جهانی دارد. در همین رابطه، جوزف نای[1] مقاله جالبی را با عنوان "قدرت سایبری[2]" به رشته تحریر در آورده است. وی برای تشریح قدرت در عصر اطلاعات از مفهوم "انتشار قدرت[3]" کمک گرفته است. نای در این مقاله قدرت وابسته به فضای سایبری را یکی از مهم‌ترین زمینه‌های جدید در سیاست جهانی می‌داند و آن را اینگونه تعریف می‌کند:"قدرت سایبری توانایی به دست آوردن نتایج ترجیح داده شده از طریق استفاده از منابع الکترونیکی در ارتباط با اطلاعات در دامنه سایبری است"(Nye, 2010: 4). وی می‌افزاید، قیمت پایین ورود، گمنامی، آسیب‌پذیری و نامتقارن‌بودن به این معنی است که بازیگران کوچکتر، از ظرفیت بیشتری برای اعمال قدرت سخت و نرم در فضای مجازی در حوزه‌های سنتی‌تر سیاست جهانی برخوردارند. تغییر در اطلاعات همواره نقش مهمی در قدرت دارد، اما دامنه سایبری هم جدید است و هم محیطی است که ساخته دست انسان می‌باشد. از ویژگی‌های فضای سایبری این است که تفاوت قدرت میان بازیگران را کاهش می‌دهد و در نتیجه، یک مثال خوب از انتشار قدرت را فراهم می‌کند که نشانگر

---

1. Joseph Nye
2. Cyber Power
3. Diffusion of Power

سیاست جهانی در قرن ۲۱ است. انتقال قدرت از دولت مسلط به دولت دیگر از رویدادهای آشنای تاریخی است، اما انتشار قدرت، فرایند جدید است. این مشکل تمامی کشورها در عصر اطلاعات است. نای اضافه می‌کند که بزرگترین قدرت بعید است که قادر به تسلط در این حوزه به اندازه دیگر حوزه‌ها، همچون دریا و هوا باشد. با وجود این، فضای سایبری این نکته را نشان می‌دهد که انتشار قدرت به معنی برابری قدرت یا جایگزینی دولت به عنوان قدرتمندترین بازیگر در سیاست جهانی نیست (Nye, 2010: 19).

بنابراین، اینترنت شرایطی را به وجود آورده که در آن، قدرت کنترل بر اطلاعات به میزان بسیار بیشتری توزیع شده است. اینترنت زمینه ارتباطات نامحدود فرد به فرد (از طریق ایمیل)، فرد به تعداد بیشتری از افراد (از طریق هوم پیج[1] شخصی یا کنفرانس الکترونیکی) را فراهم می‌کند. اینترنت، همچنین قادر است زمینه ارتباط با شمار زیادی از افراد با یک فرد (از طریق پخش برنامه الکترونیکی) را فراهم کند. شاید مهمتر از این، اینترنت شمار بیشتری از افراد را با شمار بسیاری دیگر (از طریق اتاق گفتگوی همزمان) مرتبط می‌کند. پیام‌های اینترنتی از این توان برخوردارند که به میزان بیشتر و سریعتر و با دخالت کمتری از سوی دیگران، جریان پیدا کنند. در این شرایط، حکومت‌ها اگر بخواهند جریان اطلاعات را از راه کنترل اینترنت کنترل نمایند، ناچار به تحمیل هزینه‌های بالایی خواهند شد و در آخر کار از تلاش‌های خود ثمر چندانی نخواهند گرفت. این تحول بدین معناست که سیاست خارجی، عرصه‌ای نخواهد بود که صرفاً حکومت‌ها در آن حضور داشته باشند، بلکه سازمان‌های مرتبط با افراد و بخش خصوصی، در داخل و خارج از کشور از این توان برخوردار خواهند شد که نقش مستقیمی در سیاست جهانی ایفا کنند (نای، ۱۳۸۷:۱٤۱). در نتیجه، اینترنت از طریق همین ابزارهای ارتباطی، ناراضیان را یکصدا کرده تا شنیده شوند و به عموم مردم وسیله‌ای داده است تا سازماندهی شوند. در حالی که برخی تحلیل‌گران نقش اینترنت در انقلاب‌های خاورمیانه و شمال آفریقا را انکار می‌کنند، شبکه‌های اجتماعی همچون توئیتر و

1. Homepage

فیس‌بوک، نقش بسزایی در شکل‌گیری این حوادث داشته‌اند. از سوی دیگر، اینترنت می‌تواند مورد سوءاستفاده دیکتاتورها و تروریست‌ها نیز قرار بگیرد. به عبارت دیگر، دیکتاتورها و گروه‌های افراطی نیز با استفاده از همین روش، ایدئولوژی خود را گسترش داده و در سرتاسر دنیا عضو می‌گیرند (Lord and Sharp, 2011: 14).

