امنیت سایبری

و

جنگ سایبری

ترجمه و تألیف:

علی اصغر جعفری لاری

انتشارات پندار پارس

سرشناسه : سینگر، پیتر وارن، ۱۹۷۴ - م.
(Singer, P. W. (Peter Warren
عنوان و نام پدیدآور : امنیت سایبری و جنگ سایبری
مشخصات نشر : تهران : پندار پارس ، ۱۳۹۴.
مشخصات ظاهری : ۱۸۶ ص.: مصور
شابک : 978-600-6529-76-9: ۱۴۰۰۰۰ ریال
وضعیت فهرست نویسی : فیپای مختصر
یادداشت : فهرستنویسی کامل این اثر در نشانی: http://opac.nlai.ir قابل دسترسی است
یادداشت : عنوان اصلی: cyberwar Cybersecurity and.
یادداشت : کتابنامه
شناسه افزوده : جعفری لاری، علی‌اصغر، ۱۳۶۷ -
شماره کتابشناسی ملی : ۳۸۰۲۰۴۲

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱٤، واحد ۱٦ **www.pendarepars.com**
تلفن: ٦٦٥٧٢٣٣٥ – تلفکس: ٦٦٩٢٦٥٧٨همراه: ۰۹۲۱٤۳۷۱۹٦٤ **info@pendarepars.com**

نام کتاب : امنیت سایبری و جنگ سایبری
ناشر : انتشارات پندار پارس
ترجمه و تألیف : علی اصغر جعفری لاری
چاپ نخست : اردیبهشت ۹۴
شمارگان : ۵۰۰ نسخه
چاپ، صحافی : چاپ دیجیتال روز
قیمت : ۱۴۰۰۰ تومان شابک : ۹-۷۶-۶۵۲۹-۶۰۰-۹۷۸

فهرست

پیش‌گفتار

هدف از نگارش این کتاب

توجه به امنیت سایبری در دنیای امروز، همواره مهم و ضروری است. افزایش روزافزون حملات، آسیب‌پذیری‌ها، گروه‌های هکری و ارتش‌های مختلف سایبری، امنیت فضای مجازی را تا حدودی متزلزل کرده است.

کشورهای مختلف، سرمایه‌گذاری‌های هنگفتی را صرف امنیت سایبری می‌کنند تا بتوانند از مرزهای اطلاعاتی خود به‌درستی محافظت و دفاع کنند. در برابر توجه به امنیت سایبری، جنگ سایبری هم امروزه باعث بوجود آمدن خسارت‌های فراوانی به دولت‌ها، سازمان‌ها، شرکت‌ها و حتی کاربران شده است.

این امر مهم است که ما هم همچون سربازان جنگی برای حفاظت از اطلاعات در دنیای مجازی با آگاهی و ارتقاء دانش خود، کمک چشم‌گیری به دولت و کشور خود داشته باشیم. بارها به این اشاره کرده‌ایم که امنیت مطلق نیست. فضای مجازی با دارا بودن مزیت‌های خود، ناامن‌تر از آن است که فکر می‌کنیم. برای آشنایی با مسائل مربوط به سایبری و آگاهی از پشت پرده‌های امنیت سایبری و جنگ سایبری، این کتاب به اندازه کافی مفید و جذاب است.

مرجع و اساس کتاب حاضر، کتابی با عنوان "CyberSecurity And CyberWar" نوشته‌ی P.W Singer و Allan Friedman است. تلاش کرده‌ام در بخش‌هایی از کتاب حاضر، مطالبی را از کتاب "CyberSecurity And CyberWar" بیاورم و عناوین برخی از مباحث را مطابق با کتاب مذکور مطرح نمایم. انتخاب این کتاب برای ترجمه‌ی برخی از قسمت‌ها، نوین بودن مطالب آن با توجه به تاریخ انتشار کتاب یعنی سال ۲۰۱٤، تایید افراد مهمی که این کتاب را خوانده‌اند و نظرات خود را داده‌اند و از همه مهم‌تر اهداف زیر می‌باشد:

