امنیت سایبری

و

جنگ سایبری

مترجم: علی اصغر جعفری لاری

انتشارات پندار پارس

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ١٤، واحد ١٦ **www.pendarepars.com**
تلفن: ٦٦٥٧٢٣٣٥ - تلفکس: ٦٦٩٢٦٥٧٨همراه: ٠٩٢١٤٣٧١٩٦٤ **info@pendarepars.com**

نام کتاب	**:**	**امنیت سایبری و جنگ سایبری**
ناشر	**:**	**انتشارات پندار پارس**
ترجمه	**:**	**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 ۱

هدف از نگارش این کتاب ۱

سخنی درباره‌ی مرجع اصلی این کتاب ۲

دلیل وجود شکاف در دانش امنیت سایبری و چرایی اهمیت آن ۵

سخن پایانی... ..... ۷

بخش ۱: مقدمه ای بر فضای سایبری ۹

تعریف فضای سایبری ۹

"مسائل سایبری" از کجا پدید آمد؟ ۱۲

تاریخچه‌ای کوتاه از اینترنت ۱۲

اینترنت واقعا چگونه کار می‌کند؟ ۱۵

چه کسی آن را اجرا می‌کند؟ درک حاکمیت اینترنت ۲۰

هویت و احراز هویت ۲۳

به هر حال، با "امنیت" چه کاری انجام دهیم؟ ۲۷

تهدیدها چیست؟ ۲۹

آسیب‌پذیری‌ها چیست؟ ۳۱

چگونه به فضای سایبری اعتماد کنیم؟ ۳۷

در WikiLeaks چه اتفاقی افتاد؟ ۴۲

تهدید پایدار پیشرفته چیست؟ ۴۴

مبانی دفاعی کامپیوتر ۴۷

ضعیف‌ترین پیوند کدام است؟ عوامل انسانی ۵۰

بخش ۲: مسائل مربوط به امنیت سایبری و جنگ سایبری ۵۳
معنی حملات سایبری چیست؟ اهمیت شرایط و چارچوب‌ها ۵۳
مشکل انتساب‌ها ۵۶
Hacktivism چیست؟ ۵۸
Anonymous کیست؟ ۶۱
جنایات امروز و فردا: جرائم سایبری چیست؟ ۶۳
Shady RAT و جاسوس‌های سایبری: جاسوسی سایبری چیست؟ ۶۷
آیا باید از تروریسم سایبری بترسیم؟ ۷۲
تروریست‌ها واقعا چگونه از وب استفاده می‌کنند؟ ۷۳
با تروریسم سایبری چگونه مقابله کنیم؟ ۷۶
ریسک امنیتی یا حقوق بشر؟ سیاست خارجه و اینترنت ۷۸
هکرهای میهن‌پرست چه کسانی هستند؟ ۸۰
وقتی دامنه‌های ir. هک می‌شوند... ..... ۸۴
موتور جست‌وجوگر یوز هم مثل یوزپلنگ ایرانی قدرتمند بود؟ ۸۸
Stuxnet چیست؟ ۹۰
درس پنهان Stuxnet چیست؟ ۹۳
آشنایی با جنگ سایبری ۹۵
جنگ سایبری: از هک Sony Pictures تا قطع کل اینترنت کره شمالی! ۹۵
جنگ با هر نام دیگری: جوانب حقوقی تعارض سایبری ۹۹
در واقع "جنگ سایبری"، شبیه چه چیزی است؟ عملیات شبکه‌ی کامپیوتری ۱۰۳
رویکرد نظامی آمریکا در جنگ سایبری چیست؟ ۱۰۹

رویکرد کشور چین در جنگ سایبری چیست؟ ۱۱۳

بازدارندگی در عصر جنگ سایبری چیست؟ ۱۱۷

چرا ارزیابی تهدیدها در فضای سایبری بسیار دشوار است؟ ۱۱۹

آیا امنیت سایبری جهان ضعیف است یا قوی؟ ۱۲۰

چه کسی دارای این مزیت است، تهاجم یا دفاع؟ ۱۲۲

نوع جدیدی از مسابقه تسلیحاتی: خطرات گسترش سلاح‌های سایبری چیست؟ ۱۲٤

چه درس‌هایی می‌توان از مسابقه‌ی تسلیحاتی گذشته فرا گرفت؟ ۱۲۷

آیا مجتمع صنعتی-سایبری وجود دارد؟ ۱۲۹

بخش ۳: رویکردهایی برای بهبود فضای سایبری ۱۳۳

چرا نمی‌توانیم یک اینترنت امن‌تر و جدید بسازیم؟ ۱۳۳

بازنگری امنیت: انعطاف‌پذیری چیست و چرا مهم است؟ ۱۳۵

آموختن از تاریخ: دزدان دریایی چه چیزی می‌توانند به ما درباره‌ی امنیت سایبری یاد دهند؟ ۱۳۸

حفاظت از حاکمیت گسترده‌ی جهانی برای شبکه جهانی وب: نقش نهادهای بین‌المللی چیست؟ ۱٤۱

آیا به یک معاهده‌ی فضای سایبری نیاز داریم؟ ۱٤٤

درک محدودیت‌های دولت‌ها در فضای سایبری: چرا دولت‌ها نمی‌توانند آن را اداره کنند؟ ..۱٤۸

