بررسی جرایم سایبری علیه امنیت ملی، جرایم سازمان یافته و جرایم مخل کننده ارائه خدمات عمومی به مردم

هادی شیری
دانش آموخته حقوق جزا و جرم شناسی دانشگاه آزاد اسلامی واحد ارومیه

چکیده
فضای سایبر هویت و مکان بازیگران خود را پنهان می‌کند و امکان استفاده آسان از اسامی جعلی و پروکسی‌هایی را فراهم می‌کند که نفوذ به آنها و فاش کردنشان کار دشواری است؛ همچنین فضای سایبری سرعت، حجم و محدوده ارتباطات را نه تنها در کشورهای قدرتمند و شرکتها، بلکه برای شهروندان عادی هم به میزان قابل توجهی افزایش داده است؛ فضای سایبری گسترده و بی حد ومرز است، و از نظر قانونی مبهم و از نظر شفاهی موجز و مختصر و در کل، پیچیده و دست نیافتنی است. تحقیق حاضر در پی پاسخ گویی به این پرسش است که جرایم سایبری چگونه بر امنیت ملی تأثیر می‌گذارند و این اثرگذاری در چه ابعادی خود را نمایان می‌سازد. در پاسخ می‌توان گفت این جرایم 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 سازمان یافته و افراد به معادلات قدرت جهانی شده است. بنابراین، این پدیده امنیت ملی را از ابعاد مفهوم امنیت، دولت محوری در امنیت، بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه، تحت تأثیر قرار داده است.

واژگان کلیدی: تهدید ملی، فضای سایبری، جرایم سایبری، امنیت ملی

بیان مسئله

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 2 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، ناشناس بودن، مشخص نبودن قلمرو جغرافیایی تهدیدکننده، تأثیرگذاری شگرف و عدم شفافیت عمومی در فضای سایبری، موجب شده بازیگران قوی و ضعیف اعم از دولت‌ها، گروه‌های سازمان یافته 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- ملت هایی تشکیل می دهند 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.

توسعه پدیده جهانی فنآوری اطلاعات و ارتباطات، تحولی شگرف در ابعاد مختلف حیات اقتصادی، اجتماعی، فرهنگی، امنیتی و سیاسی ایجاد نموده است. انقلاب الکترونیک تبدیل به مهم ترین پدیده تعیین کننده معاصر شده است. روزانه ده‌ها هزار رایانه ورود خود را به دنیای جدید اعلام می‌کنند. این گستره بیکران از یک سو فرصت‌های بی نظیری را فراهم ساخته و از سوی دیگر تهدیدهای جدی را متوجه بخش اعظم ساختارهای اجتماعی ساخته است.

این ویژگی دوگانه را در بسیاری از نوآوری‌ها و ابداعات بشری از جمله انقلاب صنعتی می‌توان مشاهده کرد. اما به نظر می‌رسد ابرساختار فناوری اطلاعات، دنیای جدیدی را خلق کرده است. دنیایی مملو از نوآوری‌های و پیچدگی‌ها که قاعده و نرم پذیرفته شده‌ای ندارد. این جهان متفاوت از جهان واقعی است. مالک خصوصی و دولتی ندارد. اینترنت تابع آیین نامه‌ای جهانی نمی‌باشد، هیچ قانونگذار عمومی وجود ندارد، اگرچه تلاش‌هایی به منظور توسعه قانون گذاری در شماری از مراجع چندجانبه صورت می‌پذیرد. با وجود این، امروز اینترنت اغلب به عنوان محیطی بی قانون، نامحدود، نامنظم، کنترل نشده و قابل دسترسی، دست کم به لحاظ تئوری برای همه توصیف شده است. عدم وجود ضوابط دقیق در دنیای مجازی باعث شده است که از آن به عنوان غرب وحشی جدید تعبیر شود. فناوری اطلاعات و ارتباطات نه تنها صنعت، اقتصاد، تجارت و دیگر عرصه‌ها را تحت تأثیر قرار داده است، بلکه حقوق هم از این تحولات بی بهره نبوده است. به فراخور این تغییرات بنیادین، طبعاً حقوقدانان نیز همانند متخصصین دیگر رشته‌ها باید برای هماهنگی با این فناوری و عقب نماندن از آن، به ارائه ضوابط، اصول و قواعد حقوقی جهت پیشگیری یا حل و فصل اختلافات ناشی از این تغییرات اقدام نمایند. این فضای جدید به گونه‌ای حقوق جزای سنتی را دستخوش تحولات بنیادین کرده است که تعریف از جرایم در محیط‌های مجازی انطباق چندانی با تعاریف کلاسیک نداشته و در بسیاری از موارد متفاوت است.

امنیت ملی مهم‌ترین و اصلی‌ترین وظیفه دولت ملی و مهم ترین موضوعی است که تاکنون مورد توجه دانشوران قرار گرفته است. از نظر همه دولتها، امنیت ملی واقعیتی کلیدی و شاید نخستین علت وجودی و یا نخستین هدف غایی آنها باشد.

تعریف جرائم سایبری

با پیدایش اینترنت و آمیختگی آن با ارتباطات اعم از تلفن و پست و نیز برقراری پیوند روزافزون رایانه با دیگر پدیده‌های مجازی مانند ماهواره، امواج و حتی رادیو و تلویزیون، باعث گردید تا واژه فضای سایبر که روزگاری نه چندان دور در داستانهای تخیلی به کار می‌رفت، برای نامگذاری همه پدیده‌هایی که به نحوی به رایانه وابسته‌اند یا با آن ارتباط دارند، به کار گرفته شد. جرم سایبری نیز به رفتارهایی که ضد این فضا یا بستر بی مرز و بی کران یا توسط آن ارتباط می‌یابد، اطلاق گردید. در واقع از عمر رواج اصطلاحی جرم سایبری کمتر از دو دهه می‌گذرد و پیش از آن نمی‌توان چنین واژه‌ای را در هیچ لغتنامه یا دایره المعارفی جست اما امروزه در همه لغتنامه‌های روزآمد شده اعم از اینترنتی و معمولی می‌توان چنین واژه‌ای را در هیچ لغتنامه یا دایره المعارفی جست اما امروزه در همه لغتنامه‌های روزآمد شده اعم از اینترنتی و معمولی می‌توان چنین واژه‌ای به راحتی پیدا کرد.

جرم سایبری آنقدر واژه گسترده‌ای است که تا سالها می‌تواند مفهوم و مصادیقی را که در زیر خود دارد، معرفی نماید اما دیده شده که نسبت به تعریف جرم سایبری نیز دیدگاه محدود نگر وجود داشته است؛ مثلاً در تعریفش گفته‌اند: بزه‌هایی که از طریق ارتباط اینترنتی ارتکاب می‌یابند مانند تقلب در کارتهای اعتباری یا هرزه نگاری کودکان اعم از اینکه اینترنت هدف جرم باشد یا وسیله آن، در حالی که جرم سایبری به جرم قابل ارتکاب در محیط مجازی اینترنت و مخابرات گفته می‌شود و از جرم اینترنتی عام‌تر است و علاوه بر اینکه شامل جرائم مخابراتی می‌شود می‌تواند به جرائم ضد نرم افزارهای یک رایانه که به صورت مجازی در سیستم رایانه‌ای قرار دارد نیز تسری داده شود و به همین دلیل در مقررات کشورها و اسناد بین المللی به ویژه کنوانسیون جرائم قابل ارتکاب در محیط سایبر بوداپست مصوب سپتامبر 2001 از عنوان «جرم سایبری» استفاده شده و به دلیل رواج روز افزون کشورهایی مانند استرالیا نیز این عنوان را در قوانین کیفری خود وارد کرده‌اند.

بیشتر موارد جرم سایبری و جرم رایانه‌ای یکسان دانسته شده و به کارگیری هر یک از این اصطلاحات برای توضیح بزه‌های ارتکاب یافته در فضای مجازی رایانه و اینترنت رایج است. در دایره المعارف اینترنتی ویکی پدیا که بزرگترین و پر کاربردترین وبگاه در زمینه شناسایی اصطلاحات یا اسامی یا پیوند آنها به وبگاههای دیگر است، جرم سایبری همانند جرم رایانه‌ای تعریف شده است؛ یعنی رفتار جنایی که رایانه‌ها و شبکه‌ها به عنوان ابزار یا هدف یا مکان آن مطرح می‌شوند.

تعریف فضای سایبری

خلاقیت انسان، فضای سایبر را به ما هدیه کرده است، فضایی که منافع و قابلیت‌های بسیاری دارد. اما هدایای بزرگ بهای گزافی نیز دارند. پیش از اینکه فضای سایبر به عنوان یک فناوری ظاهر شود، تعدادی از فلاسفه در ارتباط با امکان وجود "حقیقت مجازی"[1] اظهار نظر کرده بودند. برای نمونه، افلاطون در کتاب جمهوریت خود به تمثیل غار می‌پردازد و می‌گوید: «آنچه حقیقت واقعی است در بیرون غار است و ما سایه‌های آن بر دیوار غار هستیم. او می‌گوید، ما حقیقت مجازی هستیم و این یک فریب است که فکر می‌کنیم حقیقت واقعی هستیم.» در هر حال فضای سایبر عبارتی است که در دنیای اینترنتی، رسانه و ارتباطات بسیار شنیده می‌شود به نظر می‌رسد به کار گیری این اصطلاح در این زمینه و برای ارجاع به آن رنگ و بویی صرفا فنی و مکانیکی داده باشد. ملاحظه دقیق تر این اصطلاح نشان می‌دهد که این واقعیت وجوه و جنبه‌های متنوعی از جمله خصلت‌های روان شناختی.

ویژگیهای جرایم رایانه‌ای

جرائم کامپیوتری به عبارتی اقدامات زیانباری است که از سوی یک کامپیوتر یا شبکه و یا علیه آنها انجام می‌شود. این جرائم ویژگیهای متمایزی از سایر جرائم کلاسیک دارند چرا که ماهیت اینگونه جرائم به دلیل تکنولوژی پیچیده و بالا، خصوصیات

[1] Virtual Reality

منحصر به فردی داشته که می‌توان به: شیوه ارتکاب آسان، خسارات و ضررهای هنگفت با حداقل منابع و هزینه، عدم حضور فیزیکی در محل ارتکاب جرم، عدم شناسایی جرائم در بعضی موارد (غیر قانونی بودن آن ظاهراً مشخص نمی‌باشد)،خصوصیت فراملی بودن، وسعت و دامنه وسیع جرم را نام برد که در یک دسته بندی کلی، جمع بندی اینگونه جرائم را می‌توان از لحاظ خصوصیات مرتکبین، عدم تخمین میزان دقیق جرائم ارتکابی، حجم و وسعت ضرر و خسارت وارده، طبع بین المللی و نحوه تعقیب و رسیدگی بررسی نمود.

1- ویژگیهای مرتکبین جرایم سایبری

مرتکبین جرائم کامپیوتری به لحاظ سنی شامل طیف گسترده‌ای از افراد می‌باشند. نوجوانان، دانشجویان، کارمندان ناراضی، خلافکاران و تروریست‌های بین المللی و غیره که منحنی سنی مجرمین کامپیوتری سنی بین 10 تا 60 سال را نشان می‌دهد و دامنه مهارت آنان از تازه کار تا حرفه‌ای گسترده است. بسته به نوع جرم، گاه آشنایی کلی با کامپیوتر اکتفا می‌کند و گاه نیازمند تخصص در سطح بالا می‌باشد. معمولاً دو دسته از مرتکبین جرائم رایانه‌ای از هم قابل تمایز هستند: مرتکبین اتفاقی و مجرمین واقعی. دسته اول معمولاً شامل جوانانی می‌باشد که به انگیزه بازی و تفنن مرتکب جرائم رایانه‌ای می‌شوند (سازمان ملل، 1376، ص 42).

