فصلنامهٔ سیاست، مجلهٔ دانشکدهٔ حقوق و علوم سیاسی، دورهٔ ۴۵، شمارهٔ ۳، پاییز ۱۳۹۴، صفحات ۶۵۴-۶۳۵

بررسی رابطهٔ اینترنت و امنیت ملی جمهوری اسلامی ایران

محسن پالیزبان[1]

دکتری علوم سیاسی دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران

(تاریخ دریافت: ۹۳/۲/۲۲– تاریخ تصویب: ۹۳/۷/۱۹)

چکیده

ازجمله ویژگی‌های بارز امنیت ملی در جهان معاصر، تحول ابعاد و ماهیت آن است که با سرعت زیاد و چشمگیری در حال وقوع است. از این نظر، تحولات رخ‌داده در حوزهٔ فناوری اطلاعات از اهمیت بیشتری نسبت به دیگر حوزه‌ها برخوردار است. امنیت در فضای مجازی، ازجمله موضوع‌هایی است که به‌تازگی در حوزهٔ مطالعات راهبردی مطرح شده است. ماهیت اینترنت و محیط امنیتی و راهبردی متأثر از آن، به‌گونه‌ای است که در کنار فرصت‌های فراوان، قابلیت ایجاد تهدید و ناامنی داشته، الزام‌های خاص خود را در حوزهٔ امنیت ملی طلب می‌کند. از این منظر، مشخص می‌شود که امنیت ملی کشور با اینترنت و امنیت فضای مجازی پیوستگی مثبتی دارد. در این مقاله تلاش می‌شود چگونگی این پیوستگی در حوزهٔ امنیتی (تروریسم، خرابکاری، عملیات جاسوسی)، حوزهٔ سیاسی- فرهنگی و حوزهٔ نظامی- دفاعی در حد توان بررسی و ارزیابی شود.

واژگان کلیدی

امنیت سیاسی- فرهنگی، امنیت فضای مجازی، امنیت ملی، اینترنت، تروریسم، جنگ اطلاعاتی، خرابکاری، عملیات جاسوسی، فناوری اطلاعات

1. E-mail: mpalizban@ut.ac.ir

مقدمه

در حال حاضر نفوذ سریع و فراگیر فناوری اطلاعات در ابعاد مختلف حیات انسان بـه بـاوری عمومی تبدیل شده است. فناوری اطلاعات در حال دگرگون کردن زندگی و حتی طـرز تفکـر مردم سراسر جهان است؛ دگرگونی‌های بسیار بنیادینی در حال وقوع است کـه مـا را بـه عـصر جدیدی به‌نام عصر اطلاعات پیوند می‌زند. همسو با این دگرگونی‌هـا، ملاحظـات و مطالعـات امنیت ملی و همین طور مدیریت امنیت ملی در فضای مجازی، موضوعیت مـی‌یابـد و بـه‌نظـر می‌رسد بررسی چگونگی اثرگذاری فناوری اطلاعات، بـه‌خـصوص اینترنـت، بـر امنیـت ملـی جمهوری اسلامی ایران، البته بیشتر از جنبهٔ محدودیت‌ها و تهدیدها، حائز اهمیت باشد. بـدیهی است این پدیده، فرصت‌هایی را نیز برای امنیت ملی جمهوری اسلامی ایران به‌وجـود مـی‌آورد که بررسی آن به فرصتی دیگر موکول می‌شود. اینترنت که در اواخر دههٔ ۱۹۶۰ توسـط آژانـس پروژه‌های تحقیقاتی پیشرفته در وزارت دفاع ایالات متحدهٔ آمریکا ابداع شـد، شـبکهٔ رایانـه‌ای سراسر جهان را به یکدیگر متصل می‌کند و به مجموعه‌ای از استانداردها یا پروتکـل‌هـا متکـی است که برای خدماتی مانند رایانامه، گروه‌های بحث، مکان‌های گفت‌وگوی اینترنتی (چـت) و انتشار چندرسانه‌ای بر روی شبکهٔ جهانی وب به زبان‌های یکسان سخن می‌گوید.

اینترنت، تنهـا جنبـهٔ انقـلاب ارتباطـات نیـست؛ گـسترش ارتباطـات مـاهواره‌ای، افـزایش شبکه‌های تلویزیونی، دسترسی به شبکه‌های کابلی در بسیاری از کـشورها از دیگـر جنبـه‌هـای انقلاب ارتباطات است. این دگرگونی‌ها بر امـور بـین‌الملـل مـؤثر بـوده، بیـشتر تقویـت‌کننـدهٔ تأثیرهای اینترنت‌اند. اما اینترنت کیفیت خاصی داشته، با مسائل امنیت ملی بـه‌گونـه‌ای خـاص ارتباط دارد:

۱. اینترنت به انتشار اطلاعات کمک می‌کند؛
۲. اینترنت به انتشار اطلاعات گمراه‌کننده کمک می‌کند؛
۳. اینترنت به انتشار اطلاعات رمزگذاری‌شده کمک می‌کند؛
۴. اینترنت فرصت‌هایی را برای خرابکاری سامانه‌های رایانـه‌ای و دیگـر زیرسـاخت‌هـا فراهم می‌کند.
۵. اینترنت وابستگی همگانی‌ای به شبکهٔ یکپارچه به‌وجود مـی‌آورد و ممکـن اسـت در تضعیف حاکمیت ملی سهیم باشد (آلبرتس، ۱۳۸۵: ۱۶۹).

رشد اینترنت نگرانی‌های جدی در پی دارد؛ اما چون ایران و دنیا می‌توانند منافع عظیمی از دسترسی به یک شبکهٔ جهانی پویا و مقاوم در بسیاری از عرصه‌ها (تجارت، فرهنـگ، آمـوزش و...) به‌دست آورند، باید شیوه‌های مواجهه با خطرهای آن را آموخت. بی‌شک، رسیدن بـه ایـن هدف مستلزم اقدام‌های دشوار، زمان‌بر، پرهزینه، پیچیده و مستمر است. این فناوری بـا وجـود

قابلیت‌های فراوان و منحصربه‌فردی که در قالب دنیای جدیدی به‌نام فضای مجازی عرضه کرده است، به‌دلیل آسیب‌پذیری فراوانی که در برابر انواع سوءاستفاده‌های منحرفانه و مجرمانه دارد، دغدغه‌های جدی را نیز برانگیخته است و به‌سادگی نمی‌توان در برابر فرصت‌های بی‌شمارش، از تهدیدهای آن چشم‌پوشی کرد.

در این مقاله تلاش می‌شود شناختی کلی از مؤلفه‌های امنیت ملی در فضای مجازی و محیط راهبردی و امنیتی در حال ظهور به‌دست داده شود و در پی آن، چگونگی تأثیر اینترنت بر امنیت ملی جمهوری اسلامی ایران در حوزه‌های نظامی، امنیتی، سیاسی و فرهنگی به‌طور کلی بررسی شود. درنهایت و در حد بضاعت تلاش می‌شود برخی راهبردهای مدیریت امنیت ملی جمهوری اسلامی ایران در فضای مجازی معرفی شود. بنابراین، هدف این مقاله یافتن پاسخ‌های مقدماتی به این پرسش‌هاست:

– اینترنت و فضای مجازی چگونه محیط راهبردی و امنیتی و مفهوم امنیت ملی را تغییر می‌دهد؟

– اینترنت چگونه برای امنیت ملی جمهوری اسلامی ایران تهدیدزا می‌شود؟

– جمهوری اسلامی ایران چه اقدام‌هایی در رابطه با اینترنت باید انجام دهد تا بتواند به‌خوبی به مدیریت امنیت ملی بپردازد؟

چارچوب نظری

در حوزهٔ فناوری اطلاعات و امنیت ملی، به‌طور معمول سه دسته پژوهش‌های نظری انجام گرفته که عبارت است از: ۱. نظریه‌ها و پژوهش‌های عمومی دربارهٔ جامعهٔ اطلاعاتی؛ ۲. پژوهش‌های خاص عملیات نظامی و امنیت سایبر؛ ۳. مطالعات امنیتی. این‌گونه پژوهش‌ها، بیشتر تک‌بعدی بوده، تأثیر فناوری اطلاعات به‌خصوص اینترنت را بر امنیت ملی شامل نمی‌شود؛ بنابراین بهتر است به قابلیت‌های نظریه‌های اصلی روابط بین‌المللی، یعنی واقع‌گرایی[1]، لیبرالیسم[2] و سازه‌انگاری[3] در تبیین و تفسیر امنیت ملی در فضای مجازی توجه شود تا این نقص در پژوهش‌ها برطرف شود.