تجدید نظر نقش دولت‌ها: چگونه می‌توانیم امنیت سایبری را بهتر سازماندهی کنیم؟ ۱۵۲

چگونه بهترین هماهنگی در دفاع داشته باشیم؟ ۱۵٦

چگونه می‌توانیم در مقابل حوادث سایبری، بهترین آمادگی را داشته باشیم؟ ۱٦۰

چگونه مشکل سایبری افراد را حل کنیم؟ ۱٦۳

چگونه می‌توانیم از خودمان و اینترنت محافظت کنیم؟ ۱٦۵

نتیجه‌گیری ۱۷۰
نظرات برخی از خوانندگان مرجع اصلی کتاب ۱۷۱

فهرست

پیش‌گفتار ۱

هدف از نگارش این کتاب ۱

سخنی درباره‌ی مرجع اصلی این کتاب ۲

دلیل وجود شکاف در دانش امنیت سایبری و چرایی اهمیت آن ۵

سخن پایانی ۷

بخش ۱: مقدمه ای بر فضای سایبری ۹

تعریف فضای سایبری ۹

"مسائل سایبری" از کجا پدید آمد؟ ۱۲

تاریخچه‌ای کوتاه از اینترنت ۱۲

اینترنت واقعا چگونه کار می‌کند؟ ۱۵

چه کسی آن را اجرا می‌کند؟ درک حاکمیت اینترنت ۲۰

هویت و احراز هویت ۲۳

به هر حال، با "امنیت" چه کاری انجام دهیم؟ ۲۷

تهدیدها چیست؟ ۲۹

آسیب‌پذیری‌ها چیست؟ ۳۱

چگونه به فضای سایبری اعتماد کنیم؟ ۳۷

در WikiLeaks چه اتفاقی افتاد؟ ٤۲

تهدید پایدار پیشرفته چیست؟ ٤٤

مبانی دفاعی کامپیوتر ٤۷

ضعیف‌ترین پیوند کدام است؟ عوامل انسانی ۵۰

بخش ۲: مسائل مربوط به امنیت سایبری و جنگ سایبری ۵۳

معنی حملات سایبری چیست؟ اهمیت شرایط و چارچوب‌ها..... ۵۳

مشکل انتساب‌ها..... ۵۶

Hacktivism چیست؟..... ۵۸

Anonymous کیست؟ ۶۱

جنایات امروز و فردا: جرائم سایبری چیست؟ ۶۳

Shady RAT و جاسوس‌های سایبری: جاسوسی سایبری چیست؟..... ۶۷

آیا باید از تروریسم سایبری بترسیم؟ ۷۲

تروریست‌ها واقعا چگونه از وب استفاده می‌کنند؟ ۷۳

با تروریسم سایبری چگونه مقابله کنیم؟..... ۷۶

ریسک امنیتی یا حقوق بشر؟ سیاست خارجه و اینترنت ۷۸

هکرهای میهن‌پرست چه کسانی هستند؟..... ۸۰

وقتی دامنه‌های ir. هک می‌شوند... ..... ۸۴

موتور جست‌وجوگر یوز هم مثل یوزپلنگ ایرانی قدرتمند بود؟ ۸۸

Stuxnet چیست؟..... ۹۰

درس پنهان Stuxnet چیست؟ ۹۳

آشنایی با جنگ سایبری ۹۵

جنگ سایبری: از هک Sony Pictures تا قطع کل اینترنت کره شمالی! ۹۵

جنگ با هر نام دیگری: جوانب حقوقی تعارض سایبری ۹۹

در واقع "جنگ سایبری"، شبیه چه چیزی است؟ عملیات شبکه‌ی کامپیوتری ۱۰۳

رویکرد نظامی آمریکا در جنگ سایبری چیست؟.....۱۰۹

رویکرد کشور چین در جنگ سایبری چیست؟ ۱۱۳
بازدارندگی در عصر جنگ سایبری چیست؟ ۱۱۷
چرا ارزیابی تهدیدها در فضای سایبری بسیار دشوار است؟ ۱۱۹
آیا امنیت سایبری جهان ضعیف است یا قوی؟ ۱۲۰
چه کسی دارای این مزیت است، تهاجم یا دفاع؟ ۱۲۲
نوع جدیدی از مسابقه تسلیحاتی: خطرات گسترش سلاح‌های سایبری چیست؟ ۱۲٤
چه درس‌هایی می‌توان از مسابقه‌ی تسلیحاتی گذشته فرا گرفت؟ ۱۲۷
آیا مجتمع صنعتی–سایبری وجود دارد؟ ۱۲۹
بخش ۳: رویکردهایی برای بهبود فضای سایبری ۱۳۳
چرا نمی‌توانیم یک اینترنت امن‌تر و جدید بسازیم؟ ۱۳۳
بازنگری امنیت: انعطاف‌پذیری چیست و چرا مهم است؟ ۱۳۵
آموختن از تاریخ: دزدان دریایی چه چیزی می‌توانند به ما درباره‌ی امنیت سایبری یاد دهند؟ ۱۳۸
حفاظت از حاکمیت گسترده‌ی جهانی برای شبکه جهانی وب: نقش نهادهای بین‌المللی چیست؟ ۱٤۱
آیا به یک معاهده‌ی فضای سایبری نیاز داریم؟ ۱٤٤
درک محدودیت‌های دولت‌ها در فضای سایبری: چرا دولت‌ها نمی‌توانند آن را اداره کنند؟ ۱٤۸
تجدید نظر نقش دولت‌ها: چگونه می‌توانیم امنیت سایبری را بهتر سازماندهی کنیم؟ ۱۵۲
چگونه بهترین هماهنگی در دفاع داشته باشیم؟ ۱۵٦
چگونه می‌توانیم در مقابل حوادث سایبری، بهترین آمادگی را داشته باشیم؟ ۱٦۰
چگونه مشکل سایبری افراد را حل کنیم؟ ۱٦۳
چگونه می‌توانیم از خودمان و اینترنت محافظت کنیم؟ ۱٦۵

نتیجه‌گیری ۱۷۰
نظرات برخی از خوانندگان مرجع اصلی کتاب ۱۷۱

پیش‌گفتار

هدف از نگارش این کتاب

توجه به امنیت سایبری در دنیـای امـروز، همـواره مهـم و ضـروری اسـت. افـزایش روزافـزون حمـلات، آسیب‌پذیری‌ها، گروه‌های هکری و ارتش‌های مختلف سایبری، امنیت فضای مجازی را تا حدودی متزلـزل کرده است.

کشورهای مختلف، سرمایه‌گذاری‌های هنگفتی را صرف امنیت سـایبری مـی‌کننـد تـا بتواننـد از مرزهـای 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 کـرده‌ایـم کـه امنیت مطلق نیست. فضای مجازی با دارا بودن مزیت‌های خود، ناامن‌تر از آن است که فکر می‌کنیم. بـرای 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 عنـوان "CyberSecurity And CyberWar" نوشـته‌ی P.W Singer و Allan Friedman است. تلاش کرده‌ام در بخش‌هایی از کتاب حاضر، مطـالبی را از کتـاب "CyberSecurity And CyberWar" بیاورم و عناوین برخی از مباحث را مطابق با کتـاب مـذکور مطـرح نمـایم. انتخـاب ایـن کتاب برای ترجمه‌ی برخی از قسمت‌ها، نوین بودن مطالب آن با توجه به تاریخ انتشـار کتـاب یعنـی سـال ۲۰۱٤، تایید افراد مهمی که این کتاب را خوانده‌اند و نظرات خود را داده‌اند و از همـه مهـم‌تـر اهـداف زیـر می‌باشد:

نخستین، در اولویت بودن و اهمیت داشتن امنیـت سـایبری بـوده اسـت. بهتـر اسـت از کتـب مختلـف کـه به‌صورت فنی به مباحث هک و امنیت می‌پردازند، کمی فاصله بگیریم و به دیدگاهی بیاندیشیم که کمتر بـه آن پرداخته شده است و آن چیزی نیست جز "امنیت سایبری و جنگ سـایبری". نـه تنهـا پژوهشـگران و دانشجویان ما نیاز به چنین کتب جدید و مفیدی دارند بلکه مدیران و کارشناسان ارشـد و حتـی کـاربران نیز باید با مسائل مربوط به حوزه سایبر، آگاهی و دانش کاملی داشته باشند و این نیازمنـدی، هـدف دوم در تالیف این کتاب با توجه به امنیت فضای مجازی کشور و تجربیـات بـیش از ده سـاله متـرجم در ایـن 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 می‌تواند 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 پهبادها، 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 ٤٠ 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[1] 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 سایق 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 می‌تواند 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 می‌تواند 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 ترس‌ها 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

بخش ۱

مقدمه ای بر فضای سایبری

تعریف فضای سایبری

"فضای سایبری، یک کامیون نیست. فضای سایبری، یک سری لوله است."

این تعریف، تعریفی بود که Ted Stevens درباره‌ی فضای سایبر در طول یک جلسه کنگره در سال ۲۰۰۶ شرح داد؛ در حالی که برخی افراد، این تعریف مرد مسن را مسخره می‌کردند. اما واقعیت این است که تعریف ایده‌ها و اصطلاحات مسائل سایبری، دشوار است. ایده‌ی استفاده او از واژه "لوله"، قیاسی است که توسط کارشناسان این حوزه برای شرح اتصالات داده، مورد استفاده قرار می‌گرفت.

اگر او می‌خواست این تعریف را کاملا درست و دقیق بیان کند، می‌توانست از نویسنده‌ی علمی-تخیلی به‌نام William Gibson برای تعریف مفهوم اصلی فضای سایبری، کمک بگیرد. Gibson نخستین بار در یک داستان کوتاه، از واژه‌ی "cybernetics" و "space" در سال ۱۹۸۲، استفاده کرد. دو سال بعد، او از این واژه‌ها در رمانی با ژانر انقلابی با مبحث "توهم مبنی بر رضایت طرفین، روزانه توسط میلیاردها اپراتور قانونی در هر ملت تجربه می‌شود... یک نمایش گرافیکی از اطلاعات انتزاعی از بانک‌های هر کامپیوتر در سیستم انسان" تعریف کرده بود. مطالب این داستان، یک پیچیدگی غیرقابل تصور داشت...

بخشی از اینکه چرا فضای سایبری، به‌سختی تعریف می‌شود نه تنها بخاطر گسترش آن و ماهیت جهانی است بلکه در این واقعیت است که فضای سایبری امروز، تقریبا در مقایسه با شروع فروتنی خود، غیرقابل تشخیص است. وزارت دفاع ایالات متحده می‌تواند پدرخوانده‌ی فضای سایبری باشد چراکه قدمت آن به بودجه‌ی محاسبات اولیه‌ی آن و شبکه‌های اصلی مثل ARPANET برمی‌گردد.

