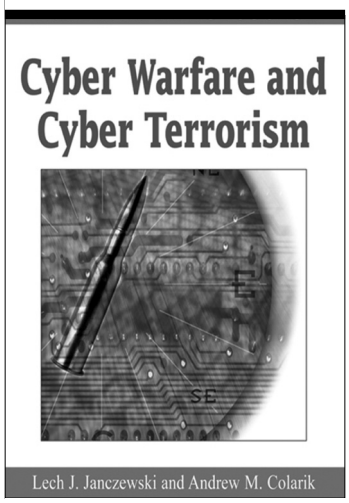
جنگ سایبری و تروریسم سایبری

نویسنده: لچ ج. جانزوسکی و آندرو م. کولاریک
معرفی و نقد: دکترحیدر علی بلوجی*

Lech J. Janczewski, Andrew M. Colarik, Cyber Warfare and Cyber Terrorism (United States and United Kingdom: Information science reference, 2006) pp. 565.



مقدمه

امروزه هیچ کشوری در دنیا نمی‌تواند خود را از حملات سایبری و تروریسم سایبری مصون بداند. این حملات اعم از این که توسط مراجع رسمی و یا حتی براساس ماجراجویی‌های شخصی صورت گرفته باشند، با استفاده از نرم افزارهای نفوذی سعی می کنند به اشکال مختلف و با تخریب و دستکاری داده‌ها به کشور هدف آسیب برسانند.

با توجه به تحولات چند سال اخیر شاید بتوان گفت که برای کشوری همچون جمهوری اسلامی ایران چنین برنامه هایی از مدت ها پیش راه‌اندازی و آغاز شده است. داستان حمله کرم استاکس نت به برخی مراکز صنعتی ایران در تیرماه گذشته آخرین نمونه از این نوع حملات بود که بازتاب جهانی داشت. البته ممکن است برخی جنگ سایبری را معادل جنگ نرم تلقی نمایند، در صورتی که جنگ و تروریسم سایبری، بخشی از جنگ نرم است و تمام آن نیست.

در چند سال اخیر، گزینه برخورد نظامی با جمهوری اسلامی ایران در دستور کار قدرت‌های خارجی مخالف قرار داشته و امکان اتخاذ این گزینه، هنوز مد نظر رهبران این کشورها می‌باشد. از جمله، جرج بوش، رئیس جمهور سابق امریکا در کتاب خاطرات خود که اخیراً آن را منتشر کرده، به اعتقاد خود نسبت به حمله نظامی به ایران اشاره می‌کند. مقامات فعلی امریکا نیز به کرات و با صراحت به تهدید نظامی ایران پرداخته‌اند. لازم به ذکر است تهدیدهای نظامی ایران منحصر به کشور و مقامات امریکایی نبوده، بلکه سران رژیم اسرائیل و برخی از قدرت‌های اروپایی نیز امریکایی‌ها را در این تهدیدات همراهی کرده‌اند.

وقتی حمله فیزیکی و جنگ واقعی در دستور کار یک کشور قرار گیرد، با توجه به مزایا و هزینه‌های کمتر جنگ نرم و از جمله جنگ و تروریسم سایبری نسبت به جنگ واقعی، این گزینه زودتر از گزینه حمله نظامی در دستور کار قرار می گیرد. چنانچه اهداف کشور مهاجم از این طریق حاصل نشد، توسل به جنگ در مرحله بعدی مورد توجه قرار می گیرد. بنابراین می توان گفت جنگ سایبری مقدمه‌ای برای جنگ واقعی است. به

* دکترای روابط بین الملل و کارشناس ارشد وزارت امور خارجه

ویژه، اگر به یاد بیاوریم با وجود محدودیت‌ها و مسئولیت‌های بین‌المللی جنگ مسلحانه و خسارات احتمالی که برای خود طرف مهاجم نیز متصور است، راه‌اندازی جنگ سایبری با این محدودیت‌ها همراه نیست.