البته، نای معتقد است با وجود چنین تحولاتی، دولت‌ها همچنان به عنوان بازیگر غالب در صحنه جهانی باقی خواهند ماند، اما کنترل آنها بر مسائل مشکل و پیچیده‌تر خواهد شد. بخش وسیعی از جمعیت، هم در داخل کشورها و هم در روابط میان کشورها به قدرتی دسترسی پیدا می‌کنند که از اطلاعات بر می‌آید. از سوی دیگر، فضای سایبری جایگزین فضای جغرافیایی نخواهد شد و حاکمیت دولت را لغو نمی‌کند، اما انتشار قدرت در فضای سایبری اعمال قدرت را پیچیده‌تر خواهد کرد (Nye, 2010: 3).

بنابراین، همانگونه که عنوان شد، در عصر جدید با توجه به توسعه فناوری اطلاعات و گسترش ارتباطات ناشی از آن، منابع قدرت دچار تحول و دگرگونی گسترده‌ای شده‌اند. دگرگونی منابع قدرت در عصر حاضر به دلیل ویژگی‌های خاص خود، تعدد بازیگران را در عرصه قدرت به دنبال داشته و این تعدد بازیگران نیز به نوبه خود، عرصه کنترل و اعمال قدرت را بر دولت‌ها تنگ نموده است. از این رو، با چنین تحولی در مفهوم قدرت و با توجه به وابستگی پیش‌گفته میان مفاهیم قدرت و امنیت، به طور کاملاً طبیعی، مفهوم امنیت نیز دچار تغییر و دگرگونی‌های عمیقی خواهد شد که در بخش بعدی مقاله بدان اشاره خواهد شد. در پایان این بخش، ابعاد فیزیکی و مجازی قدرت سایبری از نظر جوزف نای در قالب جدول به تصویر کشیده شده است.

جدول شماره ۲- ابعاد فیزیکی و مجازی قدرت سایبری

	اهداف قدرت سایبری	
	درون فضای سایبری	**بیرون فضای سایبری**
ابزارهای اطلاعاتی	سخت: ممانعت از حملات نرم: تعیین نرم‌ها و استانداردها	سخت: حمله به سامانه‌های SCADA نرم: انجام دیپلماسی عمومی با هدف ترغیب افکار عمومی
ابزارهای فیزیکی	سخت: کنترل دولت بر شرکت‌ها نرم: ایجاد زیرساخت‌هایی با هدف کمک به فعالان حقوق بشر	سخت: قطع کابل‌ها و بمباران و نرم: برگزاری اعتراض به فراهم کنندگان حمله‌های سایبری

۲. امنیت در عصر جدید

امنیت ملی امروزه با تهدیدهای بیشماری مواجه است، اما در این میان، تهدیدهای سایبری پدیده جدیدی است که همراه با فناوری اطلاعات و گسترش ارتباطات گریبان‌گیر دولت‌ها شده است. این پدیده آنقدر جدید است که بررسی پیامدهای آن برای امنیت ملی دولت‌ها تا حد زیادی مورد غفلت واقع شده است. در دو دهه اخیر یک طیف، گرایش به زیر سؤال بردن رویکرد رایجی که درباره امنیت در چارچوب مطالعات راهبردی در طول دوره جنگ سرد توسعه داده شده است، دارند. این گرایش تأکید بر ضرورت فرارفتن از آنچه در بسیاری از نگرش‌ها به عنوان تفسیر بیش از حد نظامی‌شده از امنیت در نظر گرفته شده و ملازم با ظهور چالش‌های امنیتی جدید بوده است، دارد (کلارک، ۱۳۸٦: ۲۳٦). از نظر این گروه، امروزه دیگر تهدیدهای امنیتی صرفاً نظامی نیست، بلکه مسائل زیست‌محیطی، فقر جهانی، مهاجرت و اخیراً تهدیدهای سایبری بیش از تهدیدهای نظامی، امنیت دولت‌ها را به خطر انداخته است.

بحث درباره تهدیدهای سایبری تأثیر گرفته از انقلاب مداوم اطلاعات می‌باشد که ناشی از پویایی انتشار اطلاعات و تکنولوژی‌های ارتباطات در همه جنبه‌های زندگی انسان است (Cavetly and Brunner, 2007: 15).