پارادایم واقع‌گرایی، دیدگاهی سنت‌گرایانه به‌دست می‌دهد و مطالعات راهبردی دولت‌محور و نظامی‌گرایانه را اعمال می‌کند. براساس این دیدگاه، با وجود وقوع انقلاب‌های مذهبی و قومی، تروریسم، جرایم سازمان‌یافته و گرم شدن زمین، دیگر نیازی به توسعهٔ دامنهٔ مفهوم امنیت نیست. پارادایم لیبرال، در نقطهٔ مقابل پارادایم واقع‌گرایی قرار می‌گیرد؛ در این

1. Realism
2. Liberalism
3. Constructivism

پارادایم، بر کثرت بازیگران بین‌الملل، اهمیت عوامل سیاسی داخلی در تعیین رفتار بین‌المللی دولت‌ها و جایگاه نهادهای بین‌المللی در تعیین قواعد رفتار بازیگران دولتی تأکید می‌شود. به‌تازگی، کوهن[1] و نای[2] بر تأثیر فناوری اطلاعات بر امنیت هم اشاره کرده‌اند؛ اما آنها بیشتر بر آسیب‌پذیری‌های اقتصادی تأکید داشته‌اند. نای به‌طور مستقیم به تهدیدات فناوری اطلاعات اشاره نکرده است؛ اما مفهوم قدرت نرم[3] که او به آن اعتقاد دارد، برای این منظور مناسب است.

در پارادایم سازه‌انگاری، بر تفسیر چگونگی ایجاد واقعیت تأکید شده، به این ترتیب، از واقع‌گرایی و لیبرالیسم فاصله گرفته می‌شود. در این پارادایم، واقعیت‌های اجتماعی (هویت‌ها و منفعت‌ها) ساختهٔ دست اجتماع است و بنابراین پویا بوده، در معرض تولید و بازتولید مداوم است. از این‌روی، سازه‌انگاری برخلاف واقع‌گرایی و لیبرالیسم، در پی تعمیم‌های مشروط است و نه کلی. سازه‌گرایی به طرح مفهوم پویاتری از امنیت و تحلیل‌های اساسی‌تری از سیاست امنیتی کمک کرده است؛ زیرا یک موضع کلی دربارهٔ امنیت به‌دست داده نمی‌شود، بلکه بر زمینه‌دار بودن آن تأکید می‌شود. سازه‌انگاران دربارهٔ امنیت در فضای مجازی، بر تهدید انواع مرزها به‌ویژه مرزهای هویتی از سوی جنگ اطلاعاتی تأکید دارند. فضای مجازی بر نحوهٔ ادراک از جنگ و نحوهٔ انجام گرفتن آن تأثیر می‌گذارد. دنیای مجازی، مرز میان واقعیت و خیال را از بین می‌برد (Eriksson, 2006).

در این مقاله، با توجه به آنچه گفته شد، از رهیافت‌های لیبرال و سازه‌انگارانه برای تبیین امنیت ملی در فضای مجازی بهره‌برداری می‌شود؛ ضمن اینکه بر تعمیم‌های مشروط و هم تکمیلی‌های نظری و تساهل تأکید می‌شود.

توصیف محیط امنیتی در فضای مجازی

برای اینکه بتوانیم درک درستی از وضعیت آیندهٔ امنیت ملی داشته باشیم، لازم است ماهیت فضای مجازی و محیط امنیتی و راهبردی مترتب بر آن را بهتر بشناسیم. در این فضا، سرعت اطلاعاتی که ممکن است منتقل، کنترل و تفسیر شود، به‌گونهٔ چشمگیری افزایش می‌یابد؛ همچنین گردش اطلاعات را در درون، بیرون و بین سازمان‌ها و دیگر بازیگران ملی و فراملی افزایش می‌دهد. ظرفیت انتقال اطلاعات نیز به‌گونهٔ چشمگیری فزونی می‌یابد. به این ترتیب، توانایی انتقال و تفسیر مقادیر بیشتر اطلاعات سبب می‌شود تصمیم‌گیرندگان تصویر مطلوبی از

1. Keohane
2. Nye
3. Soft Power

جهان، خود و دیگران به‌دست آورند تا براساس آن تصمیم‌گیری کنند. فناوری عصر اطلاعات، انعطاف‌پذیری گردش اطلاعات را افزایش خواهد داد و بازیگران می‌توانند به‌سراغ منابع گوناگون اطلاعات بروند و اطلاعات مورد نیاز خویش را تأمین کنند.

فناوری اطلاعات به‌دلیل ارزانی و دسترس‌پذیری، توانمندی شایان توجهی برای فقیرترین کشورها و بازیگران منطقه‌ای و جهانی فراهم می‌کند که ممکن است برای به‌چالش کشیدن و تهدید دیگران استفاده شود. در عصر اطلاعات، افزون بر دولت‌ها، شرکت‌های چندملیتی، سازمان‌های غیردولتی، گروه‌های جنایی و تروریست‌ها و حتی افراد ممکن است به جنگ اطلاعاتی و تخریبی اقدام کنند. فناوری اطلاعات، توانایی بازیگران را در زمینه فرماندهی، کنترل و برقراری ارتباط با نیروهای تحت امر خویش افزایش می‌دهد؛ همین‌طور به جمع‌آوری اطلاعات دقیق دربارهٔ اهداف، توانمندی‌ها و عملکردهای دشمنان بالقوه و بالفعل کمک می‌کند. از نظر داخلی، فناوری اطلاعات در ایجاد توانمندی‌های دفاعی، اقتصادی و سیاسی به دولت‌ها کمک می‌کند.

در محیط امنیتی جدید، افزایش سرعت، توانمندی و انعطاف‌پذیری گردش اطلاعات سبب کنترل دشوار دولت‌ها بر ورود و خروج اطلاعات می‌شود. برخی از دولت‌ها سعی می‌کنند دسترسی آزاد به اطلاعات را کنترل کنند (سلطانی‌نژاد: ۱۳۸۶)؛ این کشورها بر گردش اطلاعات کنترل دارند، اما زیان اقتصادی و اجتماعی دیگری را مانند باقی ماندن در سطح پایین توسعه‌یافتگی متحمل می‌شوند (آلبرتس، ۱۳۸۵: ۵۳). افزایش تأثیر فضای مجازی بر فناوری‌های نظامی موجب شده است که دولت‌های متوسط و حتی گروه‌های شبه‌نظامی، به سلاح‌هایی دسترسی پیدا کنند که آنها را قادر می‌سازد در جنگی نامتقارن به مقابله با قدرت‌های پیشرفتهٔ نظامی برخیزند. توانایی کشورهای فقیر برای آغاز جنگ علیه کشورهای قوی، ویژگی عصر اطلاعات است که هرچند برخی تحلیل‌گران نظامی به آن اشاره کرده‌اند، به‌طور گسترده دربارهٔ آن بحث نشده است (راجرز، ۱۳۸۴: ۲۴۰). اینترنت به‌سرعت وارد محفل‌های علمی، دانشگاهی، مؤسسه‌های تجاری و اقتصادی و جوامع در سطح جهانی شده است. اهمیت این دگرگونی در تاریخ بشری بی‌سابقه است؛ از هم‌اکنون می‌توان تأثیر ژرف آن را بر همهٔ جنبه‌های تمدن دید و این تغییرات ادامه دارد. یکی از زمینه‌هایی که دستخوش دگرگونی اساسی شده است، جمع‌آوری و استفاده از اطلاعات است. قابلیت و خصوصیت منحصربه‌فرد اینترنت به‌گونه‌ای است که خلافکاران، تروریست‌ها و به‌ویژه دستگاه‌های اطلاعاتی کشورهای بزرگ، از شبکهٔ جهانی اینترنت برای مقاصد مختلف بهره می‌گیرند. این بازیگران سازمانی و عدهٔ زیادی از افراد به‌مثابهٔ دلالان اطلاعات[1] از اینترنت برای ارتکاب جرم جاسوسی به‌شیوهٔ جدید، یعنی

1. Information brokers

جاسوسی از راه شبکه‌های رایانه‌ای استفاده می‌کنند (بونی،۱۳۸۶: ۳۴). اینترنت چنان گسترده است که یک دولت واحد نمی‌تواند آن را به‌راحتی کنترل کند. اینترنت از راه ایجاد منطقهٔ اقتصادی جهانی یکپارچه و ضد حاکمیت کشورها و قانون‌پذیری، اقتدار و حاکمیت کشورهای مستقل را با مشکل روبه‌رو می‌کند. در جهان امروز، ارتباطات و تبادل اطلاعات ممکن است برتری سیاسی، اقتصادی یا نظامی را به‌ارمغان آورد و برعکس، فقدان آن ممکن است نقایص و مشکلاتی را ایجاد کند. قدرت نظامی کشورها تا حدود زیادی تحت تأثیر قدرت اقتصادی آنهاست؛ قدرت اقتصادی هم به قدرت شرکت‌ها و مؤسسه‌های تجاری بستگی دارد که امروزه این قدرت، بیش از آنکه با تولید انبوه محصولات و کالاها اندازه‌گیری شود، با حجم داده‌ها و قدرت ارتباطی آنها اندازه‌گیری می‌شود. امکان دسترسی به اطلاعات، خطرهای جدیدی را برای نهادهای تجاری و دولتی به‌وجود آورده؛ به این ترتیب موضوع‌های امنیتی جدید یا بی‌سابقه‌ای ظهور پیدا کرده است.