با توجه به مطالب فوق، شناخت و کسب آمادگی برای مقابله با جنگ سایبری برای تمام کشورها از اهمیت حیاتی برخوردار است. در این راستا، مراکز تحقیقاتی مختلف دنیا و صاحب‌نظران مسائل استراتژیک به بررسی این موضوع پرداخته و علاوه بر تبیین عناصر و مکانیسم‌های مختلف آن به ارائه راه‌حل‌های مختلف برای مقابله و برخورد با حملات مزبور می‌پردازند.

یکی از منابع وزین ادبیات مربوطه، کتاب حاضر است که توسط ۸۶ نفر از محققین صاحب نظر که برخی از آنها سابقه پست‌های اجرایی نیز داشته‌اند، از کشورهای مختلف و زیر نظر لیک جان ژویسکی، استاد دانشگاه آکلند نیوزیلند، و آندور مک کولاریک، استاد دانشگاه امریکایی، در سال ۲۰۰۶ توسط انتشارات آی.اس.آر در امریکا و انگلیس منتشر شده است. این کتاب علاوه بر مقدمه، شامل هفت بخش و ۵۴ مقاله بوده و در ۵۶۵ صفحه به رشته تحریر درآمده است. ما علاوه بر معرفی محتوایی هر کدام از بخش‌ها به نقد و ارزیابی کلی این کتاب می‌پردازیم. شایان ذکر است هر چند روال معمول نقد و معرفی کتاب، ارائه تصویری از هر مقاله می‌باشد، اما با توجه به تعداد زیاد مقالات، تمرکز بر هر کدام از آنها موجب اطاله بیش از حد و غیر ضروری خواهد شد، در نتیجه در عین تلاش برای پوشش کامل معرفی کتاب، از معرفی هر مقاله به طور مستقل خودداری می‌گردد.

معرفی محتوایی

بخش اول کتاب شامل مطالبی درباره مفهوم و تعریف دو عبارت جنگ سایبری و تروریسم سایبری می‌باشد. در تعریف این مفاهیم گفته می‌شود تروریسم سایبری اقدامات سیاسی از قبل برنامه‌ریزی شده علیه اطلاعات، داده‌ها، سیستم‌ها و برنامه‌های کامپیوتری و با استفاده از ابزارهای مشابه توسط عوامل مختلف است. حملات اینترنتی از رایج‌ترین شیوه‌های تروریسم سایبری است. اهداف بالقوه تروریسم سایبری شبکه‌های کامپیوتری دولتی، شبکه هاب مالی و نیروگاه‌ها و غیره را شامل می‌شود. در این موارد، اطلاعات سیستم‌های هدف دستکاری، تغییر و مجدداً نگاشته شده و با نصب برنامه‌های ویروسی، عملکرد شبکه را مختل می‌کنند. بدیهی است با توجه به بستر اقدامات تروریستی (اینترنت) در این موارد، تروریست‌ها با هکرها تفاوت دارند- با بهره برداری از دانش و اطلاعات خود به عنوان ابزار قدرت، توان خود را در مقابل نهادهای قدرت مستقر به رخ می‌کشند. حملات تروریستی سایبری اخیر، این ادعا را تأیید می‌کنند. در یک عملیات تروریستی سایبری، بیت و بایت[1] حکم گلوله و بمب را در یک جنگ واقعی دارند؛ چرا که هر دو، زیر ساخت‌ها را بیشتر از روبناها هدف قرار می‌دهند، زیرا در صورت آسیب دیدن زیرساخت‌ها، امنیت کشور هدف بیشتر آسیب می‌بیند.

