فهرست مطالب

فصل اول

فضای سایبر

فضای سایبر و ویژگی‌های آن

جنگ سایبر

ملزومات امنیت فضای سایبر

تهدیدات فضای سایبر

راهکارهای پیشنهادی برای امنیت فضای سایبر

1. فضای سایبر

Douglas Conner

نویسنده کتاب‌های معرف امنیت شبکه‌ها

Computer Networks and Interne
Internetworking with TCP/IP
The Internet Book
Internetworking with TCP/IP
Essentials of Computer Architecture
Automated Network Management
Business Data Communications
Wireless Communications
Cryptography and Network Security
ISDN and Broadband ISDN, …..

1.1. خلاصه فصل

فضای سایبر سرعت، کارایی و بهره وری این فناوری در انقلاب دیجیتال علاوه بر مزیت‌های بسیاری کـه بـه ارمغـان آورده، چالش‌های جدیدی را نیز برای امنیت و محرمانگی اطلاعات و ارتباطات در شبکه‌های جهانی اطـلاع رسـانی و اینترنت ایجاد نموده است.

از ویژگی‌های منحصر به فردی که فضای سایبر را از دیگر رسانه‌ها ممتاز می‌سازد، جهانی بودن آن است. هـر فـردی در هر نقطه از جهان می‌تواند از طریق آن به‌آسانی، به جدیدترین اطلاعات دست یابد. این فصل در رابطه بـا فضـای سایبر و جنگ‌های سایبری می‌باشد.

1.2. فضای سایبر

امروزه با توسعه روز افزون فناوری اطلاعات و ارتباطات، اهمیت و نقش اساسی آن در بافت اجتماعی آینده قابل ملاحظه است. فناوری اطلاعات، محاسن بسیاری را چون سرعت، دقت، کیفیت، ایجاد شفافیت، ایجاد دسترسی و ... به همراه می‌آورد. شواهد و قراین، حاکی از آن است که کشورها ناگزیر از توسعه فناوری اطلاعات و ارتباطات هستند. امروزه فناوری اطلاعات و ارتباطات به یک زیر ساخت حیاتی برای کشورها در کنار انرژی، سوخت، غذا، حمل و نقل و .... تبدیل شده است و شرایط جدیدی را به وجود آورده که به آن فضای سایبر گویند. این فناوری روش ارتباط و تعامل انسان ها را به صورتی بنیادین دگرگون نموده است که به عنوان نمونه میتوان به کار از راه دور، پزشکی از راه دور، تجارت الکترونیک، آموزش از راه دور و دانشگاه مجازی، قضاوت از راه دور و بسیاری موارد دیگر اشاره کرد.

سرعت، کارایی و بهره وری این فناوری در انقلاب دیجیتال علاوه بر مزیت‌های بسیاری که به ارمغان آورده، چالش‌های جدیدی را نیز برای امنیت و محرمانگی اطلاعات و ارتباطات در شبکه‌های جهانی اطلاع رسانی و اینترنت ایجاد نموده است. عدم توجه کافی به این چالش ها و به عبارتی تمرکز بر توسعه انفعالی فناوری اطلاعات و ارتباطات بدون توجه به همه ابعاد آن، میتواند در درازمدت زیان‌های جبران ناپذیری را بر کشور تحمیل کند. پدیده هایی مثل جنگ سایبر و همچنین وابستگی اطلاعاتی و تکنولوژیکی ناشی از توسعه فناوری اطلاعات به کشورهای دیگر می‌تواند امنیت ملی را به مخاطره بیاندازد.

سایبر واژه‌ای است بر گرفته از لغت «kybernetes» به معنای سکاندار یا راهنما. نخستین کسی که واژه فضای سایبر را به کار برد، ویلیام گیبسون[1] نویسنده داستان‌های علمی- تخیلی، در کتاب Neuromancer بود.

فضای سایبر یا فضای مجازی[2] عبارت است از: «مجموعه‌ای از ارتباطات درونی انسان‌ها، که از طریق رایانه و وسائل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی صورت می‌پذیرد.»

فضای سایبر در واقع محیط الکترونیکی واقعی است که ارتباطات انسانی در آن به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص، به طور زنده و مستقیم روی می‌دهد. نباید تصور شود که مجازی بودن این فضا به معنای غیر واقعی بودن آن است. زیرا در فضای سایبر نیز همان ویژگی‌های تعاملات انسانی در دنیای فیزیکی، همچون مسئولیت ها، وجود دارد. همچنین فضای سایبر در واقع یک محیط است که ارتباطات در آن انجام می‌شود؛ نه صرفا مجموعه‌ای از ارتباطات. هم چنین ارتباطات به صورت زنده، واقعی و مستقیم رخ می‌دهد.

یک سیستم آنلاین نمونه ای از فضای سایبر است که کاربران آن می‌توانند از طریق ایمیل با یکدیگر ارتباط بر قرارکنند.