نیروهای اجتماعی، یعنی گروه‌های شهروندی و سازمان‌های غیردولتی (N.G.O) که در نقاط مختلف جهان گسترده‌اند و پیوسته بر حجم گستردگی آنها افزوده می‌شود، گردانندهٔ اطلاعات شبکه‌ای هستند که از راه اینترنت عمل می‌کند. در حال حاضر، شبکه‌های رایانه‌ای گردآورنده و توزیع‌کنندهٔ اصلی اخبار و اطلاعات و تدوین‌کنندهٔ راهبردها در حرکت‌ها و جنبش‌های مختلف و ترسیم‌کنندهٔ اهداف و راهبردها در میان اعضای جنبش و سازمان‌های غیردولتی پراکنده در نقاط مختلف هر کشوری‌اند.

بنابراین محیط امنیتی و راهبردی نو، پیچیده‌تر از محیط امنیتی کنونی خواهد بود؛ به‌طوری که این فناوری‌ها در عرصه‌های سیاسی، اقتصادی، نظامی، اجتماعی، فرهنگی و ارزشی نمود پیدا خواهد کرد. در این شرایط، کشورهایی که خود را با دگرگونی‌ها سازگار کنند و از دگرگونی‌ها آگاه باشند، پیشرفت خواهند کرد؛ اما کشوری که این‌گونه رفتار نکند، مجبور است به این وضعیت نو تن دردهد و درنتیجه، قدرت انتخاب و اثرگذاری خود را از دست می‌دهد. به این ترتیب، لازم است برنامه‌ریزان و استراتژیست‌های امنیت ملی، حتی در شرایط عدم درک کامل از محیط امنیتی و راهبردی نوظهور، راهبردها و راهکارهای تأمین امنیت در فضای مجازی را تدوین و تبیین کنند.

مفهوم امنیت ملی در فضای مجازی

در نظر همهٔ بازیگران ملی در نظام بین‌الملل، امنیت ملی واقعیتی کلیدی و شاید حتی نخستین علت وجودی و مهم‌ترین هدف نهایی آنها باشد. امنیت ملی، مفهوم سیال و شناوری دارد؛ اما ارزیابی عملکرد هر حکومت، دیدگاهش دربارهٔ امنیت ملی را مشخص می‌کند.

استقرار امنیت ملی به‌منظور دستیابی به چهار هدف صورت می‌گیرد:

۱. برقراری امنیت و حفاظت از شهروندان و دولت در مقابل حمله‌های فیزیکی ناشی از منابع خارجی؛

۲. ایجاد رونق اقتصادی و تأمین رفاه برای شهروندان؛

۳. حفظ اموال و ارزش‌های حاکم بر جامعه؛

۴. بهبود هنجارها، سنت‌ها و روش‌های متداول زندگی و حفظ آنها.

ثروت، جغرافیا، نیروی نظامی، زیرساخت‌های حمل‌ونقل، نظام‌های ائتلاف و اتحاد، توانمندی‌های صنعتی و سطوح تعلیم و تربیت از مهم‌ترین عناصر محسوس، عینی و قابل اندازه‌گیری برای دستیابی به اهداف ملی دولت‌هاست. راهبرد ملی، توانمندی‌های سازمانی، دانش علمی و فنی، اصول و ارزش‌های حاکم بر جامعه، توان رهبری و اراده و روحیهٔ ملی ازجمله عوامل نامحسوس و ذهنی، از دیگر عواملی است که اندازه‌گیری آنها دشوار است (آلبرتس، ۱۳۸۵: ۲۰). با ورود به عصر اطلاعات، اهمیت عناصر نامحسوس و ذهنی قدرت، همانند دانش، نسبت به عوامل محسوس و سنتی قدرت به‌طور چشمگیری رو به افزایش است. هر نوع امنیتی نسبی است. امنیت بیش از آنکه واقعیتی بیرونی باشد، ماهیتی ذهنی و گفتمانی دارد. مفهوم امنیت، تنها در رابطهٔ همنشینی یا جانشینی با مفهوم‌های دیگری همچون قدرت، منافع، اهداف، مصالح، تهدیدها و ... که همگی مفهوم‌های مبهم و سیالی‌اند، مصداق یا مصداق‌های خود را می‌یابد (تاجیک، ۱۳۸۱: ۹). افزون بر مشکل مفهومی، در شرایط کنونی، نخبگان تصمیم‌ساز در وضعیتی متناقض و چندلایه و در محیطی بدیع، مفهومی و پیچیدهٔ نظری و عملی قرار گرفته‌اند. در حالی که می‌خواهیم تهدیدهای امنیتی خود را در دنیایی واقعی جست‌وجو کنیم، متغیرهای جدید از سویی دیگر، دست اندرکار معماری دنیایی مجازی شده‌اند.

هر پدیدهٔ امنیتی با تهدیدها و فرصت‌هایی قرین بوده، پیچیده و چندچهره است و نمی‌توان برای آن هویتی شفاف ترسیم کرد و به نتیجه و پیامد مشخص و معینی امید داشت. در رویکرد و تعریفی عملیاتی، نمی‌توان بدون اشارهٔ صریح یا ضمنی به انگارهٔ تهدید، امنیت را تعریف کرد (آزر، ۱۳۷۹: ۳۴۲). با اینکه ماهیت پیچیدهٔ امنیت اجازهٔ پیشنهاد و تعریف پذیرفته‌شدهٔ عمومی و قابل اجماع را در این عرصه نمی‌دهد، به‌تعبیر بوزان تلاش برای روشن کردن اهداف سیاست امنیتی ایجاب می‌کند که تعریفی از مفهوم امنیت به‌دست دهیم:

«امنیت ملی در بعد عینی، فقدان تهدیدات نسبت به ارزش‌ها، منافع و اهداف و در جهت ذهنی، فقدان ترس از اینکه این بنیان‌های ملی (ارزش‌ها، منافع و اهداف) مورد هجوم (فیزیکی و غیرفیزیکی) واقع بشوند را مورد سنجش قرار می‌دهد» (تاجیک، ۱۳۸۱: ۴۷).

ازجمله تهدیدهای امنیتی که ممکن است اینترنت در آنها تأثیر بسزایی داشته باشد، می‌توان به محورهای زیر اشاره کرد:

– اقدام‌های مخل امنیت و برانداز گروه‌های مسلح و غیرمسلح؛

– گسترش نابسامانی‌های اجتماعی ازقبیل مواد مخدر، فساد اخلاقی، جرایم اجتماعی، سرقت و ...؛

– شکاف بین اقلیت‌های قومی، مذهبی و زبانی با نظام و افزایش گرایش‌های تجزیه‌طلبانهٔ قومی (تاجیک، ۱۳۸۱: ۴۷-۱۹۳)؛

– اقدام‌های تروریستی، خرابکاری و هکتیویسم؛

–آماده‌سازی افکار عمومی جهان علیه جمهوری اسلامی ایران در زمینهٔ پروندهٔ هسته‌ای و تشدید اقدام‌ها و تحریم‌ها علیه ایران؛

– اقدام سرویس‌های اطلاعاتی بیگانه به عملیات جاسوسی اینترنتی علیه جمهوری اسلامی ایران.

بنابراین، در عصر اطلاعات موضوع‌ها و مسئله‌های متنوع‌تری نسبت به گذشته مسائل امنیت ملی تلقی می‌شود. در این عصر، گردش آزاد اطلاعات در سراسر جهان که از راه اینترنت صورت می‌گیرد، موضوع امنیت اطلاعات را تا سطح مسائل امنیت ملی بالا می‌برد و درنتیجه، تعریف امنیت ملی بسط و گسترش می‌یابد.

اینترنت و تهدیدهای فرهنگی- سیاسی

امروزه با توجه به گستردگی اینترنت، بررسی نحوه و مقدار اثرگذاری آن بر امنیت فرهنگی و سیاسی کشور ضروری است. در حال حاضر، تبلیغات سیاسی شدیدی در اینترنت بر ضد جمهوری اسلامی ایران انجام می‌گیرد. با مراجعهٔ گذرا به یک صفحهٔ وب مانند (www.gooya.com) می‌توان به نشانی اینترنتی دست‌کم چهل گروه ایرانی مخالف تا برانداز نظام و برخی سازمان‌های فمینیستی، قوم‌مدار، نشریه‌های ضد حکومت دینی و چندین انجمن تبلیغات دینی غیراسلامی دسترسی یافت. می‌توان گفت اینترنت، ارزان‌ترین، سریع‌ترین، جذاب‌ترین و شخصی‌ترین امکان عملیات روانی را برای مخالفان سیاسی و اعتقادی جمهوری اسلامی ایران فراهم آورده است که در ادامه تلاش می‌شود برخی جنبه‌های آن تشریح شود.

