دفاع مجازی[۱]

نوشتهٔ جیمز آدامز[۲]

ترجمهٔ: حسین سلیمی

ضعف یک ابرقدرت

درست مانند جنگ جهانی اول که جنگ افزارهایی جدید و کارزاری نوین را برای قرن بیستم معرفی کرد، در حال حاضر نیز در عصری که درحال شکل‌گیری است، انقلابی در وضعیت جنگی برای قرن بیست و یکم به وجود می‌آید. در سراسر جهان، فن‌آوری اطلاعات به طور فزاینده‌ای در نظام‌های تسلیحاتی، زیرساخت‌های دفاعی و اقتصادهای ملی رواج یافته و نفوذ می‌کند. در نتیجه، فضای الکترونیکی- سیبرنتیکی به میدان نبرد و کارزاری نوین در عرصهٔ بین‌المللی بدل می‌شود. در حالی که پیروزی‌های نظامی به فائق آمدن در رویارویی‌های فیزیکی سربازان و تسلیحات بستگی داشت، جنگ اطلاعاتی امروز با خراب‌کاری در کامپیوترها به وسیلهٔ مهاجمانی که از طرف بنگاه‌های خصوصی یا دولت‌ها اجیر شده‌اند، برپا می‌شود. به طور مثال افزایش تنش‌های اخیر میان فلسطینی‌ها و اسرائیل، یک بعد برجسته مجازی داشت. از اکتبر سال ۲۰۰۰ تا ژانویه سال ۲۰۰۱ حملات کامپیوتری که به وسیلهٔ هر دو طرف انجام شد بر بیش از ۲۵۰ وب سایت عمل کرد و مهاجمان به خوبی فراتر از مرزهای خاورمیانه به شبکه‌های کامپیوتری شرکت‌ها و گروه‌های خارجی که به نظر می‌رسد یک طرف منازعه باشند، گسترش یافت.

---

1. James Adams, Virtual Defence, *Foreign Affairs*, May/June 2001, Vol. 80. No. 3.

۲. جیمز آدامز یکی از بنیان‌گذاران و رئیس مؤسسه دفاعی است که یک مؤسسه فکری، اطلاعاتی، الکترونیکی و مدیریت بحران و مخاطره است که به دفتر مشاوره مؤسسه امنیت ملی سرویس می‌دهد. او نویسندهٔ این کتاب است: "کامپیوترها، موشک و سلاح‌ها هستند و همه جا خط مقدم جبهه است."

یک دهه پس از پایان جنگ سرد، نیروی نظامی ایالات متحده این کشور را در مسند ابرقدرتی بلامعارض در نیروهای متعارف و هسته‌ای قرار داده است. به گونه‌ای کنایه‌آمیز، برتری در پوشش نظامی و کرانهٔ فن‌آوری اطلاعاتی آن که در حال پیشروی است، ایالات متحده را به کشوری مبدل کرده که بیشترین آسیب‌پذیری را در قبال حملات الکترونیکی- سیبرنتیکی دارد. ملت‌های دیگر می‌دانند که مقابل قدرت نظامی امریکا به زیر کشیده شده‌اند، لذا توجه خود را به روش‌های دیگری معطوف کرده‌اند، که تقویت کنندهٔ توانایی‌ها و ظرفیت‌های جنگی، تهاجمی و تدافعی آنها شود، این امر "وضع جنگی نامتقارن"[1] نامیده می‌شود، که پنتاگون آن را چنین تعریف می‌کند: "مقابله با توانایی و قدرت حریف به وسیلهٔ متمرکز شدن بر نقاط ضعف او".

علاوه برآن، قوای نظامی ایالات متحده به طور ریشه‌ای در حال تحول است. "انقلاب در امور نظامی" در پی به کارگیری فن‌آوری جدید، به ویژه فن‌آوری دیجیتالی اطلاعات، در مورد مفاهیم عملیاتی و راهبردی است. این امر با طراحی رده‌های مختلف تسلیحات مبتنی بر کامپیوتر و برنامه‌های تحقیقات نرم‌افزاری انجام می‌شود که اطلاعات نظامی طبقه‌بندی شده را رمزدار و محرمانه می‌کند، قوای نظامی امریکا، با بمب‌های هدایت شونده توسط کامپیوتر "هوشمند"، تا دفاع موشکی فضایی بیشتر و بیشتر به کامپیوترها و شبکه‌های اطلاعاتی وابسته می‌شوند. این دو عامل یعنی: تسلط و برتری نیروهای نظامی متعارف ایالات متحده، و استفادهٔ وسیع و فزاینده قوای نظامی از فن‌آوری اطلاعات، زمینهٔ تهاجم الکترونیکی- سیبرنتیکی را پدید آورده که سلاحی جالب و مؤثر برای استفاده علیه ایالات متحده است.

اما طرح‌های دفاعی و مفهوم امنیت ملی نزد سیاست‌گذاران امریکا، به دست‌یابی به تمهیدات جدیدی برای جنگ کامپیوتری نیانجامیده است. فی‌الواقع هشدارهای اخیر حاکی از آن است که ایالات متحده بسیار آسیب‌پذیر است. برای رویارویی با این چالش، واشنگتن به طور ضروری و فوری نیازمند نوآوری در شیوهٔ تفکر خود و فراتر رفتن از راهبردهای بازدارندگی و امنیت ملی خود می‌باشد، زیرا این اندیشه و راهبرد در دوران جنگ سرد و در جهان ماقبل اینترنت شکل‌گرفته و تثبیت شده است.

1. Asymmetrical Warfare

ویرانگری شبانه

در ماه مارس ۱۹۹۸ وزارت دفاع وقوع بیشترین فشار و جدی‌ترین تهاجم علیه امریکا را اعلام کرد. عملیاتی متداوم و در حال گسترش که جستجوگران امریکایی رمز شناسایی آن را "مارپیچ شبانه"[1] گذارده‌اند. گروهی از خرابکاران با ابزار پیشرفته و پیچیده برای ورود و در هم شکستن صدها شبکهٔ کامپیوتری در ناسا، پنتاگون و دیگر مؤسسات دولتی و نیز دانشگاه‌های خصوصی و آزمایشگاه‌های تحقیقاتی استفاده کرده‌اند. این میهمانان ناخوانده و فضول الکترونیکی- سیبرنتیکی، هزاران فایل شامل تحقیقات تکنیکی، قراردادها، اسرار فن‌آوری و طبقه‌بندی شده و حتی اطلاعات حیاتی مربوط به نظام‌های طراحی جنگی پنتاگون را به سرقت برده‌اند.

