فصلنامه علمی ـ پژوهشی مطالعات انقلاب اسلامی
سال یازدهم، پاییز ۱۳۹۳، شماره ۳۸
صفحات ۱۰۴ ـ ۸۵

ISLAMIC REVOLUTION STUDIES
A Quarterly Scientific ـ Research Journal
Vol. 11, Autumn 2014, No 38

مروری بر امنیت سایبری؛
درس‌هایی برای جمهوری اسلامی ایران

سید مهدی برقعی*

چکیده

امروزه این نگرانی برای دولت‌ها ایجاد شده که حملات مبتنی بر فضای مجازی، می‌توانند سرویس‌های ارتباطی، اقتصادی و حیاتی کشورها را مختل نموده و موجب خسارات شدیدگردند. جمهوری اسلامی ایران سال‌هاست که از فضای مجازی در بخش‌های مختلف نظامی و غیر نظامی بهره می‌گیرد. مراکز حساس ملی مانند تأسیسات هسته‌ای و وزارت نفت در سال‌های گذشته هدف حملات سایبری گروه‌ها، افراد و دولت‌ها بوده است. بدین منظور، سعی شده است تا دراین مقاله به این پرسش که چگونه حملات سایبری منجر به تهدیدات امنیتی در نظام جمهوری اسلامی ایران خواهد شد، پرداخته شود و در نهایت راهبردهای مناسب برای امنیت روزافزون فضای سایبری جمهوری اسلامی ایران در برابر حملات سایبری ارائه خواهد شد.

واژگان کلیدی

تهدیدات امنیتی، حملات سایبری، راهبرد جمهوری اسلامی ایران.

مقدمه

با گسترش فناوری‌های اطلاعاتی، هم‌اکنون شاهد گذار به دوران جدیدی هستیم که در آن، نوع و شیوه‌های تهدیدات و در نتیجه مفهوم امنیت متحول شده است. در دوران صلح، احتمال جاسوسی دشمنان درباره اوضاع عمومی کشور و دست‌یابی به اطلاعات طبقه‌بندی شده و نیز جمع‌آوری اطلاعات در مورد مواضعی از قبیل اهداف کلیدی و رخنه در زیرساخت‌هایی به مانند تأسیسات هسته‌ای به منظور تدارک تهاجم‌های سایبری متصور می‌باشد.

---

*. دانشجوی دکتری حقوق بین‌الملل عمومی دانشگاه مفید. smb_pardes66@yahoo.com
تاریخ دریافت: ۱۳۹۳/۱/۲۳ تاریخ پذیرش: ۱۳۹۳/۶/۲

در زمان جنگ یا بحران، دشمن می‌تواند با اتکای به اطلاعات جمع آوری شده به زیرساخت‌های حیاتی حمله و یا با مخدوش کردن اعتبار سیستم‌های اطلاعاتی نزد افکار عمومی و ایجاد نگرانی و هراس عمومی، شورش‌های گسترده و براندازی را تدارک ببیند. از ویژگی‌های فناوری اطلاعات و فضای مجازی، امکان ساماندهی و تدارک تهاجم سازمان‌یافته از فواصل دور علیه اهداف از پیش تعیین شده می‌باشد. این فناوری علاوه بر اینکه موجب آشکار شدن نقاط ضعف موجود در زیرساخت‌های حیاتی می‌شود، با ایجاد اختلال، مانع واکنش دفاعی و یا ایجاد تأخیر در آنها نیز می‌گردد. (حسن بیگی، ۱۳۸۳: ۱۳)

در چنین شرایطی، قسمت اعظمی از امور مهم دولتی و بین‌المللی جمهوری اسلامی ایران از طریق فضای سایبر انجام می‌گیرد. با توجه به آسیب‌پذیری و قابل نفوذ بودن چنین فضایی، اختلال در سامانه آن می‌تواند ضررهای جبران‌ناپذیری به موجودیت‌های مختلف وارد کند.

در این مقاله به ارتباط حملات سایبری با تهدیدات امنیتی ناشی از آن و خلأهای امنیتی موجود در این زمینه پرداخته می‌شود. فرضیه نوشتار حاضر این است که وابسته بودن تمام جوامع به امور رایانه‌ای و منطبق شدن کنونی مراکز حساس دولتی با فضای مجازی، موجب می‌شود تا حملات سایبری به عنوان اموری که منجر به اخلال در زمینه‌های تحقیقاتی، امنیتی و به تعویق افتادن پروژه‌های ملی خواهند شد، در نظر گرفته شوند. از این‌رو در رویکرد اول با تبیین نظریه‌های روابط بین‌الملل در حوزه امنیت به بحث امنیت در فضای سایبر وارد خواهیم شد و در رویکرد دوم به مهم‌ترین حملات سایبری که تأسیسات هسته‌ای و صنایع حساس جمهوری اسلامی ایران را نشانه رفته‌اند می‌پردازیم. در رویکرد پایانی، به راهبرد کشورهای قدرتمند در عرصه فضای سایبر و ارائه راهکارهای مناسب برای جلوگیری از وقوع حملات سایبری علیه مراکز جمهوری اسلامی ایران پرداخته خواهد شد.

امنیت سایبری

در برداشت سنتی، امنیت منحصراً در نبود خطرات فیزیکی خلاصه می‌شد. در چنین شرایطی اختلال در امنیت به یک حمله فیزیکی بستگی داشت. اما امنیت در معنای نوین را نمی‌توان به تنهایی در چارچوب مرزها و در روبط دولت ـ ملت‌ها جستجو کرد. امنیت سایبر را می‌توان به استفاده از ابزارهای مرتبط با ایمن‌سازی، توانمندسازی و صحت اطلاعاتی دانست که پردازش، حفاظت و ارتباطشان به وسیله ابزارهای الکترونیکی امکان‌پذیر است. متناسب با پیچیده‌تر شدن روابط و شبکه‌های اجتماعی در عصر پست مدرنیته و خارج شدن این روابط از حالت‌های ساده اولیه که جنبه فیزیکی و محسوس داشت، بر اهمیت افزایش امنیت فضای مجازی و بررسی فرصت‌ها و آسیب‌های احتمالی آن بر ابعاد مختلف اقتصادی، فرهنگی و سیاسی افزوده شده که این خود ضرورت تبیین نظام جامع مدیریتی برای تهدیدات امنیتی در فضای سایبری را دوچندان کرده است. از آنجا که فضای سایبر یک جریان پیوسته و پویاست، حفاظت از اطلاعات در چنین فضایی کار آسانی نیست. فضای مجازی ویژگی‌های خاص خود را دارد که پیوستگی، پیچیدگی و پیشرفت روزافزون از نمادهای آن هستند.

در این فضا کنشگران ملی و جهانی به هم پیوند می‌خورند و فاصله بسیار کم‌رنگ شده و تأثیرگذاری و تأثیرپذیری بازیگران از همدیگر به شدت افزایش می‌یابد. فضای مجازی بخش‌های مختلف را به هم وصل کرده و تفکیک‌ها را کم‌رنگ می‌کند. فضای مجازی، فضایی بسیار پیچیده، با بازیگران متعدد و اهداف و انگیزه‌های گوناگون است. همچنان که تهدیدات این حوزه پیچیده است، مقابله با آنها هم پیچیده و دشوار است. جمهوری اسلامی ایران سال‌هاست که از فضای مجازی در بخش‌های دولتی و خصوصی، نظامی و غیر نظامی بهره می‌گیرد. شبکه‌های مجازی ایران در سال‌های گذشته هدف حملات سایبری گروه‌ها، افراد و دولت‌ها بوده است و به احتمال زیاد در آینده هم تکرار خواهد شد.

برای نمونه ویروس استاکس‌نت که درسال ۲۰۱۰ در کارخانجات صنعتی و تأسیسات هسته‌ای ایران رسوخ کرد، از این طریق می‌توانست پیامدهای اقتصادی مخربی به بار آورد و موجب به تعویق افتادن پیشرفت ایران در زمینه تحقیقات هسته‌ای شود. علی‌رغم تهدیدات امنیتی ناشی از حملات سایبری سازوکارهای لازم برای مقابله با این تهدیدات در حقوق بین‌الملل هنوز پیش‌بینی نشده است. به این علت شناخت حملات سایبری، ویژگی‌های آن و راهبرد کشورها در تأمین امنیت فضای مجازی به جمهوری اسلامی ایران کمک می‌کند تا نه تنها دست به تدوین قوانین لازم در این زمینه بزند، بلکه شناخت صحیح این گونه حملات باعث خواهد شد تا با استفاده از راهکارهای مناسب امنیتی به مقابله با حملات سایبری بپردازد.