1.3. ویژگی‌های فضای سایبر

موارد زیر را می‌توان از ویژگی‌های فضای سایبر و دنیای مجازی نام برد:

- **جهانی و برون مرزی بودن**

از ویژگی‌های منحصر به فردی که فضای سایبر را از دیگر رسانه‌ها ممتاز می‌سازد، جهانی بودن آن است. هر فردی در هر نقطه از جهان می‌تواند از طریق آن به آسانی، به جدیدترین اطلاعات دست یابد.

1 William Gibson
2 Cyber Space

مرزهای جغرافیایی تاکنون نتوانسته اند که از گسترش روزافزون فضای سایبر جلوگیری کند. از این رو، هر نوع فیلتر و مرزبندی در برابر آن بسیار دشوار است.

- **دستیابی آسان به آخرین اطلاعات**

ساده‌ترین و سریع ترین راه برای دست یابی به آخرین مقاله، کتاب و یا خبری که در زمینه تخصصی، در سطح جهان منتشر شده، استفاده از فضای سایبر است.

- **جذابیت و تنوع**

رسانه‌ها از فیلم، عکس، متن و یا هر هنر دیگری برای جذاب کردن خویش استفاده می‌کنند که این ابزارها در فضای سایبر قابل دستیابی است؛ به‌ویژه آن‌گاه که هیچ نظارت و فیلتری توان محدود کردن آن را نداشته باشد. از ویژگی‌های منحصر به فردی که در تنوع و جذابیت فضای سایبر تأثیر بسزایی دارد، مشتری محوری است. در متون نوشتاری ارتباطی تنگاتنگ میان خوانندگان و نویسندگان وجود دارد که خواننده به‌راحتی می‌تواند نظر خود را با شخص نویسنده در میان بگذارد. از سوی دیگر، امکان نظرسنجی و ارزیابی در این فضا بسیار آسان‌تر است و داده پردازان، فروشندگان و عرضه کنندگان محصولات اینترنتی، این امکان را داده است که از آخرین خواسته‌های مشتریان و مخاطبان خود مطلع گردند.

- **آزادی اطلاعات و ارتباطات**

در فضای سایبر معنای واقعی آزادی اطلاعات، محقق شده است. از این رو، هر نوع اطلاعاتی، اعم از فرهنگی، سیاسی و اقتصادی، بدون محدویت‌های حاکم بر دیگر رسانه‌ها، در فضای سایبر قابل دسترسی است. آزادی ارتباطی نیز از ویژگی‌های دیگر فضای مجازی است که در دیگر وسایل ارتباطی تا این حد قابل دستیابی نمی باشد.

1.3.1. تعریف جنگ سایبر

جنگ سایبری[1] در لغت به معنای تهاجم بر عناصر سایبری است و به مفهوم استفاده دفاعی یا تهاجمی از اطلاعات و سیستم‌های اطلاعاتی در یک فضای سایبر می‌باشد. هدف آن به مخاطره انداختن عناصر ارتباطی و اطلاعاتی (اطلاعات، پروسه‌های مبتنی بر اطلاعات، سیستم‌های اطلاعاتی، شبکه‌های رایانه ای) است که دشمن به آنها تکیه می‌کند. یعنی این که او کیست؟ کجاست؟ چه کاری را در چه زمانی می‌تواند انجام دهد؟ چرا می‌جنگد؟ چه تهدیداتی در اولویت قرار دارند؟ و ... از این قبیل اطلاعات است.

در جنگ سایبر تلاش می‌شود تا به همه اطلاعات دشمن دست پیدا کرد و در عین حال او به هیچ عنصر ارتباطی دست نیابد. به بیان دیگر، هدف اصلی در جنگ سایبر بر هم زدن موازنه اطلاعات و دانش به نفع نیروهای خودی است؛ به ویژه اگر موازنه توان رزمی وجود ندارد. بنابراین در جنگ سایبر می‌توان با بهره گیری از دانش برتر، ضعف سرمایه و نفرات کمتر را جبران کرده و به پیروزی قاطع دست یافت.

