بسم الله الرحمن الرحیم

جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی

ادوارد هالپین و دیگران

ترجمه: روح اله طالبی آرانی

دفتر مطالعات سیاسی

مرکز پژوهش های مجلس شورای اسلامی

جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی/ [ویراستار] ادوارد هـالپین؛ ترجمه روح‌اله طالبی آرانی. -- تهران: مجلـس شـورای اسـلامی، مرکـز پـژوهش‌هـا، ۱۳۸۹.
۴۲۳ ص.: جدول.- (مرکز پژوهش‌های مجلس شورای اسلامی؛ ۱۳۸۹/۸۴)
ISBN: 978-964-8427-78-3: ۸۷۰۰۰ ریال
فهرست‌نویسی براساس اطلاعات فیپا.
۱. جنگ اطلاعاتی. ۲. فضای مجازی ـ اقدامات تأمینی. ۳. شبکه‌های کامپیوتری ـ اقدامات تأمینی. الـف. هـالپین، ادوارد، ویراسـتار. ب. طـالبی آرانـی، روح‌الـه، متـرجم. ج. مجلس شورای اسلامی. مرکز پژوهش‌ها. دفتر مطالعات سیاسی. د. عنوان.
۹ج/ ۱۶۳ U
۱۳۸۹

این کتاب ترجمه‌ای از اثر زیر است:

Edward Halpin & Others, *Cyberwar, Netwar and the Revolution in Military Affairs*, New York, Palgrave Macmillan, September 2006.

عنوان: *جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی*
مؤلفان: ادوارد هالپین و دیگران
ترجمه: روح‌اله طالبی آرانی
ناشر: مرکز پژوهش‌های مجلس شورای اسلامی
نوبت چاپ: اول، تابستان ۱۳۸۹
تیراژ: ۱۰۰۰ نسخه
قیمت: ۸۷۰۰۰ ریال

فهرست مطالب

سخن ناشر

هرچند انقلاب در فناوری ارتباطات و اطلاعات فرصت‌های بدیعی را در اختیار افراد و دولت‌ها می‌نهد تا بتوانند امورشان را به‌نحو بهتر تدبیر کنند اما از طرفی تهدیدآمیز نیز بوده و آسیب‌پذیری‌ها را افزون‌تر ساخته است. در این میان آنچه اهمیت دارد، شناخت جامع این روند و آگاهی از فرصت‌ها و چالش‌های ناشی از آن برای کمک به مسیر توسعه و شکوفایی ایران اسلامی است. یکی از آثار این روند دگرگون‌سازی ماهیت جنگ، مدیریت آن و نحوهٔ مقابله با تهدیدات است. در این زمینه جنگ سایبر که حلقه واسط جنگ‌های نرم و سخت است نمود خاصی می‌یابد؛ چرا که با مطالعه این موضوع ما می‌توانیم جایگاه کشورمان را در این حوزه، بهتر بشناسیم و افق‌های آینده را نیز ترسیم کنیم.

مرکز پژوهش‌های مجلس اسلامی با توجه به این ضرورت، ترجمه کتاب جنگ *سایبر، جنگ اینترنتی و انقلاب در امور نظامی* را در دستور کار خود قرار داد تا گامی در این مسیر بردارد. امید است ترجمه این کتاب و مطالعه موضوعات آن، سرآغاز فصل جدیدی برای مطالعات امنیتی در حوزه فناوری اطلاعات و ارتباطات باشد و مطالب و یافته‌های آن مورد توجه قرار گیرد.

دکتر بهزاد پورسید

معاون پژوهشی مرکز

سخن مترجم

زندگی بشر همواره متأثر از فناوری است. اما مهم آن است که با گذشت زمان و پیشرفت فناوری، این تأثیرپذیری تشدید شده است. بسیاری انقلاب صنعتی را در قرن هجدهم نقطه عطفی در این راستا می‌دانند. انقلاب صنعتی باعث شد فناوری‌های پیچیده‌تری ظهور کنند و بیش از پیش بر تحولات جوامع انسانی سایه افکنند. این فناوری‌ها افزایش تبادلات (عمدتاً در سطح فیزیکی) و پیچیدگی نسبی ارتباطات انسانی را پدید آوردند.

فناوری‌های پیچیده دوران مدرن که تمامی حوزه‌های حیات انسانی را درنوردید، به حوزه جنگ و منازعات نیز رسوخ کرد و بر پویش‌های امنیتی جوامع تأثیر نهاد. بااین‌حال، نقش‌آفرینی فناوری در حوزه جنگ‌ها و منازعات، در ابتدا به‌صورت سخت‌افزارهای نظامی بود که با تولید و به‌کارگیری تسلیحات هسته‌ای در دوران جنگ سرد به اوج خود رسید. این وضعیت در دوران جنگ سرد، بازدارندگی را به گفتمان غالب پویش‌های امنیتی در سطح بین‌المللی مبدل ساخت و درعین‌حال، باعث شد دغدغه جوامع داخلی عمدتاً تأمین امنیت جامعه در برابر تهاجم بیگانگان، آن هم در بعد سخت‌افزاری باشد.

اما تحولات نوظهور از قبیل پایان جنگ سرد، ظهور تروریسم فراملی و جهانی شدن در دو دهه اخیر ماهیت منازعات و امنیت را دگرگون ساختند. به موازات این تحولات، شیوه نقش‌آفرینی فناوری در حوزه جنگ و منازعات نیز تحول یافت، به‌گونه‌ای که بیشتر به حوزه‌های نرم‌افزاری امور نظامی معطوف شد. بدین‌سان، اصطلاحاتی از قبیل جنگ بینادولتی، جنگ داخلی، امنیت ملی و تسلیحات هسته‌ای در گفتمان نظامی کم‌رنگ شدند و به‌جای آن، اصطلاحات دیگری مثل جنگ شبکه‌ای، جنگ سایبر، امنیت انسانی، انقلاب در امور نظامی و سلاح‌های لیزری مطرح شدند.

اکنون با قطعیت می‌توان گفت «ماشین» به‌عنوان زیربنای تولید تسلیحات برای تأمین امنیت، جای خود را به فناوری‌های اطلاعات و ارتباطات داده است. در نتیجه این‌گونه فناوری‌ها، در محور استراتژی‌پردازی‌های نظامی و جنگی قرار گرفته‌اند. این وضعیت، آسیب‌پذیری‌های جوامع را به‌شدت افزایش داده و تهدیدهای امنیتی را بیش از پیش پیچیده‌تر ساخته است. در این راستا نویسندگان کتاب حاضر می‌کوشند الزامات محوریت فناوری‌های اطلاعات و ارتباطات در امور نظامی را بررسی و تبیین کنند چگونه می‌توان زیرساخت‌های اطلاعات و ارتباطات در جوامع مدرن را از گزند تهدیدهای نوظهور که ماهیت سایبری دارند و پیامدهای بسیار نامطلوبی بر جوامع انسانی می‌گذارند حفاظت کرد.

این کتاب طیف وسیعی از حوزه‌های موضوعی مرتبط با تأثیرگذاری فناوری‌های اطلاعات و ارتباطات بر امور نظامی را، بررسی می‌نماید سپس، روندهای جدید در این زمینه را ارزیابی می‌کند و رویکردهایی که برخی کشورها در پیش گرفته‌اند را می‌کاود. ازاین‌رو می‌تواند فهم نسبتاً جامعی را در مورد تحولات پیش رو در امور نظامی و تأثیرپذیری زندگی بشری از آنها نمایان کند.

مطالعه این کتاب به تمامی دانشجویان رشته‌های مرتبط با امور نظامی و مطالعات امنیتی و نیز دست‌اندرکاران و سیاستگذاران نظامی و امنیتی توصیه می‌شود. ترجمه این کتاب که حاوی طیف وسیعی از موضوعات و مباحث چندرشته‌ای و بینارشته‌ای است، کاری بس دشوار بود. ازاین‌رو مترجم سعی داشته که با مطالعه منابعی دیگر در این زمینه‌ها و بهره‌گیری از نظرهای کارشناسان، ترجمه‌ای را ارائه دهد که نه تنها به متن اصلی امانت‌دار باشد، بلکه خواننده نیز آن را روان و قابل فهم بیابد.

لازم است از تمامی کسانی که در این ترجمه مرا یاری کرده‌اند سپاسگزاری کنم. از آقای دکتر بهزاد پورسید معاون محترم پژوهشی مرکز پژوهش‌های مجلس شورای اسلامی که پیشنهاد اینجانب برای ترجمه کتاب را پذیرفتند تشکر می‌کنم. از آقای دکتر ناصر جمال‌زاده (مدیر دفتر مطالعات سیاسی)، شادروان آقای محمدحسین دیده‌گاه (معاون وقت دفتر مطالعات سیاسی) و آقای محمد جمشیدی (مدیر گروه سیاست خارجی) که سهم چشمگیری در اتمام ترجمه این کتاب داشته‌اند و همچنین از آقای عبدالرضا فاضلی (مدیر

دفتر فصلنامه مجلس و پژوهش) که به چاپ این اثر شتاب بخشیدند سپاسگزارم. از آقای دکتر علی مرشدی‌زاد که نظارت علمی ترجمه را به عهده گرفتند قدردانی می‌نمایم. از آقایان ابراهیم یوسف‌نژاد، دکتر ابوذر گوهری مقدم و دکتر مرتضی نورمحمدی که راهنمایی‌های خود را در طول فرایند ترجمه از من دریغ نکردند، تشکر می‌کنم.

از همسرم خانم اسماء محمدی، که در دشوارترین روزهای زندگی همواره مایه امیدواری‌ام بوده و شرایطی را فراهم ساخته‌اند تا بتوانم در عرصه تحصیل علم موفق باشم سپاسگزارم. ترجمه این کتاب را با مهر و سپاس به همسرم تقدیم می‌کنم. در پایان ناگفته نماند هرگونه سستی و کاستی در ترجمه، متعلق به مترجم است.

پیشگفتار

گری جامپمن*، دیگو لاتلا
و پروفسور کارلو شرف*****

موضوع این کتاب با کار مدرسه بین‌المللی خلع سلاح و تحقیقات در مورد منازعات[1] ارتباط دارد. هیچ تعریف بی‌همتا و منحصربه‌فردی در مورد اموری از قبیل جنگ اطلاعاتی[2] وجود ندارد. برای مثال، براساس نظر وزارت دفاع آمریکا، جنگ اطلاعات را می‌توان این‌گونه تعریف کرد: «جنگ اطلاعاتی مجموعه اقداماتی است که برای دستیابی به برتری اطلاعاتی انجام می‌گیرد؛ در این میان، براساسِ اطلاعات، فرایندهای اطلاعات‌محورانه، سیستم‌هایِ اطلاعاتی و شبکه‌هایِ رایانه‌ایِ دشمنان اقدام شده و درعین‌حال، از اطلاعات خودی حفاظت می‌شود و به‌عنوان اهرم فشار بر دشمنان مورد بهره‌برداری قرار می‌گیرد». وزارت دفاع بریتانیا به شیوه‌ای صریح‌تر، جنگ اطلاعاتی را «حمله حساب شده و نظام‌مند به فعالیت‌های اطلاعاتی حساس» تعریف می‌کند، که «با هدف بهره‌برداری، جرح و تغییر، مخدوش‌سازی و مختل‌سازی خدمات» انجام می‌گیرد. هرچند تعاریف بی‌همتا و منحصربه‌فردی در مورد جنگ اطلاعاتی/ جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی وجود ندارد، اما بحث‌هایی در مورد «ماهیت این پدیده‌ها، تهدیدهایی که به بار می‌آورند و تمهیدات احتمالی‌ای که دولت‌ها ـ ملت‌ها و سازمان‌های بین‌المللی برای مقابله با آنها به‌کار می‌گیرند»، نه تنها در محافل سیاسی و نظامی بلکه

---

* Gary Champman

** Diego Latella

*** Carelo Schearf

1. Internatinal School On Disarmaent And Research on Conflict (ISODARCO)
2. Information War (IW)

در مجامع علمی ـ دانشگاهی نیز در گرفته است. موضوعات مهم در این قبیل بحث‌ها عبارت‌اند از: رابطه میان رایانه‌ها و دفاع منطقه‌ای؛ تهدید تروریسم سایبر و جنگ سایبر؛ شکل‌های جدید سازمان‌دهی گروهی مثل شبکه‌ها و چگونگی پشتیبانی فناوری از آنها، تأثیر تحولات نوظهور درزمینه فناوری اطلاعات بر دکترین نظامی و سازمان‌دهی نیروهای نظامی.

بی‌شک، بعضی از موضوعات بالا با تهدیدهای واقعی پیوند دارد، اما این جنبه از چنین تهدیدهایی چندان به‌طور کامل ارزیابی و درک نشده است. بنابراین، وقتی سناریوهای جدیدی تبیین می‌شود، شمار فزاینده‌ای از اسطوره‌ها در ارتباط با جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی نیز سر برمی‌آورند. این سناریوها تهدید واقعی احتمالی علیه سیستم نظارت جهان‌گستر را که گسترده هم هست، «اسطوره‌زده» می‌سازند. عجیب آنکه، خود فناوری اطلاعات نیز فضایی مجازی ارائه می‌دهد و از این طریق از رشد فزاینده چنین اسطوره‌هایی حمایت می‌کند؛ بخش اعظم بحث‌های نوظهور درباره موضوعات بالا در این زمینه است.

همه دیدگاه‌هایی که در این کتاب بیان می‌شود، ماهیتی کاملاً شخصی دارد و لزوماً بازگوکنندهٔ دیدگاه رسمی هیچ‌یک از گردانندگان مدرسه بین‌المللی خلع سلاح و تحقیقات در مورد منازعات و سازمان‌هایی که چه‌بسا نویسندگان با آنها رابطه دارند نمی‌باشد.

بخش اول

جنگ سایبر، جنگ اینترنتی و انقلاب در امور نظامی: تعریف موضوعات

فصل اول تعریف موضوعات

فیلیپا تروارو*، استیو رایت**،**
دیوید وب*** و ادوارد هالپین******

هدف این کتاب، بررسی مهم‌ترین تحولات نوظهور در عرصه فناوری اطلاعات و تأثیر آنها بر مدیریت منازعه، آغاز جنگ‌ها و پیدایش کژکارکردی‌ها[1] در درون جوامع مدرنی است که به روندهای مستمر اطلاعات، وابسته‌اند. کتاب حاضر چگونگی برخورد با این چالش را بررسی می‌کند و الزامات و مخاطرات بلندمدت این رویکردهای جدید برای مدیریت و کنترل منازعه را ارزیابی می‌کند. ازاین‌رو، محتوای کتاب از چهار بخش اساسی تشکیل شده است. بخش اول در پی تعریف موضوعات است. بخش دوم الزامات این مسئله را می‌کاود و بخش سوم برخی از دیدگاه‌های کشورهای مختلف (غیرغربی) را مطرح می‌سازد. در نهایت، بخش چهارم این پرسش را مطرح می‌سازد که اگر بناست ما از غوطه‌ور شدن در پارادایم‌های رقیب و متناقض بپرهیزیم، فعلاً چه کار می‌کنیم و اساساً چه کار باید بکنیم. نتیجه‌گیری کتاب به نوآوری‌های قریب‌الوقوع پیش‌رو و الزامات و تبعات اجتماعی و سیاسی آنها نگاهی اجمالی می‌اندازد.

جنگ سایبر،[2] جنگ اطلاعاتی، جنگ اینترنتی[3] و انقلاب در امور نظامی[4] واژگان و

---

* Philippa Trevorrow

** Steve Wright

*** David Webb

**** Edward Halpin

1. Dysfunction
2. Cyberwar
3. Netwar
4. Revolution in Militorry Affairs (RMA)

اصطلاحاتی‌اند که صاحب‌نظران نظامی بیش از یک دهه به‌نحو گسترده‌ای به‌کار برده‌اند. در اوایل دهه ۱۹۹۰، یعنی در سال‌های آغازین پس از جنگ سرد، پژوهشگرانی از قبیل رانفلت[1] و آرکویلا[2] که برای مؤسسه رند[3] کار می‌کردند، گزارشی در مورد آنچه که «مدل نبرد مبتنی‌بر فناوری برتر»[4] خوانده‌اند، ارائه دادند.(۱) هرچند بعضی نویسندگان ادعا کرده‌اند که این بحث‌های نظری، نارسا و ناقص‌اند،(۲) اما نظریه‌ای که اقامه کردند، مدت‌ها پیش از این، یعنی قبل از سال ۱۹۹۵، در درون تشکیلات ارتش ایالات متحده اعتبار یافته بود.(۳) بخش اعظم بحث‌های اولیه در این حوزه یا به بررسی تهدیدهای ناشی از فعالیت‌های هکرهای آزاد[5] علیه جامعه اختصاص می‌یافت، یا در سطحی وسیع‌تر، احتمالات نظریه‌پردازانه را می‌کاوید. همین‌طور، مناظره بر سر انقلاب در امور نظامی اساساً نوعی گمانه‌زنی در مورد احتمالات آینده‌گرایانه‌ای[6] به‌شمار می‌آمد که هنوز حتی ردیف بودجه عمومی هم بدان اختصاص نیافته بود. اما هم‌اکنون همه اینها تغییر کرده‌اند.

حملات یازده سپتامبر ۲۰۰۱، رویدادهای مهمی معرفی شده‌اند که بر تغییر دیدگاه‌های تک‌تک دولت‌ها در مورد این موضوعات تأثیر گذاشته‌اند، اما چنین نظری تا حد زیادی اغراق‌گویی است. عوامل مهم دیگری نیز وجود دارد که در تغییر پارادایم‌های نظامی مربوط به دوران جنگ سرد نقش داشته‌اند. در حال حاضر، تسلیحات مدرن سیستم‌هایی محسوب می‌شوند که کلاهک‌ها و سازوکارهای پرتاب موشک فقط بخشی از آنهاست ـ نیروهای نظامی به کمک سیستم عصبی سیبرنتیک هوشمند و پیشرفته مستقر می‌شوند. داده‌های هدف‌گیری هم‌زمان با شبکه‌های پیچیده ارتباطی و سیستم‌های پیشرفته فرماندهی و کنترل مورد استفاده قرار می‌گیرند و جنگجویان میدان نبرد نیز اذعان دارند که حمله مستقیم به این سیستم‌های اطلاعاتی، اثربخش‌تر شده است؛ انجام حمله‌ای اثربخش و کارآمد علیه یک زیرساخت ارتباطاتی در گرو تدوین استراتژی‌های گوناگون و به‌کارگیری تسلیحات مختلف می‌باشد؛ برای مثال، در این زمینه می‌توان به تسلیحاتی که

---

1. Ronfelt
2. Arquilla
3. Rand Corporation
4. High-tech Model of Warfare
5. Free-lance Hacker
6. Futuristic

به‌جای مواد منفجره و فلزات پاره‌پاره، الکترون شلیک می‌کند اشاره کرد. وابستگی فزاینده جوامع مدرن و بالطبع ارتش‌های آنها به زیرساخت‌های اطلاعاتی لاجرم به طرح موضوعات جدید و تحلیل‌های بدیع درزمینه بررسی تهدیدها، آسیب‌پذیری‌ها و فرصت‌های آینده انجامیده است. رئیس سابق ستاد نیروی هوایی آمریکا در قالب عباراتی کوتاه اظهار داشت: «سیطره بر پهنه اطلاعات در حال حاضر به‌اندازه تصرف سرزمین یا کنترل فضای هوایی ـ که در گذشته، اهمیت زیادی داشت ـ در منازعات اهمیت یافته است».

عامل دیگر، افزایش نفوذ ایدئولوژی نظامی جدید «تسلیحات و تاکتیک‌های غیرمرگبار»[1] در تفکرات نظامی می‌باشد، به‌طوری‌که این ایدئولوژی در سال ۱۹۹۸ به تعهد رسمی سازمان پیمان آتلانتیک شمالی (ناتو) تبدیل شد. این رویکردهای به‌اصطلاح «قتل نرم»، همواره با نیروهای مرگبار پشتیبانی و تقویت شده‌اند؛ اما این ایدئولوژی، قانع‌کننده است: چرا به‌جای آنکه شهرها را درهم بکوبیم و به ویرانه‌های وسیع نیازمند بازسازی مبدل کنیم، آنها را دست نخورده باقی نگذاریم؟ بسط و توسعه استراتژی‌ها و فناوری‌هایی که می‌توانند موضوعیت فناوری‌های دیگر را از بین ببرند، بخش ذاتی چنین تفکری را تشکیل می‌دهد. یازده سپتامبر آهنگ چنین منطقی را شتاب بخشیده است. اما بااین‌حال، مدل‌های امنیت داخلی[2] آهنگ تخصیص ردیف‌های بودجه‌ای به طرح‌های تدارکاتی خاص را برای تحقق آنچه ایالات متحده در حال حاضر «سیطره فراگیر و تمام‌عیار»[3] خوانده است افزایش داده‌اند.

این تغییر پارادایم سطوح جدیدی را برای تفکرات و بودجه‌های نظامی ایالات متحده درزمینه «فضای نبرد اطلاعاتی»[4] به‌وجود آورده است. جنگ اطلاعاتی، دیگر ماجراجویی آماتوری در عرصه سرقت‌های کامپیوتری محسوب نمی‌شود، بلکه یکی از اصلی‌ترین فعالیت‌های نظامی بسیار مشروع مقتدرترین ارتش‌های جهان است که در کنار تجهیزات لجستیکی و تسلیحات هدایت‌شونده جدید به‌کار می‌گیرد. هرچند تمایزگذاری میان «اندیشه‌های حاصل از داستان علم» و بازی‌های سرگرمی و تفریحی جنگی در جهان امروز

---

1. Nonlethal Weapony and Tactics
2. Homeland Security Models
3. Full Spectrum Dominance
4. Information Battle Space

دشوار است، اما تفاوت‌های چشمگیری نیز میان این دو مقوله وجود دارد.

بررسی مارتین بایر[1] درزمینه «خشونت مجازی و جنگ واقعی» نشان می‌دهد بازی‌های جنگی رایانه‌ای در عصر حاضر به‌رغم تأثیرات سمعی ـ بصری پایداری که برجای می‌گذارد نه واقع‌گرایانه‌اند و نه معتبر و موثق. این مدعا درست در تضاد با این گرایش رسانه‌هاست که می‌خواهند داستان‌هایی در مورد کاربرد مؤثر بازی‌های جنگی در شبیه‌سازی‌ها و آمادگی‌ها برای نبرد واقعی پخش کنند. سربازان مجازی می‌توانند مقادیر زیادی تجهیزات انفرادی با خود حمل کنند، انجام تدارکات و تجدید قوا نیز تنها با فشار یک دکمه در فرسنگ‌ها دورتر از صحنه نبرد انجام می‌گیرد و تسلیحات دقیق این سربازان نیز که شبیه‌سازی شده است همیشه به هدف‌های مورد نظر آنها اصابت می‌کند. در واقعیت امر، سربازان حقیقت مسلم جنگ و نبرد را پیش روی خود ندارند که هدف‌گیری کنند، بلکه کارهای تکراری، پیش‌پاافتاده و معمولی را انجام می‌دهند. این بازی‌های سرگرم‌کننده می‌تواند به سوءبرداشت‌ها و کژفهمی‌هایی درزمینه فعالیت نظامی منجر شود؛ چرا که بازی‌های مجازی رایانه‌ای با صحنه‌های نبرد قیاس می‌شوند. درصورت بروز جنگ، یگان‌های نظامی جدید را نمی‌توان به‌آسانی باز سازمان‌دهی کرد و سربازان نیز ازلحاظ قانونی و حقوقی متعهد و ملزم‌اند که از غیرنظامیان مراقبت کنند و به اسرای جنگی و آوارگان بی‌احترامی نکنند. در آینده، اهداف اصلی نظامی، افراد انسانی نخواهند بود بلکه برای هماهنگ‌سازی و کنترل رفتار افراد، از سیستم‌های عصبی الکترونیک ـ از قبیل شبکه‌های رایانه‌ای و اینترنت ـ استفاده خواهد شد. مسلماً، جامعه بین‌المللی باید برای مقابله با تهدیدهای تخصصی‌تری که امنیت زیرساخت اینترنت، شبکه‌های مجازی و سرورها[2] را به خطر می‌اندازند آماده شود. حال سؤال این است که بازیگران اصلی در عرصه منازعه الکترونیک چه کسانی‌اند؟

گلان پیرو سیرلی[3] با مقدمه‌ای هوشمندانه درباره جنگ اطلاعاتی به این پرسش پاسخ می‌دهد. به دنبال ارتقای جایگاه و اهمیت «سیستم‌های اطلاعاتی و شبکه‌های مخابراتی در سیاست‌های دفاعی بسیاری از کشورها»، موضوع وابستگی به زیرساخت‌های

---

1. Martin Bayer
2. Servers
3. Glan Piero Siroli

اطلاعاتی بیش‌ازپیش مورد توجه قرار گرفته است. سیرلی بهره‌برداری ارتش‌ها از «فناوری اطلاعات» پیشرفته را عاملی مهم درزمینه روی آوردن کشورها به کسب فنون جنگی جدید می‌داند. از دیدگاه سیرلی، «جنگ اطلاعاتی، آن دسته از فعالیت‌هایی است که با هدف ایجاد اختلال، تخریب و جلوگیری از دستیابی دشمن به اطلاعات در عملیات‌های تدافعی و تهاجمی انجام می‌گیرد».

بخش دوم کتاب که حجم آن نیز قابل توجه است، الزام مسئله وابستگی فراگیر به فناوری اطلاعات و نیز آسیب‌پذیری‌های متعدد برخاسته از آن را بررسی می‌کند و در این خصوص بسیاری از موضوعاتی را که بار ارزشی دارند پیش می‌کشد.

ژاری رانتاپلکنن[1] در مورد بازنمایی[2] «جنگ مجازی فضیلت‌مندانه»[3] به ما هشدار می‌دهد. وی استدلال می‌کند که جنگ علیه تروریسم، مسئله‌ای سرزمینی نیست؛ بلکه برعکس، ابتکاری رسانه‌ای است که در آن فناوری جهان مجازی جنبه اخلاقی یا فضیلت‌مندانه به خود می‌گیرد. اصلاً تصادفی نیست که پنتاگون در سال ۲۰۰۱ گروه رندن[4] را به‌کار می‌گیرد تا تصویری مثبت در مورد اَشکال جدید جنگ ابداع کند. جنگ فضیلت‌مندانه با جنگ مجازی ـ که در شبکه‌های رایانه‌ای[5] بازنمایی می‌گردد ـ هم‌سنگ پنداشته می‌شود. «بمب‌های اطلاعاتی» تنها ظرفیت‌ها را نابود نمی‌سازند؛ بلکه علاوه‌بر این می‌توانند باعث فراموش شدن حافظه‌های اجتماعی شوند، روابط اجتماعی را یکسره نابود کنند و اجتماعات بین‌المللی را کاملاً از میان بردارند. در عصر «انقلاب در امور نظامی»، این شبکه‌های اطلاعاتی پیشرفته‌اند که می‌توانند اطلاعات درست یا برعکس را فراروی شمار زیادی از افراد قرار دهند و اشاعه سریع اسطوره‌ها و شایعه‌هایی را که نمی‌توان اثبات کرد تسهیل نمایند. پوشش رسانه‌ای دقیق و لحظه‌به‌لحظهٔ جنگ عراق، مرزهای میان واقعیت و خیال را مبهم و مخدوش کرد؛ زیرا برای تقویت یک مجموعه خاصی از برداشت‌ها و ادراک‌ها، «تحلیل‌ها و اطلاعات مفیدی که در واقع‌نمایی‌ها می‌توان به‌کار برد در اختیار

---

1. Jari Pantapelkonen
2. Representation
3. Virtuous Virtual War
4. Rendon Group

۵. همان سرگرمی‌های صنعتی ـ نظامی رسانه‌ای که واقعیت را آشفته و کژدسیه می‌سازند ـ م.

مخاطب قرار نمی‌گرفت، بلکه برنامه‌ها، گزارش‌ها و تصاویر تکراری پخش می‌شد؛ درحقیقت، این عنصر «تکرار» بود که نقش تعیین‌کننده‌ای را در پوشش رسانه‌ای ایفا می‌کرد.

پیتر جی. نیومن[1] در فصل پنجم با عنوان «خطرات فناوری رایانه‌ای» توجه ما را به این حقیقت جلب می‌کند که تقریباً تمام افعال و کنش‌های ما به فناوری رایانه‌ای وابسته است. چگونه ما این مسئله را حل کنیم؟ ما به سیستم‌های قابل اعتماد، ایمن و بسیار سهل‌الوصل نیاز داریم. آنچه ما فراروی خود داریم درحقیقت شبکه‌هایی است که بسیار آسیب‌پذیرند و پیوندهای بسیار سست و شکننده‌ای باهم دارند. وی استدلال می‌کند که اینترنت منبع کسب سود سرشار است؛ و هر روز فرصت‌های بیشتری را برای توسعه جهان سوم، تجارت جهانی، آموزش و جریان آزادانه اطلاعات پدید می‌آورد؛ ولی می‌تواند قدرت بسیار کمی را برای مقاومت در برابر حملات هماهنگ به آنها ارزانی دارد، چرا که تلاش چندانی صرف استحکام بخشیدن به ساختار آن نشده است. تهدیدهای دیگری که فراروی یکپارچگی و در دسترس بودن شبکه‌ها وجود دارد، عواملی از قبیل تمایل بسیاری از دولت‌ها برای کنترل و نظارت بر وب، اقدامات سوء شرکت‌هایی که می‌خواهند از وب سود ببرند و نبود مدیریت برای رفع اشکالات فنی و از میان برداشتن منابع، خیل عظیم شرکت‌های تولیدکننده فیلم‌ها و تصاویر مستهجن، کلاهبرداران، سارقان هویت[2] و جاسوسان می‌باشند که بیش‌ازپیش فضای سایبر را اشغال کرده‌اند. از دیدگاه نیومن، چالش فراروی ما چگونگی بهره‌برداری از فرصت‌های ناشی از اینترنت و درعین‌حال جلوگیری از خطرات، تهدیدها و نارسایی‌های آن است.

نیومن نمونه‌هایی از نارسایی‌های رایانه‌ای را در حوزه‌های دفاعی، هوا و فضا، کشتیرانی و دریانوردی، محیط زیست، مخابرات، حمل‌ونقل، سیستم‌های پزشکی، انتخابات امنیت و حریم خصوصی برای ما برمی‌شمارد. اگر بپذیریم که این خطرات جزء ذاتی سیستم‌های جدیدند، پس ما قادر خواهیم بود سیستم‌های مستحکمی را ایجاد کنیم، وابستگی‌هایمان را از میان برداریم و از نارسایی سیستم‌ها جلوگیری به‌عمل آوریم. این وضعیت، درست زمانی حساس و تعیین‌کننده می‌شود که سیستم‌های الگوریتمی و تشخیص

1. Peter G. Neumann
2. Identity Thieves

هویت، امکان دسترسی به بسیاری از کالاها و خدماتی را که ما مسلم فرض می‌کنیم در اختیار ما قرار دهند. تا به حال، تحقیقات درباره سیستم‌های مقاوم مغفول مانده و به‌جای آن، تحولات بازارمحور مورد توجه قرار گرفته است. این فقدان بینش درست زمانی تعیین‌کننده و زیان‌بار می‌شود که اتکای فزاینده به سیستم‌های آسیب‌پذیر فناوری‌های ارتباطاتی و اطلاعاتی، زیربنای مواضع دفاعی ما را تشکیل می‌دهد. اما، به‌رغم نارسایی‌ها و با وجود موانع مالی و تکنولوژیکی، بسیاری از برنامه‌های دفاعی ایالات متحده با سرعت هرچه تمام‌تر به‌کار خود ادامه می‌دهند.

دیوید وب نگاهی اجمالی به موضوع «دفاع موشکی» می‌اندازد و این سؤال را مطرح می‌کند که آیا این سیستم فقط محصول فرعی «اولین گام‌ها به‌سوی جنگ در فضا» به‌شمار می‌آید؟ وب علاوه‌بر این، موضوع اتکای فزاینده ارتش به سیستم‌های فضایی را نیز مدنظر قرار می‌دهد و آسیب‌پذیری این سیستم‌ها را در برابر حملات بررسی می‌کند. در اثر این آسیب‌پذیری است که فرماندهی فضایی ایالات متحده[1] سخت به دنبال سیطره بر فضاست و البته می‌خواهد ایالات متحده را در چنان موضعی قرار دهد که هرگاه ضروری بداند سایر کشورها را از دسترسی به فضا محروم سازد. شتاب گرفتن سرمایه‌گذاری‌های ایالات متحده در حوزه فناوری نظامی هوا ـ فضا به‌طور عام و سیستم‌های ضدموشکی به‌طور خاص، نمایانگر این جنبه از «انقلاب در امور نظامی» است. بااین‌حال، همان‌طور که وب بیان کرد، افزایش حجم سرمایه‌گذاری بیش از گسترهٔ ظرفیت‌های در دسترس است و چه‌بسا نتواند اهداف مورد نظر برای عملی ساختن چنین طرح‌هایی را تحقق بخشد. وانگهی، همه سیستم‌های ماهواره‌ای مستقر در فضا، علاوه‌بر پرهزینه بودن، در برابر حملات احتمالی سایر سیستم‌های ماهواره‌ای نیز همچنان آسیب‌پذیرند. بااین‌حال، این قبیل مسائل مانع از آن نشده است که ایالات متحده آمریکا همکاری‌های خود را با بریتانیا، دانمارک، گرینلند، آلاسکا، لهستان، جمهوری چک، مجارستان، رومانی، بلغارستان، استرالیا، روسیه و ژاپن گسترش ندهد. دورنمای قراردادهای تحقیقات و توسعه، انگیزه‌های نیرومندی را ایجاد کرده و تنها کاناداست که خود را از مشارکت در این عرصه کنار کشیده است.

---

1. US Space Command

استفان فریتش[1] پیامدهای این طرح را به‌صورت مبسوط بررسی می‌کند و در این راستا، «فناوری‌های اطلاعاتی و ارتباطی را به‌عنوان منبع آشوب» معرفی می‌نماید. وی می‌کوشد مدلی جامع در مورد قدرت فناوری‌های اطلاعاتی و ارتباطی مدرن در محدودسازی اقدامات سیاسی و حاکمیت‌محورانه به بیشتر دولت‌ها ارائه دهد و برای این منظور، از سه رویکرد نظری واقع‌گرایی ـ نوواقع‌گرایی، جهان‌گرایی مبتنی‌بر وابستگی متقابل[2] و سازه‌انگاری که در رشته‌های روابط بین‌الملل و اقتصاد سیاسی بین‌الملل رواج دارند، بهره می‌گیرد. وی معتقد است بسیاری از دولت‌ها بخش قابل ملاحظه‌ای از قدرت خود را از دست داده‌اند و قسمت چشمگیری از مسئولیت‌های خود را به طیف وسیعی از بازیگران جدید از قبیل شرکت‌های چندملیتی، سازمان‌های غیردولتی و غیره واگذار کرده‌اند. از بسیاری جهات، این فناوری‌ها واقعیت اجتماعی را دگرگون ساخته‌اند، ولی درعین‌حال همچنان به بافتارهای[3] اجتماعی وسیع‌تری وابسته‌اند. فریتش فصل را با سلسله مباحثی در مورد اینکه آیا این فرایندهای فناورانه صبغه جبرگرایانه دارند یا خیر، به پایان می‌برد. این قبیل ملاحظات عرصه را برای بسیاری از نویسندگانی که به دنبال یافتن تدابیر عمل‌گرایانه برای مهار و مدیریت برخی از پیامدهای منفی‌تر وابستگی امنیت مدرن به ملاحظات هوا ـ فضا هستند، تنگ کرده است.

بروس دی لارکین[4] پیامدها و تأثیرات اتکا به سیستم فرماندهی و کنترل جهان‌گستر[5] بر ارتقای فناوری‌های پرتاب تسلیحات هسته‌ای را بررسی می‌کند. لارکین خاطرنشان می‌سازد هرچند ما معتقدیم از چنین سیستم‌های بسیار پیشرفته به‌شدت حفاظت می‌شود، ولی سایر سیستم‌های پیشرفته ارتباطاتی و نظارتی ایالات متحده در هنگام آزمایش در میدان جنگ شکست خورده‌اند و دستاورد قابل توجهی نداشته‌اند. وی در این زمینه شواهدی را از عملکرد واحدهای آفندی نیروی هوایی آمریکا که در جنگ عراق با کردها همکاری می‌کردند ذکر می‌نماید. لارکین پیش‌شرط‌هایی را که ترتیبات امنیتی آرمانی برای ایجاد سیستم فرماندهی و کنترل جهان‌گستر نیاز دارند بررسی می‌کند و نتیجه می‌گیرد که

---

1. Stefan Fritcsh
2. Interdependent Globalism
3. Contexts
4. Bruce D. Larkin
5. Global Control and Command System (GCCS)

هزینه یکی از بزرگ‌ترین موانع فراروی تحقق واقعی پیش‌شرط‌های فناورانه خواهد بود.

جفری دارنتون،[1] موانع حقوقی را که در سطح بین‌المللی فرا راه تحقق اهداف جاه‌طلبانه سیطره بر فضاهای اطلاعاتی جهان قرار دارد بررسی می‌کند. دارنتون در می‌یابد که هرچند قوانین جنگی[2] تا حدودی جنگ اطلاعاتی را نیز پوشش می‌دهد، ولی این حوزه به نسبت توسعه نیافته است. چگونه می‌توان حقوق بین‌الملل موجود را برای وضعیت‌ها و رویه‌هایی که در هنگام تنظیم و تدوین معاهدات، پیمان‌ها و پروتکل‌ها حتی پیش‌بینی هم نمی‌شدند به‌کار برد؟ وی پیمان‌های خاصی را که در پرتو پیشرفت‌ها در نقش و کارویژه فناوری‌های اطلاعاتی و ارتباطاتی، خود را در معرض تفسیر مجدد قرار می‌دهند، برمی‌شمارد، ولی بسیاری از این معاهدات را پیمان‌هایی دست‌دوم می‌داند. برای مثال، توسعه زنجیره‌های عرضه و خطوط ارتباطی میان مسافت‌های دوردست، سیستم‌های آسیب‌پذیرتری هستند. قطع کردن این زنجیره‌های عرضه، اختلال‌های جدی و احتمالاً نابسامانی‌های داخلی جبران‌ناپذیری را ایجاد خواهد کرد. دارنتون نتیجه می‌گیرد بی‌شک باید اصلاحات و پیشرفت‌هایی برای ایجاد چارچوب بین‌المللی مناسبی که جنگ اطلاعاتی را پوشش دهد، انجام پذیرد؛ اما وی این سؤال را بیان می‌کند که «چه کسی آن را عملی خواهد ساخت؟».