نخستین، در اولویت بودن و اهمیت داشتن امنیت سایبری بوده است. بهتر است از کتب مختلف که به‌صورت فنی به مباحث هک و امنیت می‌پردازند، کمی فاصله بگیریم و به دیدگاهی بیاندیشیم که کمتر به آن پرداخته شده است و آن چیزی نیست جز "امنیت سایبری و جنگ سایبری". نه تنها پژوهشگران و دانشجویان ما نیاز به چنین کتب جدید و مفیدی دارند بلکه مدیران و کارشناسان ارشد و حتی کاربران نیز باید با مسائل مربوط به حوزه سایبر، آگاهی و دانش کاملی داشته باشند و این نیازمندی، هدف دوم در تالیف این کتاب با توجه به امنیت فضای مجازی کشور و تجربیات بیش از ده ساله مترجم در این حوزه، بوده است.

به‌طور خلاصه می‌توان گفت اگر قصد ورود به اینترنت را دارید، باید دانش خود را در حوزه امنیت افزایش دهید؛ وگرنه قربانی نفوذگری‌ها و حملات سایبری خواهید شد. درک اینکه دشمنان‌تان چه کسانی هستند و به چه شیوه‌هایی شما را مورد حمله قرار می‌دهند می‌توانند در دفاع از آنها و حتی پاسخ به حملات آنها موثر واقع شود. مهم‌تر از کاربران، دولت‌ها هستند که باید افزون بر صرف هزینه‌های مختلف در ایمن‌سازی زیرساخت‌ها، به هکرها و نخبه‌های علمی بها دهند تا بتوانند با مهارت‌های خود جلوی حملات سایبری دشمنان ایستادگی کنند.

بیشتر جنگ‌های سایبری با اهداف سیاسی و اقتصادی صورت می‌گیرد. در جنگ‌های سایبری تمرکز بر نفوذ به یک کاربر خاص نیست، بلکه مهم‌تر از همه، کسب اطلاعات است و آن هم از کشورها. در دوره کنونی، رهگیری پهپادها، محافظت از زیرساخت‌ها و ایمن‌سازی در مقابل هک سیستم‌های ناوبری، ایمن‌سازی وب‌سایت‌ها و پایگاه‌ها، محافظت در برابر اطلاعات سازمان‌ها و نیروهای انسانی (به‌ویژه مدیران ارشد) و دفاع در برابر نفوذگری‌ها به سیستم‌های SCADA برای کشورها از اهمیت بسیار بالایی برخوردار است.

با توجه به آنچه که گفته شد، امید است کتاب حاضر، پنجره‌ای جدید را برای آشنایی با امنیت سایبری و جنگ سایبری و همچنین ایده‌پردازی در این حوزه برای شما باز کند.

سخنی درباره‌ی مرجع اصلی این کتاب

همان‌گونه که گفته شد، مرجع و اساس کتاب حاضر، برگرفته از کتاب "CyberSecurity And CyberWar" نوشته‌ی P.W Singer و Allan Friedman است. این بدان معنا نیست که تمام و کمال این کتاب، ترجمه شده‌ی کتاب مذکور است بلکه به این معناست که از لحاظ تشابه دیدگاه و تفکر مترجم با نویسندگان کتاب "CyberSecurity And CyberWar" و همچنین، نوین بودن مطالب و اهداف مترجم، کتاب مذکور به عنوان مرجع و اساس کتاب "امنیت سایبری و جنگ سایبری"، انتخاب شده است و ذکر عنوان کتاب انگلیسی به دلیل احترام به حقوق مادی و معنوی نویسندگان کتاب بوده است.

بهتر است درباره‌ی آنچه که موجب شد نویسندگان کتاب "CyberSecurity And CyberWar" چنین کتابی را بنویسند کمی صحبت کنیم. نویسندگان کتاب در ابتدای کتاب خود می‌نویسند:

در اتاق کنفرانس Washington DC نشسته بودم. سخنران، یکی از رهبران ارشد وزارت دفاع ایالات متحده بود. موضوعی که او به آن پرداخته بود این بود که چرا او فکر می‌کند امنیت سایبری[1] و جنگ سایبری[2]

---

[1] Cybersecurity
[2] Cyberwar

بسیار مهم است و با این حال، هنگامی‌که او مسائل سایبری را شرح می‌داد، ناخواسته ما را به نوشتن این کتاب متقاعد ساخت.