در مقابل حملات تروریستی سایبری، راه‌های مختلفی برای حفاظت از داده‌ها و دارایی‌های ارزشمند از جمله مخفی کردن اطلاعات[2] وجود دارد. اما شیوه‌ها مزبور نیز دارای کاربرد دوگانه بوده و تروریست‌ها نیز می‌توانند در لوای این برنامه‌ها خود را مخفی کنند. حتی اینترنت نیز می‌تواند در خدمت تروریست‌ها قرار بگیرد. در این راستا، از رمزنویسی[3] نیز برای جلوگیری از نفوذ دشمن استفاده می‌کنند. در این شیوه کلمات با استفاده از نمادهای مخصوص رمزگذاری شده و تنها اشخاص مجاز و با استفاده از کلید رمز می‌توانند رمزگشایی نمایند.

با توجه به دسترسی تقریباً همگانی به کامپیوتر و اینترنت در سراسر جهان که خطر حملات کامپیوتری و آسیب پذیری سازمان‌های دولتی را افزایش می‌دهد، ارائه دهندگان خدمات مربوطه می‌بایست با استفاده از

1. Bit and Byte
2. Steganography
3. Cryptography

شیوه‌های دفاعی و حتی تهاجمی، در مقابل هر حمله و یا برنامه حمله، مقاومت کنند. در این صورت، اعتماد به این سرویس دهندگان افزایش خواهد یافت.

بخش دوم به بررسی پویایی و تحول جنگ سایبری و تروریسم سایبری می‌پردازد. یکی از مسائل مهم، رابطه متقابل امنیت سایبری با اقتصاد است. به عبارت دیگر، در حالی که برای مهاجمان سایبری، رسیدن به اهداف اقتصادی مورد نظر حائز اهمیت است؛ برای طرف مقابل نیز تأمین هزینه‌های تقویت امنیت سایبری حائز اهمیت است. با وجود افزایش خطر حملات سایبری، به خصوص حملات پوششی و مخفیانه علیه موسسات مالی، که فعالیت روزافزونی در زمینه تجارت الکترونیکی دارند، هنوز موافقت نامه بین المللی خاصی برای مقابله با این حملات تدوین نشده است. مقررات محدودکننده فعالیت‌های دستگاههای نظارتی، عملاً به عنوان سنگری برای ادامه حیات تروریست‌های سایبری، از سوی آنان مورد سوءاستفاده قرار می گیرد.

علاوه براین، تله‌گذاری‌های کامپیوتری برای وسوسه مهاجمین به حمله به منظور شناسایی و بررسی شیوه‌های حمله آنها آغاز شده است. ابزار دیگری که برای کاهش زمینه‌های حملات سایبری موثر است، توجه به اخلاقیات و برجسته کردن آسیب‌های اجتماعی ناشی از این حملات است. با آگاه‌سازی مردم برای محافظت بیشتر از اطلاعات شخصی خود، مهاجمین احتمالی نیز از دست زدن به حمله منصرف می‌شوند. یکی از راههای مهم مورد استفاده توسط تروریست‌های سایبری، جمع آوری اطلاعات جانبی از سازمان هدف می‌باشد، لذا هشدارهای لازم برای خودداری پرسنل از دادن هرگونه اطلاعات، باید جدی گرفته شوند. عمق چنین حوادثی چنان زیاد است که برخی معتقدند مهاجمین سایبری را مثل جنایتکاران جنگی باید مجازات کرد.

بخش سوم کتاب به ابعاد انسانی حملات سایبری اختصاص دارد. نویسندگان مقالات این بخش معتقدند تروریست‌های سایبری علاوه بر اقدامات مخرب خود، با استفاده از دانش و مهارت‌های فنی در فعالیت‌های غیرآمجاز دیگر و از جمله پول‌شویی و یا تبلیغات ایمیلی دست دارند و یا با استفاده از ویروس‌های مختلف و از جمله اسب تروجان به تخریب نرم‌افزارها و نیز جاسوسی صنعتی می‌پردازند. در این شرایط، یکی از بهترین ابزارهای مقابله و کنترلی، استفاده از نرم‌افزارهای نظارتی بر فعالیت‌ها و کامپیوترهای کاربران می‌باشد. در این زمینه، اهمیت مهندسی اجتماعی به معنی هدایت کردن افکار و رفتار مردم توسط مدیران جامعه و آگاه‌سازی بیشتر مردم، نقش مهمی در مقابله و کنترل حملات ایفا می‌کنند. در صورت بی توجهی به این موضوع مهم، پرسنل و اجزای یک سیستم، الزام چندانی برای رعایت مقررات احساس نخواهند کرد. بر این اساس، در می‌یابیم نقش فردی اجزای سیستم برای جلوگیری از هر گونه حمله بسیار مهم است.