بخش سوم کتاب دیدگاه‌های کشورهای مختلف را بررسی می‌کند. قسمت اعظم این کتاب به دیدگاه امپریالیستی ایالات متحده درزمینه سیطره بر «فضای نبرد اطلاعاتی» می‌پردازد، ازاین‌رو شگفت‌آور نیست که سایر اعضای شورای امنیت سازمان ملل متحد نیز این رویکرد برتری‌طلبانه را در پیش گرفته باشند و مسیرهای مشابه رویکرد ایالات متحده را در برنامه‌های خود اعمال کنند.

فانوریوس پانت‌گلیانیس[3] این وضعیت را از دیدگاه فدراسیون روسیه بررسی می‌کند. متفکران شوروی اولین کسانی بودند که لزوم پدیدهٔ نوظهور انقلاب در امور نظامی را به‌عنوان امری بدیهی پذیرفتند و به تجزیه و تحلیل آن پرداختند، ولی روسیه اکنون یک قدرت در حال زوال است. شکست روس‌ها در افغانستان باعث شد آنها در

---

1. Jeoffrey Dornton
2. Laws of War
3. Fanourios Pantelogiannis

اولویت‌های نظامی کشورشان بازنگری به‌عمل آورند. در این مورد، آنها به این نتیجه رسیدند که نارسایی فقط در قدرت آتش نبوده است، بلکه سرمایه‌گذاری در عرصه‌های فرماندهی زیرساخت‌های رایانه‌ای ارتباطات، نظارت و عملیات شناسایی و جنگ الکترونیکی اهمیت بیشتری دارد. فرماندهان نظامی شوروی سابق، که احساس می‌کردند از قافله عقب مانده‌اند، توجه خود را به فناوری‌های تسلیحاتی جدید معطوف ساختند و این پیشرفت‌ها را با سخت‌افزارهای نظامی روسی که به‌سرعت در حال منسوخ شدن بودند، مقایسه کردند.

اگر روسیه نمی‌خواهد از قافله پیشرفت جا بماند، دچار توهم نشده است که سرمایه‌گذاری مجدد در زیرساخت اطلاعاتی، ماهواره‌ها و غیره را حیاتی می‌داند. بااین‌همه، مقدار زیادی از ظرفیت فعلی روسیه، کهنه و در حال تحلیل است ـ این وضعیت بر همه حوزه‌های اطلاعات استراتژیک[1] از جمله ارتباطات هم‌زمان،[2] هشدار اولیه و غیره تأثیر می‌گذارد. بخشی از انگیزه روسیه برای سرمایه‌گذاری دوباره در زیرساخت مخابرات نظامی خود به‌دلیل سیاست این کشور در صدور فناوری هسته‌ای و موشکی بوده است؛ ولی باید توجه داشت که سیاست روسیه درزمینه اشاعه فناوری هسته‌ای و موشکی به سایر قدرت‌های رقیب آمریکا از قبیل چین، ایران، اندونزی و هند با دیدگاه‌های کاخ سفید که این سیاست را مایه بی‌ثباتی در جهان می‌داند، سازگار نبوده است.

روسیه همچنین به اهمیت فزاینده جنگ اطلاعاتی اذعان کرده است؛ روسیه نه تنها جنگ اطلاعاتی را ابزاری برای تقویت تأثیر روانی و سیاسی عملیات‌هایش می‌داند بلکه آن را روشی برای افزایش کارآمدی و دقت همه سیستم‌های تسلیحاتی موجود خود قلمداد می‌کند. البته همه فرماندهان نظامی روسیه این دیدگاه جدید را ندارند. اینکه آیا انقلاب در امور نظامی روسیه تداوم می‌یابد یا خیر؛ تا حد زیادی به تأمین بودجه لازم برای این بخش و نیز به‌میزان تداوم مقاومت نهادی در برابر اصلاحات درون سازمان‌های نظامی بستگی خواهد داشت.

کریس وو[3] سیر تحول تاریخی و اولویت‌های فعلی چین درزمینه جنگ اطلاعاتی را

---

1. Strategic Intelligance
2. Real Time
3. Chris Wu

بررسی می‌کند. وی فناوری‌ها و سیستم‌های جدیدی را کـه چینـی‌هـا بـرای انجـام جنـگ اطلاعاتی توسعه داده‌اند تشریح می‌کنـد ـ پیـشرفت‌هـای جدیـد چـین درزمینـه رادارهـا، ماهواره‌ها و سیستم‌های رایانه‌ای بوده اسـت ـ کـه بـا توسـعه تـسلیحات دقیقـی همچـون ماهواره‌های شکاری، سلاح‌های الکتریکی و موشک‌های کـروز تقویـت شـده‌انـد. کـریس‌وو همچنین دشواری‌ها و نقص‌هایی را که چین در رقابت برای عقب نماندن در عرصـه جنـگ اطلاعاتی فراروی خود می‌بیند خاطرنشان می‌سازد. نبود آموزش، تجربه، منابع و تأسیـسات حکایت از آن دارد که چین از ایالات متحـده آمریکـا عقـب مانـده اسـت. البتـه، چـین در گذشته، برای توسعه سیستم‌های خود به‌شدت بـه تجربیـات و محـصولات ایـالات متحـده متکی بوده و متذکر می‌شود ایـن اتکـا نقـش تعیـین‌کننـده‌ای در افـزایش آسـیب‌پـذیری سیستم‌های چینی که هیچ سازوکار حفـاظتی در برابـر حمـلات احتمـالی دشـمن نـدارد، داشته است. در پایان فصل، وی رئوس کلـی یکـی از سـناریوهای احتمـالی تاکتیـک‌هـای جنگ اطلاعاتی را که چین می‌تواند علیه تـایوان مـستقر سـازد تـشریح مـی‌کنـد. در ایـن سناریو، وی نابرابری شدید در توازن نیروها بین دو کشور را بررسی می‌کند و این سـؤال را مطرح می‌کند که: برای حراست از امنیت تایوان، چگونه مـی‌تـوان ایـن نـابرابری را تقلیـل داد؟ ازاین‌رو، او دو پیشنهاد ارائه می‌دهـد کـه دو کـشور ایـالات متحـده و تـایوان را قـادر می‌سازد تا در حوزه جنگ اطلاعاتی در تمامی سطوح، به‌طور همـه‌جانبـه بـاهم مـشارکت کنند؛ این پیشنهادها عبارت‌اند از: تقویت سیستم‌های تایوان و همکاری نزدیک‌تر تایوان بـا ایالات متحده (در حوزه‌هایی از قبیل سیستم‌های ضدموشکی).

بخش پایانی این کتاب راه‌حلی را برای مدیریت آسیب‌پذیری فردی و جمعی مـا در برابر تهدیدها و فرصت‌های اطلاعات مدرن که ناشی از سیستم‌های امنیتی دولتـی اسـت ارائه می‌دهد؛ درواقع این بخش با چالش عملی «چه اقدامی در دست انجـام اسـت و چـه باید کرد؟» سروکار دارد.

مایک مور[1] این گرایش غیرپاسخ‌گویانه و خودمحورانه به‌سمت سـیطره‌طلبـی در عرصـه فناوری‌های برتر را در فصلی با عنوان «پلی بسیار دوردست؟» مورد توجه قرار می‌دهـد. وی در برخی از موضوعات مرتبط با جنگ‌هایی که اهداف در آنها با دقتی هرچه تمام‌تر نـشانه‌گیـری

1. Mike Moore

می‌شود و نویسندگان این کتاب مطرح کرده‌اند بازنگری می‌کند و حرکت ایالات متحده به‌سوی تبدیل شدن به تنها قدرت امپریالیستی در فضا را بررسی می‌نماید. ریشه‌های این تفکر از مدت‌ها پیش در دهه ۱۹۵۰ مشهود بود ـ اما در آن زمان، فناوری ماهواره‌ای در کار نبود. حالا دیگر، تفوق نظامی ایالات متحده رفته‌رفته بیش‌ازپیش به‌سمت نوعی یک‌جانبه‌گرایی لجوجانه و اعمال فشار دوجانبه تغییر مسیر می‌دهد. جاذبه‌ها و فریبندگی قراردادهای تحقیقاتی و توسعه را که سایر نویسندگان کتاب، آن را در رابطه با دفاع موشکی مطرح کرده‌اند، می‌توان با پدیده تطهیر سیاستگذاری‌ها[1] که به نام جنگ علیه ترور انجام می‌گیرد مقایسه کرد. مور این پرسش را بیان می‌کند: «اگر یک دولت در سطح جهان بسیار قدرتمند شود، سایر دولت‌ها چگونه حاکمیت ملی کامل خود را حفظ نمایند؟» این پرسش اساساً موضوعی است که بسیار در این کتاب مطرح می‌شود. در زمان ترور، بحث‌های امنیتی بیش‌ازپیش به بحث‌های قطبی شدهٔ احمقانه مبدل می‌گردد ـ آیا شما با هستید یا علیه ما؟ چنین ساده‌انگاری‌هایی فضایی را ایجاد می‌کند که در آن، فناوری را می‌توان پدیده‌ای عینی و مشخص قلمداد کرد؛ پدیده‌ای که از ما در برابر تقویت آشوب بین‌المللی و احساس کاهش ضریب امنیت حفاظت می‌کند. اگر این پلی بسیار دوردست است، پس با این واقعیت که این ساده‌انگاری با توجه به پیشینه جنگ دائمی اتفاق می‌افتد؛ باید زنگ‌های خطر را برای فرارسیدن هر محدودیت سخت بر زیاده‌روی‌های جنگ و قدرت دولت (که از ما در برابر وحشیگری و بربریت محافظت می‌کند) به صدا درآورد. آنگاه چه اتفاقی خواهد افتاد؟

ماسیمو مائورو[2] که از اعضای کمیسیون اروپاست، برای تبیین و ارزیابی تهدیدهای برآمده از تروریسم سایبر، همکاری غیررسمی میان دولت‌های عضو اتحادیه اروپا و ده کشور آسیایی را مورد توجه قرار می‌دهد. در سال ۲۰۰۲، اجلاس آسیا ـ اروپا،[3] امنیت سایبر را اولویتی اساسی به‌شمار آورد.[4] به‌نظر می‌رسد که حملات سایبر از عوامل ذیل نشئت می‌گیرد:

---

1. Policy Laundering
2. Massino Mauro
3. Asia-Europe Meeting (ASEM)

۴. اجلاس آسیا ـ اروپا فرایندی بود که با هدف بررسی و مسائلی از قبیل ارایهٔ تدابیری برای حفاظت زیرساخت‌های حساس اطلاعاتی و حفظ توازن میان اقتضائات امنیت ملی و اجرای قوانین تشکیل شد؛ البته دراین‌میان، اقتضائات جامعهٔ تجار و بازرگانان که فعالیت آنها به بهره‌مندی از اطلاعات سری و محرمانه وابسته است، مورد توجه قرار گرفت ـ م.

۱. هکرهایی که به برنامه‌های رایانه‌ای آسیب وارد می‌کنند؛

۲. جنایتکاران مالی که مخفیانه در سیستم‌های اقتصادی نفوذ می‌کنند با این امید که به سودهای مالی کلانی برسند (بسیاری از آنها نیز اتفاقاً خودی می‌باشند)؛

۳. مخالفان سیاسی که به وب‌سایت یک کشور یا سازمان خاص حمله می‌کنند تا دسترسی یا بهره‌گیری از آن را مختل سازند. با وجود این، مائورو استدلال می‌کند که جامعه بین‌المللی باید برای مقابله با تهدیدهای ماهرانه‌تر علیه زیرساخت اینترنت، شبکه‌های رایانه‌ای شخصی، سرورها و ... آماده باشد. اما این سؤال همچنان باقی است که دشمن اصلی چه کسی است و چه سازوکارهایی برای رتبه‌بندی سایر اولویت‌ها در تخصیص بودجه ملی شکل گرفته است؟

گوس حسین، روندی را برای تعیین این اولویت‌ها شناسایی می‌کند که اتفاقاً در حال تقویت نیز می‌باشد؛ این رویه‌های تعیین دستور کار که قاعدتاً در خارج از اکثر دولت‌ها شکل می‌گیرد، بر این روند به‌شدت تأثیر می‌گذارد. نتیجه این تحولات، «تطهیر سیاست و سایر پویش‌های سیاستگذاری» است. منظور حسین این است که سیاستگذاران از اختیارات و صلاحیت‌هایشان برای نیل به اهداف خود استفاده می‌کنند. به‌نظر وی، آنها دو تاکتیک را به‌کار می‌گیرند که عبارت‌اند از: ۱. مدل‌سازی؛ حکومت‌ها از طریق آن، قوانین را براساس قوانینی که در حوزه‌های صلاحیت سایر نهادها قرار دارند شکل می‌دهند. ۲. تغییر جهت‌گیری در نهادها؛ بازیگران تا زمانی از قواعد سازمان‌های بین‌الدولی پیروی می‌کنند که با منافعشان سازگار است. در این صورت هنگام مواجهه با چالش‌ها یا مخالفت‌های این قواعد، سمت‌گیری خود را به سایر سازمان‌های بین‌الدولی تغییر می‌دهند.

به‌نظر حسین، پویش‌های جدید سیاستگذاری در هنگامی ظهور می‌کند که فرایندهای رایزنی ملی یا ازبین‌رفته یا به‌شدت تضعیف شده باشد، چرا که تصمیمات مهم در حوزه سیاستگذاری در خارج از نهادهای دمکراتیک سنتی روی می‌دهد. در چنین بافتارهایی، منافع و فرایندهای خارجی به سیاست‌ها شکل می‌دهد. وی بخش‌های قابل توجهی از فصل خود را به بررسی معاهده جرائم سایبر و مذاکرات گروه هشت در مورد جرائمی که با کمک فناوری‌های برتر انجام می‌گیرد اختصاص داده است. وی

هشدار می‌دهد که فعالیت‌های بین ـ دولتی باید بیشتر مورد توجه قرار گیرد؛ چرا که گروه‌های ذی‌نفوذ و تأثیرگذار، از جمله نمایندگان دولت‌ها در خارج با بهره‌مندی از اختیارات بی‌سابقه و آمادگی برای اخذ تصمیم‌هایی که به دور از فرایند پارلمانی یا دمکراتیک‌اند، سر میز مذاکرات می‌نشینند.

فصل نتیجه‌گیری برخی از موضوعات مورد توجه جامعه مدنی از جمله برنامه‌ریزی ارتش‌ها برای تهیه تسلیحات و سیستم‌هایی که در آینده نزدیک، اطلاعات را هدف قرار خواهند داد بررسی می‌کند. ظرفیت رهگیری داده‌های مخابراتی در سطح جهان، در حال حاضر دلهره‌های گسترده‌ای برای به خطر افتادن آینده دمکراسی آن‌گونه که ما می‌فهمیم پدید آورده است. برای شبکه راشلن که تحت سیطره ایالات متحده است، پست‌های شنود در سراسر جهان دارد که قادرند همه مکاتبات و تبادلات اطلاعات از طریق تلفن، پست الکترونیک و فکس را شنود کند. در حال حاضر، توانایی این شبکه در جذب همه مدخل‌های شاه‌راه‌های مخابراتی چه بخواهیم چه نخواهیم ضمانت‌های ملی در کشورهای مختلف جامعه اروپا را کان‌لم‌یکن ساخته است. پارلمان اروپا و کمیسیون اروپا اذعان کرده‌اند که چنین مهارتی پیامدهای عظیمی برای اصل انصاف در مذاکرات اقتصادی در سطح بین‌المللی دارد؛ ازاین‌گذشته، باعث شده است دست‌کاری‌هایی در گفتمان سیاسی انجام گیرد.

جنگ علیه ترور براساس اطلاعات جاسوسی[1] افرادی انجام می‌گیرد که نمی‌توان بر آنها نظارت کرد. ازاین‌رو، خط تمایز میان اطلاعات عادی[2] و اطلاعات جاسوسی مخدوش و مبهم است و ما رفته‌رفته آغاز اقدامات پلیسی غیرپاسخ‌گویانه را تجربه می‌کنیم. ما مشاهده کرده‌ایم که چگونه جنگ اطلاعاتی همچنان مبتنی‌بر کیفیت استخراج اطلاعات است. وقایعی که در ابوغریب، گوانتانامو و جاهای دیگر رخ می‌دهد، نمایانگر این گرایش تازه است که تعداد زیادی از افراد به اتهام احتمال همدستی دستگیر می‌شوند و زندانیان نیز به امید تولید منابع اطلاعاتی بیشتر شکنجه می‌شوند. برخی از سیستم‌های نظارت مخابراتی بر بازار از قبیل شرکت واتسون و هلمز[3] (یک سیستم نظارت مخابراتی)

---

1. Intelligence
2. Information
3. Watson and Holmes

فهرست افرادی را که باید بازداشت شوند، به‌صورت خودکار از زنجیره‌های تماس‌های تلفنی ارائه می‌دهند. مشاهده چگونگی توجیه بی‌پایه و اساس اتهام همدستی در جرم با ثبت مکالمات تلفنی که به‌منظور اجرای اقدامات بسیار سرکوبگرانه علیه برخی فعالیت‌ها یا جوامعِ مخالفِ وضع موجود انجام می‌گیرد، دشوار نیست.

انقلاب در امور نظامی دربرگیرنده توانمندی‌هایی است که در اثر پیشرفت‌ها در حوزه نانوتکنولوژی پدیدار شده‌اند. این کتاب در پایان به بررسی این موضوع می‌پردازد که اگر برای پرهیز از هرگونه پیش‌داوری بر سر تصمیمات در مورد هدف‌گیری‌های آینده (که با بهره‌گیری از تسلیحات پیشرفته و به روش‌های الگوریتمی و خودسامان اتخاذ می‌شوند) سازوکار نظارت و توازن آن‌چنان‌که بایدوشاید به اجرا درنیاید، چنین فناوری‌ای چگونه می‌تواند بر ما مستولی گردد.

پی‌نوشت‌ها

1. J. Arquilla and D. Ronfeldf, 'Cyberwar is Coming!' *Comparative Strategy,* 12(2) Spring 1993, 141-65.

2. Colonel R. Szafranski, USAF, *A Theory of Information Warfare:* Preparing for 2020, 15 July 2005. Available at http://www.jwar.org/iwar/resources /airchronicles /szfran.htm.

3. C.H. Gray, *War and Cpmputers*, New York: Routledge, 2005. http://www.dtic. mil/doctrine/jel/service_pubs/afd2_5.pdf (accessed15July 2005).

فصل دوم خشونت مجازی و جنگ واقعی؛ جنگ در بازی‌های رایانه‌ای: نبرد با واقعیت

مارتین بایر*

مقدمه

«گاهی اوقات، آنها یک جنگ را به نمایش خواهند گذارد ـ و هرکس به این بازی خواهد پیوست». با توجه به افزایش پوشش رسانه‌ای بازی‌های رایانه‌ای و تعداد واقعی این بازی‌ها، آوردن این نقل قول معروف کارل سندبرگ[1] در اینجا می‌تواند مناسب باشد. این فصل از کتاب بررسی خواهد کرد که چگونه جنگ در دنیای امروز به‌نوعی سرگرمی تعاملی تبدیل شده است و رایانه‌های شخصی و میزهای بازی را در خدمت خود قرار داده است؛ علاوه‌بر این افزایش همگرایی میان بازی‌های جنگی (که صبغه تجاری دارند) و شبیه‌سازی‌های نظامی مورد توجه قرار خواهد گرفت. ازاین‌رو بر تمایز میان به‌اصطلاح واقعیت‌نمایی این‌گونه بازی‌ها و واقعیت‌های جنگ تأکید خواهد شد. با توجه به اینکه مجال بحث در این فصل محدود است، موضوعات مهمی از قبیل انگیزه‌های گوناگون افراد برای انجام این‌گونه بازی‌ها و تأثیرات احتمالی آن بر اذهان افرادی که بازی می‌کنند بررسی نخواهد شد.

سال‌های سال بود که نه افکار عمومی و نه تشکیلات رسمی رسانه‌ای توجه چندانی به بازی‌های رایانه‌ای نداشتند. ازاین‌رو، اهمیت فزاینده این شکل نوظهور «رسانه» و حتی «هنر» مورد پذیرش قرار نمی‌گرفت و در عوض، بازیگران رایانه‌ای بچه تلقی می‌شدند یا اعضای یک خرده‌فرهنگ عجیب و قریب به‌حساب می‌آمدند که هرگز اتاق‌های تاریک

---

* Martin Bayer

1. Carl Sandburg

خود را ترک نمی‌کردند و با یک وعده پیتزا و کوکاکولا زندگی می‌کردند. اما واقعیت، جور دیگری رقم خورده است. امروزه، چرخش مالی صنعت بازی‌های رایانه‌ای، بیشتر از صنعت سینماست. جامعه «بازیگران رایانه‌ای» بیش‌ازپیش تنوع یافته؛ به‌گونه‌ای که همه گروه‌های سنی از جمله بازنشستگان را نیز در خود جای داده است. برخلاف سابق، نه تنها پسران و مردان بلکه دختران و زنان نیز جذب این‌گونه بازی‌ها شده‌اند. ورود بازی‌های جدید به بازار در بیشتر مواقع با فعالیت‌ها و مبارزه‌های تبلیغاتی چند میلیون پوندی همراه است و شخصیت‌های مجازی از قبیل لورا کرافت[1] در بازی‌های رایانه‌ای به تمثال‌های قرن بیست‌ویکمی مبدل شده‌اند.

اما بازی‌های رایانه‌ای فقط لوله‌کش‌های ایتالیایی که علاقه شدیدی به پریدن از روی موانع دارند، یا حملات بیگانه را که دفع می‌شود، یا شخصیت لورا کرافت که با عنکبوت‌ها و سارقان می‌جنگد نشان نمی‌دهد. بازی‌های رایانه‌ای بیش‌ازپیش با خشونت سروکار دارد. بااین‌حال تنها بخش اندکی از بازار بازی‌های رایانه‌ای درجه‌ای از خشونت را در خود دارد که می‌تواند با آنچه در داستان‌های کودکان توصیف می‌شود رقابت کند. به‌هرحال، خشونت در بازی‌های رایانه‌ای نه تنها در محیط‌های تخیلی به تصویر کشیده می‌شود بلکه در عرصه‌های «واقعیت‌نمایانهٔ» جنگ نیز تجلی می‌یابد. به‌علت آهنگ سریع تحولات فناورانه، بازی‌های رایانه‌ای امروز، ازنظر کیفی، برنامه‌های سمعی ــ بصری بی‌نظیر و خارق‌العاده‌ای را ارائه می‌دهند. ازاین‌رو به‌سرعت در هم‌ترازی با سینمای معاصر قرار گرفته‌اند. این کیفیت بالای سمعی ـ بصری، مانند فیلم‌های سینمایی به‌صورت اصیل و واقع‌نمایانه[2] نمایش داده می‌شوند و علاوه‌بر این، این‌گونه هم تصور می‌گردند. البته این درجه از واقعیت‌نمایی که عمدتاً گرافیکی است در بیشتر مواقع، هیچ ربطی به واقعیت ندارد؛ سربازان مجازی می‌توانند مقدار زیادی تجهیزات انفرادی نظامی را بی‌آنکه خسته شوند بر دوش خود حمل کنند، جراحت‌های مجازی به‌آسانی التیام می‌یابد و مرگ مجازی، فرصت بازی دوباره را به همراه دارد. با وجود این به‌ویژه در زمانی که تمایز میان واقعیت و مجازیت[3] بیش‌ازپیش مخدوش می‌شود، هم بازی‌های رایانه‌ای و

---

1. Lora Croft
2. Realistic
3. Virtuality

هم فیلم‌های سینمایی به برداشت‌ها در مورد جنگ‌های تاریخی و معاصر شکل خواهند داد. به‌طور سنتی تلاقی بازی‌های رایانه‌ای تجاری و شبیه‌سازی‌های نظامی افزایش خواهد یافت؛ زیرا بازی‌های رایانه‌ای تجاری بدیل‌های کم‌هزینه‌ای برای ارتش می‌باشند و در همین راستا، هزینه‌های تولید را می‌توان سرشکن و تقسیم کرد. جالب اینکه بسیاری از طراحان آینده بازی‌های رایانه‌ای از درون نیروهای نظامی ظهور خواهند کرد؛ این وضعیت چه‌بسا شبیه پدیده‌ای است که در میان روزنامه‌نگاران رسانه‌های خبری در منازعات اخیر مشاهده می‌شود.

۱-۲ طراحی برنامه‌های بازی‌های رایانه‌ای

بازی‌های رایانه‌ای در قالب برنامه‌های متنوعی عرضه می‌شود. اولین پیشرفت در ورود این محصولات به بازارهای انبوه با عرضه رایانه‌های خانگی در اوایل دهه ۱۹۹۰ تحقق یافت. رایانه‌های به‌نسبت ارزان، مردم عادی را قادر ساخت از بازی‌های رایانه‌ای در منازل خود استفاده کنند. نمودارهای گرافیکی و طرح‌های موجود در بازی‌ها به‌نسبت ساده انتخاب می‌شدند. اما بسیاری از این بازی‌های اولیه کاملاً اعتیادآور بودند. در بازی‌های جنگی اولیه، بازیگر باید سطح خیال‌پردازی بالایی می‌داشت، چرا که بازنمایی تانک‌ها، سلاح‌ها و هواپیماهای جنگنده فقط به تعدادی تصویر ـ دانه‌های معمولی، محدود می‌شد.

هدف اصلی جعبه‌های بازی رایانه‌ای، همان‌گونه که از نامشان پیداست، انجام بازی است. این «تخصصی شدن» مجال کار آسان با رایانه را فراهم می‌کند (برای مثال، اصلاً هیچ نیازی نیست که شما یک سیستم عامل رایانه را بلد باشید) و امکان اندوختن تجربه قوی درزمینه بازی رایانه‌ای را البته با قیمتی اندک و قدرت تحرّک مضاعف ایجاد می‌نماید.

بعضی از کشورها، برای مثال در ژاپن یا بریتانیا، کنسول‌هایی[1] از قبیل سونی پلی‌استیشن،[2] پی‌اس۲،[3] یا مایکروسافت اکس ـ باکس،[4] بسیار موفق عمل کردند ولی در

1. Consoles
2. Sony Play Station
3. PS2
4. Macrosoft X-Box

کشورهای دیگر، این‌گونه نبود. به‌مرور زمان، بیشتر بازی‌های کنسولی ساده و کنش ــ محور شدند. اما امروزه بازی‌های مشکل‌تری را نیز می‌توان طراحی کرد. «نشان افتخار: خط مقدم»[1] نمونه جدید بسیار موفقی از بازی‌های رایانه‌ای نسل دوم است که طی جنگ جهانی دوم طرح‌ریزی شده بود. جعبه‌های بازی یا نمایش کوتاه خودشان را ارائه می‌دهند یا به دستگاه تلویزیون وصل می‌شوند.

قدیمی‌ترین محوطه‌های تجاری برای بازی‌های رایانه‌ای، پاساژها می‌باشند که در این مکان‌ها متقاضیان، هزینه کمی را برای هر بازی می‌پردازند. دوران باشکوه این پاساژها عملاً به‌سر رسیده است، چرا که برنامه‌های کم‌هزینه‌ای از قبیل کنسول‌ها نه تنها بهای ارزان‌تر برای افرادی که همیشه و مدام بازی می‌کنند ارائه می‌دهند، بلکه طیف وسیع‌تری از بازی‌ها را عرضه می‌کنند. بیشتر بازی‌های رایانه‌ای که در پاساژها ارائه می‌شوند، بازی‌های ساده‌ای است اما بازی‌های جنگی در آنها بسیار جذاب‌اند؛ زیرا پاساژها نه تنها دکمه‌ها و دسته‌های هدایتگر را به‌عنوان ابزارهای ورود به بازی در خود دارند، بلکه ماکت‌هایی از سلاح‌های واقعی را نیز در اختیار مخاطبان قرار می‌دهند. سازنده کره‌ای بازی گیم باکس[2] حتی مدل‌های پردقت‌تری از سلاح‌های مدرن یا تاریخی نیروهای پیاده نظام را که سلاح‌های رؤیایی نامیده می‌شوند، عرضه کرده است.

برای مثال، می‌توان به سلاح آلمان‌ها در جنگ جهانی دوم به نام Mg-34 یا تفنگ‌های بریتانیایی SA-89 اشاره کرد؛ در همهٔ آنها اثر ضربات گلوله به حدی است که سلاح‌ها در بازی رایانه‌ای از شدت ضربه به عقب کشیده می‌شوند.

کیفیت بصری برنامه‌های رایانه‌ای مدرن به زندگی واقعی نزدیک شده است. ازاین‌رو رایانه‌های نسل جدید از این ظرفیت برخوردارند که با بهره‌گیری از علوم «فیزیک» و «اطلاعات جعلی»،[3] بازی‌های حال حاضر را غنی سازند. علم فیزیک بازنمایی درست رویدادهای فیزیکی را بررسی می‌کند؛ برای مثال، صحنه حرکت خودرویی که در پیچ جاده می‌لغزد و واژگون می‌شود واقعی جلوه می‌دهد. اما دانش اطلاعات جعلی دربرگیرنده واکنش کم‌وبیش هوشمندانه اشیای مجازی در برابر محیط‌شان است ـ برای

1. Medal of Honour: Frontline
2. Gamebox
3. Artificial Intelligence

مثال؛ سربازان دشمن منتظر نمی‌مانند تا کشته شوند. بلکه بعد از شلیک گلوله یا بعد از مشاهده طرف مقابل جا خالی می‌دهند یا استتار می‌کنند. متأسفانه این موضوع را می‌توان اضافه کرد که تا حد زیادی، بازی‌های رایانه‌ای برخلاف فیلم‌های سینمایی اکشن، با توجه به کیفیت سمعی ـ بصری‌شان خرید و فروش می‌شوند.

انفجارهای مهیب، صحنه‌های پرطمطراق، تسلیحات شبیه به عالم واقع و جلوه‌های ویژه خیالی از نوعی جذابیت برخوردارند. اما درهرحال، هدف اصلی یک بازی، سرگرمی است و دردناک است که مشاهده می‌کنیم چه بسیار بازی‌های رایانه‌ای که امروزه در نیل به این هدف اساسی ناکام مانده‌اند. حال آنکه برخی از بازی‌های اواسط دهه ۱۹۸۰، با وجود محدودیت‌های زیادی که ازنظر فناوری داشتند، هنوز همچنان تجربیات ارزنده‌ای درزمینه بازی‌های رایانه‌ای ارائه می‌دهند.

چشم‌انداز آینده چه‌بسا ممکن است به توصیفاتی که در رمان علمی ـ تخیلی *فارنهایت ۴۵۱*[1] اثر بای برادبرگ[2] وجود دارد شباهت داشته باشد؛ در این رمان دستگاه‌های تلویزیون سه‌بعدی، چهاردیواری اتاق‌های نشیمن را اشغال کرده‌اند. در محیط‌های مجازی رایانه‌ای، تصاویر سه‌بعدی روی شش دیوار نمایش داده می‌شوند. بازیگر رایانه‌ای با ایستادن در میانه این اتاق، دیگر نیازی ندارد که کلاه بدترکیب واقعیت مجازی را به‌سر گذارد؛ بلکه فقط باید یک عینک سبک آفتابی به چشم بزند و این اولین گام به‌سوی رؤیای سفر به ستارگان از روی عرشه کشتی است. بدین‌سان، بازیگر رایانه‌ای بدون نیاز به صفحه نمایشگر، صفحه کلید، یا ماوس می‌تواند در محیط مجازی سیر کند و کل این تجربه نیز تجربه‌ای به‌مراتب واقعیت‌نمایانه‌تر است. این محیط‌های مجازی رایانه‌ای که در حال حاضر وجود دارد، اولین بار در سال ۱۹۹۱ ایجاد شد.

حالا دیگر محیط‌های مجازی رایانه‌ای به‌قدری ارزان‌اند که مدل تجاری کارآمدی را برای سالن‌های سرگرمی فراهم می‌کنند. بااین‌همه، باید به خاطر داشت که بعضی افراد، همین الان هم در تمایزگذاری میان جهان مجازی و عالم واقع مشکلاتی دارند، ازاین‌رو ممکن است توسعه فناوری در این حوزه مشکلات جدی‌ای را درزمینه تشخیص واقعیت برای کسانی که اذهان ناپایدار و بی‌ثباتی دارند، پدید آورد.

---

1. Fahrenheit 451
2. Bay Bradbury

۲-۲ تعریف و بافتار تاریخی

آسان‌ترین راه برای تعریف بازی‌های جنگی رایانه‌ای این است که بگوییم چه بازی‌هایی، بازی‌های جنگی رایانه‌ای نیستند. بازی‌های جنگی رایانه‌ای با محیط‌های خیالی‌ای که در درون آنها استفاده از سلاح، همراه با وردهای جادویی و سایر قوای فوق طبیعی پرمایه می‌شود و بازیگران نیز با گله‌های دراگون‌ها، مرده‌های متحرک و موجوداتی از این قبیل نبرد می‌کنند، سروکار ندارند. علاوه‌بر این، محیط‌های علمی ــ تخیلی نیز مشمول این تعریف قرار نمی‌گیرند؛ البته ممکن است نبرد در فضا علیه نژادهای غیرانسانی شبیه‌سازی شود. بدین‌سان، بازی‌های جنگی رایانه‌ای به شبیه‌سازی یا نمایش دوباره منازعات تاریخی یا معاصر، از جمله رویدادهای فرضی اطلاق می‌شوند. با وجود این، یک فضای خاکستری در این تعریف وجود دارد: رویدادهای فرضی‌ای که در بازی رایانه‌ای «عملیات نقطه انفجار: بحران جنگ سرد»[1] به نمایش درآمدند می‌توان مرتبط با یک واقعیت محتمل تلقی کرد، اما مردگان متحرکی که دانشمندان دیوانه نازی، آنها را در بازی رایانه‌ای «بازگشت به قلعه ولفن اشتاین»،[2] دوباره زنده می‌کنند، مسلماً این‌گونه نیست. نمونه دیگر برای موارد «چه می‌شود اگر ...؟»، بازی رایانه‌ای «طوفان آهنین»[3] است: در این بازی، جنگ جهانی اول در سال ۱۹۱۸ پایان نیافته است، بلکه به مدت پنجاه سال دیگر نیز ادامه یافته است. از همه‌چیز که بگذریم، چنین بازی‌هایی سرگرمی‌هایی می‌باشند که گاهی اوقات، پیامی (معمولاً سیاسی) به آنها افزوده شده است. پدیده دیگری که در این زمینه در حال شکل‌گیری است، خلط بازی‌های رایانه‌ای تجاری با شبیه‌سازی‌های نظامی حرفه‌ای است.

بازی‌های رایانه‌ای جنگی در بافتارهای تاریخی متنوعی قرار می‌گیرند. بازی‌هایی از قبیل «عصر امپراتوری‌ها»، عصر حجر یا دوران باستان را به تصویر می‌کشند و بازنمایی می‌کنند. در این‌گونه بازی‌ها بازیگر حتی می‌تواند نژاد خود را از یک عصر به عصر دیگر و به‌عبارت دقیق‌تر از عصر حجر به عصر آهن تغییر دهد. در بازی‌هایی که به «سده‌های

---

1. Operation Flashpoint: Cold War Crisis
2. Return to Castle Wolfenstein
3. Iron Storm

میانه» مربوط می‌شوند، مثل بازی‌های، «عصر امپراتوری‌ها»، «دژ»[1] یا «عصر پادشاهان»،[2] ساخت قلعه‌ها و نبرد در داخل آنها معمولاً محور این بازی‌ها می‌باشد. در این بازی‌ها، ابزارهای محاصره به‌شدت مورد تأکید قرار می‌گیرند، حال آنکه تأکید بر آنها اعتبار تاریخی ندارد. در عالم واقع، محاصره‌ها معمولاً مبتنی‌بر این استراتژی بود که دشمن را با گرسنگی دادن وادار به خروج از قلعه کند: اگر این گزینه در یک بازی جای داده شود، چندان سرگرم‌کننده نخواهد بود و خستگی و ملالت مخاطب را به دنبال خواهد داشت. سوژه بازی‌هایی از قبیل «قزاق‌ها»[3] یا «شوگان‌ها»[4] به اوایل دوران مدرن بازمی‌گردد. همین که جنگ‌افزارهای گرم از قبیل اسلحه‌های آتشین مطرح می‌شوند، بردهای تفنگ‌ها در بازی‌ها بیشتر مواقع باهمتایان واقعی آنها در عالم واقع تفاوت دارند؛ این تفاوت بدان علت است که بازی‌ها با وضعیت‌های متنوع واحدهای نظامی گوناگون تطابق داشته باشند و ازاین‌رو برنامه‌های رایانه‌ای بازی پرچالشی را به نمایش می‌گذارد و توصیف آنها از رویدادهای تاریخی نیز از دقت کمتری برخوردار است. بی‌شک، دوران مدرن برای کسانی که این‌گونه بازی‌ها را توسعه داده‌اند در قیاس با سایر دوره‌ها جذابیت بیشتری دارد، چرا که این دوران سیستم‌های تسلیحاتی متعدد و همه نوع نمایش‌های جنگی را برای مخاطبان عرضه می‌کند. جنگ جهانی اول به‌ندرت به نمایش درمی‌آید چرا که تنها عمدتاً شبیه‌سازی‌های پرواز را به تصویر می‌کشد. برنامه رایانه‌ای «ظهور قهرمان»[5] در این مقوله می‌گنجد. این امر شاید تعجب‌آور هم نباشد؛ زیرا روش‌های بارز نبرد در این منازعه جهانی فقط امور پیش‌پاافتاده‌ای از قبیل گلوله‌باران سنگرها، عبور از شبکه‌های سیم‌خاردار و زیر رگبار مسلسل قرار گرفتن بود؛ به تصویر کشیدن تجربه بازی سرگرم‌کننده و هیجان‌انگیز براساس روایت‌های تاریخی در مورد جنگ جهانی اول دشوار است.