هر دو ما (نویسندگان اصلی کتاب یعنی Peter Warren Singer و Allan Friedman)، دهه‌ی سی هستیم و هنوز هم نخستین کامپیوتری را که استفاده کردیم، به یاد داریم. برای Allan پنج‌ساله، آن اوایل مکینتاش اپل در خانه‌اش در شهر Pittsburgh بود. فضای دیسک این کامپیوتر آن‌قدر محدود بود که نمی‌توانست حتی فایل الکترونیکی این کتاب را در حافظه‌ی خود جای دهد. Peter هم هفت‌سالگی با دنیای داشتن یک کامپیوتر روبه‌رو شد.

سه دهه بعد، کامپیوتر، مرکزیت زندگی ما را در بر گرفت به‌طوری که نمی‌توانستیم به غیر از "کامپیوترها" به چیز دیگری فکر کنیم. ما با ساعت کامپیوتری از خواب بیدار می‌شدیم، دوش آب‌گرمی می‌گرفتیم که توسط کامپیوتر گرم شده بود، قهوه را در کنار کامپیوتر می‌خوردیم، بلغور جو گرم شده با کامپیوتر را می‌خوردیم و سپس به محل کار با خودرویی رانندگی می‌کردیم که توسط صدها کامپیوتر کنترل شده بود. بیشتر روزمان صرف فشار دادن دکمه‌های کامپیوتر می‌شد. با این حال، شاید بهترین راه برای دور بودن از دنیای مدرن کامپیوترها، پایان روز بود یعنی دراز کشیدن روی تخت و خاموش کردن چراغ‌ها.

این دستگاه‌ها هنوز در همه جا فراگیر نشده بودند. کامپیوترهایی که ما از آن استفاده می‌کردیم برای بچه‌های کوچک بود. تنها نسل پیشین اینترنت، کمی بیشتر از یک ارتباط بین چند محقق دانشگاهی بود. نخستین "پست‌الکترونیکی" در سال ۱۹۷۱ فرستاده شده بود. فرزندان این دانشمندان، هم‌اینک در جهانی زندگی می‌کنند که تقریبا چهل تریلیون پست‌الکترونیکی هر ساله فرستاده می‌شود. نخستین "وب‌سایت" در سال ۱۹۹۱ ساخته شده بود. تا سال ۲۰۱۳، بیش از ۳۰ تریلیون صفحه‌ی وب منحصربفرد ساخته شده است.

افزون بر این، اینترنت دیگر تنها به ارسال پست‌الکترونیکی یا جمع‌آوری اطلاعات خلاصه نمی‌شود: اینترنت هم‌اینک همه چیز را، از ارتباط نیروگاه‌های برق تا پیگیری خرید عروسک باربی را در خود جای داده است. در واقع، سیسکو[1]، شرکتی که بسیار به اجرای اجزای پایانی اینترنت کمک شایانی کرد، برآورد کرد که ۸.۷ میلیارد دستگاه به اینترنت تا پایان سال ۲۰۱۲ متصل شده بودند. باور داریم که تا سال ۲۰۲۰ –همانند خودروها، یخچال‌ها، دستگاه‌های پزشکی و ابزارهایی که در تصور مخترع آن نمی‌گنجید که روزی آن‌قدر افزایش یابند– حدود ۴۰ میلیارد کامپیوتر به اینترنت متصل خواهند شد. به‌طورخلاصه، در حوزه تجارت که ارتباطات به زیرساخت‌های حیاتی مرتبط است و قدرت تمدن امروز ماست، این حوزه نیز به شبکه‌ی جهانی از شبکه‌ها تبدیل شده است.