در بخش چهارم، موضوع ابعاد فنی تروریسم سایبری مورد بررسی قرار گرفته است. باید بدانیم یکی از راههای عملی حملات سایبری، کمین کردن تروریست‌ها با استفاده از تکنولوژی‌های پیشرفته است. امکان مخفی شدن زیر اسم‌های مختلف نیز به این امر کمک می‌کند. باوجود این، کمین کردن تروریست‌ها کمتر مورد توجه قرار گرفته است. در این زمینه نیز، پیش‌بینی و پیش‌گیری نقش مهمی در کاهش خسارات خواهد داشت و این امر مستلزم تشکیل بانک اطلاعاتی از تمام حملات قبلی به منظور بررسی‌های کارشناسانه از تمام ابعاد آنها می‌باشد. متاسفانه تاکنون بانک اطلاعاتی قوی‌ای در این زمینه تشکیل نشده است. پیش‌بینی نیز باید براساس یک مدل و مبتنی بر سئوالات مختلف باشد تا امکان تجزیه و تحلیل از زوایای مختلف را فراهم آورد. البته، با توجه به این که تروریست‌های سایبری مثل هکرها حمله می‌کنند، امکان پیش‌بینی عملیات‌های احتمالی آنها زیاد است.

با استفاده از گزینه‌های مختلف می‌توان خسارت‌ها را تا حدود زیادی کاهش داد. بررسی اسپم‌ها[1] و نصب

1. Spam

آنتی‌اسپم‌های مناسب نیز در کاهش خسارات موثر است. با وجود اینکه سرویس‌دهندگان اینترنت و دریافت کنندگان ایمیل، به دریافت اسپم تمایلی ندارند، این امر در حجم انبوه هنوز هم ادامه دارد. عدم ارائه سرویس و خدمات اینترنتی به تروریست‌های شناخته شده نیز گزینه دیگری در این زمینه است. هر چند که این گزینه، تبعات و محدودیت‌هایی نیز برای استفاده‌کنندگان صحیح از اینترنت و از جمله شرکت‌های تجاری می‌تواند داشته باشد. شایان ذکر است مسئولیت مقابله در برابر حملات سایبری تنها بر عهده سرویس‌دهندگان اینترنتی نیست، بلکه سازمان‌ها و مراجع دیگر نیز باید به طرق مختلف و از جمله ردیابی و تعقیب تروریست‌ها، متخصصین اینترنتی را در نظارت مداوم بر روندها و عملکردها و به خصوص زیرساخت‌های مهم، همراهی کنند. پیشرفت‌ها و امکانات امروزی همچون امکان کسب اطلاعات از راه دور و از طریق ماهواره‌ها، فرصت‌های موازی را برای نهادهای مستقر و تروریست‌ها فراهم می‌کنند و هر کدام که برنامه‌ریزی بهتر و تلاش بیشتری بکنند، موفق‌تر خواهند بود.