«مادر همه جنگ‌ها» که سوژه بازی رایانه‌ای جنگی قرار گرفته است، به‌طورقطع جنگ جهانی دوم است؛ هر چیزی که بازیگر رایانه‌ای می‌خواهد برای این نوع سرگرمی

---

1. Stronghold
2. The Age of Kings
3. Cossacks
4. Shoguns
5. Dawn of Ace

داشته باشد، در رویداد تاریخی جنگ جهانی دوم وجود دارد. اولاً، تمایزی آشکار میان خیر (قهرمانان) و شر (جنایت‌کاران) وجود دارد. با وجود این، برگزیدن شر چه‌بسا ممکن است شور و هیجان خاصی را برای برخی ایجاد کند. ثانیاً، انواع و اقسام سیستم‌های تسلیحاتی غول‌پیکر، از جمله تانک‌ها، زیردریایی‌ها، کشتی‌های جنگی و گونه‌های متنوعی از سلاح‌های پیاده‌نظام وجود دارد. نبرد و ستیز نیز می‌تواند روی زمین، در هوا و بر سطح آب و حتی زیر سطح آب انجام گیرد. ثالثاً، آن صحنه‌های جنگ و نبرد که به نمایش درمی‌آیند، از بیابان‌های شمال آفریقا تا سواحل اقیانوس اطلس، از جزایر اقیانوس آرام تا جنوب شرق آسیا، از نروژ تا ایتالیا و از بریتانیا تا استپ‌های وسیع اتحاد شوروی را دربرمی‌گیرند. بدین‌سان، بازیگرانی که محیط‌های نامتعارف و عجیب‌وغریب را ترجیح می‌دهند درواقع همان کسانی هستند که محیط‌های «محلی» از قبیل شهر یا کشور خودشان را ترجیح می‌دهند. فهرست بازی‌های مرتبط با جنگ جهانی دوم تقریباً پایان‌پذیر است. نمونه‌های جدید، بازی‌های رایانه‌ای موفقی از قبیل مجموعه‌های «نشان افتخار» و «میدان نبرد ۱۹۴۲» و بازی‌های استراتژی‌پردازانه مثل «بلیتزریگ»[1] و «مخفی و خطرناک ۲»[2] و «مأموریت نبرد»[3] را شامل می‌شود.

به‌ندرت اتفاق افتاده است که جنگ سرد، سوژه‌ای برای بازی‌های رایانه‌ای باشد؛ بااین‌حال در این اواخر، تعداد قابل توجهی از بازی‌های رایانه‌ای ـ برای مثال، وایتکنگ[4] ـ براساس جنگ ویتنام طراحی شده است. به‌نظر می‌رسد که بیشتر جنگ‌های نیابتی[5] از آن هیجان‌های مورد نیاز برای بازی‌های رایانه‌ای بی‌بهره‌اند، چرا که کنشگران اصلی جنگ سرد (حداقل نه در مقیاس وسیع) با یکدیگر به‌طور مستقیم وارد جنگ نمی‌شدند. ازاین‌رو، در بازی‌هایی که جنگ سرد را به‌عنوان پس‌زمینه برمی‌گزینند، معمولاً برمبنای رویدادهای فرضی طراحی می‌شود. داستان بسیار واقعیت‌نمایانهٔ «عملیات نقطه انفجار: بحران جنگ سرد»[6] براساس سرگذشت یک ژنرال پست‌فطرت و جانی شوروی است که

1. Blitzrieg
2. Hidden and Dongerous II
3. Combat Mission
4. Vietcong
5. Proxy Wars
6. Operation Flashpoint: Cold War Crisis

بعد از به قدرت رسیدن گورباچف در اواسط دهه ۱۹۸۰ به کشور خیالی اورن[1] در اروپای شرقی حمله می‌کند.(۱) بازی‌هایی که جهان معاصر را پوشش می‌دهد در بیشتر موارد رویکرد مشابهی را به‌کار می‌گیرد؛ برای مثال، بازی رایانه‌ای «منطقه منازعه یا جنگ واقعی» دشمنان خیالی مثل سازمان‌های تروریستی، شرکت‌های بین‌المللی، یا اتحادهای دولتی را نمایش می‌دهد؛ این بازی‌ها با این رویه، سازمان آتلانتیک شمالی (ناتو)، سازمان ملل متحد یا به‌طورکلی غرب را به چالش می‌کشد. در بازی رایانه‌ای «جنگ جهانی سوم ـ طلای سیاه»[2] بازیگر باید از میان سه طرف جنگ یعنی آمریکا، چین و عراق یکی را برای جنگیدن بر سر آخرین ذخایر نفتی جهان انتخاب کند؛ ـ بسته به دیدگاه و بینش شما ـ اما به‌نظر می‌رسد که این بازی در حال حاضر منسوخ شده و از رواج افتاده است، یا دیگر هیچ مناسبت و موضوعیتی ندارد.

در جهان واقعی امروز، هم‌اکنون تروریسم موضوع داغی برای بازی‌های رایانه‌ای است. اندکی بعد از یازده سپتامبر، تعدادی بازی ساده و خانگی بر اینترنت ظاهر شد؛ یکی از آنها بازی «مشروب‌های بن‌لادن»[3] بود. در این بازی، بازیگر می‌توانست یک اسامه بن‌لادن مجازی را بکُشد. در بسیاری از بازی‌ها که هر روز بر تعدادشان افزوده می‌شود، از قبیل «سلول انشعابی»،[4] مجموعه‌های «نیزه یاغی»،[5] «سرباز شانس ۲»[6] و «رزمنده زمینی ۳»،[7] جنگ علیه تروریسم را می‌توان حتی در جبهه خانه‌ها و منازل نیز پی گرفت. دیدگاهی که در این بازی‌ها مطرح می‌شد، دیدگاهی عمدتاً غربی بود، اما باید خاطرنشان ساخت تعداد زیادی از این بازی‌ها را سازمان‌هایی از قبیل حماس یا حزب‌اله تولید می‌کنند. بازی‌هایی از جمله «نیروی ویژه» این مجال را برای بازیگر رایانه‌ای فراهم می‌کند که در فضایی مجازی با سربازان رژیم صهیونیست بجنگد. این بازی‌ها مانند ارتش آمریکا در نهایت می‌کوشند سربازان جدیدی را برای امور واقعی جذب کنند و بنابراین، بعد جدیدی را که

---

1. Everon
2. World War III-Black Gold
3. Bin Laden Liquors
4. Splinter Cell
5. The Rogue Spear
6. Soldier of Fortune II
7. Land Warrior III

همان پس‌زمینه سیاسی است فراروی بازی رایانه‌ای می‌گشایند. به‌طبع، بازی‌هایی از قبیل «بازگشت به بغداد»[1] همواره بعد سیاسی نیز دارد،(۲) اما این بعد سیاسی نیز برای جامه عمل پوشاندن به ایده‌های سیاسی در مقیاسی به‌مراتب گسترده‌تر به «بازی‌های جذب نیرو» نیاز داشت. باز هم جالب خواهد بود که ببینیم چگونه محتوای سیاسی بازی‌های جنگی در چند سال آینده، به‌ویژه در جهان غیرغربی گسترش خواهد یافت.

۳-۲ ژانرهای بازی‌های رایانه‌ای

تقریباً تمامی ژانرهای بازی‌های رایانه‌ای (به‌جز ژانرهای ورزشی و مسابقات) می‌توانند جنگ را به‌عنوان موضوع اصلی خود برجسته سازند. در برنامه‌های ماجراجویانه، بازیگر از شخصیت از پیش تعریف شده‌ای استفاده می‌کند که می‌تواند مجموعه‌ای از پازل‌ها را حل نماید و در نهایت نیز در بیشتر مواقع به کمک تعامل با افراد دیگر (به‌عبارت دقیق‌تر، شخصیت‌های مجازی) به هدف اصلی دست می‌یابد. هدف اصلی می‌تواند محدود مثل نجات یک شاه‌بانو، یا وسیع‌تر مثل نجات کل جهان باشد؛ معمولاً، برنامه‌های ماجراجویانه فقط بازی‌های تک بازیگراند. یکی از بازی‌های جنگی پرشمار با این ژانر، برنامه ماجراجویانه سه بعدی واکنشی به نام «زندانی جنگی»[2] است که در آن، بازیگر در نقش افسر نیروی هوایی آمریکا که در اردوگاه‌های مختلف زندانیان جنگی آلمان در اسارت نازی‌هاست، برای آنکه خودش را از بند اسارت آزاد سازد، ناگزیر است پازل‌هایی را حل کند. اما ازآنجاکه حل پازل‌ها برای تحقق «هدف عالی‌تر» کفایت نمی‌کند، وی ناگزیر است اطلاعاتی در مورد برنامه‌ای که آلمان‌ها برای توسعه تسلیحات کشتارجمعی طراحی کرده‌اند به‌دست آورد. افسر نیروی هوایی آمریکا با به انجام رساندن این مأموریت بسیار جدید، در نهایت جهان را نجات می‌دهد.

بازی‌هایی که در آنها بازیگر درواقع نقش یک شخصیت را بازی می‌کند تاحدی به برنامه‌های رایانه‌ای ماجراجویانه شباهت دارد. در این بازی‌ها بازیگر ناگزیر است مجموعه‌ای از پازل‌ها را حل کند. علاوه‌بر این، بازیگر نه تنها یک شخصیت از پیش

---

1. Back to Baghdad
2. Prisoner Of War (POW)

تعریف شده، بلکه کل مجموعه شخصیت‌هایی را که توانایی‌های آنها (برای مثال، استفاده از تسلیحات خاص یا غافلگیرسازی یا کسب مخفیانه اخبار) می‌تواند در سراسر بازی بهبود و افزایش یابد، هدایت می‌کند. بیشتر این‌گونه بازی‌ها در عالم خیال قرار می‌گیرند، اما به‌واقع، نوعی بازی‌های جنگی موجود است که بازیگر نقش فرماندهی گروه مزدوران را بازی می‌کند؛ مجموعه‌های «اتحاد پر فراز و نشیب»[1] در این مقوله می‌گنجد. ارتش آمریکا با طراحی بازی رایانه‌ای جدیدی با نام «سربازان ارتش آمریکا»[2] که به‌زودی منتشر می‌شود، رویکرد واقعی جذابی را در پیش گرفته است. در این بازی، بازیگر می‌تواند شغلی در ارتش آمریکا انتخاب کند و همچنین می‌تواند درباره تشکیلات و دورنماهای احتمالی شغل خود اطلاعاتی کسب کند. این تأکیدگذاری بر ابعاد آموزشی، اقدام شگفت‌آوری نیست چرا که این برنامه درواقع یک «بازی عضوگیری و جذب افراد» در ارتش است و ازاین‌رو مجانی بین افراد پخش شده است.

بازی‌های اکشن ساده، که «بزن و بکش» نیز نامیده می‌شوند، در حال حاضر بیش‌ازپیش منسوخ شده‌اند. در مورد بازی‌های جنگی؛ اولاً، محتوای این بازی‌ها فقط کشتن تعداد زیادی از افراد دشمن در حداقل زمان ممکن است که به‌نظر می‌رسد این نوع محتوا برای بسیاری هیچ جذابیتی ندارد. ثانیاً، این نوع بازی‌ها در آلمان به یک نوع شاخص بدل شد. پیشینه تمجید از جنگ و خشونت در آلمان باعث شده که این کشور به سومین بازار بازی‌های اکشن در سراسر جهان مبدل شود.(۳) یکی از نمونه‌های بارز این بازی‌ها، به نام «نیروهای ویژه لیبی» است، در این بازی، وظیفه بازیگر فقط این بود که امواج اتهامات علیه فرزندان قذافی را از بالای صفحه نمایشگر به‌سمت پایین آن گلوله‌باران کند. بیشتر مواقع، داستان متن از پیش نوشته نشده است؛ در بازی اکشن، فقط دشمنان ناشناس‌اند که برای کسب امتیاز باید آنها را کشت و البته این دشمنان به هیچ کشور یا آرمانی وابستگی ندارند.

یک ژانر بسیار مهم در بازی‌های جنگی، شبیه‌سازی است که البته سلطهٔ فناوری‌های پیچیده بر همگان مشهود است. ممکن است جنگیدن در جنگ واقعی حتی کم‌اهمیت

---

1. Jagged Alliance
2. America's Army Soldeiers

برداشت شود؛ چرا کـه تقریباًهمـه نـوع تجهیـزات جنگـی، از تانـک‌هـا (مـثلاً در «هـشت زره‌پوش») گرفته تا زیردریایی‌ها (در «قهرمانان اعماق»)[1] و از هلی‌کوپترهـا (در «هلـی‌کـوپتر شکاری!»)[2] گرفته تا هواپیماهای جنگنده (در «مجموعه‌های شبیه‌ساز پروازهـای جنگـی»)[3] در حال حاضر شبیه‌سازی شده‌اند. اما با وجود این، تمایزی نیز میان شبیه‌سازی‌های بـسیار دقیق و شبیه‌سازی‌های اکشن‌محور[4] وجود دارد. در شبیه‌سازی‌هـای بـسیار دقیـق، بـازیگر برای احاطه بر سازوکار و تشکیلات بازی به فرصت معمول قابل ملاحظـه‌ای نیـاز دارد؛ امـا در مقابل، بازی‌هایی که در گروه دوم جای می‌گیرند تأکید بیشتری بـر عنـصر «سـرگرمی» دارند که در مورد شبیه‌سازان صحنه‌های نبرد و رزم، واقعی است.

تجهیزات جنگـی براسـاس پیچیـدگی‌هـای تمـام‌عیـاری کـه دارنـد، شـبیه‌سـازی نمی‌شوند. یک نمونه از این شبیه‌سازی‌های اکشن، مجموعه «کومانخه»[5] است کـه در آن، هلی‌کوپتر ار. ای. اچ ـ ۶۶[6] نقش اول را بـازی مـی‌کنـد. در برخـی از شـبیه‌سـازی‌هـای واقعیت‌نمایانه‌تر احتمال دارد نقص و نارسایی نیز وجود داشته باشد (برای مثـال، ممکـن است برخی خمپاره‌ها عمل نکرده باشند یا اینکه برخی موشک‌هـا بـه هـدف مـورد نظـر اصابت نکنند). بااین‌حال، ممکن است بازی‌هایی هم که پیچیدگی کمتـری دارنـد نـوعی (سوء) برداشت به دنبال داشته باشند: در چنین شبیه‌سازی‌هایی، سلاح‌های بسیار دقیق همیشه به هدف می‌خورند. اما این میزان دقت حتی در مورد پیشرفته‌ترین سیستم‌هایی که در دسترس ارتش می‌باشند، صدق نمی‌کند. بازیگران[7] می‌پذیرند که سخت‌افزارشـان[8] در منازعات واقعی به‌کار می‌روند و ازاین‌رو تجربه خود را بـه اشـتباه، بـه واقعیـت پیونـد می‌زننـد. یکـی از نمونـه‌هـای بـارز ایـن وضـعیت، شکـست‌ناپـذیری بـازیگر در بعـضی بازی‌هاست. وانگهی، در بازی‌های رایانه‌ای، رنج‌ها و مصیبت‌های شایعی که در اثر جنـگ

---

1. Aces of the Deep
2. Gunship
3. Combat Flight Simulator
4. Action-oriented Simulations
5. Comanche
6. RAH-66
7. Gamer

۸. سخت‌افزاری که در بازی‌های رایانه‌ای به تصویر کشیده می‌شود ـ م.

به بار می‌آید اصلاً در نظر گرفته نمی‌شود. ازاین‌رو، بازی‌های رایانه‌ای جنگی بیشتر مواقع نوع پاک[1] و جوانمردانه‌ای از رزم‌های تن‌به‌تن مانند نبردهای شوالیه‌ها و شهسواران در دوران گذشته به‌شمار می‌آیند. این نوع بازی‌های رایانه‌ای به‌ویژه درباره روایت‌های شبیه‌سازان عملیات پروازی، که بیشتر صبغه تاریخی دارند، صدق می‌کند. یکی از ابعاد مهم در این مورد همگرایی شبیه‌سازان حرفه‌ای با بازی‌های شبیه‌سازی تجاری است. برای مثال، «شبیه‌ساز پرواز»[2] مایکروسافت در حال حاضر برای ارائه آموزش‌های نظری درزمینه پرواز مورد استفاده نیروهای مسلح آمریکا قرار می‌گیرد، چرا که این برنامه رایانه‌ای، از یک‌سو هم‌سطح مناسبی از واقعیت‌نمایی در ارائه خدمات را رعایت می‌کند و ازسوی‌دیگر دستمزد ارزانی را درزمینه حق امتیاز خود به‌ویژه در مقایسه با شبیه‌سازی‌های حرفه‌ای از ارتش دریافت می‌کند.

یکی از مردم‌پسندترین ژانرها در بازی‌های رایانه‌ای معاصر، به‌اصطلاح «بازی استرتژی‌محور» است. تعداد زیادی بازی‌های استراتژی‌محور غیرخشونت‌آمیز وجود دارند که برای مثال، بازیگر باید زیرساخت یک شهر را توسعه دهد (مجموعه «سیم‌ـ سیتی» در این مقوله می‌گنجد). بااین‌حال، بسیاری از بازی‌های استراتژی‌محور بر محتوای نظامی تأکید دارند و محتوای نظامی را محور قرار می‌دهند. برای زدودن سوءبرداشت شایع، در همین آغاز باید گفت بیشتر بازی‌های استراتژی‌محور جنگی، برخلاف نامشان، نه به سطح استراتژیک رزم بلکه بالعکس به سطح تاکتیکی آن می‌پردازند. تانک‌های تک‌سرنشین یا سربازان (یا حداکثر، گروهی از آنها) هدایت می‌شوند، که در برخی موارد به نوعی «خرده ـ مدیریت جنون‌آمیز»[3] می‌انجامد. در بازی‌های استراتژی‌محور دو نحلهٔ عمده وجود دارد: یکی، بازی‌های استراتژی‌محور نوبتی[4] و دیگری، بازی‌های استراتژی‌محور هم‌زمان،[5] بازی‌های نوبتی را می‌توان دنباله[6] بازی شطرنج با ابزاری دیگر

---

1. Clean
2. Flight Simulator
3. Frantic Micro-management
4. Turn-ba
5. Real Time
6. Continuation

توصیف کرد چرا که مبتنی‌بر صفحه بازی و بازی‌های قلم و کاغذی است. دو ارتش (یا بیش از دو ارتش) با یکدیگر می‌جنگند و هر بازیگر در هر نوبت می‌تواند تعداد معین و مشخصی حرکت انجام دهد؛ برای مثال، یک بازیگر می‌تواند یک تانک را به‌سمت موقعیت معینی حرکت دهد و این در صورتی است که نقاط درگیری، حجم آتش تیراندازی، یا مسلح کردن مجدد تانک به مقدار کافی وجود داشته باشد. برخی از این بازی‌ها سطح بسیار عمیقی از شبیه‌سازی را در خود دارند. برای مثال، بازی «جبهه شرقی»[1] در این مقوله می‌گنجد: در این بازی، همه سلاح‌های پیاده‌نظام انواع و اقسام تانک‌ها، یا انواع خاصی از منازعه تاریخی در یک زمان و مکان مشخص به نمایش درمی‌آیند. البته، عوامل بسیاری وجود دارند که می‌توانند در اجرای مطلوب بازی اختلال به‌وجود آورند، که دراین‌میان می‌توان به نوع منطقه درگیری،[2] ارتفاع آن، مجموعه دامنه دید، یا آب‌وهوا اشاره کرد. بازی‌هایی از قبیل مجموعه «ژنرال زره‌پوش»[3] که اولین قسمت آن در آلمان منتشر شد، از دقت کمتری برخوردار بود، ولی بیشتر مورد استقبال قرار می‌گرفت؛ چرا که در این بازی‌ها بازیگر ناگزیر بود به جنگ تجاوزگرانه دست بزند.

از اوایل دهه ۱۹۹۰، بازی‌های استراتژی‌محور هم‌زمان به یکی از موفق‌ترین ژانرهای بازی مبدل شده‌اند. ویژگی اصلی بازی‌های استراتژی‌محور هم‌زمان این است که همه اقدامات بازیگران (از جمله اقدامات مجازی آنها) بدون رعایت نوبت به‌صورت هم‌زمان انجام می‌گیرند. این امر بازی را پرشتاب‌تر می‌سازد و برای بسیاری از بازیگران نیز خوشایند می‌باشد.

هرچند ممکن است این نوع ژانر فراگیر باشد، اما رویکردهای متنوعی که هریک از این بازی‌ها به‌کار می‌گیرند، واقعاً قابل توجه و چشمگیرند. برای مثال، در «کماندوی ۲»،[4] وقتی بازیگر مأموریت‌هایی را در پشت خطوط نبرد آلمانی‌ها برعهده می‌گیرد، نباید حتی یکی از سربازان نیروهای ویژه خود را از دست بدهد. درست برخلاف بازی‌های استراتژی‌محور هم‌زمان، بازیگر نمی‌تواند واحدهای نظامی بیشتری را تدارک ببیند و

1. Eastern Front
2. Terrain
3. Panzer General
4. Commando II

سرانجام به یُمن برتری و مزیتی که ازنظر تعداد نیرو و ادوات دارد، دشمن را از پای در می‌آورد. «منطقه منازعه»[1] و «جنگ واقعی»[2] نمونه‌های بارزتری از بازی‌های استراتژی‌محور هم‌زمان‌اند. در این بازی‌ها، بازیگر می‌تواند با احداث کارخانه‌های تولید سلاح یا پادگان‌های تربیت نیروی انسانی و استفاده از منابعی از قبیل پول، نفت یا جایگاهش در نزد افکار عمومی یگان‌های نظامی‌اش را ایجاد کند. در این خصوص، مجموعه «حمله ناگهانی» از رویکرد واقعیت‌نمایانه‌تری بهره می‌گیرد. در این مجموعه، بازیگر می‌تواند در روند بازی، نیروهای کمکی دریافت کند، اما نمی‌تواند سربازان جدید خلق کند یا تجهیزات جدید بسازد. تقریباًهمه این بازی‌ها به‌اصطلاح از چشم‌انداز ایزومتریک[3] استفاده می‌کنند که معمولاً چندین سطح زوم[4] را در خود دارد. شمار یگان‌هایی که به نمایش درمی‌آیند از تعدادی معدود (مثلاً در «کماندوها») شروع می‌شود و تا چند صد یگان (مثلاً در بلیتزریگ) می‌رسد.

یکی از ژانرهای بسیار مهم، که البته به‌هیچ‌وجه نیز مسلط نبوده است ژانر «اولین تیرانداز (یا خود تیرانداز)[5] است. در چنین بازی‌هایی، بازیگر، جهان سه بعدی مجازی را از چشمان شخصیت بازی،[6] درحالی‌که سلاح به‌دست گرفته است و راهش را از میان دشمنان بی‌شمار می‌پیماید، مشاهده می‌کند. بازیگر تنها ناگزیر است شخصیت بازی را از روی آتش تسلیحات و ادوات جنگی که سخت‌افزار رایانه فراروی او قرار داده است عبور دهد. اگر قهرمان بازی مجروح شود، برای نجات فوری وی می‌توان از بسته‌های خدمات بهداشتی بهره گرفت. بازی سه‌بعدی «قلعه ولفن اشتاین» که در سال ۱۹۹۲ به بازار عرضه شد، اولین مورد از این نوع بازی‌هاست. هرچند اولین نمونه از ژانر «اولین تیرانداز» درواقع یک بازی جنگی بود، اما سال‌ها گذشت تا ژانری از این نوع تولید شود؛ چرا که فضاهای علمی ـ تخیلی یا خیال‌پردازانه در ژانرهای «اولین تیرانداز» بازار عرضه

---

1. Conflict Zone
2. Real War
3. Isometric Perspective
4. Zoom Levels
5. Ego-or First-Person shooter

۶. که بازیگر را نمایندگی می‌کند ـ م.

این نوع بازی‌ها را تسخیر کرد. اما در سال‌های اخیر، بازی‌های جنگی در این نوع ژانرها غلبه کردند. تا اواسط دهه ۱۹۹۰ هم فضا و هم اهداف به‌نسبت ساده بودند؛ بازی‌ها در این خلاصه می‌شدند که: راه خروجی را بیاب و هر چیزی را که حرکت می‌کند بکش.

از آن تاریخ تاکنون، این ژانر به میزان چشمگیری توسعه و تکامل یافته است و عرصه برای طراحی سناریوهای پیچیده و همکاری مهیا شده است. از یک‌سو، مانند شبیه‌سازی‌ها، تک‌تیراندازهای واقعیت‌نمایانه‌تری وجود دارند (مثل بازی «ارتش آمریکا: عملیات‌های نظامی و عملیات نقطه انفجار») و ازسوی‌دیگر بازی‌های اکشنی[1] از قبیل نشان افتخار یا میدان نبرد ۱۹۴۲[2] تولید شده‌اند. «ارتش آمریکا: عملیات‌های نظامی و عملیات نقطه انفجار» بر تجربه «واقعیت‌نمایانهٔ» نبرد تأکید دارد؛ در این بازی، بازیگر باید مخفی شود، منتظر بنشیند، ادوات نظامی را ذخیره کند و به سیاق تاکتیک‌های نظامی عمل کند و پیش برود. اما بازی‌های نشان افتخار یا میدان نبرد ۱۹۴۲ بر صحنه‌های اکشن تأکید دارند: در این نوع بازی‌ها، ادوات و تجهیزات نظامی به وفور فراهم‌اند، شمار دشمنانی که قرار است کشته شوند زیاد است، بازیگر می‌تواند سلاح‌های زیادی را با خود حمل کند و (اگر جراحتی دید)، جراحتش بی‌درنگ التیام می‌یابد، اما درعین‌حال باید گفت تاکتیک‌هایی مثل پریدن و به مسلسل بستن (از کناره‌ها دشمن را محاصره کردن و در همان حال، تیراندازی به‌سوی نیروهای دشمن) در قیاس با عالم واقع، معقول و منطقی‌اند. بیشتر بازی‌هایی که در آنها تیراندازی محوریت دارد، طرف‌های بازی بیش از دو طرف است و تنها دو طرف از میان چهار، هشت یا گاهی اوقات بیش از هشت بازیگری که وجود دارند، با یکدیگر مبارزه می‌کنند و می‌جنگند. یکی از نمونه‌های معروف این بازی‌ها، بازی «نیمه‌جان: ضدحمله»[3] است. در این بازی، گروهی از تروریست‌ها با گروهی از نیروهای پلیس می‌جنگند. برای آنکه پاسبان‌ها و سارقان بتوانند در این نبرد مجازی به‌نحوی موفق و مناسب عمل کنند بازیگران باید ارتباطات گسترده‌ای باهم برقرار نمایند و تاکتیک‌های خود را به‌نحو کارآمدی با یکدیگر هماهنگ سازند.

---

1. Action-Oriented
2. Battlefeild 1942
3. Half Life: Counterstrike

۲-۴ واقعیت‌نمایی[1] در برابر واقعیت

در بازی‌های رایانه‌ای مانند صنعت سینما، تمایل به واقعیت‌نمایی «مطلق» در انجام بازی زیاد است: بیشتر مواقع، این مؤلفه در فعالیت‌های تبلیغات بازرگانی به‌عنوان یکی از اصلی‌ترین عوامل جذب مشتری به‌کار می‌آید. اما، چه نوع واقعیت‌نمایی‌ای مطلوب است؟ برای پاسخ دادن به این پرسش، انجام یک مطالعه موردی کوتاه می‌تواند مفید باشد: بازی «شما بازی نمی‌کنید ـ شما داوطلب می‌شوید»[2] شعار تبلیغاتی برای بازاریابی بازی نشان افتخار است. جالب اینکه اجرای این پروژه زمانی آغاز شد که طراحانش پیش از آن، یک فیلم سینمایی جنگی را تولید کرده بودند؛ این فیلم سینمایی سطوح جدیدی از واقعیت‌نمایی را به نمایش می‌گذاشت و سازندگان آن تمام تلاش خود را به بهترین نحو به‌کار بسته بودند تا مخاطب را درگیر صحنه‌های اکشن فیلم نمایند؛ در این راستا، آنها از جلوه‌های ویژه سمعی ــ بصری استفاده کرده بودند؛ سبک کار آنها از نوع فیلم‌های خبری بود که به‌خوبی توانسته بودند تصویری واقعیت‌نمایانه از صحنه‌های خشونت‌های دسته‌جمعی را به نمایش بگذارند.

در بازی نشان افتخار، طراح بازی می‌خواست یک تجربه تعاملی[3] را خلق کند به‌گونه‌ای که بازی رایانه‌ای تا آنجا که امکان دارد به ویژگی‌های فیلم سینمایی نزدیک شود. سازندگان این بازی رایانه‌ای اثر بی‌نظیری را تولید کردند؛ بدین‌سان، هم «نشان افتخار: حمله متفقین» و هم «نشان افتخار: خط مقدم» ازلحاظ کیفیت تصویر و صدا در سطح حیرت‌انگیزی بودند. هر دو بازی بسیار موفق بودند و زمینه‌های بسیار مساعد و مناسبی را برای انجام بازی رایانه‌ای در اختیار مخاطب قرار دادند. فوق‌العاده‌ترین صحنه بازی نشان افتخار حمله قایق فرانسوی نورماندی[4] به کشتی دی ـ دی[5] در ششم ژوئن ۱۹۴۴ است. در همین سطح، نشان افتخار از این نظر که هم جذاب است و هم به نوعی ناکامی را در پی دارد یک بازی رایانه‌ای است که مخاطب، صحنه‌های آن را واقعیت می‌انگارد، چرا که تنها وظیفه بازیگر این است که از معرکه جان سالم به در ببرد. وی

---

1. Realism
2. You don't Play-you Volunter
3. Interactive
4. Normandy
5. D-day

عملاً نمی‌تواند از خود دفاع کند و تنها راهی که برای نجات دارد زیر آب رفتن و روی آوردن به دور بعدی بازی است. بازیگر در حین رفتن به دور بعدی بازی، صحنه‌های سربازان زخمی، سربازان وحشت‌زده‌ای که نای حرکت کردن ندارند و اجسادی را که نقش بر زمین شده‌اند مشاهده می‌کند. البته بسیار بعید است که یکی از این همه گلوله‌های بی‌شماری که از فاصله‌ای دوردست به‌سوی بازیگر رایانه‌ای شلیک می‌شود وی را از پای درآورد. معمولاً سازندگان بازی به‌عمد مخاطب خود را در معرض این چنین سطوح بالای ناکامی و سرخوردگی قرار می‌دهند، چرا که جان سالم به در بردن در نظر وی فقط یک حسن تصادف و نوعی خوش‌شانسی به شمار می‌آید. این دقیقاً همان‌جایی است که «واقعیت‌نمایی واقعی»[1] رخت برمی‌بندد.

اکثر بازی‌های جنگی، هرچند ادعا می‌کنند که مبتنی‌بر واقعیت‌اند،[2] ولی تعاریف بسیار نامأنوسی از «واقعیت‌نمایی» ارائه می‌دهند. این وضعیت چندان هم نباید شگفت‌آور به‌نظر آید، چرا که هدف از طراحی و عرضه این بازی‌ها، رعایت منتها درجه واقعیت‌نمایی است که فقط می‌تواند خسته‌کننده، مایه دل‌زدگی و سرخوردگی، نفرت‌انگیز، یا آمیزه‌ای از این عوامل باشد و یا حتی به عوامل منفی‌تر منتهی شود. برای تبیین این موضوع، آوردن نقل قولی از تهیه‌کنندهٔ بازی «نشان افتخار: حمله متفقین» کفایت می‌کند. وی اظهار داشت: ما توجه خود را نه الزاماً بر واقعیت‌نمایی تمام‌عیار، بلکه بر موثق بودن صحنه‌ها معطوف می‌کنیم. ما می‌خواهیم بازی تا آنجا که امکان دارد جذاب و لذت‌بخش باشد و می‌کوشیم سرگرمی را قربانی «نمایش دقیق پرتاب موشک‌ها و واقعیت‌های عینی» نسازیم.

برای تمایزگذاری میان «واقعیت‌نمایی» و «واقعیت»، ضرورت دارد که برخی از جنبه‌های نبردهای واقعی و شبیه‌سازی شده بررسی شوند. در بازی‌های جنگی، مانند فیلم‌های سینمایی اکشن، نقش و جایگاه تسلیحات بسیار برجسته است. سازندگان بازی‌ها برای آنکه هنرپیشه‌های مجازی خود را واقعی جلوه دهند در وب‌سایت‌هایشان اعلام می‌کنند که در صحنه‌های بازی سلاح‌های تاریخی اصل را به نمایش می‌گذارند. امروزه، بازیگران رایانه‌ای می‌توانند انتظار داشته باشند که تسلیحات مختلف در بازی مانند

---

1. Real Realism
2. Realistic

تسلیحات واقعی به‌نظر خواهند رسید، چرا که در بازی‌های رایانه‌ای فعلی صداهای فشنگ‌گذاری تفنگ، مسلح کردن اسلحه و تیراندازی، نمونه‌برداری شده است. این تمایز میان بازی و واقعیت معمولاً با به‌کارگیری این تسلیحات آغاز می‌شود. اولاً، در بسیاری از بازی‌ها، بازیگر می‌تواند حجم قابل توجهی از تجهیزات انفرادی را با خود حمل کند. برای مثال، در بازی «نشان افتخار»، بازیگر می‌تواند یک تپانچه کمری، اسلحه برای تیراندازی در کمین، مسلسل، تفنگ خودکار (سلاح بسیار سنگینی که در جنگ جهانی دوم مورد استفاده قرار می‌گرفت) و یک بازوکا [1] (ضدتانک، به همراه بیش از ۱۲۰۰ گلوله در همهٔ کالیبرهای اسلحه) و تعداد زیادی نارنجک دستی با خود حمل کند؛ در نبرد واقعی، هیچ سربازی نمی‌تواند باری با این وزن را بر دوش بگیرد، ولی در بازی رایانه‌ای، سرباز در طول نبرد همیشه همه این اقلام را همراه خود دارد. بازی‌هایی از قبیل «عملیات نقطه انفجار» استثنا محسوب می‌شوند؛ چرا که در این بازی‌ها، بازیگر فقط یک سلاح ابتدایی و یک سلاح کمری با خود حمل می‌کند و تنها مقدار معقولی تجهیزات در اختیار دارد.

البته، این محدودیت در تجهیزات، کل فضای حاکم بر بازی را نیز تغییر می‌دهد: اگر سرباز تنها به یک تفنگ و شصت گلوله مجهز باشد، دیگر نمی‌تواند با یک گروهان از سربازان دشمن درگیر شود. اما در بازی‌های اکشن، شلیک هزاران گلوله در هر سطحی که باشد استثنا محسوب نمی‌شود. برای مثال، مجله *پلی‌استیشن پلنت* [2] در بررسی بازی «نشان افتخار: خط مقدم» نوشت: «بی‌شک، نشان افتخار» بهترین و واقعیت‌نمایانه‌ترین بازی جنگی‌ای است که شما می‌توانید خریداری کنید. فکر و ذهن شما به‌قدری مشغول کشیدن ماشه خواهد بود که متوجه گذشت زمان نخواهید شد. بفرمایید این هم از واقعیت‌نمایی. اما مهم‌ترین و اصلی‌ترین اقدام سربازان در جنگ همانا انتظار کشیدن (و تلاش برای زنده ماندن) است که اصلاً تجربهٔ هیجان‌انگیزی برای بازی کردن نیست».

روش به‌کار بردن این تسلیحات نیز اهمیت دارد. در بیشتر بازی‌هایی که ژانرشان «اولین تیرانداز» است، سلاح‌هایی که انتخاب شده است در بخش پایین صفحه نمایشگر نشان داده می‌شود و نقطه هدف‌گیری اسلحه نیز در وسط صفحه نمایشگر با هاشور

---

1. Bazooka
2. Polystation Planet

مشخص می‌گردد. در بسیاری از بازی‌ها، بازیگر سلاحش را شلیک می‌کند و در این میان حتی با تیراندازی‌های مکرر و متوالی، حمله‌ای دقیق علیه هدف مورد نظر انجام می‌گیرد. این تسلیحات، مانند آنچه در فیلم‌های سینمایی وسترن دیده می‌شود، نسنجیده طراحی شده‌اند، به‌طوری‌که لگد زدن تفنگ در اثر شلیک گلوله اصلاً در نظر گرفته نمی‌شود. اما بازی‌های واقعیت‌نمایانه‌تری از قبیل «عملیات نقطه انفجار» این خصوصیت را دارد: ممکن است طراحی تسلیحات و تجهیزات در این بازی‌ها نسنجیده باشد، اما اصابت گلوله‌ها به اشیا و پدیده‌های بی‌ربط، بسیار بعید است. بازیگر برای هدف‌گیری درست باید از مگسک اسلحه به هدف نگاه کند، در نتیجه، دید او نیز محدود می‌شود. بااین‌همه، نه تنها شلیک گلوله و لگد زدن اسلحه در اثر آن، بلکه حتی نفس کشیدن بازیگر را نیز باید در نظر گرفت؛ چرا که همین عوامل، وی را وادار می‌سازد تا لحظه درست و دقیق را برای کشیدن ماشه انتخاب کند. با وجود این، به‌هیچ‌وجه، این امر آموزش تمام‌عیار تیراندازی به‌شمار نمی‌آید؛ زیرا بیشتر اشتباهات تیراندازی در عالم واقع به نحوه استفاده از مگسک یا کشیدن بسیار سریع ماشه اسلحه مربوط می‌شود. فقط «میادین تیر» مجازی‌اند که مجال چنین آموزش‌های واقعیت‌نمایانه‌ای را فراهم می‌آورند. اما، گفتنی است که شرکت‌های تولیدکننده بازی‌های رایانه‌ای از قبیل بوهمیا اینتراکتیو[1] (شرکت تولیدکننده بازی «عملیات نقطه انفجار» از کشور چک) شبیه‌سازهای نظامی نیز عرضه می‌کنند. مسلماً، همگرایی[2] بازی‌های رایانه‌ای با برنامه‌های رایانه‌ای نظامی در آینده بیشتر از امروز خواهد شد.