اینترنت هم نیاز به سواد و مهارتی خاص دارد و هم الگوهای فرهنگی و رفتاری ویژه‌ای را به‌دنبال می‌آورد؛ مهم‌ترین مسائل اینترنت از لحاظ فرهنگی، عدم تطابق محتوای عرضه‌شده با الگوهای فرهنگی و هنجارهای رفتاری جوامع مختلف است. فناوری اینترنت برای بیشترین سرعت و کمترین کنترل طراحی شده است؛ بنابراین اعمال کنترل‌های اخلاقی در آن دشوار

است (آشنا، ۱۳۸۲: ۲). دیگر مشکل فرهنگی اینترنت، غلبهٔ زبان انگلیسی و فقدان منابع غنی با زبان‌های دیگر است؛ درنتیجه سلطهٔ زبان انگلیسی بر زبان‌های دیگر به‌وسیلهٔ اینترنت تقویت می‌شود. بنا بر نظر عده‌ای از اندیشمندان، جریان بین‌المللی اطلاعات جریانی مرکز- پیرامونی از شمال و غرب به‌سوی جنوب و شرق است؛ از کشورهای توسعه‌یافته به‌سوی کشورهای در حال توسعه. این جریان یکسویه، عمودی، تحقیرگرا، منفی‌گرا و سلطه‌جویانه است (مولانا، ۱۳۷۱: ۶۶-۶۰).

پرسش مهم این است که ورود وسایل ارتباطی و دیجیتالی به جوامع در حال توسعه چه تغییری ایجاد خواهد کرد؟ آیا سبب سست شدن بیشتر هویت‌ها می‌شود یا آنکه به خلق هویت‌های نو یاری می‌رساند که بحران هویت را در این کشورها تخفیف دهد؟ بی‌شک، این پرسش پاسخ قطعی و یک‌جانبه‌ای ندارد. شرایط هر جامعه فرق می‌کند و نمی‌توان به صدور احکام مطلق در این زمینه بسنده کرد. افزون بر آن، تدبیر مدیران جامعه، پویایی فرهنگ عمومی و ساختار اقتصادی نیز در تعیین نوع پاسخ لازم دخالت دارد و شدت و ضعف این عوامل، هر کدام اثرگذار است (معینی علمداری، ۱۳۸۴: ۱۱۷). پندارگرایی و گرفتار آمدن در چنبرهٔ امور مجازی و عدم توانایی در ایجاد ارتباط با واقعیت، بحران‌زاست. این دوگانگی ذهن و عین در جهان سوم، آثار منفی سیاسی و فرهنگی به‌همراه می‌آورد. در این میان، اینترنت جایگاه و عملکرد حساسی دارد؛ به‌طوری که تضعیف خطوط قدیمی هویت‌ها به‌وسیله اینترنت، در تشدید بحران در این جوامع مؤثر است.

اینترنت مانند دیگر فناوری‌های جدید در جوامع در حال توسعه به‌صورت کاملاً تعریف‌شده به‌کار گرفته نمی‌شود و این جوامع از نظر بهره‌برداری از اینترنت، در موقعیت حاشیه‌ای قرار دارند. در این جوامع، جذب فناوری‌های جدید، ازجمله اینترنت، به‌نحوی کاملاً پراکنده و برنامه‌ریزی‌نشده صورت می‌گیرد. در بسیاری از کشورهای در حال توسعه، اینترنت سوء کارکرد دارد و به‌شکل حاشیه‌ای و وسیله‌ای برای سرگرمی است و آن‌گونه که باید، به‌عنوان وسیلهٔ اطلاعاتی استفاده نمی‌شود. درنتیجه، با وجود رشد کمّی شایان توجه عدهٔ کاربران اینترنتی، تحول ساختاری در این زمینه مشاهده نمی‌شود. بسیاری از صاحب‌نظران، فقدان راهبرد و جهت‌گیری روشن، واقع‌بینانه و منطبق با رویکردهای علمی را یکی از مشکلات اصلی جمهوری اسلامی ایران، در مواجهه با اینترنت می‌دانند. در سالیان اخیر، همزمان با ایجاد خلل در انتشار و اشاعهٔ ارزش‌ها، قشرهای مختلف جامعه به‌خصوص جوانان، گروه‌های هدفی هستند که در معرض پیام‌ها و ارزش‌هایی قرار گرفته‌اند که بیگانگان منتشر می‌کنند و اینترنت این فرایند را تسهیل و تسریع کرده است. جامعهٔ جوان ما در مقاطعی احساس فقدان ارزش کرده و از این‌روی، تلاش کرده است این نقصان را با وامگیری از

دیگران و با ابزاری مانند اینترنت مرتفع کند (تاجیک، ۱۳۸۱: ۱۶۰). رواج اینترنت در جوامع در حال توسعه، وضعیتی را پدید آورده است که از آن با نام سوپرمارکت فرهنگی یاد می‌شود. به‌عبارت دیگر، وسایل ارتباط دیجیتالی در جهان سوم با سوپرمارکت قابل مقایسه است؛ همان‌طور که شخص در سوپرمارکت، چرخ‌دستی خود را مملو از انواع کالاها می‌کند، شبکه‌های اینترنتی بسته‌های مختلفی شامل انواع ارزش‌ها و گرایش‌های فرهنگی را به مشتریان عرضه می‌کنند (معینی علمداری، ۱۳۸۴: ۱۱۸).

تارنمای خدمت در تاریخ ۹ دی ۱۳۸۶ گزارش می‌دهد همایشی با عنوان اینترنت در ایران و زوایای مختلف آن در دانشگاه تل‌آویو در فلسطین اشغالی برگزار شده است. در این همایش، دربارهٔ جایگاه اینترنت در جامعهٔ امروز و نبرد اینترنتی بحث و تبادل نظر شده است. جایگاه وبلاگ‌نویسی در ایران و تأثیر اینترنت بر موسیقی رپ و به‌وجود آمدن موسیقی‌های دیگر و گروه‌های تقلیدکننده از فرهنگ غرب در ایران از دیگر محورهای مورد علاقهٔ صهیونیست‌ها دربارهٔ اینترنت در ایران بود!!!

گروه‌های اپوزیسیون با تکیهٔ روزافزون بر شبکه‌های رایانه‌ای، از نظر بهره‌گیری از فناوری پیشرفته، مهارت روزافزونی پیدا کرده‌اند. از سوی دیگر، هکرها سیاسی‌تر شده و خود را درگیر مسائل اجتماعی و سیاسی کرده‌اند. به این نیروهای اجتماعی مرکب، به‌طور کلی، شبکه‌های شهروندی گفته می‌شود (وارک، ۱۳۸۴: ۲۸۷). اینترنت در هماهنگ‌سازی راهبردهای مبارزهٔ شبکه‌های شهروندی تأثیر بسزایی دارد. تبادل اطلاعات راهبردی و سازماندهی و اطلاع‌رسانی، همواره یکی از مشخصات بارز تارنماهای شبکه‌های شهروندی بوده است. این گروه‌ها از اینترنت به‌مثابهٔ ابزاری کارساز برای برنامه‌ریزی و تحریک اعتراض مردمی بهره‌برداری می‌کنند.

درمجموع، باید گفت گرچه انقلاب اطلاعات و رسانه‌های نو تا حدودی به افزایش قدرت کشورهای کوچک کمک می‌کنند، جوزف نای معتقد است تأثیر آن بر افزایش قدرت کشورهای بزرگ، بسیار بیشتر است؛ زیرا جمع‌آوری و تهیهٔ اطلاعات جدید، اغلب مستلزم سرمایهٔ سنگینی است. کشورهایی مانند آمریکا، انگلستان و فرانسه دارای توان زیادی در زمینهٔ جمع‌آوری و تهیهٔ اطلاعات‌اند که کشورهای دیگر را تحت‌الشعاع قرار می‌دهد. از سوی دیگر، کشورهای پیشرو اغلب ایجادکنندگان معیارها و اساس سامانه‌های اطلاعاتی‌اند. به‌کارگیری زبان انگلیسی در اینترنت، نمونهٔ بسیار خوبی برای این موضوع است (نای، ۲۰۰۷).

اینترنت و تهدیدهای امنیتی (تروریسم و خرابکاری)

تروریسم یکی از موانع اساسی بشر در راه رسیدن به آرامش است و لذت دستیابی به علم و فناوری‌های جدید را به کمترین حد می‌رساند و تا زمانی که اخلاق نتواند خود را در نهادهای

اثرگذار به‌مثابهٔ واقعیتی لازم و ضروری، پایدار سازد، این نگرانی بیشتر خواهد شد. دیگر نمی‌توان تروریسم را تهدیدی داخلی تلقی کرد و از جنبهٔ بین‌المللی آن غافل ماند؛ امروزه تروریسم، تهدیدی بین‌المللی و علیه کل بشریت است و تمام جوامع را در برگرفته است. امروزه تروریست‌ها همگام با پیشرفت فناوری اطلاعات و بدون احساس تعهد نسبت به قوانین و اصول آن، رشد کرده و پیش آمده‌اند. تروریست‌ها تحت تأثیر فضای مجازی به بازیگرانی بین‌المللی تبدیل شده‌اند و می‌توانند به‌طور تقریبی، در هر کجا که بخواهند اقدام‌های تروریستی و خرابکارانهٔ خود را اجرا کنند؛ بنابراین هیچ منطقه، ملت یا دولتی ازجمله جمهوری اسلامی ایران، از اقدام‌های آنها مصون نمی‌ماند.