در طول دهه گذشته، شماری از ویژگی‌های عمومی حملاتی که به وسیله کامپیوتر شکل گرفته و به تهدیدهای سایبری معروف شده‌اند، به عنوان یکی از بدترین تهدیدهای منافع ملی امروز شناسایی شده است (Cavetly, 2010: 180). با توجه به آنچه گفته شد، می‌توان امنیت سایبری را به طور کلی به عنوان «حفاظت از زیرساخت‌های اطلاعاتی مهم و فرایندها و محتوای آن تعریف کرد»(Theohary and Rollins, 2009). بنابراین، همانطور که یکی از مهمترین بخش‌های قدرت ملی امروز از قدرت اطلاعات بر می‌خیزد، یکی از مهمترین بخش‌های امنیت ملی نیز از امنیت و حفاظت از اطلاعات بر می‌آید.

به موازات افزایش ابعاد خدمات‌رسانی اینترنت در حوزه‌های مختلف زندگی بشر و به ویژه در امور تجاری و بازرگانی، مهاجمان رایانه‌ای، سارقان و جاسوسان اطلاعاتی، حجم تهدیدها و آسیب‌های ناشی از این فناوری را به شدت افزایش داده‌اند. این تهدیدها امروزه علاوه بر اینکه روز به روز گسترش می‌یابند و پیچیده‌تر می‌شوند، امنیت ملی کشورها و دولت‌ها را به طور مستقیم تحت تأثیر قرار می‌دهند (میرمحمدی و محمدی‌لرد، ۱۳۸۷: ۳٦).

حجم و گستردگی این تهدیدها به حدی است که ایالات متحده آمریکا اعتراف کرده است که این برای اولین بار در طول تاریخ است که به تنهایی نمی‌تواند از زیرساخت‌هایش حمایت کند. آمریکایی‌ها اعتراف کرده‌اند که نمی‌توانند ارتش و یا نیروی پلیس به اندازه کافی بزرگی را برای حمایت از تمامی خطوط تلفن و یا شبکه‌های کامپیوتری شهروندان آمریکا، به خدمت بگیرند، به خصوص زمانی که ۹۵ درصد از این زیرساخت‌ها متعلق به بخش خصوصی هستند (Vatis, 2002: 2).

البته این خود منوط به این است که به کارگیری ارتش و نیروی پلیس بتواند در مقابله با این تهدیدها کارساز باشد که با توجه به ویژگی‌های خاص پیش‌گفته در مورد ماهیت تهدیدهای سایبری، کارایی این نیروها برای مقابله با این تهدیدها محل تردید است.

مسایلی که به نظر می‌رسد نه تنها ایالات متحده، بلکه تمامی کشورها در رابطه با تلاش‌های امنیت سایبری با آن مواجه هستند، شامل:

- عدم اطمینان از موقعیت جغرافیایی عاملان حملات اینترنتی
- ادغام در حال تحول دستگاه‌های فناوری تلفن همراه به زیرساخت‌های اطلاعاتی حساس
- آسیب‌پذیری‌های جدید به زیرساخت‌های کشور از تهدیدهای پیچیده و فزاینده
- ضعف هماهنگی بخش دولتی و خصوصی به خطرات در حال ظهور؛ و
- ابهامات قانونی برای پاسخ به اینگونه حمله‌هاست (Theohary and Rollins, 2009).

این مسایل دست کم چهار پیامد مهم را برای دولت‌های ملی در پی خواهد داشت: نخست، تغییر برداشت دولت‌ها درباره چگونگی تعریف منافع، پایگاه‌های قدرت و امنیت‌شان؛ دوم، بالاگرفتن چالش‌هایی در برابر توانایی دولت‌ها برای اداره و کنترل انتشار اطلاعات (روزنا و دیگران، ۱۳۹۰: ۱۳۰). سوم، ارتباط موضوع امنیت با شبکه‌های جهانی و چهارم، کاهش ظرفیت دولت‌ها در تولید امنیت شهروندان خود (کلارک، ۱۳۸٦: ۲٤۳).