در طول این سال‌ها برای فضای سایبری دست‌کم ۱۲ تعریف مختلف مطرح شده است. این تعاریف در محدوده‌ی "محیط مفهومی که در آن اطلاعات دیجیتالی با شبکه‌های کامپیوتری ارتباط برقرار می‌کنند" قرار داشت که مورد پذیرش واقع نشد زیرا استنباط می‌شد که فضای سایبری تنها برای ارتباطات و تا حد زیادی تخیلی می‌باشد. در تعریف دیگری آورده شده بود که "دامنه‌ای است که با استفاده از طیف

الکترومغناطیسی و الکترونیکی مشخص شده است"، همچنین این تعریف هم مورد پذیرش واقع نشد چراکه به‌روی همه چیز احاطه داشت، از کامپیوترها و موشک‌ها تا نور خورشید...

در اقدامی در سال ۲۰۰۸، پنتاگون، تیمی از کارشناسان را جمع‌آوری کرد که تا زمانی بیش از یک سال، تعریفی را از فضای سایبری ارائه کنند. این بار آنها این‌طور تعریف کردند که "دامنه‌ای جهانی در محیط اطلاعاتی است که متشکل از شبکه‌ای وابسته به زیرساخت‌های فناوری اطلاعات از جمله اینترنت، شبکه‌های ارتباطاتی، سیستم‌های کامپیوتری و کنترل‌کننده‌ها و پردازشگرهای جاسازی شده می‌باشد" و قطعا این تعریف، دقیق‌تر از تعاریف پیشین، ارائه شده بود.

با توجه به اهداف این کتاب، شاید بهتر باشد تعریفی ساده ارائه کنیم. فضای سایبری (در ذات خود)، قلمرویی از شبکه‌های کامپیوتری (و کاربران پشت آن) است که در آن اطلاعات، ذخیره می‌شوند، به اشتراک گذاشته می‌شوند و ارتباطات آنلاین برقرار می‌شود. اما به‌جای تلاش برای پیدا کردن تعریفی کاملا دقیق از فضای سایبری، مفید است که آنچه این تعاریف را شکل داده است، بررسی کنیم. ویژگی‌های لازمی که نه تنها فضای سایبری را ایجاد می‌کند، بلکه آن را منحصربفرد می‌سازد، چیست؟

فضای سایبری (یا همان فضای مجازی) در درجه‌ی نخست، یک محیط اطلاعاتی است. این محیط، داده‌های دیجیتالی را ایجاد و ذخیره می‌کند و مهم‌تر از همه، به اشتراک می‌گذارد. این بدان معناست که صرفا یک مکان فیزیکی نیست و درنتیجه از اندازه‌گیری در هر نوع ابعاد فیزیکی به دور است.

اما فضای سایبری صرفا مجازی نیست. این فضا شامل کامپیوترهایی است که داده‌ها را افزون بر سیستم‌ها و زیرساخت‌ها که اجازه می‌دهند این داده‌ها در جریان باشد، ذخیره می‌کنند. این زیرساخت‌ها شامل اینترنت کامپیوترهای شبکه شده، اینترانت (یا شبکه داخلی)، فناوری‌های تلفن‌همراه، کابل‌های فیبرنوری و ارتباطات مبتنی بر فضا، می‌باشد.

در حالی که بیشتر ما از "اینترنت" یا همان دنیای دیجیتال استفاده می‌کنیم، فضای سایبری در پشت کامپیوترهای مردم قرار گرفته است و نحوه‌ی ارتباطات آنها را جایگزین جامعه‌شان کرده است. یکی از ویژگی‌های کلیدی فضای سایبری این است که سیستم‌ها و فناوری‌ها، ساخت بشر است. به این ترتیب، فضای مجازی به اندازه‌ی قلمروی شناختی خود (فیزیکی یا دیجیتالی) تعریف شده است.

فضای سایبری ممکن است جهانی باشد اما "بی‌وطن" یا "عوام جهانی" نیست که هر دو این اصطلاح، گاهی در رسانه‌ها استفاده می‌شود. همانطور که ما انسان‌ها، جهان را به سرزمین‌هایی تقسیم کرده‌ایم که به آن "ملت" می‌گوییم، به نوبه‌ی خود، انسان‌ها نیز به انواعی از گروه‌های مختلف مثل "ملیت" تقسیم شده‌اند. چنین کاری نیز می‌تواند با فضای سایبری انجام شود. این امر متکی به زیرساخت فیزیکی و کاربرانی است که به جغرافیا گره خورده‌اند و به این ترتیب، مفاهیم انسانی ما مثل حاکمیت، ملیت و اموال نیز موضوع ما شده‌اند.

فضای سایبری مثل زندگی، پی‌درپی در حال تحول است. ترکیب دورگه‌ی فناوری و انسان که همیشه در حال تغییر هستند، اجبارا هر مقیاس و اندازه فضای سایبری را به نقش‌های فنی و سیاسی که به دنبال هدایت این فضا هستند، تغییر داده است. جغرافیای فضای سایبری، بسیار ناپایدارتر از محیط‌های دیگر است. کوه‌ها و اقیانوس‌ها سخت به حرکت می‌افتند اما بخش‌هایی از فضای سایبری می‌تواند با یک کلیک، تغییر کند. ویژگی‌های ضروری به قوت خود باقی می‌مانند اما توپوگرافی ثابت باقی می‌ماند. فضای سایبری امروزی، مشابه آن چیزی است که گفتیم؛ اما با فضای سایبری سال ۱۹۸۲ کاملا متفاوت است.

برای نمونه، سخت‌افزار و نرم‌افزاری که فضای سایبری را می‌سازد، در اصل برای عملیات کامپیوترها از خطوط تلفن و سیم‌های ثابت، طراحی شده بودند. دستگاه‌های تلفن‌همراه ابتدا برای افراد خاص بودند و سپس به‌صورت عمومی درآمدند. امروزه، درصد رشد تلفن‌های‌همراه طوری افزایش یافته است که دست هر کودکی یک تبلت یا تلفن‌همراه می‌بینیم.

همراه با فناوری فضای سایبری، انتظاراتی که از آن داریم نیز در حال تحول است. این فضا، هنجارهای جدیدی از رفتار را تولید کرده است. این نظر را باید بپذیریم که تمام افراد به فضای مجازی دسترسی دارند و در این فضا، همه نوع اطلاعات قرار دارد؛ از مدل مو گرفته تا بیوگرافی‌ها، مطالب آموزشی، سایت‌های خبری و... .

آنچه که به منزله‌ی خود اینترنت است در شیوه‌ای اساسی‌تر، در حال تکامل است. اینترنت به‌طور همزمان بزرگ‌تر و بزرگ‌تر شده است (هر روز حدود ۲۵۰۰۰۰۰۰۰۰۰۰۰۰۰۰ بایت به عرضه‌ی جهانی اطلاعات دیجیتالی، اضافه می‌شود) و به مراتب شخصی‌تر. به‌جای دریافت انفعالی این هجوم اطلاعات آنلاین، کاربران شخصی در حال ساخت و طراحی سایت‌ها برای استفاده‌ی شخصی هستند تا بتوانند بیشتر خود را به‌صورت آنلاین، آشکار و معرفی کنند. این سایت‌ها دامنه‌ای از شبکه‌های اجتماعی مثل Facebook و Twitter است.