تعریفی که می‌توان از تروریسم با تأکید بر تروریسم اینترنتی به‌دست داد، عبارت است از: اقدام‌های برنامه‌ریزی‌شده و هدفمند همراه با اغراض سیاسی و غیرشخصی، علیه رایانه‌ها و امکانات و داده‌های ذخیره‌شده در درون آنها از راه شبکهٔ جهانی و هدف از چنین اقدامی، نابودی آنها یا وارد آوردن آسیب‌های جدی به آنهاست (تارنمای جامعهٔ اطلاعاتی). بی‌شک یکی از پیچیده‌ترین ابزارهایی که تاکنون از آن برای اهداف تروریستی بهره برده شده، اینترنت است. تنها در دنیای اینترنت است که تروریست‌ها می‌توانند با هزاران نام مجازی و بدون اینکه ردی از خود بر جای گذارند، به خشونت و امیال خود بپردازند. در فضای مجازی، سه شیوهٔ فعالیت برای بازیگران غیردولتی قابل تصور است: اکتیویسم[1]، هکتیویسم[2] و سایبرتروریسم[3]. هرچند مرزبندی بین این سه شیوهٔ فعالیت گاهی مبهم است، برای تشریح و توضیح اهداف و چگونگی اقدام‌های گروه‌های تروریستی، مفید است. اکتیویسم به استفادهٔ معمول و غیرمختل‌کننده از اینترنت اشاره دارد که در حمایت و پشتیبانی از منظور خاصی باشد؛ مانند گشت زدن در شبکهٔ جهانی برای کسب اطلاعات، ایجاد و ساخت وب‌سایت و ارسال موضوع و مطلب از راه آن، مباحثه دربارهٔ موضوع و مطلب خاص، ائتلاف‌های مجازی، برنامه‌ریزی و ایجاد هماهنگی در اقدام‌های مورد نظر. هکتیوسیم، یکپارچه کردن عمل هک کردن و عمل‌گرایی است؛ برای نمونه عملیات‌ها و اقدام‌هایی با استفاده از شگردهای هک کردن برای حمله به سایتی اینترنتی با هدف ایجاد اخلال در آن بدون وارد آوردن آسیب جدی؛ مانند اعتراض‌های خاموش، انسدادهای مجازی، بمب‌های خودکار ارسالی به رایانامه‌ها، ویروس‌ها و کرم‌های رایانه‌ای. سایبرتروریسم عبارت است از تقارب و همگرایی میان فضای مجازی و فعالیت تروریستی؛ برای نمونه اقدام به هک کردن و کاربرد آگاهانهٔ آن با هدف وارد آوردن آسیب‌های جدی همچون کشتار یا وارد آوردن خسارت‌های اقتصادی شدید.

1. Activism
2. Hactivisim
3. Cyber Terrorism

نگرانی و ترس از اینکه گروه‌ها یا افرادی در حوزهٔ الکترونیک و مجازی ملت یا کشوری وارد شوند و به سامانه‌های امنیتی، دفاعی، حمل‌ونقل، خطوط هوایی، سدها، انتقال انرژی، مبادله‌های تجاری و اقتصادی و غیره، آسیب جدی وارد کرده، آن را مختل کنند، همه و همه با پدیدهٔ شناخته‌شدهٔ سایبرتروریسم در ارتباط‌اند (Carleton University, 2006). در میان سه شیوهٔ فعالیت یادشده که بیان‌کنندهٔ دگرگونی در ماهیت تروریسم است، نگرانی اصلی و عمده مربوط به عواقب و نتایج آسیب‌های حمله‌های الکترونیکی موفقیت‌آمیز است.

ساختار شبکه‌ای رایانه و به‌ویژه اینترنت، قابل مقایسه با ساختار گروه‌های تروریستی است؛ یعنی ساختار غیرمتمرکز و غیرسلسله‌مراتبی (آلبرتس، ۱۳۸۵: ۱۸۲). گروه‌های تروریستی متشکل از سازمان‌های مختلف‌اند که منابع و تجربهٔ خود را با هم مبادله می‌کنند. شبکهٔ تروریستی، بی‌شکل و نامنسجم است و دارای هیچ‌گونه مرکزیت یا فرماندهی مشخص سازمان‌های متعارف نیست. گروه‌های یادشده هر زمان که بخواهند از راه اینترنت، خود را به شبکهٔ تروریستی متصل کرده، در دیگر موارد مستقل عمل می‌کنند.

تروریست‌های سایبر، فاقد جایگاه جغرافیایی معینی بوده، نیاز چندانی هم به در دسترس قرار دادن موقعیت خود ندارند؛ بنابراین می‌توانند از موقعیت‌های نامشخص اقدام به حمله کنند. این‌گونه حمله‌ها با هزینه و عدهٔ کمتری انجام می‌گیرد؛ اما صدمه‌های بزرگی به شرکت‌های تجاری و اقتصادی و زیرساخت‌های کشور وارد می‌کنند. استفاده از اینترنت به‌منظور ایجاد رعب و وحشت از راه پیام‌های تهدیدآمیز و پخش تصویرها و فیلم‌های رعب‌آور، مانند صحنهٔ اعدام گروگان‌ها، از اقدام‌های گروه‌های تروریستی است که در قالب جنگ روانی در حال اجراست.

از راه نفوذ و جاسوسی شبکه‌ای، تروریست‌ها به اطلاعات ارزشمندی دربارهٔ سامانه‌های دفاعی کشور هدف، زیرساخت‌های حمل‌ونقل و انتقال انرژی، بندرها و پالایشگاه‌ها، امور اقتصادی و تجاری و همین‌طور برنامه‌های ضد تروریستی دستگاه‌های امنیتی، دست پیدا می‌کنند که به آنها در طراحی و عملیات و شناخت نقاط آسیب‌پذیر کشور هدف کمک می‌کند. نکتهٔ مهم اینجاست که در بسیاری از موارد، تروریست‌ها می‌توانند از راه جمع‌آوری آشکار اطلاعات و تجزیه و تحلیل آن به مقاصد خود دست یابند. «با استفادهٔ آشکار از اطلاعات موجود و بدون استفاده از روش‌های غیرقانونی و پنهانی، این امکان وجود دارد که حداقل هشتاد درصد تمامی اطلاعات مورد نیاز دربارهٔ دشمن را جمع‌آوری کرد.» این جمله‌ها، سخنان تحلیل‌گران اطلاعاتی و امنیتی نیست، بلکه جمله‌هایی برگرفته از دفترچهٔ راهنمای آموزشی القاعده است که در ژانویهٔ ۲۰۰۳ در افغانستان به‌دست آمده است (آلبرتس، ۱۳۸۵).

حادثهٔ ۱۱ سپتامبر ۲۰۰۱، شاید گویاترین نمونه از رابطی به‌نام اینترنت برای طراحی، هماهنگی، سازماندهی و اجرای عملیات باشد. پس از این حادثه، سایبرتروریسم شکلی متفاوت به‌خود گرفت و مسئلهٔ «آسیب‌پذیری از درون بدون تعرض موشکی از بیرون» مطرح و موضوعیت یافت (روحانی، ۱۳۸۰)؛ به‌طوری که نمایندگان جمهوریخواه کنگرهٔ آمریکا، در بیانیهٔ خود اعلام کردند تنها فشار دادن چند کلید صفحه‌کلید و یک ارتباط اینترنتی برای ویرانی اقتصاد و به‌خطر انداختن زندگی مردم کافی است و یک موشواره ممکن است به اندازهٔ یک بمب، خطرناک باشد؛ در حال حاضر، بیشتر حکومت‌های پیشرفته و دولت‌های صاحب قدرت، در برابر سایبرتروریسم راهبردهای عمده‌ای در دنیای مجازی اتخاذ کرده و گروه‌های امنیتی را برای مبارزه با این پدیده به‌خدمت گرفته‌اند.

آسیب‌رسانی به کشور، به‌ویژه از راه اینترنت، امری واقعی و شدنی است؛ این قابلیت در حد نگران‌کننده‌ای رو به فزونی است و ما در رویارویی با آن، وسیلهٔ دفاعی چندانی نداریم. این واقعیت که بسیاری از رایانه‌های دولتی و شخصی به‌هم متصل‌اند، چنین به ذهن متبادر می‌کند که عده‌ای اندک با حمله‌های هماهنگ می‌توانند فعالیت‌های نظامی و کشوری گسترده‌ای را مختل کنند.

خرابکاران و مجرمان بین‌المللی، مانند باندهای جرایم سازمان‌یافتهٔ خطرناک، قاچاقچیان مواد مخدر، کلاهبرداران مالی و غیره نیز از اینترنت برای تسهیل رفتارهای مجرمانهٔ خود استفاده می‌کنند. مجرمان، نهادهای مالی را تهدید کرده‌اند که در صورت عدم برآوردن خواسته‌هایشان، سامانه‌های حیاتی رایانه‌ای آنها را از کار خواهند انداخت. این باندهای جنایی که در مکان‌های ناشناسی فعالیت می‌کنند، تهدیدهای رمزگذاری‌شده به تجهیزات بسیار حساس رایانه‌ای مورد نظرشان می‌فرستند و چیزی شبیه این می‌گویند: «اکنون آیا باور می‌کنید که ما می‌توانیم رایانهٔ شما را نابود کنیم؟» (آلبرتس، ۱۳۸۵: ۱۸۶).