بنابراین، از گفته بالا چنین بر می‌آید که مفهوم امنیت ملی سنتی، به معنای نبود تهدید علیه ارزش‌های حیاتی کشور نیز در حال تغییر است. آسیب واردشدن از محل دستکاری در زیرساخت‌های اطلاعاتی ممکن است از نظر مالی و جانی بیشتر از آثار برخی جنگ‌ها باشد. امروزه، مهاجمان به کشور ممکن است دولت‌ها، گروه‌ها، افراد و یا ترکیبی از آنها باشد. احتمال دارد مهاجمان سرشتی ناشناخته داشته باشند و حتی تا نزدیکی کشور نیز نیایند. به عنوان مثال، در سال ۱۹۹۸، واشنگتن در ارتباط با هفت نشانی اینترنت مسکو[1] که در سرقت اسرار پنتاگون و ناسا دست داشتند، به دولت روسیه اعتراض کرد. روس‌ها پاسخ دادند شماره تلفن‌هایی که با آنها حمله‌های مزبور صورت گرفته است، معتبر نیستند. بنابراین، ایالات متحده راهی نداشت تا بفهمد آیا دولت روسیه در این سرقت شرکت داشته است یا خیر؟ (نای، ۱۳۸۷: ۱٤۷).

---

1. Moscow Internet Address

بر اساس نگرش سنتی، دولت‌ها به تضمین بقای خود و تأمین امنیت نظامی‌شان، اهمیت زیادی می‌دهند. در عین حال، باید توجه داشت که دولت‌ها امروزه ناچارند ابعاد جدیدی از امنیت را در نظر بگیرند. برای مثال، کانادایی‌ها امروزه نگران این نیستند که سربازان آمریکایی برای دومین بار (همانند سال ۱۸۱۳)، تورنتو را در آتش بسوزانند، بلکه از این نگرانند که رایانه‌ای در تگزاس، تورنتو را با مشکلی عمده روبرو کند (نای، ۱۳۸۷: ۱۲٤). مفاهیم سنتی جنگ بر اساس حمله و دفاع، توسط پیچیدگی‌های فضای مجازی به چالش کشیده شده‌اند و با سرعت تغییر پیدا می‌کنند و این تهدید به نوعی مفاهیم سنتی جنگ را تغییر داده است. تهدید سایبر نامتقارن است و از این رو، نیاز به سرمایه‌گذاری بزرگی برای استفاده از آن یا حمله از طریق آن وجود ندارد. در مقابل، دفاع در برابر تهدید سایبر باید تمام جوانب را در نظر بگیرد که هزینه‌های آن امروزه در حال افزایش است (Tabansky, 2011: 88).

مسئله دیگری که از تهدیدهای سایبری بر می‌آید، ناشی از ابهامات قانونی آن است، بدین معنی که قانونی در زمینه فعالیت‌های خرابکارانه سایبری، به خصوص جنگ سایبری وجود ندارد. در قوانین جنگ به شیوه مرسوم و سنتی آن، توافقنامه‌ها و تعهداتی همچون کنواسیون ژنو و منشور سازمان ملل وجود دارد که به صراحت بیان می‌دارند که هیچ ملتی نمی‌تواند از زور علیه تمامیت ارضی یا استقلال سیاسی دیگر کشورها استفاده کند. این در حالی است که دشوار بتوان جنگ سایبری را در این چارچوب تعریف کرد (Markoff and Shanker, 2009).

بنابراین، چالش امنیت سایبری، هم مهم و هم پیچیده است. دستیابی به ترتیبات مؤثر حکومت در این حوزه، به راهبرد جامع که شامل اقدام‌های هماهنگ به وسیله حکومت، بخش خصوصی و شهروندان باشد، نیاز دارد. جامعه جهانی نیز به صورت واضح، منافع مشترکی در حمایت از امنیت سیستم‌های سایبری و همکاری و اقدام فوری در این زمینه دارد (Chertoff, 2008: 484). در راستای چنین اهمیتی بود که در ۲۹ می سال ۲۰۰۹، رئیس جمهور آمریکا اعلام کرد فضای سایبری به عنوان دارایی مهم ملی است که ایالات متحده به تمام معنی از آن دفاع می‌کند (Lewis, 2011: 3).

از این رو، امنیت سایبری در ارتباط مستقیم با امنیت ملی کشور است. امروزه دیگر نمی‌توان امنیت ملی را منحصراً در ارتباط با مرزهای خارجی و حفاظت از جان شهروندان به وسیله نیروهای نظامی تعریف کرد. امروزه به لطف اینترنت و یک دستگاه رایانه، دشمن بدون اینکه متوجه حضور فیزیکی‌اش باشیم، تا خانه‌های ما رخنه کرده است. چنین خطر نافذی، تمامی برداشت‌های رایج و سنتی از مفهوم امنیت ملی را زیر سؤال برده است. در پایان این بخش، آسیب‌پذیری‌های سایبری و انواع دولت‌ها را طی یک نمودار به تصویر می‌کشیم.