از زمانی که مارپیچ شبانه برای اولین بار کشف شد، جامعهٔ اطلاعاتی ایالات متحده، برای بزرگترین جستجو و تحقیق اطلاعات الکترونیکی- سیبرنتیکی دست به کار شده است. اما بیش از سه سال کار آنها به طور نگران کننده‌ای، کلیدها و نشانه‌های اندکی پدید آورده است. حملاتی که آشکار شده‌اند از ۷ نشانی اینترنتی روسی سرچشمه گرفته‌اند ولی روشن نیست که ابتکار، پیشنهاد یا پشتیبانی آنها از سوی دولت باشد. سال گذشته واشنگتن اخطاریه‌ای را به دولت روسیه و ادارات رسمی که شماره تلفن‌های آنها برای حملات استفاده شده بود، اعلام کرد. پاسخ مسکو این بود که این شماره‌ها در حال کار نبوده‌اند و هرگونه اطلاع قبلی از این حملات را رد کرد.

در این حال تهاجمات و حملات خرابکارانه بی‌کم و کاست ادامه دارد. مهاجمان "دری سیاه" ساخته‌اند که از طریق آنها می‌توانند دوباره وارد نظام‌های بدون فیلتر شده و اطلاعات بعدی آنها را نیز به سرقت ببرند، آنها همچنین در پشت‌ابزارهایی که ترافیک مخصوص شبکه را از راه روسیه تغییر مسیر می‌دهد، از آن خارج می‌شوند، به‌رغم همه تلاش‌هایی که برای تجسس انجام می‌شود، ایالات متحده هنوز نمی‌داند که چه کسی در پشت این حملات قرار دارد، چه اطلاعات اضافه‌ای برده شده‌اند، و چرا؟ به کدام بخش‌های عمومی و خصوصی داخل شده‌اند و پس از خروج آنها کدام شبکه‌های دیگر هنوز می‌توانند آسیب پذیر باشند؟

دامنهٔ تخریب در این است که مارپیچ شبانه تنها یک نمونه از خطراتی است که پیش

1. Moonlight Maze

خواهد آمد. رهبران نظامی امریکا به طور فزاینده‌ای در می‌یابند که از دست دادن اطلاعات جنگ، به طور کلی و در هر زمینه‌ای به معنی سستی و ناتوانی در جنگیدن است. به طور مثال زمانی که حملات دیجیتالی نرم‌افزارها، زیربنا و شالودهٔ دفاع موشکی را سست و تضعیف می‌کند، این طرح دیگر ارزش آن را نخواهد داشت که میلیاردها دلار خرج آن شود. مخالفان و رقبای دفاع موشکی می‌توانند به وسیلهٔ حمله به منابع فن‌آوری آن و از طریق ورود و در هم ریختن شبکه‌های به هم پیوستهٔ کامپیوتری که سیستم را طراحی می‌کنند، نظام آن را در مرحلهٔ پیشرفت، دچار نقصان و نارسایی کنند و از طریق ایجاد تغییراتی جزئی هزینه‌هایی عظیم و تأخیرهایی طولانی را به وجود آورند.

آسیب پذیری و ضعف نیروی نظامی ایالات متحده در برابر حملات الکترونیکی- سیبرنتیکی در ژوئن ۱۹۹۷ روشن شد، زمانی که مجموعهٔ مشترکی از مسؤولان یک رمز آزمایشی با نام "گیرندهٔ گزیده"[1] را برای آزمایش کردن دفاع‌های کامپیوتری ملی اجرا کردند. در سناریوی آنها یک بحران نظامی در شبه جزیرهٔ کره فرض شد که واشنگتن را مجبور می‌کرد که به سرعت نیروهای کره جنوبی را به وسیلهٔ افراد و ناوگان هوایی خودی تقویت کند. سی و پنج زن و مرد از مؤسسه امنیت ملی (NSA) به چهار گروه تقسیم شدند، سه گروه در ایالات متحده و یک گروه در یک کشتی در اقیانوس آرام برای شبیه‌سازی مهاجمان کامپیوتری که از سوی کره شمالی اجیر شده بودند تا در عملیات امریکایی‌ها اخلال کنند. این مهاجمان هیچ اطلاعات پیشرفته‌ای دربارهٔ شبکه‌های اطلاعاتی ایالات متحده نداشتند و تنها می‌توانستند اطلاعات، دانش و تجهیزاتی را به کار گیرند که برای عموم قابل دسترسی است آنها حتی اجازه نداشتند که قوانین ایالات متحده را زیرپا بگذارند، و فقط می‌توانستند از کامپیوترهایی استفاده کنند که برنامه‌هایی راکه روی اینترنت به طور آزادانه امکان یافتن آن‌ها هست، مورد حمله قرار دهند.(حدود ۳۰/۰۰۰ ایستگاه اینترنتی، کدهای مهاجمان را که می‌توانست رمزهای ورودی را بشکنند. سیستم‌ها را در هم بریزد و اطلاعات را سرقت کند، ارسال نمودند).

در این مورد پس از دو هفته گروه‌هایی که از کامپیوترهای تجاری استفاده کردند، از روی برنامه‌های اینترنتی به طور همزمان حفاظ‌های ۹ شهر امریکا راشکسته و با ایجاد شکاف در ۹۱۱

1. Eligible Receiver

سیستم ایمنی توانستند به درون آنها رخنه کنند. این آزمایش ثابت کرد که مهاجمان واقعی کامپیوتری که سوء نیت هم دارند، با فشار تعداد زیادی دکمه می‌توانند این مجموعه‌های قدرت را خاموش و منحرف سازندو از عمل کردن سرویس‌های امنیتی محلی در زمان بحران جلوگیری کنند.

برای اطمینان از این درهم ریختگی غیرنظامی و سردرگمی واشنگتن، کارگزاران مؤسسهٔ امنیت ملی NSA به ۴۱ هزار از یکصد هزار شبکهٔ کامپیوتری پنتاگون حمله کردند. از این تعداد فقط ۲ مورد ثبت و گزارش شده بود. این مأموران همچنین می‌توانستند در درون شبکه‌ها پرسه بزنند و ویرانی و بدگمانی را در هر جا که رفتند بیافشانند. برای مثال آنها می‌توانستند چراغ‌های جلوی کامیون‌ها را به جای موشک‌های درخواستی یک اسکادران جنگنده F-16 بفرستند و سوخت هواپیمای ارسالی برای یک پایگاه هوایی را به سوی یک بندر تغییر مسیر دهند. مهاجمان کامپیوتری به وسیلهٔ فلج کردن و گسترش اغتشاش و سوء ظن، به آلوده سازی نظام فرماندهی و کنترل انسانی مبادرت کردند، مثلاً فرمان‌هایی از یک فرماندهی کل قلابی صادر و آشکار می‌شدند و اخبار و گزارش‌های تقلبی از بحران و ویرانی‌ها، از سوی مقامات شهری می‌رسیدند. در نتیجه در زنجیره فرماندهی از رئیس جمهور گرفته تا پائین‌ترین سطوح، هیچ کس هیچ چیز را نمی‌توانست باور کند. گروه مهاجمان هر چند از منافع قابل دسترسی برای عموم استفاده می‌کردند اما می‌توانستند به طور مؤثری از نبرد ایالات متحده با دشمنان جلوگیری کنند.