حملات سایبری

حمله‌های سایبری، نوعی حمله است که در آن یک مؤلفه رایانه‌ای وجود دارد که سیستم‌های هدف را غیر قابل استفاده نموده، کارایی آنها را کم کرده و با تزریق اطلاعات غلط، دقت تصمیم‌گیری کاربران را کاهش می‌دهد و حتی منجر به سرقت اطلاعات می‌شوند. (مرادیان، ۱۳۸۷: ۵۷) حمله‌های سایبری چند تفاوت عمده با شکل‌های معمول حمله دارند: اول اینکه حمله‌های سایبری توسط عوامل نامعلوم صورت می‌گیرد و ردیابی و یافتن محل اختفای آنها بسیار دشوار است. این‌گونه حمله‌ها، فاصله و مکان را (که در حمله سنتی در آن استقرار می‌یافتند) محو کرده و از بین می‌برند. دوم اینکه حمله‌های سایبری بسیار ارزان‌تر از حمله در جنگ‌های معمولی است و در عین حال که فاقد آسیب‌پذیری و هزینه هستند، بیشتر مورد توجه شخص مهاجم قرار می‌گیرند. سوم اینکه ساختارهای شبکه‌ای گروه‌های مهاجم، آنها را در مقابل هرگونه اقدام تلافی‌جویانه ایمن ساخته و باعث افزایش توان خود ترمیمی آنها می‌گردد. (کاکاوند، ۱۳۸۲: ۲۷ ـ ۱۱)

چندین نوع حمله سایبری وجود دارد که در طیفی از کم‌شدت تا شدید، دسته‌بندی شده‌اند:

۱. خرابکاری اینترنتی[1]: دشمن، امکان نفوذ و خرابکاری در سیستم‌های اطلاعاتی نظامی و غیر نظامی خود را با قطع شبکه‌های اطلاعاتی، به ویژه قطع شبکه جهانی اینترنت، برای کشور مقابل سلب می‌کند.

1. Web vandalism.

۲. گردآوری داده‌ها: دسترسی به اطلاعات طبقه‌بندی شده که امکان جاسوسی از نقـاط مختلـف جهـان را فراهم می‌کند.

۳. حمله گسترده اخلال در سرویس‌دهی[1]: در این نوع حمله، شمار زیادی از رایانه‌ها در یک کشور مبـادرت به ایجاد اخلال در سرویس‌دهی به سیستم‌های کشور دیگر می‌کنند.

٤. اخلال در تجهیزات[2]: فعالیت‌های نظامی که در آنها از رایانه و ماهواره برای هماهنگی استفاده می‌شود، در خطر این نوع حمله قرار دارند؛ زیرا مهاجمان می‌توانند فرمان‌ها و ارتباطات را رهگیری کرده یا تغییر دهند.

۵. حمله به زیرساختارهای حیاتی: نیروگاه‌های برق، تأسیسات آب‌رسانی و سوخت‌رسانی، ارتباطات و حمـل و نقل در برابر این نوع حمله آسیب پذیری بالایی دارند. (عبدالله‌خانی، ۱۳۸۶: ۱۳۶)

٦. رهگیری[3]: در این روش، نفوذگران می‌توانند به شکل مخفیانه از اطلاعات نسخه‌برداری کنند.

۷. افزودن و تغییر اطلاعات: در این روش نفوذگر، اطلاعات اضافی را بر اطلاعات اصلی اضافه کـرده و یـا آن را تغییر می‌دهد.

۸. وقفه[4]: در این روش نفوذگر باعث اختلال در شبکه و تبادل اطلاعات می‌شود. (پوروستایی، ۱۳۸۹: ۲۶)

۹. افزایش سرعت در تصمیم‌گیری: سیستم‌های اطلاعاتی کمک شایانی به بهبود سرعت و دقـت در امـر تصمیم‌گیری توسط فرماندهان می‌کنند. (قاضی‌زاده، ۱۳۸۷: ۲۳۲)

آشنایی با بزرگترین حملات سایبری جهان

حملات سایبری دامنه متنوعی دارند؛ از شوخی‌های معمولی گرفته تا کرم‌های مخرب رایانه‌ای که بـه واسـطه حافظه‌های قابل حمل جابه‌جا شده و امنیت کلی کشوری را به خطر می‌اندازند. از آنجایی کـه امـروزه تمـامی زندگی ما به تکنولوژی، رایانه‌ها و اینترنت گره خورده است اطمینان از ایمن بودن ایـن ابزارهـا بسـیار حیـاتی است. با بررسی حملات سایبری چند سال اخیر به مواردی خواهیم رسید که بیشترین آسیب‌پذیری را در برابـر حمله‌های تبهکارانه سایبری داشته‌اند.

استونی ـ ۲۰۰۷

در این سال کشور استونی در معرض سیلی از حملات سایبری قرار گرفت که کل زیرساخت‌های اینترنتی آن کشـور را تحت تأثیر خود قرار دادند و البته هدف اصلی، وب سایت‌های دولتی و سازمانی، بانک‌هـا و روزنامـه‌هـا بودنـد. بـا توجه به زمان‌بندی حملات که در زمان مجادله این کشور و روسیه، بر سر برداشتن یادبود شوروی از پایتخـت

1. Distributed Denial of Service Attacks.
2. Equipment Disruption.
3. Interception.
4. Interruption.

استونی بود، مقامات استونی روس‌ها را عامل اصلی این حملات می‌دانند. با این حال امکان ردیابی منشأ اصلی این نوع حملات وجود نداشته است.

گرجستان ـ ۲۰۰۸

در سال ۲۰۰۸ و درست یک هفته پس از حمله نظامی روسیه به گرجستان، حمله‌ای سایبری، دولت و وب‌سایت‌های رسانه‌ای گرجستان را دچار اختلال کرد. همان‌طور که در سال ۲۰۰۷ نیز جو سیاسی اقتضا می‌کرد که کرملین دستور یک حمله سایبری را به استونی صادر کند، در این مورد هم روسیه از مظان اتهام خارج نبود.

با این تفاوت که افرادی که به گرجستان حمله کردند سیستم‌های رایانه‌ای سازمانی این کشور را نیز بی‌نصیب نگذاشتند. این حمله به «بات نت»[۱] شهرت داشته و به گونه‌ای است که هر شهروند روسی می‌توانسته است آگاهانه یا ناآگاهانه و با دانلود نرم‌افزاری سبک، به ایجاد اضافه بار بر روی وب‌سایت‌های دولتی و سازمانی گرجستان کمک کرده باشد.

فرماندهی مرکزی ایالات متحده آمریکا ـ ۲۰۰۸

برخی از سازمان‌ها به ویژه سازمان‌های دولتی، رایانه‌های خود را از دسترس عموم و یا عضویت در شبکه‌های غیر ایمن خارج می‌کنند تا از بروز شکاف‌های امنیتی در آن جلوگیری کنند. در زبان رایانه‌ای این شکاف به شکاف هوایی شهرت دارد. با این همه، با ظهور رسانه‌های قابل حمل مانند حافظه‌های USB و یا CD تبهکاران سایبری فرصتی مناسب را برای نفوذ به درون شبکه‌های بسیار ایمن به دست آوردند. در سال ۲۰۰۸ وزارت دفاع آمریکا با چنین حملاتی مواجه شد که منبع اصلی آن یک حافظه USB غیر ایمن بود که به یک لپ تاپ وصل شده بود. این حافظه حاوی کدهای مخربی بود که در سرتاسر رایانه‌های وزارت دفاع آمریکا پخش شد و اطلاعات موجود در این رایانه‌ها را به سرورهای خارجی ارسال کرد.

عملیات آئورا ـ ۲۰۰۹

در سال ۲۰۰۹ میلادی، گوگل، آدوبی و در حدود ۳۰ شرکت دیگر اعلام کردند قربانی حملات به شدت پیچیده سایبری شده‌اند. هکرها طی این حملات توانسته بودند با بهره‌برداری از نقطه ضعفی شناخته نشده در مرورگر اینترنت اکسپلورر، به اطلاعات حیاتی و خصوصی این شرکت‌ها دست پیدا کنند. نام این حمله سایبری توسط نایب رئیس شرکت مک کافی، آقای «دیمیتری آلپروویچ» انتخاب شده است. وی با ردیابی فایل‌های آلوده موفق به کشف واژه «آئورا» به معنی سپیده دم در میان فایل‌ها شد. این بار هم با وجود اینکه امکان اطمینان یافتن برای منشأ اصلی این نوع حملات وجود نداشت، باز همه نگاه‌ها متوجه چین شد و

۱. (botnet) بات نت برنامه‌ای مخرب است که برنامه‌نویسان توسط آن رایانه‌های بسیاری در یک شبکه گسترده را به ویروس آلوده می‌کنند تا به صورت پنهانی اوضاع را تحت نظر داشته باشند.