ارتکاب این جرائم از آنجایی که منعکس کننده معایب سیستم‌ها و نحوه نفوذپذیری به شبکه و سیستمهای کامپیوتری است لذا اتخاذ تدابیر پیشگیرانه امنیتی مفید است. جرائم خطرناک و جدی که موجب خسارت مالی هنگفت می‌گردد از سوی مرتکبینی که دارای تخصص فنی یا تحصیلات دانشگاهی هستند وقوع می‌یابند که این دسته از مجرمین را باید جدی گرفت.

در یک سری از جرائم کامپیوتری انگیزه اصلی کسب منفعت مالی است ولیکن انگیزه‌های دیگری چون انتقام جویی شغلی، سرگرمی، اثبات برتری قدرت، خود نمائی، علل روانی، چالش و ... وجود دارد. لذا یکی از وجوه تمایز مرتکبین جرائم کامپیوتری از یکدیگر نوع انگیزه آنان می‌باشد. بر این اساس سه گروه از مجرمین از یکدیگر شناخته شده‌اند، مزاحمان کامپیوتری، خلافکارها و خرابکاران. انگیزه گروه اول صرفاً دستیابی به سیستم‌های کامپیوتری و اطلاعات موجود در آن می‌باشد و اکثراً نوجوانانی هستند که برای تفریح و سرگرمی و ارضای حس برتری جوئی دست به این اقدامات می‌زنند. انگیزه دسته دوم یعنی خلافکارها کسب منفعت مالی است و عمدتاً در دو مقوله جاسوسی و کلاهبرداری فعالیت دارند که روز به روز بر تعداد این افراد در جهان افزوده می‌شود. بالاخره انگیزه دسته سوم تنها صدمه زدن و ایراد خسارت به دیگران است، که نه به قصد کسب منفعت و نه سرگرمی و تفریح می‌باشد بلکه افرادی هستند که دارای اختلالات روانی بوده و یا قصد انتقام جوئی دارند. آنچه در مورد مرتکبین جرائم رایانه‌ای حائز اهمیت می‌باشد آن است که این دسته از مجرمین در اذهان عمومی جایگاه چندان نامطلوبی ندارند و به نظر می‌رسد که نسبت به مجرمان دیگر در اجتماع از مقبولیت بیشتری برخوردارند چه بسا به عنوان یک قهرمان و یا بزرگترین بزهکاری کامپیوتری سال در تمام دنیا مشهور شده و نامشان زبانزد عام می‌شود (خرم آبادی، 1390، ص 98). جالب اینکه بعضی از مجرمان رایانه‌ای اقدام به تشکیل انجمن یا گروه نموده‌اند که بعنوان نمونه به انجمن خدشه زنندگان می‌توان اشاره کرد.

2- حجم و وسعت ضرر و خسارات وارده

بوسیلهٔ تکنولوژی کامپیوتر، مرتکبین با کمترین سرمایه و هزینه (یک کامپیوتر شخصی) می‌توانند با ورود به شبکه اطلاعاتی و نفوذ در آن خسارت هنگفتی وارد نمایند، سهولت ارتکاب با حجم زیاد موضوعات مطروحه، سرعت عملکرد کامپیوتر، عدم نیاز به تخصص خاص یا بالا، عدم نیاز حضور فیزیکی مرتکب در محل و ... همگی موجب گردیده تا حجم صدمات و خسارات وارده افزون گشته و گاه به چندین هزار برابر جرائم معمولی برسد (جلالی فراهانی، ۱۳۸۶، ص 99).

وسعت خسارات وارده ناشی از یک نفوذ غیرقانونی یا گسترش ویروس در اینترنت می‌تواند در کسر ثانیه صدها هزار استفاده کننده در سراسر جهان را متحمل خسارت نماید.

عواقب جرائم کامپیوتری علاوه بر خسارات اقتصادی سنگین می‌تواند تهدیدی جدی برای امنیت بشر باشد. وابستگی امور حساس کشورها در زمینه‌های پزشکی، مخابراتی، هواپیمائی، امور امنیتی و نظامی و ... به عملکرد کامپیوترها باعث می‌شود تا کوچکترین اختلال و خدشه در کار این سیستم‌ها، عواقب وخیم و جبران ناپذیری را به دنبال داشته باشد.

مطالعات آماری بیانگر جایگاه مهم جرائم کامپیوتری در میان تمامی خاطرات وابسته به کامپیوتر می‌باشد. به موجب ارقام منتشره از سوی باشگاه فرانسوی امنیت کامپیوتر در سال 1991، 10/4 میلیارد فرانک خسارت کامپیوتری در شرکتها و مؤسسات فرانسوی دیده می‌شود که بیش از نیمی از آن ناشی از اعمال مجرمانه می‌باشد. انجمن بانکداری انگلیس طی تخمینی میزان تقلب و دزدی کامپیوتری را معادل سالانه 8 میلیارد دلار یا روزانه 22/4 میلیون دلار اعلام نموده است (خبرنامه انفورماتیک، 1374، ص 42). به عنوان یک نمونه کوچک از جرائم کامپیوتری که منجر به خسارات فراوانی گردیده می‌توان به ویروس ملیسا در سال 1999 میلادی اشاره نمود. این ویروس با ایجاد اختلال در سیستمهای پست الکترونیکی (E-Mail) در سراسر جهان موجب بروز میلیونها دلار خسارت گردیده. خالق این ویروس ادعا نمود که ویروس را روی کامپیوتر شخصی خود تولید کرده بود و برای ورود به سایت AOL[2] فقط از یک نام و رمز عبور به سرقت رفته استفاده کرده است (خبرنامه انفورماتیک، 1382، ص 7).

3- خصوصیت فراملی و بین المللی جرایم سایبری

به دلیل فراملی بودن ماهیت جرائم کامپیوتری اینگونه جرائم را من بعد بایستی جرائم بدون مرز نامید. جرائم کامپیوتری به دلیل ماهیت و تکنولوژی خاص، اختصاص به محیط فیزیکی معین و محدودی ندارد و به راحتی در مقیاس بین المللی قابل تحقق می‌باشد. مسافت، زمان و مکان مانعی برای آن به حساب نمی‌آید. حضور فیزیکی شخص در محل وقوع حادثه معنایی ندارد. با کمک کامپیوتر و از طریق اینترنت سرقت از یک بانک یا دستیابی به اطلاعات محرمانه نظامی در ظرف چند ثانیه امری بعید و دور از دسترس نمی‌باشد.

از طریق دسترسی به سیستم کامپیوتری در کشور A، پردازش در کشور B و نتایج حاصله در کشور C یا کل کشورهای جهان این امکان را به کاربران غیر مجاز اینترنت می‌دهد که به راحتی به بانکهای اطلاعاتی مستقر در قاره‌ای دیگر دسترسی یابند. نمونه بارز در زمینه فراملی بودن جرائم کامپیوتری، ویروسها و کرمها هستند که می‌توانند با سرعتی بسیار زیاد گسترش یافته و برنامه‌های کل شبکه بین المللی مرتبط را مبتلا ساخته و اثرات مخرب خود را بجا بگذارد.

با توجه به افزایش روز افزون جرائم کامپیوتری و بدون مرز شدن جرائم جدیدتر (جرائم سایبر)، عدم حضور فیزیکی مجرم در محل، سرعت بالا و زمان اندک ارتکاب جرم، لزوم هر چه سریعتر تعاون بین المللی را برای دستیابی به یک سیاست کیفری هماهنگ را ایجاب می‌کند (ترکی، ۱۳۸۹، ص 143).

4- نحوه تعقیب و رسیدگی به جرائم کامپیوتری

همانگونه که در مباحث قبلی اشاره شد نوین بودن جرائم کامپیوتری و شیوه ارتکاب اینگونه جرائم، نحوه رسیدگی و تعقیب را از جهت مسائل آیین دادرسی با چالش‌هایی روبرو نموده است به طوریکه تدابیر کلاسیک حقوقی به هیچ عنوان پاسخگو نبوده و با مشکلات عدیده‌ای در این زمینه روبرو می‌باشد. نوع تحقیق، بازرسی محل و وقوع جرم، توقیف اسباب و آلت جرم با جرائم کلاسیک متفاوت بوده و بدون تخصص و مهارت کافی مقامات قضائی، کشف جرم میسر نمی‌باشد. مأموری که به تحقیقات

[2] – سایت American Online یک آدرس متعلق به یک مرجع دولتی در آمریکا می‌باشد.

جنایی مشغول است و تخصصی در این زمینه ندارد نمی‌داند که در محیط کامپیوتری به دنبال چه بگردد. از طرف دیگر در جرائم جدید کامپیوتری، به خصوص جرائم مرتبط با اینترنت که اغلب جرائم در غیر از محل وقوع جرم و غیر حضوری ارتکاب یافته است تحقیقات و کشف بسیار دشوار و غیر قابل دسترس می‌باشد. در یک سری از جرائم بدون اثرگذاری در محیط کامپیوتری مسائل خاص و پیچیده‌ای مطرح می‌شود. حق بازرسی و توقیف یک شبکه یا تأسیسات کامپیوتری خاص تا چه حدی شامل حق بازرسی بانکهای اطلاعاتی و شبکه‌های مادر می‌شود که فقط در دسترس کاربر و یا یک مؤسسه قرار دارد. در زمینه بازرسی و توقیف «پایگاه داده‌ها» از طریق سیستمهای مخابراتی بین المللی نیز مسائل خاصی در رابطه با حقوق بین المللی عمومی مطرح می‌شود، چرا که نفوذ مستقیم در بانکهای داده‌های خارجی به وسیله مقامات تعقیب معمولاً تجاوز به حاکمیت کشوری و یا تجاوز به شبکه و یا بانک اطلاعاتی مادر می‌باشد که اطلاعات در آن ذخیره شده است، در واقع جایگزین شدن موضوعات غیر ملموس و مجازی به عوض ادله مثبت ملموس و عینی در عرصه تکنولوژی اطلاعات، مسائل حقوقی نوینی را مطرح ساخته و از خصوصیات بارز جرائم کامپیوتری و اینترنتی می‌باشد (باستانی، 1390، ص 37).

ابعاد امنیت

موضوع امنیت از لحاظ سطوح به امنیت فردی، امنیت گروهی، امنیت ملی، و بین المللی و ابعاد متنوعی همچون سیاسی، اجتماعی، اقتصادی، حقوقی و غیره تقسیم می‌گردد که به تشریح آن می‌پردازیم.

1- امنیت فردی

امنیت فردی عبارت است از حالتی که فرد - جسماً و روحاً - در آن فارغ از ترس و آسیب به جان و یا مال و یا آبروی خود یا از دست دادن آنها زندگی کند. علاوه بر جنبه های مادی فردی و اجتماعی، و بنا به آیه شریف الا بذکرالله تطمئن القلوب (رعد: 28)، امنیت فردی را باید در ایمان واقعی، آرامش روحی، اطمینان و طمانینه نفس و یاد خداوند متعال جستجو کرد.

2- امنیت اجتماعی

امنیت اجتماعی شخص به معنی امنیت جان، مال، آبرو و موقعیت اجتماعی شخص از جانب عوامل اجتماعی می باشد. در اندیشه اسلامی، امنیت اجتماعی را باید در سایه تقوا، عدالت، رعایت حرمت، حقوق انسان ها و دفاع از مظلومان و محرومان و برخورد با مفسدان، مجرمان، بزهکاران و رفع فقر، تامین رفاه و معیشت مردم و حفظ آزادی های مشروع و حاکمیت عادلانه، قانونی و معیارهای انسانی جست و جو کرد.