در اکتبر سال ۱۹۹۹ تمرین دومی انجام شد که رمز آن ستارهٔ زنیت[1] بود و می‌خواست درس‌های آموخته شده از "گیرندهٔ گزیده" را مورد آزمایش قرار دهد. در این فرصت، مهاجمان کامپیوتری، قدرت سیستم‌هایی که تعداد زیادی از پایگاه‌های نظامی ایالات متحده را تغذیه می‌کردند مورد آزمایش و تهاجم قرار داده و سپس ۹۱۱ سیستم امنیتی و اورژانس محلی رابا سیلی از علائم تولید شده کامپیوتری مستغرق و تضعیف کردند. این آزمایش نشان داد که پس از به وجود آمدن گیرندهٔ گزیده، بعضی از اصلاحات و به‌سازی‌ها انجام شده اما هنوز هماهنگی میان مؤسسات دولتی ضعیف است و زیرساخت‌ها و زیربناهای ملی در مقابل تهاجمات آسیب‌پذیر مانده‌اند.

1. Zenith Star

کابوس وحشتناک "گیرنده گزیده" و ستازه زنیت" همانند خراب‌کاری واقعی و مداوم مارپیچ شبانه، علائم قابل ملاحظهٔ یک جنگ جدید را دارند که قبلاً در فضای الکترونیکی سیبرنتیکی در حال کارزار بوده‌اند. این جنگ به طورعمده از منظر عمومی پنهان است، ولی زیرساخت‌های لازم برای محافظت در مقابل آن، هزینه‌های گزافی را از بخش خصوصی و میلیون‌ها پرداخت کننده مالیات در ایالات متحده، می‌طلبد. به این نحو، جنگ در محیطی آشفته و نزدیک اتفاق خواهد افتاد. به عکس دوران جنگ سرد که در آن مواضع اتمی، قواعد بازی قابل درک خود را تولید کرده و در قالب ساز وکار بازدارندگی شناخته شدند، در تهاجمات الکترونیکی- سیبرنتیکی هیچ مرز قانونی و شناخته شده‌ای وجود ندارد. وضعیت جنگی اطلاعاتی فارغ از محدودیت‌ها و با بازیکنانی همراه است که برای پیوستن به این بازی و دست و پنجه نرم کردن با هم بیش از پیش شتاب می‌کنند.

جنگ با ابزارهای دیگر

دولت ایالات متحده هم اکنون معتقد است که ۳۰ ملت برنامه‌های حملات جنگی کامپیوتری خود را توسعه داده‌اند. این فهرست روسیه و چین، دولت‌هایی چون ایران و عراق و حتی متحدان ایالات متحده مثل اسرائیل و فرانسه را نیز شامل می‌شود. نورسیدگان جاه‌طلبی مثل هند و برزیل نیز در پی آنند که در جهان کارزار مجازی، تبدیل به قدرت شوند.

امریکائی‌ها جنگ خلیج فارس را تحت عنوان "یک پیروزی عمده برای نیروهای نظامی ایالات متحده" و به عنوان اثبات توانایی ساختار دفاعی خود جشن گرفته و گرامی داشتند. ولی در بیرون ایالات متحده درس دیگری هم وجود داشت: "یک رویارویی مستقیم نظامی با ایالات متحده به طور گریزناپذیری به شکست می‌انجامد." از زمانی که امریکا به توسعهٔ نیروهای متعارف خود ادامه داد (بودجهٔ دفاعی پنتاگون در حال حاضر از جمع بودجهٔ ۱۲ کشوری که بیشترین قدرت نظامی پس از آن رادارند، بیشتر است)، دیگر کشورها به دنبال یافتن چیزهای دیگری برای امتیازات نامتقارن خود هستند. آرت مانی[1] معاون فرماندهی، کنترل و اطلاعات وزیر دفاع اظهار داشته که "مابقی جهان پی‌برده‌اند که نباید در یک مواجههٔ نظامی در برابر ایالات

1. Art Money

متحده قرار گیرند، اما ممکن است بتوانند آن را از طریق صدمات جدی دیگری در یک راه انحرافی به زیر بکشند"، از دیدگاه وی "نقطهٔ ضعف ایالات متحده در اینجا است."

یکی از کشورهایی که اطلاعات امریکایی‌ها را به طور نزدیک ضبط می‌کند، چین است که فعالانه به کشف نقاط آسیب‌پذیری احتمالی جدید امریکایی‌ها مشغول است. به دلیل آن که پکن دریافته که ایالات متحده اصلی‌ترین خصم این کشور در قرن بیست و یکم است، رهبران نظامی چینی و سیاست‌سازان آن، تلاش نافذ و مؤثری را برای اجرای درسی دارند که در جنگ خلیج فارس از نیروهای نظامی امریکا آموخته‌اند.

بحث‌های داغ و هیجانی چینی‌ها در این باره که چگونه به هر ترتیب ممکن، یک امتیاز و برتری نظامی نسبت به ایالات متحده پیدا کنند، پاسخ ناقص خود را در کتاب "وضعیت جنگی نامحدود"[1] بازیافته که توسط دو سرهنگ ارتش آزادی‌بخش خلق (PLA)، ژیانولیانگ و وانگ جیانگ نوشته شده است. این کتاب به روشنی در این باره است که چگونه جنگ خلیج فارس آخرین هیاهو برای شیوهٔ قدیمی جنگ‌آوری بوده است.

"عصر هم‌گرایی فن‌آوری و جهانی شدن رابطهٔ میان تسلیحات و جنگ را دوباره تنظیم کرده است.. آیا تهاجم یک مهاجم کامپیوتری تنها، اقدامی خصمانه از سوی دشمن محسوب می‌شود؟ آیا می‌توان ابزارهای مالی راکه برای نابودی اقتصاد یک کشور استفاده می‌شود، به عنوان یک صحنهٔ کارزار تلقی کرد؟ آیا تبلیغات CNN در مورد کشاندن جنازه یک سرباز امریکایی در خیابان‌های موگادیشو، لرزش تسلط امریکا به عنوان پلیس جهانی و به این طریق جایگزینی وضعیت استراتژیک جهان است؟ ولی ما ناگهان در می‌یابیم که تمامی این اعمال غیرجنگی ممکن است عوامل جدیدی باشد برای ساختن وضعیت جنگی آینده، ما به این سو خواهیم رفت که بر این شکل جدید جنگ، نامی تازه بگذاریم: جنگی که از تمامی مرزها و محدوده‌ها فراتر رفته و به طور مختصر: "وضع جنگی نامحدود".