صحبت کردن سربازان و حرکات و رفتار افراد، نزدیکی چندانی با آنچه که در این بازی‌ها به‌خوبی شبیه‌سازی شده است ندارند. معمولاً، هیچ کار مشکلی وجود ندارد و سربازان مجازی چه‌بسا ممکن است بی‌آنکه خسته شوند، مدام و بی‌وقفه بدوند. در بسیاری مواقع، به‌دلیل یک رویارویی طبیعی و برای تضمین سطوح بالای معقولیت بازی، فعالیت‌ها و حرکات و سکنات افراد نیز بسیار محدود می‌شود. تا حدودی عجیب و غریب است که یک سرباز نمی‌تواند بی‌آنکه بدنش را نشان دهد، به دوروبر خود نگاه

1. Bohemia Interactive
2. Convergence

کند؛ این موضوع در مورد بسیاری از تیراندازها در بازی‌های رایانه‌ای صدق می‌کند. همین‌که در بازی، حرکتی انجام گیرد، بسیاری از راه‌های «طبیعی» نیز بسته می‌شود ـ برای مثال، یک سرباز چه‌بسا فقط به‌علت آنکه اجازه ندارد، نمی‌تواند از موانع دفاعی عبور کند و از روی خندق‌ها بپرد. علاوه‌بر این، در بازی‌ها، جنگ همیشه اکشن است، ولی در واقعیت، اکثر زمانی که سربازان صرف می‌کنند، اگر کارهای ملال‌آوری از قبیل تمیز کردن اسلحه یا نگهبانی نباشد، انتظار کشیدن و معطل شدن و نیز کارهای تکراری انجام دادن است. این مسئله به‌ویژه در مورد بازی‌هایی که موضوع آنها جذب نیرو و سربازگیری است (مثل بازی رایانه‌ای «ارتش آمریکا»)[1] صدق می‌کند: ممکن است این بازی باعث شود که بازیگر برداشت غلطی از زندگی در ارتش به‌دست آورد، چرا که در این بازی اگر او در نهایت به خدمت سربازی می‌رود، به‌سرعت حالش خوب خواهد شد. مسئله جانبی جالبی که در این بازی می‌توان به آن اشاره کرد، رعایت «برابری نژادی»[2] است. «ارتش آمریکا» اولین بازی‌ای است که بازیگر می‌تواند هرکدام از رنگ‌های مختلف پوست را که پسند کرد و متناسب با زمینه تصویر (آسیایی، آفریقایی ـ آمریکایی، آمریکای لاتینی، یا قفقازی) تشخیص داد، انتخاب کند.

آنچه عجیب‌تر از محدودیت‌های فراروی بازیگر جلوه‌گر می‌شود، همانا رفتار دشمنان پرشماری است که بازیگر روبه‌روی خود می‌بیند: به‌نظر می‌رسد که دشمنان، مدت‌ها پیش کشته شده‌اند، زیرا پنهان شدن و پناه گرفتن یا تیراندازی کردن و درعین‌حال، خود را در معرض دید طرف مقابل قرار ندادن، در نزد بسیاری از دشمنان مجازی مهارت‌هایی آشکارا غیرممکن‌اند. اما این نکته را باید اضافه کرد که در طول چند سال گذشته، این نوع «حماقت‌های تصنعی»[3] حتی فراتر از آن چیزی است که در لفظ به این واژه اطلاق می‌کنیم. ازاین‌رو، به‌کارگیری مفرط «هوشمندی تصنعی» یکی از ضعف‌های اصلی این بازی‌ها به‌شمار می‌آید.

یکی از جنبه‌های بارز بازی‌های جنگی، به تصویر کشیدن جراحت‌ها و نیز کشته

---

1. America's Army
2. Racial Equality
3. Artificial Stupidity

شدن سربازان است. چهار روش متفاوت برای به تصویر کشیدن جراحت‌ها در بازی‌ها وجود دارد: روش اول اینکه هیچ جراحتی نشان داده نشود، برای مثال، در بازی «نشان افتخار» از این روش استفاده شد. ممکن است سربازان آهسته‌تر راه بروند یا بلنگند، اما حمام خون، زخم‌های عمیق، یا جراحت‌های وخیم اصلاً به نمایش درنمی‌آیند. جالب اینکه به‌نظر می‌رسد این رویکرد، یکی از رویکردهایی است که بیشتر بازیگران بدان علاقه‌مندند؛ زیرا آنها بازی نمی‌کنند که مجروح سازند، به قتل برسانند، یا از تماشای رنج بردن دیگران لذت ببرند و سرگرم شوند، بلکه بازی می‌کنند تا با ارتباط برقرار کردن و انجام کنش‌هایی هماهنگ با اعضای تیمشان در این مأموریت‌ها موفق گردند. بسیاری از بازیگرانی که نقش «ضدحمله»[1] را در بازی رایانه‌ای برعهده می‌گیرند، گزینه‌ای که خونریزی را به تصویر می‌کشد، خاموش می‌کنند. روش دوم، که در بازی رایانه‌ای «ارتش آمریکا: عملیات» به‌کار می‌رود، این است که اگر چنانچه تیری به سربازی اصابت کند، قطره‌های قرمز رنگی (مانند بازی پینت‌بال)[2] که روی یونیفورم او نقش بسته، به تصویر کشیده می‌شود. روش سوم، خشونت و درگیری و جراحت‌های سربازان را به شیوه‌ای کم‌وبیش واقعیت‌نمایانه نشان می‌دهد. در بازی «عملیات نقطه انفجار»، آن قسمت از یونیفورم سرباز که گلوله بدان اصابت کرده است به‌صورت مجازی آغشته به خون می‌گردد. خوشبختانه روش چهارم بسیار به‌ندرت مورد استفاده قرار می‌گیرد. برخی از بازی‌ها فقط جلوه‌های واقعیت‌نمایانه‌ای از صدماتی که بر سربازان وارد می‌شود، نمایش می‌دهند، اما درحقیقت، تجربه‌ای دهشتناک و خونین را به نمایش می‌گذارند و طبعاً نیتشان از اتخاذ این رویکرد باز در مورد خشونت، چیزی جز جذب مشتری نیست. در نتیجه، نه تنها صاحب‌نظران بلکه مخاطبان نیز چنین بازی‌هایی را به‌شدت مورد انتقاد قرار داده‌اند و هیچ وجهه‌ای در میان اکثر بازیگران رایانه‌ای ندارند، زیرا توجه و تمرکز این بازی‌ها نه بر تیراندازی علیه دست و پای اهداف یکدیگر، بلکه به خود بازی است. در این خصوص اگر کسی به طرف اهداف بی‌ربط تیراندازی کرد، برایشان هیچ فرقی نمی‌کند؛ زیرا به صدها اصولی که درزمینه پویایی‌نمایی وجود دارد، بی‌توجه‌اند. معمولاً،

---

1. Counterstrike

۲. پینت‌بال (Paint ball)؛ نوعی بازی است که در آن، افراد توپ‌هایی از رنگ را به طرف یکدیگر شلیک می‌کنند.

جراحت‌های «پاک»[1] بر فضای بیشتر بازی‌های رایانه‌ای حکم‌فرماست؛ هیچ کس نقص عضو پیدا نمی‌کند، دست و پای خود را از دست نمی‌دهد و زمین‌گیر هم نمی‌شود.

اما در میدان‌های نبرد، گلوله‌های توپ و بمب‌ها معمولاً بیشترین میزان تلفات را به بار می‌آورند و در بسیاری مواقع جراحت‌های عمیق و حادی را بر افراد وارد می‌سازند. بااین‌همه، در این بازی‌ها مانند فیلم‌های سینمایی جنگی، افراد نه قهرمانانه، اما به‌سرعت کشته می‌شوند. نه تنها به تصویر کشیدن جراحت‌ها، بلکه تأثیرات و معالجه آنها نیز ابعاد جالبی دارد. در بیشتر بازی‌ها، بازیگر می‌تواند بلافاصله سلامتی خود را به‌دست آورد یا با استفاده از «بسته‌های درمانی»[2] که در سراسر بازی می‌توان یافت، حتی خودش را مداوا کند. در فیلم‌های اکشن، کاملاً طبیعی است که در طی مأموریت واحد، ۱۵۰ گلوله یا بیشتر از آن به طرف هدف شلیک شود؛ مادامی‌که بسته‌های درمانی به‌اندازه کافی در دسترس است، هیچ مشکلی پیش نمی‌آید؛ البته، هیچ تأثیر بلندمدتی در کار نیست.

بازی‌هایی از قبیل «عملیات نقطه انفجار»، چنین مداواهایی را به نمایش نمی‌گذارند. اگر گلوله‌ای به بازیگر اصابت کند (بسته به موقعیتی که در آن تیر خورده است)، حوزه عمل او محدود می‌شود. مسئله دیگر اینکه هرچه دشمن درجه بالاتری داشته باشد، ضرباتی که می‌تواند وارد کند بیشتر است؛ این امر در عمل با عالم واقع مطابقت ندارد، چرا که یک افسر ستادی معمولاً در پوشش زرهی خود، چیزی بیش از یک سرباز پیاده نظام به تن نمی‌کند.

بعد از آنکه سطح سلامتی یک سرباز مجازی به صفر درصد می‌رسد، او می‌میرد. تا قبل از آن موقع، با وجود اینکه بازیگر به‌شدت صدمه دیده است، حرکات و سرعت وی در بسیاری مواقع محدود نمی‌شود. حتی اگر بازیگر فقط یک درصد توانایی‌اش را داشته باشد، می‌تواند بدود و جست‌وخیز کند. در بیشتر بازی‌ها، کشته‌شدگان به معنای واقعی کلمه می‌افتند و می‌میرند و به‌ویژه در بازی‌های اکشن، چند ثانیه بعد از آن نیز غیب می‌شوند. نمایش صحنه قدم زدن روی این تَل عظیم جنازه‌های سربازان کشته شده دشمن چه‌بسا احمقانه و مضحک است، چرا که در یک دور بازی تک‌نفره (که یک ربع یا

---

1. Clean Wounds
2. Health Packs

نیم ساعت طول می‌کشد)، کشتن صد سرباز دشمن یا بیشتر از آن تا اندازه‌ای زیاد است. البته، دراین‌میان، بزرگ‌ترین (و آشکارترین) اختلافی که با واقعیت دیده می‌شود، این است که همیشه امکان شروع مجدد و به عبارتی، ازسرگیری بازی نیز وجود دارد. مادامی‌که تمایزی آشکار میان عالم واقع و جهان مجازی وجود دارد، این وضعیت هیچ مشکلی را به‌وجود نمی‌آورد.

جالب آنکه، به اسارت گرفتن سربازان (یا نابود نکردن دشمن) در بیشتر بازی‌ها هدف نیست. بسیار به‌ندرت اتفاق می‌افتد که مأموریت‌ها در بازی‌ها امکان به اسارت گرفتن سربازان دشمن را در خود جای داده باشند. اما در اکثر بازی‌ها، سربازان دشمن نه آزاد می‌شوند و نه فرار می‌کنند. حتی اگر تعداد سربازان دشمن نیز بیشتر باشد، تا زمانی که آخرین سرباز دشمن کشته نشده است، دشمن به نبرد ادامه می‌دهد. این رویکرد «جنگ تمام‌عیار»[1] که مبتنی‌بر کشتن همه افراد طرف مقابل می‌باشد، چه‌بسا ممکن است شباهتی با حمام خون که در نبردهای واقعی روی می‌دهد داشته باشد؛ نبود تسلیم و زندانی جنگی به‌طور قطع وضعیتی نامأنوس و عجیب و غریب است. (البته یک استثنا وجود دارد: در نبردهای ملاطفت‌آمیز چه‌بسا ممکن است بازیگر ناگزیر باشد زندانی‌های جنگی را آزاد کند). هیچ راهی برای مذاکره وجود ندارد، هیچ احتمالی غیر از کشتن طرف مقابل را نمی‌توان در نظر گرفت: هرچه بیشتر بهتر. در بسیاری از بازی‌ها برای به اتمام رساندن یک سطحی از بازی یا دریافت یک نشان، حتی باید همه یگان‌های نظامی دشمن نابود شوند.

مانند فیلم‌های سینمایی جنگی، غیرنظامیان در بیشتر بازی‌های جنگی در صحنه‌ها ظاهر نمی‌شوند. اگر غیرنظامیان به تصویر کشیده می‌شوند، چه‌بسا آنها مردم عادی نیستند که در مناطق جنگی سکونت دارند، بلکه دانشمندان نازی دیوانه‌ای می‌باشند که در هر صورت قرار است کشته شوند. اگر آن مسائلی که در عصر حاضر در رابطه با تلفات غیرنظامیان وجود دارد، یا شمار بالای غیرنظامیانی که از آغاز قرن بیستم تاکنون در همه منازعات کشته شده‌اند به یاد آوریم، این وضعیت، در مورد سناریوهای مربوط به جنگ شهری حتی غیرعادی‌تر و شگفت‌آورتر است. برخی از بازی‌ها می‌کوشند

---

1. Total War

توجیهی ارائه دهند؛ برای مثال، در یکی از مأموریت‌های بازی «نشان افتخار: حمله متفقین» که در یکی از شهرهای نیمه‌مخروبه فرانسه به اجرا درمی‌آید، راهنمای بازی می‌گوید که «همه غیرنظامیان پیش از آغاز نبرد از شهر تخلیه شده‌اند». البته، وقتی هیچ غیرنظامی‌ای وجود ندارد، اصلاً هیچ نیازی هم نیست که از کشتن غیرعمدی آنها نگران باشیم یا حق روابط نظامیان و غیرنظامیان را در طول عملیات نظامی در نظر بگیریم.

اصطلاح «خسارات و تلفات جانبی» مدت‌هاست که موضوعی بحث‌برانگیز و داغ در عرصه بازی‌های رایانه‌ای بوده است و نفوذ و تأثیرگذاری رسانه‌ها بر بروز و روند جنگ‌ها (برای مثال، در مورد جلب حمایت مردمی از عملیات جنگی) بر همگان آشکار است. اما در بازی‌های جنگی، این مسائل اصلاً موضوعیت ندارند. البته استثنائاتی هم وجود دارد؛ برای مثال، می‌توان بازی «منطقه منازعه» را نام برد؛ اگر بازیگر طرف خیر[1] منازعه (سازمانی شبیه سازمان ملل) را انتخاب کند، بازیگر نه تنها باید به غیرنظامیان حمله نکند، بلکه وظیفه دارد از آنها محافظت کند، آنها را از منطقه جنگی خارج سازد و از وارد کردن خسارت‌های جانبی به آنها بپرهیزد. اما اگر بازیگر، طرف شر[2] منازعه (مجموعه‌ای از دولت‌های یاغی و گروه‌های مسلح بین‌المللی غیردولتی) را انتخاب کند، می‌تواند برای پیشبرد اهداف تبلیغاتی خود از رسانه‌ها نیز بهره‌برداری کند.

عملیات لجستیکی، که بخش چشمگیری از هر فعالیت نظامی را دربرمی‌گیرد، هم ازلحاظ اهمیت و هم ازلحاظ هزینه به‌ندرت به عاملی تعیین‌کننده در بازی‌های جنگی تبدیل می‌شوند. در بسیاری از بازی‌های استراتژی‌محور[3] یگان‌های جدید را به‌آسانی می‌توان سازمان‌دهی یا حتی ایجاد کرد. بازی‌های استراتژی‌محور هم‌زمان، تا حد زیادی، می‌کوشند جنبه‌های واقعیت‌نمایانه‌ای از امور لجستیکی را نیز به نمایش گذارند. بنابراین برای مثال ایجاد فوری نیروهای اضافی را نمایش می‌دهند و بازی‌ها را به این سمت سوق می‌دهند که به نمایش تدارکات نظامی نیز بپردازند. اما تانک‌ها و سایر تسلیحات در بیشتر مواقع سوخت و تجهیزاتشان را تمام نمی‌کنند و حتی اگر این جنبه نیز اصلاً

---

1. Good Side
2. Evil Side
3. Strategy Game

در نظر گرفته نشود، فقط یک مجازات در ازای آن پیش‌بینی می‌شود.

«دقت» درزمینه سلاح‌های کوچک و سیستم‌های تسلیحاتی عظیم نیز مطرح است. فقط شبیه‌سازی‌هایی که مهارت بیشتری می‌طلبند، احتمال اختلال در آنها وجود دارد. در بسیاری موارد، موشکی که سیستم ردیابی در آن وجود دارد، همیشه به هدف مورد نظر خود اصابت می‌کند. در برخی از بازی‌های تیمی، برای مثال در بازی «کشمکش: طوفان صحرا»، در مورد تعداد اصابت موشک به سربازان خودی اغراق می‌شود و تجهیزات دشمن را می‌توان به‌آسانی نابود کرد. به‌نحو مستدل می‌توان گفت اگر استفاده از تجهیزات هدایت‌شونده و دقیق تاکنون در جنگ‌های واقعی نتیجه مثبتی داشته است، گزارش‌ها در مورد استفاده موفقیت‌آمیز از چنین مهارتی چه‌بسا باورپذیرتر خواهد بود.

۵-۲ بازی‌ها و شبیه‌سازی‌های نظامی حرفه‌ای

همگرایی میان بازی‌های تجاری و شبیه‌سازی‌های حرفه‌ای نظامی همچنان تداوم خواهد یافت. ارتش آمریکا بازی «ارتش آمریکا: عملیات‌ها» را به‌عنوان برنامه‌ای برای جذب نیرو در ارتش تولید کرده است. در عرض چند هفتهٔ اول انتشار، بیش از هفتصد هزار نفر از این بازی رایگان در اینترنت استفاده کردند و البته چندین میلیون سی‌دی نیز توزیع شد. این بازی در عرض چند ماه، به یکی از موفق‌ترین بازی‌های موجود در اینترنت مبدل شده بود. شاید علت استقبال، این است که بازی، رایگان بوده و علاوه‌بر این، تصاویر و نوع بازی جالب و قوی داشته است. در حدود ۲۵ درصد همه درخواست‌ها برای کسب اطلاعات درزمینه ورود به ارتش در حال حاضر با وب‌سایت «ارتش آمریکا» دریافت می‌شود. برخلاف باور بسیاری از مأموران جذب نیرو (که قبل از استقبال مخاطبین، این بازی را حقّه‌ای بیش نمی‌دانستند و آن را نکوهش می‌کردند)، این استقبال، موفقیتی عظیم برای دولت آمریکا محسوب می‌شود. وانگهی، متخصصان ساخت بازی‌های رایانه‌ای از شرکت مطالعات عالم‌گیر،[1] دو بازی دیگر را نیز برای ارتش آمریکا در دست تولید دارند. یکی از آنها به نام «رزمنده تمام‌عیار»،[2] که بازی جنگی در مورد عملیات نظامی

1. Pandemic Studies
2. Full Spectrum Warrior

تاکتیکی در ناحیه شهری است، این بازی نه تنها به‌عنوان یک بازی تجاری منتشر خواهد شد، بلکه در نسخه‌ای مجزا با اندکی جرح و تعدیل، برای آموزش سربازان پیاده‌نظام مورد استفاده قرار خواهد گرفت.

کشورهای دیگر نیز همین مسیر را می‌پیمایند. برای مثال، ارتش بریتانیا بازی «نیمه جان» [1] را به‌گونه‌ای بازنگری کرده است که برای آموزش نظامیان به‌کار آید. تولیدکنندگان چنین بازی‌هایی کاربران خود را تشویق می‌کنند که سناریوهای مورد نظر خودشان را طراحی نمایند. این رویکرد، برای شرکت‌هایی که قصد دارند بازی‌های تولیدیشان را بازنگری کنند، تا به حال ارزان‌ترین روش بوده است. در این صورت، هزینه تنظیم بازی‌ها در مرحله بازنگری کمتر از هشتاد هزار پوند بود. این مبلغ تنها بخش ناچیزی از هزینه‌هایی است که برای تولید یک بازی جدید صرف می‌شود. هرچند رسانه‌ها در بسیاری مواقع، تصویری منفی از این‌گونه بازی ها ارائه می‌دهند و آنها را «آموزگاران قاتل» معرفی می کنند، ولی باید خاطرنشان ساخت که نظامیان از چنین بازی‌هایی برای آموزش اموری از قبیل جنگیدن، افزایش روحیه تجاوزگری، یا حتی کشتن افراد دشمن به‌دست سربازان استفاده نمی‌کنند. بلکه هدف اصلی از این رویکرد، آموزش مهارت‌های ارتباطی در درون دسته‌های ارتش، تقویت کار گروهی، ارتقای سطح آموزش رویه‌ها و آیین‌نامه‌های نظامی (برای مثال، نحوه نظافت کردن ساختمان) است. اما، در واقعیت امر، بسیار بعید است که چنین عملیاتی به این جهت هدایت شود، چرا که خطر خسارت‌ها و جراحت‌هایی که خود بازیگر در «عملیات نظامی در ناحیه شهری» در اثر آتش خودی می‌بیند، بسیار بالاست.

علاقه نظامیان به طراحی شبیه‌سازی‌های بهتر برای آموزش سربازان، به‌ویژه در ارتش ایالات متحده بالاست. ازاین‌گذشته، بازی‌های رایانه‌ای به‌عنوان بخشی از محیط آموزشی به‌کار گرفته شده‌اند. در حال حاضر، کنفرانس‌هایی از قبیل اجلاس بازی‌های جدّی [2] برگزار می شود که درباره بازی‌هایی که اهدافی جدی را دنبال می‌کنند بحث و تبادل نظر می‌شود. هرچند بسیاری از صنایع و سازمان‌های درمانی به این حوزه علاقه نشان داده‌اند ولی حرکت اصلی و عمده در این زمینه از جانب ارتش است. بازی‌های رایانه‌ای

---

1. Half Life
2. Serious Games Summit

مزایای متعدد و متنوعی دارند. اولاً، آنها به‌آسانی نصب می‌شوند؛ دستورالعمل‌ها و آموزش‌های لازم درزمینه نحوه استفاده از آنها را می‌توان در هر جایی بدون نیاز به تجهیزات اضافی انجام داد. ثانیاً مأموریت‌های اضافی برای این بازی‌ها را به‌آسانی می‌توان توسعه داد. این گزینه راهکاری بسیار خوب برای تغییر دادن فضاهای بازی‌ها به‌شمار می‌آید. ثالثاً، بازی‌ها برای جذب نیرو در آینده نیز جذاب تلقی می‌شوند. همان‌گونه که دکتر مایکل ماکدنیا[1] رئیس دانشمندان شاغل در مرکز فرماندهی شبیه‌سازی، آموزش و ابزارسازی[2] ارتش آمریکا(۴) نیز گفت، اعضای جدید ارتش می‌خواهند شور و هیجانی همراه باهمدلی داشته باشند و ما می‌توانیم نوعی هیجان همدلانه به آنها اعطا کنیم.(۵) علاوه‌بر این، بازی‌های رایانه‌ای می‌توانند مهارت های ارتباطی و همکاری‌جویی، آگاهی شغلی و حتی آگاهی فرهنگی را نیز آموزش دهند ـ این مهارت‌ها به‌صورت خاص برای نبرد در مناطق شهری، یا به‌طورکلی برای مأموریت‌های حفظ صلح و اجرای صلح ضروری است.

با توجه به تحولاتی که در بالا گفته شد، بازی‌های رایانه‌ای به‌طورقطع آینده‌ای روشن در ارتش خواهند داشت. می توان تصور کرد که انسان در آینده می تواند هواپیماهای بدون سرنشین را در هر جای دنیا که باشد کنترل کند، اما این وسایل در حال حاضر در دنیای مجازی رایانه‌ها وجود دارند. نرم‌افزارها و سخت‌افزارهای هدایت این پرنده‌ها به شبیه‌سازی‌های رایانه‌ای شباهت دارند. درست همین الان، در حدود ده سرباز برای کنترل یک پرنده شکاری مورد نیاز است. این وضعیت قرار است در آینده‌ای نزدیک به یک عملگر[3] در ازای پنج پرنده تقلیل یابد. برای آنکه این شرایط محقق شود، بهره‌مندی از تجربه بازی‌های رایانه‌ای به‌طورقطع سودمند است. البته، جنبه‌های منفی در این حوزه وجود دارد. هرچند نسل‌های حال و آینده جذب نیرو برای خدمت در ارتش ممکن است دانسته‌های بسیاری در مورد فناوری اطلاعات و بازی‌های رایانه‌ای داشته باشند، اما روی‌هم‌رفته، آنها فاقد توانایی‌های فیزیکی‌اند. نیروهای مسلح هیچ کاربردی درزمینه پرورش سیب‌زمینی ندارند. ازاین‌گذشته، این خطر وجود دارد که تجربه‌های موفق بازی‌های رایانه‌ای به غلط به حوزه اقدامات نظامی واقعی تسری داده شوند و به این موضوع

---

1. Michael Macedonia
2. Simulation and Training, Instrumentation, Command Centre (STRICDM)
3. Operator

مهم توجه نشود که واقعیت و مجازیت دو مجموعه متفاوت‌اند. هوشمندی تصنعی دشمن فقط می‌تواند تصویری ذهنی[1] در مورد اقدامات احتمالی دشمنان (که برای غلبه بر محدودیت‌های فراروی خود ـ برای مثال محدودیت‌های وسایل سنگین زرهی و داده‌های فناوری‌های نوین ـ می‌کوشند خلاقیت زیادی به خرج دهند) ارائه دهد.

براساس بسیاری از گزارش‌های رسانه‌ها در مورد بازی‌های رایانه‌ای خشونت‌آمیز، مسئله دیگری وجود دارد که نظامیان می‌توانند از آن سوءاستفاده کنند: این بازی‌ها، به‌ویژه بازی‌های جنگی واقعیت‌نمایانه، به شکل «آموزگاران قاتلی»[2] درمی‌آیند که برای مثال، قلع‌وقمع هزاران دشمن مجازی و اعطای امتیاز در ازای آن را به امری عادی تبدیل می‌کنند و این رویه را در جریان بازی آموزش می‌دهند و با این کار، آستانه قتل انسان‌ها را پایین می‌آورند.

این استدلال، منطقی و قابل قبول به‌نظر می‌رسد، زیرا محیط و فضای این بازی‌ها یا جنگ واقعیت‌نمایانه است یا عملیات‌های مبارزه با تروریسم؛ و به‌نظر می‌رسد استفاده نیروهای مسلح از این بازی‌ها کاربرد آنها را توجیه و تأیید می‌کند. اما باید در نظر داشت که واقعیت، چیزی متفاوت است. اولاً، نیروهای مسلح در سراسر جهان ابزارهای آزمون شده‌تر و به‌مراتب بهتری را برای تقلیل دادن آستانه اقدام سربازانی که در یک محیط جنگی به‌سر می‌برند در اختیار دارند؛ برای مثال، آموزش‌هایی در مورد جنگ‌های تن‌به‌تن و نحوه استفاده از سرنیزه به سربازان ارائه می‌دهند. ثانیاً، نیروهای مسلح نه برای آموزش تیراندازی یا حتی تعلیم کشتن، بلکه برای آموزش نحوه تعامل و ارتباطات، همکاری و آگاهی از وضعیت عمومی نظامیان در هنگام جنگ و نیز سایر مهارت‌هایی که عمدتاً کاربردی دوگانه دارند از این بازی ها استفاده می‌کنند. حرکت دادن نشانگر روی صفحه نمایشگر رایانه با استفاده از یک ماوس[3] و شلیک اسلحه مجازی با فشار ماوس با هدف‌گیری و شلیک سلاح واقعی کاملاً فرق دارد. این تفاوت نه تنها ازنظر فنی بلکه ازلحاظ زمان دقیق شلیک گلوله به طرف هدف نیز (به‌ویژه اگر هدف، انسان باشد) دیده می‌شود.(۶) ثالثاً، و مهم‌تر از همه اینکه، براساس مطالعات بی‌شماری که در مورد رفتار انسان انجام گرفته است، بازیگران در همه دوره‌ها می‌توانند بین واقعیت های واقعی و مجازی تمایز قائل شوند (البته استثنا هم وجود دارد و آن در مورد

---

1. Idea
2. Killer Trainers
3. Mouse

افرادی است که اختلالات شخصیتی حادی دارند). مادامی‌که بازیگران با صفحه‌های نمایشگر و ابزارهای میانجی‌ای از قبیل صفحه کلید و ماوس با واقعیت مجازی تعامل دارند، این وضعیت همچنان حکم‌فرما خواهد بود. وقتی پیوند ذهنی دقیق (و تعامل مستقیم میان مغز انسان و رایانه) طراحی شود، این فصل نیز به‌ناچار به‌گونه‌ای دیگر نگارش خواهد یافت. اما تا امروز، مشخص و آشکار است که فقط با انجام بازی‌های رایانه‌ای نمی‌توان کُشتن را آموزش داد.

۶-۲ نتیجه‌گیری

به‌طورکلی، بیشتر بازی‌های جنگی رایانه‌ای، به‌رغم جنبه‌های صوتی ـ تصویری حیرت‌انگیزی که دارند، کاملاً غیرواقعیت‌نمایانه‌اند. جنبه‌های تصویری این بازی‌ها به‌طورقطع هر روز بهبود خواهند یافت و به‌زودی کیفیت تصاویر رایانه‌های خانگی به‌گونه‌ای خواهد شد که گویی این تصاویر زنده به‌نظر می‌رسند. گرچه بازی‌هایی از قبیل «عملیات نقطه انفجار»، «ارتش آمریکا: عملیات‌ها» و «رزمنده تمام‌عیار» ثابت می‌کنند که تولید بازی‌های جنگی جذاب و (به‌نسبت) واقعیت‌نمایانه امکان‌پذیر است، ولی باید خاطرنشان ساخت که پیشرفت‌های بیشتر در عرصه واقعیت‌نمایی ممکن است نامطلوب باشند، زیرا این پیشرفت‌ها چه‌بسا باعث می‌شوند که بازی‌ها برای بازیگرانی که به دنبال سرگرمی می‌باشند، آشکارا پیچیده، ملال‌آور و مایه دلزدگی شوند. وانگهی، اکثریت قاطع بازیگران نیز مایل نیستند تصویری واقعیت‌نمایانه از خشونت، جراحت و قتل را مشاهده کنند. بنابراین، حتی اگر سیستم‌های برنامه تصویری در آینده را در نظر بگیریم، هرگونه تجربه مجازی درباره جنگ در بازی‌های رایانه‌ای تجربه‌ای بسیار محدود خواهد بود. این وضعیت، با قصد و آگاهی بوده است و شگفت‌آور هم نیست؛ زیرا هدف بازی در نهایت تفریح و سرگرمی است.

صنعت سرگرمی خاطره‌هایی را که شما تا ابد برای خود ثبت می‌کنید خلق می‌کند، ولی ما (نظامیان) می‌خواهیم خاطره‌هایی خلق کنیم که شما آنها را فراموش کنید و درعین‌حال، از آن خاطره‌ها چیزهایی می‌آموزید.[۷] اما بااین‌حال، این سؤال طرح می‌شود که تا چه سطحی می‌توان یک فعالیت ذاتاً خشونت‌آمیز را سرگرمی تلقی کرد؟ اولاً، باید به خاطر داشت که اگرچه گزارش‌های رسانه‌ای تصاویر خاص خود را در مورد بازی‌های رایانه‌ای ارائه می‌کنند؛ ولی اکثر بازی‌های رایانه‌ای را بازی‌های خشونت‌بار یا حتی جنگی تشکیل نمی‌دهند. ثانیاً،

جنگ همیشه یکی از فعالیت‌های محوری آدمیان بوده است که جاذبه نیرومند خاص خودش را دارد ـ و البته هنوز نیز همچنان این‌گونه است. همان‌طور که در سایر اشکال رسانه‌ها جنگ همواره موضوع مهمی بوده است، این پدیده همچنان در بازی‌های رایانه‌ای نقش مهمی ایفا خواهد کرد.

در حال حاضر، به‌خصوص به دنبال وقوع حوادثی از قبیل قتل دانش‌آموزان در دبیرستانی واقع در کلمبیا (۱۹۹۹) بازی‌هایی از قبیل ضدحمله[1] همواره «آموزگاران قاتل» توصیف می‌شوند، زیرا نظامیان از نسخه‌های جرح و تعدیل‌یافته بازی‌های جنگی تجاری برای اهداف آموزشی خودشان استفاده می‌کنند. بسیاری از افراد تصور می‌کنند اگر نظامیان به‌عنوان کسانی که کار ویژه و اصلی‌شان کشتن است، از چنین بازی‌هایی استفاده می‌کنند، پس این‌گونه بازی‌ها نباید بر آنها بی‌تأثیر باشد؛ زیرا این بازی‌ها یا آستانه اقدام انسان درزمینه کشتن هم‌نوع خود را با فرایند تبدیل آن به یک عادت و روال عادی[2] تقلیل می‌دهد و یا فقط مهارت‌های هدف‌گیری و تیراندازی سربازان را تقویت می‌کند. در این خصوص، داو گراسمن،[3] روانشناس سابق نظامیان آمریکایی به بازی‌های ویدئویی که از مدل‌های ماکتی تسلیحات در صحنه‌های بازی استفاده می‌کنند حمله می‌کند. وی استدلال می‌کند که فرایند تبدیل اقدامات نظامی به یک عادت و روال عادی در حال رخ دادن است و بازیگران بازی‌های خشونت‌بار در عالم واقع ـ اگر جان هم‌نوع خود را نیز نگیرند ـ در قیاس با سایر افراد، تمایل بیشتری برای انجام رفتار خشونت‌بار از خود نشان می‌دهند. اما باید در نظر داشت که همه این قاتلان جوان، هم به سلاح‌های واقعی دسترسی دارند و هم آموزش‌هایی را درزمینه نحوه استفاده از آنها دریافت کرده‌اند. علاوه‌بر این، هرچند بعضی از نیروهای مسلح از این بازی‌های رایانه‌ای تجاری برای اهداف آموزشی استفاده می‌کنند، اما هدف آنها از به‌کارگیری این بازی‌ها، نه کاهش آستانه انجام قتل بوده است (نظامیان ابزارهای به‌مراتب بهتری را برای انجام قتل در اختیار دارند)، نه تقویت مهارت‌هایی غیر از ارتباط، همکاری و روحیه تیمی. همه این مهارت‌ها آشکارا کاربردهای دوگانه‌ای دارند و فعالیت‌هایی مثبت برای زندگی غیرنظامیان به‌شمار می‌آیند.

---

1. Counterstrike
2. Habitualisation
3. Dave Grossman

با توجه به تداوم و سرعت بالای پیشرفت فناوری، توسعه بازی‌های سرگرمی در آینده را آشکارا می‌توان پیش‌بینی و تصور کرد. هم بازی هولودک[1] و هم پیوند ذهنی[2] (که امکان تصویرپردازی و برانگیختن احساسات را به طور مستقیم در درون مغز فراهم می‌نماید) هنوز پدیده‌هایی علمی ـ تخیلی‌اند. اما ازآنجاکه هم سرگرمی و هم جنگ موضوعاتی است که بازارهای وسیعی را قبضه می‌کنند، ما کاربرد آنها را در تمام مدت زندگی‌مان به‌خوبی مشاهده می‌کنیم. به‌علاوه، تأثیر احتمالی بازی‌های رایانه‌ای بر ادراک رویدادهای گذشته و حال را با رسانه‌های جدید (از جمله امکان کپی‌برداری و جعل کردن واقعیت) نباید دست‌کم گرفت. نشان افتخار می‌تواند واقعیت رویدادها را برای نسل جوان و نیز نسل‌های آینده ـ بازی‌هایی از قبیل میدان نبرد ۱۹۴۲ ـ نشان دهد. این بازی‌ها بسیار نافذ به‌نظر می‌رسند. سطح بالای واقعیت‌نمایی در این بازی ها را می‌توان به عنوان دلیلی بر اثبات کیفیت بالای آنها معرفی و تبلیغ کرد. ازاین‌رو، مسئولیت تولیدکنندگان محصولات رسانه‌ای چه‌بسا در آینده افزایش خواهد یافت.

بااین‌همه، نباید از بازی‌های رایانه‌ای انتظار داشت که تبیین‌های کاملی را درزمینه علل جنگ‌ها، پیشینه جامعه‌شناختی و تاریخی جنگ‌ها و انگیزه‌های قهرمانان اصلی جنگ‌ها در اختیار کاربران‌شان قرار دهند. این نبود اطلاعات واقعی، ارائهٔ راه‌حل‌های (نظامی) ساده و تمایزهای آشکار میان خیر و شر، کمتر به دلیل گرایش مرسوم بازی‌ها به ساده‌سازی امور است؛ علت اصلی این وضعیت، بیش از هرچیز، منبعث از واقعیت‌های سیاسی است. شعار تبلیغاتی برای ترویج خرید بازی استراتژی‌محور «بلیتزریگ» ـ که در مورد جنگ جهانی دوم است ـ دلیل این وضعیت را به‌خوبی نشان می‌دهد: «به بازی جنگی روی آورید، اما نجنگید». حتی اگر جنگ واقعی در معنای دقیق کلمه به‌عنوان یک فعالیت عادی (یعنی فراتر از سطوح سیاست های معاصر) یا به‌عنوان سرگرمی تلقی نشود، باز هم حقیقت به‌طورقطع به ارزشی بسیار گران‌بها مبدل خواهد شد. تشخیص و تفکیک واقعیت از مجازیت در آینده‌ای نه‌چندان دور، یکی از ابعاد مهم زندگی خواهد شد.

---

1. Holodeck
2. Mind Link

پی‌نوشت‌ها

۱. جالب است خاطرنشان سازیم که تولیدکنندگان بازی‌های رایانه‌ای برنامه‌های شبیه‌سازی را برای ارتش تولید می‌کنند.

۲. به قول یکی از آگهی‌های بازرگانی درزمینه این بازی‌ها «شما به بغداد بازمی‌گردید تا جنگی را که جرج بوش پیش از موعد مقرر متوقف ساخت تمام کنید. شما جنگنده "F-16CBlock 50" (یک هواپیمای جنگنده چندمنظوره) را که به تمامی جنگ‌افزارهای مورد نیاز برای انجام امور جنگی مجهز است، هدایت می‌کنید.