[1] Cisco

اما با ظهور "تمام مسائل مربوط به سایبری"، این مسئله بسیار مهم تلقی شد ولی به‌طور باور نکردنی تاریخچه‌ی کوتاه کامپیوترها و اینترنت را به یک نقطه‌ی تعریف رساند. تنها با صعود دامنه‌ی سایبری، با سرعت و اغلب با عواقب غیرمنتظره، ناهمواری‌ها به دامنه‌ی فیزیکی رسید.

ما تعداد حیرت‌انگیزی از محدوده‌ی تهدیدها را که پشت "مسائل مربوط به سایبری" قرار دارد، کشف کردیم: ۹۷ درصد از ۵۰۰ شرکت ثروتمند، هک شده‌اند و بیش از یکصد پایگاه دولتی درگیر جنگ در حوزه آنلاین قرار گرفتند. این مشکلات پی‌درپی می‌تواند منشاء سیاسی و مسائل مربوط به آن باشد، از جمله رسوایی‌هایی مثل WikiLeaks و نظارت NSA، سلاح‌های سایبری مثل Stuxnet و قواعدی که شبکه‌های اجتماعی بازی می‌کنند و منجر به نگرانی حریم خصوصی اشخاص می‌شوند.

باوجود امید و اعتماد به عصر اطلاعات، ما نیز در زمان "اضطراب سایبری" قرار داریم. در یک بررسی که در جهان مطرح شد، مجله سیاست خارجه شرح داده بود که ناحیه سایبر "بزرگ‌ترین خطر در حال ظهورست"، درحالی‌که Boston Globe ادعا کرده بود هم‌اینک، اینجا "یک جنگ جهانی سایبری" در حال پیشرفت است که "به‌صورت خونین در سنگرهای دیجیتال" به اوج خود رسیده است.

وجود ترس بین کاربران و شرکت‌ها، کسب‌وکار امنیت سایبری را بزرگ و پررونق کرده است و یکی از سریع‌ترین صنایع در حال رشد در جهان را معرفی کرده است. همچنین باعث شده است که دفاتر دولتی جدید و نیروهای مسلحی مثل ارتش‌های سایبری را در سراسر جهان پدید آورد که ماموریت آنها، مبارزه با جنگ سایبری و پیروز شدن در فضای سایبری است.

همانطور که به آن اشاره خواهیم کرد، این جنبه‌های سایبری و خطرات آن در حال افزایش است و ما چگونه باید آن را درک و به خطرات آن پاسخ دهیم. Joe Nye رئیس سابق دانشگاه هاروارد اشاره کرده است که اگر کاربران، اعتمادشان را نسبت به ایمنی و امنیت اینترنت از دست دهند، از فضای مجازی عقب‌نشینی می‌کنند.

ترس در امنیت سایبری، به‌طورفزاینده‌ای تصورات ما را از حریم خصوصی به خطر می‌اندازد و باعث می‌شود که نظارت و فیلترینگ اینترنت، به‌طور رایج‌تر و قابل قبول‌تری در محل کار، خانه و در سطح دولتی صورت گیرد. تمام سازمان‌های ملی، بیش از حد به عقب رفته‌اند که این امر باعث تضعیف در مزایای حقوق انسانی و اقتصادی می‌شود که ما آن را از ارتباطات جهانی می‌بینیم. کشور چین هم‌اکنون شبکه شرکت‌های خود را در پشت "دیوارآتش بزرگی" توسعه داده است که اجازه می‌دهد پیام‌های دریافتی را مشاهده کنند و در صورت نیاز، کاربران را از اتصال به اینترنت جهانی محروم سازند. در یک مقاله در دانشکده‌ی حقوق دانشگاه Yale این‌طور اشاره شده بود که "همگرایی به یک طوفان کاملی تبدیل شده است که ارزش‌های آزادی، همکاری و نوآوری در اینترنت سنتی را تهدید می‌کند. همچنین حکومت و تبادل آزاد اندیشه‌ها را نیز محدود می‌کند."