نمودار شماره ۳- آسیب‌پذیری‌های سایبری و انواع دولت‌ها (Hare, 2010)

		یکپارچگی سیاسی- اجتماعی (SC)	
		قوی(S)	ضعیف(W)
قدرت (P)	ضعیف (W)	حمله‌های عمده بر روی زیرساخت‌های حساس	اقدامات غیرثبات‌ساز سیاسی در فضای سایبری، حمله به زیرساخت‌های اینترنتی، فعالیت‌های جنایی
	قوی (S)	فعالیت‌های جنایی در فضای سایبری	اقدامات غیرثبات‌ساز در فضای سیاسی

P_W-SC_W: بر اساس این مدل، دولت‌هایی که در یک چهارم بالای سمت چپ قرار دارند، در برابر انواع تهدیدها در فضای سایبری از جمله غیرثبات‌سازی سیاسی، حمله به زیرساخت‌های اینترنتی و اقدامات جنایی که می‌توانند به سرعت سیستم‌های مالی و رفاه شهروندانشان را تضعیف کنند، آسیب‌پذیر هستند. نهادهای حکومتی در این دولت‌ها اغلب فاقد تخصص چگونگی تأمین امنیت سیستم‌های اطلاعاتی‌شان و همچنین، فهم میزان واقعی تهدیدهای پیش رو هستند.

P_W-SC_S: در حالت متداول، اینگونه دولت‌ها بـه رغـم اینکـه دارای انسـجام سیاسـی- اجتماعی هستند، در برابر اغلب تهدیدهای نیروی نظامی آسیب‌پذیرنـد، زیـرا زیرسـاخت‌هـا و جمعیت‌شان در مقابل حمله نظامی آسیب‌پذیر هستند.

P_S-SC_S: این دولت‌ها توانـایی حفـظ نیروهـای اقتصـادی و نظـامی خـود را در نظـام بین‌الملل دارند و اغلب تمایلی به امنیتی‌کردن تهدیدها در فضای سـایبری در سـطوح همسـان آنها که تهدیدهای متدوالی دارند، ندارند.

P_S-SC_W: این دسته کشورها از نظر نظامی قدرتمند هستند، اما فاقد یکپـارچگی سیاسـی- اجتماعی قوی در درون مرزهایشان می‌باشند. این دولت‌ها تمایل به امنیتی‌کردن تهدید غیرثبات‌ساز صادرشده از درون مرزهایشان و احزاب ناسازگار با حاکمیت‌شان دارند (Hare, 2010: 217-219).

۳. رویکردهای نظری و تهدیدهای سایبری

شاید بسیط‌ترین بحث در زمینه امنیت، متعلق به مکتب کپنهـاگ باشـد کـه عرصـه مطالعـات امنیتی را به پنج مقوله از نظامی، سیاسی، اقتصادی، اجتماعی تا بحث تأثیرات امنیتی محیط زیست نیز پیش برده است، اما حتی این مکتب نیز بحث خود را به تأثیرات زیست‌محیطی ختم می‌کند و از تهدیدهای سایبری سخنی به میان نمی‌آورد. با وجـود ایـن، اگرچـه تـا بـه امـروز تهدیـدهای سایبری به رغم اهمیت و گستردگی همچنان و تا حد زیادی از سوی رویکردهای مختلف مـورد بی‌توجهی قرار گرفته است، اما گستردگی تهدیدهای سایبری به حدی است که دیگـر نمـی‌توانـد بیش از این مورد غفلت رویکردهای نظری در روابط بـین‌الملـل قـرار گیـرد. در ایـن بخـش بـه تأثیرگذاری تهدیدهای سایبری بر روی نظریه‌پردازی در روابط بین‌الملل می‌پردازیم.

استفن والت در چارچوب مکتب واقع‌گرایی تدافعی ادعا می‌کند که مطالعات امنیتی بایستی بر روی «پدیده جنگ» که به وسیله قدرت‌های نظامی که تحت کنترل سیاسی بـازیگران دولتـی اداره می‌شوند، تمرکز کند. این مطالعات همچنین می‌تواند شامل کنتـرل تسـلیحات و مـدیریت بحران که به طور مستقیم در ارتباط با مسایل نظامی هستند، باشد. بنـابراین، نوواقـع‌گرایـان در مقابل توسعه دستور کار مطالعـات امنیتـی، شـامل امنیـت سـایبری، مـادامی کـه هنـوز دربـاره تأثیرگذاری واقعی حمله‌های سایبری بر امنیت فیزیکی دولت‌ها و ظرفیت نظامی‌شان مشـاجره