بنابراین، درحالی‌که فضای سایبری یک‌بار تنها عرصه‌ی ارتباطات بود و پس از آن، تجارت‌الکترونیک (رسیدن به بیش از ۱۰ تریلیون دلار در فروش یک سال) شد، این فضا شامل آنچه که ما از آن به "زیرساخت‌های حیاتی" سخن می‌گوییم، گسترش یافته است. اینها، بخش‌های اساسی است که در تمدن مدرن امروز ما اجرا شده است اعم از کشاورزی و توزیع مواد غذایی تا بانکداری‌ها، بهداشت و درمان، حمل‌ونقل، آب و برق. هر کدام از اینها، زمانی از هم جدا بودند اما اکنون، به هم وصل شده‌اند و به فضای سایبری بوسیله‌ی فناوری اطلاعات مرتبط شده‌اند. این مجموعه با عنوان "سیستم کنترل سرپرستی و اکتساب داده‌ها" یا سیستم‌های SCADA[1] شناخته می‌شود. SCADA، سیستم‌های کامپیوتری است که فرایندهای دیگر زیرساخت‌های حیاتی را نظارت، تنظیم سوئیچینگ و کنترل می‌کنند. گفتنی است، بخش خصوصی تقریبا ۹۰ درصد از زیرساخت حیاتی آمریکا را کنترل می‌کند و شرکت‌هایی که در پشت

[1] Supervisory Control and Data Acquisition

استفاده از این فضای سایبری هستند، در میان وظایف دیگر، مسئول متعادل کردن سطح کلر آب در شهرها، کنترل جریان گازی که خانه‌ها را گرم می‌کند و اجرای معاملات مالی که ثبات قیمت ارز را نگه می‌دارد، هستند.

یکی از رئیس‌جمهورهای پیشین کشور آمریکا اذعان داشت که فضای سایبری در حال تحول، "سیستم عصبی و کنترلی اقتصاد کشور آمریکاست" و در همین راستا، سردبیر مجله‌ی Wired یعنی Ben Hammersley شرح داد که فضای سایبری، به "پلت‌فرم غالب، برای زندگی در قرن ۲۱" تبدیل شده است.

برای بسیاری، عملکرد اینترنت با آزادی بیان و اتصال خوب به شبکه‌های اجتماعی، یک نشانه نه از مدرنیته است بلکه نشانه‌ای از خود تمدن است. ما در اینترنت، زندگی می‌کنیم، کسب‌وکار می‌کنیم و ارتباط تصویری برقرار می‌کنیم. اینترنت، پلت‌فرم مرکزی تجارت، فرهنگ و روابط شخصی است. اینترنت برخلاف زندگی، لوکس نیست و برای بیشتر مردم، آگاهانه یا ناآگانه، گونه‌ای از زندگی است.

همانطور که در زندگی، هیچ‌کس نقش خود را به‌خوبی ایفا نمی‌کند، اینترنتی که ما همه با آن بزرگ شدیم و آن را دوست داشتیم، اکنون به‌طورفزاینده‌ای به محلی خطرناک تبدیل شده است.

"مسائل سایبری" از کجا پدید آمد؟

تاریخچه‌ای کوتاه از اینترنت

"Lo"، نخستین واژه‌ای بود که از طریق شبکه کامپیوتری که به اینترنت تکامل یافته، منتقل شد. این امر، سرآغاز بیانیه‌ی عمیقی مانند "Lo and behold" بود. در سال ۱۹۶۹، محققان UCLA سعی کردند که به کامپیوتری در موسسه تحقیقاتی Stanford وارد شوند؛ اما پیش از اینکه آنها بتوانند حرف "g" از واژه‌ی "log" را تایپ کنند، کامپیوتر Stanford خراب شد. با این حال، پروژه‌ی ARPANET از آنجا که توسط آژانس پروژه‌های تحقیقاتی پیشرفته (ARPA) سرمایه‌گذاری شده بود به نام ARPANET نامگذاری شد. در نهایت، نحوه‌ی به‌اشتراک‌گذاری داده‌ها و همه چیز کامپیوترها، دگرگون شد.

آنچه که باعث می‌شود اینترنت متمایزتر از شبکه‌های ارتباطی پیشین مثل تلگراف‌های قدیمی و شبکه‌های تلفنی شود، بسته‌ی سوئیچ شده به‌جای مدار سوئیچ شده است. بسته‌ها، پاکت دیجیتالی کوچکی از داده‌ها هستند. ابتدای هر بسته، اساسا "خارج" از پاکت بود یعنی بسته شامل هدری[1] بود که حاوی جزئیاتی درباره‌ی مبداء و مقصد شبکه و برخی اطلاعات پایه‌ای درباره‌ی محتوای بسته بود. با شکست جریان داده به قطعات کوچک‌تر، هر یک می‌توانست در مدی مستقل و غیرمتمرکز تحویل داده شود و سپس در نقطه‌ی پایانی، دوباره به هم وصل شوند. شبکه‌ها، هر بسته را که می‌رسید، مسیریابی می‌کردند و این یعنی یک معماری پویایی که هم انعطاف‌پذیر بود و هم ارتجاعی.

[1] Header

سوئیچینگ بسته، به دستور ایالات متحده برای حفظ ارتباطات حتی در رویدادهای حملات هسته‌ای (که باوری نادرست اما رایج بود) توسعه داده نشد. این امکان واقعا برای بهتر ساختن اتصالات کارآمدتر و قابل اعتمادتر بین کامپیوترها توسعه داده شده بود. پیش از ظهور آن در سال ۱۹۷۰، ارتباطات بین دو کامپیوتر نیاز به یک مدار اختصاص داده شده یا پهنای باند قبلا اختصاص داده شده، داشت. این امکان، ارتباط مستقیمی بود، بدین معنا که منابع نمی‌توانست توسط هیچ‌شخصی دیگر مورد استفاده قرار گیرد حتی هنگامی‌که هیچ داده‌ای منتقل نشود. با شکست این گفتگوها به بخش‌های کوچک‌تر، بسته‌ها از چند گفتگوی مجزا توانستند همان ارتباطات شبکه را به اشتراک بگذارند. همچنین بدین معناست که اگر یکی از ارتباطات شبکه‌ی بین دو دستگاه، در میان ارتباطات پایین بیاید، انتقال به‌طور خودکار بتواند بدون از دست دادن ظاهر اتصال، جایگزین شود.

ARPA (که اکنون به DARPA تبدیل شده است، که D آن، از ابتدای واژه‌ی "Defense" گرفته شده است)، سازمانی بود که توسط پنتاگون برای جلوگیری از مشکلات فناوری توسعه یافته شده بود. کامپیوترها در اواخر سال ۱۹٦۰ افزایش یافته بودند اما محققان بیشتر می‌خواستند که از آنها استفاده کنند. ARPA، به‌دنبال یافتن روش‌هایی بود که به مردم اجازه دهد در هر زمانی، از کامپیوترهای استفاده نشده در موسسات مختلف سراسر کشور، استفاده کنند.

به‌جای اختصاصی کردن و گران کردن قیمت‌ها، اتصالات بین دانشگاه‌ها، چشم‌اندازی از شبکه‌ی ارتباطات داده‌های به اشتراک گذاشته شده و اشتراک گذاری منابع محاسباتی بود. دستگاه‌های منحصربفرد، هریک با یک پردازشگر رابط پیام متصل شده بودند که به اتصالات واقعی شبکه رسیدگی می‌کرد. این شبکه، ARPANET بود و با ارسال واژه‌ی "Lo" دوران سایبری را شروع کرد.

برای اهداف مدرن اینترنت، مجموعه‌ای از بسته‌ها بین دستگاه‌ها در یک شبکه‌ی واحد فرستاده می‌شد که به عنوان "اینترنت" به حساب نمی‌آمد. اینترنت به اتصال بسیاری از شبکه‌های مختلف دلالت دارد. این شبکه‌های کامپیوتری مختلف چیزی فراتر از ARPANET است.

چالشی که مطرح بود، این بود که شبکه‌های مختلف از فناوری‌های زیربنایی بسیار متفاوتی استفاده می‌کنند. مشکل فنی، چگیده‌ی این تفاوت‌ها و اجازه دادن ارتباطات کارآمد بود. در سال ۱۹۷۳، راه‌حل پیدا شد. Vint Cerf، استاد دانشگاه Stanford و Robert Khan از ARPA، ایده‌ی پروتکل انتقال را تعریف کردند. این "پروتکل"، انتظارات یک ارتباط موثر را فراهم می کرد و آن چیزی نبود جز یک دست‌تکانی سه‌طرفه[1].