3- امنیت ملی

به تعبیر رابرت ماندل: «معنی کردن مفهوم امنیت ملی در جهان امروز کار پیچیده‌ای است.» (رابرت مندل، 1389، ص 43). این واژه در قرن بیستم و به ویژه بعد از جنگ جهانی دوم متداول شده است. در ساده ترین تعاریف، امنیت ملی این گونه تعریف می شود: توانایی یک ملت برای حفاظت از ارزش‌های حیاتی داخلی در مقابل تهدیدات خارجی و این که کشورها چگونه سیاست‌ها و تصمیمات لازم را برای حمایت از ارزش‌های داخلی در مقابل تهدیدات خارجی، اتخاذ می کنند. محمد ایوب معتقد است که مفهوم سنتی امنیت ملی کاربرد خود را از دست داده است. وی بر عوامل داخلی امنیت عنایت خاصی داشته و بر تفاوت معضلات و نگرش امنیتی کشورهای شمال و جنوب تأکید می‌کند و معتقد است که تفسیر شمالی‌ها از امنیت به نحوی است که ناامنی جنوبی‌ها از آن متبادر می‌شود و برعکس. در واقع امنیت جنوب، ناامنی شمال و امنیت شمال، ناامنی جنوب تلقی می‌شود (United statd linne,1995, p213).

در دیدگاه اسلامی، می‌بایست امنیت ملی را در سایه اقتدار، استقلال، دانایی و توانایی، ارتباطات قوی و سازنده امت اسلامی در کلیه ابعاد و زوایا و ایستادگی در برابر یورش و توطئه و تهدید دشمن و بیگانگان و بیگانه پرستان و نفوذ ایادی شیطانی آنان پیگیری کرد.

امروزه هیچ کشوری در تامین امنیت ملی، تنها به مقابله با تهدیدات نظامی بسنده نمی‌کند، بلکه انواع تهدیدات سیاسی، اقتصادی، فرهنگی، روانی، رسانه ایی و... را در نظر می‌گیرد.

4- امنیت سیاسی

امنیت سیاسی به معنای تامین آرامش و طمانینه لازم توسط حاکمیت یک کشور برای شهروندان قلمرو خویش از راه مقابله با تهدیدات مختلف خارجی و همچنین تضمین حقوق سیاسی آنان در مشارکت جهت تعیین سرنوشت اجتماعی و سیاسی آن ها می باشد. نظام سیاسی در راستای امکان بخشی و تسهیل مشارکت و دخالت مردم در تعیین سرنوشت خود و جامعه می بایستی امنیت و حضور آزادانه و برابر ایشان را فراهم آورد و هیچکس را به داشتن باور سیاسی خاصی وادار یا بازداشت نکند.

از مهم ترین مسائلی که مستقیماً بر امنیت سیاسی جامعه تاثیرگذار است، نحوه توزیع قدرت و شکل رژیم سیاسی می باشد. نظام سیاسی بسته و مشارکت گریز که تداول قدرت و چرخش نخبگان را بر نمی تابند، فاقد امنیت سیاسی لازم هستند.

5- امنیت فرهنگی

بسیاری معتقدند بحث از امنیت فرهنگی در ذیل موضوع امنیت ملی قرار دارد و یکی از مؤلفه های اصلی آن را تشکیل می دهد. امنیت فرهنگی یکی از مهم ترین ابعاد امنیت ملی و به مفهوم آن است که از یک سو فرهنگ جامعه از مولفه های عقلایی، واقع بینانه، سازنده، عادلانه، پویا و منطبق با معیارهای مطلوب علمی شکل گرفته باشد و از سوی دیگر فرهنگ و تولیدات فرهنگی جامعه نیز ضمن درامان بودن از خطر تهدیدها، از روند رشد فزاینده ای برخوردار باشند.

از منظر اسلامی، امنیت فرهنگی به معنای از بین بردن کلیه تنوع ها و تفاوت های موجود در بین افراد اجتماع در حوزه فرهنگی و یکسان سازی آن ها نیست. البته لازم است در هر نظام سیاسی مواظبت شود تا تفاوت‌ها به شکاف‌های عمیق تبدیل نشوند و این شکاف‌ها دائماً می بایستی از حیث عمق و سطح توسط دولت‌ها کنترل شود تا جامعه دچار ازهم پاشیدگی نگردد.

از سوی دیگر مقابله با تهاجم فرهنگی در تضمین امنیت فرهنگی بسیار مهم است که دارای سه صورت «تحمیل فرهنگی»، «تخریب فرهنگی» و «تهدید فرهنگی» می باشد.

6- امنیت اقتصادی

از سال 1945، ایده امنیت اقتصادی جایگاه والایی در دستور کار نظام های سیاسی یافته است. و همه آنها تلاش نموده اند که برای مردم خود امنیت اقتصادی ایجاد کنند.

از نظر رابرت ماندل امنیت اقتصادی عبارت است از میزان حفظ و ارتقای شیوه زندگی مردم یک جامعه از طریق تامین کالاها و خدمات؛ هم از مجرای عملکرد داخلی و هم حضور در بازارهای بین المللی.

در همین راستا قانون اساسی جمهوری اسلامی ایران، دولت را به پی ریزی اقتصادی صحیح و عادلانه بر طبق ضوابط اسلامی جهت ایجاد رفاه و رفع فقر و برطرف ساختن هر نوع محرومیت در زمینه‌های تغذیه، مسکن، کار، بهداشت، تعمیم بیمه، تامین خودکفایی در علوم و فنون و صنعت و کشاورزی موظف کرده است.

7- امنیت حقوقی یا قضایی

امنیت حقوقی حکایت از وجود امنیت در محیط حقوق دارد. گاهی ممکن است مقصود از امنیت حقوقی، بخشی از مجموعه خاص حقوقی باشد که به امنیت ارتباط دارد. از چنین منظری باید امنیت حقوقی را به مفهوم حقوق امنیت یا حقوق امنیتی به کاربرد. شاید بتوان امنیت حقوقی و قضایی در معنای اول را بیشتر به قواعد ماهوی مورد مشاهده قرار داد. بنابراین امکان دادخواهی، وجود دادگاه با شرایط رسیدگی منصفانه، امکان داشتن وکیل، فقدان موانع برای دفاع، اعمال اصل برائت، وجود صلاحیت نسبی و تخصصی در دادگاه ها، رعایت اصل قانونی بودن جرم و مجازات و صلاحیت ضابطان و مجریان قضایی را باید از شاخص های امنیت حقوقی و به ویژه امنیت قضایی دانست.

در مفهوم دوم (حقوق امنیتی)، مقررات مربوط به نظم عمومی، اخلاق حسنه مانند قوانین جزایی، مقررات مربوط به نظم سیاسی و بین المللی مانند قانون اساسی و برخی کنوانسیون ها و موافقت نامه ها و مقررات خاص امنیتی مورد توجه است.

8- امنیت زیست محیط

از جمله ابعاد نوین امنیت، بعد زیست و شرایط اقلیمی هر کشور می باشد. محیط زیست از آن جنبه که می تواند موجبات تقویت بنیه‌های اقتصادی و سلامت جسمی و روانی کشور را فراهم سازد، عاملی مطلوب و تقویت کننده در جهت اهداف امنیت ملی به شمار می‌آید.

امنیت محیط زیست، به مفهوم وجود شرایطی است که امنیت نسبی مطلوبی را در برابر خطرها و تهدیدهای ناشی از فعل و انفعال‌های گهواره‌ی زمین، پدیده‌های جوی، آلودگی خاک، آب و هوا، آلودگی صوتی و اشاعه‌ی بیماری‌ها برای ادامه‌ی حیات سالم،ثمربخش و با نشاط انسان، جانوران، گیاهان و به طور کلی تمامی موجودات زنده و عدم تخریب جامدات، فراهم می‌سازد (همان منبع).

نظام‌های سیاسی با مطالعه دقیق ویژگی‌های زیست محیطی کشورهایشان و برنامه ریزی علمی در این راستا و رعایت استانداردهای حفظ محیط زیست، موجبات تقویت امنیت ملی و منطقه ای را فراهم خواهند ساخت (اخوان کاظمی، 1385، ص 23).

منافع ملی و رابطه آن با امنیت ملی

منافع ملی، اهداف عام و همیشگی است که ملت در راه تحقق آنها فعالیت می‌کند. هر جامعه باید به مثابه یک کل و دارای مسوولیت و هنجارهای مشترک برای تمامی شهروندانش در نظر گرفته شود. منافع جامعه همان خیر مشترکی است که از طریق ارزیابی بهره مندی اجتماع در رهگذر برنامه، تحقق بهترین زندگی مشترک ممکن برای افراد تعیین می شود. منافع ملی، پدیده ها و اموری را در برمی گیرد که تحقق آنها معطوف به بیشینه سازی امنیت همه جانبه ملت و دولت می باشد. در واقع هرچه بیشتر بتوان منافع ملی یک کشور را وسیع تر ساخت و مصداق آن را در نظام بین الملل گسترش بخشید، به همان میزان به صورت بالقوه می توان نسبت به بهره مندی از محیط و امکانات موجود امیدوار بود. در مباحث جدید امنیت ملی، علاوه بر وجه سلبی و نبود تهدید، برای تعریف امنیت، داشتن وجه ایجابی آن یعنی وجود اطمینان خاطر ضروری است. در این جا، «امنیت ملی» مجموع توانمندی های (طبیعی، بهره برداری و راهبردی) یک نظام برای دستیابی به منافع ملی را شامل می‌شود که نبود تهدید صرفا مقدمه آن است. بر این اساس امنیت ملی ظرفی تلقی می گردد که در چارچوب آن می توان بدون دغدغه خاطر جوانب مختلف منفعت ملی را دنبال نمود. خلاصه باید گفت ملاحظات امنیت ملی در راس منافع ملی (منافع حیاتی و اولیه) همه کشورها قرار دارند.

ماهیت تهدیدات سایبری

تهدیدهای سایبری پدیده‌ای جدید است که در دهه‌های اخیر، همزمان با تحول فن آوری 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.

در همایشی که در 2 مارس 2010 از سوی مؤسسه بین المللی 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).

با توجه به نقش مؤثر اینترنت به عنوان منبع عظیم از اطلاعات در دنیای فناوری و ارتباطات امروزی و کارکردهای وسیع آن به عنوان یک شبکه بین المللی که سبب اتصال جهان و کاربران مختلف به یکدیگر شده است و با توجه به اینکه بیش از دو دهه است که اینترنت بازندگی انسان‌ها عجین شده است، می‌توان از اینترنت به عنوان ابزاری که سبب قرار گرفتن دولت‌ها در مقابل چالش‌ها و تهدیدات جدیدامنیتی شده است، نام برد.

تهدیدات سایبری از جمله مسائل غیرقابل انکار می‌باشد که نقش مهمی در حوزه سیاست جنایی کشورها را داراست که می‌تواند سبب ضعف زیرساخت‌های امنیتی کشورها شود. ویژگی‌های خاص اینترنت مانند مخفی بودن و ناشناس بودن افراد، کم هزینه بودن ورود، جهانی بودن و بی حد و مرز بودن از لحاظ موقعیت جغرافیایی، سبب گردیده که افراد به راحتی بدون داشتن کمترین محدودیتی وارد این فضا شوند و تهدیدهایی همچون جرایم سایبری، جاسوسی سایبری، آشفتگی‌های سایبری، حمله‌های سایبری و مانند آنها را به وجود آورند. امروزه چالش تهدیدهای سایبری از اهمیت وپیچیدگی خاصی برخوردار است، که این اهمیت و پیچیدگی به ماهیت جدید بودن تهدیدهای سایبری و ویژگی‌ها و ساختارهای خاص آن بر می‌گردد.

ویژگی‌های تهدیدات سایبری

با توجه به تأثیر گذاری شگرف اینترنت در عصر اطلاعات بر روی زندگی انسان‌ها و بدلیل گستردگی و تنوع تهدیدات سایبری در زمینه‌های مختلف اجتماعی، نظامی، اقتصادی وغیره به شناسایی ویژگی‌های این تهدیدات که عبارتند از چند وجهی و متنوع بودن، سهولت انجام جرم، عدم شناسایی آسان مجرمان، تأثیر گذاری شگرف، خواهیم پرداخت.