۳. آلمان قوانین نسبتاً سختی در مورد «به تصویر کشیدن خشونت در رسانه‌ها» دارد. بازی‌های رایانه‌ای برای آنکه در بازار عرضه شوند باید به تأیید کمیته‌ای رسمی که دولت تشکیل داده است، برسند. ازسوی‌دیگر، حتی اگر محتوای این بازی‌ها برای کودکان طراحی شده باشد و نسبتاً بی‌ضرر هم باشد، باز هم محصولاتی مختص بزرگسالان به‌شمار می‌آیند. اگر بازی‌هایی از قبیل مجموعه «زلزله» محتوای اصلی خود را بر محوریت خشونت قرار دهد، در لیست سیاه قرار می‌گیرند. تبلیغات بازرگانی چنین بازی‌هایی نباید در رسانه‌ها پخش شود و درصورت اخذ مجوز، تنها به بزرگسالان فروخته می‌شود. بسیاری از بازی‌کنندگان در اولین سال‌های عرضه بازی‌های رایانه‌ای این شاخص را مهر تأیید متناقضی می‌دانستند، اما باید اذعان کرد که ممنوعیت پخش تبلیغات بازرگانی یک بازی رایانه‌ای، در جهان امروز که هزینه تولید کالا در آن بالا و رقابت تولیدکنندگان بسیار شدید است، جایگاه آن را در بازار عرضه این‌گونه محصولات در معرض آسیب جدی قرار می‌دهد. اگر یک بازی رایانه‌ای نمادهای نازی‌ها را به تصویر بکشد یا از آرمان‌های نازیسم تمجید کند، تولید و نمایش آن به‌کلی ممنوع می‌شود و اصلاً نمی‌توان آن را توزیع کرد.

4. US Army Simulation, Training and Instrumentation Commond (STRICOM).

5. Conference presentation, Defence simulation and Training, London, 7 November, 2002.

۶. براساس پژوهشی که ارتش آمریکا در طول جنگ جهانی دوم انجام داد، ۲۵ درصد از سربازان آمریکایی در این جنگ، حتی در موقعیت‌های پدافندی به طرف دشمن به‌طور مستقیم آتش گشوده بودند، این در حالی است که بیشتر آنها پیش از جنگ، نه تیراندازی کرده بودند و نه به طرف دشمن آتش گشوده بودند. در نتیجه، اقداماتی برای کاهش آستانه بالای کشتن انجام گرفت و آموزش‌های بنیادین در این زمینه اصلاح شد.

7. Dr. M. Macedonia, Conference Presentation, Defence Simulation and Training, London, 7 November 2002.

منابع و مآخذ

Anderson, C.A and K.E. Dill (2000), Video Games and Aggressive Thoughts, Feelings, and Behaviour in the Laboratory and in life, *Journal of Personality and Social Psycology,* 78 (4). Available at http://www.apa. Org/ journals/ psp/psp 784772.html.

Albrecht, H. Blut und Spiele, Die Zeit, 19/2002. Available at http://www.zeit.de /2002 /19/Politik/print _200219_computerspiele.html.

Büttner, C., (1995). Zum Verhältnis von phantasierter zu Realer Gewalt, Available at http://www.bpb.de/snp/referate/buettner.htm.

Demaria, R, and J.I. Wilson, (2000). High Score! The Illustrated History of Electronic Games Berkeley, CA: McGraw-Hill/ Osborne.

Der Derian, J., (2001), Virtuous War: Mapping the Military-Industrial-Media-Entertainment Network, Boulder, CO: Westview Press.

Eng. P., (2002). 'A Play for Bettrer Soldier-The Rise of Computer Games to Recruit and Train US Soldiers', abcNews.com, Available at http://abcnews.go.com/ sections/scitech/DailyNews/wargames020821.html.

Fritz, J. and W. Fehr, (1996). 'Computerspiele zwischen Faszination und Gewalt', Available at http/www.bpb.de/snp/referate/fritzst8.htm.

____, (1997). 'Gewalt. Aggression und Krieg-Bestimmende Spielthematiken in Computerspielen', in J, Fritz and W. Fehr, *Handbuch Medien: Computerspiele-Theorie, Forschung, Praxis, Bonn: Bundeszentrale Für Politische Bildung.*

Gieselmann, H., (2002). Der Virtuelle Krieg-Zwishen Schein und Wirlichkeit im Computerspiel, Hannover: Offizin.

____, (2002). 'Spiel mit dem Terror', *Heise News,* Available at http://www.heise, de/newsticker/data,hag-2008.02.000.

____, (2003). 'Spielplatz Zweiter Weltkrieg', c't, No. 7.

____, (2003). 'Braune Minderheit', c't, No. 8.

Grossman, Lt Col. D., (1996), On Killing: The Psychological Cost of Learning to Kill in War and Society, Boston: Little Brown & Co.

____, (2002). Stop Teaching our Kids to Kill, Boston: Little, Brown & Co, 1999.

Holert, T. and M. Terkessidis, (2002). Entsichert-Krieg als Massenkultur im 21. Jahrhundert, Cologne: Kiepenheuer & Witsch.

Leiner, M.K., (1999). Schlachtfelder der Elektronischen Wüste-Schwarzkof, Schwarzenegger, Black Magic Johnson, Berlin: Merve.

Mertens, M. and T.O. Mebner, (2002). Wir waren Space Invaders-Geschichten vom Computer spielen, Frankfurt am Main: Eichborn.

Meves, H., (2002). 'Das falsche Spiel mit der Gewalt-Computerspiele und die Gewalt in der Gesellschaft', Telepolis, Available at: http://www.telepolis.de/deutsch/special/game/12973/1.html.

National Reserch Council and et. al. (ed.), (1997). Modeling and Simulation: Linking Entertainment and Defense, Washington, DC: National Academy Press.

Osunsami, S., (2002). 'Simulated Sniping-US Army Recruits Teens with Internet Game', *ABCNews*, Available at:http://abcnews.go.com/ sections/ wnt/ DailyNews/ army_game021031.html.

Poole, S., (2000). Trigger Happy: The Inner Life of Videogames, London: Fourth Estate.

Rötzer, F., (2000). 'üben für den Krieg im Irak-Wartainment: Computerspiele für den Krieg und zur Anwerbung', Telepolis, Available at:http://www.telepolis.de /deutsch /special /game/13367/1.html.

Streibl, R.E., (1996). 'Krieg im Computerspiel', Available at: http://www.bpb.de/snp / referate/streib12.htm.

Streibl, R.E., (1996). 'Spielend zum Sieg!,' Available at: http:www.bpb.de/snp/ referate/ stteibl2.htm.

Thompson, C., (2002). Violence and the Political Life of Videogames', in L. King (ed), Game on: The History and Culture of Videogames, Exhibition Catalogue, London: Laurence King.

Villanueva, Lt Col. F. and Maj. A. Huber, (2002). 'Out of Box-Usnig COTS Products to Build Collective Skills', Training and Simulation, June/july.

Willmann, T., (2002). 'Death's a Game', Telepolis, Available at http://www.telepolis.de/deutsch/kolumnen/wil/12679/1.html.

____, (2002). 'Ganz anders als Krieg sollte ein gutes Spiel Immer Spaß machen', Telepolis, Available at http://www.telepolis.de/deutsch/special/game/12928 /1.html.

Woznicki, K., (2002). 'Krieg als Massenkultur', Telepolis, Available at http://www.telepolis.de/deutsch/inhalt/co/13059/1.html.

Wright, K., (2000). 'Does Media cause Violent Behaviour? A Look at the Research', womengamers.com, Available at:http://www.womengamers.com/ articles/gameviolence1.html.

فصل سوم درآمدی بر جنگ اطلاعاتی استراتژیک

جیان پیرو سیرلی*

«کسب یک‌صد پیروزی در یک‌صد نبرد، اوج برتری نیست؛ به زانو درآوردن ارتش دشمن بدون جنگیدن، نقطه اوج حقیقی برتری است».

سون تزو، هنر جنگ، در حدود سال ۵۰۰ پیش از میلاد[1]

مقدمه

فناوری‌های اطلاعاتی و ارتباطاتی از میانه دهه ۱۹۸۰[2] به‌نحوی بسیار سریع تکامل یافته و به موازات آن سیستم‌های اطلاعاتی نیز در سراسر جهان به‌شدت گسترش یافت. گسترش و همگرایی شتابنده فناوری‌های ارتباطاتی، سیستم‌های رایانه‌ای و فرایندهای اطلاعاتی در جهان معاصر، زیرساخت اطلاعاتی[3] را در تمامی سطوح جامعه، به‌ویژه در کشورهای صنعتی شده غربی گسترش داده و عمق بخشیده است؛ شهروندان، فعالیت‌های اقتصادی و سازمان‌های دولتی بیش‌ازپیش به فناوری‌های اطلاعاتی[4] وابسته شده‌اند.

این فرایند تکاملی، جنبه‌های مثبت زیادی دارد. اما ضروری است این فرایند ازنظر وابستگی فزاینده به زیرساخت اطلاعاتی جهانی ـ که به‌صورت شبکه‌ای است و در حال حاضر در دست ساخت می‌باشد ـ براساس معیار میزان آسیب‌پذیری و الزامات امنیتی احتمالی آن تحلیل شود. اتکای گسترده به فناوری‌های اطلاعات‌محور چه‌بسا جامعه را به‌سمت سطح بی‌سابقه‌ای

---

* Gian Piero Siroli

1. Sun Tzu, The Art of War, About 500 BC
2. Information and Communication Technologies (ICT)
3. Information Infrastructure
4. Information Technologies (IT)

از به‌هم پیوستگی و وابستگی متقابل گسترده جهانی سوق خواهد داد. آسیب‌پذیری‌های جدید، که در سطوح متعدد و متنوعی می‌توان از آنها بهره‌برداری کرد، در اثر تلاقی و تداخل فزاینده زیرساخت‌های حساس سنتی یک کشور (برای مثال، زیرساخت‌های حیاتی‌ای مثل سیستم‌های توزیع انرژی یا خدمات فوریتی) با زیرساخت‌های اطلاعاتی نوظهور امروزی (که در معرض حمله‌های الکترونیکی است) پدید می‌آیند.

زیرساخت های اطلاعاتی، که از سیستم های اطلاعاتی و شبکه های مخابراتی به همراه تمامی فناوری‌های مرتبط با آنها تشکیل شده‌اند، در حوزه سیاست‌های دفاعی بسیاری از کشورها بیش ازپیش اهمیت یافته‌اند چرا که در شرایط خاصی یکی از آماج‌های مهم حملات نظامی می‌شوند. وانگهی، نباید فراموش کرد که اطلاعات و اطلاعات جعلی[1] همواره عاملی اساسی در جنگ بوده‌اند. بهره‌برداری از فناوری اطلاعاتی پیشرفته در میدان نبرد، باعث توسعه فنون جنگی جدید شده و معضلاتی را در هر دو حوزه امنیت ملی و بین‌المللی پدید آورده است.

این فصل درواقع، درآمدی بر موضوع جنگ اطلاعاتی استراتژیک است ـ که به عبارت بهتر، فناوری‌های اطلاعاتی را در بافت و چارچوب امنیت ملی و بین المللی بررسی می‌کند؛ در این خصوص، آسیب‌پذیری‌های احتمالی زیرساخت‌های حساس در کشورهای توسعه‌یافتهٔ مدرن را توصیف می‌کند. گزارشی که کمیسیون حفاظت از زیرساخت های حساس[2] (وابسته به نهاد ریاست جمهوری آمریکا) در سال ۱۹۹۷ منتشر کرد، در اینجا به‌عنوان یک مطالعه موردی بررسی خواهد شد و برخی از نتیجه‌گیری‌های اصلی آن مورد بحث و بررسی قرار خواهد گرفت.

منظور از جنگ اطلاعاتی چیست؟ از دیدگاهی عام، جنگ اطلاعاتی دربرگیرنده اقداماتی است که برای کسب برتری انجام می‌گیرد؛ برای نیل به این هدف، نه تنها باید در اطلاعات، فرایندهای اطلاعات‌محور، سیستم‌های اطلاعاتی و شبکه‌های رایانه‌ای دشمن نفوذ کرد، بلکه باید از زیرساخت اطلاعاتی در داخل کشور خود نیز دفاع و محافظت نمود. به‌عبارت‌دیگر، جنگ اطلاعاتی، مجموعه فعالیت‌هایی است که هدف از آن ایجاد اختلال در منابع اطلاعاتی دشمن، نابودسازی این منابع و یا جلوگیری از دستیابی دشمن به

---

1. Disinformation
2. US President's Commission on Critical Infrastructure Protection (PCCIP)

آنهاست. جنگ اطلاعاتی، هم عملیات تهاجمی و هم عملیات تدافعی را در درون خود دارد؛ اما بسیاری مواقع، هم‌پوشانی میان این دو بعد (تهاجمی و تدافعی)، چشمگیر است.

۱-۳ بافت

ایالات متحده آمریکا ازنظر فناوری اطلاعاتی، احتمالاً پیشرفته‌ترین کشور جهان است؛ و درعین‌حال، وابسته‌ترین کشور به زیرساخت‌های ارتباطاتی نیز به‌شمار می‌آید. در نتیجه، در حوزه فناوری اطلاعاتی، در مقایسه با سایر کشورها به‌مراتب آسیب‌پذیرتر است. در ایالات متحده، فعالیت ها و برنامه‌های پژوهشی متنوعی درزمینهٔ جنگ اطلاعاتی در سطوح مختلف انجام می‌گیرد. ازاین‌رو، به موضوعاتی از قبیل حفاظت، تضمین و اطمینان و نیز بقاپذیری[1] زیرساخت‌های حیاتی توجه می‌شود.

اقداماتی هم که دولت آمریکا انجام می‌دهد در حیطه این فعالیت‌ها می‌گنجد؛ در اینجا برای نشان دادن این روند، تنها به برخی از مهم‌ترین اقدامات آن اشاره می‌کنیم. در ژانویه ۱۹۹۵ وزارت دفاع آمریکا به‌منظور طراحی و تحقق اهداف ملی درزمینه جنگ اطلاعاتی، شورای اجرایی جنگ اطلاعاتی[2] را تأسیس و شش ماه بعد، دستورالعمل شماره ۳۹ ریاست جمهوری،[3] خط‌مشی‌ها درزمینه تهدیدهای تروریستی را تعیین کرد؛ در این سند، فعالیت‌های مربوط به جنگ اطلاعاتی نیز گنجانده شده بود. در جولای ۱۹۹۶، دستورالعمل اجرایی شماره ۱۳۰۱۰[4] کمیسیون حفاظت از زیرساخت‌های حساس را تأسیس کرد. این نهاد که زیر نظر رئیس‌جمهور اداره می‌شد، وظیفه داشت تهدیدهای فیزیکی و سایبر علیه زیرساخت‌های حیاتی آمریکا را ارزیابی کند و استراتژی‌هایی را برای حفاظت از آنها تدوین نماید. هم‌زمان با تشکیل این کمیسیون و به‌منظور تقویت هماهنگی درزمینه حفاظت از زیرساخت‌ها، نیروی ویژه حفاظت از زیرساخت‌ها[5] نیز ایجاد شد.

اصول اساسی سیاست ایالات متحده در مورد حفاظت از زیرساخت‌های حساس، در دستورالعمل شماره ۶۳[6] رئیس‌جمهور، که در مه ۱۹۹۸ صادر شد، مشخص شدند. به

---

1. Survivalability
2. Information Warfare Executive Baord (IWEB)
3. Presidential Decision Directive 39 (PDD39)
4. Executive Order 13010
5. Infrastructure Protection Task Force (IPTF)
6. PDD63

دنبال این دستورالعمل، دو سازمان تأسیس شد: یکی، مرکز ملی حفاظت از زیرساخت‌ها،[1] که مقر آن در اف.بی.ای بود؛ و دیگری، دفتر تضمین زیرساخت‌های حساس[2] که در وزارتخانه بازرگانی مستقر بود. درعین‌حال، پروژه‌های دیگری نیز پیشنهاد شد. برای مثال، می‌توان به شبکه فدرال کشف تعرضات به زیرساخت‌ها[3] اشاره کرد. هدف از تأسیس این نهاد، حفاظت از دولت و مراکز اصلی بخش خصوصی با نظارت وسیع بر شبکه‌ها و سیستم‌ها بوده است.

در جولای ۱۹۹۹، دستورالعمل اجرایی شماره ۱۳۱۳۰[4] شورای تضمین زیرساخت‌های ملی[5] را تأسیس کرد. بعد از آن، در ژانویه ۲۰۰۰، دولت آمریکا برنامه ملی حفاظت از سیستم‌های اطلاعاتی[6] را، که وابستگی‌ها و تهدیدهای جدید را توصیف می‌نماید، تدوین کرد. این برنامه پیشنهاد داد که برای طرح‌ریزی سیستم دفاعی سایبر، بخش‌های دولتی و خصوصی باهم مشارکت کنند و برنامه‌های آموزشی نیز در این راستا تدوین شوند. این برنامه شبکه فدرال کشف تعرضات به زیرساخت‌ها را به‌منظور حفاظت از سازمان‌های غیرنظامی فدرال در خود جای داد. خاطرنشان می‌شود بودجه‌ای که این سازمان‌ها برای سال مالی ۲۰۰۱ درخواست کرده بودند افزون‌بر ۱۰ میلیون دلار بوده است. ابتکار شبکه فدرال کشف تعرضات به زیرساخت‌ها، که سیستم‌های هشداردهنده برای نظارت بر شبکه‌های رایانه‌ای حساس به‌شمار می‌آید، بعدها لغو شد و سیستم دیگری جایگزین آن شد. اما درهرحال هدف از طرح این ابتکار، این است که اگر توانمندی واکنش به حوادث رایانه‌ای فدرال،[7] به هرگونه فعالیت خصمانه‌ای مشکوک شود، باز هم دولت بتواند به مرکز ملی حفاظت از زیرساخت‌ها آماده‌باش دهد. در سال ۲۰۰۲، شورای حفاظت از زیرساخت‌های حساس (که زیر نظر رئیس‌جمهور آمریکا فعالیت می‌کند) گزارشی درزمینه «استراتژی ملی تأمین امنیت فضای سایبر» منتشر کرد و کمیته اقتصادی مشترک کنگره

---

1. National Infrastructure Protection Centre (NIPC)
2. Critical Infrastructure Assurence Office (CIAO)
3. Federal Intrusion Petection Network (FIPNET)
4. Executive Order 13130
5. National Infrastructure Assurance Council
6. A National Plan for Information Systems Protection
۷. Federal Computer Incident Response Capability (FedCIRC): مرکز اصلی تحلیل و هماهنگ‌سازی اطلاعات است که به مسائل مرتبط با امنیت رایانه‌ها رسیدگی می‌کند ـ م.

نیز طرح «امنیت در عصر اطلاعات» را ارائه داد. این طرح، طیفی از دیدگاه‌ها در مورد حفاظت از زیرساخت های اطلاعاتی را تشریح کرده است. از آن زمان تاکنون، بسیاری از فعالیت‌های دیگر در تمامی سطوح در این بافت، توسعه یافته است.

بعد از این اقدامات دولت آمریکا، برنامه‌های مشابهی در اروپا آغاز شد؛ اما بااین‌حال هدف اروپایی‌ها از آغاز این گونه برنامه‌ها در بسیاری مواقع با اهداف آمریکا تفاوت داشت. در سال‌های ۱۹۹۷ و ۱۹۹۸ چهار کارگاه آموزشی با حضور دانشگاهیان، صاحبان صنایع و مقامات دولتی برگزار شد؛ هدف برگزارکنندگان کارگاه‌های آموزشی، این بود که زمینه طرح‌ریزی «ابتکار قابلیت اعتماد به داده‌های اطلاعاتی در اروپا»[1] را در چارچوب «برنامه فناوری‌های جامعه اطلاعاتی»[2] فراهم سازند و مدیریت آن را به نهاد اداره کل انجمن اطلاعاتی، که زیرمجموعه‌ای از کمیسیون اروپایی است بسپارند. هدف، این بود که راه‌حل‌هایی را درزمینه نحوه مقابله با چالش‌های ناشی از وابستگی به فناوری‌های اطلاعاتی و ارتباطاتی و ظهور آسیب‌پذیری‌های جدید بیابند تا از این راه، اعتماد و اطمینان به سیستم‌ها و خدمات را تقویت کنند.

در سال ۱۹۹۹، تیمی از نهاد «برآورد گزینه‌های علمی و فناورانه»،[3] چهار پژوهش را در پاسخ به درخواست «کمیته آزادی و حقوق شهروندان، امور قضایی و امور داخلی»[4] سفارش داد. پژوهش اول پیشرفته‌ترین نظارت الکترونیک با جاسوسی ارتباطات[5] را که از توانمندی‌های رهگیری در مقیاسی جهانی برخوردار است، بررسی می‌کند. پژوهش دوم، سازوکارهایی را که برای محافظت از کشورها در برابر رهگیری‌های ارتباطات به‌کار می‌روند می‌کاود. پژوهش سوم به بررسی قانونی بودن رهگیری ارتباطات الکترونیک می‌پردازد و ازاین‌رو سیاست‌ها و موافقت‌نامه‌های بین‌المللی موجود را ارزیابی می‌کند. پژوهش آخر، آن خطرات اقتصادی‌ای که در اثر رهگیری‌های ارتباطات پدیدار می‌شوند، تحلیل می‌کند. کانون توجه این فعالیت‌ها اندکی با محور ابتکارهای ایالات متحده تفاوت دارد؛ چرا که این

---

1. European Dependability Initiative (EDI)
2. Information Society Technologies (IST)
3. Scientific and Technological Options Assessment (STOA)
4. Communication Intelligence
5. Committee on Citizen Freedom and Rights, Justice and Home Affairs

فعالیت‌ها هم موضوع حفاظت از داده‌ها را در خود جای داده‌اند و هم به جنبه محرمانه بودن ارتباطات توجه دارند؛ این وضعیت نشان می‌دهد که این فناوری‌ها پیامدهای مهمی در همه بخش‌های گوناگون جامعه دارند. در اینجا باید خاطرنشان کرد که در نوامبر ۲۰۰۱، شورای اروپا «معاهده جرائم سایبر»[1] را امضا کرد. جرائم سایبر حتی اگر یکی از مهم‌ترین وجوه امنیت ملی و بین‌المللی نباشد، دست‌کم یکی از ابعاد آن به‌شمار می‌آید.

اما در سال‌های اخیر، بعضی از کشورهای اروپایی، از جمله آلمان، هلند، نروژ، سوئیس و بریتانیا، ابتکارهایی را براساس تحلیل‌هایی که در مورد آسیب‌پذیری‌های زیرساخت‌هایشان و براساس طرح کلی سیستم‌های هشداردهنده اولیه که در اختیار دارند به اجرا درآورده‌اند؛ حتی در برخی موارد تدابیری را برای مقابله با این آسیب‌پذیری‌ها پیشنهاد داده‌اند و سیاست‌هایی را در این چارچوب تدوین کرده‌اند. اتریش، فنلاند، فرانسه و ایتالیا نیز بیش‌ازپیش در این حوزه فعال شده‌اند.

سازمان ملل متحد هم به اهمیت این مسئله اذعان نمود. در دسامبر ۱۹۹۸، مجمع عمومی قطعنامه ۵۳/۷۰[2] را صادر کرد. این قطعنامه، موضوع امنیت سیستم‌های اطلاعاتی و مخابراتی را که گستره فعالیت آنها جهانی بود، مورد توجه قرار داد و از بررسی تهدیدهای موجود و بالقوه در حوزه امنیت اطلاعاتی حمایت به‌عمل آورد. در سال ۱۹۹۹، دو نهاد سازمان ملل متحد ـ اداره امور خلع سلاح[3] و مؤسسه تحقیقات خلع سلاح[4] ـ اجلاسی را در مورد «تحولات در حوزه اطلاعات و مخابرات و تأثیر آنها بر امنیت بین‌المللی» برگزار کردند. اگر تماس‌های دوجانبه و چندجانبه در این زمینه را در نظر نگیریم، این اجلاس، اولین نشست در مورد این موضوع بود که سازمان ملل متحد برگزار کرد. در دسامبر ۱۹۹۹، براساس دیدگاه‌ها و ارزیابی‌هایی که برخی از کشورها ارائه داده بودند، قطعنامه دوم به شمارهٔ ۵۴/۴۹[5] در این زمینه صادر شد. این قطعنامه از کشورهای عضو سازمان ملل متحد دعوت کرد به‌منظور تقویت امنیت سیستم‌های اطلاعاتی و مخابراتی که حوزه عمل آنها در سراسر جهان است، حدود و ثغور مفاهیم

1. Convention on Cybercrime
2. Resolution 53/70
3. Department of Disamament Affairs
4. Institute for Disarmoment Research
5. Resolution 54/49

پایه‌ای مرتبط با امنیت اطلاعات و توسعه اصول بین‌المللی در این زمینه را مشخص سازند. از آن تاریخ تاکنون، مجمع عمومی سازمان ملل قطعنامه‌های دیگری[1] را نیز در این خصوص به تصویب رسانده است. این تکاپوی سازمان ملل متحد نشانگر علاقه‌ای است که به این موضوع وجود دارد.

۲-۳ زیرساخت‌های حساس[2]

در ابتدای این بخش، دو سؤال مطرح می‌کنیم: منظور ما از اصطلاح زیرساخت به‌طور دقیق در این بافتار چیست و چرا باید از زیرساخت حفاظت کرد؟ یک زیرساخت، مجموعه ساختاریافته‌ای از شبکه‌ها و سیستم‌های وابسته به هم است که در بسیاری از سطوح مختلف (از جمله صنایع، نهادها و توانمندی‌های توزیع که امکان گردش کالا یا خدمات را فراهم می‌آورند) با یکدیگر پیوند دارند. اگر دقیق‌تر شویم، می‌توان پنج حوزه اصلی را در این خصوص شناسایی کرد،[3] که هریک از آنها به‌نوبه خود، حوزه‌های بسیار وسیعی را دربرمی‌گیرند:

۱. اطلاعات و ارتباطات،
۲. انرژی،
۳. بانکداری و امور مالی،
۴. توزیع فیزیکی،[4]
۵. خدمات انسانی حیاتی.

در این بخش، هریک از این حوزه‌های پنج‌گانه را به‌ترتیب بررسی خواهیم کرد. اما نباید فراموش کرد که «طرح گزارش زیربناهای حساس، فقط یکی از طرح‌هایی است که می‌توان از آنها برای تحلیل و توصیف پیچیدگی مسئله امنیت زیرساخت‌ها استفاده کرد». برای بررسی این موضوع، رویکردهای دیگری نیز وجود دارد. برای مثال،

---

1. Res. 55/28, 56/19, 57/53, 58/199
2. Critical Infrastructures
۳. این تقسیم‌بندی به پیروی از طرح گزارشی تحت عنوان «زیربناهای حساس» (Critical Foundations) که کمیسیون حفاظت از زیرساخت‌های حساس منتشر کرد انجام گرفته است.
4. Physical Distribution

زیرساخت‌ها را می‌توان برحسب مؤلفه‌ها یا شبکه‌هایی که در خود دارند یا براساس خدماتی که ارائه می‌دهند بررسی کرد. این زیرساخت‌ها از آن جهت «حساس» به‌شمار می‌آیند که فرض می‌شود آنها برای زندگی روزمره و عادی شهروندان، ضروری‌اند و ایجاد اختلال یا تخریب آنها امنیت اقتصادی یا توانمندی‌های دفاعی کشور را سست خواهد ساخت. گفتنی است که این پنج بخش نه تنها مستقل و جدا از یکدیگر نیستند بلکه پیوندهای بسیار شدیدی با یکدیگر دارند. آنچه در ذیل می‌آید توصیفی بسیار دقیق در مورد زیرساخت‌های حساسی است که در هریک از این پنج بخش جای گرفته‌اند.

بخش «اطلاعات و ارتباطات» اموری از قبیل همه تجهیزات مخابراتی، فنون فناوری‌های رایانه‌ای و شبکه‌ای (اعم از سخت‌افزاری و نرم‌افزاری) و خطوطی که امکان ارتباط عرضه خدمات اینترنتی را فراهم می‌نمایند شامل می‌شود. شبکه‌های تلفن همگانی که امکان ارتباط صوتی و تصویری خطوط ارتباطی خصوصی را فراهم می‌آورند و میلیون‌ها رایانه‌ای که برای کاربردهای تجاری، علمی و دولتی مورد استفاده قرار می‌گیرند و یا در منازل یافت می‌شوند، همه‌وهمه در بخش اطلاعات و ارتباطات جای می‌گیرند. این بخش درواقع پایگاهی برای تسهیل پردازش، ذخیره و ارسال داده‌ها و اطلاعات به‌شمار می‌آید. در حال حاضر، ما شاهد ادغام همه این زیرساخت‌ها با یکدیگر در مقیاسی جهانی هستیم.

سیستم‌های پیچیده تولید، ذخیره و توزیع همه اشکال انرژی (از جمله گاز طبیعی، نفت خام، فراورده‌های نفتی، انرژی هسته‌ای، تأسیسات فراوری انرژی و برق) در حوزه انرژی جای می‌گیرند. برای مثال، شبکه برق‌رسانی یک کشور، بخشی از این زیرساخت است؛ این حوزه، حمل‌ونقل، فعالیت‌های تولیدی و ارائه خدمات رفاهی (آب، برق و گاز) را تسهیل می‌کند و اساس بسیاری از زیرساخت‌های دیگر را تشکیل می‌دهد؛ این زیرساخت درواقع، مهم‌ترین و اصلی‌ترین مؤلفه برای سایر زیرساخت‌ها به‌شمار می‌آید و برای ثبات اقتصادی هر کشور حیاتی است.

بخش بانکداری و امور مالی، پدیده‌هایی از قبیل بانک‌ها، سازمان‌های تجاری، نهادهای سرمایه‌گذاری، مراکز صنعتی ـ تجاری و سازمان‌های عملیاتی مرتبط با آنها و فعالیت‌های پشتیبانی مثل خدمات مبادله مالی، پرداخت‌های الکترونیکی و سیستم‌های ارسال پیام در این حوزه را در خود جای داده است. برای مثال، در ایالات متحده آمریکا، این زیرساخت،

تریلیون‌ها دلار گردش پولی (از سپرده‌های اشخاص و چک‌های بانکی گرفته تا انتقال وجه برای انجام فعالیت‌های بزرگ تجاری در مقیاس جهانی) را مدیریت می‌کند.

شبکه‌های راه‌ها و بزرگراه‌ها، خطوط راه‌آهن و سیستم حراست از حریم هوایی (خطوط هوایی، هواپیماها و فرودگاه‌ها) در زمره عناصر بخش توزیع فیزیکی است؛ این بخش خط لوله‌های سراسری، بنادر و آبراه‌ها را نیز دربرمی‌گیرد. زیرساخت توزیع فیزیکی امکان جابه‌جایی کالا و رفت‌وآمد افراد در داخل و خارج از مرزهای کشور را فراهم می‌کند.

سرانجام، بخش خدمات انسانی حیاتی، اموری از قبیل خدمات اورژانس (برای مثال پلیس، آتش‌نشانی و نجات حادثه‌دیدگان)، خدمات دولتی، نهادهای محلی و ایالتی و سیستم‌های سراسری آبرسانی را که خدمات مهمی را در اختیار بخش‌های صنعت، کشاورزی و نیز منازل قرار می‌دهند در خود جای داده است.

این درهم‌تنیدگی بخش‌های مختلف، زیرساخت‌های جهان‌گستر را بسیار پیچیده می‌سازد. تعیین و ترسیم دقیق مرزها، ارزیابی تأثیرات رویدادها و شناسایی مسئولیت‌هایی که برای اداره این چارچوب‌های گوناگون برعهده اشخاص و نهادها گذارده می‌شود، بسیار دشوار است. باید خاطرنشان کرد که دو زیرساخت ـ یعنی، بخش انرژی (به‌ویژه، توزیع برق (برق‌رسانی)) و بخش اطلاعات و ارتباطات ـ زیربنای سایر زیرساخت‌ها را تشکیل می‌دهند، به‌طوری‌که بروز اختلال یا وقفه در این بخش‌ها به‌طور بالقوه می‌تواند گسترده‌ترین تأثیر را داشته باشد. روند فعلی، این است که تمامی زیرساخت‌های حساس بیش‌ازپیش به فناوری‌های اطلاعاتی و ارتباطاتی وابسته شده‌اند.

این امکان وجود دارد که وقوع فاجعه‌های طبیعی و سوءرفتارها و اشتباهات انسانی به این زیرساخت‌ها ضربه بزند. ازاین‌گذشته، هریک از این زیرساخت‌ها، بسته به اقتضائاتی از قبیل طرح، عملیات اجرایی و عملکردی که دارند، در معرض تخریب یا اختلال‌اند و تا حدودی آسیب‌پذیر. این آسیب‌پذیری می‌تواند در سطح فیزیکی، سایبر، یا به شکلی که آمیزه‌ای از دو عامل فیزیکی و سایبر وجود دارد، رخ دهد. آسیب‌پذیری در حالتی که هر دو عامل فیزیکی و سایبر نقش دارند، به‌ویژه در وضعیتی که به‌طور هم‌زمان، نوعی وابستگی فیزیکی و سایبر وجود دارد، مبهم‌ترین شرایط را ایجاد می‌کند. مسئله‌ای که در آغاز سال ۲۰۰۰ در اثر ثبت نادرست فرمت دو رقم آخر تاریخ سال میلادی در بسیاری از

برنامه‌های کاربردی رایانه‌ها به‌وجود آمد، یکی از نمونه‌های بارز این‌گونه آسیب‌پذیری در وضعیت ابهام‌آمیز است. توجهی که به‌ویژه، کشورهای غربی به برآورد پیامدهای احتمالی این وضعیت مبذول داشتند نشان می‌دهد که در حال حاضر اگر نرم‌افزارها در بسیاری از سیستم‌های رایانه‌ای و زیرساخت‌های اطلاعاتی اساسی گسترش و اشاعه یافته باشند، برآورد تأثیرات نقص و اختلال جزئی در آنها، حتی با وجود آنکه اختلال‌ها به نسبت ساده و غیرعمدی هم باشند، دشوار است. هرچند ممکن است رسانه‌ها مشکل احتمالی رایانه‌ها در آغاز سال ۲۰۰۰ را بزرگ‌نمایی کرده باشند یا اهداف تجاری در پس آن سناریو نهفته باشد، اما این واقعیتی است که کاربران (در برخی اوقات نه تنها کاربران بلکه متخصصان نیز علاوه‌بر بی‌اطلاعی از اختلالات نرم‌افزاری)، آگاهی چندانی از همه ویژگی‌های ریز و به‌ظاهر کم‌اهمیت ـ که در هر برنامه کاربردی رایانه‌ای وجود دارد ـ ندارند و مهم‌تر از همه اینکه، درزمینه پیامدهای غیرمستقیم این ویژگی‌ها، به‌ویژه در سیستم‌های پیچیده نیز کم‌اطلاع‌اند. این معضل در حوزه امنیت سیستم‌های رایانه‌ای، بسیار مشهود است.

۳-۳ آسیب‌پذیری‌ها

نمونه‌های آسیب‌پذیری احتمالی در حوزه‌های مختلف کدام‌اند؟ «انرژی» و «توزیع فیزیکی» به درجات مختلف در معرض آسیب‌پذیری‌های فیزیکی قرار دارند. نمونه بارز این آسیب‌پذیری‌ها فاجعه‌های طبیعی یا خرابکاری‌اند. اما در اینجا ما می‌خواهیم توجه خود را به آن مسائل و تهدیدهای احتمالی که سرشتی متفاوت دارند، معطوف نماییم.

۳-۳-۱ اطلاعات و ارتباطات

علاوه‌بر فاجعه‌های طبیعی، مهم‌ترین تهدیدها فراروی این بخش، نقص‌ها، اختلال‌ها و بی‌ثباتی‌هایی است که در اثر افزایش حجم و پیچیدگی ارتباطات پدید می‌آیند. در گذشته، حملات و رخنه‌ها در سیستم‌های رایانه‌ای با ایجاد اختلال در دستگاه‌های شبکه‌ها و سیستم‌های مدیریتی به‌نحوی حساب شده انجام می‌گرفت. در سال‌های اخیر، شبکه‌های تلفن همگانی بیش‌ازپیش نرم‌افزاری شده‌اند و اداره و کنترل آنها به‌هیچ‌وجه با شبکه‌های رایانه‌ای انجام نمی‌گیرد، که این امر نیز به‌نوبه خود، احتمال نفوذهای

الکترونیک را افزایش داده است. وجود مراکز بزرگ برای حمایت از فعالیت‌های رایانه‌ای قانونی فقط نارسایی‌ها را ایجاد می‌کند و هدف‌گیری اقدامات خصمانه را آسان‌تر می‌سازد. آسیب‌پذیری در زیرساخت اطلاعات و ارتباطات در دهه ۱۹۹۰ تشدید شده است؛ تا آنجا که به اینترنت مربوط می‌شود، در طول روند تکاملی و استقرار شبکه اینترنت، ضریب بالای امنیت، دغدغه اصلی در طراحی آن نبود.

۲-۳-۳ انرژی

گسترش سریع سیستم‌های اطلاعاتی و ارتقای آن به سطح تولید صنعتی که براساس ساختارهای آشکار در محیطی عملیاتی به‌کار گرفته شد، باعث افزایش درجه آسیب‌پذیری این بخش گردید. این وضعیت اتکا به پیوندها در ارتباطات را که گاهی اوقات به شبکه‌های تلفن همگانی کشیده می‌شود، تشدید می‌کند. برای مثال، استفاده گسترده و فراگیر از «سیستم‌های کنترل نظارتی و دستیابی به داده‌ها»[1] به‌منظور کنترل و نظارت بر زیرساخت‌های انرژی، این خطر را در پی دارد که اقدامات خصمانه با استفاده از ابزارهای سایبر، خسارت‌های جدی بر آنها وارد سازد و در نتیجه، اختلال‌های قابل ملاحظه‌ای در آنها پدیدار شود. سیستم‌های کنترل نظارتی و دستیابی به داده‌ها با نیروی برق کار می‌کنند و در این میان، از صنایع نفت و گاز هم تغذیه می‌شوند. اگر عامل خرابکاری بتواند به این سیستم دسترسی یابد و داده‌هایی که برای تصمیمات عملیاتی به‌کار می‌روند، تغییر دهد یا بر روند تهیه تجهیزات حساس، کنترل و اشراف داشته باشد، در این صورت، خرابکاری احتمالی از طریق شبکه‌های تلفن همگانی اختلال‌های قابل توجهی را به بار خواهد آورد. استفاده گسترده از سخت‌افزارها و نرم‌افزارهای تجاری نیز خطراتی در پی دارند. این دستگاه‌ها و برنامه‌ها خطرساز به‌شمار می‌آیند، زیرا ممکن است مشخصات کامل برخی از قطعات در دسترس نباشد و یا اصلاً راهنمای استفاده از آنها وجود نداشته باشد. همین امر به‌نوبه خود، از کارآمدی آنها می‌کاهد و اختلال‌هایی را به‌وجود می‌آورد؛ زیرا درواقع، آنها استاندارد نیستند. نرم‌افزارها و سخت‌افزارهای تجاری گاهی اوقات، نوعی آسیب‌پذیری ذاتی در خود دارند و این وضعیت ممکن است مشکلاتی را درزمینه امنیت و

1. Supervisory Control and Data Acquisition Systems (SCDAS)

اطمینان به آنها به بار آورد. به‌علاوه، گاهی اوقات، اطلاعات درزمینه آسیب‌پذیری‌ها، که برای هدف قرار دادن فعالیت‌های نظامی متعارف مفیدند، در دسترس عموم قرار می‌گیرد.