1 Cyber War

محدوده عملیاتی جنگ سایبری بسیار گسترده است؛ از تولید پارازیت‌های مخابراتی گرفته تا عملیات روانی، و از تغییر صفحات وب سایت گرفته تا بمباران ایمیلی. ولی در نهایت، اصل همان تهدیدات منابع اطلاعاتی است، به نحوی که امنیت ملی دشمن مورد مخاطره قرار بگیرد. بنابراین بستر عملات سایبری، همان زیر ساخت‌های اطلاعاتی می‌باشد.
همچنین باید خاطر نشان کرد که اگرچه طراحی و اجرای یک جنگ سایبر تمام عیار مستلزم دسترسی به فناوری پیشرفته است. اما جنگ سایبر به خودی خود به فناوری پیشرفته وابستگی قطعی ندارد. در واقع برای جنگ سایبر فقط حضور فناوری پیشرفته الزامی نیست، بلکه ابعاد روانی و سازمانی آن به اندازه ابعاد فنی اهمیت دارد. در تحت شرایط خاص شاید واقعا بتوان با استفاده از فناوری سطح پائین یک جنگ سایبر را آغاز کرد.
به طور کلی برای پیروزی در یک جنگ سایبری باید از تواناییهای زیر برخوردار بود:
– دانش و تخصص کافی
مهتمرین مسئله در یک حمله سایبری داشتن تخصص کافی است. این دانش در صورتی می‌تواند به طور بهینه مورد استفاده قرار گیرد که اطلاعات دشمن به طور کامل در اختیار باشد.
– داشتن تجهیزات کافی
مسلما تجهیزات عام یک عملیات سایبری، همان عناصر رایج و عمومی فضای سایبری هستند. ولی برای انجام حرکات خاص باید تجهیزات خاصی را دارا بود و عناصر خاصی از فضای سایبر را در اختیار داشت.

1.3.2. جنگ‌های اطلاعاتی نهفته در جنگ سایبر

جنگ سایبر ترکیبی از شش مورد از انواع جنگهای اطلاعاتی دیگر است. این شش مورد جنگ اطلاعاتی عبارتند از:

– جنگ فرماندهی و کنترل: هدف آن قطع کردن سر دشمن، یعنی از بین بردن مغز متفکر دشمن، است.
– جنگ برپایه اطلاعات: متشکل از طراحی، حفاظت و ممانعت از دسترسی به سیستم هائی است که برای برتری بر فضای نبرد در جستجوی دانش کافی هستند.
– جنگ الکترونیک: به معنی استفاده از تکنیک‌های رادیوئی، الکترونیک، یا رمزنگاری است.
– جنگ روانی: در آن از اطلاعات برای تغییر ذهنیت و طرز فکر دوستان، بی طرف ها و دشمنان استفاده می‌شود.
– جنگ هکرها: در آن به سیستم‌های رایانه ای حمله می‌شود.
– جنگ اطلاعاتی اقتصادی: هدف آن ایجاد مانع در برابر اطلاعات یا تسهیل جریان اطلاعات با هدف کسب برتری اقتصادی است.

1.3.3. مشخصات عملیات سایبری

شاید بتوان مشخصه‌های یک عملیات سایبری را عینا از روی عملیات جنگی فیزیکی نمونه‌برداری کرد. این عملیات دارای موارد زیر می‌باشد:
– انگیزه: بدون شک، حمله کننده باید ابتدا انگیزه داشته باشد. این انگیزه امکان دارد مستقیما تولید شده و یا به صورت غیر مستقیم ایجاد گردد.

- هدف[1]: با توجه به انگیزه حمله، محدوده عملیات مشخص می‌گردد. این همان چیزی است که از آن با نام هدف یاد می‌شود.
- جمع‌آوری اطلاعات: در هر عملیاتی، چه فیزیکی و چه سایبری، باید به جمع‌آوری اطلاعات دقت و توجه کافی داشت. کسب اطلاعات از عناصر سایبری دشمن به عنوان مهم ترین بخش از عملیات سایبری مورد توجه قرار می‌گیرد.
- نقاط ضعف: بعد از کامل شدن اطلاعات حمله کننده درباره ماهیت سایبری هدف، مرحله تعیین نقاط ضعف آغاز می‌شود.
- نفوذ: با معین شدن نقاط ضعف و با در نظر گرفتن اطلاعات به دست آمده و همچنین با آگاهی از مکانیزم‌های ردیابی، عملیات سایبری در جهت نفوذ به هدف پیش می‌رود.

1.3.4. نفوذگران و اهداف آنها

ابداع واژه نفوذگر[2] به دهه شصت میلادی در دانشگاه MIT باز می‌گردد. در آن زمان، تعریف نفوذگر بدین گونه بود: «نفوذگر کسی است که از سرکش ی کردن به جزئیات سیستم‌های قابل برنامه ریزی و نفوذ و رسوخ در آن لذت می‌برد و مصمم به شکست دادن توانایی محاسباتی ماشین در مقابل هوش و ذکاوت بشری خویش است. نفوذگر فردی که با سماجت و به گونه ای لجوجانه شیفته برنامه نویسی است. این شخص بدخواه نیست و صدمه نمی‌زند.»
در آن زمان این افراد نه تنها بدنام و مورد غضب نبودند، بلکه از آنها به نیکی و احترام یاد می‌شد.
در مقابل کلمه hacker، کلمه Cracker ابداع گردید. این افراد با یادگیری برخی از مهارت‌های نفوذگری به کارهای بی ارزشی همانند دزدیدن Pass Word دیگران، مزاحمت غیر اخلاقی و غیرقانونی می‌پرداختند.
با گذشت زمان، نفوذگر یک فرد مخرب تلقی گردید. لذا هکرهای واقعی سعی کردند بر سر واژه هکر کلاه‌های رنگی بگذارند که در ادامه انواع آنها شرح داده شده است:

- **گروه نفوذگران کلاه سفید:** هر کس که با دانش خود بتواند از سد موانع امنیتی یک شبکه بگذرد و به داخل شبکه راه پیدا کند اما اقدام خرابکارانه ای انجام ندهد را یک هکر کلاه سفید می‌خوانند. هکرهای کلاه سفید متخصصین شبکه ای هستند که سوراخ‌های امنیتی شبکه را پیدا می‌کنند و به مسوولان گزارش می‌دهند.
- **گروه نفوذگران کلاه سیا:** به این گروه Cracker می‌گویند. این گروه افرادی هستند که وارد کامپیوتر قربانی خود شده و به دستکاری اطلاعات و یا جاسوسی و یا پخش کردن ویروس و غیره می‌پردازند.
- **گروه نفوذگران کلاه خاکستری:** شاید سخت ترین کار توصیف حوزه این گروه از نفوذگرهاست. به این نفوذگرها بعضا whacker هم می‌گویند (البته زیاد مصطلح نیست). این گروه از نفوذگر ها بنا به تعریفی حد وسط دو تعریف گذشته هستند.

1 Target
2 Hacker

– **گروه نفوذگران کلاه صورتی:** این گروه افراد کم سوادی هستند که فقط با نرم افزارهایی به خرابکاری و آزار و اذیت بقیه اقدام می‌کنند.

1.3.5. تاثیرات جنگ‌های سایبری

میزان تاثیرات چنین جنگ هایی به میزان تداخل فضای سایبری با فضای حقیقی بستگی کامل دارد.

- در بهترین شرایط
ویروس ها و کرم ها
حملات Dos

- در شرایط خوب – به سیستم‌های کامپیوتری دولتی نفوذ کرده و اسرار نظامی و فن‌آوری رمزنگاری را می‌ربایند.
اختلال در خطوط نیرو.
سیستم‌های اورژانسی مورد مخاطره قرار می‌گیرد و بدین شکل سعی و کوشش در رساندن کمک و نجات مختل می‌گردد.

- در شرایط بد – فیبرهای نوری مابین نقاط اصلی مورد تهدید قرار می‌گیرند.
بمباران سرورهای دامنه و بانک ها

- در بدترین شرایط – بمباران عناصر اینترنتی محقق شده و پایین آوردن اینترنت محتمل است.

میزان تاثیرات چنین جنگ هایی به میزان تداخل فضای سایبری با فضای حقیقی بستگی کامل دارد. در بهترین شرایط می‌توان حملات DOS و ویروس ها و کرم‌های رایانه‌ای را نام برد. اما مهاجمان می‌توانند بیشتر در فضای حقیقی مداخله کنند. به عنوان مثال حمله کننده ها به سیستم‌های کامپیوتری دولتی نفوذ کرده و اسرار نظامی و فن‌آوری رمز نگاری را می‌ربایند، یا در خطوط نیرو اختلال ایجاد می‌کنند، سیستم‌های اورژانسی مورد مخاطره قرار می‌دهند و بدین شکل سعی و کوشش در رساندن کمک و نجات مختل می‌گردد. در شرایط بدتر، فیبرهای نوری مابین نقاط اصلی مورد تهدید قرار می‌گیرند. بمباران سرورهای دامنه و بانک ها از این قبیل هستند. ولی در بدترین شرایط ممکن، بمباران عناصر اینترنتی محقق شده و پایین آوردن اینترنت محتمل است.

1.3.6. نمونه جنگ‌های سایبر

– دهه 80 میلادی، کره شمالی و آمریکا: در این دهه کره شمالی در عکس‌العمل به توان مضاعف دشمن، اقدام به تأسیس مدرسه هک با بیش از ۱۰۰ سرباز آموزش دیده نمود. جنگ‌های این دهه را می‌توان پیامدهای مشخصی از جنگ سرد دانست.

– سال 1994، حملات همزمان در این سال به مراکز هوائی ـ تحقیقاتی Rome در نیویورک، انستیتو تحقیقات اتمی کره‌جنوبی و نهایتاً مرکزی علمی در لاتویا (از کشورهای تازه استقلال یافته شوروی سابق): سه حمله همزمان

صورت گرفت. درحالی که کنترل شبکه در دستان حمله‌کننده‌ها بود، ولی منبع مشخصی نداشت. با این حال در این حملات ردپاهایی از انگلستان مشاهده شد.