[1] Cyberspace

این مسائل، عواقبی فراتر از اینترنت دارد. حس روبه‌رشد آسیب‌پذیری‌ها در دنیای فیزیکی به حملات سایبری در دنیای مجازی منتقل شده است. در گزارشی با نام "مسابقه‌ی جدید ارتش‌های سایبری" شرح داده شده بود که جنگ‌ها تنها با سربازان با اسلحه یا با هواپیماهای بمب‌افکن صورت نمی‌گیرد. آنها می‌توانند با فشردن کلیدها به‌روی صفحه‌کلید کامپیوتر طوری صورت گیرد که نیمی از جهان مختل شود و یا صنایع بحرانی مثل آب و برق، حمل و نقل، ارتباطات و انرژی از بین رود. چنین حملاتی می‌توانند شبکه‌های نظامی را غیرفعال کند که این امر می‌تواند باعث به کنترل درآوردن حرکت سربازان، مسیر جنگنده‌های جت و فرماندهی و کنترل کشتی‌های جنگی توسط دشمن شود."

چشم‌انداز چنین جنگی بدون صرف هزینه یا شکست فوری یا حوادث مشابه، کاملا وابسته به حملات سایبری است. واقعیت پیچیده‌تر از این حرف‌هاست و ما آن را در ادامه کتاب پوشش خواهیم داد. چنین چشم‌اندازی، نه تنها به درس‌ها دامن می‌زند بلکه به‌طور بالقوه منجر به نظامی کردن خود فضای سایبری می‌شود. این دیدگاه، حوزه‌ای را تهدید می‌کند که حجم انبوهی از اطلاعات، نوآوری و رفاه را ارائه می‌کند.

به‌طور خلاصه، هیچ موضوعی به اندازه‌ی امنیت سایبری مهم و ضروری نیست. با این حال، هیچ موضوعی وجود ندارد که "مسائل سایبری" را ضعیف درک کنیم.

دلیل وجود شکاف در دانش امنیت سایبری و چرایی اهمیت آن

" به ندرت چیزی بسیار مهم است و به همین ترتیب درباره‌ی شفافیت کمتر و درک کمتر امنیت سایبری صحبت می‌کنیم. من در جلسه‌ی یک گروه خیلی کوچک در واشنگتن نشسته‌ام... ما قادر نیستیم تصمیمی بگیریم چراکه فاقد تصویری روشن از پیامدهای بلند مدت حقوقی و سیاسی هر تصمیمی که ممکن است بگیریم، هستیم."

این سخنرانی ژنرال Michael Hayden، مدیر سابق CIA بود که در آن، شکاف دانش امنیت سایبری را مطرح کرده بود و خطرات آن را ارائه کرده بود. بخش عمده‌ای از این مشکلات، نتیجه‌ی فقدان تجربه‌ی اولیه کار با کامپیوتر یا نبود دانش امنیت سایبری بین بسیاری از مدیران است. جوانان امروز، "بومی‌های دیجیتالی" هستند؛ چراکه در جهانی رشد کرده‌اند که در آن، کامپیوترها وجود داشته‌اند و ویژگی‌های طبیعی آنها بارز بوده است. اما جهان، هنوز هم عمدتا توسط "مهاجران دیجیتالی" یا نسل مسن‌تر که مسائل مربوط به کامپیوترها و اینترنت برای آنها گیج‌کننده است، اداره و مدیریت می‌شود.

در اواخر سال ۲۰۰۱، مدیر FBI در دفتر خود یک کامپیوتر هم نداشت، در حالی که وزیر دفاع آمریکا به دستیار خود می‌گفت که پست الکترونیکی‌اش را چاپ کند و برای او ارسال کند. یک دهه بعد، وزیر امنیت داخلی آمریکا که مسئول حفاظت از تهدیدات سایبری کشور بود در سال ۲۰۱۲ در یک کنفرانس اذعان کرد که: "بخندید اما من هیچ‌وقت از آدرس پست‌الکترونیکی استفاده نمی‌کنم." به نظر او، آدرس

پست‌الکترونیکی مفید و سودمند نیست اما به نظر می‌رسد، ترس از امنیت، او را به استفاده نکردن از این سرویس مجبور کرده است.