نویسندگان معتقدند که چین هرگز نمی‌تواند با برتری فن‌آوری آمریکایی برابری کرده و هماورد آن شود. به علاوه این تجربه نیز قابل یادآوری است که مسکو خود را وقف تلاشی ناهوشیارانه برای پیروزی در رقابت نظامی در دوران جنگ سرد کرد، لذا چین در پی آن خواهد

1. Unrestricted Warfare

بود که از اشتباهی مشابه اجتناب ورزد. در عوض حملهٔ دیجیتالی امتیازی نامتقارن و پراهمیت به چین می‌دهد که نویسندگان حتی شکست ایالات متحده توسط آنها را مطرح می‌کنند. در نتیجه چین سرمایه گذاری عمده‌ای در فن‌آوری جدید برای ارتش آزادی‌بخش خلق کرده و یک دفتر رزمی- اطلاعاتی ویژه را برای هماهنگ کردن حملات و دفاع ملی تأسیس نموده است. ناظران امور چین در پنتاگون از این تلاش‌ها به عنوان پیدایش یک "دیوار آتش عظیم چین" یاد کرده‌اند.

بخشی از این عمل تهاجمی به این دلیل است که چین سوءظن برده که قبلاً مورد حملهٔ الکترونیکی- سیبرنتیکی از سوی ایالات متحده واقع شده است. تمامی قطعات سخت افزار و نرم افزار کامپیوتر که از امریکا یا متحدان آن وارد می‌شود، زمان رسیدن به مرزها مورد بازرسی و بازبینی دقیق قرار می‌گیرد. تکنسین‌های خود چین نیز سپس محصولات و هر مقاومت یا قطعه‌ای که متخصصان غربی بر روی تجهیزات خود نصب کرده‌اند را مورد کنترل قرار می‌دهند.

چنین محدودسازی و کنترلی در روسیه نیز اجراء می‌شود، درجایی که رهبران سیاسی و نظامی پذیرفته‌اند که در جنگ الکترونیکی- سیبرنتیکی درحال شکست از ایالات متحده هستند. در دو سال گذشته، مسکو به آرامی در میان اعضای شورای امنیت سازمان ملل تلاشی برای تهیهٔ پیش‌نویس یک معاهدهٔ کنترل تسلیحاتی در فضای الکترونیکی- سیبرنتیکی انجام داده است. ایالات متحده و متحدان آن متن پیشنهادی را رد کردند زیرا از موضع ملتی ناامید با اقتصاد اطلاعاتی ضعیف که در حال شکست درجنگ الکترونیکی- سیبرنتیکی تهیه شده بود. در واقع از چشم‌انداز قدرت‌های دارای فن‌آوری اطلاعاتی مثل امریکا، معاهدهٔ کنترل تسلیحات که بیشتر به نفع ملت‌های شکست خورده در منازعه است، معنایی ندارد.

ناامنی ملی

اگرچه ایدهٔ مسکو برای یک معاهدهٔ بین‌المللی برای محدودسازی جنگ اطلاعاتی دور از دسترس به نظر می‌رسد، اما مفهوم یک رژیم بازدارنده مؤثر برای فضای الکترونیکی- سیبرنتیکی در واشنگتن نیز رواج و اعتبار دارد. همانطور که انقلاب اطلاعات گامی دسته جمعی بود، فراوانی و ناخالص سازی حملات به شبکه‌های ارتباطات و کامپیوتری ایالات متحده نیز چنین است. این حملات به روشنی خیره کننده‌ای گویای دو تحول خطرناک در ساختارهای نظامی و امنیت ملی

ایالات متحده است.

اولاً در طی جنگ سرد، واشنگتن مراحل توسعه فن‌آوری را با سرمایه گذاری ۷۰٪ از تحقیقات فن‌آوری کنترل می‌کرد. امروز این اندازه کمتر از ۵٪ است ابتکار و نوآوری در فن‌آوری هم اکنون در خدمت منافع خصوصی است که از وابستگی به سیستم‌های کهنه و مهجور واشنگتن امتناع می‌کند. در عوض سرمایه گذاران و گردانندگان فن‌آوری در تکاپوی افزایش بی‌وقفه و دائمی سرعت تحولات هستند.

این جابه‌جایی از سرمایه گذاری عمومی به خصوصی با توسعهٔ یک برنامهٔ جدید تسلیحاتی که با عنوان کامپیوترهای شخصی شناخته می‌شود، همراه شده است. مهمات این تسلیحات- ابزارهای حملهٔ کامپیوتری- به صورت آزاد و رایگان در شبکه‌ها وجود دارند و همیشه هم به روز هستند. یک فرد فقط نیاز به دسترسی به یک کامپیوتر، امکانات اینترنت واندکی زیرکی و زبردستی تکنیکی دارد تابه یک جنگجوی اطلاعاتی بدل شود. برخلاف تسلیحات قرن بیستمی که مدتی نزدیک به پانزده سال برای ورود به بخش نظامی را نیاز داشت، امروزه جدیدترین انواع کامپیوترها و نرم‌افزارها که در همه جا قابل دست‌یابی است، این امکان را برای همه در یک زمان فراهم ساخته است.

ثانیاً خطوط جبهه در جنگ جدید تغییر کرده است. در قرن گذشته، جبههٔ سرنوشت ساز جنگ، عموماً در مکانی تلقی می‌شد که سربازان، ملوانان و خلبانان در موقعیت جنگی در مقابل یکدیگر قرار می‌گرفتند. برای ایالات متحده که در مرزهای خود همسایهٔ متجاوزی نداشت، دفاع از میهن به معنی توسعهٔ قدرت ماورای بحار در زمانی بود که منافع امریکا به خطر می‌افتاد. از هنگامی که این ملت بنیاد گذارده شد، این راهبرد به خوبی کار می‌کرد، برخلاف بیشتر قدرت‌های بزرگ جدید، ایالات متحده به ندرت مورد تاخت و تاز و تجاوز نیروهای خارجی واقع شده است.

اما درجهان الکترونیکی- سیبرنتیکی این پارادایم تغییر کرده است. برای اجتناب از رویارویی مستقیم نظامی با نیروهای ایالات متحده متجاوزان بالقوهٔ خارجی روی به تهاجم علیه نرم‌افزارهای پایه‌ای امریکا در قالب "بخش خصوصی" آورده‌اند. در عمل تلافی کردن این تهاجم از تلافی نظامی بسیار دشوارتر است زیرا ریشهٔ این تهاجم ناشناخته است و مرتکبان آن در

شبکه‌های شهری و یا فرماندهی نظامی خرابکاری می‌کنند. هم اکنون بخش‌های خصوصی و عمومی در کنار هم خط مقدم جبههٔ جنگ قرن بیست و یکمی را تشکیل می‌دهند و شهروندان غیرنظامی احتمالاً اولین اهداف آن هستند.