بخش پنجم به تشخیص هویت و اجازه دسترسی به کاربران اینترنت اختصاص دارد و در ابتدای بحث با تمرکز بر روش‌ها و فلسفه مورد علاقه هکرها، به تفاوت میان آنها و دزدان تجاری می‌پردازد. از نظر آنها، هکرها نه تنها به اینترنت لطمه‌ای نمی‌زنند بلکه به اخلاقیات پایبند بوده و تنها به عنوان یک منتقد، ضعف سیستم‌های امنیت را نشان می‌دهند. این نقدها، باعث پیشرفت سیستم‌های مزبور می‌شوند. از نظر صاحب‌نظران، نظارت و کنترل کاربران و صدور مجوز کاربری هیچ مغایرتی با حفظ حریم شخصی و حق دسترسی به اطلاعات ندارد و فراتر از آن زمینه‌های خطر را کاهش می‌دهد. در این راستا، نصب نرم‌افزارهای شناسایی کاربران و به تبع آن تفکیک سوءاستفاده‌کنندگان از تکنولوژی اطلاعات، تحلیل محتوایی و کنکاش دائمی عرضه و تقاضای اطلاعات و طبقه بندی آنها و محلی کردن ارائه خدمات اینترنتی و داشتن اطلاعات تماس کاربران توصیه شده است.

شایان ذکر است مسئولیت، دقت عمل و کارآمدی سازمان‌های دولتی برای حفظ ایمنی و امنیت دنیای سایبری نسبت به بخش خصوصی بسیار حایز اهمیت است. از نظر فنی نیز تمرکز بر فایل‌های صوتی و تصویری بسیار مهم‌تر و عملا پیچیده تر از فایل‌های مکتوب و نوشتاری است و نظارت و کنترل آنها مستلزم روش‌های دیگری است.

در بخش ششم، ادامه فعالیت‌های اینترنتی توضیح داده شده و اینکه نمی‌توان به خاطر ریسک حملات سایبری، این فعالیت‌ها را محدود یا متوقف کرد. یکی از فرصت‌هایی که برای تروریست‌ها در فضای سایبری به وجود می‌آید، اوضاع آشفته‌ای است که در ارائه کمک‌های اضطراری به قربانیان حوادث و بلایای غیرمترقبه بر قرار می‌شود. تقریباً در تمام حوادث سال‌های اخیر از حادثه یازده سپتامبر ۲۰۰۱ گرفته تا سونامی سال ۲۰۰۴ و طوفان کاترینا در سال ۲۰۰۵ ، حملات اینترنتی افزایش یافته‌اند. لذا در مدیریت بحران‌ها، علاوه بر لزوم حساسیت سازمان‌های ذیربط باید مدل خاصی را برای مقابله با حملات سایبری در شرایط مزبور در نظر بگیرند. به طور طبیعی، می‌توان از مزایای این مدل‌ها در بحران‌ها و در مناطق دیگر نیز بهره‌برداری کرد.

استفاده از روش‌های کارآگاهی و مبادله اطلاعات در سطح بین‌المللی مثل طرح اشلون که توسط امریکا و متحدین آن برای ضبط کلیه ارتباطات الکترونیکی شامل مکالمه‌های تلفنی، دریافت و ارسال فکس و ایمیل و نیز تبادل اطلاعات لازم طراحی و اجرا شده است- و استفاده از زبان و علائم مشترک در سطح بین‌المللی، در عین رعایت ملاحظات اجتماعی و رفتاری در سطح یک جامعه، برای شناسایی مجرمینی که به راحتی می‌توانند هویت واقعی خود را مخفی کرده و خود را به اسم دیگری معرفی کنند، لازم است.

نکته بسیار مهم در جنگ سایبری، تکیه بر تاکتیک‌ها

و استراتژی‌هایی است که در جنگ‌های واقعی و در رابطه با سلاح‌های متعارف و غیرمتعارف در جریان است. به عنوان مثال، همچنان که در استراتژی‌های بازدارندگی، توان ضربه اول و دوم شرط بقا در یک درگیری هسته‌ای تلقی می‌شود؛ چنین وضعیتی در دنیای سایبری نیز قابل تصور است و کشورها می‌بایست به توان بقا پس از دریافت حملات سایبری، توجه ویژه‌ای داشته باشند.