انتشار اسنادی درباره ارتباط دولت چین با این حمله سایبری توسط وب‌سایت جنجالی ویکی لیکس، فرضیه مجرم بودن چین در این حملات گسترده سایبری را تقویت کرد.

کرم استاکس نت ـ ۲۰۱۰

این کرم در سال ۲۰۱۰ کشف شد و متخصصان این کرم را به عنوان یکی از پیچیده‌ترین کرم‌های رایانه‌ای که تا به حال مشاهده شده می‌شناسند. این کرم به سیستم‌های رایانه‌ای صنعتی که سیستم‌های ماشینی نیروگاه‌ها و کارخانه‌ها را تحت کنترل دارند، حمله می‌کند. این کرم با بهره‌برداری از چهار نقطه ضعف که پیش از این در سیستم عامل ویندوز ناشناخته باقی مانده بودند، فعالیت می‌کند.

برای مثال یکی از آسیب‌پذیری‌های ویندوز به استاکس نت کمک می‌کند در میان شبکه‌های محلی گسترش پیدا کند؛ دیگری به پخش شدن کرم در میان سخت‌افزارهای قابل جابه‌جایی از قبیل حافظه‌های USB و یا درایورهای CD کمک می‌کند. قابلیت‌های این کرم در استفاده از بیش از یک نقطه ضعف سیستم عامل رایانه‌ها کاملاً بی‌سابقه است و نشان از حمایت دولتی و پشتیبانی مالی شدید از این کرم رایانه‌ای دارد. با وجود اینکه هنوز تعیین قطعی هدف اصلی استاکس‌نت امکان‌پذیر نیست، اما حملات این کرم به شکلی مشخص و نامتناسب به سوی ایران متمرکز بوده است. (همشهری آنلاین، ۱۳۹۱)

ویروس فلیم ـ ۲۰۱۱

فلیم جدیدترین ویروسی است که توسط سیستم‌های امنیتی غربی علیه جمهوری اسلامی ایران طراحی شده است. پس از انتشار خبر کشف بد افزار اینترنتی جدید با نام فلیم (شعله) و موفقیت در ایران در ارائه نسخه پاک کننده آن، بسیاری از منابع غربی اذعان می‌کنند که این بدافزار یک محصول اسراییلی است. ظاهراً شرکت نرم‌افزاری کاسپرسکی در روسیه کاشف فلیم بوده است. این ویروس بر خلاف استاکس نت فقط برای جاسوسی و جمع‌آوری اطلاعات طراحی شده است. این ویروس از صفحه نمایشگر رایانه عکس می‌گیرد و میکروفون رایانه را روشن می‌کند تا مکالمات محیط ضبط شود. بعداً اطلاعات گردآوری شده به منبع منتشر کننده ویروس منتقل می‌شود. کارشناسان می‌گویند به علت بزرگی و پیچیدگی ویروس فلیم، کشف کامل برنامه آن و اینکه چه کارهایی انجام داده است سال‌ها زمان می‌برد. با این حال، از یافته‌هایی که تاکنون به دست آمده مشخص شده است که ویروس فلیم می‌تواند از طریق یو اس پی، بلوتوث یا دیگر ابزارها در یک شبکه گسترش پیدا کند.

در دستگاه‌های آلوده، این ویروس می‌تواند برای اجرا شدن منتظر نرم‌افزارهای خاصی شود و سپس به تصاویر دست یابد؛ میکروفون‌های داخلی را برای ضبط مکالمات روشن کرده و ایمیل‌ها و چت‌ها را رهگیری کند. این ویروس می‌تواند اطلاعات به دست آمده را بسته‌بندی و رمزگذاری کرده و آنها را برای رایانه‌های مشخصی در سراسر جهان بفرستد.

به زبان فنی می‌توان گفت ویروس فلیم مانند یک «کرم» عمل می‌کند؛ به این صورت که بدون نیاز به دخالت انسان گسترش می‌یابد و برای رساندن اطلاعات ربوده شده به دست گردانندگانش کانال‌هایی را برای خود باز می‌کند.

ویژگی حملات سایبری

۱. کم هزینه بودن

هزینه ورود به حملات سایبری کم است و بر خلاف جنگ با فناوری سنتی، توسعه جنگ‌افزارهای مبتنی بر روش‌های سایبری احتیاج به منابع مالی گسترده ندارد. داشتن متخصص سیستم‌های کامپیوتری و دسترسی به شبکه‌های مهم، تنها شرایط لازم برای انجام این قسم حملات است. کشورهای جهان، میلیاردها دلار در سال هزینه هواپیما، بمب، موشک و گلوله می‌کنند، در صورتی که اگر یک کشور تصمیم بگیرد تا یک دهم هزینه سالانه خود را که صرف خرید یا ساخت سلاح‌های سنتی می‌کند، صرف پیشرفت در زمینه فضای مجازی و حملات سایبری کند، در طول سال قادر خواهد بود به طور غیر قابل باوری به صنایع و نظام اداری کشورهای مختلف دسترسی پیدا کند.

۲. خدشه وارد کردن در مرزبندی‌های سنتی

مخدوش شدن مرزهای سنتی از ویژگی‌های حملات سایبری است. متعدد بودن مخالفان احتمالی، تنوع در جنگ‌افزارها و گوناگونی راهبردها موجب شده است تا شناسایی منابع تهدید در این جنگ به طور فزاینده‌ای با مشکلات فراوانی روبه‌رو شود؛ به طوری که بیشتر اوقات با دشواری می‌توان بین منابع داخلی و خارجی تهدیدهای سایبری، تفاوت قائل شد.

۳. گسترش فریب و مدیریت افکار عمومی

در حملات سایبری این امکان وجود دارد تا با تکیه بر تکنیک‌های اطلاعاتی، توانایی فریب و دستکاری را افزایش داد، به طوری که تصاویری ارائه شود که کاملاً متفاوت از واقعیت‌های موجود باشد. در حقیقت، این فرصت برای عناصر حملات سایبری به وجود آمده است تا با کمک گرفتن از اطلاعات کلیدی، فهم همگانی را دستکاری کنند و به این ترتیب، افکار عمومی را در مسیر دلخواه سوق دهند. به طور مثال گروه زاپاتیست‌های مکزیک با تبلیغاتی که در شبکه اینترنت به راه انداختند، توانستند برای خود حمایت سیاسی به دست آورند.

۴. دشواری مشکلات هشدار دهنده تاکتیکی و ارزیابی حمله

در حال حاضر، هیچ گونه سیستم هشدار دهنده تاکتیکی با کفایتی که قادر باشد بین حملات استراتژیک سایبری و انواع دیگر فعالیت‌های ارتباطات رایانه‌ای مانند جمع‌آوری اطلاعات یا حوادث اتفاقی تفاوت قائل

بشود، وجود ندارد. نتیجه این است که حتی کشورهای پیشرفته قادر به دانستن اینکه چه وقت بـه آنهـا حملـه می‌شود، چه کسی حمله می‌کند و تهاجم چگونه هدایت می‌شود، نیستند.

۵. آسیب‌پذیری کشورهای توسعه یافته

اقتصاد کشورهای توسعه یافته به طور فزاینده‌ای به شبکه‌های متصل به سیستم‌هـای پیچیـده بـرای خطـوط لوله گاز و نفت و انتقال نیروی برق وابسته است.

آسیب‌پذیری در حال حاضر، بـه طـور کامـل درک نشـده اسـت. عـلاوه بـر ایـن، مفهـوم بازدارنـدگی و پاسخ‌گویی در زمینه تهدیدهای سایبری هنوز نامعلوم است.

۶. فرد در برابر جمع

در حمله سایبری یک فرد می‌تواند با طراحی یک ویروس و یا نرم‌افزار مخرب همه کشورهای دنیا را بـا خطـر مواجه سازد. این ویژگی نتیجه دانایی‌محور بودن این نوع حملات است. به عبـارت دیگـر، در حملـه سـایبری کسی که دانش و خلاقیت بیشتری داشته باشد، قدرتمندتر است.