به رغم علائم هشدار دهنده، ایالات متحده هنوز اولویت و اهمیت درجهٔ یکی به تهدید بخش خصوصی نمی‌دهد و به گونه‌ای کارآمد برهمکاری میان شهروندان و دولت در این دفاع پافشاری نمی‌کند. در موارد بسیاری، واشنگتن به خاطر ردکردن اطلاعات مربوط به تهدیدات بخش خصوصی، به لحاظ قانونی تحت فشار و اجبار باقی مانده است. به طور مثال مقامات اطلاعاتی اکنون معتقدند که عمدهٔ سخت افزارها و نرم‌افزارهای وارد شده از روسیه، چین، اسرائیل، هند و فرانسه، با تمهیداتی آلوده شده‌اند و می‌توانند اطلاعات را بخوانند یا سیستم‌ها را نابود کنند. نام این شرکت‌ها و تولیدات مشکوک، برای بخش خصوصی قابل دسترسی نیست، به همین دلیل نیز اطلاعات و آمارهای آن، با درجه‌ای بالا طبقه‌بندی شده‌اند و امکان شناخت و تردیدها و گمانه‌زنی وجود ندارد.

به علاوه، وضعیت دفاعی ایالات متحده براساس قدرت‌نمایی طراحی شده نه برای دفاع از سرزمین اصلی، به همین دلیل نیز شبکه‌های اطلاعاتی وارتباطاتی کشور آسیب‌پذیر شده‌اند. اخیراً هیچ سازوکاری برای دفاع مؤثر از شبکه‌های کامپیوتر مراکز اداری و تجاری، دریچه‌های مشبک برق فشار قوی شهرهای امریکا، وحتی شبکه‌های اطلاعاتی دولت فدرال وجود ندارد. در واقع دفاع الکترونیکی- سیبرنتیکی به اف.بی.ای واگذار شده، درحالی که این مؤسسه برای پی‌گیری قانونی و مجازات جنایت‌کاران است، نه مؤسسه‌ای برای دفاع از یک ملت. علاوه بر آن، کوشش‌های اف.بی.ای برای هماهنگ سازی یک دفاع الکترونیکی- سیبرنتیکی به خاطر فقدان منابع و مهارت‌های تکنولوژیکی، بی‌فایده و مختل خواهد شد. گمان می‌رود که این اداره در پی هماهنگ‌سازی و سهیم کردن اطلاعات بخش‌های خصوصی و دولتی است، اما در واقع برنقش سنتی خود یعنی اجبار قانونی متمرکز شده است.

عکس‌العمل سازمان اداری کلینتون به این چالش‌ها، پراکنده و سازمان نیافته بوده است. تصور می‌شد که فرماندهی جنگ الکترونیکی- سیبرنتیکی با شورای امنیت ملی باشد، اما این امر چندان جامهٔ عمل به خود نپوشید. روابط بین اف.بی.ای با شورای امنیت ملی وخیم و روابط

شورای امنیت ملی با پنتاگون خراب‌تر از آن بود، آنها به لحاظ اداری یکدیگر را نمی‌پذیرفتند و حتی با یکدیگر گفتگو نمی‌کردند. همکاری میان بخش‌های نظامی نیز ضعیف باقی مانده است، به رغم آن که تلاش‌هایی شد تا مجموعهٔ جنگ کامپیوتری زیرنظر یک واحد یعنی فرماندهی فضایی ایالات متحده قرار گیرد. با این حال هر بخشی با دوباره کاری‌های وسیع و عظیم، ظرفیت‌های جنگ اطلاعاتی خودش را با هزینه‌های بسیار سنگین گسترش داده است. بر همین منوال، سیا، مؤسسه دفاع اطلاعاتی و ناسا نیز هر یک تلاش‌هایی مستقل و جداگانه برای جنگ اطلاعاتی انجام داده‌اند و حداقل همکاری و هماهنگی را با هم داشته‌اند.

سخت‌گیری

پس از جنگ جهانی دوم انفجار دو بمب اتمی در ژاپن، آنقدر وحشت آفرین بود که اقداماتی سریع و تهیج کننده در درون دولت‌های جهان و مجامع آکادمیک به وجود آورد که در زمان ما به توسعهٔ استراتژی بازدارندگی هسته‌ای انجامید. جهان فهمید که یک حملهٔ هسته‌ای علیه امریکا یا یکی از متحدان آن، یا علیه شوروی و متحدانش می‌تواند در لحظهٔ آغازین، پاسخ و تلافی هسته‌ای داشته باشد. طراحان امور دفاعی سپس چنین راهبرد بازدارنده‌ای را نیز برای جلوگیری از کاربرد سلاح‌های شیمیایی و بیولوژیکی طراحی کردند. در طی جنگ خلیج فارس به عنوان مثال صدام حسین دریافت که اگر سلاح‌های شیمیایی یا بیولوژیک به کاربرد باید انتظار عکس‌العملی ویرانگر و انهدامی نامعین را داشته باشد.

اما بدون یک راهبرد بازدارندهٔ ایالات متحده برای تلافی و مقابله به مثل در جهان مجازی و بدون اندیشه‌ای روشن در موردیک رژیم حقوقی برای تلافی در مقابل تهاجم الکترونیکی- سیبرنتیکی، مهاجمان کامپیوتری می‌توانند بدون هراس و خطری وارد کارزار با امریکا شوند. به آنچه در ماه مه سال ۲۰۰۰ میلادی رخ داد توجه کنید. در آن زمان یک مهاجم کامپیوتری در فیلیپین ویروس "نامهٔ عشق" را در سرتاسر جهان منتشر کرد. در ایالات متحده مدیریت بهداشت سربازان قدیمی، ۷ میلیون پیام "دوستت دارم"[1] دریافت کرد، ۱۰۰۰ فایل ناسا صدمه دیدند و بازسازی خسارات ناشی از این حملات به ادارهٔ کار، به بیش از ۱۶۰۰ نفر- ساعت کار، و ۱۲۰۰ ساعت

1. I Love you

پیمانکاری نیاز داشت. هزینهٔ این حمله به ایالات متحده بین ۴ تا ۱۵ میلیارد دلار تخمین زده می‌شود یا معادل "بمباران همه جانبه" یک شهر امریکایی در جنگ‌های متعارف. هر چندآن مهاجم کامپیوتری دستگیر شد اما پس از مدتی آزاد گردید، زیرا قوانین فیلیپین برای مقابله با چنین جرائمی طراحی نشده است.

مداوایی برای این ویروس

مسائل نظام دفاع کنونی ایالات متحده و پارادایم امنیت ملی به راحتی قابل توضیح است. اما علاج حملهٔ مجازی به وسیلهٔ بازدارندگی و دفاع مؤثر بسیار دشوارتر است. نظم بخشیدن به مرزهای جدید جنگ اطلاعاتی نیازمند راهبردی نیرومند و تاکتیک‌های دقیق و استوار خواهد بود.