در بخش هفتم و آخر کتاب، مقابله با حملات و تروریسم سایبری در سطح ملی و بین‌المللی مورد بررسی قرار گرفته است. البته، در بعد انفورماتیک و سیستم‌های امنیتی مربوطه، همان شکاف بین کشورهای پیشرفته و در حال توسعه مشهود است؛ لذا گروه اول در این زمینه نیز نسبت به گروه دوم جلوتر هستند. با وجود این، حملات سایبری تنها دارایی‌های این کشورها را هدف قرار نمی‌دهد، اتفاقاً آنها چون به سیستم‌های امنیتی پیشرفته‌تری مجهز هستند، آسیب‌پذیری‌شان کمتر است آنچه در این کشورها، به نوعی محدودکننده می‌باشد، وجود مقررات زیاد در حمایت از حقوق شهروندی و لزوم برخورد قانونی با تبهکاران می‌باشد که در برخی مواقع، سازمان‌های مسئول را از برخورد سریع نسبت به خطرات بازداشته است. در نتیجه، ایجاد تعادل در پاسخگویی به تهدیدات مزبور هم در سطح ملی و هم در سطح بین‌المللی الزامی است. در این زمینه، برخی سازمان‌های منطقه‌ای مثل اتحادیه اروپایی ابتکاراتی برای مقابله با جرایم اینترنتی داشته‌اند؛ اما تا زمانی که این ابتکارات، بین‌المللی و جهانی نشوند، خطر حمله تروریست‌های سایبری وجود خواهد داشت.

دولت امریکا و به خصوص آژانس امنیت ملی این کشور نیز برخورد با این حملات را در دستورکار تمام سازمان‌های ذیربط و حتی ارتش این کشور قرار داده و امروزه افسران ویژه‌ای در ارتش امریکا برای انجام وظیفه در مقابل حملات اینترنتی آموزش داده می‌شوند. در این راستا، یک هدف مهم ارتش امریکا کسب برتری اطلاعاتی، عملیاتی و تکنولوژیکی نسبت به تروریست‌ها است.

نقد و ارزیابی

همانگونه که از محتوای کتاب مشخص است، بحث حملات سایبری یک بحث فنی و تخصصی است که درک و کاربرد آن برای مخاطبین خاص نظیر سازمان‌های دولتی و محققین و صاحب‌نظران محافل آکادمیک و فعالان خصوصی در عرصه انفورماتیک امکان‌پذیر می‌باشد. در این کتاب نیز همین متخصصین از زوایای مختلف به تجزیه و تحلیل و ریشه‌یابی تهدید جنگ و تروریسم سایبری و راههای مقابله با آن پرداخته‌اند.

این کتاب را می‌توان تحقیقی توام با رویکرد بنیادی و کاربردی دانست که در عین تمرکز بر بعد نظری این مشکل، به طور گسترده به مسائل عملی نیز می‌پردازد. سوابق علمی و اجرایی نویسندگان مقالات نیز به خوبی به غنای مطالب ارائه شده کمک کرده است. در عین حال با توجه به اینکه جنگ و تروریسم سایبری یکی از معضلات و تهدیدات امنیتی جاری در نظام بین‌الملل محس.ب می‌شود، اهمیت نقش و کمک مباحث این کتاب برای تأمین و تقویت امنیت بین‌المللی بسیار روشن است.

یک ویژگی مهم این کتاب بهره‌گیری از مفاهیم و نظریات رایج در دیگر زمینه‌های علمی و فکری و از جمله مفاهیم رایج در اقتصاد و یا بحث‌های استراتژیک و کاربرد آنها در جنگ و تروریسم سایبری است که به فهم آسان مباحث کمک می‌کند.

با ملاحظه موارد فوق می‌توان گفت این کتاب می‌تواند یکی از منابع مرجع برای آموزش، در دانشگاهها و در مراکز اجرایی مورد استفاده قرار گیرد. بنابراین مطالعه تفصیلی آن هم برای محققین و هم مسئولین و دست‌اندرکاران سازمان‌های اجرایی ذیربط پیشنهاد می‌گردد. ترجمه و انتشار آن نیز کمک مهمی به غنای ادبیات مربوطه در کشورمان خواهد بود.