۳-۳-۳ بانکداری و امور مالی

این بخش، امن‌ترین حوزه قلمداد می‌شود، چرا که آسیب‌پذیری‌های اصلی آن، ماهیتی فیزیکی دارند. در بسیاری از کشورها و به‌ویژه در ایالات متحده آمریکا، تدابیر قاطعانه‌ای در این حوزه اندیشیده شده و اقداماتی نیز انجام گرفته است؛ از جمله، تأسیسات مهم مالی مقاوم‌سازی شده‌اند، امنیت این زیرساخت ارتقا یافته و سیستم فراگیری در این زمینه تدارک دیده شده است؛ اما همچنان خطراتی هم این حوزه را تهدید می‌کند؛ این خطرات از ایجاد اختلال در شبکه‌های مخابراتی و خدمات برق‌رسانی نشئت می‌گیرد. گذشته از آسیب‌پذیری‌های وسیعی که در این زیرساخت وجود دارد، زمینه‌های سرقت و تقلب در هریک از نهادهای وابسته به آن نیز بسیار چشمگیر و فراوان است. خودی‌ها،[1] یعنی کسانی که مجوز دسترسی به گردآوری اطلاعات محرمانه را دارند یا از سیستم‌ها برای سود شخصی استفاده می‌کنند، مزمن‌ترین تهدید امنیتی به‌شمار می‌آیند. نهادهای مالی به‌علت حساسیتی که در ذات اطلاعات محرمانه وجود دارد و نیز به‌دلیل حفظ و استمرار اعتماد عمومی به آنها، در بیشتر مواقع انکار می‌کنند که درزمینه حل مشکل احتمالی سیستم خود، از سازمان‌های بیرونی[2] استفاده می‌نمایند. این وضعیت، شفافیت آن سیستم را کاهش می‌دهد و کشف اختلالات و نفوذها به سیستم و نیز حفاظت از کل زیرساخت را پیچیده‌تر می‌سازد.

۳-۳-۴ توزیع فیزیکی

آسیب‌پذیری‌های سایبر در حوزه توزیع فیزیکی نیز مانند سایر حوزه‌ها رفته‌رفته پدیدار می‌شود. این بخش هر روز بیش از گذشته به زیرساخت‌های ارتباطات و فناوری اطلاعات، وابسته می‌شود. همه جنبه‌های صنعت حمل‌ونقل در معرض آسیب‌پذیری‌های سایبر قرار دارند. برای مثال، استفاده از سیستم‌های حمل‌ونقل هوشمند[3] به‌سرعت

---

1. Insiders

۲. منظور، سازمان‌هایی است که خارج از تشکیلات نهاد مالی فعالیت دارند.

3. Intellignt Transportation Systems

گسترش یافته و این امر، در بهینه‌سازی شبکه حمل‌ونقل مؤثر بوده و در کل، کارایی آن را نیز افزایش داده، اما بااین‌حال، بیش‌ازپیش در معرض آسیب‌پذیری‌های سایبر قرار گرفته است. در برخی موارد، داده‌هایی که اینترنت در دسترس عموم قرار می‌دهد، چه‌بسا برای گردآوری اطلاعات درزمینه اهداف[1] نظامی احتمالی[2] مورد استفاده قرار می‌گیرند. گزارش زیربناهای حساس تصریح می‌کند در ایالات متحده آمریکا چشمگیرترین آسیب‌پذیری‌هایی که مطرح می‌شود، آسیب‌پذیری‌هایی است که ناشی از نوسازی «سیستم هوایی ملی»[3] اند. این سیستم، حمل‌ونقل هوایی را کنترل می‌کند و علاوه‌بر این، می‌کوشد «سیستم موقعیت‌یاب جهانی»[4] را به‌عنوان یگانه مبنای جهت‌یابی و رهگیری رادیویی در آمریکا تا سال ۲۰۱۰ به تصویب رساند.

در حال حاضر، سیستم هوایی ملی تا حدودی از نفوذ خرابکاران در امان است؛ این سیستم، سیستم‌های فرعی و شبکه‌هایی در خود دارد که رخنه کردن در آنها بسیار دشوار است. احتمال می‌رود این معماری[5] نوظهور در زیرساخت‌ها به موازات بهره‌گیری از محصولات نرم‌افزاری و سخت‌افزاری تجاری، از سیستم‌های غیرمحرمانه و شبکه‌های ارتباطی همگانی نیز استفاده کند. در نتیجه، خطر دسترسی غیرقانونی و احتمال اقدامات موذیانه نیز به‌شدت افزایش خواهد یافت. تا آنجایی که به سیستم موقعیت‌یاب جهانی مربوط می‌شود، طرح‌های فعلی چه‌بسا می‌تواند به اتکای بیش از حد به این سیستم بیانجامد. این وضعیت نیز در برابر اقداماتی از قبیل ایجاد پارازیت در امواج و کلاهبرداری‌ها (ارسال اطلاعات غلط درزمینه سیستم موقعیت‌یاب جهانی)، آسیب‌پذیر است.

۵-۳-۳ خدمات انسانی حیاتی

در این بخش، دغدغه اصلی در رابطه با آسیب‌پذیری‌های سایبر، اتکای روزافزون به سیستم‌های «کنترل نظارتی و دستیابی به داده‌ها»ست که برای نظارت بر نحوه آب‌رسانی

---

1. Target
2. Potential
3. National Airspace System (NAS)
4. Global Positioning System (GPS)
5. Architecture

مورد استفاده قرار می‌گیرد. علاوه‌بر این، برخی از سیستم‌های اضطراری[1] ممکن است در معرض سوءاستفاده قرار گیرند، به صورتی که بیش از ظرفیتی که دارند، خدمات ارائه دهند. خدمات دولتی، پایگاه‌های عظیم اطلاعاتی را در اختیار دارند که با آنها می‌توانند اطلاعات فوق‌العاده سّری در مورد وضعیت شهروندان را برای خود نگه دارند؛ نفوذ و رخنه سایبر به درون این پایگاه‌های اطلاعاتی، یک نگرانی به‌شمار می‌آید؛ زیرا این پایگاه‌ها نیز همه به فناوری رایانه‌ای وابسته‌اند. ازاین‌گذشته، این امکان نیز وجود دارد که در اقدامات شناسایی، ردگیری تجهیزات و ادوات نظامی از روش سایبر استفاده شود.

نمونه‌های مفصل‌تری را نیز می‌توان ارائه داد: نمونه اول به شبکه‌های تلفن همگانی مربوط می‌شود، که سطح آسیب‌پذیری آنها رو به رشد است. در سال‌های اخیر، شمار پیوندها میان شرکت‌های مخابراتی افزایش یافته است؛ پیوندها به‌ویژه با اینترنت انجام گرفته است. این وضعیت باعث می‌شود که دو شبکه مخابراتی متفاوت که مثلاً از استانداردهای سامانه سیگنال‌دهی از کانال مشترک ـ ۷[2] استفاده می‌کنند، می‌توانند با شبکه پروتکل اینترنتی[3] به یکدیگر متصل شوند. به‌عبارت‌دیگر، یک پیام تلفنی می‌تواند از نقطه شهری تماس‌گیرنده به ورودی پروتکل اینترنتی SS7[4] ارسال شود و با شبکه پروتکل اینترنتی به ورودی دومی راه یابد که در آنجا نیز برای رسیدن به مقصد نهایی خود، دوباره وارد شبکه تلفن دیگر می‌شود. شبکه ارسال پیام شماره ۷ (SS7) استاندارد جهانی است که اتحادیه بین‌المللی مخابرات تعریف کرده است. این استاندارد، رویه‌ها و پروتکل‌هایی را بررسی می‌کند که اعضای «شبکه همگانی تغییر مسیر خطوط تلفن» با آنها، در سراسر یک شبکه دیجیتالی برای ایجاد، تعیین مسیر و کنترل پیام به تبادل اطلاعات می‌پردازند. استاندارد SS7 در اصل برای مجموعه محدودی از شرکت‌های مخابراتی طراحی شده بود، اما در این اواخر، شاهد گسترش روزافزون خدمات جدید در این شبکه بوده‌ایم و شمار فروشندگان SS7 که محصولات نرم‌افزاری و سخت‌افزاری را عرضه می‌کنند به‌شدت افزایش یافته است. این روند لاجرم تا حد زیادی انتشار و توزیع اطلاعات و استانداردسازی

1. Emergency Systems
2. Common Channel Signalling System 7
3. Internet Protocol (IP)
4. SS7 IP Gateway

آن را ارتقا می‌دهد و در کل، بر آسیب‌پذیری این سیستم جهان‌گستر می‌افزائد؛ در حال حاضر، تعداد زیادی از بازیگران دیگر نیز در این حوزه فعالیت دارند؛ در این میان، این وضعیت، فرصت‌هایی را برای وقوع حملات که مسبب آنها نیز خودی‌ها هستند، فراهم آورده است. نکته مهمی که در اینجا باید بر آن تأکید کرد، ارتباط نزدیک به‌نسبت جدیدی است که میان سیستم‌های سنتی مخابرات و شبکه‌های اطلاعاتی دیجیتال پدیدار شده است: رهگیری خطوط تلفن با شبکه پروتکل اینترنت، به‌نسبت آسان‌تر از رهگیری خطوط تلفن با SS7 است. در برخی موارد، فایروال‌های[1] فعلی SS7، کافی و کاملاً مطمئن نیستند، این «فایروال‌ها» به قالب‌های خارج از پروتکل اینترنت اجازه می‌دهند از راه ورودی پروتکل اینترنت وارد شبکه تلفن شوند. به‌عبارت کلی‌تر، اگر SS7 نیز کنار گذاشته شود، بسیاری سیستم‌های فعلی تلفن را می‌توان با ارتباط‌های شبکه‌ای فایروال‌ها از فاصله‌ای دور مدیریت کرد. این سیستم‌ها بر روی رایانه‌های بسیار پیشرفته‌ای نصب می‌شوند که سیستم عامل‌های استانداردی را به‌کار می‌اندازند و البته، آسیب‌پذیری‌های آشکار و شناخته شده‌ای هم دارند. یکی از پیامدهای احتمالی نفوذ در این سیستم‌ها کنترل غیرقانونی تماس‌ها یا دست‌کاری مسیرهای تماس در مکالمات تلفنی می‌باشد.

یکی دیگر از نمونه‌های بارز آسیب‌پذیری در این حوزه، به ساختار انتقال و جابه‌جایی در شبکه‌های تغییر خطوط تلفن مربوط می‌شود. شبکه‌های نوری هم‌زمان[2] بسیاری از تأسیسات شبکه فیبر نوری را به‌نحو مناسبی سازمان‌دهی می‌نمایند. این شبکه‌ها از خدمات «شیوه انتقال غیرهم‌زمان»[3] نیز حمایت می‌کنند. در شبکه‌های نوری هم‌زمان، بسیاری از این عناصر با ارتباطات شبکه‌ای داده‌ها ـ که البته گاهی اوقات در برابر نفوذهای الکترونیک، آسیب‌پذیرند ـ از فواصل دور مدیریت می‌شوند؛ همچنین، این امکان نیز وجود دارد که مراکز نگهداری و کنترل وسایل و دستگاه‌های شبکه مورد حمله قرار گیرند. هرچند به‌علت دگرگونی در فناوری‌ها ممکن است این سناریو در این

---

۱. Firewall: بخشی از یک سیستم رایانه‌ای است که از دستیابی بدون مجوز افراد به اطلاعات جلوگیری می‌کند اما امکان دریافت اطلاعاتی را که به آنها ارسال می‌شود، برایشان فراهم می‌نماید.

2. Synchronous Optical NETworks (SONET)

3. Assynchronous Transfer Mode (ATM)

روزها کمتر موضوعیت داشته باشد، اما باید گفت در گذشته، علت اصلی قطع گسترده شبکه، حمله سایبر به شبکه بود.

یکی دیگر از نمونه‌های آسیب‌پذیری، به سیستم‌های اضطراری مربوط می‌شود. در آوریل ۲۰۰۰ مرکز حفاظت از زیرساخت‌های ملی «هشدارنامه‌ای» را در مورد نوشته «۹۱۱»[۱] که ماهیتی خود ـ رواج‌دهنده دارد، منتشر کرد. این نوشته از طریق هر چهار شرکت اصلی ارائه‌دهنده خدمات اینترنتی در آمریکا که هزاران رایانه از آنها تغذیه می‌کنند، اشاعه یافته است. سیستم‌های قربانی، شماره ۹۱۱ را خواهند گرفت؛ همین امر، مشکلاتی را برای مقامات مسئول به‌وجود می‌آورد و باعث می‌شود که آنها تعداد زیادی از شماره‌های تماس غلط را چک کنند و در نتیجه، بار سنگینی را بر این زیرساخت تحمیل می‌کند.

حملات به سیستم «هماهنگ‌سازی و توزیع در ارائه خدمات»[۲] در این وضعیت، وقتی تعداد زیادی پیام‌های درخواست به‌سمت سرورها هجوم می‌آورند، سرورها نمی‌توانند به این همه پیام پاسخ دهند، چرا که پیام‌ها از موقعیت‌های متعددی در اینترنت به سرورها ارسال می‌شوند و در برخی موارد خسارت‌های مالی جدی و قابل ملاحظه‌ای را به دنبال داشته‌اند. این وضعیت در فوریه ۲۰۰۰ نیز روی داد. در این تاریخ، چند حمله پرسروصدا برخی از وب‌سایت‌های مهم تجارت الکترونیک در اینترنت را به‌طور موقت از کار انداخت؛ به‌نظر می‌رسد ابزارهای پیشرفته سیستم «هماهنگ‌سازی و توزیع رد ارائه خدمات» نیز در مسیر توسعه، آزمایش و استقرار در اینترنت قرار گرفته‌اند.

در قسمت قبلی، به سیستم‌های «کنترل نظارتی و دستیابی به داده‌ها» اشاره شد. این سیستم‌ها همراه با «سیستم‌های کنترل توزیع شده»[۳] جزئی از «سیستم‌های کنترل صنعتی» به‌شمار می‌آیند که در بیشتر مواقع برای اداره و نگهداری از زیرساخت‌های حساس به‌کار می‌روند. این سیستم‌ها، که برای دستیابی به داده‌ها (با کنترل حسگرها) و کنترل (با

---

۱. کنایه به یازده سپتامبر، ۲۰۰۱/۰۹/۱۱؛ اما ۹۱۱ در ایالات متحده آمریکا شماره تلفن خدمات اضطراری (اورژانس و فوریت‌ها) است.

2. Coordinated Distributed Denial Of Service (DDOS)

3. Distributed Control Systems

ابزارهای مکانیکی خاص)[1] مورد استفاده قرار می‌گیرند، کارویژه‌های مهمی را درزمینه ارائه خدمات اساسی در حوزه‌های تولید و توزیع برق، زیرساخت آب‌رسانی، سیستم‌های دفع زباله و صنایع نفت و گاز انجام می‌دهند. این شبکه‌های کنترل‌کننده از همان ابتدا با این هدف طراحی شده‌اند که کارآمدی در این حوزه‌ها را ارتقا بخشند، اما این شبکه‌ها به موضوع امنیت در این حوزه‌ها که در بسیاری موارد یا اصلاً وجود ندارد یا ضعیف است توجه نکردند.

در گذشته، موضوع امنیت به‌عنوان معضل به‌شمار نمی‌آمد چرا که هیچ پیوند و اتصالی با شبکه‌های دیگر نداشت و اساساً فقط با عملگرهای مجاز که روی زیرساخت‌های اختصاصی[2] نصب می‌شوند، قابل دسترسی بود. اصولاً ساختار قدیمی برای دورهٔ گذر[3] از دنیای قیاسی[4] به جهان دیجیتال که در حال حاضر در روند است، طراحی نشده بود. «سیستم‌های کنترل» جدیدتر که از سیستم کنترل نظارتی و دستیابی به داده‌ها استفاده می‌کند به‌شدت به فناوری‌های اطلاعاتی دیجیتالی که ابزارهای نرم‌افزاری، سیستم‌های عامل و پروتکل‌های ارتباطی استانداردی را به‌کار می‌گیرد، متکی است. در برخی موارد، این سیستم‌های کنترل با شبکه فراگیر دیگری پیوند دارد و به شیوه‌ای عمل می‌کند که پیش از این، هرگز بدان منظور طراحی نشده بود. در نتیجه، «سیستم‌های کنترل» جدید، آسیب‌پذیری‌های بخش فناوری اطلاعات را به ارث می‌برند و در معرض حملات سایبر قرار می‌گیرند. در بیشتر مواقع، سیاست‌ها درزمینه مدیریت «رمزهای عبور»[5] کافی نیست و هیچ حفاظتی نیز از آنها در برابر ایجاد اختلال یا دست‌کاری در داده‌ها انجام نمی‌گیرد؛ ازاین‌رو سیستم‌های عامل تجاری و پروتکل‌های ارتباطی دارای ضعف‌های مشهود و مشخصی است و بیشتر مواقع نیز هیچ حفاظتی از آنها در برابر کلاهبرداری در ارتباطات اساسی‌ای که کم‌اهمیت تلقی می‌شوند، انجام نمی‌گیرد.

برخی از کنترلگرهای[6] منطقی نیز حتی شکست می‌خورند و کنترل دستگاه و سیستم رایانه‌ای را از دست می‌دهند؛ و در نتیجه، ویروس‌ها و کرم‌های رایانه‌ای به‌طور ویژه

---

1. Actuaters
2. Dedicated
3. Transition
4. Analogue World
5. Passwords
6. Controller

برای هدف قرار دادن «زیرساخت‌های کنترل نظارتی و دستیابی به داده‌ها» طراحی می‌شوند.

۳-۴ کنشگران: چگونه و چه کسانی

نمونه‌های قسمت قبلی نشان می‌دهد زیرساخت ارتباطات اساسی، از جمله شبکه‌های تلفن و اینترنت، در شرایطی معین تا چه اندازه می‌توانند آسیب‌پذیر باشند؛ باید خاطرنشان کرد بخش‌های دیگر به‌علت فعالیت‌های عادی روزمره‌ای که دارند به این شبکه‌ها وابسته‌اند. همه زیرساخت‌های حساس با شبکه‌های ارتباطاتی بیش‌ازپیش به یکدیگر پیوند خورده‌اند و درهم‌تنیده شده‌اند. این روند به‌نسبت جدید، کارایی این زیرساخت را در سطح جهانی افزایش می‌دهد، اما به‌عنوان پیامدی جانبی، از انعطاف‌پذیری آن می‌کاهد؛ همه اذعان کرده‌اند که وابستگی متقابل و به هم پیوستگی، آسیب‌پذیری‌های جدیدی را به بار می‌آورد. مدیریت سیستم‌های درهم‌تنیده و پیچیده، به‌ویژه به دلیل وابستگی‌های متقابلی که میان آنها وجود دارد، کاری بس دشوار است. اگر از چشم‌انداز امنیتی به این مسئله بنگریم، خطرات در سطوح مختلف وجود دارد؛ این خطرات از جرائم عام[1] مثل کلاهبرداری‌ها یا فعالیت‌های مجرمانه‌ای که در آنها از شبکه اینترنت استفاده می‌شود، تا خرابکاری، رهگیری، مزاحمت و اخلالگری در اینترنت را دربرمی‌گیرد. طیف اهداف نیز بسیار گسترده است و از افراد تا نهادها را شامل می‌شود.

اگر بحث را فقط به بخش فناوری اطلاعات محدود سازیم، احتمال دستبرد و دزدی در سطوح کاربر، رایانه و شبکه، بالاست. به‌آسانی می‌توان انواع و اقسام وسایل و ابزارآلات دستبرد در رایانه‌ها را در اینترنت یافت؛ این ابزارآلات به‌قدری پرشمار و متنوع (و بیشتر مواقع، پیچیده)اند که برای طبقه‌بندی آنها می‌باید نوعی رویکرد جانورشناختی اتخاذ کرد. برای مثال، می‌توان براساس برنامه‌های «اسکنر»،[2] انواع شبکه‌های اینترنتی را طبقه‌بندی کرد و محتوای بسته‌هایی را که خطوط اطلاع‌رسانی برنامه‌های رایانه‌ای سارق‌یاب[3] را می‌پیمایند، رهگیری و بررسی نمود. این احتمال نیز وجود دارد که

1. Generic Crimes
2. Scanner
3. Sniffer

ابزارآلات به «سرویس نام عرصه»[۱] دستبرد زنند یا آن را مختل کنند و یا گسترده‌ترین اختلالات را به‌وجود آورند به‌نحوی‌که می‌توانند حتی قابلیت دسترسی به شبکه اینترنت را به‌شدت کاهش دهند. در شرایط معینی می‌توان رایانه‌ها یا دستگاه‌های شبکه اینترنت را از راه دور مختل کرد یا از کار انداخت و یا بعضی از کارکردهای آنها را محدود ساخت. این امکان نیز وجود دارد که به‌منظور دسترسی به سیستم‌های رایانه‌ای، از «برنامه‌های رمز عبورگشا»[۲] استفاده کرد و یا رمز را در فضای حافظهٔ ذخیره شده یا محافظت نشده پیاده نمود. ما می‌توانیم اسب‌های تروا،[۳] ویروس‌ها یا کرم‌ها را (که به‌طور خود ـ سامان، نسخه‌های بدل خودشان را به روی شبکه انتقال می‌دهند) به این فهرست خطرات اضافه کنیم.

به‌طورکلی، دو مرحله اصلی در انجام حمله در روند جنگ اطلاعاتی وجود دارد: گام اول، ترسیم مفصّل نقشه یک شبکه می‌باشد؛ در این مرحله، برای ارائه هرگونه تحلیل در مورد آسیب‌پذیری، داده‌های مربوط به برنامه‌های فعال شبکه گردآوری می‌شوند. در این خصوص، بسیاری از شبکه‌هایی که در مقیاس جهانی فعالیت دارند، به‌وجود فعالیت نقشه‌برداری، که کم‌وبیش مرتب و یکدست است و بیشتر مواقع، منابع ناشناخته‌ای هم آن را انجام می‌دهند، پی می‌برند. در مرحله دوم، سلاح نرم‌افزاری مناسب با داده‌ها عرضه می‌شود. عرضه سلاح نرم‌افزاری به معنای فعال شدن آن نیست؛ فعال‌سازی بعد از این مرحله با برنامه‌ای خاص و در زمانی معین و در شرایطی مشخص و منطقی انجام می‌شود. در برخی موارد، برای پی بردن به میزان توانمندی‌های دفاعی سیستم‌هایی که مورد حمله قرار می‌گیرند، می‌توان واکنش‌هایی را از پیش در برابر حمله به‌صورت آزمایشی انجام داد.

کنشگران درگیر در این‌گونه فعالیت‌ها چه کسانی‌اند؟ در اینجا نیز باز طیف کنشگران، بسیار گسترده است. هرچند قصد ما این نیست که طبقه‌بندی جامع و مانعی را ارائه دهیم، اما می‌توان در میان کنشگران، چند طبقه کلی را از یکدیگر تمیز داد.

---

۱. Domain Name Service (DNS) کارویژه اصلی این سیستم، تبدیل آدرس‌های پروتکل اینترنت به نام‌های رایانه‌ای است.

2. Password Cracker

۳ Trojan Horses: برنامه‌های رایانه‌ای کاربردی بدلی.

رسانه‌هایی مثل تلویزیون یا روزنامه‌ها در بیشتر مواقع به هکرهای (سارقان اینترنتی) معلوم‌الحال که ممکن است حرفه‌ای، مبتدی و یا افراد اهل تفنّن[1] باشند در میان کنشگران وجود دارند، آنهایی که اهل تفنن‌اند بیشتر مواقع، هیچ سوءنیت آشکاری ندارند، بلکه فعالیت‌های خود را نوعی عرض اندام شخصی می‌دانند. گروه دوم، خودی‌هایی می‌باشند که بیشتر به جاسوسی در بخش‌های صنعتی و اقتصادی و شرکت‌ها و بنگاه‌ها می‌پردازند؛ محرک این گروه بیشتر، مسائل مالی یا انتقام‌جویی است و می‌توانند تهدید چشمگیری برای سازمان‌ها ایجاد کنند. گروه سوم، تبهکارانی‌اند که به اراده خود یا در چارچوب قواعد سازمانی و تشکیلاتی فعالیت می‌کنند. برای مثال، آنها منابع اطلاعات مالی را هدف قرار می‌دهند. شرکت‌ها و مؤسساتی که با جدیتی هرچه تمام‌تر به دنبال کشف اسرار تجاری رقبای خود هستند و در بیشتر مواقع از همان اعضای گروه رقیب استفاده می‌کنند، در این مقوله می‌گنجند. وانگهی، گروه‌های دولتی و غیردولتی نیز وجود دارند که انگیزه‌ای سیاسی در فعالیت‌های آنها نهفته است. این گروه‌ها از سازمان‌های جاسوسی ـ اطلاعاتی یا واحدهای نظامی گرفته تا گروه‌های تروریستی را دربرمی‌گیرند؛ اهداف این گروه‌ها می‌تواند اموری از قبیل گردآوری اطلاعات، تبلیغات، نظارت الکترونیک، سانسور و خرابکاری باشد.

در مورد منابعی که برای چنین فعالیتی ضروری‌اند، باید خاطرنشان کرد حتی اگر هزینه ورود به شبکه و ریزرایانه‌ها به‌نسبت پایین باشد، برای اینکه بتوان به یک کنشگر مهم در این بافت تبدیل شد، علاوه‌بر بهره‌مندی از میزان بالای مهارت فنی و دسترسی به منابع فراوان، گردآوری اطلاعات نیز لازم می‌باشد.

۵-۳ پرسش‌ها و دیدگاه‌هایی که هنوز جای بحث دارند

قبل از آنکه برخی از دیدگاه‌های عام را مطرح نماییم، اجازه دهید بار دیگر به گزارش اکتبر ۱۹۹۷ کمیسیون حفاظت از زیرساخت‌های حساس رجوع کنیم و چکیده‌ای از اهداف استراتژیک ایالات متحده آمریکا را آن‌چنان‌که در این سند تنظیم شده است، ارائه دهیم. این گزارش اذعان می‌کند که توانمندی وسیعی برای بهره‌برداری از آسیب‌پذیری‌های زیرساخت‌ها وجود دارد و تصریح می‌کند جامعه آن‌چنان‌که باید و

---

۱. افرادی که شب‌گذرانی در مقابل صفحه نمایشگر رایانه و نفوذ در سیستم‌های الکترونیک را دوست دارند.

شاید آگاهی چندانی در مورد این موضوع ندارد؛ علاوه‌بر این، به اقدامات گوناگونی که دولت انجام داده است، اشاره می‌کند. اولاً، این مسئله باید به‌نحو دقیق‌تری تعریف شود. برای تدوین یک استراتژی دقیق درزمینه حفاظت از زیرساخت‌های حساس، ضروری است که این زیرساخت‌ها به‌صورت نظام‌مندانه‌ای بررسی شوند و علاوه‌بر این، ارزیابی بسیار مبسوطی نیز در مورد آنها انجام گیرد. وجود درهم‌تنیدگی میان سیستم‌های مختلف و نیز وضعیت وابستگی متقابل میان جهان‌های فیزیکی و سایبر می‌باید به‌صورت تفصیلی تحلیل گردند تا بتوان ارزیابی دقیقی از میزان آسیب‌پذیری زیرساخت‌ها ارائه داد. پیچیدگی این مسئله نیز می‌باید مورد توجه قرار گیرد. علاوه‌بر این، ضرورت دارد که سطح فعلی حفاظت و درجه ریسک‌ها نیز مشخص شود.

دومین گام منطقی، جمع‌آوری اطلاعات از دولت در یک‌سو و دارندگان و دست‌اندرکاران زیرساخت‌ها (برای مثال، شرکت‌های تلفن و ارائه‌دهندگان خدمات شبکه‌ای) در سوی دیگر است، به‌طوری‌که بتوان فهمی مناسب از اینکه دقیقاً «چه کسانی بر کدام بخش‌ها کنترل دارند» ارائه داد. به‌علاوه، برای اینکه بفهمیم چه کسانی حق اقدام دارند، باید زیرساخت‌ها را برحسب اینکه کدام مرجع (بخش دولتی، بخش خصوصی، یا ترکیبی از این دو به‌صورت مشترک) مسئولیت اداره آنها را برعهده دارد طبقه‌بندی کنیم. این سند، آغاز هماهنگی تنگاتنگ میان بخش خصوصی و دولتی و همکاری میان دولت و صنایع را خاطرنشان می‌سازد و از مشارکت این دو بخش برای ایفای نقش درزمینه حفاظت از زیرساخت‌های مهم و خاص حمایت می‌کند و آن را ترویج می‌دهد. حکومت باید رهبری فعالیت‌های مرتبط با مدیریت امنیت اطلاعاتی را برعهده گیرد، هماهنگی میان نهادهای ذی‌ربط را ارتقا دهد و به‌منظور افزایش کارآمدی امور حفاظتی، منابع مالی لازم را برای قانونگذاری درزمینه توسعه چارچوبهٔ قانونی فراهم نماید.

آگاهی ملی در مورد تهدیدها و آسیب‌پذیری‌های فراروی زیرساخت‌ها نیز باید ارتقا یابد. ازاین‌رو می‌توان از تمهیداتی از قبیل آموزش و سایر برنامه‌های متناسب سود جست. در آغاز سال ۲۰۰۰، رئیس‌جمهور آمریکا در سخنرانی‌هایی که برای عامه مردم ایراد نمود به این موضوع توجه کرد. گزارش کمیسیون حفاظت از زیرساخت‌های حساس اعلام کرد، برای حفاظت از این زیرساخت‌ها، دولت باید توانمندی ملی هشدار درزمینه

حملات سایبر را به‌دست آورد به‌طوری‌که با این توانمندی بتوان فوراً و هم‌زمان، حملات نافرجام سایبر علیه زیرساخت‌های حساس را کشف کند. هدف، همانا نظارت، ارائه هشدارهای اولیه، فرمان آماده‌باش و انجام واکنش سریع به‌منظور تجدید سازمان یک زیرساخت کارآمد می‌باشد. این گزارش همچنین توصیه کرد که حجم سرمایه‌گذاری در حوزه تحقیقات و طراحی درزمینه ضریب امنیت زیرساخت‌ها از ۲۵۰ میلیون دلار به ۵۰۰ میلیون دلار در سال ۱۹۹۹ افزایش یابد و طی یک دوره پنج‌ساله تا سال ۲۰۰۴ به یک میلیون دلار برسد. این سند جامع، حاوی جزئیات بسیار جالبی است. هرچند دیدگاه‌های متفاوتی در مورد این موضوع وجود دارد، اما باید اذعان کرد که این کمیسیون دولتی سهم زیادی در ارائه این گزارش داشت و ازاین‌رو، جایگاه آن را نمی‌توان دست‌کم گرفت.

در ژانویه ۲۰۰۰، کاخ سفید «طرح ملی حفاظت از سیستم‌های اطلاعاتی» را ارائه داد. این طرح، تلاشی درزمینه طراحی شیوه‌ای برای حفاظت از فضای سایبر به‌شمار می‌آید. طرح مذکور را می‌توان بسط و گسترش گزارش کمیسیون حفاظت از زیرساخت‌های حساس (که مسلماً نقطه آغازی در این عرصه بوده است) محسوب کرد. این طرح به‌نحوی بسیار زیرکانه و دقیق از آن دیدگاه‌های استراتژیکی که در گزارش ۱۹۹۷ آمده است، پیروی می‌کند و پیشنهادهایی درزمینه طراحی و تحقیقات فنی و برنامه‌های آموزش را در خود گنجانده است؛ علاوه‌بر این، از فعالیت‌هایی که به افزایش آگاهی عمومی می‌انجامد و حفاظت از آزادی‌های مدنی و حفاظت از داده‌های انحصاری ـ اختصاصی را تضمین می‌کنند حمایت می‌نماید. مشارکت بخش‌های خصوصی و دولتی با هدف ایجاد پایگاهی برای دفاع سایبر به‌شدت تشویق شده است. قرار بود این طرح تا قبل از اواسط سال ۲۰۰۳ به‌طور کامل عملیاتی شود؛ به‌نظر می‌رسد دولت فعلی ایالات متحده اساساً همین دیدگاه‌های موجود در این بحث را دارد. گذشته از ایالات متحده، چند کشور دیگر نیز در حال حاضر اولین گام‌ها در عرصه تحلیل مبسوط زیرساخت‌هایشان را برمی‌دارند و در این میان، توجه خود را به وابستگی‌های متقابل میان زیرساخت‌ها و آسیب‌پذیری‌های آنها معطوف ساخته‌اند.

به‌رغم همه فعالیت‌هایی که در این حوزه انجام گرفته است، چند پرسش بی‌پاسخ و

برخی مسائل حل نشده و مهم همچنان باقی مانده‌اند. در ذیل، بعضی موضوعات به‌طور مختصر مورد بحث و بررسی قرار خواهند گرفت، اما بسیاری از جزئیات و تحلیل‌های مبسوط‌تر را می‌توان در قسمت منابع و مآخذ که در پایان این فصل آمده است یافت، که توجه خواننده را به مطالعه آنها جلب می‌کنیم. مسئله اول، در مورد مشارکت اطلاعاتی میان بخش‌های خصوصی و دولتی است؛ کاملاً آشکار و مشهود است که برای نیل به هدف تحلیل و نظارت متمرکز، لاجرم باید نوعی مشارکت اطلاعاتی، حداقل در سطحی معقول میان این دو بخش انجام گیرد. این مشارکت به دلایل متعددی می‌تواند مشکل‌آفرین باشد؛ یکی از دلایل اصلی این امر، حساسیت اطلاعات مشترک و منافع و علایق احتمالاً متفاوت این کنشگران می‌باشد. سازمان‌ها و نهادهای امنیتی معمولاً اکراه دارند که اطلاعات طبقه‌بندی شده و محرمانه را منتشر نمایند؛ صنایع نیز که در بازار باهم رقابت می‌کنند ترجیح می‌دهند اسرار تجاری و اطلاعات انحصاری ـ اختصاصی خود را مخفی نگه دارند.

اگر ما شرکت‌های خارجی یا چندملیتی را نیز در نظر بگیریم، این وضعیت حتی پیچیده‌تر می‌گردد. این امکان وجود دارد که مسئولیت‌های دولت و بخش خصوصی با یکدیگر در تعارض قرار گیرد و منافع آنها نیز متفاوت و حتی متضاد باشد؛ نمونه‌ای که در گذشته اتفاق افتاد، اختلاف میان یک شهروند آمریکایی و وزارت خارجه آمریکا بر سر رمزگذاری اطلاعات[1] بود. موضوعات بحث‌برانگیز دیگر، سؤالات ذیل است: مسئولیت دولت به‌طور دقیق چیست؟ دفاع از کشور همواره حق مسلم و انحصاری دولت بوده است، اما این مسئولیت در حال حاضر، دیگر نه مطابق با واقع است و نه حتی عملی است؛ زیرا دیگر نمی‌توان با مداخله نیروهای نظامی، از بخش غیرنظامی جامعه به‌طور کامل حفاظت کرد. به‌علاوه، در این سناریوی جدید، مالکان و دست‌اندرکاران غیردولتی زیرساخت‌ها می‌باید نقش‌های مهمی در حفاظت از زیرساخت‌ها در برابر نفوذ بیگانه، کلاهبرداری‌ها یا حملات خارجی احتمالی ایفا نمایند. خط تفکیک میان مسئولیت‌های بخش‌های دولتی و خصوصی در کجا ترسیم شود؟ آیا اصلاً می‌توان چنین خطی را ترسیم کرد یا آیا تاکنون امکان‌پذیر شده است؟ همکاری نزدیک میان شهروندان و

---

1. Encryption

نهادهای امنیتی ملی چه‌بسا ما را به‌سمت یک جامعه نظارت‌ـ محور[1] سوق خواهد داد.

در حال حاضر، که فرایند مقررات‌زدایی[2] اقتصادی در جریان است، این مسئله حتی پیچیده‌تر می‌شود. فرایند مقررات‌زدایی اقتصادی افزایش سطح آسیب‌پذیری در زیرساخت‌ها را به دنبال داشته است. ازهم‌گسستگی فزاینده سیستم‌ها کنترل هریک از عملگرها بر زیرساخت‌ها را کاهش می‌دهد، در بیشتر مواقع، حجم تولید را محدود می‌سازد و به‌طورکلی بر شکنندگی و بی‌ثباتی می‌افزائد. به‌ویژه در بخش مخابرات، ظهور میانجی‌های متعدد و جدید به حوزه‌ای که روزگاری پشت سر هم خدمات ارائه می‌داد، سطح وابستگی متقابل عملیاتی را حتی پیچیده‌تر می‌سازد. در نتیجه، مدیریت و ایجاد هماهنگی میان سیستم‌های پیچیده، بسیار دشوارتر می‌شود. گزارش کمیسیون حفاظت از زیرساخت‌های حساس و طرح ملی حفاظت از سیستم‌های اطلاعاتی در این میان، فعالیت‌های طراحی و تحقیقات درزمینه موضوعاتی مثل کنترل و کشف نفوذ در سیستم‌ها و تشخیص و واکنش در برابر وقایع را پیشنهاد می‌کند و از آن حمایت می‌نماید.