مسؤولیت نخستین، ابتدایی و اصلی دفاع الکترونیکی- سیبرنتیکی ملت باید بر عهدهٔ بخش "دفاعی" باشد. شورای امنیت ملی در هدایت جنگ در کارزار کامپیوتری شکست خورده است. بخشی از آن به این دلیل است که فاقد بازوان و ابزارهای مالی و نظامی لازم برای انجام این کار است. در مارپیچ اداری واشنگتن، بخش‌ها و مؤسسات مختلف در رقابت و هم‌چشمی برای پول هستند و به نظر می‌رسد تهدید الکترونیکی- سیبرنتیکی تنها بهانهٔ دیگری برای پیروزی در رقابت تأمین منابع بیشتر مالی است. اما این امر باید به عنوان وظیفهٔ شبکهٔ دفاعی تلقی شود. زیرا این بخش فاقد منگنه‌ها و تنگناهای اداری است، شورای امنیت ملی دربارهٔ تهدیدات الکترونیکی- سیبرنتیکی امنیت ملی هشدار می‌دهد که خود تاکنون نسبت به آن بی‌اعتنا بوده است.

اف.بی.ای منابع، ابزارها و آموزش‌های لازم را برای تحقیق و شناسایی مهاجمان دارد و می‌تواند نقشی حیاتی در مبارزه با جرائم سیبرنتیکی- الکترونیکی ایفا کند، ولی نباید در جنگ مشارکت ورزد. حضور آن در گسترش ارتباط بین دولت و بخش خصوصی پی‌آمدهای ناامید کننده‌ای به بار آورده است. مسؤولان رسمی اف.بی.ای در مورد این طرح معتقدند که اداره آن‌ها به نقش خود در دفاع الکترونیکی- سیبرنتیکی متعهد نیست و افراد، پول و فن‌آوری لازم را برای آن تخصیص نداده است.

به طور حتم تردیدهایی در مورد حکمت آن که پنتاگون سرپرستی دفاع اطلاعاتی را برعهده گیرد، وجود دارد. دشمنان خارجی ایالات متحده، رودرروی سرویس‌های نظامی امریکا قرار می‌گیرند که مرجع حفاظت و دفاع از ملت هستند، به همین نحو نیز مؤسساتی چون اف.بی.ای باید ناظر و مجری حقوق شهروندان امریکایی باشند، حقوقی که قوانین داخلی در مورد آنها ایجاد اجبار و ضرورت می‌کند. در نتیجه قانون سازان و آزادی گرایان اجتماعی و غیرنظامی به گونهٔ قابل درکی از گسترش قدرت نظامی در داخل سرزمین اصلی خشمگین می‌شوند. ولی ایالات متحده دو امکان و دارایی استفاده نشده دارد که بهره گیری از آن باعث اجتناب از این حرکت متداوم خواهد شد: "ذخیره‌های نظامی" و "گارد ملی". این گروه‌ها قبلاً از مهارت‌های تکنولوژیکی که برای راه‌اندازی یک دفاع مؤثر اطلاعاتی مورد نیاز بود، برخوردار بودند زیرا پرسنل آن‌ها هم زمان در بخش‌های خصوصی صاحب تکنولوژی نیز حضور داشتند. "دفاع از وطن" با همکاری پنتاگون و استفاده از گارد ملی و نیروهای ذخیره، راهی است که می‌تواند از شبکه‌های امریکا محافظت کند.

پنتاگون منابع لازم رابرای هدایت و مدیریت دفاع اطلاعاتی دارد اما میلی به انجام این مأموریت نداشته است. برای برعهده گرفتن این نقش جدید و اضافی نیازمند تنظیم دربارهٔ اولویت‌های بخش دفاع، تقسیم دوبارهٔ منابع و برآورد سنتی قدرت، برای دفاع از وطن هستیم. اما به هرحال دفاع ملی کار پنتاگون است و در عصر اطلاعات، دفاع ملی باید شامل دفاع الکترونیکی- سیبرنتیکی نیز باشد.

برای طراحان امور دفاعی، جهت هماهنگ ساختن راهبردی برای فضای الکترونیکی- سیبرنتیکی باید تعریفی دوباره از امنیت ملی و روش‌های مناسب مدیریت آن ارائه شود. "امنیت ملی" اغلب به معنی حفاظت از مرزهای ملی در مقابل تهاجم بیگانگان است و برداشت موجود ازمنافع ملی غالباً به حفاظت از قدرت نظامی امریکا در ماورای بحار برای دفاع از وطن منجر می‌شود. اما همان‌طور که چینی‌ها به درستی دریافته‌اند، جنگ آینده متمرکز در مرزها و مناقشات سرزمینی نخواهد بود. به علاوه، این که تصمیمات نتیجهٔ یک منازعه باشد قبلاً در عرصهٔ کارزار شکست خورده است و در هیچ جنگی، تهاجم به بخش خصوصی یک کشور اولی بر حمله به مجتمع‌های صنعتی آن نبوده است. با وجود این در فضای الکترونیکی- سیبرنتیکی امتیازی

نامتقارن برای هرکسی وجوددارد که درک کند یک تهاجم کامپیوتری موفق علیه شبکه‌های اطلاعاتی بخش خصوصی، تأثیر یک حمله تسلیحاتی توسط نیروهای نظامی را دارد. این برای فرماندهان نظامی و رهبران سیاسی مفهومی ناراحت کننده خواهد بود ولی باید آن را درک کرده و فرصت آن را غنیمت شمرند، زیرا این امر اولاً نیازمند پذیرش ضرورت برداشتن موانع و سدهای موجود مابین بخش‌های دولتی و خصوصی است و ثانیاً شامل نوآوری‌های راهبردی است که مهارت‌های تکنولوژیک جدید را به بخش خصوصی بدهد و آسیب‌پذیری آن را به حساب آورد.

علاوه بر آن، دفاع مؤثر به معنی بازدارندگی از حملات قبل از وقوع آنها است. تهدید به تلافی و مقابله به مثل، یک استراتژی بازدارندهٔ خوب است. همه ملت‌ها پیشاپیش، نتایج استفاده از تسلیحات کشتار جمعی علیه ایالات متحده را می‌دانند. واشنگتن باید به همین شیوه جهان را متوجه سازد که اقدام به یک تهاجم الکترونیکی- سیبرنتیکی علیه هر موجود امریکایی، اقدام به جنگ خواهد بود و عکس‌العمل مناسبی در پی خواهد داشت. این امر نیز باید روشن شود که ایالات متحده بین روش‌های مختلف حمله تفکیک وجداسازی نخواهد کرد، حال می‌خواهد اصابت یا انفجار یک بمب باشد یا یک ویروس کامپیوتری، این کشور تنها به اثرات آن اهمیت می‌دهد. ولی به هر حال اقدامات تجاوزکارانه علیه شبکه‌های اطلاعاتی ایالات متحده به وقوع خواهد پیوست و باید راهنمائی‌ها و رهنمودهایی برای عکس‌العمل در مقابل آنها توسعه یابد. همان‌گونه که واشنگتن از "مارپیچ شبانه" آموخته، انداختن تقصیر به گردن گروه‌ها یا ملت‌های خاص سخت و دشوار است. بسیاری از ملت‌ها با چالش‌های مشابه از تروریسم در اواخر دههٔ ۱۹۶۰ و اوایل دههٔ ۱۹۷۰ مواجه بودند، در آن زمان آنها از کمبود انتقادآمیز اطلاعات، همکاری اندک میان دولت‌ها و فقدان ظرفیت دفاع شهری یا نظامی برای حفاظت از پدیدهٔ جدید و فراملی تروریسم لطمهٔ فراوانی دیدند. با این حال در اواسط دههٔ ۱۹۸۰، اطلاعات به طور شگفت‌انگیزی گسترش یافت، ملت‌ها بیشتر با هم به همکاری پرداختند و سنجش‌های دفاعی در مکان خود قرار گرفت. نتیجهٔ آن مهار مشکل تروریسم بود، هر چند این مسأله هرگز به طور کامل ریشه کن نخواهد شد. اقدام مشابهی نیز لازم است در فضای الکترونیکی- سیبرنتیکی اعمال شود.