اینترنت و عملیات جاسوسی

عملیات جاسوسی علیه کشور، ازجمله تهدیدهای امنیتی به‌شمار می‌رود؛ اما به‌دلیل اهمیت و گستردگی موضوع و آسیب‌های جدی که از این ناحیه، کشور را تهدید می‌کند، این موضوع به‌صورت مستقل بررسی می‌شود.

ازآنجاکه در دنیای کنونی دانش، اطلاعات حساس و طبقه‌بندی‌شده بخش مهمی از ارزش و دارایی شرکت‌ها، سازمان‌ها و نهادهای خصوصی و دولتی را تشکیل می‌دهد، شاه‌راه عبوری این اطلاعات که به‌صورت داده‌هایی الکترونیکی است، نزد بازیگران فروملی و فراملی از اهمیت شایان توجهی برخوردار است. این شاهراه اطلاعاتی یا اینترنت، امروزه نقش بارزی در

کسب، حفظ و مهار قدرت در رقابت با حریفان و دیگر بازیگران دارد و این وضعیت، جاسوسی اینترنتی را به‌مثابهٔ ابزاری مهم برای پیروزی در این رقابت مطرح می‌سازد:

امروزه شرکت‌ها و مؤسسه‌های تجاری و نهادهای دولتی برای انجام دادن فعالیت‌های خود، ناگزیر از تکیه به اینترنت‌اند؛ به‌طوری که بدون آن، فعالیت روزمرهٔ آنها مختل می‌شود. ذخیره‌سازی، پردازش و انتقال اطلاعات حساس، حیاتی، اختصاصی، امنیت ملی و تجاری و غیره به‌صورت مستمر در حال انجام گرفتن است. وسایل و ابزار انتقال این اطلاعات، هدف خوبی برای عوامل جاسوسی شبکه‌ای است. عوامل جاسوسی شبکه‌ای می‌توانند به اطلاعات صدمه بزنند، آنها را نابود، دستکاری یا تغییر دهند؛ در حالی که در ظاهر به‌نظر می‌رسد که این اطلاعات به‌صورت اصلی و اولیه‌اند. اطلاعات را می‌توان از منابع ذخیره‌سازی الکترونیکی آن سرقت یا نسخه‌برداری کرد و با سرعت نور به هر نقطه از جهان منتقل کرد.

عوامل جاسوسی اینترنتی، هر روز پیشرفته‌تر و مجهزتر می‌شوند و آسیب‌پذیری نرم‌افزارها و نفوذپذیری آنها را به‌راحتی کشف می‌کنند. در اینترنت، محدودیت‌های مربوط به عنصر زمان و مکان، معنا ندارد؛ بنابراین اینترنت فضایی به‌نسبت آرمانی را برای جاسوسان شبکه‌ای به‌وجود آورده است. یافتن مرکز رایانه‌ای در آن سوی دنیا به راحتی یافتن شمارهٔ تلفنی در دفترچهٔ تلفن است. جاسوسان اینترنتی این توانایی را دارند که به‌سادگی اهداف خود را شناسایی کرده، به آن حمله کنند. اینترنت، فاصله، مرز و زبان نمی‌شناسد. در دنیای کنونی، به‌اندازه‌ای که نحوهٔ ارتباطات دچار تغییر اساسی شده، نحوهٔ جرایم رایانه‌ای و جاسوسی شبکه‌ای نیز دستخوش دگرگونی شده است. جاسوسان شبکه‌ای و تحلیل‌گران اطلاعاتی رقیب که همیشه منتظر فرصت‌اند، می‌توانند از راه شبکهٔ اینترنت به اطلاعات حساس دسترسی پیدا کنند. محتوای هر رایانامه ممکن است حاوی برنامه‌های راهبردی اقتصادی، تجاری یا امنیتی باشد و این اسرار را می‌توان در لحظه‌ای از یک سوی دنیا به سوی دیگر ارسال کرد. جاسوسان شبکه‌ای، تغییر چندانی در اهداف خود نداده‌اند؛ آنچه به‌راستی جدید است، فضایی است که آنها در آن عمل می‌کنند. اینترنت، آنها را راحت‌تر و سریع‌تر به اهداف خود می‌رساند و به عوامل جاسوسی شبکه‌ای، امکان نقل و انتقال جهانی می‌دهد و آنها می‌توانند در کوتاه‌ترین زمان اقدام کنند؛ بدون اینکه در چنگ قانون گرفتار شوند. عواملی چون مکان جغرافیایی، زمان و کنترل‌های مرسوم، دیگر محدودکننده نیستند.

وقتی نوجوانی می‌تواند در سامانه‌های رایانه‌ای و پایگاه‌های اینترنتی نفوذ کرده، به آنها خسارت وارد کند، تصور کنید که عامل جاسوسی شبکه‌ای که از آموزش و قابلیت‌های زیادی برخوردار است و از سوی سازمان یا نهادی ملی یا بین‌المللی حمایت می‌شود، تا چه اندازه

می‌تواند به این‌گونه اقدام‌ها دست بزند؛ ضمن اینکه خسارت ناشی از جاسوسی شبکه‌ای بسیار بیشتر از سرقت فیزیکی است.

به‌طور معمول، مدیران سازمان‌ها، نهادها و شرکت‌ها باور ندارند که اطلاعات ارزشمندی وجود دارد که به دزدیده شدن می‌ارزند. مجموع فعالیت سازمان‌ها، نهادها و شرکت‌ها بر کل قدرت اقتصادی و دفاعی کشور تأثیر دارد و اگر آنها در معرض جاسوسی قرار گیرند، اقتصاد و امنیت کشور تضعیف می‌شود.

ممکن است نقطهٔ آغاز جاسوسی اقتصادی اینترنتی، جمع‌آوری اطلاعات آشکار از پایگاه اینترنتی سازمان‌ها و شرکت‌های تجاری و صنعتی باشد؛ جالب توجه اینکه اغلب اطلاعات حساس، بر روی پایگاه‌های اینترنتی این سازمان‌ها و شرکت‌ها یافت می‌شود؛ در حالی که مدیران آنها متوجه نیستند که این اطلاعات چه اندازه برای رقیبان ارزشمند است. امتیاز دیگر اینترنت، استفاده از قابلیت‌های آرمانی آن برای انتقال اطلاعات بین عامل جاسوسی و سازمان متبوع وی است؛ زمانی که جاسوس، اطلاعات مورد نظر را دریافت کرد، می‌تواند آن را به رایانامه‌ای پیوست کند یا آن را در لوح فشرده‌ای ذخیره کند و پوشه‌های آن را رمزگذاری کند یا پنهان سازد و استفاده از آن را مستلزم داشتن گذرواژه کند. سرویس‌های جاسوسی بیگانه تلاش می‌کنند افرادی را داخل شرکت‌ها، سازمان‌ها و نهادهای حساس شناسایی کنند که به‌مثابهٔ منابع مطلع، اطلاعات لازم را در اختیار دارند؛ چنانچه از این افراد برای کسب اطلاعات محرمانه استفاده شود، سرویس جاسوسی بیگانه از خط قرمز فعالیت‌های قانونی و اخلاقی فراتر رفته، به‌اصطلاح در منطقهٔ خاکستری یا سیاه عمل می‌کند. منطقهٔ خاکستری یعنی عملی غیراخلاقی اما قانونی و منطقهٔ سیاه یعنی عمل غیراخلاقی و غیرقانونی؛ در حالی که منطقهٔ سفید مربوط به عملی می‌شود که نه خلاف قانون و نه خلاف اخلاق است (بونی، ۱۳۸۳: ۱۷۱). یکی از شیوه‌هایی که جاسوسان شبکه‌ای به‌کار می‌برند، بهره‌برداری از خطاها، غفلت‌ها یا اشتباه‌های نهادها، سازمان‌ها و شرکت‌ها در ارسال رایانامه‌هاست که ممکن است حاوی اطلاعات حساسی باشد. رقبای باهوش در پوشش شرکت‌های مختلف، پایگاه‌هایی به‌وجود می‌آورند که می‌توان آن را پایگاه‌های همزاد نامید؛ به‌گونه‌ای که این پایگاه‌ها تقلید نشانی اینترنتی و رایانامهٔ شرکت هدف است. کسی که بخواهد پیامی را به مدیران شرکت به نشانی واقعی آن ارسال کند، ممکن است پسوند org را با پسوند com اشتباه گرفته، پیام خود را به‌طور مستقیم برای رقبای آنها بفرستد. ابزار دیگری که ممکن است برای جاسوسان اینترنتی مفید باشد، نرم‌افزار Net Eraser است. یکی از مقام‌های سازمانی سیا گفته است: کاربرد اصلی این برنامه در این است که تحلیل‌گران سازمان می‌توانند پایگاه‌های اینترنتی خارجی را کنترل کنند و به‌دلیل تغییر مستمر نشانی، شناخته نمی‌شوند. برخی گزارش‌ها حاکی از آن است که آمریکا