همان‌گونه که در بالا اشاره کردیم، دولت آمریکا قصد دارد توانمندی ملی خود را در مورد ارائه هشدار در برابر حملات سایبر افزایش دهد. در اینجا بررسی تفصیلی این طرح، جالب به‌نظر می‌رسد: تحقق این طرح، ظرفیت کنترل و نظارت تقریباً هم‌زمان بر زیرساخت‌های مخابراتی، توانایی شناسایی، گردآوری و ترسیم نابهنجاری‌های مرتبط با حملات و در نهایت، توانمندی ردگیری، مسیریابی و جداسازی سیگنال‌های الکترونیکی را که با یک حمله ارتباط دارند، ایجاد خواهد نمود، پیچیدگی در کل این سیستم، که مدام نیز تغییر می‌کند، اعلام هشدارهای تاکتیکی و ارزیابی حملات را به مسئله‌ای بسیار دشوار مبدل می‌سازد. تمایزگذاری میان «سطح اختلال» رویدادهای تصادفی روزمره از یک‌سو و حملات واقعی ازسوی‌دیگر و علاوه‌بر این، توانایی ردگیری منبع یک حمله چه‌بسا می‌تواند کاری دشوار باشد. در مورد این موضوع، گفتنی است که صنایع رایانه و شبکه‌سازی، محصولات و برنامه‌های رایانه‌ای کنترل نفوذ را تولید می‌کنند و علاوه‌بر این، جنبه تجاری به آن داده‌اند.

اگر قوانین درزمینه جلوگیری از سوءاستفاده از این تسهیلات و تأسیسات به‌درستی وضع نشوند، در آن صورت، خطر حرکت به‌سمت شکل‌گیری جامعه نظارت ـ محور چه‌بسا

---

1. Surveillence Society
2. Deregulation

حتی بیشتر خواهد شد. برای مثال، در ایالات متحده آمریکا، کشمکش چه‌بسا بر سر «اصلاحیه چهارم» خواهد بود. این اصلاحیه از امور شخصی و زندگی خصوصی افراد در برابر تعدّیات غیرموجه حکومت حفاظت و حمایت می‌کند. جا دارد به کشمکش‌های احتمالی در عرصه قانونگذاری و بحث‌ها و مجادلات بر سر حدود اختیارات و صلاحیت‌های دولت اشاره کنیم. این مسئله یک حوزه موضوعی جدیدی است که بحث علنی در مورد آن، بسیار جالب خواهد بود. می‌توان این سؤال را از خود پرسید که آیا کنشگران، علاوه‌بر ابزارها و فنون دفاعی، توانمندی‌های تهاجمی را نیز در حوزه جنگ اطلاعاتی به‌طور فعالانه در خود ایجاد می‌نمایند. مرز میان امنیت ملی و امنیت بین‌المللی مانند تمایز بخش‌های نظامی و غیرنظامی هر روز کم‌رنگ‌تر می‌شود.

۶-۳ نتیجه‌گیری

کمیسیون حفاظت از زیرساخت‌های حساس هیچ مدرکی دال بر وجود حمله قریب‌الوقوع سایبر ـ که تأثیر مخربی بر زیرساخت‌های حساس دارد ـ نیافت (بنابراین، در آن زمان، هیچ تهدید قریب‌الوقوعی مشاهده نشده است)؛ اما می‌توان اذعان کرد که توانمندی‌های گسترده‌ای برای بهره‌برداری از آسیب‌پذیری‌های زیرساخت‌ها وجود دارد. البته، مانند بسیاری از بحث‌ها و مناظره‌های دیگر، دیدگاه‌های تندروانه‌ای نیز وجود دارد؛ بعضی تصور می‌کنند هکرها (سارقان اینترنتی) در آستانه نابودسازی زیرساخت‌های اساسی در کشورهای توسعه‌یافته‌اند. اما بعضی دیگر درباره این ادعا تردید دارند و معتقدند طرح این سناریوی فاجعه‌بار فقط جنبه شعاری دارد و هدف از این‌گونه ادعاها، جذب حجم عظیمی از بودجه دولت آمریکا برای پیشگیری از روی دادن این فرضیه‌های مهمل است. سناریویی که در قسمت‌های قبل ترسیم شده بسیار پیچیده است و این پیچیدگی نیز ازنظر خواننده پنهان نمانده است؛ چرا که این امکان را برای خواننده فراهم می‌کند تا تصویری کلی از وضعیت امنیت اطلاعاتی به‌دست آورد. ازاین‌رو، فصل حاضر می‌کوشد درآمدی بر این موضوع ارائه دهد. برای جلوگیری از اطاله کلام، بسیاری از بحث‌ها به‌صورت مختصر و بسیار ساده اشاره شده‌اند و به همین دلیل، بررسی برخی از آنها از قلم افتاده است. برای آنکه از دام پیچیدگی‌های مباحث دور بمانیم، تلاش

خواهیم کرد توجه خود را به برخی واقعیت‌ها و ارائه شرحی مختصر از بعضی عناصر و عوامل مهم متمرکز سازیم.

با توجه به تحولات اخیر و نوظهور درزمینه دیجیتالی شدن امور در کشورهای صنعتی شده، مسلم و بدیهی است که زیرساخت‌های حساس وابستگی فزاینده‌ای به سیستم‌های اطلاعاتی و فناوری‌های ارتباطی شبکه‌ای از خود نشان دهند؛ این وابستگی در بسیاری از سطوح، منبع آسیب‌پذیری است. اتکای فراگیر به فناوری‌های مبتنی‌بر اطلاعات، حجم بی‌سابقه‌ای از به‌هم پیوستگی و وابستگی متقابل را در مقیاسی جهانی به‌وجود آورده، به‌طورکلی مدیریت را پیچیده‌تر ساخته، اختلال‌های بالقوه‌ای را به بار آورده و مانند واکنش زنجیره‌ای، تأثیرات آن به تمامی ابعاد زندگی بشری سرایت کرده است. به‌علاوه، اگر ازمنظر امنیتی بنگریم، این سرایت و نیز روند فعلی ادغام زیرساخت‌های حساس سنتی و زیرساخت‌های اطلاعاتی باعث افزایش آسیب‌پذیری آنها در سراسر جهان شده است؛ این آسیب‌پذیری‌ها بیشتر در برابر حملات الکترونیکی نمود می‌یابند، حملاتی که تا پیش از مقطع کنونی، فقط به بخش فناوری اطلاعات محدود می‌شدند.

در میان‌مدت، توسعه ابزارهای پیشرفته و ابداع سیستم‌های مقاوم‌تر می‌تواند این آسیب‌پذیری را کاهش دهد. با توجه به اینکه اخیراً تلاش‌هایی در این جهت انجام گرفته است، امیدواریم این وضعیت نیز تحقق یابد. در حال حاضر، بدیهی است که وقوع حملات سایبر با سطوح پیچیدگی متفاوتی که دارد، ازنظر فنی امکان‌پذیر است. نه تنها بروز این حملات امکان‌پذیر است، بلکه در هر زمان و در شبکه‌های جهان‌گستر روی می‌دهد. برآورد پیامدهای این‌گونه حملات، که بیشتر مواقع فقط ماهیت اقتصادی هم ندارد، دشوار است.

هر کارشناس امنیت رایانه یا شبکه کاملاً بدیهی می‌داند که زیرساخت‌های فناوری اطلاعات در برابر یک حمله محدود نیز حداقل در سطح محلی، بسیار آسیب‌پذیرند. ایجاد اختلال‌های موقتی یا اندک چه‌بسا می‌تواند تا حدودی آسان باشد. اما اگر حملات در مقیاس وسیع‌تری انجام گیرند، ارزیابی درجهٔ ریسک و آسیب‌پذیری‌های مرتبط با آن، بسیار دشوار است. ارزیابی تأثیرات عملکرد و ارتباطات داخلی میان سیستم‌ها و زیرساخت‌های بسیار گوناگون و متنوع چه‌بسا کاری بسیار پیچیده و دشوار است. تنها در

حال حاضر است که ما نحوه کنترل سیستم‌هایی با سطح بالای پیچیدگی را می‌آموزیم.

در این بافت، آن فعالیت‌های جاسوسی و نظامی را که در قالب نقش‌های تدافعی و تهاجمی انجام می‌گیرند، نمی‌توان نادیده گرفت. ازاین‌رو، برخی از کشورها آشکارا به این فعالیت‌ها توجه می‌کنند. بهره‌برداری از سطوح پیشرفته فناوری اطلاعات باعث ظهور پدیده‌ای شده است که بعضی افراد، آن را «انقلاب در امور نظامی» توصیف می‌کنند. برخی کشورها نیز به واکاوی تأثیرات احتمالی ایجاد اختلال در زیرساخت‌های اطلاعاتی دشمن بالقوه می‌پردازند. به‌طور قطع، امنیت ملی برای هر کشوری در جهان، مهم‌ترین و اصلی‌ترین اولویت به‌شمار می‌آید، ولی ضروری است توازنی بین این مقوله از یک‌سو و حق احترام به اسرار خصوصی و امنیت اطلاعات شخصی و تجاری در پهنه جهانی ازسوی‌دیگر برقرار شود. با توجه به ماهیت فراملی این مسئله و برای ارتقای امنیت سیستم‌های اطلاعاتی و مخابراتی که در مقیاسی جهانی فعالیت دارند، باید اصول بین‌المللی مشخصی در این زمینه شکل گیرد که مورد توافق همه کشورها نیز باشد.

قطعنامه‌های سازمان ملل متحد که به تصویب مجمع عمومی رسیده‌اند ضرورت تعریف مفاهیمی را که با «مداخله غیرمجاز» سروکار دارند و مصادیق سوءاستفاده از سیستم‌ها و منابع اطلاعاتی را مشخص می‌سازند، به رسمیت شناخته و پذیرفته‌اند. برای مثال، برخی از نهادهای بین‌المللی (سازمان ملل متحد، دیوان بین‌المللی دادگستری، گروه هشت، مذاکرات دوجانبه و چندجانبه یا سایر سازمان‌ها و نهادها) را می‌توان برای بررسی نحوه مقابله با اهداف غیرصلح‌آمیز بهره‌برداری از فناوری‌های اطلاعات و ارتباطات به‌کار گرفت. ماهیت شبکه‌های جهان‌گستر به‌گونه‌ای است که آنها پا را از حدود و مرزهای صلاحیت هر کشور نیز فراتر می‌گذارند، ازاین‌رو تدوین چارچوب قانونی مناسب برای وضع قوانین یکپارچه در این حوزه، ضروری است. تحقق این وضعیت در گرو ارائه تعریفی مشخص در مورد مسئولیت‌های هریک از کنشگران مختلف در این حوزه است. همکاری بین‌المللی نیز در سطوح مختلف می‌باید تقویت شود. برخی ابتکار عمل‌ها نشان می‌دهند که فعالیت‌ها و کارویژه‌های نظامی و غیرنظامی به‌سمت درهم‌تنیدگی و ادغام در یکدیگر پیش می‌روند. فناوری اطلاعات را می‌توان یکی از نمونه‌های بارز فناوری‌هایی قلمداد کرد که کاربردهای دوگانه دارند. بااین‌همه، باید خاطرنشان کرد بسیاری از

تحولات علمی و فنی در گذشته نیز چنین خصوصیتی داشتند و البته همچنان نیـز ایـن روند ادامه دارد. توسعه امور نظامی در سطح ابعاد سایبر در حال حاضر روند تکاملی خود را طی می‌کند. «سلاح اطلاعاتی» چه‌بسا در آینده فقط یک مفهوم مجـازی نخواهـد بـود. روند تکاملی این حوزه (که گسترده‌ترین فرصت‌های مثبت را شناسایی می‌کند) بایـد در چـارچوب امنیـت بـین‌المللـی دنبـال شـود؛ چـرا کـه از ایـن طریـق، مـی‌تـوانیم جلـو سوءاستفاده‌های احتمالی از این فناوری‌ها و به‌کارگیری آنهـا بـرای اهـداف تبهکارانـه را بگیریم و از تضعیف ثبات بین‌المللی ممانعت به‌عمل آوریم.

منابع و مآخذ

Centre for International Security and Arms Control, *Workshop on Protecting and Assuring Critical National Infrastructure*: Next Step, Stanford, CA: Stanford University, 1998.

Chapman, G. 'National Security and the Internet', Paper Presented at the Annual Convention of the Internet Society, Geneva, 1998.

Denning, D.E. Information Warfare and Security, Boston: Addison Wesley, 1999.

Joint Economic Committee US Congress, 'Security in the Information Age: New Challenges, New Strategies', Report of the Joint Economic Committee US' Congress, USA, 2002.

McClure, S.J. Scambray and G.Kurtz, Hacking Exposed, California: Osborne McGrawHill, 1999.

Molander, R.S. Riddile and P. Wilson , Strategic Information Warfare: A New Face of War, Washingtion RAND: MR-GG1-OSD, 1996.

Neumann, P.G. Computer Related Risks, Boston: Addison Wesley Professional. ACM Press, 1995.

Northcutt, S.J. Novak and D. Mclachlan, Network Intrusion Detection: An Analyst's Handbook, 2nd edn, USA: New Riders Publishing, 2000.

President's Critical Infrastructure Protection Board, The National Strategy to Secure Cyberspace, Report of the President's Critical Infrastructure Protection Board USA, 2002.

Rathmell, A 'Cyber-Terrorism: The Shape of Future Conflict?', *Royal United Service Institute Journal*, October 1997.

Siroli, G.P. 'Strategic Information Warfare, Research Paper 2001/2, Geneva International Peace Research Institute (GIPRI), 2001.

Sun Tzu Ping Fa, and R.d. Sawyer, The Art of War: Sun-tzu Ping Fa, Boulder, CO: Westview Press, 1994.

بخش دوم

دلالت‌های مسئله

فصل چهارم جنگ مجازی فضیلت‌مندانه

ژاری رانتاپل کنن*

مقدمه

در سال ۲۰۰۱، ژنرال تامی فرانکس[1] رئیس ستاد فرماندهی مرکزی ایالات متحده و ملا محمد عمر، رهبر مذهبی طالبان، اتفاق‌نظر داشتند که جنگ علیه تروریسم، موضوعی سرزمینی نیست. رهبران امنیت ملی آمریکا جان دبلیو، رندان[2] را که یک کارشناس حرفه‌ای در امور تبلیغاتی است، استخدام کردند. وی به جرگه کسانی پیوست که به‌طور سنتی درگیر امور جنگی بودند (به‌عبارت بهتر، درواقع به اقتضای منصبی که داشت، در میان سیاست‌مداران، سربازان، دیپلمات‌ها و گزارشگران جای گرفت). آقای رندان در مورد نقش خود اظهار داشته است:

«من یک استراتژی‌پرداز امنیت ملی یا یک تاکتیک‌پرداز[3] نظامی نیستم ... من یک سیاست‌مدارم ... و فردی هستم که از ارتباطات برای اجرای سیاستگذاری‌های دولت و نیل به اهداف مشترک در سیاستگذاری‌ها استفاده می‌کنم. درحقیقت، من یک رزمنده اطلاعاتی‌ام و کسی هستم که اطلاعات و ادراک را مدیریت می‌کند. این جایگاه احتمالاً در گفته‌های هانتر اس. تامپسون[4] به بهترین نحو توصیف شده است. وی نوشت: «وقتی امور، غیرعادی و اسرارآمیز می‌گردند، این امور غیرعادی و اسرارآمیز (رفته‌رفته) حرفه‌ای می‌شوند ... .

اگر هریک از شما در عملیات آزادسازی شهر کویت (۱۹۹۱) شرکت می‌کردید ... یا آن را در تلویزیون مشاهده می‌کردید، هزاران کویتی را می‌دیدید که پرچم‌های کوچک

---

* Jari Rantapel Konen

1. Tomy Franks
2. John W. Rendon
3. Tactician
4. Hunter S.Thampson

آمریکا را در دست داشتند و تکان می‌دادند ... آیا شما هرگز از خود نپرسیده‌اید که مردم شهر کویت، پس از تحمل هفت ماه طولانی و دردناک اسارت، چگونه توانستند پرچم‌های آمریکا را به‌دست بگیرند؟ و به همین اعتبار، چگونه توانستند پرچم‌های سایر کشورهای ائتلاف را در دست گیرند؟ خوب، شما حالا جواب را می‌دانید. آن اقدام، یکی از کارهای من بود» (Miller and Rompton, 2001: P.11).

پنتاگون «گروه رندان» را برای کمک به ارتش آمریکا در عصر اطلاعات استخدام کرده بود. هدف از به‌کارگیری گروه رندان، این بود که این گروه تصویر مثبتی از جنگ به نمایش بگذارد و از این طریق به پیروزی آمریکا در نبرد جهان‌گستر برای جلب افکار و قلوب ملت‌ها کمک نماید. در اوایل سال ۲۰۰۲، گروه رندان با انعقاد قراردادی متعهد شد با اداره نفوذ استراتژیک[1] همکاری کند. هدف شرکت روابط عمومی رندان این بود که بکوشد شرایط مناسبی را برای برکناری صدام حسین یا تشویق به سرنگونی وی فراهم نماید (Dao and Schmitt, 2002).

این فصل توجه خود را به ارتباط میان اطلاعات، فناوری اطلاعات و جنگ متمرکز می‌سازد. دراین‌میان، کاربرد واژگان، تصاویر[2] و برداشت‌ها[3] در جنگ علیه تروریسم (یازده سپتامبر، افغانستان و عراق) با نگاهی انتقادی بررسی می‌شود. در این خصوص، روایت امنیت به‌عنوان شیوه تعیین آنچه واقعیت جهان‌شمول تصور می‌گردد، مورد توجه قرار می‌گیرد. بدین‌سان، واقعیتی که پدید آمده است، نتیجه استفاده از پدیده فراگیر فناوری اطلاعات به‌منظور تأمین امنیت ملی است. هدف این فصل،(۱) این است که حدود مدارا در جنگ اطلاعاتی را تشخیص دهد و علاوه‌بر این رئوس کلی آن را نیز تبیین نماید. البته، باید توجه داشت که منظور کشف حقیقت غایی نیست؛ بلکه برعکس، این فصل می‌کوشد نتایج احتمالی نگرش غیرانتقادی به (فناوری) اطلاعات و نیز آن استدلالات در مورد جنگ را که مبتنی‌بر اغراض ناصواب گوناگون است و تا حدودی هم از تناقضات کمک می‌گیرد بررسی کند.

جنگ علیه تروریسم به‌طورقطع، جنگ اطلاعاتی صرف نیست که تهدید، رنج، یا

---

1. Office of Strategic Influence
2. Images
3. Prceptions

مرگ واقعی در آن وجود نداشته باشد. این فصل مدعی نیست که جنگ علیه تروریسم را می‌توان تنها یک روایت کلان[۲] و انگاره‌ای ذهنی تصور کرد. علاوه‌بر این، قصد ندارد بگوید که وقایع واقعی از قبیل دیکتاتوری رژیم صدام حسین بر اقتباس روایت کلان جنگ علیه ترور تأثیر نمی‌گذارد، بلکه هدف، ارزیابی انتقادی روایت‌هایی است که واقعیت را ساده می‌انگارند و مبتنی‌بر این فرض است که وقتی یک دولت، ملت و متحدان خود را به‌نحوی گسترده بسیج می‌کند (که این اقدام معمولاً با کمک حمایت رسانه‌ای انجام می‌گیرد) روایت‌های منتج از آن از جنبه‌های متعددی کاملاً مشکل‌آفرین‌اند.

۱-۴ نظریه، فناوری اطلاعات و تصادف

برای آنکه اعتبار قابل قبولی به این بحث ببخشیم، طرح دو دیدگاه نظری در اینجا ضروری است. ابتدا، بخش را براساس نظریه جنگ فضیلت‌مندانه جیمز در دریان بررسی می‌کنیم. به‌نظر در دریان نبردهایی که در واقعیت مجازی انجام می‌گیرد، به مدل جنگ واقعی شکل می‌دهد (Der Derian, 2001). در کانون جنگ فضیلت‌مندانه، عواملی از قبیل توانمندی‌های فنی برتر و نیز نوعی قاعده الزام‌آور اخلاقی (خوب در برابر بد) قرار دارد که تهدید به خشونت و درصورت لزوم، عملی ساختن خشونت از فاصله‌ای دور را توجیه می‌کند.

مدل جنگ مجازی، ماهیت فضیلت‌مندانه‌ای به جنگ می‌بخشد ـ یا درواقع، ماهیت فضیلت‌مندانه را به جنگ بازمی‌گرداند. در گذشته، تمایزگذاری میان واژگان «مجازی»[۱] و «فضیلت‌مندانه»[۲] و نیز تمایزگذاری میان جهان‌هایی که هریک از این دو واژه بازنمایی می‌کنند، تقریباً غیرممکن بود. استدلال‌های در دریان مبتنی‌بر بازی‌های جنگی است زیرا جنگ‌های شبیه‌سازی شده‌ای که در رایانه‌ها به‌صورت بازی درمی‌آیند و جنگ‌هایی که در صفحه‌های نمایشگر رایانه‌ها نمایش داده می‌شوند، هیچ تمایزی میان فناوری (جهان مجازی) و اخلاق (رویه‌های فضیلت‌مندانه) برقرار نمی‌سازند. جنگ فضیلت‌مندانه این احساس تناقض‌گونه را ایجاد می‌کند که جنگ می‌تواند بدون خونریزی، بشردوستانه و تمیز باشد.

---

1. Virtual
2. Virtouous

براساس مدل جنگ فضیلت‌مندانه، جنگ‌ها به شیوه‌ای که شهروندان، آنها را در شبکه‌های مجازی می‌بینند، به راه می‌افتند. کلیپ‌های واقعیت‌نمایی ویدئویی، با بهره‌گیری از فناوری برتر وارد تلویزیون‌ها و رایانه‌های شخصی می‌شوند. فناوری برتر، چارچوبی را برای جنگ‌های شبکه‌ای تقریباً بی‌خطر فراهم می‌کند. بررسی جوهره مدل جنگ فضیلت‌مندانه از وجود نیرویی عظیم در آنها پرده برمی‌دارد: این نیروی عظیم همانا شبکه «برنامه‌های سرگرمی رسانه‌ای براساس سناریوهای صنایع نظامی»[1] است. جنگ‌های دوره و زمانه ما با جنگ‌های آینده درآمیخته‌اند. این امر به آشفتگی واقعیت می‌انجامد. اخبار سی.ان.ان، فیلم‌های سینمایی هالیوود، دره سیلیکان[2] و بازی‌های جنگی دیجیتالی همه‌وهمه تصویر بسیار یک‌طرفه‌ای از جنگ را ترسیم می‌کنند.

جنگ شبیه‌سازی شده تنها می‌تواند رویه‌های جنگ واقعی را برای سربازان تعریف و مشخص کند، اما آیا این جنگ، واقعی است؟ رویای یک جنگ تمام‌عیار، بینندگان را با این پنداره به حال خود رها می‌کند که جنگ، مجازی است و به عبارتی، نوعی سرگرمی و درواقع، یک بازی است. در جنگ مجازی، فقط آبی، قرمز، یا قهوه‌ای و به‌عبارت‌دیگر، صفر و یک، که نمادهای تصویری در نمایشگر رایانه‌اند، وجود دارد و بنابراین، نه جسم انسان در کار است و نه خون و خونریزی. پرسشی که در دریان در مورد فناوری اطلاعات مطرح می‌کند، چیزی بیش از مسئله‌ای مرتبط با وقایع روز است: آیا جنگ، آسان‌تر خواهد شد و آیا برقراری صلح با خونریزی بیشتری همراه خواهد بود؟

در وهله دوم، ما آن دیدگاه‌های نظری را که برگرفته از سرعت‌شناسی[3] است و پل ویریلیو بیان کرده است به‌کار خواهیم گرفت. ویریلیو از سرعت شتابنده اطلاعات و فناوری مدرن انتقاد کرده است. وی نشان داده که برخی از تحولات فناورانه از کنترل خارج شده‌اند. ازنظر ویریلیو، فناوری اطلاعات و به‌طورکلی، تحولات فناورانه بی‌آنکه محتوای رویدادها را زیر سؤال ببرند، رویدادها را شتاب می‌بخشند.

این «شتاب» پیامدهای مهمی در پی دارد. به گفته ویریلیو (۱۹۸۶)، این ماشین جنگی جدید، نوعی غیب‌شدگی و به عبارتی نابودی دوگانه را به‌صورت توأمان به همراه

---

1. Military Industrial Media Entertainment (MIME)
2. Silicon Valley
3. Dromology (The Theory of Speed)

دارد: غیب شدن موضوع[1] و غیب شدن مکان.[2] در نهایت، هر فناوری، شکلی از خاص تصادف را دارد: وضعیت فوق‌العاده، نابودی نژاد بشر را به دنبال دارد و فناوری اطلاعات، فاصله را از میان برمی‌دارد؛ این امکان نیز وجود دارد که آنچه محلی است، با حقیقتی جهانی[3] که آن را بازنمایی می‌کند درمی‌آمیزد.

وقتی اندیشه‌های مندرج در نظریه سرعت را به‌کار می‌گیریم، توجه جدی به مفهوم تصویر نیز اهمیت می‌یابد زیرا: «از هم‌اکنون به بعد، هر چیزی با تصویر تجلی می‌یابد. تصویر بر موضوع[4] و گاهی اوقات حتی بر موجودات فیزیکی نیز اولویت دارد. همان‌طور که زمان بر مکان اولویت دارد. بنابراین، تصویر جنبه فراگیر و همه‌جانبه پیدا کرده و نقش آن فقط در حوزه هنر، عرصه نظامی یا حوزه فنی نیست، بلکه تصویر به‌عنوان یک واقعیت در همه‌جا وجود دارد» (Virilio, 1988, PP.4-7).

این وضعیت، به این اندیشه ساده‌انگارانه می‌انجامد که مجازیت، واقعیت را نابود می‌کند یا فناوری به‌عنوان راه‌حل نهایی، به‌جای واقعیت انسانی می‌نشیند. اطلاعات به‌صورت ارتباطات درمی‌آید؛ ارتباطاتی که در همه جا و هر زمان وجود دارد. البته، درهم‌تنیدگی پرسرعت آن نیز به معنای واقعی کلمه، جایگزین درهم‌تنیدگی کم سرعت‌تر نظام‌های سیاسی سنتی شده است. بمباران اطلاعات، تصاویر ذهنی، شایعات و دروغ‌پردازی‌ها را به واقعیت تبدیل می‌کند و کسانی که در مورد چشم‌انداز، دستور کار و تبعات جنگ می‌اندیشند همین واقعیت را به‌آسانی می‌پذیرند. وقتی از اطلاعات فقط برای تبیین موضوع مورد نظر استفاده می‌شود، آنگاه اطلاعات و اطلاعات گمراه‌کننده را می‌توان از یکدیگر تمییز داد، چرا که در چنین شرایطی، اطلاعات برای بیان محتوای مبتنی‌بر تجربه مورد استفاده قرار نمی‌گیرد. به کلام در دریان، واقعیت از شبکه «برنامه‌های سرگرمی رسانه‌ای براساس سناریوهای صنایع نظامی» به‌دست می‌آید نه از تجربه شخصی. بنابراین، پدیدارشناسی برداشت[5] به لجستیک‌شناسی[6] برداشت مبدل

---

1. Disappearance of Matter
2. Disappearance of Place
3. Global Truth
4. Object
5. Perception
6. Logistics

می‌شود که در آن، تصاویر جنگ با یکدیگر از راه فناوری جدید (فناوری‌های برداشت)، خود، جایگزین واقعیت می‌گردند.

به گفته ویریلیو، فناوری‌های جدید می‌کوشند واقعیت مجازی را از واقعیت واقعی[1] قدرتمندتر سازند. واژگان و تصاویر مهم‌تر از آن اشیایی هستند که آنها بازنمایی می‌کنند؛ این وضعیت، همان تصادف حقیقی[2] است. این تصاویری که در اینجا و حالا وجود دارد بر خاستگاه و منبع خود در جنگ اطلاعاتی اولویت دارند و همین تصاویر، اطلاعات را همگن می‌سازد و با این کار، واقعیت ناهمگن را آلوده می‌کند، اگر همین تصویر در هر جایی ظاهر شود، تهاجمی[3] می‌گردد و به روایتی کلان مبدل می‌شود که «شبکه برنامه‌های سرگرمی رسانه‌ای براساس سناریوهای صنایع نظامی»، با حسن‌نیت، آن را نقل می‌کنند. این وضعیت، شکلی از خشونت و تهدیدی برای دمکراسی است، زیرا وجه تمامت‌خواهانه سلطه را ایجاد می‌کند. این روایت کلان، مشروعیت سیاسی خود را با ارجاع دادن به ارزش‌های خودش کسب می‌کند و بدین‌سان به‌نحو تناقض گونه‌ای به بروز بحران اطلاعات می‌انجامد. این نوع جنگ اطلاعاتی، موضوع بمب اطلاعاتی را پیش می‌کشد. ویریلیو بمب‌های اطلاعاتی را به همان اندازه بمب‌های اتمی، مرگبار می‌داند، زیرا به‌نظر او بمب‌های اطلاعاتی می‌توانند حافظه اجتماعی، روابط و حتی جامعه بین‌المللی را در یک چشم به هم زدن با سرازیر ساختن سیلی از اطلاعات یک‌طرفه، نابود سازند. این وضعیت به یک «تصادف کامل» می‌انجامد؛ که شبکه‌های جهانی، مرزهای اجتماعی و طبیعی را نابود می‌کنند، روند اطلاعات، اندیشه و تفکر را دور می‌زند؛ حقیقت به‌سرعت، نسبی می‌گردد و بحران‌ها مانند بیماری‌های واگیردار شیوع و گسترش می‌یابند. منازعات محلی، دیگر وجود ندارند؛ در عوض، تنها عنصر هم‌زمان وجود دارد که مجال رخوت و سستی، مقاومت، یا انتقاد نمی‌دهد. بدین‌سان، جنگ با توسل به قاعده الزام‌آور اخلاقی که از آن ارائه می‌شود، به‌نحو تناقض‌گونه‌ای اجتناب‌ناپذیر می‌گردد (Ibid., 1997).

فناوری اطلاعات، برداشت‌ها درباره جنگ را نیز دگرگون ساخته است. ویریلیو گرایش‌هایی را مشاهده می‌کند که جنگ مدرن را دگرگون ساخته و پیامدهای بنیادینی

---

1. Actual Reality
2. True Accident
3. Invasive

هم به بار می‌آورد. داگلاس کلنر[1] استدلال کرده است که برداشت ویریلیو در مورد فناوری به «جنبه‌های توانمندساز و دمکراسی‌زای فناوری‌های رسانه‌ای و رایانه‌ای جدید» توجه نمی‌کند. استدلال کلنر این است که تمرکز شدید ویریلیو بر جنگ و فناوری نظامی بیش از حد معمول بر بینش وی درباره فناوری تأثیر می‌گذارد و این بینش نیز به‌نوبه خود، وی را به‌سمت دیدگاهی عمدتاً فناوری‌هراسانه[2] درزمینه ذات فناوری و فناوری‌های جدید دوران معاصر سوق می‌دهد (Kellner, 2000, P.103).

«نظریه سرعت» ـ که ویریلیو بنا کرده ـ شایسته بررسی است؛ برای مثال، در جنگ مدرن، زمان به میزان کافی وجود ندارد، زیرا تفکر آدمی به حداقل می‌رسد. در اثر سرعت، سروصدا و خودکارسازی دستگاه‌ها[3] حقیقت نسبی می‌گردد. بیشتر مواقع، در طول یک بحران نظامی، رسانه‌ها تمایل دارند برنامه‌های خود را بر موضوعاتی خاص متمرکز سازند و این موضوعات نیز با شبکه‌های رسانه‌ای تقویت و پررنگ می‌شوند. این وضعیت در رسانه‌ها برخلاف عملکرد شبکه‌های اطلاع‌رسانی است. شبکه‌های اطلاعاتی، امکانات بدیل ارائه می‌دهند. این بدان معناست که گرچه فناوری اطلاعات از ظرفیت اطلاع‌رسانی به توده‌های مردم برخوردار است، اما این توانمندی را هم دارد که اطلاعات گمراه‌کننده در اختیار توده‌های مردم قرار دهد. این همان موضوع فناوری اطلاعات و جنگ اطلاعاتی (و مبتنی‌بر اطلاعات گمراه‌کننده)[4] است که ویریلیو می‌کوشد آن را در بحث خود مطرح نماید. ماهیت فناوری اطلاعات به‌گونه‌ای است که این فناوری به یکی از ضرورت‌های زندگی تبدیل گشته و همه‌گیر و فراگیر شده است؛ به همین دلیل، انواع و اقسام مرزهای مختلف از قبیل مرز میان اطلاعات و اطلاعات گمراه‌کننده نیز غیرقابل تشخیص می‌شوند. بنابراین، جنگ اطلاعاتی، با کمک گرفتن از فناوری اطلاعات، امکانات تحریف واقعیتی را که ویریلیو تحلیل می‌کند، افزایش می‌دهد. در اینجا، بر امکانات گرایش‌های معمولی به تحریف واقعیت، از جمله ساده‌سازی‌ای که به گفته ویریلیو، باید از آن آگاه باشیم، تأکید می‌شود.

---

1. Dauglas Kellner
2. Techophobia
3. Automation
4. (dis) Information-Warfare

۲-۴ جنگ علیه تروریسم: وضعیت اضطراری

در مورد یازدهم سپتامبر ۲۰۰۱ باید گفت که این واقعه، چیزی بیش از یک حمله به نمادهای قدرت غرب بود. رسانه‌ها با بیان واژگان و نمایش تصاویر، اقدامات تروریستی را مرتب بازگو می‌کردند؛ به‌طوری‌که، به‌نظر می‌رسید در واقعیت صدها، هزاران و بلکه ده‌ها هزار حمله تروریستی به مرکز تجارت جهانی شده است. همه تصور می‌کردند فهم دقیق حملات به مرکز تجارت جهانی و پنتاگون، غیرممکن است و البته، رسانه‌ها نیز قادر نبودند علت بروز این حملات را تبیین کنند. رسانه‌ها فقط آنچه را در آن زمان دیده شده بود، تکرار می‌کردند، گویی تکرار آن، فهم این حملات را آسان‌تر می‌سازد. بروز اقدامات تروریستی پیش‌بینی نشده و پس از آن نمایش باشکوه آنها در رسانه‌ها تأثیر زیادی بر عواطف و رفتار افراد گذاشت و به‌این‌ترتیب، فضای خاصی را بر جهان حکم‌فرما ساخت.

نمونه بارز این وضعیت، خانم آینک ویبن[1] است؛ وی تجربیات خود را درباره یازده سپتامبر روی کاغذ آورده است. با مطالعه نوشته‌های او درمی‌یابیم که وی جوهره جنگ مجازی را لمس کرده است. تصاویری که در صفحه‌های نمایشگر رایانه نشان داده می‌شود و او نیز می‌بیند، این احساس را در وی ایجاد می‌کند که خودش نیز جزئی از این فاجعه بوده است: «ما همگی آنجا بودیم، اما آنجا نبودیم. ما این فاجعه را دیدیم، اما هیچ‌گاه آن را ندیدیم. ما همچنان می‌گفتیم که این واقعی نیست، درحالی‌که نیک می‌دانستیم که آن واقعیت داشت. ما شاهد کشته شدن افراد بودیم، اما هیچ جسد بی‌جانی ندیدیم و هیچ خونی را مشاهده نکردیم. به برکت فناوری اطلاعات، ما به کسانی که در یازده سپتامبر حضور داشتیم تبدیل شدیم. این وضعیت، ما را با مسئولیت جدیدی مواجه می‌سازد و این مجال را فراروی ما می‌گذارد تا به جرگه کسانی که در مورد موضوع تروریسم جهان‌گستر تحقیق می‌کنند بپیوندیم (Wibben, 2001)».

تروریسم، روایت کلانی است که به‌آسانی می‌توان آن را تصور و مرتب بازگو کرد؛ تروریسم درواقع، یک ماشین جنگی است. بعد از یازده سپتامبر، به دنبال تعاریفی که جرج دبلیو بوش و وزیر دفاع وی، دونالد رامسفلد از جنگ ارائه دادند، صحبت از «جنگ جدید» و «جنگ علیه تروریسم» به میان آمد. آشکارا به بینندگان تلویزیونی تفهیم شده

1. Annick Wibben

بود که حملات تروریستی، یک اقدام جنگی و درواقع، پرل‌هاربر دوم[1] است. دو ویژگی حملات یازده سپتامبر، این تصویر ذهنی[2] را تقویت کرد: نخست، اقدامات تروریستی در داخل خاک ایالات متحده رخ دادند؛ دوم، پنتاگون که مراکز فرماندهی نظامی آمریکا در آن قرار دارد، آماج حملات بود.

هر روز، همین موضوعات و پیامدها در همه شبکه‌های تلویزیونی و رادیویی، روزنامه‌ها و مجلات و اینترنت، پخش و تکرار می‌شد. در صفحه‌های نمایشگر رایانه‌ها، تنها فضا برای شعارهای «جنگ علیه آمریکا» و «جنگ جدید آمریکا» وجود داشت. با توجه به آنکه نوع وضعیت، جنگی تعریف شده بود، بسیار بدیهی بود که رویارویی با این چالش با به‌کارگیری نیروی نظامی به‌آسانی توجیه شود. در هفتم اکتبر ۲۰۰۱، یعنی در همان آغاز عملیات «آزادی ماندگار»[3] (عملیات نظامی در افغانستان)، شعار «جنگ علیه تروریسم» به همراه واژگان، «آمریکا مقابله‌به‌مثل می‌کند» روی صفحه نمایشگر رایانه‌ها ظاهر شد.

اصطلاح «جنگ علیه تروریسم» با ذکاوت خاصی انتخاب شده بود؛ چرا که در این جنگ، علاوه‌بر خود تروریست‌ها، شمار بسیار اندکی از افراد خواهان پیروزی آنها می‌باشند. سوگند یاد کردن به نام جنگ علیه تروریسم، آسان است حتی اگر هیچ اتفاق‌نظری در مورد معنای آن وجود نداشته باشد. پاسخ به این سؤال که «آیا مسئله چیزی غیر از وجود وضعیت اضطراری»[4] در روبه‌رو شدن با تروریسم است در هاله‌ای از ابهام قرار گرفت.