۷. غافلگیرانه، نامشخص و مبهم

مهاجم سایبری جایی را خراب می‌کند که هیچ احتمال نفوذ به آن داده نمـی‌شـود. ردیـابی چنـین مهاجمـانی دشوار است.

۸. آسیب‌رسانی غیر قطعی

در یک بمب فیزیکی که در محل منفجر می‌شود می‌توان قدرت تخریـب آن را بـر آورد کـرد، امـا در فضـای مجازی معلوم نیست که اگر شیری دستکاری شود و آب روی شهری باز شود تا چه میزان مـی‌توانـد تخریـب کند. این در حالی است که مهاجم در لحظه حمله خود از معرض هرگونه آسیبی به دور است.

۹. ماهیت تروریستی

به دلیل حذف بعد مکان، هر کسی می‌تواند در هـر کشـور خـارجی دیگـر، عملیـات خرابکـاری انجـام دهـد. همچنین ماهیت حمله سایبری به گونه‌ای است که در آن، مهاجم بیشتر اهداف غیر نظامی را نشانه مـی‌رود و قربانیان آن تا حد زیادی بی‌دفاع هستند. (حسن بیگی، ۱۳۸۳: ۱۱۳ ـ ۱۱۱)

راهبرد کشورهای قدرتمند در عرصه تأمین امنیت فضای مجازی

راهبرد نظامی کشورها تابعی از نوع تهدیدات و توانمندی‌های آنها برای مقابله بـا تهدیـدات اسـت. سـه دهـه پیش نه صحبتی از حملات سایبری بود و نه راهبردی برای مقابله با ایـن تهدیـدات. عمـر حمـلات و جنـگ

سایبر به دو دهه گذشته و به گسترش اینترنت در جهان برمی‌گردد. با پیدایش فضای مجازی در جهان، اتصال ساختارهای رایانه‌ای به یکدیگر و دسترسی افراد، گروه‌ها و کشورها به شبکه جهانی رقابت و کشمکش در این عرصه ابعاد زیادی یافت. از زمانی که حملات اینترنتی علیه مراکز رقیب به اقدامی برای تضعیف طرف مقابل، تأمین اهداف و منافع و نشان دادن خود، تبدیل شد و مقابله با این اقدامات به شیوه‌های مختلف صورت گرفت، می‌توان ادعا کرد که نوعی منازعه سایبری پا به عرصه وجود گذاشت.

الف) راهبرد امنیت فضای مجازی آمریکا

فضای مجازی در آمریکا به شکل گسترده در تمام ارکان دولتی و خصوصی حضور دارد و همه کارها به نوعی به این فضا وابسته است. وزارت دفاع آمریکا بر پایانه‌های متعددی که در آن بالغ بر هفت‌میلیون رایانه و پانزده‌هزار شبکه وجود دارد، استوار است. این شبکه‌ها نیروهای نظامی، اطلاعاتی و عملیاتی آمریکا را پشتیبانی می‌کنند. حملات سایبری به این شبکه‌ها می‌تواند موجب لو رفتن برنامه‌ها و اقدامات نیروهای نظامی و امنیتی، تضعیف موقعیت و توان و آسیب‌پذیری آنها در برابر نیروهای رقیب و دشمن شود. در مقابل، دسترسی آنها به اطلاعات و داده‌های مهم کشورهای رقیب و متخاصم می‌تواند به تأمین اهداف با هزینه‌های اندک منجر شود. در هر دو جنبه سلبی و ایجابی، فضای مجازی اهمیت فزاینده‌ای برای آمریکا و سایر کشورها پیدا کرده است. (Armed- services.senate.gov/statement, 2010: 19-24)

در ماه مه ۲۰۱۱ سند راهبرد سایبری آمریکا منتشر شد. بر اساس این سند، فضای سایبری مدنظر دولت آمریکا دارای چهار ویژگی اساسی است:

۱. گشایش برای نو آوری؛

۲. امنیت کافی برای کسب اعتماد مردم؛

۳. عملی بودن در سراسر جهان؛

۴. قابل اطمینان بودن برای حمایت از کار مردم.

بر اساس این سند در محیط سایبری هنجارهایی مانند حمایت از آزادی بنیادین، احترام به حق مالکیت، ارزش قائل شدن برای حوزه خصوصی کاربران، حق دفاع مشروع، قابل اجرا بودن در سطح جهانی، ثبات شبکه، دسترسی مطمئن، حاکمیت چندگانه و پشتکار لازم برای حفظ امنیت سایبری، دنبال خواهد شد.

در بخش اولویت‌های سیاست‌گذاری نیز تأکید این سند بر موارد زیر است:

۱. اقتصاد: ارتقای معیارها و ابتکارات بین‌المللی و تقویت بازار آزاد.

۲. حفاظت از شبکه و افزایش امنیت، اعتماد و انعطاف‌پذیری.

۳. اجرای قانون: گسترش همکاری و حاکمیت قانون.

۴. حوزه نظامی: کسب آمادگی برای چالش‌های امنیتی در قرن ۲۱.

در حوزه نظامی به طور خاص روی سه محور تمرکز شده است:

ـ شناسایی و سازگار شدن با نیازهای فزاینده ارتش برای برخورداری از شبکه‌های مطمئن و امن.

ـ ایجاد و تقویت اتحادهای نظامی برای مقابله با حملات سایبری.

ـ گسترش همکاری‌ها با متحدان و شرکا در فضای سایبری به منظور بالا بردن امنیت دسته جمعی.

در سند راهبرد سایبری آمریکا به رئوس اساسی سیاست‌های آمریکا اشاره شده است و کوشش شده در سایه این سند ساختارهای مناسب ایجاد و اقدامات آمریکا در این زمینه بیش از پیش هماهنگ شود. همچنین ایجاد یک مرکز سایبری در دستور کار قرار گرفته است تا هماهنگی وظایف فضای سایبری دولت آمریکا را درون دفتر اجرایی رئیس جمهور بر عهده گیرد و رئیس آن به عنوان مشاور رئیس جمهور در زمینه امنیت سایبری فعالیت خواهد کرد. (www.defense.gov)

به رغم انتشار سند راهبردی آمریکا، درباره توانایی‌های جنگ سایبری آمریکا پیچیدگی‌ها و ابهامات زیادی وجود دارد. بسیاری از ابعاد تلاش آمریکا برای توسعه این‌گونه جنگ‌ها و تعریف استفاده قانونی از حملات سایبری به صورت محرمانه باقی مانده و بسیاری از مقامات مربوطه از هرگونه اظهارنظر درباره این موضوع خودداری می‌کنند. موضوع اساسی این است که آیا دولت آمریکا دستور جنگ سایبری علیه دولت‌های دیگر را صادر کرده است؟ یا در چه شرایطی به چنین اقدامی دست می‌زدند؟ یکی از ابداعاتی که از سوی مقامات آمریکایی در دست بررسی قرار دارد، این است که به صورت مخفیانه وارد یک سرور رایانه‌ای در روسیه یا چین شوند و یک بات‌نت را قبل از اینکه در شبکه‌های رایانه‌ای ایالات متحده منتشر شود، نابود کند. همچنین، سازمان‌های اطلاعاتی آمریکا می‌توانند کدهای مخربی که به صورت مخفیانه در تراشه‌های رایانه‌ای در هنگام تولید ذخیره شده را فعال کنند تا آمریکا بتواند نظارت بر رایانه‌های کشورهای مورد نظر خود را با کنترل از راه دور و از طریق اینترنت در دست داشته باشد. (forum.p30world.com)

سند راهبرد سایبر آمریکا و اسناد و گزارش‌های تهیه شده در پنتاگون و مرکز فرماندهی سایبری آمریکا هیچ کدام به صراحت، دولتی را دشمن آمریکا در فضای سایبری طرح نمی‌کنند. اما اغلب سخنرانی‌ها و تحلیل‌های مقامات و صاحب‌نظران آمریکایی، دو دولت چین و روسیه را بیش از دیگران، دشمنان آمریکا در فضای سایبری تلقی می‌کنند. جهت‌گیری اصلی اسناد آمریکا و اقدامات این کشور در این زمینه نشان دهنده ترس و نگرانی آنها از اقدامات دولت‌های چین و روسیه در فضای مجازی است.