در همکاری با متحدان نزدیک خود چون انگلیس، استرالیا و کانادا، نظام جهانی نظارت و کنترل ایجاد کرده است. این نظام به‌اختصار اشلون[1] نامیده می‌شود و برای ردگیری همهٔ «مکالمات تلفنی و پیام‌های الکترونیکی و نمابرها»ست (بونی، ۱۳۸۳: ۱۷۴). بی‌شک این حجم عظیم جمع‌آوری اطلاعات، شامل اطلاعات حساس کشورمان نیز می‌شود. فناوری موجود کنونی، به رایانه‌ها امکان بررسی حجم بزرگی از ارتباطات را می‌دهد؛ به‌طور کلی، این گروه از فناوری‌ها به متن و داده‌یابی موسوم‌اند. متن و داده‌یابی یا غواصی الکترونیکی و شگردهای نو، از انبوه داده‌های جمع‌آوری‌شده برای استخراج اخبار مورد نظر به‌صورت برخط[2] استفاده می‌کند. سپس رایانه‌ها داده‌ها را با هم درمی‌آمیزند و به‌هم ربط می‌دهند تا استفاده و کنترل آنها برای تحلیل‌گران اطلاعاتی آسان باشد (وارک، ۱۳۸۴: ۱۸۰). گسترش اینترنت به کاهش امتیازهای کشورهای بزرگ در زمینهٔ شنود و جاسوسی منجر می‌شود. کاربرد مفید اینترنت و گسترش رمزگذاری قوی از راه آن، امکان حمایت سریع از کشورهای کوچک و بازیگران فروملی در برابر جاسوسی و رمزشکنی را افزایش می‌دهد (آلبرتس، ۱۳۸۵: ۱۷۵).

همچنین، به‌نظر می‌رسد دولت آمریکا که خود را حافظ امنیت جهانی می‌داند، برای حفظ امنیت دو دنیای ما، یعنی دنیای مجازی و واقعی، دست به جاسوسی سیاسی بزند؛ موضوعی که دولت آمریکا پس از حادثهٔ ۱۱ سپتامبر آن را تصویب و عملی کرد.

امروزه سیزده کارگزار ریشه (میزبان و پشتیبان) در جهان وجود دارد که از این تعداد، ده کارگزار در خاک آمریکا و سه کارگزار دیگر، در کشورهای انگلستان، سوئد و ژاپن قرار دارند. همچنین، مرکز ثبت چهار دامنهٔ اصلی، یعنی com، net، org و biz، شرکت‌های آمریکایی است و شرکتی که امتیاز ثبت دامنهٔ info را دارد، بیشتر سرمایه‌اش آمریکایی است. دامنه‌های mill و gov نیز مختص دستگاه‌های نظامی آمریکا و دامنهٔ edu اختصاصی دانشگاه‌های آمریکاست. به این ترتیب، آمریکا با در اختیار داشتن مدیریت منابع اینترنتی، به‌خوبی فرصت اطلاع از تمام وقایع شبکهٔ جهانی را دارد. دکتر ماری سیگال دربارهٔ اصطلاح جاسوسی اینترنتی می‌گوید: آمریکایی‌ها پیش از حمله به عراق کوشیدند از راه اینترنت به درون شخصیت مردم عراق پی برده، به‌اصطلاح شمار بیشتری از آنها را جذب کنند (سایت باشگاه اندیشه). همین شیوه در گرجستان و دیگر جمهوری‌های شوروی سابق که دچار انقلاب رنگی شدند، اجرا شده است. اینترنت فقط پنجره‌ای رو به جهان نیست، بلکه ابزاری خطرناک برای ورود به خصوصیات شخصیتی دیگران و استفاده از این افراد برای اهداف جاسوسی هم است. افرادی که وارد چنین شبکه‌هایی می‌شوند، نمی‌دانند اسرار کشورشان را فروخته، خیانت می‌کنند.

1. ECHELON
2. on line

جمهوری اسلامی ایران، به‌خصوص در شرایط موجود و مطرح بودن موضوع هسته‌ای، هدف سرویس‌های جاسوسی به‌شمار می‌رود و مجموع عملیات جاسوسی شناخته‌شدهٔ اینترنتی علیه آن به‌طور جدی مطرح است.

اینترنت و جنگ اطلاعاتی

از زمان وقوع جنگ خلیج فارس، گونه‌ای از جنگ به‌وجود آمده است که اسامی مختلفی بر آن اطلاق می‌شود: جنگ دقیق، جنگ سایبرنتیک[1]، جنگ اطلاعات و جنگ موج سوم. انقلاب مستمر کنونی که در امور نظامی صورت گرفته است، تا حدودی از تغییرات در فناوری‌ها، به‌ویژه فناوری‌های مرتبط با انقلاب اطلاعات ناشی شده است (اشنایدر، ۱۳۸۵: ۳۱۸). افزون بر آن، تقابل و سیاست مهار کشورهایی مانند جمهوری اسلامی ایران بر ماهیت شکل‌های جدید جنگ تأثیر می‌گذارد. اعتقاد بر آن است که این کشورها تهدیدی عظیم و نو برای جهان غرب‌اند.

در جنگ اطلاعاتی، منطق نابودسازی دقیق و اشراف و برتری اطلاعاتی جایگزین منطق نابودی جمعی می‌شود که ویژگی جنگ تمام‌عیار صنعتی است. از اواخر سدهٔ بیستم و در پی تغییر بنیان‌های فناوری‌های جنگ، از میکروالکترونیک، تراکم دیجیتالی و فناوری‌های انتقال سریع اطلاعات برای اهداف نظامی استفاده شده است. تغییر چشمگیر دیگر، پیشرفت‌های به‌وجودآمده در ساختار اطلاعات نظامی است. تغییر در اصول جنگ، خود را در محفل‌های نظامی غرب به‌شکل حرکت به‌سوی توجه بیشتر به نقش دانش در جنگ به‌مثابهٔ شکل جدید جنگ نمایان ساخته است.

سازمان‌های جمع‌آوری پنهان به‌مثابهٔ پشتیبان یگان‌های دفاعی، بدون جلب توجه، درون سامانه‌های ارتباطات راه دور دنیا کار می‌کنند؛ اطلاعات آنها ستون فقرات اطلاعات موجود برای تحلیل‌گران امنیتی و دفاعی است. این سازمان‌ها متناسب با شرایط سدهٔ بیست‌ویکم، بار دیگر سازماندهی شده‌اند؛ از جملهٔ این سازمان‌ها، آژانس امنیت ملی آمریکاست که جمع‌آوری و پردازش اطلاعات گرفته‌شده از ارتباطات اینترنتی رادیویی و تلفنی کشورهای هدف را برعهده دارد. سامانه‌های جمع‌آوری این آژانس، به جاروبرقی‌های عظیم اخبار معروف‌اند (آیزندراس، ۱۳۸۳: ۲۵۳). هر عبارتی که وارد فهرست مراقبت شود، رایانه‌ها به جست‌وجوی آن در شبکهٔ جهانی اینترنت می‌پردازند و در مرحلهٔ بعدی، به‌سرعت تمام این منابع به‌طور منظم در اینترنت ردیابی می‌شوند. اینترنت همچون خون در رگ‌های آژانس امنیت ملی و سازمان‌های مشابه عمل می‌کند که دارای توان سخت‌افزاری و نرم‌افزاری انحصاری خود هستند.

1. Cybernetics

در جنگ اطلاعاتی که بر پایهٔ جمع‌آوری، تفسیر و عمل براساس اطلاعات از راه سامانهٔ جدید ارتباطی (اینترنت) استوار است، از رسیدن اطلاعات به دشمن جلوگیری می‌شود یا شبکهٔ اطلاعاتی و فرایند گردش اطلاعات دشمن مختل می‌شود تا نتواند بر اوضاع تسلط یافته، عملیات و تحرکات نیروهای خود را فرماندهی کند. همان‌طور که در جنگ عراق اتفاق افتاد، تبادل تصویری مشترک و کامل از عملیات بین مراکز فرماندهی، به‌وسیله اینترنت تاکتیکی فراهم آمده است.

درمجموع، می‌توان گفت روند شتابان توسعهٔ فناوری اطلاعات به موضوعی راهبردی برای کشورها در بررسی و دسترسی به شیوه‌های جدید جنگ تبدیل شده است. انگارهٔ بهره‌برداری از فناوری اطلاعات در امور دفاعی و نظامی و ترکیب آن در ساختار نیروهای نظامی کشورها، در حال حاضر از رونق زیادی برخوردار است؛ به‌طوری که به اینترنت به‌مثابهٔ شبکهٔ عظیم اطلاع‌رسانی، بانک وسیع اطلاعاتی و موضوع مهم راهبردی توجه شده است.