اگر ایالات متحده می‌خواهد به گونه‌ای مؤثر در مقابل تهاجم الکترونیکی- سیبرنتیکی عکس‌العمل نشان دهد، در درجهٔ اول باید بداند چه کسی مسؤولیت این تجاوز را برعهده دارد.

یافتن مجرمانی که از طریق شبکه‌های کامپیوتری عمل می‌کنند، چالشی سخت و دشوار است. تهاجم به فضای الکترونیکی- سیبرنتیکی می‌تواند به طور هم زمان از چند نقطه بیاید، و ریشه و نقطهٔ شروع خود را عوض کرده و یا مبدل سازد. برای مثال در فوریه سال ۱۹۹۸ زمانی که تنش‌هایی دوباره با عراق در گرفت، پنتاگون مجموعهٔ کار کشته و زبردستی از نفوذی‌ها را، که به درون تعدادی از سیستم‌های اطلاعاتی بخش دفاعی نفوذ کرده بودند، کشف کرد. این حملات که رمز ورودی "طلوع شمسی"[1] داشتند به نظر می‌رسید طراحی شده باشند تا اطلاعات طرح‌های ایالات متحده برای اقدام در عراق را گرد آورند و سیستم‌های فرماندهی و کنترل و گزارش‌دهی را متلاشی سازند. فرض می‌شد که این حملات از سوی عراق سازمان‌دهی شده است و ریشهٔ آن نیز در ابوظبی ردیابی شده بود. یک نیروی اکتشافی برای آن نزد دولت‌های خلیج فرستاده شد و پس از اخذ مجوزهای لازم از دولت‌های آنان وارد ساختمانی شدند که می‌پنداشتند گروه کامپیوتری عراق در آن مخفی شده‌اند. ولی در حقیقت هیچ عراقی در آن ساختمان ساکن نبود و تنها پردازشگرهای[2] کامپیوتری بودند. آن حملات به دستور بغداد انجام نشده بود و ابوظبی به سادگی ردپایی نادرست بود که توسط مهاجمان کامپیوتر وارد شده بود. به طور خلاصه، بعدها دو نوجوان در کالیفرنیا دستگیر شدند و روشن شد که آن‌ها و یک مهاجم کامپیوتری اسرائیلی "طلوع شمسی" را اجراء کرده بودند و انگیزهٔ آنها هیچ ربطی به اقدام علیه عراق نداشت.

سیاست‌گذاران ایالات متحده همچنین باید مسائل حقوقی و اخلاقی مطرح دربارهٔ تلافی و مقابله به مثل در جنگ اطلاعاتی را حل کنند. براساس اصول حقوقی که به طور نسبی درمورد مسائل مربوط به حاکمیت ملی اعمال می‌شود، یک ملت تمامی حقوق لازم را برای استفاده از زور برای دفاع از خود در مقابل یورش تهاجم آمیز سرزمینی دارد. ولی هیچ ادراک روشنی از این وجود ندارد که چگونه باید این قانون را به طور نسبی دربارهٔ جنگ اطلاعاتی نیز به کار برد. زیرا جمعیت شهری غیرنظامی را بسیار وسیع‌تر از جنگ‌های سنتی درگیر می‌سازد. اگر چین شبکه‌ای از حملات برای خاموش کردن برق را در وسط زمستان شیکاگو اجرا کرد، و تعداد زیادی از ساکنان شهر کشته شدند، آیا ایالات متحده توجیه و مجاز است که با سیستم‌های کنترل از راه دور،

1. Solar Sunrise
2. Servers

دریچه‌های یک سد را در چین بالا ببرد و چینی‌هایی را که در مقابل آن زندگی می‌کنند، هلاک سازد؟ آیا پاسخ دادن به یک تهاجم الکترونیکی- سیبرنتیکی با نیروهای نظامی متعارف، به لحاظ قانونی، اخلاقی یا سیاسی قابل پذیرش است؟ اینها سؤالاتی دشوار هستند که رزمندگان کامپیوتری و حقوق دانان را به یک اندازه ناراحت و مأیوس ساخته‌اند.

در چنین فضای گیج کننده‌ای، مؤسسات اطلاعاتی باید منابع و روش‌های خودرا پیشرفت دهند. آنها مجبور خواهند بود که وسایل و ابزارهای جدیدی را برای حمایت از گروه‌های مختلف بخش خصوصی یا دولتی که برای جنگ در فضای الکترونیکی - سیبرنتیکی اجیر شده‌اند، توسعه دهند. سیاگروهی از دشمنان ایالات متحده را هدف گرفته و عملیاتی را علیه آنها پوشش می‌دهد، چنین روشی نیز باید در مقابل کسانی که شبکه‌های کامپیوتری را به عنوان صحنهٔ کارزار از خودبرگزیده‌اند، به کار رود.