ب) راهبرد سایبری دولت‌های اروپایی

به موازات استفاده وسیع از فضای مجازی و گسترش حملات اینترنتی، دولت‌ها به ضرورت سیاستگذاری منسجم و برخورداری از سیاست راهبردی واحد در این زمینه بیش از پیش آگاه شده و نسبت به آن اقدام می‌کنند. مجلس اعیان انگلیس در اواسط ماه مارس سال ۲۰۱۱ میلادی طی گزارشی به صراحت اظهار داشت:

بریتانیا نیاز دارد تا به طور نزدیک‌تری با ناتو همکاری کند تا از شالوده‌های حساس ملی خود در مقابل «حملات سایبری» دشمنان سابق دوران جنگ سرد از جمله روسیه و چین، دفاع کند؛ زیرا خطرات حملات اینترنتی، شبکه‌های تلفن همراه و بانک‌ها سه سال پیش و با حمله روس‌ها به استونی آشکار شده است. (cabinetoffice.gov.uk)

پیش از اظهارات مجلس اعیان انگلیس، «اندرس راسموسن»[1] دبیر کل ناتو در حالی که طی سخنانی در فنلاند «خط مشی استراتژیک» جدید این اتحاد نظامی ـ امنیتی را تحسین می‌کرد، با اشاره به بند پنج پیمان آتلانتیک شمالی بار دیگر تصریح کرد که دفاع از ۲۸ کشور عضو ناتو همچنان مهم‌ترین عملکرد ناتو محسوب می‌شود. وی همچنین تأکید کرد:

اینکه فقط سربازان، تانک‌ها و تجهیزات نظامی را در مرزها به خط کنیم، کافی نیست. بلکه اتحاد ناتو نیاز دارد تا به خطرات فضای سایبر هم توجه کند؛ زیرا دشمن ممکن است هر جایی در فضای سایبر ظاهر شود. (www.gafele.blogsky.com)

موضوعات امنیت سایبر با توجه به ماهیت آنها از جمله تهدیداتی هستند که به شدت بدون نظم و قاعده مشخص و مبهم، پیش می‌روند و یا می‌توان آنها را ابداع کرده و یا وانمود کرد که چنین تهدیدی وجود دارد.

جپ هوپ شفر[2] (دبیر کل وقت ناتو) در سخنرانی خود در ناتو، به طور خاص به توضیح مسئله امنیت سایبر پرداخت و تأکید کرد که ناتو باید قابلیت‌های منحصر به فردی که در قوای نظامی حملات سایبری وجود دارد را مورد توجه قرار دهد. برای مثال ناتو می‌تواند پاسخ سریعی را برای حمایت از متحدان و حتی شاید شرکای خود در صورت بروز یک حمله، در نظر بگیرد. پرسش این است که آیا اعضا پیمان ناتو این را پذیرفته‌اند که در صورت حمله سایبری از سوی دولت یا منبع ناشناخته بر اساس بند پنج پیمان عمل خواهند کرد و آن را حمله‌ای علیه امنیت ملی خود تلقی خواهند نمود؟ شفر در برنامه خود برای عملی کردن بند پنج پیمان ناتو با بهره‌گیری از فضای سایبر به این موارد اشاره کرد:

قطع منابع تأمین انرژی یا حمله سایبری به زیرساخت‌های حیاتی یک کشور می‌تواند منجر به تخریب کالبد اجتماعی و اقتصادی آن شود که همانند جنگی است که تیری در آن شلیک نشود. بنابراین بسیار حیاتی است که ناتو نیز به تعریف اقداماتی بپردازد که قادر به انجام آنها است. برای مثال محافظت از زیرساخت‌های حیاتی، تأمین امنیت خطوط انتقال انرژی و امنیت فضای مجازی از جمله آنها است. کشورهای عضو پیمان ناتو با تأکید بر بند پنج پیمان آتلانتیک شمالی به این موضوع اذعان داشتند که کشورهای عضو ناتو می‌بایست بر اساس هدف اصلی پیمان یک پدافند جمعی را شکل دهند. (strategicreview.org)

افراد زیادی در حوزه مطالعات راهبردی معتقدند که حملات سایبری هم‌اکنون نقشی مشابه با نقش

1. Anders Rasmussen.
2. Jaap Hoop Scheffer.

جنگ‌های هوایی در قرن بیستم ایفا می‌کنند. حملات سایبری روسیه علیه استونی (۲۰۰۷) و گرجستان (۲۰۰۸)، حملات چین علیه شرکت گوگل (۲۰۱۰) و برخی سازمان‌ها و نهادهای آمریکایی و در نهایت حملات آمریکا و رژیم اشغالگر اسرائیل علیه تأسیسات هسته‌ای ایران، نشان‌دهنده شروع دوره جدیدی است که در آن امنیت ملی کشورها با فضای مجازی پیوند نزدیک دارد. در واقع، امنیت سایبر، دفاع و تهاجم سایبری از جمله مسائلی هستند که به حقایق زندگی امروز و دغدغه ذهنی دولت‌مردان تبدیل شده‌اند. مادلین آلبرایت[1] وزیر خارجه اسبق آمریکا گزارش «گروه متخصصان» خود را در رابطه با خط‌مشی راهبردی ناتو در قرن ۲۱ در بروکسل ارائه کرد. در این گزارش بر تهدیدات سایبری و ضرورت اتخاذ راهبردی واحد برای مقابله با این تهدیدات در قالب پیمان ناتو تأکید شده است. (www.tebyan.net)

پدافند سایبر و بخش اجتناب‌ناپذیر آن یعنی جنگ سایبر، اجزای دکترین جنگی ناتو هستند که در آخرین خط‌مشی راهبردی ناتو که به طور رسمی در نوامبر ۲۰۱۰ در لیسبون پرتغال منتشر شد، تشریح شده است. در این راهبرد مجموعه‌های قابل دفاع در برابر حملات سایبری، از دفاع در مقابل نیروهای زرهی دشمنان فرضی، اولویت و اهمیت بیشتری یافته است. در ذهنیت تازه دفاعی ناتو تجهیز و نگهداری ارتش‌های پرشمار، نظیر آنچه ترکیه تاکنون به داشتن آن می‌بالید، جای خود را به شبکه مبادله اطلاعات و افزایش قدرت مقابله با مخاطرات حملات سایبری داده است.

راهبرد سایبری ناتو برای افزایش توانمندی‌های این اتحاد بر موارد زیر تأکید می‌کند:

۱. تقویت منابع اطلاعاتی از طریق پاسخ‌گویی به حوادث، مشارکت در اطلاعات، به روز نگهداری سامانه‌های رایانه‌ای برای کاهش آسیب‌پذیری‌ها.

۲. در نظر گرفتن منازعات سایبری به عنوان یک مسئله امنیت ملی از سوی سیاستگذاران. حملات سایبری و مقابله با آنها اقدامی تاکتیکی نیست و باید در سطح راهبرد امنیت ملی مد نظر قرار گیرد و تصمیمات و اقدامات مناسب با آن انجام شود.

۳. گستره شبکه‌های اساسی اروپا به خصوص در حوزه زیرساخت‌های ملی که ممکن است نیروهای نظامی ناتو بر آنها متکی باشند، باید حداکثر به اعضای اتحادیه اروپا محدود شود.

۴. ناتو باید به دنبال راه‌هایی برای به اشتراک‌گذاری چند جانبه برخی توانمندی‌های دفاعی در کشورهای عضو، در حوزه پاسخ به رویدادها، آموزش امنیتی و ابزارها و فناوری‌ها باشد. ناتو نمی‌تواند برای هر کدام از ملت‌های عضو این سازمان، ساختار امنیتی مجازی جداگانه‌ای در نظر بگیرد.

۵. همکاری با بخش خصوصی ضروری است. نحوه تعامل با بخش خصوصی نباید تنها به اشتراک‌گذاری اطلاعات خلاصه شود. بسیاری از سازمان‌های غیر دولتی دارای قابلیت‌های قابل توجهی در مبارزه با جرایم

1. Madeleine Albright.

اینترنتی، مقابله با رویدادها و آموزش نیروها دارند که لازم است از آنها استفاده شود. این تعامل به سود هر دو طرف بوده و هزینه را برای همه بخش‌ها کاهش می‌دهد. فضای مجازی به لحاظ ویژگی‌های آن با چهار میدان دیگر نبرد متفاوت است. فضای مجازی حوزه جدیدی است که در آن بازیگران متعددی حضور دارند. به همان میزان که تهدیدات آن نسبت به حوزه‌های دیگر متفاوت است، مقابله با آنها نیازمند اقدامات متفاوتی است.