ویژگی بارز این مدل، نحوه‌ی شکستن ارتباطات در لایه‌ها بود و اینکه اجازه می‌داد هر لایه به‌طور مستقل کار کند. این لایه‌ها، به‌نوبه‌ی خود می‌توانستند بسته‌ها را به‌روی هر نوع شبکه‌ای (از امواج صدا تا امواج رادیویی) ارسال کنند. چنین پروتکل کنترل حمل‌ونقل یا TCP[2] توانست به‌روی انواع پروتکل‌های بسته

[1] Three-way handshake
[2] Transport Control Protocols

مورد استفاده قرار گیرد اما اکنون ما از پروتکلی به نام IP[1] یا پروتکل اینترنت تقریبا به‌طور انحصاری در اینترنت مدرن استفاده می‌کنیم.

این پروتکل قادر به ایجاد شبکه‌ای از شبکه‌هاست. البته، اینترنت به همین‌جا ختم نمی‌شود. لینک‌های جدیدی در اتصال دستگاه‌ها سرآمد اما انسان همیشه در ساخت فناوری‌ها با امیال خود حرکت می‌کرد. همانطور که مردم از دستگاه‌های به اشتراک گذاشته شده برای تحقیقات استفاده می‌کردند، آنها انتظار سرویسی برای ارتباط بیشتر با یکدیگر و ارسال پیام داشتند. در سال ۱۹۷۲، Ray Tomlinson در شرکت مشاوره‌ی فنی BBN، برنامه‌ی پایه‌ای را برای خواندن، نوشتن و ارسال پیام نوشت. این برنامه، e-mail یا همان پست‌الکترونیکی بود که جزء نخستین برنامه‌های اینترنتی به‌شمار می‌رفت. در طی یک سال، بالاترین ترافیک در سراسر شبکه به‌روی همین e-mail ایجاد شد. اکنون، ارتباطات شبکه شده برای مردم امکان‌پذیر بود.

آخرین مرحله در ایجاد اینترنت مدرن، از بین بردن موانع ورود به آن بود. استفاده‌ی اولیه، تنها محدود به آنهایی بود که به کامپیوترهای شبکه شده در موسسات دفاعی و تحقیقاتی دسترسی داشتند. این سازمان‌ها از طریق خطوط داده‌ی اختصاصی ارتباط برقرار می‌کردند. همانطور که مشهود است ارزش ارتباطات شبکه‌ای رشد کرد و قیمت کامپیوترها کاهش یافت و بیشتر سازمان‌ها به‌دنبال پیوستن به آن بودند. مودم‌ها، که داده‌ها را به امواج صدا تبدیل می‌کرد و آنها را برمی‌گرداند، این امکان را فراهم کرد که از طریق خطوط تلفن عمومی، لینک به کامپیوترهای دیگر صورت گیرد.

به زودی، محققان خارج از علوم کامپیوتر تمایل به دسترسی به اینترنت را داشتند، نه تنها برای استفاده از منابع محاسباتی به اشتراک گذاشته شده، بلکه برای مطالعه‌ی خود فناوری جدید شبکه. بنیاد ملی علوم آمریکا، ابرکامپیوترهای موجود در سراسر کشور را به NSFnet متصل نمود که همین امر باعث رشد سریع و گسترش مدیریت بازرگانی مورد نیاز شد. بهبود امکانات، تقاضاهای بیشتری را به ارمغان می‌آورد و نیاز بود که ظرفیت‌ها و زیرساخت‌های سازمان‌یافته نیز افزایش یابد. معماری "ستون فقرات[2]" که ترافیک بین شبکه‌های مختلف منطقه‌ای را مدیریت می‌کرد، یک راه‌حل کارآمد را ارائه کرد.

این دوران نیز، مقدمه‌ای بر کسب سود در گسترش اینترنت را فراهم کرد. به‌عنوان مثال، Vint Cerf به یک شرکت ارتباطاتی به‌نام MCI پیوست. در سال ۱۹۸۳، او تلاش کرد تا MCI mail را شروع کند. ابتدا سرویس پست‌الکترونیکی به‌روی اینترنت به‌صورت تجاری بود. در اواخر سال ۱۹۸۰، آشکار شد که مدیریت اینترنت نوپا، کسب‌وکار جامعه‌ی پژوهشی نیست. صاحبان تجاری می‌توانند پشتیبانی سرویس‌های لازم شبکه را در اینترنت ارائه دهند و همچنین به مصرف‌کنندگان مشتاق بپیوندند. بنابراین دفتر علوم و فناوری کاخ سفید ، طرحی برای گسترش و تجاری‌سازی سرویس‌های ستون فقرات اینترنت را توسعه داد.

---

[1] Internet Protocol
[2] Backbone

این طرح که بیشتر جنبه‌ی خصوصی‌سازی داشت، همزمان با اختراعات جدید مختلف و پیشرفت‌هایی حرکت کرد که اینترنت برای مردم به حد محبوبیت خود رسیده بود. در سال ۱۹۹۰، یک محقق در مرکز تحقیقاتی CERN در سوئیس، شکل نسبتا مبهم ارائه اطلاعات در مجموعه‌ای از اسناد لینک شده‌ی کامپیوتری را گرفت و یک رابط جدید شبکه برای آن ساخت. با پدید آمدن پروتکل انتقال ابرمتن یا HTTP[1] و یک سیستم همراه برای شناسایی اسناد لینک شده، مخترع جهان گسترده‌ی وب کسی نبود جز Tim Berners-Lee. چند سال بعد، محققان دانشگاه Illinois، مرورگر وبی به نام Mosaic را معرفی کردند که هم طرح وب را ساده‌سازی کرده بود و هم فعالیت جدیدی با اصطلاح "گشت زدن در وب یا همان وبگردی" را برای عموم مردم معرفی کرد.

چه بخواهیم باور کنیم یا نه، در این دوره، متاسفانه صنعت پورنوگرافی به تاریخچه‌ی اینترنت قدم برداشت. دامنه‌ی تیره‌ای که برخی برآورد کردند حدود ۲۵ درصد از تمام جست‌وجوهای اینترنتی را به خود اختصاص داد.

و سرانجام، رسانه‌های جریان اصلی، از خواب بیدار شدند و به این واقعیت رسیدند که اتفاقی بزرگ در فضای مجازی رخ داده است. همانطور که New York Times در سال ۱۹۹٤ گزارش داد که: "افزایش تجاری‌سازی اینترنت، تحول آن را به دور از یک سیستم ارتباطی محرمانه برای دانشمندان کامپیوتر آمریکایی سرعت بخشید و به یک سیستم بین‌المللی برای جریان داده‌ها، متن، گرافیک، صدا و ویدیو در میان کسب‌وکار، مشتریان و تامین‌کنندگان تبدیل شد."

اینترنت واقعا چگونه کار می‌کند؟

در فوریه‌ی سال ۲۰۰۸، پاکستان تمام ویدیوهای جهان را از آن خود کرد...

این وضعیت هنگامی رخ داد که دولت پاکستان در تلاش بود تا از دسترسی شهروندان خود به آنچه که محتوای توهین‌آمیز می‌خواندند، جلوگیری کند و به مخابرات دستور داد دسترسی به وب‌سایت YouTube را (که یک وب‌سایت به‌اشتراک‌گذاری ویدیو است) مسدود کند. برای این کار، مخابرات پاکستان به‌دروغ و اشتباه به کامپیوترهای مشتریان خود، مستقیم‌ترین مسیر برای دسترسی به این وب‌سایت را از طریق مخابرات پاکستان، اعلام کرد و سپس، کاربران پاکستانی را از رسیدن به سایت واقعی YouTube باز داشت. شبکه‌ی شرکتی که این ادعای نادرست را فراتر از شبکه‌ی خود به اشتراک گذاشته بود و اخبار دروغ مستقیم‌ترین روش برای دسترسی به YouTube را در سراسر مکانیزم اساسی اینترنت گسترش داده بود، شناسایی شد. به‌زودی بیش از دو سوم از تمام کاربران اینترنت جهان به محل جعلی YouTube هدایت شدند که خود شبکه‌ی مخابرات پاکستان نیز به نوبه‌ی خود در این هجوم اطلاعاتی غرق شد.