با توجه به ارتباط آسان و روز افزون رایانه‌ها به عنوان وسیله ارتباط جمعی امکان اتصال و ارتباط کاربران و مشترکین بسیاری دراقصی نقاط جهان بوجود آمده است و همین امر سبب شده است که هرکسی بتواند به آسانی وارد این فضا شده و بدور از چشم قانون و افراد دیگر مرتکب جرایمی شود. این فضا افراد مختلفی را شامل می‌شود از جمله کاربران متنوع، سازمان‌ها ، شرکت‌ها، به همین دلیل از دیگر ویژگی‌های اینگونه تهدیدات می‌توان به پردامنه بودن و با نفوذ بودن و برخورداری از وجوه و ساختارهای مختلف اشاره داشت. دراینگونه تهدیدات از تمامی فنون، علوم، روش‌ها و ارزشهای موجود استفاده می‌گردد.

همچنین دراین فضا ارتکاب جرم به سهولت امکان پذیر می‌باشد، هر کس با داشتن یک رایانه و آگاهی اندک در زمینهٔ استفاده ازآن می‌تواند به آسانی مرتکب جرم شود البته برای ارتکاب جرایم حرفه‌ای ترنیاز به بالا بردن سطح آگاهی می‌باشد، پس با افزایش میزان آشنایی بر درجات و شدت ارتکاب جرم نیز افزوده خواهد شد. بطور مثال برای سرقت از یک شرکت یا سازمان

بزرگ، شاید مدت‌های زیادی برای برنامه ریزی و طراحی سرقت، آشنایی با اطلاعات مالی، امنیتی و جستجو در سایر جزئیات لازم می‌باشد .

دراین فضا همچنین بدلیل ناشناخته بودن کاربران آن امکان شناسایی، تحقیق و تعقیب جرایم در محیط سایبر نیز بسیار دشوار است.

«به همین دلیل امکان ارتکاب جرم راحت و امکان دستگیری مجرمین نیز کمتر است، مجرمین سایبر به این نکته واقفند که به جای ارتکاب سرقت اموال در جهان واقعی که خطرات آن به مراتب بیشتر است، مرتکب کلاهبرداری رایانه‌ای شوند که ریسک کمتری دارد.» (فضلی، 1391، ص 74)

حملات یا حوادثی که در این فضا رخ می‌دهد سبب تأثیرگذاری بیشتر، و پیامدهای وخیم‌تری را نیز به همراه دارد. زیرا که اینگونه حمله‌ها سبب آسیب پذیری زیر ساخت‌ها و سامانه‌های ارتباطی و در نتیجه بروز اختلال در اطلاعات حساس، شبکه‌ها و غیره می‌شوند.

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:

1- تعدد بازیگران در فضای سایبری

هزینه کم فن آوری رایانه ای، اتصال گسترده به اینترنت و سهولت ایجاد یا به دست آوردن نرم افزارهای مخرب به این معناست که تقریباً هر کسی می‌تواند به این فضا وارد شود. این بازیگران شامل افراد، گروه‌های سازمان یافته جنایی، گروه‌های تروریستی، شرکت‌های خصوصی و دولت– ملت هستند (Charney,2009: 5).

2- 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 پیچیده تر سایبری نیازمند صرف هزینه‌های بالاتری است (Lord and Sharp, 2011: 20).

3- ناشناس ماندن بازیگران و عدم قابلیت ردیابی

اینترنت به عنوان سیستم نامتمرکز طراحی شده و کاربران آن، غالباً شناخته شده 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, 2011, p 21).

4- 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: 2011, p 22).

5- کمرنگ شدن 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 کلیدی شان هستند (Starr, 2009, p 18).

6- 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 دشو ارتر کرده است (Charney, 2009, p 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 فن آوری در حال تکامل برای پشتیبانی از سیستم‌های حیاتی است (Haller et al., 2010, p 4).

7- پایین بودن احتمال تنبیه یا بازخواست اقدا مهای 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 مطمئن تر و دارای خطرات کمتری می‌بینند (Lord and Sharp, 2011).

انواع تهدیدهای سایبری

آژانس مدیریت فوق العاده فدرال[3]، تروریسم سایبری را اینگونه تعریف می‌کند: تهدید و حمله غیرقانونی علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن، زمانی که برای ترساندن یا مجبورکردن حکومت یا مردم آن در پیشبرد اهداف سیاسی یا اجتماعی صورت می‌گیرد (Congressional Research Service, 2008, p 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، برنامه ریزی 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, p 18).

در عرصه فضای سایبری کاربران با نفوذ و عملیات مختلفی به منظور دستیابی به اهداف اجتماعی، ایدئولوژیکی، فرهنگی، نظامی و غیره با استفاده از قدرت سایبری دست می‌یابند.

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.

در این گفتار بطور جداگانه به بررسی هر کدام از این موارد و تأثیرهر کدام بر امنیت ملی خواهیم پرداخت.

1- جنگ سایبری[4]

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 جاه طلبی‌های به مراتب بزرگتر همچون وارد کردن آسیب جدی به دولت یا شهروندان آن همچون تخریب، تضعیف و غیرفعال کردن زیرساخت‌های نظامی و غیرنظامی باشد، چنین رفتاری در واقع چیزی نزدیک به اقدام جنگی در مفهوم سنتی است (Cornish

[3] . Federal Emergency Management Agency
[4] . Cyber War

(et al., 2010, p 12-13). در سال 2007 ، استونی به عنوان کشور کوچک مدرن در مقیاس بزرگ مورد حمله‌های اینترنتی قرار گرفت. فن آوری بالای این کشور زمینه ای مناسب برای حمله‌های اینترنتی با انگیزه‌های سیاسی بود (Tiirma-Klaar, 2011).
همانطور که ریچارد کلارک[5] 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 et al., 2010, p13).

جنگ در فضای سایبری را می‌توان حمله‌های اینترنتی طراحی شده از سوی گروه‌ها، سازمان‌های مختلف، علیه سامانه‌ها وبرنامه‌های رایانه‌ای با اهداف به مراتب بزرگتر مانندستیابی به سود مالی یا آسیب جدی وارد کردن به شهروندان یا دولت بوسیله روشهای مجرمانه مانند کلاهبرداری، جعل، تخریب و اخلال در داده‌ها، سرقت، تضعیف یا غیرفعال کردن زیرساخت‌های نظامی و غیرنظامی انجام می‌شود، تعریف نمود.

«عملیات جنگ اطلاعات تهاجمی، عملیاتی است که یک منبع اطلاعات خاصی را هدف و مورد بهره برداری قرار می‌دهد و هدفش افزایش ارزش آن برای بازیگرمهاجم و کاستن ارزش آن برای بازیگردفاعی است. بنابراین این حالت یک موقعیت برد-باخت را برای هردو بازیکن پش می‌آورد. فرض این است که دفاع با چنین تمهیدی موفق نیست. عملیات یک عمل خصمانه ویا حداقل بدون اجماع محسوب می‌شود منبع اطلاعات، لازم نیست که تحت مدیریت یا مالکیت دفاع باشد، هرچندکه اغلب اینگونه است.» (دنینگ، 1383، ص 32)

درجنگ سایبری هدف حمله کننده برهم ریختن ساختار اداری، خدماتی و در یک جمله می‌توان گفت تعادل کشور مورد حمله از طریق فضای سایبری می‌باشد. این حملات در اشکال گوناگون خود را نمایان می‌سازد. مهاجم می‌تواند یک فرد یا یک گروه یا یک کشور باشد و در مقابل نیز فرد یا گروه یا کشور قرار دارند و به دفاع می‌پردازند، که درفضای سایبری تهاجم بسیار آسان تر از دفاع می‌باشد. در این فضا باید سعی نمود تابتوان جغرافیای فضای مجازی را به نفع خود تغییر نمود.

جنگ سایبری شکل جدیدی از مبارزه در فضای مجازی می‌باشد که توسط گروه‌ها یا دول متخاصم انجام می‌شود ولی تروریسم سایبری اقدامی است که از طرف تروریست‌ها به صورت حمله غیرقانونی علیه رایانه‌ها، شبکه‌ها و اطلاعات انجام می‌گردد.

2- تروریسم سایبری[6]

از لحاظ لغوی واژه «تروریسم» از کلمه «ترور» برگرفته شده است ؛ و در زبان لاتین به معنای «ترس» به معنای وحشت است. ولی واژه تروریسم سایبری از دو اصطلاح تروریسم و سایبربرگرفته شده است. واژه تروریسم دارای گونه‌های متفاوتی می‌باشد مانند تروریسم رسانه‌ای، تروریسم بین المللی، تروریسم فرهنگی، تروریسم سایبری و غیره.

در تروریسم سایبری که برجسته‌ترین انواع آن می‌باشد خشونت به شکلی که در اقسام دیگر تروریسم است، وجود ندارد ولی ارتکاب رفتار مجرمانه می‌تواند آسیب‌های جبران ناپذیری بر پیکره جامعه وارد نماید و به عنوان تهدید جدی برای امنیت ملی به شمار آید.

«تعاریف مربوطه به واژه تروریسم سایبری از حیطه‌های بسیاری محدود تاحیطه‌های بسیارگسترده متغیرهستند. در تفکیک مهم میان دو مفهوم استفاده از اینترنت، به عنوان یک عامل تبعی و تسهیل کننده، در پیشبرد تروریسم و تهاجمات صرف سایبری، گروه بسیاری معتقدند فقط گزینه دوم در مفهوم تروریسم سایبری می‌گنجد؛ برای مثال تحلیل‌گر پیشرو در عرصه تروریسم سایبری، «دوروتی دنینگ»[7] چنین می‌گوید: «تروریسم سایبری همگرائی تروریسم وفضای سایبری است و عموماً به

[5] . Richard Clarke
[6] . Cyber Terrorism
[7] . Dorothy Denning

معنای تهاجم غیرقانونی و تهدید به تهاجم علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن‌ها، به منظور ارعاب یا اعمال زوربر دولت یا ملتی جهت پیشبرد هدف‌های سیاسی یا اجتماعی است. بعلاوه، درتوصیف تروریسم سایبری، تهاجم باید منجر به تعرضی علیه شخص یا اموال شود یا حداقل سبب صدمه‌ای شود که ایجاد ترس نماید. تهاجماتی که موجب مرگ یا جراحت بدنی، انفجار، سقوط هواپیما، آلودگی آب یا خسارت‌های شدید اقتصادی می‌شوند، مثال‌هایی در این زمینه هستند. تهاجمات شدید علیه زیرساخت‌های حیاتی را، بسته به میزان اثرات آن‌ها، می‌توان در رده اقدامات تروریستی قرار داد و تهاجماتی که خدمات غیراساسی را مختل می‌سازند یا عمدتاً مزاحمتی پرهزینه هستند، در این مقوله قرار نخواهند گرفت.» (پاکزاد، 1390، ص 90)

تروریست‌ها ازفضای سایبری به عنوان کارزاری جهت انجام اقدامات خاص بانیتهای متفاوت و ضربه وخسارات مالی زدن و اقدامات مجرمانه استفاده می‌کنند، در حقیقت از دنیای واقعی به جهان مجازی واردشده‌اند و با آگاهی کامل و شناختی که از این فضا دارند و بدون آنکه به راحتی مورد شناسایی مجریان قانون قراربگیرند دست به خرابکاری بزنند.

«تاریخچه اقدامات تروریستی گواه این مسأله است که تروریست‌ها تقریباً از همان ابتدا به سیستم‌های رایانه‌ای به عنوان یک هدف ارزشمند توجه داشته‌اند. البته این مسأله در مورد کلیه فناوری‌های سطح بالا صدق می‌کند که نمونه بارز آن فناوری اطلاعات وارتباطات الکترونیکی بوده و هست. برای مثال، بریگادسرخ، طی دهه 1970، در ایتالیا 11 واحد ازتأسیسات اصلی پردازشگرهای ارتباطاتی را تخریب کرد. میزان خسارت وارده، پانصد هزار دلار برآوردشد.این گروه طی بیانیه‌ای استفاده روز افزون از رایانه‌ها را بخشی از توطئه بیشینه کردن نظارت‌های اجتماعی برشمرد. به نظر این گروه، رایانه‌ها به مثابه ابزاری جهت درگیری‌های طبقاتی به کار می‌رفتند و از این رو لازم بود به این شبکه‌های نظارتی تعرض شود تا ازبین بروند.» (جلالی فراهانی، 1389، ص 177) بنابراین تروریسم سایبری توسط گروهی با بهره برداری از نقاط آسیب پذیردر منابع اطلاعات وبا اقدامات خشونت آمیز با ویژگی‌ها و اهداف متفاوت صورت می‌گیرد که گاهی معادل عملیات جنگ اطلاعات تهاجمی به کاربرده می‌شود.