– سال 1995، حمله به Citibank آمریکا: در این حمله ۴۰۰ هزار دلار توسط گروه هکرهای روسی به سرقت رفت. البته در نهایت با شناسائی مهاجمین روسی بخشی از زیان‌ها جبران شد.

– سال 1999، حمله به یوگسلاوی در ماه می: این سال براساس دستور بیل کلینتون، رئیس‌جمهور وقت ایالات متحده آمریکا، سازمان امنیت و اطلاعات این کشور طرح حمله به سامانه‌های رایانه‌ای یوگوسلاوی را پی‌ریزی کردند. به سبب فاش شدن اسرار این حمله، مقامات آمریکایی ناگریز آن را تأیید کردند. از جمله اقدامات انجام شده در این حمله می‌توان به موارد ذیل اشاره نمود: نفوذ به حساب‌های بانکی، قطع نمودن خطوط تلفن، تهدید مراکز سوخت‌رسانی و غذا.

– سال 1999، جنگ 78 روزه در ماه سپتامبر: این سال خبرگزاری رویتر رسماً اعلام کرد که وزارت دفاع آمریکا، طرح حمله به شبکه‌های کامپیوتری «صرب» را به منظور تهدید تسلیحات نظامی و خدمات اجتماعی با جدیت ادامه می‌دهد. این حمله 78 روز ادامه داشته است.

– سال2000، حمله علیه چین در ماه آگوست: این سال Straits Times اعلام کرد که هنگ کنگ خواهان استقلال خود از کشور چین است. این کشور از این نوع جنگ به منظور ضربه زدن و اعمال فشار به چین استفاده نمود. هنگ‌کنگ در این حملات با استفاده از ویروس‌های خود مراکز انرژی، نظامی وبانک‌های چین را تحت تأثیر قرار داد و توانست فعالیت آنها را مختل نماید.

– سال 2001، آمریکا و چین: در این سال بر سر موضوع برخورد هواپیمای جاسوسی آمریکا با جت چینی جنگ سایبری دنباله داری بین دو کشور در گرفت که دامنه‌های آن تاحدودی به اروپا نیز کشیده شد. سایت دولتی چین، اولین قربانی این جنگ بود. در بین جنگ‌های سایبری در گرفته بین آمریکا و چین، این مشهورترین نمونه می‌باشد. درصد آسیب‌های وارده به زیرساخت‌ها و تخریب در چین بر اثر این جنگ‌ها 10 برابر آمریکا بوده است.

– سال 2001، آمریکا و روسیه: در آوریل این سال روزنامه روسی Moskovsky Komsomolets از استخدام هکرهای روسی، برای نفوذ به شبکه خدمات امنیتی این کشور توسط آمریکا خبر داد.

– سال 2001، برج‌های دو قلو: هرچند آمریکا مسئولیت مستقیم عملیات یازدهم سپتامبر را به طور مشخص به القاعده و عمل انتحاری اعضای این گروه نسبت می‌دهد، اما باید توجه داشت شواهد نشانگر طرح‌ریزی بسیار دقیق و اجرای عملیات در طی حدود یک سال و نیم، است که بدون پشتوانه جنگ سایبری امکان‌پذیر نبوده است.

– سال 2003، آمریکا و عراق: در ماه می‌این سال آمریکا با طرح‌ریزی و اجرای یک جنگ تبلیغاتی سایبری راه را برای تجاوز به عراق و توجیه اقدام خود برای افکار عمومی جهانی باز نمود.

– سال 2003، حمله علیه تایوان: در این سال چین مبادرت به حمله سایبری به دولت تایوان نمود. ابزار مورد استفاده در این حمله انتشار اسب‌های تروآ بوده است.

– سال 2006، جنگ 33 روزه: در آغاز این جنگ، آمریکا، اسرائیل، متحدان اروپایی آنها و برخی از سران سازش کار عرب، با قاطعیت و اطمینان از نابودی حداکثر 3 روزه حزب‌الله سخن می‌گفتند. اما به دلیل عدم توجه اسرائیل به

تکنیک‌های دفاع غیرعامل و برتری حزب‌الله در نبردهای اطلاعاتی با به کارگیری تکنیک‌های پدافند غیرعامل در حوزه فناوری اطلاعات و استفاده از ابزارآلات و تجهیزات بومی، موجب ناکامی اسرائیل در دستیابی به اهداف خود شد. تهدید سایت‌های اینترنتی طرفین، حملات متناوب DoS که به منظور ایجاد اختلال در سرویس‌دهی با ایجاد حجم بالای ترافیک صورت می‌گیرد و استفاده از تکنیک‌های شنود و جاسوسی، از جمله اقدامات انجام شده در حوزه فضای سایبری در جنگ 33 روزه می‌باشد.