نقش بر جسته فناوری‌های جدید و پراکندگی تهدیدگران و تنوع اقدامات و اهداف تهدیدات نباید موجب غفلت از اقدام در سطح ملی شود. جدا از راهبرد سایبری سازمان آتلانتیک شمالی (ناتو)، برخی دولت‌های اروپایی نیز راهبردهای سایبری خود را در عرصه مجازی اعلام کرده‌اند یا در پی تهیه و تصویب آن هستند. دولت انگلستان راهبرد امنیت سایبری خود را در سال ۲۰۰۹ اعلام کرد. راهبرد امنیت سایبری انگلستان ضمن تأکید بر کاهش خطرات عرصه مجازی، بر استفاده از فرصت‌ها در جهت تقویت علم و دانش و افزایش ظرفیت‌ها برای تصمیم‌گیری در انگلستان تأکید می‌کند. دولت انگلستان بر این باور است که کاهش خطرات در عرصه مجازی از طریق کاهش انگیزه‌ها و توانایی‌های کنش‌گران رقیب، کاهش آسیب‌پذیری منافع دولت انگلستان در عرصه مجازی و کاهش تأثیرات عملیات سایبری علیه منافع انگلستان صورت می‌گیرد. فرصت‌های نهفته در این عرصه از طریق جمع‌آوری اطلاعات از تهدیدات و کنشگران تهدیدزا، تقویت حمایت از سیاست‌ها و خط مشی‌های دولت انگلستان و اقدام علیه کنشگران رقیب افزایش می‌یابد. (Cyber Security Strategy of the United Kingdom) با تقویت دانش و آگاهی‌ها، توسعه توانمندی‌های انسانی و فنی می‌توان به بهبود توانمندی‌های سیاستگذاری در عرصه مجازی امیدوار بود.

این راهبرد بر تهیه و اجرای برنامه مبارزه علیه تهدیدات سایبری میان حکومت‌ها، کار و هماهنگی نزدیک میان بخش‌های مختلف عمومی، صنعتی و شرکای بین‌المللی، ایجاد مرکزی برای عملیات سایبری با عنوان csoc علیه رقبا تمرکز دارد. انگلستان، مرکز نظارت بر فضای سایبر را در پاسخ به اقدامات و رویدادهای تهدیدزا ایجاد کرده است و می‌کوشد درک درستی از حملات سایبری علیه انگلستان به دست آورد و به بهترین نحو ممکن نسبت به آنها پاسخ دهد. در سال ۲۰۱۱ دولت انگلستان اعلام کرد که تهدیدات سایبری علیه انگلستان به شدت افزایش یافته و به تهدید اول علیه این کشور تبدیل شده است. به ویژه اگر این تهدیدات با اقدامات و تهدیدات تروریستی ترکیب شوند، بسیار خطرناک‌تر خواهد بود. (www.carlisle.army, 1391)

فرانسه نیز یکی دیگر از قدرت‌های بزرگ اروپایی است که راهبرد مکتوبی را برای امنیت سایبری خود تهیه و منتشر کرده است. این سند در سال ۲۰۱۱ منتشر شد و عموماً شامل مواردی است که راهبرد ناتو و انگلستان در نظر گرفته‌اند. (www.number10.gov.uk)

جمهوری اسلامی ایران و امنیت سایبری

بسیاری از کارشناسان و تحلیل‌گران حوزه امنیت، بر این باورند که پایان یافتن دوران جنگ سرد نه تنها منجر به امن ترشدن جهان نشده است، بلکه به وجود آمدن چالش‌های امنیتی غیرنظامی جدیدی همچون تخریب

محیط زیست، رفاه اقتصادی، سازمان‌های جنایی بین‌المللی و مهاجرت گسترده افراد، امنیت جهانی را با چالش‌های جدی‌تری نسبت به گذشته مواجه ساخته است. تحلیل‌گران بر این باورند که اهمیت این مسائل 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 پراهمیت به نظر می‌رسد، توجه اندکی داشته‌اند. آنچه در مورد این تهدیدهای جدید قابل توجه است، این است که ویروس‌ها 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. (کلارک، ۱۳۸۶: ۳۴۲)

نگاهی به سه حمله بزرگ سایبری به کشورمان که به وسیله بدافزارهای استاکس نت، دوکو و فلیم انجام گرفت، نشان می‌دهد که ابزارهای به کارگرفته شده در این حملات به مرور تکمیل شده‌اند و هر بار بر درجه تخریب آنها افزوده شده است. از دیدگاه فنی، پیچیدگی‌های فوق‌العاده بالای بدافزارها، هوشمندی در طراحی و به کارگیری، خلاقیت در نحوه عملکرد و سازگاری با فناوری‌های امنیتی شناخته شده و رایج، نشان از آن دارد که این ابزارها به وسیله دولت‌ها و با اهداف خاص طراحی و اشاعه داده شده‌اند. به این ترتیب، جنگ سایبری در نگاه دولت‌های دیگر نه تنها گزینه‌ای محتمل بلکه عملاً جنگی تمام‌عیار است که مدتی نیز از شروع آن می‌گذرد. به موازات اقدامات در حوزه‌های تکنیکی و عرصه‌های دیپلماتیک، غرب فعالیت خود را برای چارچوب‌بندی و تعیین خطوط قرمز و تحمیل آن به دیگر بازیگران آغاز کرده است. به نحوی که پس از دو سال فشار از سوی پنتاگون برای ارائه پیش‌نویس قواعد جنگ سایبری آمریکا، سرانجام این دستورالعمل‌ها در ماه‌های قبل تنظیم و به امضای باراک اوباما رسید و در پی آن اعلام شد که هرگونه حمله سایبری از سوی کشورهای دیگر اقدام جنگی بوده و با حمله نظامی پاسخ داده خواهد شد. (Theohary and Rollins, 2009) در واقع، ایشان در تبعیض آشکار دیگری در عرصه بین‌المللی خود را مجاز به پاسخ‌گویی به این به اصطلاح، جنگ متمدنانه دانسته و از طرفی به صورت پیش‌دستانه از خوف حملات تلافی‌جویانه کشورهایی مانند ایران به تهدید و ارعاب جهانی می‌پردازند تا از این رهگذر خود را در حاشیه امن قرار دهند.

با نگاهی به گذشته و مراحل طی شده از سوی غرب در رابطه با تسلیحات با تکنولوژی‌های نوین می‌توان متوجه این روند شد که غرب در رویارویی با تکنولوژی‌های دفاعی مدرن به استفاده و آزمایش آن در عرصه‌های مختلف با نیت شناسایی ابعاد تکنیکی، مدیریتی حقوقی و کنترلی و استراتژیک آن می‌پردازد که نتیجه آن حرکت در لبه پیش رونده تکنولوژی و تدوین نظام حقوقی ـ مدیریتی بین‌المللی (مانند نظام منع گسترش تسلیحات اتمی، میکروبی شیمیایی و حتی موشک‌های بالستیک ...) برای محدودسازی ورود و پیشرفت دیگر تمدن‌ها در آن حوزه دفاعی تکنولوژیک است. از همین روست که پنتاگون در سند نوین استراتژی جنگ

سایبری آمریکا بر این نکته تأکید می‌کند که قواعد نزاع مسلح که جنگ‌های سنتی را هدایت می‌کند، از یک سری معاهدات بین‌المللی از جمله معاهده ژنو نشأت گرفته است. اما جنگ سایبری تحت معاهدات موجود قرار ندارد و ایالات متحده در پی یافتن اجماعی بین هم‌پیمانان خود در خصوص طریقه پیشبرد این مسئله است.

از طرف دیگر، بحث و گفتگو درباره این تهدیدات، متأثر از انقلاب مداوم اطلاعات و رسوخ آن به تمام جنبه‌های زندگی بشر امروز است. به نظر می‌رسد نه تنها جمهوری اسلامی ایران، بلکه تمامی کشورها در رابطه با امنیت سایبری با این قبیل مشکلات مواجه هستند:

ـ اطمینان نداشتن از موقعیت جغرافیایی عاملان حملات اینترنتی.

ـ ادغام در حال تحول دستگاه‌های فناوری اطلاعات و رایانه‌های مدرن به زیرساخت‌های اطلاعاتی حساس.

ـ آسیب پذیری‌های جدید در کنار نفوذ به زیرساخت‌های کشور از تهدیدهای پیچیده و فزاینده.

ـ ضعف هماهنگی بخش دولتی و خصوصی به خطرات در حال ظهور و ابهامات قانونی برای پاسخ به اینگونه حمله‌ها.