نتیجه

شالودهٔ کشور بر پایهٔ مجموعه‌ای از سازمان‌ها و نهادهای دولتی و خصوصی فعال در بخش‌ها و سطوح مختلف استوار است. اگرچه این سازمان‌ها و نهادها و موضوع فعالیت آنها برای مردم شناخته‌شده است، به فضای مجازی با وجود اهمیت و تأثیرهای عمدهٔ آن، کمتر توجه شده؛ دلیل این امر آن است که بخش‌های نخست، جنبهٔ عینی و محسوس دارند و مانند اعضای ظاهری بدن انسان‌اند که در منظر عمومی قرار دارند، حال آنکه فضای مجازی مانند شبکهٔ عصبی بدن انسان است که وجود دارد و بسیار مهم است و امنیت و سلامت بدن به آن وابسته است، اما محسوس نیست و دیده نمی‌شود. بر این اساس، شبکه‌ای موسوم به شبکهٔ جهانی اینترنت وجود دارد که صدها هزار رایانه، سرور و کابل‌های نوری را به یکدیگر متصل می‌سازد تا امور جاری کشور در حوزه‌های گوناگون اقتصادی، مالی، تجاری، صنعتی، علمی و پژوهشی، دفاعی، امنیتی، انتظامی، بهداشتی و درمانی انجام گیرد. ماهیت اینترنت و محیط راهبردی متأثر از آن، به‌گونه‌ای است که قابلیت ایجاد تهدید و ناامنی را داشته، الزام‌های خاص خود را در حوزهٔ امنیت ملی اقتضا می‌کند. از این منظر، مشخص می‌شود که امنیت ملی کشور با اینترنت و امنیت فضای مجازی، پیوستگی مثبت خواهد داشت که در این مقاله سعی شد چگونگی این پیوستگی در حوزهٔ امنیتی (تروریسم، خرابکاری و عملیات جاسوسی)، حوزهٔ سیاسی- فرهنگی و حوزهٔ نظامی- دفاعی در حد بضاعت بررسی و تبیین شود. در ادامه، برخی راهکارهای اولیه‌ای معرفی شد که در مواجهه با مدیریت امنیت ملی در فضای مجازی به‌نظر می‌رسید.

برای اینکه توفیق در مدیریت امنیت ملی در فضای مجازی، باید بـه شـرایط حـال و آینـده آگاه بود، متغیرهای اثرگذار و محوری در امنیت ملی را آن‌گونه کـه هـستند، درک و اسـتخراج کرد و در چارچوب نظام ارزشی و قانونی، به ترسـیم راهبردهـا و کـشف و معرفـی راهکارهـا پرداخت. بر این اساس، راهکارهای زیر برای تأمین امنیت فضای مجازی توصیه می‌شود:

۱. به‌نظر می‌رسد تهدید اصلی کشور از ناحیهٔ اینترنت، فقدان گفتمـان امنیتـی دربـارهٔ ایـن پدیده است. متأسفانه نگاه مدیران و دستگاه‌های مربوط در توسعهٔ فناوری اطلاعـات بـدون در نظر گرفتن الزام‌های امنیت فضای مجازی، سبب ایجاد تبعات منفی داخلـی و خـارجی زیـادی شده است. بنابراین، توسعهٔ فناوری اطلاعات باید همراه با لحاظ کردن الزام‌های امنیـت فـضای مجازی صورت گیرد.

۲. تقویت امنیت و حفاظت از اطلاعات حساس و سامانه‌های ارتباطاتی نهادها، سازمان‌هـا، و ارگان‌های مهم که به‌نحوی در خدمات‌رسانی عمومی دخالت دارند؛ زیرا هرگونـه اخـلال در انجام گرفتن مأموریت این سازمان‌ها، ممکن است آسیب‌های جبران‌ناپذیری در پی داشته باشد.

۳. ازآنجاکه تهدیدها و آسیب‌های مجازی به‌سرعت تحـول و تغییـر مـی‌یابـد، لازم اسـت نهادهای متولی مدیریت آنها، از انعطاف‌پذیری مناسب و مطمئن در برنامه، سازمان و مأموریـت برخوردار باشند.

۴. فرایند مدیریت امنیت ملی در فضای مجازی و مواجهه بـا تهدیـدهای آن، فراینـدی در حال شدن است و نباید آن را پایان‌یافته تلقی کرد؛ این امر، اصـلاح و تکمیـل هـر سـالهٔ نظـام جامع امنیت را در فضای مجازی با توجه به شرایط و یافته‌های نو ضروری می‌کند.

۵. اینترنت از دو جهت با آزادی‌های مدنی و خصوصی در ارتباط است: از یک سو، امکان سوءاستفاده از این ابزار نو برای تروریست‌ها، خرابکاران و دیگر بـازیگران فروملـی و فراملـی وجود دارد و از سوی دیگر، این امکان وجود دارد که برنامـهٔ مبـارزه بـا تهدیـدها و مـدیریت امنیت فضای مجازی به تهدید آزادی‌های مدنی به بهانه تأمین امنیت منجر شود. تصمیم‌سـازی در این حوزه، بسیار دشوار است و لحاظ کـردن هـر دو جنبـهٔ آن در مـدیریت امنیـت فـضای مجازی و تدوین قوانین مربوط به جرایم رایانه‌ای ضروری است.

منابع و مآخذ

الف) فارسی

۱. آلبرتس، دیوید (۱۳۸۵). گزیده‌ای از عصر اطلاعات. ترجمهٔ علی علی‌آبادی. تهران: انتشارات پژوهشکدهٔ مطالعات راهبردی.
۲. آزر، ادوارد (۱۳۷۹). امنیت ملی در جهان سوم. ترجمهٔ پژوهشکدهٔ مطالعات راهبردی. تهران: انتشارات پژوهشکدهٔ مطالعات راهبردی.

۳. آشنا، حسام‌الدین (۱۳۸۲). اینترنت و امنیت سیاسی و فرهنگی. تهران: مرکز مطالعات فرهنگ و ارتباطات دانشگاه امام صادق (ع).
۴. آیزندراس، کریج (۱۳۸۳). ناامنی ملی. ترجمهٔ سیدمجید نوری. تهران: انتشارات دانشکدهٔ امام محمدباقر (ع).
۵. اشنایدر، کریگ (۱۳۸۵). امنیت و راهبرد در جهان معاصر. ترجمهٔ اکبر عسگری صدر. تهران: انتشارات پژوهشکدهٔ مطالعات راهبردی.
۶. بونی، ویلیام (۱۳۸۳). جاسوسی شبکه‌ای: تهدید جهانی اطلاعات. ترجمهٔ معاونت پژوهشی دانشکدهٔ امام محمدباقر (ع). تهران: انتشارات دانشکدهٔ امام محمدباقر (ع).
۷. تاجیک، محمدرضا (۱۳۸۱). مقدمه‌ای بر استراتژی امنیت ملی ج.ا.ا: رهیافت‌ها و راهبردها. ج۱. تهران: فرهنگ لقمان.
۸. ذکایی، سعید (۱۳۸۳). «جوانان و فراغت مجازی». فصلنامهٔ مطالعات جوانان. ش۶.
۹. راجرز، پال (۱۳۸۴). زوال کنترل: امنیت جهانی در قرن ۲۱. ترجمهٔ امیرمحمد حاجی‌یوسفی. تهران: انتشارات پژوهشکدهٔ مطالعات راهبردی.
۱۰. روحانی، حسن (۱۳۸۰). «امنیت عمومی، امنیت ملی و چالش‌های فراروییی». نشریهٔ راهبرد. ش۲۰: ۴۵-۵.
۱۱. سلطانی‌نژاد، احمد (۱۳۸۶). «کاربرد فناوری اطلاعات در سیاست». جزوهٔ درسی دورهٔ دکتری. دانشکدهٔ حقوق و علوم سیاسی دانشگاه تهران.
۱۲. کاخ سفید (۱۳۸۶). امنیت در فضای مجازی. ترجمهٔ اصغر افتخاری. چ۲. تهران: پژوهشکدهٔ مطالعات راهبردی.
۱۳. گرگی، عباس (۱۳۸۵). «اینترنت و هویت». فصلنامهٔ مطالعات ملی. س۷. ش۱: ۶۹-۵۳.
۱۴. ماندل، رابرت (۱۳۷۷). چهرهٔ متغیر امنیت ملی. ترجمهٔ پژوهشکدهٔ مطالعات راهبردی. تهران: انتشارات پژوهشکدهٔ مطالعات راهبردی.
۱۵. معینی، جهانگیر (۱۳۸۴). «هویت و مجاز: تأثیر هویتی اینترنت». فصلنامهٔ مطالعات ملی. س۶. ش۴: ۱۲۳-۱۰۷.
۱۶. مولانا، حمید (۱۳۷۱). جریان بین‌المللی اطلاعات. ترجمهٔ یونس شکرخواه. تهران: مرکز مطالعات و تحقیقات رسانه‌ها.
۱۷. وارک، وسلی (۱۳۸۴). مجموعه مقالات اطلاعاتی- امنیتی. ترجمهٔ معاونت پژوهشی دانشکدهٔ امام محمدباقر (ع). ج۴. تهران: انتشارات دانشکدهٔ امام محمدباقر(ع).

ب) خارجی

18. Eriksson, Johan (2006). "The Information Revolution, Security , and International Relations: (IR) relevant Theory?". International Political Science Review. Vol. 27. No. 3: 221-244.
19. Nye, Joseph S. (2001). "soft power and conflict management in the information age". Turbulent peace, challenge of managing international conflicts. united states institute of peace press. chapter 22.
20. The Canadian center for Intelligence and security studies (Carleton University) (2006). "A framework for understanding terrorist use of the Internet". Vol. 2006-2.