- سال 2007، حمله به استونی: در آوریل این سال، پس از تصمیم استونی برای نابود کردن مجسمه برنزی شکست شوروی در جنگ جهانی دوم، سایت‌های احزاب سیاسی، بانک‌ها، روزنامه‌ها و وزارتخانه‌های این کشور حدود 3 هفته تحت حملات سایبری قرار گرفتند.
- سال 2008، اوستیای جنوبی: در نخستین ساعات آغاز جنگ روسیه و گرجستان، آتش این جنگ در فضای سایبر نیز روشن شد. بسیاری از کارگزارهای شبکه گرجستان کمی قبل از آغاز عملیات نظامی روسیه به مناطق استقلال طلب اوستیای جنوبی مورد حملات سایبری قرار گرفتند. به طوری که سایت‌های وزارت امور خارجه، وزارت دفاع گرجستان، سایت رسمی میخائیل ساکاشویلی[1] رئیس‌جمهور گرجستان و شبکه‌های اصلی تلویزیونی این کشور بر اثر حملات مستمر DoS کاملاً مسدود و بلااستفاده شده بودند. در نتیجه این حملات سایت‌ها به‌روزسازی نمی‌شدند و نمی‌توانستند اخبار جدید را دریافت یا اعلام کنند.

1.4. ملزومات امنیت فضای سایبر

اهمیت توسعه فناوری اطلاعات و ارتباطات و فراگیر بودن آن، اهمیت امنیت شبکه‌های اطلاع رسانی را به دنبال دارد. اگر امنیت شبکه برقرار نگردد، مزیت‌های فراوان آن نیز به خوبی حاصل نخواهد شد. پول و تجارت الکترونیک، خدمات به کاربران خاص، اطلاعات شخصی، اطلاعات عمومی و نشریات الکترونیک و ... در معرض دستکاری و سواستفاده‌های مادی و معنوی هستند. همچنین دستکاری اطلاعات به عنوان زیر بنای فکری یک ملت توسط گروه‌های سازماندهی شده بین المللی، به نوعی مختل کننده امنیت ملی و تهاجم علیه یک دولت محسوب می‌شود.

برای کشور ایران که بسیاری از نرم افزارهای پایه از قبیل سیستم عامل و نرم افزارهای کاربردی و اینترنتی خود را از طریق واسطه ها و شرکت‌های خارجی تهیه می‌کند، بیم نفوذ از راه‌های مخفی وجود دارد. در آینده بانک ها و بسیاری از نهادها و دستگاه‌های دیگر از طریق شبکه به فعالیت می‌پردازند. برای مثال، چنانچه یک پیغام خاص از طرف شرکت مایکروسافت به کلیه سایت‌های ایرانی ارسال شود و سیستم‌های عامل در واکنش به این پیغام، سیستم ها را خراب کنند و از کار بیندازند، ضررهای هنگفتی به امنیت و اقتصاد مملکت وارد خواهد شد. نکته جالب اینکه بزرگترین شرکت تولید نرم افزارهای امنیت شبکه شرکت چک پوینت[2] است که شعبه اصلی آن در اسرائیل می‌باشد. مساله امنیت شبکه برای کشورها مساله‌ای استراتژیک است. بنابراین کشور ایران نیز باید به آخرین تکنولوژی‌های امنیت

1 Mikheil Saakashvili
2 Check Point

شبکه مجهز شود و از آن جایی که این تکنولوژی ها به صورت محصولات نـرم افـزاری قابـل خریـداری نیسـتند، در نتیجه باید صنعت امنیت شبکه در کشور به طور جدی پا بگیرد.
اهمیت پشتیبانی برای حضور کاربران در محیط مجازی، به اندازه‌ای است که در کشورهای پیشرفته کاربران امنیـت سـخت افزار و نرم افزار خود را بیمه می‌کنند. هم چنین به عقیده برخی از کارشناسان استفاده از ابراز هـایی چـون فیلترینـگ بـرای ریسک‌های غیرقابل پیش بینی با شرط هوشمند بودن این سیستم، می‌تواند در برقراری محیطی امن مفید باشد. سالم سازی فضای سایبر، ایجاد محیطی برای حفظ اطمینان کاربران از گردش در اینترنت است و به گفته کارشناسان مهم ترین اقدامی که باید برای جلوگیری از تهدیدات محیط سایبر، به ویژه در کشور ایران صورت بگیرد، تدابیر پیشگیرانه اجتماعی است که با آموزش کاربران به خصوص خانواده ها و ایجاد کدهای رفتاری برای کاربران حرفه‌ای عملی می‌شود.
عمده تهدیداتی که امنیت و سلامت فضای سایبر را با مشکل رو به رو می‌کند، در قالب محتوای غیر اخلاقـی، نقـض مالکیت معنوی آثار دیجیتال، ویروس ها و کدهای مخرب، دسترسی غیرمجاز به داده ها، سرقت و جعل اطلاعـات بـه همراه کلاه برداری رایانه‌ای است.
از میان تهدیدکنندگان فضای سایبر می‌توان به موارد زیر اشاره کرد:

- جاسوس‌ها و عوامل خارجی
- تروریست‌ها و گروه‌های افراطی
- جنایتکاران و گروه‌های جنایی
- هکرها و گروه‌های با انگیزه‌های تفننی

1.5. چالش‌های ناشی از تهدیدات فضای سایبر

در این بخش، برخی از چالش‌های ناشی از این تهدیدات، که حکومتها در اثر توسعهٔ فناوری اطلاعات و ارتباطات با آن مواجه هستند، مورد بررسی مختصر قرار می‌گیرد.