---

[1] Hyper Text Transfer Protocol

اثرات این رویداد، موقت بود اما به اهمیتِ دانستن چگونگی کار اینترنت، تاکید می‌کرد. بهترین راه برای بدست آوردن این درک، توجه به این است که چگونه اطلاعات از محلی به محلی دیگر در دنیای مجازی حرکت می‌کند. این درک، کمی پیچیده است اما آن را به‌گونه‌ای آسان شرح می‌دهیم.

فرض کنید می‌خواهید از یک وب‌سایت آموزنده و سرگرم‌کننده مثل وب‌سایت موسسه‌ی Brookings بازدید کنید. در اصل، شما از دستگاه‌تان درخواست می‌کنید که با کامپیوتری که در واشنگتن Brookings را کنترل می‌کند صحبت کند. دستگاه‌تان باید بداند که در آن کامپیوتر، یک اتصال برای فعال کردن ارتباط، مستقر شده است.

نخستین چیزی که کامپیوترتان به دانستن آن نیاز دارد، نحوه‌ی پیدا کردن سرورهایی است که صفحه‌ی وب Brookings را میزبانی کرده‌اند. برای انجام این کار، کامپیوترتان از شماره‌ی IP یا پروتکل اینترنت استفاده خواهد کرد که آدرس‌ها را برای نقطه‌ی پایانی به‌روی اینترنت، سرویس‌دهی کند. دستگاه‌تان احتمالا به‌طورخودکار، آدرس IP را توسط ارائه‌دهنده‌ی سرویس اینترنت‌تان یا هر شبکه‌ای که از آن استفاده می‌کنید، اختصاص می‌دهد. همچنین از آدرس مسیریاب یا مسیری که اینترنت گسترده‌تر شود، آگاه است. در پایان، کامپیوترتان، از آدرس DNS Server (سرور سیستم نام دامنه) آگاه می‌شود.

سیستم (یا سرور) نام دامنه یا همان DNS، پروتکل و زیرساختی است که در آن، کامپیوترها به نام‌های دامنه (مثل Brookings.edu)، به متناظر آدرس IP آنها (مثل 192.245.194.172) متصل هستند. DNS، جهانی و غیرمتمرکز است. معماری آن شبیه یک درخت به نظر می‌رسد. "ریشه‌ی" درخت، به عنوان نقطه‌ی جهت‌گیری سیستم نام دامنه است. در بالاترین آن، دامنه‌های سطح بالا وجود دارد. این دامنه‌ها، کدهای کشور هستند مثل us. که برای آمریکا و ir. که برای ایران است و همچنین دامنه‌های دیگر مثل com. و net. که معمولا عنوان دامنه‌های عمومی را به خود می‌گیرد. هر یک از این دامنه‌های سطح بالا، تقسیم‌بندی‌هایی دارد. بسیاری از کشورها، دامنه‌های سطح دوم خاصی نیز دارند مثل co.ir. و یا ac.ir. که بدین معنی است که دامنه‌ی نخست مربوط به کسب‌وکار و دامنه‌ی دوم مربوط به موسسات علمی و دانشگاهی می‌باشد.

دامنه‌های سطح بالا از طریق ICANN[1] که یک سازمان خصوصی و غیرانتفاعی ایجاد شده در سال ۱۹۹۸ است به‌صورت بین‌المللی کنترل می‌شود. هر دامنه‌ی سطح بالا با ثبت مجموعه‌ای از سیاست‌های داخلی خود درباره دامنه، اجرا می‌شود. سازمان‌ها مانند Brookings یا Apple یا وزارت امور خارجه آمریکا، دامنه‌ی خود را از طریق واسطه‌هایی که به آنها registrars (یا ثبت‌کننده) می‌گویند، بدست می‌آورند. این واسطه‌ها با یکدیگر برای اطمینان از اینکه نام دامنه در هر دامنه سطح بالا به‌طور منحصربفرد باقی مانده است یا خیر، هماهنگی به عمل می‌آورند. به نوبه‌ی خود، هر دامنه، زیردامنه‌های خود را مدیریت می‌کند مثل mail.yahoo.com.

[1] Internet Corporation for Assigned Names and Numbers

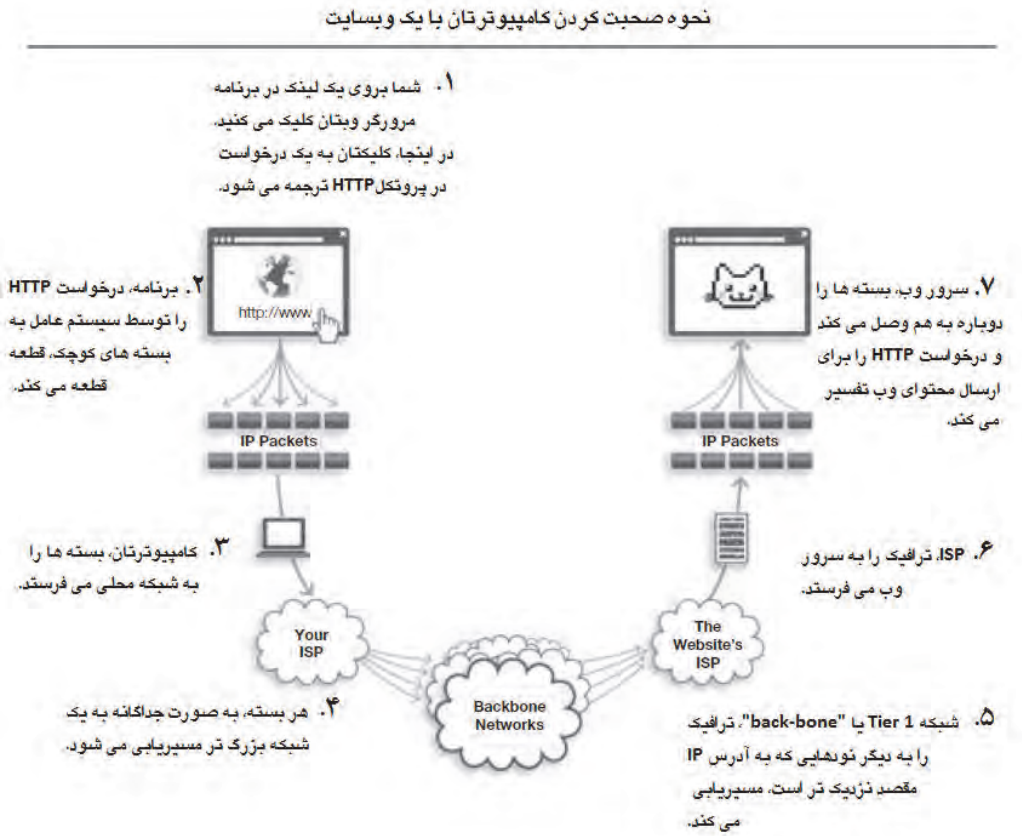
برای رسیدن به دامنه‌ی Brookings.edu، کامپیوترتان از طریق یک سری از تفکیک‌کننده‌ها[1] به سیستم DNS پرس‌وجو[2] می‌کند. دامنه‌ی edu. توسط Educause مدیریت می‌شود. Educause، سازمانی است از ۲۰۰۰ موسسه‌ی آموزشی که در آن، لیستی از دامنه‌های ثبت‌شده با پسوند edu. قرار دارد. از این لیست، کامپیوترتان، آدرس IP خاص سرور نام داخلی Brookings می‌آموزد. این امر اجازه می‌دهد که کامپیوتر، آدرس خاص را در مورد محتوا یا برنامه‌های کاربردی از داخل دامنه‌ی Brookings پرس‌وجو کند. سپس، سرور نام Brookings، کامپیوترتان را به محتوای خاصی که به دنبال آن می‌گشتید با بازگشت آدرس IP دستگاهی که آن را میزبانی کرده است، هدایت می‌کند.