3- حمله‌های سایبری[8]

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, pp 9-10). حمله‌های سایبری شامل چهار حوزه می‌شود: 1- از دست دادن تمامیت، 2- از دست دادن قابلیت، 3- از دست دادن اطلاعات محرمانه و 4- تخریب فیزیکی (Army, 2005, pp 1-3).

آب، برق، بانکداری و حمل ونقل هوایی، تنها چند نمونه از خدماتی است که توسط زیرساخت‌های اطلاعات و ارتباطات در حال اجراست. این زیرساخت‌ها به طور فزاینده ای 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 تأثیر ات بالقوه حملات اینترنتی است (Islan et al., 2011, pp 5-6).

4- جرایم سایبری[9]

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 مختل کردن آنها و یا کپی از اطلاعات طبقه بندی شده می‌شود (Nagre and Warade, 2008). تحلیل گران هزینه جرایم اینترنتی را برای صنعت جهانی بیش از هزار میلیارد دلار در موارد نقض مالکیت

[8] . Cyber Attacks
[9] . Cyber Crime

فکری و از دست دادن اطلاعات تخمین زده‌اند. برای مثال، شخصی در سال 2009، چندین ترابایت از داده‌های مربوط به سیستم الکترونیکی و طراحی اطلاعات از برنامه جنگنده‌های مشترک 300 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, p 5).

5- جاسوسی سایبری[10]

جاسوسی سایبری از رایانه‌ها و سیستم‌های مربوط به آن استفاده می‌کند تا اطلاعات محرمانه را جمع آوری 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 دزدیده شده را با اهداف مختلف مورد استفاده قرار می‌دهند که برخی از آنها عبارتند از تهدید، اخاذی و مختل کردن اقدامات رقبای سیاسی (Lord and Sharp, 2011, p 17).

6- اخلال سایبری

اخلال سایبری به معنای ایجاد هرج و مرج و برهم زدن نظم و به عبارت دیگر خلل وارد ساختن در ساختار شبکه‌ای داده‌ها و ایجاد مانع در جهت دستیابی کاربر مجاز به اطلاعات و سیستم‌های رایانه‌ای و مخابراتی می‌باشد. همین اقدام سبب از کار انداختن یا مختل شدن و در نتیجه برهم خوردن یکپارچگی سامانه‌ها و شبکه‌ها خواهد شد.

اخلال در زیر ساخت‌های حیاتی به عنوان یکی از اصول ترین و خشن ترین تهدیدات سایبری می‌باشد که می‌تواند امنیت ملی را تهدید کند.

سیستم‌های رایانه‌ای در برابر حملات و تهدیدات سایبری از آسیب پذیری بیشتری برخوردار می‌باشند و به همین دلیل درصددافزایش قدرت مقابله با عملکردها و حملات هستند.

«آسیب پذیری زیر ساخت‌ها نسبت به حمله‌های سایبری بستگی به میزان وابستگی آنها به فضای سایبر است. در کشورهای پیشرفته بعلت افزایش این وابستگی امکان حمله تروریستی نیز افزایش می‌یابد.» (پاکزاد، 1390، ص 381)

7- خرابکاری سایبری

خرابکاری سایبری به معنای تحریف و جعل یا ازبین بردن داده‌ها و اطلاعات می‌باشد. خربکاری بوسیله اتلاف داده‌ها یا تحریف اطلاعات صورت می‌گیرد. به طور کلی اتلاف داده به معنای ازبین بردن، مختل کردن، تخریب، حذف داده‌هامی باشد که توسط رایانه و در فضای سایبری رخ می‌دهد. تخریب داده‌ها به اشکال مختلف صورت می‌گیرد گاهی نتیجه حمله فیزیکی به تأسیسات کامپیوتری و آسیب رساندن به سرویس دهنده‌های وب می‌باشد و گاهی نیز این اعمال از طریق و روشهای مختلف مانند ویروس‌های کامپیوتری یا بمب‌های منطقی صورت می‌گیرد و خطرناک ترین موارد، برنامه‌های ویروسی می‌باشد که سبب اخلال و تخریب در داده‌ها می‌باشد.

«ازمیان بردن داده‌ها جزوجرایم رایانه‌ای خاص یا محض نیست؛ زیرا از میان بردن و تخریب به طور سنتی از قدیم وجود داشته واکنون نسبت به داده نیز اعمال می‌شود، بنابراین نمی‌توان آن راجزو جرم‌هایی دانست که صرفاً باروی کار آمدن محیط سایبر خلق شده‌اند.» (فضلی، 1391، ص 169)

تخریب اطلاعات به معنای تغییر ماهیت و محتوای آن‌هاست. تحریف اطلاعات از طریق تغییر در برنامه و کنترل داده‌ها که سبب تغییر در شکل، صفحه وب می‌باشد.

[10] . Cyber Espionage

اختلال و تخریب در یک سیستم سبب اختلال در دیگر سیستم‌ها خواهد شد و همین امر سبب ایجاد حملات اینترنتی خواهد شد که می‌تواند امنیت ملی را تهدید کند.

8- آشفتگی سایبری[11]

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[12]، مدیر سایت جنجالی ویکی لیکس، حمله‌های سایبری گسترده‌ای انجام دادند. برخلاف جرایم سایبری و جاسوسی سایبری که هدف شان 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، آسیب رساندن 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, 2011, p 18).

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.

تأثیر تهدیدهای سایبری بر امنیت ملی

بسیاری از کارشناسان و تحلیل گران حوزه امنیت، بر این باورند که پایان یافتن دوران جنگ سرد نه تنها منجر به امن تر شدن جهان نشده است، بلکه به وجود آمدن چالش‌های امنیتی غیرنظامی جدیدی همچون تخریب محیط زیست، رفاه اقتصادی، سازمانهای جنایی بین المللی و مهاجرت گسترده افراد، امنیت جهانی را با چالش‌های جدی تری نسبت به گذشته مواجه ساخته است. تحلیل گران 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 داشته اند. همانطور که در بخش‌های پیشین اشاره شد، آنچه در مورد این تهدیدهای جدید قابل توجه است، این است که ویروس‌ها، کر مها، 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 تهدید ات متأثر از انقلاب مداوم اطلاعات و رسوخ آن به تمام جنبه‌های زندگی بشر امروز است. بنابراین، در بخش پیش رو، ابتدا به انقلاب

[11] . Cyber Agitation
[12] . Julian Assange

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.

از آنجا که در مورد تأثیر تهدیدات سایبری بر امنیت ملی نظرات و دیدگاه‌های مختلفی توسط تحلیل گران مسائل امنیتی بیان گردیده است ولی آنچه بطور کلی حائز اهمیت است بیان این مطلب می‌باشد که امروزه مسائل مختلفی مانند: مبادلات، ارتباطات، بانکداری، تجارت الکترونیکی و غیره در فضای سایبر سبب تخریب اطلاعات و در نتیجه ایجاد چالش در حوزه امنیت شده است. پس پایان یافتن جنگ سرد نه تنها سبب امن تر شدن جهان نشده است بلکه به وجود آمدن چنین چالش‌هایی، امنیت جهانی را با تهدید مواجه ساخته است.

امروزه حمله‌های مختلف مانند :محوریت هک (استفاده از قوه خلاقیت در یک مسئله یا پروژه برنامه سازی و همچنین تغییر رفتار یک برنامه کاربردی یا یک سیستم عامل از طریق تغییر دستورات و نه اجرای برنامه و انتخاب گزینه‌ها).و کرک (دستیابی غیر مجاز به یک شبکه از طریق گذشتن از اقدامات امنیتی است و متضمن تفسیر و درک اطلاعات رمز گذاری شده می‌باشد.)، کرم‌ها، بمب منطقی (که سبب ایجاد خسارت، تغییر و تخریب در داده‌ها و یا برنامه‌های کامپیوتر می‌شود) جزء واقعیتهای غیر قابل انکار می‌باشند.

این حملات وسیع می‌تواند به عنوان تهدید جدی منافع ملی یک کشور را به چالش بکشاند. بطوریکه کشورهای مختلف مانند: ایالات متحده آمریکا ،چین، مالزی، به برخورد فیزیکی با این حملات پرداخته اند و اسناد مختلفی در زمینهٔ تأمین امنیت در فضای سایبر به تصویب رسیده است.

1- رویکردهای نظری متفاوت به امنیت ملی

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

واقع گرایان معتقدند در سطح سیاست داخلی، مسئله ای به نام امنیت وجود نداشته و امنیت صرفاً در سطح بین المللی معنا می‌یابد. به بیان دیگر، امنیت ملی نزد آنان چیزی جز امنیت بین الملل نیست و در این راستا ناامنی ویژگی بارز نظام بین الملل است (عبدالله خانی، 1387، ج1، ص 70).

از نظر واقع گرایان، عدم امنیت اصلی ترین مسأله، قدرت مهم ترین ابزار، دولت مهم ترین بازیگر و جنگ، بارزترین جلوه بروز ناامنی در عرصه بین المللی است (یزدان فام، 1389، ص 731). بنابراین، محور تمرکز واقع گرایی در موضوع امنیت، نظامی است.

همانطور که استفن والت[13] تعریف می‌کند، مطالعات امنیتی، مطالعه تهدید، استفاده و کنترل نیروی نظامی است (Williams and Krause, 1996).

جدای از مسائل نظامی، سایر عوامل هم در بحث امنیت می‌توانند مهم باشند، اما واقع گرایان و نوواقعگرایان معمولاً تنها تا جایی آنها را مهم می‌شمارند که به توسعه توانایی‌های نظامی کمک کند (تریف، 1383). از نظر واقع گرایان، هر چیزی ممکن است بر امنیت تأثیرگذار باشد، اما موضوع امنیت هر چیزی نمی‌تواند باشد. به باور واقع گرایان، چون دولت‌ها بازیگران اصلی در نظام بین الملل می‌باشند، بنابراین آنان مرجع امنیت قرار خواهند گرفت (عبدالله خانی، 1387، ج1، ص 83).

در نقطه مقابل، لیبرالیسم کلاسیک ضمن قبول وجود آنارشی در عرصه بین المللی، با انتقاد از سیاست قدرتمندانه واقع گرایی 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 واقع گرایی قبول دارد که عرصه بین

[13] . Stephen Walt

المللی، عرصه آنارشی است و چنین فضایی امنیت ملی و بین المللی را به خطر می‌اندازد، اما برای حفظ امنیت، راه حل متفاوتی دارد. صاحب نظران 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 بین المللی میسر است (یزدان فام، 1389، ص 732).

از سوی دیگر، مکتب کپنهاگ نیز مخالف دیدگاهی است که هسته اصلی مطالعات امنیتی را جنگ و زور می‌داند. بوزان معتقد است در دیدگاه واقع گرایان مفهوم پیچیده امنیت به مفهومی مترادف با قدرت کاهش پیدا کرده است (بوزان، 1388، ص 8). 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 عالی تر دولتی و بین المللی می‌باشند.

بنابراین، مکتب کپنهاک نیز با رد فردمحوری در مرجع امنیت، تمرکز خود را بر دولت به عنوان محور امنیت قرار می‌دهد (عبدالله خانی، 1387). بوزان در یکی از نوشته‌های خود با عنوان «الگوی جدید مطالعه امنیتی در قرن 21»، الگوی جدید مطالعات امنیتی را بر اساس مؤلفه‌های پنج گانه سیاسی، نظامی، اقتصادی، اجتماعی و زیست محیطی می‌داند (Buzan,1991, p 433).