این مسائل دست کم چهار پیامد مهم را برای جمهوری اسلامی ایران در پی خواهد داشت:

نخست، تغییر برداشت جمهوری اسلامی ایران درباره چگونگی تعریف منافع، پایگاه‌های قدرت و امنیت در حوزه سایبر؛

دوم، بالاگرفتن چالش‌ها و توجه بیشتر جمهوری اسلامی ایران در برابر توانایی اداره و کنترل حملات سایبری؛

سوم، ارتباط موضوع امنیت ملی و شهروندان با تهدیدات جدید سایبری نظیر استاکس نت و فلیم؛

چهارم، حفاظت بیشتر از مراکز حساس دولتی نباید منجر به کاهش ظرفیت جمهوری اسلامی ایران در ارائه خدمات مجازی شود.

جمهوری اسلامی ایران طی سال‌های گذشته بارها هدف حملات سایبری قرار گرفته است و شاید بتوان ادعا کرد یکی از هدف‌ها و قربانیان اصلی حملات سازمان‌یافته سایبری در جهان به شمار آید. اما به صورت مشخص جمهوری اسلامی ایران راهبرد مکتوب و مشخصی را تاکنون منتشر نکرده است. عدم تدوین سند راهبردی در این موضوع در ایران به معنای بی‌توجهی به فضای مجازی و تهدیدات ناشی از حملات سایبری نیست، بلکه اینترنت اساساً پدیده‌ای شکل گرفته در دولت‌های پیشرفته صنعتی است و اغلب شرکت‌های ارائه‌دهنده خدمات در این کشورها قرار دارند و لذا ایران در این حوزه آسیب‌پذیر شده است. حفاظت از داده‌های اساسی سیاسی، امنیتی، نظامی، اقتصادی و صنعتی بسیار سخت و دشوار است و بدون در پیش گرفتن راهبردی دقیق، اراده سیاسی قدرتمند برای حمایت از آن، انجام اقدامات اساسی و پشتیبانی مردمی از این راهبردها و اقدامات، تأمین منافع ملی در عرصه مجازی ممکن نیست.

نگاهی به عملکرد ایران در عرصه فضای مجازی نشان دهنده این است که جمهوری اسلامی ایران نسبت به تلاش دیگران در آسیب زدن به زیرساخت‌های اساسی کشور، آگاه است و اقداماتی را در این عرصه

شروع کرده است. تصویب قانون جرایم اینترنتی در بهمن ۱۳۸۹ از سوی مجلس شورای اسلامی، ابلاغ سیاست‌های کلی شبکه‌های اطلاع‌رسانی رایانه‌ای از سوی مقام معظم رهبری (زندی، ۱۳۸۹) تصویب مقررات و ضوابط شبکه‌های اطلاع‌رسانی از سوی شورای عالی انقلاب فرهنگی، ایجاد سازمان تنظیم مقررات و ارتباطات رادیویی در وزارت ارتباطات و فناوری اطلاعات و همچنین تأسیس سازمان پدافند غیر عامل در ستاد کل نیروهای مسلح و تشکیل پلیس سایبری فضای تولید و تبادل اطلاعات (فتا) در نیروی انتظامی به منظور مقابله با جرایم اینترنتی از جمله اقداماتی است که از سوی جمهوری اسلامی ایران برای مقابله با تهدیدات سایبری انجام شده است. بیشترین حساسیت در مقابله با تهدیدات مجازی در ایران به مسائلی معطوف گشته است که ارزش‌های دینی، سیاسی و اجتماعی جمهوری اسلامی ایران را تهدید می‌کنند.

این موضوع در قالب جنگ نرمی است که از فضای مجازی بیش از ساز و کارهای دیگر استفاده می‌کند. بر این اساس، افراد و گروه‌های داخلی اعم از مخالف و بی‌طرف و موافقان نظام در معرض این تهدید قرار دارند و اقدامات باید همه آنها را پوشش دهد. چنین شرایطی به محدودسازی دسترسی به فضای مجازی منجر شده است که در قالب ساماندهی سایت‌ها، فیلتر کردن اینترنت، طرح اینترنت ملی و... منجر شده است. این موضوعات منجر شده است تا توجه به حملات سایبری تحت الشعاع قرار گیرند.

نکته دوم در مورد سیاست‌ها و اقدامات جمهوری اسلامی ایران در مقابله با تهدیدات مجازی این است که محوریت این اقدامات با نیروها و سازمان‌هایی است که اساساً جنبه نظامی و امنیتی دارند. در این سیاستگذاری به وجه مردمی و غیر نظامی آن کمتر توجه شده است و عملاً جایگاهی برای بخش خصوصی و توانمندی آنها در نظر گرفته نشده است. ارتش سایبری، نیروی مقاومت بسیج، سازمان پدافند غیر عامل، مخابرات و کمیته فیلترینگ بیش از سایر بخش‌ها و سازمان‌ها در این زمینه فعال هستند و جنبه سلبی در آن بیش از جنبه ایجابی مورد توجه بوده است. حملات سایبری به اهداف ایران در دو سال گذشته نشان‌دهنده آسیب‌پذیری جمهوری اسلامی ایران در بخش‌های صنعتی، اقتصادی و مالی است. حملات سایبری با بدافزارهای استارس، دوکو، استاکس نت و فلیم و جاسوسی اطلاعات در زمینه فضای مجازی نشان‌دهنده ضرورت توجه به این حوزه و مقابله با تهدیدات بالفعل و بالقوه در این زمینه است و بی‌توجهی به آن ممکن است آسیب‌های جدی به شبکه زیر ساخت‌های حیاتی ایران وارد آورد.

آنچه مهم است و هم اکنون نیز خارج از توان بزرگواران سکاندار امنیتی کشور نیز نیست، تدوین «استراتژی امنیت ملی سایبری» کشور است که نیاز به آن به صورت روزافزون احساس می‌شود. توجه به این موضوع، زمانی دارای اهمیت دو چندان می‌شود که دریابیم دشمنان و رقبای ایران اسلامی در تلاش برای تکمیل حلقه‌های امنیت سایبری داخلی همچون تدوین استراتژی امنیت سایبری آمریکا در بخش بازرگانی و نظام‌مندسازی امنیت سایبری بین‌المللی در راستای اهداف خود هستند. تدوین «استراتژی امنیت ملی سایبری»

دربرگیرنده چهار حوزه امنیت ملی است: سیاسی ـ امنیتی، فرهنگی ـ اجتماعی، اقتصادی و نظامی که نحوه تصمیم‌گیری، هدایت و کنترل امور را از سطح تکنیک تا استراتژیک در حوزه‌های سلبی ـ ایجابی، آفندی ـ پدافندی و خارجی ـ داخلی کشور پوشش دهد.

این طرح می‌بایست مأموریت‌ها، وظایف، الزامات و اصول و فرمول‌های هدایت راهبردی، ایجاد ساختارهای نوین، خط مشی‌ها، رویه‌ها، پروتکل‌ها و چارچوب چینش و هماهنگی و هدایت یکپارچه عناصر را از بالا به پایین پوشش دهد و توسعه تاکتیک‌ها و تسلیحات ویژه این جنگ را در دستور کار قرار دهد. با تدوین و اجرایی کردن این طرح در ذیل و راستای «استراتژی بزرگ» کشور است که می‌توان کنش‌ها و واکنش‌های کشور را در حوزه سایبر و تمامی حوزه‌های مربوط تنظیم کرد.

همچنین با داشتن راهبردی جامع می‌توان بخش آموزش‌های مردمی و ملی را هم تحت پوشش قرار داد تا حتی رایانه‌های خانگی هم از خطر آسیب‌های حملات سایبری در امان باشند. حملات سایبری به اهداف ایران در دو سال گذشته نشان دهنده آسیب‌پذیری جمهوری اسلامی ایران در بخش‌های صنعتی، اقتصادی و مالی است. حملات سایبری با بدافزارهای استارس، دوکو، استاکس نت و فلیم و جاسوسی اطلاعات در زمینه فضای مجازی نشان دهنده ضرورت توجه به این حوزه و مقابله با تهدیدات بالفعل و بالقوه در این زمینه است و بی‌توجهی به آن ممکن است آسیب‌های جدی به شبکه زیر ساخت‌های حیاتی ایران وارد آورد. نگهداری اطلاعات به خصوص تنظیمات امنیتی و ساختار آن به صورت درون‌سیستمی بهترین روش اطمینان از امنیت سیستم‌ها است. متخصصان کشور می‌توانند با تولید داخلی سیستم‌های کنترل فرآیندی، شامل نرم‌افزارها و سخت‌افزارهای کنترلی که با کیفیت مشابه نمونه‌های خارجی تولید می‌شود و امنیت آن قابل اطمینان است، جایی برای استفاده از سیستم‌های خارجی نگذارند. (karbord.net, 1390)

در نتیجه جایگزینی سیستم‌های به روز داخلی، به جای نمونه‌های خارجی که هیچ گونه پشتیبانی ندارند، در جهت درون‌سیستمی نگه داشتن اطلاعات، با رویکرد استفاده از تنظیمات امنیتی پویا و ساختارمند کردن رفتارهای آن و استفاده از دیوارهای آتش و استحکام سامانه‌های امنیتی، می‌تواند راهکار مناسبی برای مقابله با استاکس‌نت و دیگر بد افزارهای بعدی باشد.