در واقع، این فرایند کمی پیچیده‌تر است. به‌عنوان مثال، سرورها اغلب داده‌ها را به‌صورت محلی در کش یا نهانگاه‌ها[3] برای استفاده در آینده ذخیره می‌کنند، به‌طوری‌که هر پرس‌وجو که وجود ندارد به ریشه می‌رود و پروتکل، دارای شرایط خاص خطا برای اداره‌ی خطاهای قابل پیش‌بینی می‌باشد. با این حال، طرح بالا، چگونگی کارکرد اینترنت را به‌سادگی بیان می‌دارد.

اکنون که کامپیوترها دارای محل داده‌ها هستند، چگونه کامپیوترتان داده‌ها را دریافت می‌کند؟ سرور Brookings نیاز دارد که بداند، باید داده‌ها را به دستگاه‌تان ارسال کند و این داده‌ها نیاز دارد که دریافت شود. شکل ۱-۱ نشان می‌دهد که چگونه کامپیوترتان، یک صفحه‌ی وب را با شکست درخواست به بسته‌ها و ارسال آنها در سراسر اینترنت، درخواست می‌کند. ابتدا، در لایه‌ی کاربردی، مرورگرتان، کلیکی که برای مشاهده‌ی یک سایت در پروتکل انتقال ابرمتن انجام داده‌اید را تفسیر می‌کند. این عمل، به لایه‌های پایین‌تر یعنی لایه‌ی حمل‌ونقل و شبکه، منتقل می‌شود. لایه‌ی حمل‌ونقل مسئول شکست داده‌ها به تکه بسته‌های هم‌اندازه است و مطمئن ساختن از اینکه این تکه‌ها بدون خطا به مقصد می‌رسند و به‌طور صحیح برای استفاده در لایه‌ی بالا یعنی کاربردی، دوباره به هم وصل می‌شوند. لایه‌ی شبکه مسئول است که بهترین حرکت و جهت‌یابی بسته‌ها را در سراسر اینترنت، انجام دهد. این‌طور فکر کنید که داده‌هایی که سعی می‌کنید به عنوان پکیج اطلاعات، ارسال و دریافت کنید، لایه‌ی حمل‌ونقل مسئول بسته‌بندی و دریافت آن پکیج است و لایه‌ی شبکه، مسئول حرکت دادن آنها از مبدا به مقصد است. در اینجا، مقصد، بسته‌ها را دوباره به هم وصل می‌کند و بررسی می‌کند و سپس به بالا یعنی لایه‌ی کاربردی منتقل می‌کند- در این مورد، سرور وب، محتوای وب درخواست شده را ارسال می‌کند.

---

[1] resolvers
[2] query
[3] caches



اما چگونه بسته‌ها می‌دانند که در سراسر اینترنت به مقصدشان رسیده‌اند یا خیر؟ مانند DNS که به کامپیوترتان کمک می‌کرد تا وب‌سایتی را که می‌خواستید ببینید، پیدا کند، شبکه اینترنت سازمان نیز می‌تواند به‌صورت سلسله مراتب استدلال کند. هر کامپیوتر، بخشی از یک شبکه است مثل اتصال شبکه‌ای که به تمام مشتریان خود سرویس اینترنت را ارائه (ISP) می‌کند. ISP یا ارائه دهنده‌ی سرویس اینترنت اساسا سازمان‌هایی هستند که دسترسی به اینترنت را فراهم می‌کنند. همچنین سایر سرویس‌های مرتبط مثل پست‌الکترونیکی یا میزبانی وب‌سایت‌ها را نیز می‌توانند ارائه کنند. بیشتر ISPها، خصوصی و شرکت‌هایی غیرانتفاعی هستند.

این شبکه‌ها به نوبه‌ی خود به‌صورت گره‌هایی[1] (یا در اصطلاح نودها) هستند که سیستم خودمختار[2] (AS) در اینترنت جهانی نام دارند. سیستم‌های خودمختار، معماری اتصالات اینترنت را تعریف می‌کنند. ترافیک به‌صورت محلی از طریق AS مسیریابی می‌شود و توسط سیاست‌های آن سازمان، کنترل

[1] nodes
[2] autonomous

می‌شود. هر AS دارای مجموعه‌ای از بلوک‌های به‌هم پیوسته از آدرس‌های IP است و نقش خانه را برای این مقصدها ایفا می‌کند. تمام ISPها، دست‌کم یک اتصال به AS دیگری دارند درحالی‌که ISPهای بزرگ ممکن است اتصالات بیشتری را نیز داشته باشند. بنابراین مسیریابی به یک آدرس IP خاص به‌سادگی یک مسئله از یافتن AS می‌باشد.

مشکلی که وجود دارد این است که: اینترنت بزرگ است. امروزه بیش از ٤٠٠٠٠ نود AS به‌روی اینترنت وجود دارد و ارتباطات درونی‌شان در طول زمان تغییر و تعویض می‌شود. با توجه به این مقیاس، یک رویکرد جهانی برای مسیریابی همه چیز به همان شیوه، غیرممکن است.

در عوض، اینترنت از یک سیستم توزیع شده و پویا استفاده می‌کند که یک چشم‌انداز دائمی از آنچه که شبکه به نظر می‌رسد، حفظ نمی‌کند. اصل مسیریابی نسبتا ساده است: در هر نقطه از شبکه، روتر[1] یا مسیریاب، آدرس‌های بسته‌ی ورودی را نگاه می‌کند. اگر مقصد در داخل شبکه باشد، بسته را نگه می‌دارد و آن را به کامپیوتر مربوطه ارسال می‌کند. وگرنه، برای تعیین بهترین گام بعدی به‌منظور ارسال بسته به نزدیک‌ترین مقصد خود، از جدول مسیریابی مشورت می‌گیرد.

از آنجا که هیچ دفترچه آدرس جهانی وجود ندارد، نودها در شبکه، اطلاعات کلیدی را با روترهای دیگر به اشتراک می‌گذارد. این فرایند به‌طور جداگانه از فرایند مسیریابی اینترنت اتفاق می‌افتد. روترها همچنین همراه انتقال اطلاعات به همسایه‌های خود، اخبار به‌روزی درباره‌ی وضعیت شبکه و اینکه چه‌کسی می‌تواند با آنها صحبت کند را به اشتراک می‌گذارند. سپس هر روتر، مدل موقتی از نحوه‌ی بهترین مسیریابی ترافیکی که می‌آید را در داخلی خود، می‌سازد. این مدل جدید، به‌نوبه‌ی خود، طوری به اشتراک گذاشته می‌شود که یک روتر همسایه بداند که چگونه ترافیک جدید را منتقل کند.

اگر کمی این مباحث پیچیده است بخاطر همین مطلب بالا می‌باشد. تنها در چند صفحه، آنچه که در چند دهه از تحقیقات علوم کامپیوتر رخ داده است را مرور کردیم. ایده‌ی امنیت سایبری این است که کل سیستم بر اعتماد استوار باشد. سیستمی که به‌طور موثر کار می‌کند، می‌تواند یا با یک اتفاق تصادفی یا با یک تغذیه‌ی مخرب، نقض شود.