رویکرد سازه انگاری نیز ضمن رد ماهیت آنارشیک نظام بین الملل، هویت را به عنوان دستور العمل، وارد بررسی‌های امنیتی و سیاست خارجی دولت‌ها کرد. در این چارچوب، دولت‌ها بر اساس هویت شان، 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 برساخته شده و قوام می‌یابد. توجه به امنیت انسانی، به عنوان مرجع نهایی امنیت و گرایش به مفاهیم جهان شمول در امنیت جهانی، از ویژگیهای نظریه سازه انگاری است (یزدان فام، 1389، ص 737).

البته، باید اضافه کرد که برخی نویسندگان همچون جسیکا تاچمن به دنبال برخی تحولات جهانی بر گسترش مطالعات امنیتی به مسائلی همچون تهدیدهای زیست محیطی، رفاه اقتصادی و رشد جمعیت تأکید کرده‌اند (Tuchman, 1989, p 162).

بنابراین، با این بررسی هر چند اجمالی، در پایان این بخش به همان نتیجه ای 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، 1389، ص 55) در نتیجه، هیچ یک از تعاریف و رویکردهای مربوطه نتوانسته اند به خوبی و همه جانبه 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 کشیده شدن مفهوم امنیت به فضای مجازی، نه تنها درک روشنی از فضای جغرافیایی تهدید وجود ندارد، بلکه با گستردگی منابع تهدیدکننده امنیت نیز مواجه هستیم.

2- رویکردهای متفاوت به تهدیدات سایبری

امروزه مفهوم امنیت تنها محدود به دو بعد امنیت داخلی و خارجی نمی‌باشد بلکه این واژه گسترش بیشتری یافته است و دارای متغیری نسبی است. بوزان امنیت را به پنج مقوله تقسیم کرده است: نظامی، سیاسی، اقتصادی، اجتماعی، زیست محیطی. هر چند این تقسیم بندی کامل به نظر می‌رسد ولی باز هم تهدیدات سایبری در این تقسیم بندی گنجانده نشده است.

از آنجا که تهدیدات سایبری دارای گستردگی و ویژگی جهانشمول بودن است دیگر امروزه نمی‌توان ازآن غافل شد و باید به رویکردهای متفاوت در روابط بین المللی اشاره شود و راهکارهای مقابله با این تهدیدات بیان شود.

واقع گرایان به داشتن جایگاه مشخصی برای تهدیدات سایبری توافق ندارند. آنها در مقابل دستور کار مطالعات امنیتی، دربارهٔ تأثیر گذاری واقعی حمله‌های سایبری بر امنیت فیزیکی دولت‌ها و ظرفیت نظامی شان بحث می‌کنند. آنها معتقدندکه این چالش‌ها برامنیت داخلی دولت‌ها تأثیر گذاشته ولی سبب فروپاشی نظام بین الملل نخواهد شد.

«لیبرال‌ها هم به مانند واقع گرایان، دولت‌ها را بازیگران اصلی سیاست جهان می‌دانند، ولی برخلاف آنها می‌گویند دولت‌ها به هیچ وجه یگانه بازیگرانی نیستند که در روابط بین الملل نقش مهمی بازی می‌کنند. درواقع، بارزترین تغییری که در سال‌های اخیر در حوزه سیاست بین الملل رخ داده است، سر برآوردن مجموعه گسترده‌ای از بازیگران غیر دولتی بین المللی 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، 1390)

در حقیقت لیبرال‌ها امنیت را به مراتب وسیع تر از واقع گرایان تعریف نموده به گونه‌ای که آنها مفهوم امنیت را از عرصه محدود ژئوپلیتیک و نظامی خارج کرده و به نحو وسیع و گسترده یعنی مسائلی مانند ثروت-رفاه و موضوعات زیست محیطی را دراین تعریف وارد می‌سازند. بازیگر این صحنه تنها دولت‌ها نیستند بلکه شامل سازمآن‌های بین المللی، فراملی و غیر حکومتی نیز می‌شود.

در مقابل این نظریات دیدگاه‌های متفاوتی نیز جهت مقابله با تهدیدات سایبری بیان گردیده است. بسیاری از دانشمندان، شرکت‌های خصوصی، نهادهای دولتی در تلاش جهت ارئه راهکارهای مناسب برای ایمن سازی سیستم‌های رایانه‌ای ارائه کرده‌اند.

«در رویکرد نخست بیشتر سعی در «پیشگیری وضعی»و ارائه راهکاری فنی در جهت مبارزه با حملات است. براین اساس در مواردی نظیر حفظ امنیت و محرمانگی اطلاعات بر عهدهٔ صنعت مربوطه است و علاوه بر استفاده از راهکارهای فنی همچون استفاده از نرم افزارهای ضد ویروس و ضد اختلال، با وضع مقرارت لازم جهت برخورد با حملات و خطرات این فضا و تهدیدات آن گام برداشته شود. در رویکرد دوم فرهنگ سازی و آموزش مبارزه با برنامه‌های مخرب و حملات رایانه‌ای به کاربران مورد توجه قرار می‌گیردتا کاربران کمتر مورد حملات خطرناک اینترنتی قرار گیرند.» (فضلی، 1391، ص 195)

در سطح بین الملل مهمترین تغییرات در حوزهٔ تهدیدات سایبری، می‌توان به تأسیس وزارت امنیت داخلی که مورد حمایت کمیسیون امنیت ملی ایالات متحده قرار گرفت، اشاره نمود.

همانطور که مرزهای فیزیکی کشورها در خطر حملات مختلف می‌باشند، مرزهای سایبری و مجازی بسیار پر نفوذ ترهستند که می‌توانند زیر ساخت‌های حیاتی کشورها مخصوصاً زیر ساخت اقتصادی هر کشوری را هدف حمله قرار دهند و بر امنیت ملی تأثیر بگذارند.

1-2- قدرت در عصر اطلاعات

امروزه جهان وارد عرصه جدیدی از مبادلهٔ اطلاعات در زمینهٔ تجارت،اقتصاد،بازرگانی و غیره شده است که هرگونه تحول در مفهوم قدرت سبب تغییر و تحول در مفهوم امنیت خواهد شد.

دانشمندان علم سیاست بین دو مفهوم قدرت و امنیت وابستگی می‌دانند و معتقدند که تغییر در مفهوم قدرت سبب تغییر در مفهوم امنیت خواهد شد.

«می‌توان میان قدرت رفتاری[۱۴] یعنی توانایی به دست آوردن نتایج مطلوب و قدرت منابع[۱۵] 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.

[14] . Behavioral Power

برهمین اساس، منابع قدرت درحال تغییرند. درسده هجدهم، سرزمین، جمعیت و کشاورزی منبع قدرت تعیین کننده بود. در سده نوزدهم، ظرفیت صنعتی، درمیانه سده بیستم نیز علم و به ویژه فیزیک هسته ای، منابع قدرت تعیین کننده‌ای در اختیار قدرت‌ها قرار داده بود. در سده حاضر، توانایی اطلاعاتی در تعریف وسیع خود، احتمالاً تعیین کننده ترین منبع قدرت است.» (خلیلی پور رکن آبادی و نورعلی وند، 1391، ص 181)

امروزه اینترنت ارتباط نامحدود بین افراد با یکدیگر در سطح گسترده‌ای بوجود آورده است و سبب افزایش قدرت کنترل بر اطلاعات شده است. افراد می‌توانند سریعاً و با صرف هزینه اندک به پیام‌های اینترنتی دسترسی پیدا کنند.همین امر باعث ایجاد چالش در کنترل جریان اطلاعات توسط حکومتها شده است.

«این بدین معناست که سیاست خارجی، عرصه‌ای نخواهد بود که صرفاً حکومتها درآن 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 و حتی مورد سوء استفاده دیکتاتورها و تروریست‌ها نیز قرار بگیرد و آنها با استفاده ازآن، ایدئولوژی خود را گسترش دهند.» (نای، 1387)

بنابراین تحولاتی که در سطح جهانی در زمینه تکنولوژی ارتباطات و فناوری آن بوجود آمده است، سبب ایجاد تحول و دگرگونی در منابع قدرت شده است همانگونه که بیان شد تحول در قدرت سبب تحول در امنیت خواهد شد زیرا این دو به یکدیگر وابسته هستند و بر یکدیگر تأثیر مستقیم خواهند گذاشت، همین امر موجب شده که هرگونه چالش و تهدید در منابع قدرت سبب ایجاد اختلال در امنیت کشور شود.

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[16] چهارصد سال پیش نوشت، اطلاعات قدرت است. انقلاب اطلاعات را به معنی پیشرفت‌های سریع فناوری در عرصه رایانه‌ها، ارتباطات و نرم افزار می‌دانیم که با خود کاهش چشمگیر هزینه پردازش و انتقال اطلاعات را به همراه آورده است (روزنا، 1390، ص 362). جهان در حال حاضر به عصر جدیدی وارد شده که ویژگی‌های خاص خود را دارد. تجارت الکترونیک، فعالیت‌های اقتصادی شبکه ای 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، 1387، ص 52).

می توان میان قدرت رفتاری[17]، یعنی توانایی به دست آوردن نتایج مطلوبمان و قدرت منابع[18]، 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، 1390، ص 367). 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 بین المللی، عواملی همچون فن آوری، آموزش و رشد اقتصادی اهمیت بیشتری یافته اند 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، 1387، ص 98).

---

15 . Resource Power
16 . Francis Bacon
17 . Behavioral Power
18 . Resource Power

در سده هجدهم، سرزمین، جمعیت و کشاورزی منبع قدرت تعیین کننده بود. در سده نوزدهم، ظرفیت صنعتی، در میانه سده بیستم نیز علم و به ویژه فیزیک هسته‌ای، منابع قدرت تعیین کننده ای در اختیار قدرت‌ها قرار داده بود. در سده حاضر، توانایی اطلاعاتی در تعریف وسیع خود، احتمالاً تعیین کننده ترین منبع قدرت است (روزنا، 1390، ص 369). 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, p13).

بنابراین، اینترنت شرایطی را به وجود آورده که در آن، قدرت کنترل بر اطلاعات به میزان بسیار بیشتری توزیع شده است. اینترنت زمینه ارتباطات نا محدود فرد به فرد (از طریق ایمیل)، فرد به تعداد بیشتری از افراد (از طریق هوم پیج[19] 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، عرصه ای 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، 1387، ص 141). در نتیجه، اینترنت از طریق همین ابزارهای ارتباطی، ناراضیان را یکصدا کرده تا شنیده شوند و به عموم مردم وسیله ای داده است تا سازماندهی شوند. در حالی که برخی تحلیل گران نقش اینترنت در انقلاب‌های خاورمیانه و شمال آفریقا را انکار می‌کنند، شبکه‌های اجتماعی همچون توئیتر و فیس بوک، نقش بسزایی در شکل گیری 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, p 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 پیچیده تر خواهد کرد (Nye, 2010, p 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 گسترده ای 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.

2-2- 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 گریبان گیر 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

[19] . Homepage

رویکرد رایجی که درباره امنیت در چارچوب مطالعات راهبردی در طول دوره جنگ سرد توسعه داده شده است، دارند. این گرایش تأکید بر ضرورت فر ارفتن از آنچه در بسیاری از نگرش‌ها به عنوان تفسیر بیش از حد نظامی شده از امنیت در نظر گرفته شده و ملازم با ظهور چالش‌های امنیتی جدید بوده است، دارد (کلارک، 1386، ص 236). از نظر این گروه، امروزه دیگر تهدیدهای امنیتی صرفاً نظامی نیست، بلکه مسائل زیست محیطی، 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, p 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 خدمات رسانی اینترنت در حوزه‌های مختلف زندگی بشر و به ویژه در امور تجاری و بازرگانی، مهاجمان رایانه ای، 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 پیچیده تر می‌شوند، امنیت ملی کشورها و دولتها را به طور مستقیم تحت تأثیر قرار می‌دهند (میرمحمدی و محمدی لرد، 1387، ص 36).