وجود دارد، بحث می‌کنند. در هر صورت، به نظر می‌رسد نوواقع‌گرایان بر روی جایگاه تهدید سایبری در این زمینه توافق ندارند (Hare, 2010: 215). از قرار معلوم، برخورد واقع‌گرایان با چالش انقلاب اطلاعات بسیار شبیه برخوردی است که پیش‌تر با چالش‌های فراملی‌شدن، وابستگی متقابل پیچیده و جهانی‌شدن داشته‌اند. آنها این گرایش‌ها را به چشم یک رشته پی‌پدیدار[1] می‌بینند که کاملاً ممکن است بر سیاست‌ها و ساختارهای داخلی دولت‌ها تأثیر بگذارند، ولی نظام اقتدارگریز سیاست بین‌الملل را متزلزل نمی‌کنند و بنابراین به اولویت دولت به عنوان عالی‌ترین واحد سیاسی لطمه‌ای نمی‌زنند (روزنا و دیگران، ۱۳۹۰:۲۱).

بری بوزان معتقد است مطالعات امنیتی جنبه‌هایی از دستور کار گسترده‌تر و عمیق‌تر دارند. از نظر مکتب کپنهاگ، اگرچه دولت‌ها در مطالعات امنیتی نقش محوری را دارند، اما این عرصه هر بازیگری از سطح فردی و بین‌المللی را شامل شرکت‌ها، دولت‌ها و اجتماعات در بر می‌گیرد. در این حالت، چون از نظر این مکتب مسایل امنیتی حتی اگر در سطح بازیگر فردی و یا تهدید وجودی اقتصادی باشد، مهم‌اند. بنابراین، تهدیدهای سایبری می‌توانند در چارچوب تحلیل مکتب کپنهاگ جای گیرند (Hare, 2010: 214).

لیبرال‌ها هم مانند واقع‌گرایان، دولت‌ها را بازیگران اصلی سیاست جهان می‌دانند، ولی بر خلاف آنها می‌گویند دولت‌ها به هیچ وجه یگانه بازیگرانی نیستند که در روابط بین‌الملل نقش‌های مهمی بازی می‌کنند. در واقع، بارزترین تغییری که در سال‌های اخیر در حوزه سیاست بین‌الملل رخ داده است، سر برآوردن مجموعه گسترده‌ای از بازیگران غیردولتی بین‌المللی جدید (شرکت‌های فرامرزی، جنبش‌های اجتماعی، گروه‌های فشار، شبکه‌های احزاب سیاسی، مهاجران و تروریست‌ها) بوده است. بدین ترتیب، لیبرال‌ها بالقوه می‌توانند به پیدایش گروه‌های اینترنتی جدیدی که در اتاق‌های گفتگوی اینترنتی و «وبلاگ‌ها» و از طریق انواع فناوری‌های دیداری-شنیداری اطلاعات و ارتباطات فعالیت دارند، واقف باشند (روزنا و دیگران، ۱۳۹۰:۲۳).

در معدود تفسیرهای برسازانه‌ای که در حال حاضر درباره امنیت در دوران دیجیتال وجود دارد، به طور عمده بر این تأکید می‌شود که چگونه جنگ اطلاعات، مجموعه متعددی از

---

1. Epiphenomenon

مرزبندی‌ها به ویژه مرزهای هویت را به چالش می‌کشد. ادورارد[1] جنگ اطلاعات پایه را نوع خاصی از «جنگ هویت» می‌داند که در آن تمامی انواع مرزبندی‌ها از جمه تفکیک قدیمی داخلی- بین‌المللی به چالش کشیده می‌شود. بر این اساس، هویت دولت ملی به خطر می‌افتد. البته، این امکان وجود دارد که دولت به جای تسلیم‌شدن در برابر رخنه مداوم به مرزهای رسمی حاکمیت خویش و سر برآوردن و ابراز هویت‌های جدید در فضای مجازی، خود را با آن سازگار کند. تحلیل برسازانه قدرت و امنیت در جهان مجازی، متضمن تأکید بر اهمیت تصورات و نمادها در کنار واقعیت‌های مادی رایانه‌ها و کابل‌هاست (روزنا و دیگران،۱۳۹۰: ۳۰).