البته این موضوع تنها به سن مربوط نیست و نمی‌توان این باور را داشت که کسی‌که جوان است به طور خودکار دارای درکی از مسائل کلیدی است. امنیت سایبری، یکی از حوزه‌هایی است که گرایش مدیریتی آن بیشتر از گرایش فنی‌اش است. هر چیزی که به صفر و یک دنیای دیجیتال مربوط است، موضوعی است که تنها برای دانشمندان کامپیوتر و کارشناسان فناوری اطلاعات بوده است.

نگرانی عمده‌ی بخش دولتی و خصوصی، جوانی است که با زرنگی و دانایی خود مشغول کار با کامپیوتر است. او، یک هکر یا نفوذگرست که اهداف مختلفی را در سر می‌پروراند. در کشور ما یعنی ایران، میانگین سنی بیشتر هکرها زیر ۲۵ سال است و این امر نشان‌دهنده‌ی جوان بودن گروه هکرها، دانش بالای جوانان ایرانی و توانمند بودن این دسته از افراد است.

خطرات گوناگونی در حوزه هک وجود دارد که ما در نوشتن این کتاب به آن نخواهیم پرداخت. هر یک از ما، نقشی را در زندگی بازی می‌کنیم و باید درباره‌ی امنیت سایبری که در آینده فراتر از جهان کامپیوترها، شکل می‌گیرد، تصمیم بگیریم. بیشتر ما این کار را بدون ابزار مناسب انجام می‌دهیم و از شرایط اساسی و مفاهیم ضروری این حوزه آگاهی زیادی نداریم.

این شکاف، پیامدهای گسترده‌ای به بار می‌آورد. یکی از ژنرال‌های آمریکایی شرح داد که "هم‌اینک درک سایبر، مسئولیت فرمانده است" و تقریبا در هر بخشی از جنگ سایبری تاثیر می‌گذارد. با این حال، یکی دیگر از ژنرال‌های آمریکایی گفت که:"کمبود واقعی، آموزه‌ها و سیاست‌ها در فضای سایبری جهان است." نگرانی او، تنها داشتن سمت نظامی لازم برای انجام کار بهتری در "حوزه سایبری" نبود بلکه در سمت غیرنظامی هم هیچ هماهنگی یا راهنمایی فراهم نشده بود. چنین شکافی امروز مثل زمان جنگ جهانی اول است، هنگامی‌که نظامیان اروپایی برنامه‌ریزی کردند که از فناوری‌های جدید مثل راه‌آهن استفاده کنند. مشکل این بود که آنها، رهبران غیرنظامی و مردم پشت سر آنها، درکی از این فناوری‌ها یا مفاهیم نداشتند و تصمیمات ناآگاهانه طوری گرفته می‌شود که سهوا سازمان‌ها در جنگ رانده می‌شدند. چنین شکاف‌هایی را می‌توان به اوایل جنگ سرد، سلاح‌های هسته‌ای و پویایی سیاسی که به خوبی درک نشد، شبیه دانست.

روابط بین‌المللی هم‌اینک به این مشکلات (که طرفین چه چیزی درک می‌کنند و چه چیزی می‌دانند) دچار شده است و نمونه بارز آن، موافقت‌نامه‌ی هسته‌ای بین دو کشور آمریکا و ایران بوده است که دو طرف درک و شناخت خوبی از محتوا نداشتند. از آنجا که نویسندگان کتاب حاضر، هر دو آمریکایی هستند به همین دلیل، مثال‌ها و "مسائل سایبری" بیشتر به این کشور مربوط می‌شود اما مترجم در تمام محتوای این کتاب آنچه که با حوزه سایبری داخلی مرتبط می‌شود را بدون اینکه تاثیر نادرستی به‌روی محتوای اصلی کتاب به جا گذارد، شرح می‌دهد.

سخن پایانی...

پس از سپاس و ستایش به درگاه پروردگار، از تمام دوستان و همکاران محترم از جمله مهندس حسین یعسوبی مدیر مسئول انتشارات پندار پارس که مهربانانه دست مرا در انجام این هدف مهم فشردند، تشکر و قدردانی می‌نمایم.

علی اصغر جعفری لاری

Http://parsing.ir

Http://securityadviser.ir

admin@parsing.ir

admin@securityadviser.ir