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 95 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 پیش گفته 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
- آسیب پذیری‌های 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، 1390، ص 130). سوم، ارتباط موضوع امنیت با شبکه‌های جهانی و چهارم، کاهش ظرفیت دولت‌ها در تولید امنیت شهروندان خود (کلارک، 1386، ص 243). 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 1998 ، واشنگتن در ارتباط با هفت نشانی اینترنت مسکو[20] 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، 1387، ص 147).

بر اساس نگرش سنتی، دولت‌ها به تضمین بقای خود و تأمین امنیت نظامی شان، 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 1381)، تورنتو را در آتش بسوزانند، بلکه از این نگرانند که رایانه ای در تگزاس، تورنتو را با مشکلی عمده روبرو کند (نای، 1387، ص 124). 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 سرمایه گذاری 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, p 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, p 484). در راستای چنین اهمیتی بود که در 29 می‌سال 2009 ، 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, p 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.

پس هدف از ایجاد امنیت سایبری دریک کشور محافظت از سیستم‌ها و ساختارهای اطلاعاتی یک کشور و جلوگیری از افشای اطلاعاتی است که می‌تواند به تمامیت ارضی یک سرزمین آسیب جدی وارد سازد.

به وجود آمدن چالش در امنیت سایبری یکی از مسائل مهم و پیچیده می‌باشد، از آنجا که تهدیدات سایبری تنها به عنوان خطری برای دولت‌ها محسوب نمی‌شود بلکه به عنوان تهدید جدی برای افراد و سازمآن‌های خصوصی نیز می‌باشد باید سعی در رسیدن به امنیتی دراین زمینه نمود.

[20] . Moscow Internet Address

در رسیدن به چنین امنیتی نیاز به برنامه ریزی اصولی و مهم تنها از طرف دولت‌ها نمی‌باشد بلکه دراین زمینه باید ارگان‌های مختلف، سازمان‌ها، افراد و گروههای جامعه، بخش خصوصی به همکاری با دولت بپردازند.

در روابط بین الملل نیز جامعه جهانی سعی در ارائه راهکارهایی جهت حمایت از امنیت سیستم‌ها و همکاری بین دولت‌ها دراین زمینه نموده است.

رویکردهای نظری و تهدیدهای سایبری

شاید بسیط ترین بحث در زمینه امنیت، متعلق به مکتب کپنهاگ باشد که عرصه مطالعات 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 زیست محیطی ختم می‌کند و از تهدیدهای سایبری سخنی به میان نمی‌آورد. با وجود این، اگرچه تا به امروز تهدیدهای سایبری به رغم اهمیت و گستردگی همچنان و تا حد زیادی از سوی رویکردهای مختلف مورد بی توجهی قرار گرفته است، اما گستردگی تهدیدهای سایبری به حدی است که دیگر نمی‌تواند بیش از این مورد غفلت رویکردهای نظری در روابط بین الملل قرار گیرد. در این بخش به تأثیرگذاری تهدیدهای سایبری بر روی نظریه پردازی در روابط بین الملل می‌پردازیم.

استفن والت در چارچوب مکتب واقع گرایی تدافعی ادعا می‌کند که مطالعات امنیتی بایستی بر روی «پدیده جنگ» که به وسیله قدرت‌های نظامی که تحت کنترل سیاسی بازیگران دولتی اداره می‌شوند، تمرکز کند. این مطالعات همچنین می‌تواند شامل کنترل تسلیحات و مدیریت بحران که به طور مستقیم در ارتباط با مسایل نظامی هستند، باشد. بنابراین، نوواقع گرایان در مقابل توسعه دستور کار مطالعات امنیتی، شامل امنیت سایبری، مادامی که هنوز درباره تأثیرگذاری واقعی حمله‌های سایبری بر امنیت فیزیکی دولت‌ها و ظرفیت نظامی‌شان مشاجره وجود دارد، بحث می‌کنند. در هر صورت، به نظر می‌رسد نوواقع گرایان بر روی جایگاه تهدید سایبری در این زمینه توافق ندارند (Hare, 2010, p 215).

از قرار معلوم، برخورد واقع گرایان با چالش انقلاب اطلاعات بسیار شبیه برخوردی است که پیش تر با چالش‌های فراملی شدن، وابستگی متقابل پیچیده و جهانی شدن داشته اند. آنها این گرایش‌ها را به چشم یک رشته پی پدیدار[۲۱] می‌بینند که کاملاً ممکن است بر سیاست‌ها و ساختارهای داخلی دولت‌ها تأثیر بگذارند، ولی نظام اقتدارگریز سیاست بین الملل را متزلزل نمی‌کنند و بنابراین به اولویت دولت به عنوان عالی ترین واحد سیاسی لطمه‌ای نمی‌زنند (روزنا، 1390، ص 21).

بری بوزان معتقد است مطالعات امنیتی جنبه‌هایی از دستور کار گسترده تر 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 بین المللی 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، مهم اند. بنابراین، تهدیدهای سایبری می‌توانند در چارچوب تحلیل مکتب کپنهاگ جای گیرند (Hare, 2010, p 214).

لیبرال‌ها هم مانند واقع گرایان، دولت‌ها را بازیگران اصلی سیاست جهان می‌دانند، ولی بر خلاف آنها می‌گویند دولت‌ها به هیچ وجه یگانه بازیگرانی نیستند که در روابط بین الملل نقش‌های مهمی بازی می‌کنند. در واقع، بارزترین تغییری که در سال‌های اخیر در حوزه سیاست بین الملل رخ داده است، سر برآوردن مجموعه گسترده ای از بازیگران غیردولتی بین المللی جدید (شرکت‌های فرامرزی، جنبش‌های اجتماعی، گروه‌های فشار، شبکه‌های احزاب سیاسی، مهاجران و تروریست‌ها) بوده است. بدین ترتیب، «وبلاگ‌ها» لیبرال‌ها بالقوه می‌توانند به پیدایش گروه‌های اینترنتی و از طریق انواع فناور ی‌های دیداری جدیدی که در اتاق‌های گفتگوی اینترنتی و شنیداری اطلاعات و ارتباطات فعالیت دارند، واقف باشند (روزنا، 1390، ص 23).

[21] . Epiphenomenon

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 مرزبندی‌ها به ویژه مرزهای هویت را به چالش می‌کشد. ادوارد[۲۲] جنگ اطلاعات پایه را نوع خاصی از «جنگ هویت» می‌داند که در آن تمامی انواع مرزبندی‌ها از جمه تفکیک قدیمی داخلی - بین المللی به چالش کشیده می‌شود. بر این اساس، هویت دولت ملی به خطر می‌افتد. البته، این امکان وجود دارد که دولت به جای تسلیم شدن 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، 1390، ص 3).

نتیجه گیری

تکنولوژی‌های جدید اطلاعات موجب جلب بزهکاران فراوانی به این فضا می‌باشد از این فضا می‌توان به عنوان محیطی جهت انجام اقدامات تروریست‌ها برضد داده‌ها نام برد.

همین امر باعث جلب توجه حقوقدانان، جرم شناسان، نیروی پلیس در سطح ملی و بین الملل به شناسایی و کشف اینگونه جرایم می‌باشد.پس تهدیدات سایبری به عنوان یکی از مسائل مهم وانکار ناپذیر در حوزه سیاست جنایی دولت‌ها می‌باشد.در واقع جامعه بین المللی با یک مشکل جدی مواجه می‌باشد.

دولت‌ها باید با اتخاذ تدابیر و راهکارهای مناسب درجهت سالم سازی و مقابله با اجتماعات آلوده به فساد گام بردارند، البته قوانینی را که تا کنون دولتها وضع نموده‌اند ناظر بر اینگونه اهداف بوده است.

گسترش فزاینده فناوری اطلاعات و ارتباطات به تحول و دگرگونی در ابعاد مختلف مؤلفه‌های اقتصادی، سیاسی، اجتماعی و فرهنگی و نظامی منجر خواهد شد و مجموعه فعالیت‌ها در زمینه‌های تولید، بهره برداری، بانکداری، برقراری ارتباطات با رایانه‌های شبکه بندی شده را دستخوش تغییرات جدی قرار خواهد داد. در آینده نزدیک زیرساخت‌های حیاتی در زمینه‌های اقتصادی، مسائل اجتماعی فرهنگی و دفاعی و امنیت ملی کشورها به فناوری اطلاعات و ارتباطات وابستگی پیدا خواهد نمود این زیرساخت‌ها عبارتند از: انرژی (نیروی برق، نفت و گاز)، حمل ونقل (راه آهن، هوایی و دریائی)، بانکداری، مخابرات، بهداشت عمومی، خدمات فوریتی، آبرسانی، صنایع دفاعی، تغذیه، کشاورزی، امور بارگیری کالا و....

امروزه به دلیل گستردگی آسیب پذیری‌های ناشی از تهدیدات سایبری نمی‌توان امنیت راتنها محدود به مسائل نظامی و مرزهای داخلی و خارجی تعریف نمود بلکه باید به امنیت اقتصادی، اجتماعی غیره نیز اشاره داشت. تهدید امنیت ملی می‌تواند خطر افت زندگی را برای ساکنان کشور پیش آورد و با خطر جدی کاهش طیف خط مشی‌هایی که حکومت‌ها می‌توانند از میان آنها دست به انتخاب بزنند، همراه باشد.

ضربه وارد شدن و حمله به هر کدام از ساختارهای امنیتی در سطوح مختلف ملی و بین المللی، به عنوان تهدیدی نوین و ویرانگر علیه امنیت می‌باشد که می‌تواند موجبات فروپاشی و نابودی زیر ساخت‌های حیاتی و بنیان یک جامعه شود.

امنیت اطلاعات می‌تواند افشاء اطلاعات سری و محرمانه باشد که سبب ضربه زدن به امنیت ملی می‌شود. تأمین امنیت و حفاظت از اطلاعات یکی از مهم‌ترین بخشی‌هایی است که قدرت دولت‌ها را نشان می‌دهد. امنیت سایبری محافظت از سیستم‌ها و ساختارهای اطلاعاتی یک کشور می‌باشد که جهت مهار ومقابله با اینگونه تهدیدات تلاش دولت‌ها به تنهایی کافی به نظر نمی‌رسد و نیاز به همکاری مؤثر بین دولت‌ها و افراد می‌باشد.

از آنجا که در مواجه شدن با اینگونه جرایم بزه دیدگان به دلایل مختلفی حاضر به اعلان جرم به مقامات قضائی نمی‌باشند باید به آنها آموزش‌های لازم در خصوص اعلان به موقع جرایم واقع شده داده شود.

[22] . Edverard

علاوه بر آسیب‌پذیری‌های داخلی ناشی از ضعف زیرساخت‌های فنی و نیز کمبودها و ضعف‌های آموزشی، طیف وسیعی از عوامل مهاجم وجود دارند که می‌توانند علیه زیرساخت‌های اطلاعاتی حساس دست به تهاجم بزنند. مهم ترین نگرانی در این باره تهدید ناشی از حملات سایبری سازمان یافته است که قادر به تحمیل لطمه‌های جبران ناپذیر بر زیرساخت‌های حیاتی کشور می‌باشد.

قدر مسلم آن است که همگام با توسعه روزافزون فناوری اطلاعات، ابزارها و شیوه‌های مختلف تهاجمی نیز به سرعت گسترش یافته و توان تخصصی و درجه پیچیدگی نفوذگران عامل تخریب یا غارت سیر صعودی پیدا کرده است.

علاوه بر پیچیدگی روزافزون ابزارهای مورد استفاده در حملات رایانه‌ای، بر شمار عاملانی که قدرت یورش علیه زیرساخت‌ها را دارند هم روزبه روز افزوده می‌شود.