نتیجه‌گیری

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 نامتقارن‌بودن، پدیده انتشار قدرت را به وجود آورده است، بدین معنی که اگر تا کنون 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، اگر چه هنوز این دولت‌ها هستند که در این عرصه نقش مهمی را بازی می‌کنند. به طبع، 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 دست کم از جهت شناسایی کار چندان دشواری نبود. سوم، گستردگی آسیب‌پذیری‌های ناشی از تهدیدهای سایبری است. این تهدیدها پراکنده، چندبعدی و چندسویه‌اند و چون در ارتباط با شبکه‌های ارتباطی و زیرساخت‌های حساس می‌باشند، سطح آسیب‌رسانی آنها بسیار بالاست. چهارم، این

1. Edverard

تهدیدها را صرفاً با شیوه‌های سنتی همانند به کارگیری ارتش و نیروی پلیسی نمی‌توان مهار کرد و برای مقابله با آنها تلاش دولت‌ها به تنهایی 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 بر می‌آید، تهدیدهای سایبری صرفاً متوجه دولت‌ها نیست، بلکه افراد و شرکت‌ها نیز از آسیب‌های این تهدیدها بی‌نصیب نخواهند بود. ششم، چون امنیت در عصر اطلاعات صرفاً دولت‌محور نیست، بنابراین رویکردهای مختلف نظری در روابط بین‌الملل که به طور عمده بر مبنای دولت‌محوری به ساختاربندی نظریات خود پرداخته‌اند، یا به راحتی از کنار این تهدیدها گذشته‌اند و یا در تحلیل‌های خود با سردرگمی مواجه شده‌اند. در پایان، ذکر این نکته ضروری است که مجموعه عوامل بالا سبب خواهد شد دولت‌ها و محافل دانشگاهی دیر یا زود در برداشت‌های خود نسبت به منافع، پایگاه‌های قدرت و امنیت‌شان تجدید نظر کنند.

منابع

بوزان، بری (۱۳۷۸)؛ ***مردم، دولتها و هراس***، ترجمه پژوهشکده مطالعات راهبردی، تهران: پژوهشکده مطالعات راهبردی.

تریف، تری و دیگران (۱۳۸۳)؛ **"مطالعات امنیتی نوین"**، مترجمین علیرضا طیب، وحید بزرگی، تهران: پژوهشکده مطالعات راهبردی.

روزنا، جیمز و دیگران (۱۳۹۰)؛ **"انقلاب اطلاعات، امنیت و فناوریهای جدید"**، مترجم علیرضا طیب، تهران: پژوهشکده مطالعات راهبردی.

درویشی سه تلانی، فرهاد (۱۳۷٦)؛ **"تاملی نظری بر امنیت ملی تهدیدات و رهیافتها"**، تهران: معاونت تحقیق و پژوهش سپاه پاسداران انقلاب اسلامی.

روشندل، جلیل (۱۳۷٤)؛ **"امنیت ملی و نظام بین المللی"**، تهران: انتشارات سمت.

عبدالله‌خانی، علی (۱۳۸۲)؛ **"نظریه‌های امنیت: مقدمه‌ای بر طرح‌ریزی دکترین امنیت ملی(۱)"**، جلد اول، تهران: موسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران.

کلارک، یان (۱۳۸٦)؛ **"جهانی شدن و نظریه روابط بین الملل"**، ترجمه فرامرز تقی لو، تهران: دفتر مطالعات سیاسی و بین المللی.

مندل، رابرت (۱۳۷۹)؛ **"چهره متغیر امنیت ملی"**، ترجمه پژوهشکده مطالعات راهبردی، تهران: پژوهشکده مطالعات راهبردی.

میرمحمدی، مهدی و محمدی لرد، عبدالمحمود (۱۳۸۷)؛ **"سیاست و اطلاعات: مطالعه موردی ایالات متحده آمریکا"**، تهران: موسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.

نای، جوزف (۱۳۸۷)؛ **"قدرت در عصر اطلاعات (از واقعگرایی تا جهانی شدن)"**، ترجمه سعید میرترابی، تهران: پژوهشکده مطالعات راهبردی.

یزدان‌فام، محمود (۱۳۸٦)؛ "دگرگونی در نظریه‌ها و مفهوم امنیت بین‌المللی"، **فصلنامه مطالعات راهبردی، شماره ۳۸**،صص ۷۲۵-۷۵۰.

Army, U. (2005); " Cyber Operations and Cyber Terrorism" In U. Army**, *U.S. Army Trainin*.**

Buzan, Barry (1991); "New Pattern of Global Security in the first-twenty Century", ***International Affairs***, 67.3.