- **امنیت سیاسی و محدودهٔ حاکمیت**

این چالش دیر یا زود در بسیاری از کشورهایی که کورکورانه مسیر توسعهٔ فناوری اطلاعات و ارتباطات را می‌پیمایند، به وجود خواهد آمد. از آنجا که در فضای سایبر محدودیت مکانی و جغرافیایی وجود ندارد، تشـکیل هـر گـروه و حـزب و انجام هر فعالیت سیاسی مخالف اصول اساسی کشورها، در مقیاسی وسیع و گسترده امکان پذیر خواهـد بـود و امکـان تبلیغ هر اندیشه و خط سیاسی به سادگی ایجاد خواهد شد. تشکیل کشورهای مجازی و یـارگیری از کلیـهٔ کشـورهای جهان، شاید مقدمه ای بر این مساله باشد.
توسعهٔ ارتباطات به همراه بهره برداری عده ای از آن در راستای عقاید خودشان حتی می‌تواند حکومت ها را ناپایـدار و جابجا نماید.

- **امنیت اقتصادی**

یکی از مشخصات اصلی هر کشور در بعد اقتصادی، پول آن کشور است. بدون پول ملی، کشور هویت اقتصادی نخواهد داشت. چنانچه زیرساخت‌های پول الکترونیک ملی به سرعت در کشور فراهم نشود، این احتمال وجود دارد که توسعهٔ زیرساختهای شبکه‌های اطلاع رسانی وهمچنین ارائهٔ خدمات پول الکترونیک توسط سایر کشورها، موج مهاجرت ثروت و درآمد کشور به بانکهای خارجی را تشدید کند و عملا مردم پول آ نها را به رسمیت بشناسند.
در فضای سایبر بستن مرزها به روی بانک ها خارجی امری دشوار و ناممکن است. بنابر این باید پول الکترونیک ملی را در شرایط رقابتی تقویت نمود.

- **امنیت اجتماعی و فرهنگی**

تهاجم فرهنگی اولین چالش توسعهٔ فناوری اطلاعات و ارتباطات است که باید برای آن راه حلهایی اندیشید. یکی از این راه ها، بستن برخی از سایت هاست. اما این فقط یکی از راه ها است و باید به موارد دیگری مثل حضور فعال، مدبرانه و خلاقانه در صحنهٔ دفاع فرهنگی، آموزش عمومی و افزایش آگاهی‌های اجتماعی و ایجاد بیداری نسبت به عواقب تهاجم فرهنگی، تدوین قوانین مناسب و همچنین توسعهٔ خدمات مفید و مؤثر در شبکه ها به منظور کاهش تاثیر تهاجم فرهنگی، نیز اشاره نمود.

1.6. دلایل نفوذپذیری سایت‌ها

مساله نفوذ و از کار افتادن سرورهای وب دغدغه هر مدیری است. بررسی جوانب این مشکلات به طور خلاصه عبارتند از.

– نبود قوانین بازدارنده

با وجود کاربران زیاد اینترنت، متاسفانه تاکنون قانون جامعی برای برخورد با جرم‌های اینترنتی و به خصوص نفوذ غیر مجاز به حریم دیگران وجود ندارد. بر خلاف ایران، در سایر کشور ها و به خصوص آمریکا، نفوذ به شبکه‌های کامپیوتری جرم محسوب شده و با جریمه‌های سنگین نقدی، زندان و محرومیت استفاده از اینترنت همراه است.

– عدم امکان پیگیری نفوذگران در ایران

یکی دیگر از مشکلات در برخورد با مجرمان، عدم امکان شناسایی نفوذگران است. در نظام فعلی، بسیاری از ISP ها فاقد شناسنامه اند. از سوی دیگر به دلیل وجود سیستم فروش کارتی، عملا دستیابی به نفوذگران غیرممکن خواهد بود. اما در صورتی که تمامی ISPهای ایران دارای شناسنامه باشند و بانک اطلاعاتی در باره IPهای مورد استفاده آنها وجود داشته باشد و از سوی دیگر بستر مخابراتی برای ردیابی خطوط ISP ها آماده شده باشد (راه اندازی سیگنالینگ No.7)، به راحتی می‌توان کوچک ترین نفوذ را پیگیری و در صورت نیاز با آن برخورد نمود. به نظر می‌رسد با تشکیل کمیته‌ای خاص و به کمک مخابرات بتوان به راحتی نفوذگران را شناسایی کرد که این امر نیازمند اراده مسئولین حکومتی است.