پیچیده شدن مؤسسات اطلاعاتی که وظیفهٔ یافتن مهاجمان کامپیوتری را دارند، واقعیتی است که نشان می‌دهد این مهاجمان می‌توانند از ریشه‌ها، مبدأها و زمینه‌های مختلفی استفاده کنند، چنانچه حمله‌ای که به نظر می‌رسد از لندن نشأت گرفته در واقع ریشه در برزیل دارد و به سوی ایالات متحده و از طریق مسکو و آنتورپ[1] گذر می‌کند. ردیابی یک ویروس پست الکترونیکی به منابع آن باز می‌گردد، به طور مثال نیازمند شناخت مراجع شخصی هستیم که از مسیر قلمروهای حکومتی و قضایی عبور کرده است. این کار طاقت فرسا، توانایی اجبارسازی قانون رابرای دستگیری یک مهاجم و نیز توانایی پنتاگون را برای تلافی، محدود می‌سازد. کنگره باید قوانین جدیدی را به تصویب رساند که اجازه دهد کسانی که بدون مجوز از طریق اینترنت وارد می‌شوند، تحت تعقیب قرار گیرند. قوانین دیگری نیز مورد نیاز است که به عاملان و مجریان قانون اجازه دهد که هنگامی که یک جرم الکترونیکی- سیبرنتیکی اتفاق می‌افتد، همانطور که می‌توانند خطوط تلفن را تحت کنترل قرار دهند، به شبکه‌های کامپیوتری نیز نفوذ کنند. اگر اولویت این مسأله برای امنیت ملی روشن شود، چنین کنترل‌هایی به وسیلهٔ قانون مجاز شمرده می‌شوند. کنگره از قبل مرجع تصویب چنین قوانینی بوده است، در واقع جامعهٔ اطلاعاتی- امنیتی محل و منبع جمع کردن اطلاعات از شبکه‌های کامپیوتری خارجی هستند. ولی برای کنگره به-

1. Antwerp

دست آوردن اعتبار قانونی لازم و تغییر مسیر سیاسی برای گذر از سنجش‌های مؤثر و قابل ادراک و همکاری با دیگر دولت‌ها، لازم است.

در طی جنگ سرد، ایالات متحده و پایه گذاران سیاست خارجی آن به خوبی تشخیص داده بودند که یک مخاصمهٔ نظامی می‌تواند دسترسی به منابع حیاتی نفتی را تهدید کند. واشنگتن این مشکل را بااین وسایل مدیریت کرد: قرار دادن منابع در مناطق ریسک، گسترش نیروهای واکنش سریع و شکل دادن اتحادهای بین‌المللی. در زمان وقوع مخاصمه، نیروهای امریکا و متحدانش می‌توانستند به سرعت برای حفاظت از منابع نفتی وارد عمل شوند، همان‌گونه که در جنگ خلیج فارس اتفاق افتاد. چنین راه حلی در جهانی که حملات رایانه‌ای دسترسی امریکائی‌ها به منابع حیاتی اقتصادی مشابهی را یعنی شبکه‌های کامپیوتری، قطع می‌کند نیز می‌تواند وجود داشته باشد. اگرچه ایالات متحده بعضی تسلیحات الکترونیکی- سیبرنتیکی راکه می‌تواند شبکهٔ کامپیوتری دشمن را نابود ساخته و منابع سوخت و آب یک ملت را منهدم کند، توسعه داده است، اما در این باره که چه زمانی و چگونه باید آن‌ها را مورد استفاده قرار دهد،اختلاف نظر وجود دارد.

این سؤالات باید به بیرون از ایالات متحده نیز تعمیم داده شود تا از آن نوع سردرگمی که در مورد بوسنی پدید آمد، اجتناب شود. در آنجانظامیان می‌خواستند بعضی حملات اطلاعاتی را علیه صرب‌های بوسنی به راه بیاندازند، ولی مقامات دادگستری مسأله‌ای جدی و واقعی را طرح کردند که آیا چنین حملاتی قانونی است؟ همکاری با متحدان ایالات متحده برای مشارکت در اطلاعات موجود درباره تهدیدات و نتایج احتمالی آن‌ها نیز لازم است. در طی جنگ سرد، امریکا و متحدانش یک سیستم مؤثر هشدار دهنده برای ردیابی و شناسایی اقدام به استفاده از موشک‌های هسته‌ای را توسعه داده بودند، موشک‌هایی که می‌توانست ظرف چند دقیقه به اهداف خود برسد. به همین منوال یک تهاجم تکنیکی یا یک ویروس پست الکترونیکی که در اروپا توسعه می‌یابد می‌تواند در چند دقیقه به ایالات متحده ضربه بزند. ولی تاکنون هیچ هشدار دهندهٔ مؤثری در مقابل حملات سیبرنتیکی وجود ندارد.

شکاف دیگری که در دفاع اطلاعاتی ایالات متحده وجود دارد، در مورد کشورهایی با برنامه‌های تجاوز جنگی- اطلاعاتی است که از مؤسسات خصوصی به عنوان پوششی برای کار

گذاردن کدهای خراب کننده، استفاده می‌نمایند که البته در ظاهر نرم‌افزارهای کامپیوتری بی‌خطری به نظر می‌رسند. برای مثال هند یا اسرائیل ممکن است یک نرم افزار به یک مؤسسهٔ دولتی امریکا بفروشند، هیچ راهی برای مقایسهٔ یک قطعه از این نرم‌افزار با محصولات تجاری قابل دسترسی دیگر برای چک کردن هرگونه تفاوتی در منبع اصلی کد وجود ندارد. ابزارهای تکنیکی در حال توسعه برای معاینهٔ کدهای نرم‌افزارها باید برای بخش‌های خصوصی و دولتی دارای یک اولویت باشد. رئیس جمهور می‌تواند این وظیفه را برعهده "بنیاد دانش ملی" بگذارد. در عین حال، شرکت‌های خارجی نیازمند ادارک آن هستند که اگر یک کد خراب کننده در تولیدات آنها یافت شود، هزینهٔ گزاف اقتصادی مانند یک تحریم وارداتی خواهد داشت، چنین تهدیدی به سرعت شرکت‌های خارجی را قانع می‌کند که چون بر پاکردن جنگ کامپیوتری بیشترین منافع اقتصادی را برای آنها در برندارد، با دولت خود همکاری کنند.

مواجههٔ دلیرانه با جهان جدید

حتی اگر واشنگتن قدم‌هایی را برای به وجود آوردن، هدایت و اداره کردن یک راهبرد منسجم برای مبارزه با تهدید سیبرنتیکی علیه امنیت ملی بردارد، دفاع مؤثر تنها با همکاری بخش خصوصی امکان‌پذیر خواهد بود. یک مشارکت و همکاری جدید باید میان سیاست‌گذاران و جامعهٔ فن‌آوری عالی پدید آید که به طور کلی اندیشه و تفکر بهتری دربارهٔ تهدیدات شبکهٔ اطلاعاتی به وجود آید، آنچه موجب آسیب‌پذیری شبکهٔ دولتی ایالات متحده شده، یک مسأله مشترک است و باید یک راه حل مشترک داشته باشد.

دستگاه اداری و مدیریتی بوش فرصتی برای تعریف دوبارهٔ محیط امنیتی ملی دارد. تهدید حملات الکترونیکی- سیبرنتیکی نیازمند رهبری و اندیشهٔ خلاقی است که راه حل‌های جدیدی تولید کند. اگر دستگاه اداری و مدیریتی، در موضع منسوخ پارادایم جنگ سرد متوقف بماند، موقعیت ایالات متحده به عنوان یک ابرقدرت نظامی به وسیلهٔ بازیگران جدید جهان سیبرنتیکی به مخاطره خواهد افتاد. امریکا باید امتیاز نامتقارن درگیری در جنگ مجازی را خنثی کند.