مثالی که درباره‌ی دولت پاکستان ارایه شد نشان می‌دهد که هنگامی‌که اعتماد مورد سوء استفاده قرار می‌گیرد، چه اتفاقی رخ می‌دهد. سانسورهای دولت با ادعای دروغ دسترسی مستقیم به آدرس IP که وب‌سایت YouTube سرویس‌دهی می‌کرد، موجب خرابی و نقض اینترنت شده بود. این امر یک اطلاعیه با انگیزه‌های سیاسی، محلی و کوته‌فکر بود. اما بخاطر نحوه‌ی کار اینترنت، به‌زودی هر ISP در آسیا سعی کرده بود که تمام ترافیک YouTubeشان را به پاکستان مسیریابی کنند، صرفا بخاطر اینکه آنها تصور می‌کردند نزدیک‌ترین مقصد واقعی در نظر گرفته شده است. آنها این مدل را براساس اطلاعات نادرست ساخته بودند. بیشتر شبکه‌ها، این ترافیک را انتقال دادند و همسایگان تصور می‌کردند که YouTube،

[1] router

آدرس IP پاکستانی است. این مشکل حل نشد تا زمانی که مهندسان گوگل، مسیرهای صحیح را در سراسر شبکه تبلیغ کردند.

در مجموع، درک معماری غیرمتمرکز پایه‌ی اینترنت، دو بینش را برای امنیت سایبری ارائه می‌کند. این بینش، بها دادن به نحوه‌ی توابع اینترنت بدون هماهنگی از بالا به پایین است و همچنین نشان می‌دهد که باید به کاربران اینترنت اهمیت داد.

چه کسی آن را اجرا می‌کند؟ درک حاکمیت اینترنت

در سال ۱۹۹۸، یک محقق کامپیوتر و یک رهبر مورد احترام در جامعه‌ی شبکه‌ای به‌نام Jon Postel، پیام بی‌ضرری را برای هشت نفر ایمیل کرد. او از آنها خواست که سرورهایشان را مجددا پیکربندی کنند به‌طوری که ترافیک اینترنت‌شان را با استفاده از کامپیوترشان در دانشگاه کالیفرنیای جنوبی به‌جای یک کامپیوتر Herndon (در Virginia)، هدایت کنند. آنها بدون هیچ سوالی، Postel (کسی که در راه‌اندازی ARPANET اصلی نقش داشت) را به‌عنوان مدیر اصلی برای سیستم نامگذاری شبکه انتخاب کردند.

با یک پست‌الکترونیکی، ابتدا Postel مرتکب کودتایی در اینترنت شد. افرادی که او به آنها، ایمیل زده بود، از هشت نفر به دوازده سازمانی تبدیل شدند که تمام نام سرورها را کنترل می‌کردند- کامپیوترها در نهایت مسئول ترجمه‌ی نام دامنه مانند "Brookings.edu" به یک آدرس IP قابل آدرس‌دهی کامپیوتر، شدند- و کامپیوترها را در Virginia که او دو سوم سرورهای ریشه‌ای اینترنت به دور از کنترل توسط دولت آمریکا بود را مورد هدف قرار داد. در حالی که Postel بعدا گفت که او کنترل بیشتر سرورهای ریشه‌ای اینترنت را به‌عنوان یک "آزمایش" به دست گرفته است و دیگران فکر کردند که او اعتراض کرده است و می‌خواسته به دولت آمریکا نشان دهد که نمی‌تواند کنترل اینترنت را از جامعه‌ی گسترده‌ی محققانی که شبکه را در طول سه دهه قبل، ساخته و نگهداری کردند، به زور بگیرد.

کودتای Postel، نقش بسیار مهمی از مسائل حکومتی را حتی برای یک فضای فنی، نشان می‌دهد. همانطور که اینترنت از یک شبکه تحقیقاتی به زیربنای جهانی از جامعه‌ی دیجیتالی ما رشد کرد، پرسشی را که چه کسی آن را اجرا کرده است به یک پرسش بسیار بسیار مهم تبدیل کرده است. Eric Schmidt (که مدیر عامل شرکتی کوچک بود که اکنون با نام گوگل شناخته شده است) در یک کنفرانس برنامه‌نویسی در San Francisco (در سال ۱۹۹۷) گفت:"اینترنت، نخستین چیزی است که انسان‌هایی ساخته‌اند که آن را درک نمی‌کنند. بزرگ‌ترین آزمایش در هرج‌ومرجی که ما تا به حال با آن مواجه شده‌ایم."

از آنجا که منابع دیجیتالی مانند منابع سنتی، کمیاب نیستند، خود پرسش حاکمیت کمی متفاوت است. به این معنا که پرسش اصلی حاکمیت اینترنت، از قابلیت همکاری و ارتباطات است، نه مسائل کلاسیک توزیعی که مصرف سیاسی متفکران از سقراط تا مارکس را دارد. با این حال، حتی در دنیای دیجیتال

منابع به ظاهر بی‌پایان، مسائل سنتی حاکمیت در فضای سایبری نیز بوجود آمده است از جمله نمایندگی، قدرت و مشروعیت.

تصمیم کلیدی chokepoints[1] (یک استراتژی دفاعی) حول استانداردهای فنی برای قابلیت همکاری، توزیع شماره‌های IP که به کامپیوترها اجازه می‌داد تا بسته‌ها را ارسال و دریافت کنند و مدیریت سیستم نامگذاری اینترنت، می‌چرخید.

عملیات اینترنت نیاز به بازیگران مستقلی دارد تا قواعد پایه‌ای که قابلیت همکاری را به عنوان استانداردها تضمین می‌کند، دنبال کنند. این رویکرد مبتنی بر استانداردها به آغاز اینترنت برمی‌گردد هنگامی‌که مهندسان ساخت سیستم‌های اولیه، "درخواست‌ها برای نظرات یا RFC[2]" را منتشر کردند تا بازخوردی در استانداردهای ارائه شده دنبال شود. با گذشت زمان، این گروه از محققان و مهندسان شبکه، سازمان استانداردی را داوطلبانه و بین‌المللی به‌نام نیروی ضربت مهندسی اینترنت یا IETF[3] رشد دادند. IETF، پروتکل‌ها و استانداردهای جدید اینترنت را توسعه داد و برای عملکرد بهتر، آنچه که موجود بود را تغییر داد. همه چیز توسط IETF تحت گروه‌های خاص کاری که در حوزه‌هایی مثل مسیریابی، برنامه‌های کاربردی و زیرساخت‌ها تمرکز داشتند، توسعه یافته بود. این گروه‌ها، انجمن‌هایی را باز کردند که کار عمده‌ی آن از طریق لیست‌های پست‌الکترونیکی بود. بسیاری از افراد در این انجمن‌ها، شرکت‌های بزرگ فناوری هستند اما هیچ‌کس یا بخش کوچکی نمی‌تواند این فرایند را زیر سلطه‌ی خود قرار دهد چراکه متکی بر اجماع است.

با وجود حس سرگرم‌کننده‌ای که بین اعضا در گروه‌های کاری IETF وجود دارد، امنیت یک نگرانی اصلی است. افزون بر گروه‌های کاری که به‌روی مسائل امنیتی خاص تمرکز دارند، هر استاندارد پیشنهاد شده باید یک بخش صریح "ملاحظات امنیتی" را داشته باشد. همچنین، ریاست بخش امنیت، تمام استانداردهای پیشنهاد شده را از گروه‌های کاری، بررسی می‌کند.

در حالی که IETF، هیچ هیئت رسمی یا رهبری رسمی ندارد، گروه راهبری مهندسی اینترنت یا IESG[4]، نظارت و راهنمایی را هم به‌روی فرایندهای استانداردها و هم به‌روی خود استانداردها ارائه می‌دهد. به نوبه‌ی خود، هیئت معماری اینترنت یا IAB[5] که از هیئت مشاوران فنی مدیریت اصلی ARPANET در اوایل سال ۱۹۷۰ تکامل یافته است، نظارت بیشتری را به‌روی IESG ارائه می‌کند.

هر دوی این سازمان‌ها زیر نظارت جامعه‌ی اینترنت یا ISOC هستند. ISOC، یک گروه بین‌المللی است که در سال ۱۹۹۲ تشکیل شد که به‌روی بسیاری از فرایندهای استانداردهای فنی نظارت کند. ISOC زمانی

---

[1] http://en.wikipedia.org/wiki/Choke_point
[2] Requests For Comments
[3] Internet Engineering Task Force
[4] Internet Engineering Steering Group
[5] Internet Architecture Board