– پشتیبانی ضعیف از سرورها

اکثر سرورهای وب شرکت‌های ایرانی در کشورهای آمریکا، کانادا و انگلیس قرار دارند. معمولا این سرورها توسط شرکتهای ایرانی اجاره شده و خدمات و پشتیبانی آن به عهده طرف ایرانی است. متاسفانه به دلیل کنترل از راه دور،

مسئول پشتیبانی سرور امکانات محدودی در اختیار دارد. این مشکل به خصوص در زمان حمله‌های اینترنتی دو چندان می‌شود. حتی در برخی موارد دسترسی مسئول پشتیبانی به سرور از دست می‌رود و و علاوه بر این ها، Bug هایی که در نرم افزار کنترل از راه دور سرور ها وجود دارد، امکان نفوذ به سرورها را به نفوذگران می‌دهد.

از طرف دیگر به دلیل جدید بودن این نوع سرویس، مدیران سرورها عملا در جلوگیری و مقابله با مشکلات خاص عملات تجربه‌ای نداشتند. البته با گذشت زمان این مشکل به شکل محسوسی تغییر کرده است و بسیاری از مسئولین پشتیبانی در برابر حملات و مشکلات حرفه‌ای شده اند.

- فروش خدمات بدون در نظر گرفتن مسائل جانبی

در حال حاضر، شرکت‌های زیادی اقدام به ارائه خدمات تخصیص فضا می‌کنند. در صورتی که بسیاری از این شرکت ها تنها فروشنده خدمات هستند و صاحبان سرورها طبق شرایط خاصی فضا را در اختیار فروشندگان قرار می‌دهند. امکاناتی مانند حذف و یا اضافه کردن سایت در سرورها که در اختیار فروشندگان است، موجب شده که طیف گسترده‌ای از سایت ها مانند سایت‌های شخصی، خبری، تفریحی، تجاری و ... روی یک سرور قرار بگیرند. شاید این مساله در نگاه اول چندان مشکل ساز نباشد، اما توجه بیشتر نفوذگران به سایت‌های مشهور و به خصوص سایت‌های خبری، امنیت سایر سایت‌های موجود در سرور را مورد تهدید قرار می‌دهد. از سوی دیگر با توجه به پشتیبانی تمامی سرورها از برنامه نویسی طرف سرور[1] این امکان برای نفوذگران وجود دارد که با اجاره فضا از سرورها و استفاده از Bugهای برنامه‌های تحت سرور مانند Php و ASP، سرور را از کار بیاندازند و یا به آن نفوذ کنند.

- مشکلات طراحی سایت‌ها

در سال‌های اخیر بسیاری از سایت‌های خبری، تجاری و حتی تفریحی به دلیل قابلیت‌های فراوان برنامه نویسی تحت وب[2] به این روش روی آورده اند. اما متاسفانه در برخی از سایت‌های ایرانی، به دلیل آشنا نبودن برنامه نویسان به مساله امنیت، نفوذگران به راحتی و با استفاده از دستورات خاص، به بانک اطلاعاتی سایت دسترسی پیدا می‌کنند و حتی اقدام به تغییر در آن می‌نمایند. این مشکل با توجه برنامه نویسان، به مسائل امنیتی و استفاده مدیران سایت ها از برنامه نویسان حرفه‌ای به سادگی قابل حل است.

- نبود فرهنگ مناسب اینترنتی

با وجود رشد سریع اینترنت، متاسفانه تاکنون فرهنگ سازی مناسبی برای استفاده از اینترنت انجام نگرفته است و فرهنگ احترام به حریم دیگران در اینترنت رعایت نمی شود. این مشکل حتی در اتاق‌های گفت و گو[3] کاملا مشخص است. علاوه بر این در دسترس بودن نرم افزارهای هک در بازار، به این مشکلات دامن می‌زند. از سوی دیگر برخی رسانه ها، اخبار مربوط به نفوذگران را با آب و تاب فراوان شرح می‌دهند؛ به طوری که خوانندگان خود را به طور غیر مستقیم تشویق به این امر می‌کنند. حتی برخی از روزنامه ها فراتر می‌روند و اقدام به چاپ چگونگی نفوذ به برخی سایت‌های ایرانی می‌نمایند. شاید طرح این مسائل در فروش روزنامه ها تاثیر بسزایی داشته باشد، اما این مطلب بر جامعه و کاربران اینترنتی اثر عمیقی خواهد گذاشت.

1 Server Side Programming
2 Web Programming
3 Chat Room