نتیجه

با بررسی تهدیدات سایبری، راهبردها و اقدامات کشورهای گوناگون در فضای مجازی برای جلوگیری و محافظت از وقوع این‌گونه حملات علیه جمهوری اسلامی ایران باید به نکات زیر توجه کرد:

۱. تهدیدات سایبری منافع حیاتی جمهوری اسلامی ایران را هدف قرار داده‌اند و مقابله با آنها نیازمند راهبردی هوشمندانه و اقداماتی اساسی و هماهنگ و هوشمند است.

۲. راهبرد امنیت مجازی ایران باید به گونه باشد که به هماهنگی میان بخش‌های گوناگون منجر شود.

تهدیدات سایبری صرفاً علیه اهداف نظامی و امنیتی نیست. همه بخش‌های نظامی و غیر نظـامی در معـرض این حملات قرار دارند. مقابله با این تهدیدات از عهده یکی از این بخش‌ها بر نمی‌آید و چنین اقدامی نیازمنـد هماهنگی میان همه آنها است. چنانکه حملات ویروس استاکس نت به تأسیسات نطنز و فلیم به وزارت نفـت در سال‌های اخیر دلیل این ادعا می‌باشد.

۳. هر چند به ظاهر مقابله با تهدیدات سایبری اقدامی فنی و نیازمند متخصصان کامپیوتر و نـرم‌افزارهـای به روز است، اما در عمل بدون پشتیبانی مردمی، پذیرش آن از سوی اکثریت جامعه، وجـود رغبـت درونـی در هر کدام از شهروندان و کارگزاران دولتی و خصوصی نمی‌تواند قرین موفقیـت باشـد یـا در صـورت موفقیـت بسیار پر هزینه خواهد بود.

۴. راهبرد جمهوری اسلامی ایران بایـد در پـی تقویـت زیرسـاخت‌هـای علمـی و فنـی کشـور باشـد تـا آسیب‌پذیری‌ها را کاهش دهد. ترسیم حصارهای ملی در عرصه مجازی نمی‌تواند مانع تهدیدات سایبری باشد. همچنین استفاده مطلق از نرم افزارهای کشورهای پیشرفته در زمانی که مرزهای ملی هر روز بـیش از پـیش مورد تهدید قرار می‌گیرند، موجب افزایش حملات سـایبری خواهـد شـد. همـاهنگی بـا تحـولات و افـزایش توانمندی‌های خاص در این عرصه می‌تواند مفیدتر از راهبردهایی باشـد کـه منجـر بـه جداسـازی صـرف یـا وابستگی کامل خواهد شد.

۵. با توجه به آسیب‌پذیری کشورها در برابر حملات سایبری و اهمیت فوق‌العاده فضای امن مجازی بـرای همه آنها، جمهوری اسلامی ایران ضمن تقویت خود از گزنـد حمـلات سـایبری، بایـد بـه تـدوین یـک سـند راهبردی در آینده نه چندان دور اقدام ورزد. حمایت از فضای مجازی امـن یـک ارزش بـین‌المللـی بـه شـمار می‌آید و جمهوری اسلامی ایران باید سیاست خود را بر پایه حمایت از چنین فضایی پایه‌ریزی کند تا بتوانـد هـم فضای امنی برای فعالیت‌های خود بیابد و هم از آن برای نشان دادن نقـش مثبـت خـود در عرصـه بـین‌المللـی استفاده کند. مشروعیت‌سازی در عرصه فضای مجازی توسط جمهوری اسلامی ایران در نظام بـین‌الملـل زمـانی صورت خواهد گرفت که در عین حال که خود قربانی حملات سایبری است، خواسـتار حمایـت از فضـای امـن و قانونی شدن هر چه بیشتر این فضا باشد. بنابراین به لحاظ فنی، علمی، اخلاقی و راهبردی حمایت از فضای امـن برای همه کشورها، سیاستی اصولی و مفید به حساب می‌آید و باید آن را راهنمای عمل قرار داد.

منابع و مآخذ

۱. پور روستایی، محمدعلی، ۱۳۸۹، «جنگ با سلاح فناوری اطلاعـات»، ***خبرنامه الکترونیکی فناوری اطلاعات***، شماره اول.

۲. جهان بزرگی، احمد، ۱۳۸۸، «نقش امنیت اقتصادی در حفظ انقلاب اسلامی»، ***فصـلنامه علمـی ـ پژوهشـی مطالعات انقلاب اسلامی***، شماره ۱۶، بهار ۸۸.

۳. حسن بیگی، ابراهیم، ۱۳۸۳، ***حقوق و امنیت در فضای سایبر***، تهران، مؤسسه ابرار معاصر.

٤. زندی، محمدرضا، ۱۳۸۹، ***تحقیقات مقدماتی در جرائم سایبری***، تهران، جنگل.

۵. سلیمی، حسین، ۱۳۸٤، «دولت مجازی یا واقع‌گرایی تهاجمی: بررسی مقایسه‌ای نظریه ریچارد روزکرانس و جان مرشایمر»، ***مجله پژوهشی حقوق و سیاست***، شماره ۱۷، پاییز و زمستان ۸٤.

٦. عبدالله خانی، علی، ۱۳۸۳، ***نظریه‌های امنیت: مقدمه‌ای بر طرح ریزی دکترین امنیت ملی(۱)***، تهران، انتشارات مؤسسه مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران.

۷. عبدالله خانی، علی، ۱۳۸٦ ***جنگ نرم ۳: نبرد در عصر اطلاعات***، تهران، مؤسسه ابرار معاصر.

۸. قاضی‌زاده فرد، سیدضیاءالدین، ۱۳۸۷، ***فناوری اطلاعات و ارتباطات و مبانی سیستم‌های اطلاعاتی***، تهران، مؤسسه چاپ و انتشارات دانشگاه امام حسین﵇.

۹. کاکاوند، عباس، ۱۳۸۲، «حملات سایبری چالش جدید آمریکا»، ***نشریه رسالت***، شماره ۱۰.

۱۰. کلارک، یان، ۱۳۸٦، ***جهانی شدن و نظریه روابط بین‌الملل***، ترجمه فرامرز تقی لو، تهران، دفتر مطالعات سیاسی و بین‌المللی.

۱۱. مرادیان، محسن، ۱۳۸۷، «جنگ‌های اطلاعاتی و رایانه‌ای»، ***ماهنامه اطلاعات راهبردی***، شماره ٦۵.

۱۲. مشیرزاده، حمیرا، ۱۳۸٤، ***تحول در نظریه‌های روابط بین‌الملل***، تهران، سمت.

۱۳. نصیری، قدیر، ۱۳۸۳، ***روش و نظریه در امنیت پژوهی***، تهران، پژوهشکده مطالعات راهبردی.

14. Alexander, Keith, ***Advance Questions for Lieutenant General***.
15. USA Nominee for Commander, United States Cyber Command: www.armed-services.senate.gov/statement/2010/04.04-15-10.pdf.
16. Cyber Security Strategy of the United Kingdom-Cabinet Office: www.cabinetoffice.gov.uk/media/216620/css0906.pdf.
17. www.carlisle.army.mil/.../UK%20Cyber%20Security%20Strategy/1391/1/2.
18. David Baldwin(ed), ***Neorealism and Neoliberalism: The Contemporary Debate***, New York: Colombia University Press, 1993.
19. www.defense.gov/home/features/2011/0111_nsss//jan2011.
20. www.hamshahrionline.ir/print-122765.aspx, 1391/1/16.
21. www.number10.gov.uk/news/uk–france-summit-2010-declaration-on-defence-and-security cooperation /November 2010.
22. www.karbord.net/?content=DetailsArticle&id/90/9/21.
23. www.official-documents.gov.uk/document/cm76/7642/7642.pdf. Cyber Security Strategy of the United Kingdom safety, security and resilience in cyber space.
24. www.strategicreview.org/1389/03/11.
25. www.tebyan.net/newindex.aspx?pid=14047, 1390/8/9.