CACI International Inc. and U.S Naval Institute (July 2010); "Cyber Threats to National Security, Symposium One: Countering Challenges to the Global Supply Chain", www.caci.com,20/05/2011

Lewis, James A. (2011); "Cyber Security Two Years Later", ***Center for Strategic & International Studies (CSIS)***, available at:

http://www .csis.org/publication/cybersecurity-two-years-later, (accessed by June 13, 2011).

Charney, Scott (2009); "Rethinking the Cyber Threat A Framework and Path Forward", ***Microsoft Corp. • One Microsoft Way • Redmond, WA 98052-6399 • USA.***

Chertoff, Michael (2008), "The cyber security Challenge", ***Regulation & Governance.***

Congressional Research Service(CRS) (2008); "Botnets, Cybercrime and Cyber terrorism: Vulnerabilities and Policy Issues for Congress", available at: www.crs.org, (accessed by July 23, 2011).

Cornis, Paul & Livingstone, David & Clemente، Dave & Yorke, Claire (November 2010); "On Cyber Warfare", ***A Chatham House Report***, www.chathamhouse.org.uk

"Cyber Security: accept vulnerability World Foresight Forum is an initiative of Doctrine Command", Handbook No. 1.02, www.worldforesightforum.org**;** (accessed by September 5, 2011).

Dunn Cavetly M. & Brunner E. (2007); "Information Power and Security: An Outline of Debates and Implication" in Dunn Cavetly M. & Mauer V. & Krishna-Hensel, (eds); ***Power and Security in the Information Age: Investing the Role of the State in Cyberspace***, Aldershot: Ashgate pp: 1-18.

Dunn Cavetly, Myriam & Mauer, Victor (2010); The ***Routledge Handbook of Security Studies***, Routledge Handbooks.

Haller, John & Merrell, Samuel A. & Butkovic, Matthew J. & Willke, Bradford J. (2010); ***Best Practices for National Cyber Security: Building a National Computer Security Incident Management Capability***, Software Engineering Institute.

Hare, Forrest (2010); "The Cyber Threat to National Security: Why Can't We Agree?" ***CCD COE Publications***, Tallinn, Estonia.

Islam Qasem, Teun van Dongen, Marjolein de Ridder (April 2011); "Dealing with Cyber Security: accept vulnerability", **World Foresight Forum is an initiative of** www.worldforesightforum.org

Krause, Keith and Williams, Michael c. (1996); "Broadening the Agenda of Security Studies: Politics and Methods", ***Mershon International Studies Review***.

Lord, Kristin M. & Sharp, Travis (2011); "America's Cyber future Security and Prosperity in the Information Age", ***Center for a New American Security***, Volume I.

Markoff, Jaud & Shanker, T. (2009); "Halted'03 Plan Illustrates U.S Fear of Cyberwar Risk", ***The New York Times***.

Nagre, Dhanashree& Warade, Priyanka (2008); "Cyber Terrorism Vulnerabilities and Policy Issues "Facts Behind The Myth**",** http://www.andrew.cmu.edu/user/dnagre/

Nye, Joseph s. (2010); "Cyber Power", ***Belfer Center for Science and International Affairs***.

Peritz, AkiJ & Sechrist, Michael (2010); "Protecting Cyberspace and the U.S. National Interest", ***Belfer Center for Science and International Affairs***.

Rodriguez, Carlos A. (2006); "Cyber terrorism**", *Inter-American Defense College as a prerequisite for the Diploma approved***

Starr, Stuart H. (2009); "Towards an Evolving Theory of Cyber power", National Defense University, ***Center for Technology and National Security Policy***.

Tabasco, Lior (May 2011); "Basic Concepts in Cyber Warfare", **Military and Strategic Affairs,** v. 3, n. 1

Theohary, Catherine A. & Rollins, Johan (2009); "Cyber Security: Current Legislation, Executive Branch Initiative, and Options for Congress", ***Congressional Research Service***.

Tiirmaa-Klaar, Heli (2011); "Cyber Security Threats and Responses: At Global, Nations State", available at: http://www.Ceri-Scienes-po.org.

Tuchman, Jessica (1989); "Redefining Security", ***Foreign Affairs,*** Vol. 68, No. 2.

Vatis, Michael (2002); ***Cyber Attacks: Protecting American's Security against Digital Threats***, John F. Kennedy School of Government, Harvard University.

Wolfers, Arnold (1962); ***Discord and Collaboration***, Baltimore: Johns Hopkins University Press.

http://www.bbc.co.uk/go/wsy/pub/email/ft/-/persian