در دوران صلح و آرامش احتمال جاسوسی دشمنان درباره اوضاع عمومی کشور و دستیابی به اطلاعات طبقه بندی شده و نیز جمع آوری اطلاعات در مورد مواضعی از قبیل اهداف کلیدی و رخنه در زیرساخت‌ها به طرق مخفی و سایر شیوه‌های دستیابی به اطلاعات به منظور تدارک تهاجم‌های سایبری متصور بلکه مسلم است.

در زمان جنگ یا بحران دشمن می‌تواند به اتکای اطلاعات جمع آوری شده به زیرساخت‌های حیاتی و فعالیت‌های اقتصادی عمده حمله و یا با مخدوش کردن اعتبار سیستم‌های اطلاعاتی نزد افکار عمومی و نیز ایجاد نگرانی و هراس عمومی شورش‌های گسترده و براندازی را تدارک نماید.

از ویژگی‌های فناوری اطلاعات و بویژه اینترنت، امکان ساماندهی و تدارک تهاجم سازمان یافته از فواصل دور علیه اهداف از پیش تعیین شده می‌باشد و به مهاجمان این امکان را می‌دهد تا علیه اهداف خود اقدام و ایجاد اختلال کنند. این فناوری علاوه بر اینکه موجب آشکار شدن نقاط ضعف موجود در زیرساخت‌های حیاتی می‌شود، با ایجاد برقراری ارتباط مخرب مانع از واکنش‌های دفاعی و یا ایجاد تأخیر در آنها نیز می‌گردد. در تهاجم از طریق شبکه اینترنت حتی کشورهایی که بدلیل موقعیت جغرافیائی از بسیاری از تهاجم‌های فیزیکی مصونیت دارند نیز در امان نخواهند بود زیرا در فضای مجازی مرزهای کشورها مفهوم چندانی نداشته و اطلاعات بی محابا از مرزبندی‌های سیاسی، اخلاقی و اجتماعی عبور کرده و تبادل می‌شود.

بخاطر اهمیت جهانی فضای مجازی (ارتباطات رایانه‌ای)، آسیب پذیری‌های موجود در سراسر جهان کاملاً قابل پیش بینی است و هرکس در هر نقطه از جهان به صرف دارا بودن توان آشکارسازی و در اختیار داشتن ابزارهای لازم می‌تواند مبادرت به حمله و آسیب رساندن به فضای مجازیِ هدف نماید. لذا مهاجمان رایانه‌ای قادرند بدون کوچکترین هشداری به شبکه‌های ملی یورش آورده و با آنچنان سرعتی گسترش یابند که بسیاری از مواضع هدف، حتی فرصت شنیدن صدای آژیر خطر را نیز پیدا نکند و حتی در صورت هشدار قبلی هم به احتمال زیاد فرصت لازم برای محافظت از خود را نداشته باشند.

از این جهت لازم است تا در سطح ملی ضمن شناسایی نقاط ضعف و قوت و نیز آسیب پذیری‌های احتمالی و با درنظر گرفتن فرصت و فشارها در محیط بین الملل، اقدامات بازدارنده متناسب، پیش بینی و چاره اندیشی شود.

آنچه مسلم است ایجاد شبکه امن و محافظت از زیرساخت‌های فناوری اطلاعات مستلزم تلاش همه دستگاههای مسؤول مبتنی بر راهبرد مشخص است که بایستی توسط مسؤولین تعیین خط مشی پس از احصاء آسیب پذیری‌ها و تهدیدات احتمالی طراحی و به مرحله اجرا درآید.

از آنجایی که کلیه اقدامات مربوط به طراحی شبکه، اقدامات به هم پیوسته‌ای است که بروز ضعف در هر یک موجب آسیب پذیری سایر اقدامات می‌شود لذا این عملیات از قبیل استفاده از نرم افزار، معماری شبکه مدیریت اطلاعات و امنیت شبکه، استانداردسازی و اقدامات کاربرها، مستلزم هماهنگی و پیش بینی راهکارهای علمی و امنیتی می‌باشد.

در بخش مربوط به قوانین، مسائل حقوقی و قضایی نیز، اینترنت قواعد سنتی حاکم بر رسیدگی‌های قضایی را دستخوش تحولات اساسی کرده است. تعریف از جرائم در محیط‌های مجازی انطباق چندانی با تعاریف کلاسیک نداشته و در بسیاری از موارد متفاوت است. در سیستم امنیتی متعارف برای اجرا و اعمال مقررات جزایی یک محدوده و مرز جغرافیایی وجود دارد که

همیشه و بطور اصولی محدود به خاک یک کشور و تحت حاکمیت یک دولت می‌شود به عبارت دیگر اعمال حاکمیت از سوی یک دولت مطرح است. همچنین شرط استرداد مجرمین، عدم تعارض این عمل با حاکمیت دولت‌ها در عرصه‌های سیاسی و قضایی است.

بنابراین رسیدگی به جرائم ارتکابی در محیط‌های مجازی در ابعاد داخلی و در ابعاد بین المللی با کمبودها و چالش‌های اساسی مواجه است.

با گسترش شبکه جهانی اطلاع رسانی (اینترنت) به لحاظ مشکلاتی که به آنها اشاره شد جرائمی در محیط‌های مجازی به وقوع پیوسته که سیستم قضایی کشورهای مختلف نتوانسته‌اند با آنها برخورد جدی نمایند. همین امر باعث شده که شبکه اینترنت فارغ از سلطه قوانین در دنیا و فضای مستقر خود به راه خود ادامه دهد.

از دیدگاه حقوق خصوصی نیز اینترنت چالش‌هایی از قبیل صلاحیت محلی دادگاهها، قانون حاکم بر قضیه و تعارض قوانین کشورهای مختلف را فراروی همه کشورها قرار داده است.

همچنین در تجارت الکترونیکی مسائل مربوط به تصدیق امضای الکترونیک و تضمین صحت داده‌ها مشکلات جدیدی ایجاد کرده است.

بنابراین از آنجا که درگذار از جامعه صنعتی به فراصنعتی و ورود به دوره پست مدرن، حقوق نیز از حقوق صنعتی به حقوق اطلاعات و به تبع آن فناوری اطلاعات و ارتباطات تغییر و تحول یافته از اینرو شاخصه‌ها و بحث‌های خاصی را دارا شده است. بخشی از این تحول در خصوص فناوری اطلاعات ناظر به ابعاد مدنی و تجارت (حقوق خصوصی)، بخشی ناظر به حقوق عمومی (اساسی و اداری)، بخشی ناظر به حقوق جزا و بخشی دیگر ناظر به جنبه‌های بین المللی یا حقوق بین الملل است. در مقاله ی حاضر به عنوان چکیده یی از یک رساله حجیم تلاش شده است که به توسعه شبکه ملّی دیتا، چالش‌های فراروی و تهدیدهای متوجّه امنیت ملّی عنایت شده و در ضمن بذل توجه به این مهمّ آن را در حوزه‌ی امنیت ملّی جمهوری اسلامی ایران مطمح نظر قرار دهد.

منابع

اخوان کاظمی، بهرام، 1385، امنیت در نظام سیاسی اسلام، کانون اندیشه جوان

باستانی، برومند، 1390، جرائم کامپیوتری و اینترنتی، تهران، انتشارات بهنامی

بوزان، بری، مردم - دولت‌ها و هراس، 1388، تهران، پژوهشکده مطالعات راهبردی

پاکزاد، بتول، 1390، تروریسم سایبری، تهدیدی نوین علیه امنیت ملی . تهران: انتشارات دانشگاه آزاد اسلامی- دفتر گسترش تولید علم

ترکی، غلام عباس، جاسوسی رایانه‌ای، ماهنامه دادرسی، شماره ۷۹، سال چهاردهم، ۱۳۸۹

تریف، تری، 1383، مطالعات امنیتی نوین، ترجمه علیرضا طیب و وحیدبزرگی. تهران: پژوهشکده مطالعات راهبردی

جلالی فراهانی، امیر حسین، صلاحیت کیفری در فضای سایبر، فصلنامه فقه وحقوق، شماره ۱۱، ۱۳۸۶

جلالی فراهانی، امیر حسین، مزیت‌ها و محدودیت‌های فضای سایبر . مجله حقوقی. شماره 59، 1389

خرم آبادی، عبدالصمد، 1390 جزوه درس جرایم رایانه‌ای و اینترنتی، ویژه کارآموزان قضایی

خلیلی پور رکن آبادی و نورعلی وند یاسر، تهدیدات سایبری و تأثیرات آن برامنیت ملی، فصلنامه مطالعات راهبردی، شماره 20، 1391

دنینگ، دوروتی، 1383، جنگ اطلاعات و امنیت، ترجمه گروه مترجمان، انتشارات فرهنگی هنری پردازش هوشمندعلائم

روزنا، جیمز، 1390، انقلاب اطلاعات، امنیت و فناوری‌های جدید، ترجمه علیرضا طیب، تهران، انتشارات پژوهشکده مطالعات راهبردی

سازمان ملل «نشریه بین المللی سیاست جنایی» (ش. 43 و 1994/44) ترجمه دبیرخانه شورای انفورماتیک، سازمان برنامه و بودجه 1376

فضلی، مهدی، مسؤلیت کیفری در فضای سایبر، تهران، انتشارات خرسندی، 1391

فضلی، مهدی، تخریب و اختلال در داده‌ها و سیستم‌های رایانه‌ای. مجموعه مقاله‌های همایش بررسی جنبه‌های حقوقی فناوری اطلاعات، 1391

عبدالله خانی، علی، 1387، نظریه‌های امنیت: مقدمه‌ای بر طرح ریزی دکترین امنیت ملی (1)، جلد اول، تهران، مؤسسه فرهنگی مطالعات و تحقیقات ابرار معاصر تهران

کلارک، یان، 1386ریال جهانی شدن و نظریه روابط بین الملل، ترجمه فرامرز تقی لو، تهران، دفتر مطالعات سیاسی و بین الملل

مندل، رابرت، 1389، چهره متغیر امنیت ملی، ترجمه پژوهشکده مطالعات راهبردی، تهران، انتشارات پژوهشکده مطالعات راهبردی

میرمحمدی، مهدی و محمدی لرد، عبدالمحمود، 1387، سیاست اطلاعات: مطالعه موردی ایالات متحده آمریکا، تهران، مؤسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر تهران

نای، جوزف، 1387، قدرت در عصر اطلاعات : از واقع گرایی تاجهانی شدن. ترجمه سعید میرترابی. انتشارات پژوهشکده مطالعات راهبردی

یزدان فام، محمود، دگرگونی در نظریه‌ها ومفهوم امنیت بین المللی. فصلنامه مطالعات راهبردی. شماره 38، 1389

Barney, Prometheus wired:the Hope for Democracy in the Ageof Network Technology, 2001.

Brenner, Susan, Toward a criminal Law for cyber space: Distributed Security, University of Dayton School of Low.

Carter,Computer Crime Categories:How Techno-criminals operate,FBI Law Enforcement Bolletin,1995.

Charney, Computer Crime: Law Enforcement's shift From a corpored Enrironment to the In tangible,Electronic world of cyber space,Federal Bar News,1994.

Collier/ Spaul, Problems in policing computer crime, policing and Society 1992.

Comer, Internet working with Tcp/Ip-Principles,Protocols and Architecture, 2006.

United Statd Linne,The Third world security predicament ,Mohammad Ayoob, p213 ,1995 ,rinnerpublishher

Gercke,The slow wake of a Global Approach Against cyber crime,computer Law Review International 2006.

Gordon/ Ford, On the Definition and classification of cybercrime, Journal in computer Virology 2006.

Masuda, The Information Society as Post-Industrial Society,1980.

Sieber, The Threat of cyberscrime, organised crime in Europe:the threat of cybercrime, 2005.

Statd linne - cunited ,The Third world security predicament ,Mohammad Ayoob,1995