۳-۴ ضرورت وجود دشمن و مشکل‌سازی[5] آن

اگر دشمن، مشخص و آشکار نباشد، رفتن به میدان نبرد برای هر سربازی دشوار است. براساس سخنرانی‌هایی که بوش رئیس‌جمهور آمریکا در سپتامبر ۲۰۰۱ ایراد کرد، ایالات متحده آمریکا در جنگ بین خیر و شر قصد داشت نه تنها شر را از صحنه روزگار

---

1. Second Pearl Harbor
2. Mental Image
3. Enduring Freedom
4. State Of Emergency
5. Problematics

پاک کند بلکه افراد شریر (افراد وحشی) را نیز از مخفی‌گاه‌هایشان بیرون بکشد و تحت تعقیب قرار دهد. ارائه تعاریفی مبهم از «دشمن» یا «تروریست» کافی نبود؛ ازاین‌رو، دیری نپایید چهره دشمن نیز نشان داده شد؛ در این بحبوحه، ابتدا چهره اسامه بن‌لادن و بعد از آن، چهره صدام حسین به‌عنوان مصادیق دشمن معرفی شدند.

وقتی دشمن به‌اندازه تصویری که از آن خلق شده است، شر و غیرعقلانی باشد، آغاز مذاکرات با وی غیرممکن است. در این شرایط برای آنکه «خیر» بر سر قدرت بماند، دشمن را باید به‌طور کامل شکست داد و علاوه‌بر این، وی را از صحنه روزگار محو کرد. حال باید این سؤال را بیان کرد که در وهله اول، چگونه می‌توان این دشمن را به‌ویژه در شرایطی که نامرئی شده است، شکست داد. پاسخ کلنر به این سؤال، این است: بنابراین، برای شکست دادن شبکه بن‌لادن، نه تنها باید طالبان و گروه القاعده در افغانستان را نابود کرد، بلکه باید کل شبکه جهان‌گستری را قلع‌وقمع نمود که در همهٔ حوزه‌های حقوقی، سیاسی، قضایی، نظامی، ایدئولوژیکی و آموزشی همواره به دنبال ایجاد ائتلاف و فعالیت چندجانبه‌اند (Kellner, 2002).

هرچند «دستگیری دشمن چه زنده و چه مرده» به‌صورت هدفی درآمد که به‌سرعت تثبیت شد، اما بااین‌حال، این هم هدفی منطقی به‌شمار می‌رفت. پس از آنکه بن‌لادن به‌عنوان فردی وحشی تعریف شد، سرنوشت وی نه لزوماً از طریق قانونگذاری‌های مرسوم بلکه با اجرای قواعد غرب وحشی[1] رقم خورد؛ چرا که ساکنان ایالات متحده و تگزاس، بیش از اروپاییان با این قواعد آشنایی داشتند و درواقع، این قواعد برایشان قابل فهم‌تر بود. ماهیت دیجیتالی فناوری اطلاعات[2] نیز در روایت‌های رهبران سیاسی حکم‌فرما بود. به‌این‌ترتیب، در نبرد میان خیر و شر نیز که به طرف‌داری از تمدن و در مخالفت با بربریت درگرفت، وضعیت «یا این یا آن» پدیدار شد.[3]

ازسوی‌دیگر، «وجههٔ شیطانی بخشیدن» به بن‌لادن در فرایند تعریف دشمن نیز چه‌بسا جایگاه یک قهرمان را که در جهان عرب علیه غرب به پا خاسته به وی بخشیده

---

1. Wild West

۲. منظور، این است که در آن دو انتخاب وجود دارد: روشن یا خاموش؛ صفر یا یک ـ م.

۳. به‌عبارت بهتر، در این نبرد، دو انتخاب وجود داشت: شما یا با ما هستید یا علیه ما ـ م.

است. اما بااین‌حال، آنچه می‌توان مسئله مهم‌تری تلقی کرد، گفتمان شر است که به دنبال این وضعیت شکل می‌گیرد و مبتنی‌بر منطق دوگانه‌انگارانه «فضیلت‌های ما»[1] و «نیروهای جهل و ظلمت آنها»[2]ست. ماهیت این منطق، مطلق‌گرایانه است، چرا که براساس آن، هیچ دولتی در میان دو حدّ افراط وجود ندارد. کاملاً متناقض‌نمایانه است که حتی اگر این رویکرد هیچ فضایی را برای شک و شبهه باقی نگذارد، باز هم همین «جهل و ظلمت» دشمن بود که اقدام مبتنی‌بر شبهه و تردید محض را توجیه می‌کرد. اما در زمانی که تروریست‌ها بازداشت شدند و در پایگاه کمپ اکس ـ ری[3] در گوانتانامو زندانی گردیدند، آنها نه زندانی جنگی بلکه «پیکارگر قانون‌گریز»[4] معرفی شدند؛ با این رویداد بود که قوت و انسجام این استدلال دوگانه‌انگارانه خیر و شر زیر سؤال رفت.

در همان نخستین لحظات آغاز جنگ، به‌نظر می‌رسید که هیچ‌کس از مکان مخفی‌گاه بن‌لادن (یعنی دشمن اصلی) خبر ندارد. همه تصور می‌کردند که وی در تورا بورا،[5] پاکستان، سودان، یا حتی جایی در ایالات متحده مخفی شده است. بنابراین، نتیجه منطقی این بوده که حملات نظامی نه تنها در افغانستان بلکه در سایر مناطق نیز باید روی دهد. به پیروی از دیدگاه کلنر، می‌توان گفت: «شکست دادن شبکه بن‌لادن، در گرو نابودسازی کل این شبکه در سراسر جهان است».

تأکید و تمرکز بیش از حد بر بن‌لادن باعث شد به یک دشمن غیرقابل مشاهده و مجازی تقلیل داده شود؛ درواقع، دشمن، همان دشمنی بود که تنها در روزنامه‌ها، تلویزیون، اینترنت و در نتیجه، تنها در تصاویر ذهنی ما حضور داشت. این بینش براساس چهره بن‌لادن که در صفحه نمایشگر رایانه‌ها پدیدار گردید، طراحی شده بود. مسئله‌ای که درباره وجود یک دشمن نامرئی وجود دارد، این است که اهمیتی ندارد چقدر نیروی نظامی برای مقابله با آن مورد استفاده قرار گیرد، بلکه مسئله این است که اگر دشمن در جهان واقعی همچنان ناپیدا باقی بماند، نمی‌توان آن را نابود کرد. بنابراین،

---

1. Our Virtues
2. Their Forces Of Darkness
3. Camp X-Ray Base
4. Unlawful Combatants
5. Tora Bora

دشمن مجازی قادر است حتی به داخل اتاق‌های نشیمن ما رخنه کند. به‌نظر می‌رسد حمله تبلیغاتی علیه یک دشمن نامرئی نه برطرف مقابل (دشمن) بلکه تنها بر خودمان تأثیر گذارد (Huhtinen and Rantapelkonen, 2002). حال با جرح و تعدیل و ساده کردن دیدگاه کلنر، سؤال این است که: برای پیروزی در جنگ اطلاعاتی، آیا واقعاً راه دیگری غیر از نابودسازی شبکه‌های (رسانه‌ای) جهان‌گستر وجود دارد؟

تعیین هویت دشمن برای مشروعیت بخشیدن به جنگ، ضروری است. حتی اگر دشمن‌هایی از قبیل بن‌لادن یا صدام حسین از بین رفته باشند یا از صفحه‌های نمایشگر رایانه‌ها پاک شده باشند، یا به‌نحوی موفقیت‌آمیز مرده یا زنده، دستگیر شده باشند، باز هم «دشمن‌های شر خوب»[1] بعدی معضلی جدید ایجاد خواهند کرد. پرزیدنت بوش، در نطق سالیانه خود (۲۹ ژانویه ۲۰۰۲)، دشمن بعدی را (ایران، عراق و کره شمالی) معرفی کرد و آنها را محور شرارت خواند.

در می سال ۲۰۰۲، این گروه «دولت‌های سرکش» خوانده شدند و ازاین‌گذشته، شمولیت آن به کشورهای کوبا، لیبی و سوریه نیز گسترش یافته است. بعد از دستگیری صدام حسین در سال ۲۰۰۳، دشمنان جدید متولد شدند.[2]

اما نابودسازی محور شرارت لزوماً کافی نخواهد بود، زیرا چنین ادعا شده است که گروه‌های تروریستی در بیش از ۶۰ کشور وجود دارند. این وضعیت، بحث‌های بیشتری را درزمینه نظریه دشمن پیش می‌کشد، زیرا براساس این نظریه، یک دوست که با ما دشمن می‌شود، دیری نمی‌پاید که می‌تواند به واقعیت مبدل گردد (Hairle, 2000). مسئله‌ای که درباره گفتمان محور شرارت وجود دارد، این است که این گفتمان کشورهای مورد نظر را بیشتر از گذشته منزجر می‌سازد و نفرت از جهان غرب را نیز تشدید می‌کند. علاوه‌بر این واقعیت که دشمن نیز ممکن است به دوست مبدل شود، «دشمن در داخل»[3] فقط افسانه نیست.(۳)

فناوری به تنهایی نمی‌تواند این مسئله را حل کند. برای مثال، در دهه ۱۹۹۰، این

---

1. Good Evil Enemeis

۲. درواقع تراشیده شدند ـ م.

3. Enemy Within

گزارش‌ها به گوش می‌رسید که اسلوبودان میلوسویچ و اسامه بن‌لادن مردانی‌اند که شما می‌توانید با آنها معامله کنید. ریچارد هالبروک[1] بعدها به بررسی این موضوع پرداخت که بن‌لادن[2] چگونه می‌تواند از یک غار با پیشروترین جامعه ارتباطاتی و اطلاعاتی ارتباط برقرار کند. حتی اگر غرب رسانه‌های اطلاعاتی دیجیتال را نیز کنترل می‌کرد، تروریست‌ها با ابزارهای نامتقارنی که در اختیار داشتند می‌توانستند چنان تأثیری را برجای گذارند که کنترل‌کنندگان و پیام‌رسان‌های رسانه‌ها نیز از انجام اقدامات برای مقابله با آن عاجز می‌ماندند.

اگر مشکلی را که لفاظی‌های دشمن در مورد قابلیت عملیاتی اقدامات نظامی ایجاد می‌کند، در نظر بگیریم باید خاطرنشان سازیم که چالش اساسی فراروی سربازان، نیروهای نظامی و سیستم‌های اطلاعاتی و جاسوسی، نحوه شناسایی و تشخیص دشمن است، زیرا اطلاعات دیجیتالی در میدان نبرد پست‌مدرن، کافی نیست. یک سرباز باید از خود سؤال کند که چگونه خواهد توانست سرباز دشمن را از شهروند غیرنظامی در بغداد بازشناسد، یا در مورد افغانستان، چگونه می‌توانیم یک تروریست القاعده‌ای را از رزمنده آزادی بازشناسیم. این گروه‌ها ده سال است که تلاش‌های زیادی را انجام داده‌اند تا خودشان را از چنگال یکدیگر آزاد سازند.

۴-۴ جنگ در افغانستان، از لحظات پسامدرن تا انزوای اطلاعاتی

به‌علت وجود فناوری اطلاعات، شایعات و افسانه‌ها به‌سرعت در دهکده جهانی گسترش می‌یابد. رهبران نظامی، سربازان و آنهایی که بر موج شبکه‌های اطلاعاتی سوار می‌شوند نمی‌توانند صحت این شایعات را ثابت کنند. عبارت‌های ذیل نشان می‌دهد هوارد کرتز[3] چگونه آغازین لحظات پسامدرن در زمان حمله نظامی به افغانستان را (که اکتبر ۲۰۰۱ رخ داد) توصیف می‌کند: وقتی شبکه‌های کابلی به موضوع علائم «آمریکا مقابله‌به‌مثل می‌کند» می‌پرداختند، ویلیام برایان[4] برخی از جنگنده‌هایی را که در جنگ شرکت داشتند،

---

1. Richard Holbrooke

۲. که سیا وی را آموزش داده است.

3. Howard Kurtz
4. William Brian

معرفی می‌کرد و می‌گفت: اگر بینندگان بتوانند در چشم ذهن خود به تصویر بکشند، ...

اقدامات چشمگیری در رسانه‌ها انجام نمی‌گرفت. برای مثال، جنینز[1] مصاحبه‌ای تلفنی با عبداله، وزیر خارجه شورشیان افغان که به ائتلاف شمال معروف بودند، انجام داد.

اما تا حد زیادی، آشفتگی حکم‌فرما بود. سی.ان.ان صحنه‌هایی از اظهارنظر یکی از وزرای طالبان را که شبکه الجزیره تصویربرداری کرده بود نشان می‌داد؛ در این صحنه این وزیر گروه طالبان ادعا کرده بود که «ما در این حملات یکی از جنگنده‌ها را سرنگون کردیم». اما پنتاگون این ادعا را رد کرد. براون[2] گفت هیچ راهی وجود ندارد که با آن بتوان این ادعاهای متناقض را اثبات کرد.

ساعت پنج بعدازظهر، در *فاکس نیوز*، شپرد اسمیت[3] گوینده خبر از استیو هاریگان[4] «گزارشگر این شبکه در افغانستان» سؤال کرد آیا وی از گزارش‌ها در مورد موج دوم حملات به کابل اطلاع دارد یا خیر؟ شپرد در پاسخ گفت: «نه، اما شما می‌توانید جنب‌وجوش فعالیت‌هایی را که در میان مخالفان طالبان در اینجا وجود دارد واقعاً حس کنید. وقتی سی.بی.اس به امواج رادیویی واشنگتن بازگشت، بینندگان نگاهی به زیرنویس تصاویر انداختند و گزارشی از خبرگزاری *رویترز* از مقابل دیدگانشان گذشت. گزارشگر این خبرگزاری می‌گفت: «خط تاریخ کابل». «انفجارهایی قوی، امروز مناطق شمالی کابل را به لرزه درآورد» (Kurtz, 2001, C1).

پخش اخبار در چند روز اول جنگ افغانستان، فقط به چند خبر کوتاه و فوری، آن هم به‌صورت محدود و پراکنده خلاصه می‌شد؛ اما عمدتاً تصاویر برفکی در طول پخش خبر بر صفحه‌های تلویزیون نقش می‌بست. با وجود این وضعیت، گزارشگر یا کارشناس، گزارشی قانع‌کننده در مورد اینکه در جنگ چه می‌گذرد ارائه می‌دادند. حتی همین الان هم، وقایع میدان نبرد برای بیشتر ما موضوعی مبتنی‌بر حدس و گمان است.

اما در جنگ اطلاعاتی، این موضوع اهمیت دارد که رویدادها، متون و تصاویر نه تنها باهم هماهنگ شده‌اند، بلکه تلاش‌هایی نیز برای این هماهنگی ازسوی مخاطب

---

1. Jennings
2. Brown
3. Shepard Smith
4. Harrigan

انجام گرفته است. ستاد مشاوران نظامی رئیس‌جمهور آمریکا نیز به این تلاش‌ها باور داشته‌اند و آشکار کرده‌اند که عملیات‌های اطلاعاتی با هدف تأثیرگذاری نظام‌مندانه بر ایستارها[1] و عواطف اتباع آمریکا و البته در راستای اهداف ایالات متحده انجام می‌گیرند (Joint Chiefs of Staff,1998, II-1-II-7).

جرج دبلیو بوش نیز در نطق سیزدهم فوریه ۲۰۰۱، اظهار داشت: «بهترین راه برای حفظ صلح، بازتعریف جنگ براساس ملاحظاتی که خودمان در نظر می‌گیریم می‌باشد». در همان مراحل آغازین جنگ ابهام‌آلود، مغشوش و مشوش، رسانه‌ها طبق معمول، روایت‌های کلان عقلایی در مورد رهبران و فرماندهان نظامی عقلایی را ضبط و پخش می‌کنند؛ این اقدام رسانه‌ها برای خدمت به هدف فضیلت‌مندانه است. افرادی که این روایت‌ها را ایجاد و کسانی که به آنها استناد می‌کنند و به آنها گوش می‌دهند معمولاً فاصله چندانی از میدان نبرد ندارند.

کنترل محیط همواره بخشی از فرهنگ امنیت ملی و نیز فرهنگ نظامیان بوده است. دراین‌باره، محیط اطلاعاتی، همان کارویژه‌ای را که هر فضای نبرد دیگر انجام می‌دهد، اجرا می‌کند؛ ارائه اطلاعات سازگار با روایت کلان نیز اهمیت دارد، زیرا فضای نبرد آشفته به همراه اطلاعات تکه‌تکه شده و پسامدرن، فضیلت‌مندانه نیست.

باید خاطرنشان کرد که شهروندان نیز از تلاش‌ها برای ایجاد روایت کلان حمایت می‌کنند. در همان اوایل جنگ علیه تروریسم در افغانستان، همه گمان می‌کردند که استراتژی کنترل اطلاعاتی و محدودیت‌هایی که مقامات دولتی اعلام می‌کردند حمایت‌های مردم را کاهش می‌دهند.

براساس نظرسنجی‌ای که در آن زمان انجام گرفت، بیشتر آمریکایی‌ها معتقد بودند مقامات دولتی، همه اطلاعاتی را که قبل از یازده سپتامبر می‌دانستند، به آنها نمی‌گویند و همه اطلاعاتی هم که مقامات در مورد عملیات‌ها علیه تروریسم در اختیار دارند، به آنها نمی‌رسد. بیشتر شهروندان نیز این وضعیت را قابل قبول و منطقی یافتند.

هرچند «عملیات آزادی ماندگار»[2] به‌آسانی حمایت جوامع ملی و بین‌المللی را کسب

---

1. Attitudes
2. Operation Enduring Freedom

کرد، اما انجام اولین اقدامات درزمینه فعالیت اطلاعاتی برای سیطره بر اذعان و قلوب (که با هدف کسب نفوذ استراتژیک انجام می‌گرفت)، چالشی شدید برای ایالات متحده آمریکا محسوب می‌شد.

ایالات متحده، مدتی طولانی برای کسب اعتبار خود در جهان عرب جنگیده بود. اما این کشور، به‌عنوان شر و درواقع مسبب همه مشکلات خاورمیانه شناخته شد. فضای اطلاعاتی افغانستان با وضعیت عمومی نیروهای خارجی در این کشور، بیگانه بود. طالبان استراتژی «انزوای اطلاعاتی»[1] را به اجرا درآورده بود و ازاین‌رو، مزیت اطلاعاتی در افغانستان را کسب کرد.

سپس، نمونه‌هایی در مورد فن «منزوی‌سازی دشمن» بیان خواهیم کرد. منزوی‌سازی دشمن با این هدف انجام می‌گیرد که از ابتکار عمل او درزمینه ارائه انواع «دیگری» از اطلاعات به دهکده اطلاعاتی جهانی جلوگیری به‌عمل آید. این نمونه‌ها به سطح نظامی یا پایگاه عملیاتی مربوط می‌شود. پس از آنکه عملیات نظامی در افغانستان در سال ۲۰۰۱ آغاز شد، «تصاویر قدرت» و فضیلت‌مندی[2] نیروهای مسلح به ما نشان داده شد. در وهله اول، تصاویر بمباران‌های دقیق، که در کلیپ‌های ویدئویی به نمایش در می‌آمدند، در کنفرانس‌های مطبوعاتی برای گزارشگران و نیز برای مردم سراسر جهان پخش می‌شدند. سپس، نیروهای مسلح بروشورها و اعلامیه‌هایی را با هواپیما در نواحی عملیاتی می‌انداختند. استراتژی سوم این بود که نیروهای نظامی، با هواپیما مواد غذایی در سرزمین‌های جنگ‌زده می‌ریختند. این نیروهای مسلح برای انجام عملیات‌های بشردوستانه نیز آماده شده بودند؛ اگر این‌گونه اقدامات را مبنای تحلیل و بررسی قرار دهیم، جنگ افغانستان، فضیلت‌مندانه به‌نظر می‌رسید؛ اما بااین‌حال، هدف از این جنگ، ریشه‌کن ساختن تروریسم، نابود کردن شر و دستیابی به صلح بود.

اما بااین‌حال نیز، این اطلاعات مجازی که از راه پاور پوینت[3] منتقل می‌شدند درواقع امر، اخبار افراد درگیر در جنگ ـ یا همان واقعیت تکان‌دهنده جنگ ـ را انعکاس نمی‌دادند. ازاین‌رو است که جنگ مجازی فضیلت‌مند و بمب‌های دقیق هدایت‌شونده در

---

1. Information Isolation
2. Virtuosity
3. Power Point

این جنگ، امیدواری‌های بسیاری را در دل عامه مردم ایجاد می‌کردند. اگر فضای اطلاعاتی با اطلاعات ضد و نقیض پر شود، جامه عمل پوشاندن به این امیدواری‌ها امکان‌پذیر نیست. بسیاری از مصادیق خسارت‌های جانبی[1] از جمله بمباران مسیرهای عبور سران قبایل، محموله‌های صلیب سرخ و مراسم جشن عروسی خانواده افغان، کشتن کودکان و زنان به خبرها نیز راه یافتند. بااین‌حال، این حملات موجه معرفی می‌شوند. وانگهی، پس از گذشت سال‌ها از آغاز این بمباران‌ها، کشمکش میان قبایل افغانستان و منازعات در داخل این قبایل همچنان ادامه دارد و علاوه‌بر این، آنها با تمام نیرو و بیشترین ظرفیت خود به کشت و تولید تریاک می‌پردازند.

اما هدف طالبان فرق می‌کرد. کنفرانس مطبوعاتی که طالبان برگزار نمود، در همه نمایشگرهای دهکده جهانی دیده شد. طالبان ادعا می‌کند که صلح‌طلب است و تمایل ندارد به کسی آسیب برساند؛ علاوه‌بر این، ادعا کرده است بن‌لادن عامل و مسبب حملات تروریستی نبود. به گفته طالبان، ایالات متحده آمریکا وقتی نیروهای نظامی خود را به قلمرو سرزمینی در فراسوی مرزهای خود روانه کرد در نقش یک تروریست ظاهر شد. البته، بیشتر ادعاهای طالبان دروغ بود. واقعیت‌ها و نیز زندگی در میان مردم عادی افغانستان وحشتناک بود.

بااین‌حال، ترس از برتری اطلاعاتی احتمالی طالبان باعث شد آمریکا فوراً ایستگاه‌های رادیویی و تلویزیونی طالبان در افغانستان را منهدم سازد. تعطیل شدن سفارتخانه طالبان در پاکستان نیز موجب شد گروه طالبان نتواند دیدگاه‌های خود را به گوش جهانیان برساند و کنفرانس‌های مطبوعاتی را، که در آنها، پیش‌روی نیروهای رسانه‌ای دهکده جهانی قرار می‌گرفتند، برگزار نماید. اینکه بگوییم طالبان و القاعده فقط دشمنان نظامی آمریکا محسوب می‌شوند، افسانه‌ای بیش نیست.

۵-۴ نبرد برای حقیقت استراتژیک[2]

هدف از بیان این مطلب، ارائه نمونه دیگری از رویه[3] و فن پدیده مناقشه‌برانگیز جنگ

---

1. Collateral Damage
2. Strategic Truth
3. Practice

اطلاعاتی است که به‌منظور دستیابی به حقیقت استراتژیک درمی‌گیرد. با وجود همه چالش‌ها و مشکلات، ایالات متحده آمریکا در نخستین مرحله جنگ اطلاعاتی علیه تروریسم، موفق بود. این موفقیت تاحدی از واژگان و تصاویری که رهبران آمریکا درزمینه امنیت ملی به‌کار می‌گرفتند نشئت می‌گرفت و همچنین تا اندازه‌ای به‌دلیل فعالیت‌هایی بود که با هدف ارتقای تصویر منفی از دشمن در میان مردم به کمک نهادهای خبری از جمله شرکت‌های روابط عمومی[1] و هالیوود دنبال شد. در جبهه سیاسی در سطح بین‌المللی نیز موفقیت اطلاعاتی آمریکا این تصور تجلی یافت که «جنگ، کوتاه‌مدت نخواهد بود» و علاوه‌بر این، نباید انتظار داشت که جنگ، نتایجی فوری و سریع به همراه داشته باشد. وانگهی، هرچند بیشتر زندانی‌های جنگی، مسلمان بودند، اما دشمن نمی‌توانست تقابلی جدی میان مسیحیان و مسلمانان ایجاد کند. باید خاطرنشان کرد هرچند جایگاه زنان در افغانستان به‌هیچ‌وجه، موضوع جدیدی نبود، اما تنها اندکی قبل از طرف‌داری مردم آمریکا از جنگ علیه تروریسم بود که این وضعیت در افغانستان بر سر زبان‌ها افتاد.

اما بن‌لادن با سخنان و پیام‌های خود که در قالب فیلم‌هایی ویدئویی پخش می‌شد، توانست شک و تردیدهایی را در مورد منطقی و عقلایی بودن عملیات‌های نظامی غرب برانگیزد. در ۱۰ اکتبر ۲۰۰۱، کاندولیزا رایس[2] مشاور امنیت ملی به رسانه‌ها گفت که نوارهای ویدئویی بن‌لادن نباید نشان داده شوند زیرا این نوارها چه‌بسا ممکن است حاوی پیام‌های رمزدار باشند یا به‌صورت برنامه‌ای تبلیغاتی برای پیشبرد اهداف بن‌لادن درآیند (Fleischer, 2001). این موضع‌گیری، حدس و گمان‌هایی را در مورد احتمال سانسور اخبار و وقایع ایجاد کرد و علاوه‌بر این، مسئله معانی نهفته در پیام‌ها و مواضع را به‌نحو گسترده‌تری مطرح کرد. با وجود این، این فیلم‌هایی ویدئویی در شبکه‌های خبری خارجی و اینترنت نیز به نمایش درمی‌آمد. هدف از پیام‌های ویدئویی بن‌لادن، این بود که آمریکا را به خروج از عربستان سعودی و رژیم صهیونیستی را به عقب‌نشینی از فلسطین مجبور کند.

---

1. PR Companies
2. Condoleezza Rice

حتی اگر بپذیریم فیلم‌های ویدئویی بن‌لادن با هدف پیشبرد مقاصد تبلیغاتی هم تولید می‌شدند، اما نواری که دسامبر ۲۰۰۱ در جلال‌آباد پیدا شد و در آن بن‌لادن موفقیت خود را به رخ آمریکا می‌کشید، مدرکی مهم محسوب می‌شود که خلاف این مدعا را نشان می‌دهد. بیش از ۵۰ فیلم ویدئویی که در تابستان ۲۰۰۲ پیدا شده بود، به‌عنوان سندی برای اثبات شرارت‌های القاعده در شبکه سی.ان.ان پخش شد. تفکر و تأمل بی‌پایان در مورد «زنده بودن یا زنده نبودن بن‌لادن» و «واقعی یا جعلی بودن نوارهای ویدئویی» چه‌بسا فقط باعث می‌گردد که رهبر تروریست به یک اسطوره[1] مبدل شود ـ شکست دادن یک اسطوره نیز بسیار دشوارتر از شکست دادن دشمن عادی و زنده است. این وضعیت چه‌بسا ممکن است این تصور را ایجاد کند که نیروهای ائتلاف نمی‌توانند بن‌لادن را پیدا کنند. این بدان معنا خواهد بود که نیروهای ائتلاف، برای شکست دادن دشمن واقعی، توجه خود را فقط‌وفقط به جنگ معطوف ساخته‌اند.

نبرد برای القای تصاویر و نمایش حقیقت استراتژیک شتاب گرفت. براساس مقاله روزنامه *نیویورک تایمز* که در ۱۹ فوریه ۲۰۰۲ به چاپ رسید، پنتاگون اداره نفوذ استراتژیک[2] را تأسیس کرده بود. هدف این نهاد، اشاعه نظام‌مندانه اطلاعات به نفع عملیات‌های ایالات متحده آمریکا بود. پیگیری این هدف فضیلت‌مندانه، پدیده جدیدی نیست؛ فریب، جزء ذاتی و طبیعی جنگ است. اما اعلام شد که هدف، انتشار گزارش‌ها، اطلاعات و اطلاعات غلط برای متحدان آمریکا با اینترنت و پست الکترونیکی به شیوه‌ای است که خاستگاه آنها را نتوان به پنتاگون نسبت داد. روزنامه‌نگاران، شهروندان و متحدان نیز این هدف‌گیری را که متوجه ملت خودشان است عجیب و غریب وبی‌سابقه یافتند. آنچه در مورد اداره نفوذ استراتژیک، عجیب و غیرعادی به‌نظر می‌رسید این بود که مقامات دولتی در این شیوه، یکی از اصول مسلم و بدیهی جنگ را آشکار و شفاف ساختند. اما بااین‌حال، اداره نفوذ استراتژیک به‌عنوان ابزاری برای سیاستگذاری‌ها، قدری سریع چنین جاروجنجالی را ایجاد نمود که یک هفته بعد، دونالد رامسفلد[3] وزیر دفاع آمریکا اعلام کرد جرج بوش تصمیم گرفته است این اداره را تعطیل کند. البته، در ۲۵

1. Myth
2. Office of Strategic Influence
3. Donald Rumsfeld

فوریه ۲۰۰۲، بوش به روزنامه‌نگاران قول داد: «ما حقیقت را به مردم خواهیم گفت».

۶-۴ جنگ علیه عراق: تفاوت‌ها در برداشت‌ها

در سپتامبر ۲۰۰۲، یعنی در زمانی که بوش خواستار مشروعیت‌یابی بین‌المللی برای جنگ علیه عراق با مجوز سازمان ملل متحد شد، برداشت‌های جهانی در مورد جنگ، از افغانستان به عراق معطوف گردید. این وضعیت بدان معنا بود که در انظار افکار عمومی آمریکا، دشمن از بن‌لادن به صدام حسین، چهره عوض کرده است. شورای امنیت سازمان ملل متحد با تصویب قطعنامه ۱۴۴۱ به اتفاق‌آرا، مجوز خلع سلاح کامل و فوری تسلیحات کشتارجمعی عراق را تحت نظارت بازرسان تسلیحاتی سازمان ملل متحد صادر کرد.

اوایل فوریه ۲۰۰۳، کالین پاول[1] وزیر خارجه آمریکا، اطلاعاتی را به شورای امنیت سازمان ملل متحد ارائه داد و هدف آن، طرح این ادعای بی‌پاسخ بود که صدام حسین قصد دارد تسلیحات کشتارجمعی تولید کند (چیزی که بازرسان تسلیحاتی سازمان ملل متحد هیچ مدرکی دال بر آن پیدا نکرده بودند). پاول در سخنرانی خود در شورای امنیت، از چند فن برای قانع کردن آنها استفاده کرد؛ که عبارت‌اند از: ارائه کاست‌هایی از مکالمات تلفنی رهگیری شده و مدارکی در مورد طرف‌داران و حامیان عراق، تصاویر جاسوسی ماهواره‌ای و ارائه تصاویر به‌صورت پاور پوینت با ذکر جزئیاتی در مورد برنامه‌های تسلیحاتی مخفیانه عراق و پیوندها میان شبکه‌های تروریستی و بغداد. به اعتقاد آمریکایی‌ها، اینها مدارک قانع‌کننده‌ای بودند، اما باز هم برای صدور قطعنامه دوم شورای امنیت سازمان ملل متحد که مجوز اقدام نظامی را صادر کند، کافی نبود (Walkom, 2003).

وقتی مقامات بریتانیایی سه سند جاسوسی ـ اطلاعاتی قابل توجه را منتشر کردند، نبرد اطلاعاتی بر سر واقعیت و ادعای بی‌اساس، شدیدتر شد. هدف از ارائه اسناد مذکور، این بود که نشان داده شود عراق با فریب و پنهان‌کاری، تأسیسات نظامی عظیمی درزمینه تسلیحات کشتارجمعی در اختیار دارد. کمی بعد از آنکه پاول این گزارش را به‌عنوان مدرکی بی‌نظیر و عالی ستود و حتی در سازمان ملل نیز به تفصیل بدان استناد کرد، دولت بریتانیا پس از اذعان به جعلی بودن آن، خود را در وضعیت دشواری یافت. برای تقویت ادعاها،

---

1. Colin Powell

غلوهای بی‌اساسی هم در این گزارش، که بر پایه اطلاعات جاسوسی جدید تدوین گردید، درج شده بود. این گزارش درواقع کپی‌برداری از نوشته‌های پایان‌نامه فوق‌لیسانس یک دانشجوی ۲۹ ساله کالیفرنیایی بود که حتی غلط‌های املایی آن نیز در گزارش تکرار شده بود. این دانشجو در پایان‌نامه خود، اسناد حمله آمریکا به کویت در سیزده سال پیش را بررسی کرده بود. جدای از این اتهامات، سخن‌گوی تونی بلر،[1] نخست‌وزیر بریتانیا این گزارش را منسجم و دقیق خواند (Hinsliff and et. al., 2003). این استدلالات مهم درزمینه لزوم جنگ علیه عراق در بحبوحه بحران‌های اطلاعات و بحران‌های مشروعیت مطرح شد.

استدلالات به طرف‌داری از جنگ، فضیلت‌مندانه بود. برای مثال، جرج بوش، در نطق رادیویی خود در اول مارس ۲۰۰۳ گفت: «ما نیز برای پیشبرد آزادی، فرصت‌ها و امیدها ایستادگی می‌کنیم. جان و آزادی مردم عراق هیچ اهمیتی برای صدام ندارد. اما مردم عراق اهمیت زیادی نزد ما دارند». ایالات متحده آمریکا یک تهدید را از میان برنداشت، بلکه به منطقه‌ای که در استبداد غوطه‌ور بود، وعده دمکراسی داد.

با وجود حضور این نوع از روایت کلان آزادی، بسیاری از کشورهای مهم ـ از جمله چین، فرانسه و آلمان ـ همچنان در مورد این محرکه‌های اقدام نظامی سوءظن داشتند. علاوه‌بر این، آنها درباره نوع مدارکی که ارائه شده بود به دیده تردید می‌نگریستند و البته غرور و خوی استکبارگری آمریکا نیز آنها را سرخورده کرده بود. این کشورها همچنان بازرسی‌های تسلیحاتی را برای تحقق اهداف خود در عراق کاملاً مناسب می‌دانستند. جانا مک گیری[2] در مجله *تایم* می‌نویسد: «ازنظر بسیاری از اروپایی‌ها، این جنگ شبیه امپریالیسم آمریکایی به‌نظر می‌رسد که تزویر در آن موج می‌زند. آمریکایی‌ها نمی‌بینند که چرا دیپلماسی می‌تواند قضیه برنامه تسلیحات هسته‌ای کره شمالی را حل‌وفصل کند اما در مورد عراق چنین راه‌حلی امکان‌پذیر نیست و نمی‌بینند که چرا قطعنامه‌های سازمان ملل متحد باید در مورد عراق به اجرا درآیند اما در مورد رژیم صهیونیستی نه؛» ازاین‌گذشته، ایگور ایوانف[3] وزیر امور خارجه روسیه اظهار داشت:

---

1. Tony Blair
2. Johnana MeGeory
3. Igor Ivanov

«ایالات متحده باید مراقب باشد گام‌های یک‌جانبه‌ای برندارد که وحدت کل ائتلاف (مبارزه با) تروریسم را تهدید کند» (Mc Geonry).

جنگ مجازی ماه‌ها پیش از آنکه موشک‌ها عملاً به‌سمت بغداد پرتاب شوند آغاز شده بود. بدیل‌ها و مدل‌های مختلفی درزمینه حمله در صفحات متعدد اینترنتی شبیه‌سازی شد. اما در واقعیت، ایستگاه‌های راداری در عراق بمباران شدند. به‌این‌ترتیب، جنگ علیه عراق به‌طور هم‌زمان، هم آغاز شد و هم آغاز نشد. *واشنگتن پست*، درست پیش از صدور اعلان جنگ عراق ـ که جنبه شعارگونه‌ای داشت ـ این وضعیت نظامی را تشریح کرد: «فاز اول، همین الان در جریان است. نیروهای عملیات ویژه برای فراهم کردن زمینه حملات بعدی، در حال انجام مأموریت در داخل خاک عراق‌اند. جنگنده‌های آمریکایی و بریتانیایی که به‌ظاهر مناطق پرواز ممنوع در شمال و جنوب عراق را اجرا می‌کنند، شمار و حجم حملات هوایی خود را افزایش داده‌اند و در این اواخر موشک‌های زمین به زمین عراق را نیز در فهرست اهداف خود گنجانده‌اند ... .

رابرت اندروز[1] یک مقام سابق پنتاگون که بر فعالیت‌های عملیات ویژه نظارت گفت: همین الان هم تعداد زیادی از ادوات حمله را آماده ساخته‌ایم و زمینه‌های حمله (اقدامات هوایی، عملیات‌های روانی، عملیات ویژه) را فراهم کرده‌ایم (Ricks, 2003).

حمله واقعی علیه عراق، یعنی همان حمله پیش‌دستانه‌ای که نیروهای ائتلاف به رهبری ایالات متحده در ۲۰ مارس ۲۰۰۳ آغاز کردند، با حملات جراحی‌گونه‌ای[2] آغاز شد که صدام حسین و حلقه نزدیکان وی را هدف قرار داده بودند. از آن زمان به بعد صفحه‌های تلویزیون و نمایشگرهای رایانه‌ها ـ که به دنبال آشناپنداری صحنه‌ها[3] در اذهان بینندگان بودند ـ بار دیگر مملو از حملات شامگاهی گردیدند. هرروزه، همان موضوعات و پیام‌ها پخش شدند و بارها و بارها با برداشت‌های متعدد بر صفحات تلویزیون، رادیو، روزنامه‌ها، اینترنت و خدمات تلفن همراه نقش بستند. اما حالا دیگر، در این صفحه‌های نمایشگر رسانه‌های جمعی، تنها فضا برای شعارهای «عملیات آزادی عراق» و «جنگ در عراق» وجود داشت.

---

1. Robert Andrews
2. Surgical Strikes
۳. Deja VU: این احساس که فرد پیش‌تر چیزی را که برایش در زمان حال روی می‌دهد تجربه کرده است.

حتی همان سؤال‌ها نیز تکرار شد: «صدام: مرده یا زنده؟»، «آن مرد یونیفرم‌پوشی که در تلویزیون دولتی عراق، سخنرانی ضبط شده‌ای را ارائه داد، یکی از افراد بدل صدام است؟»، «صدام چند تا بدل دارد؟». کاملاً مشخص است که شایعات در چنین لحظاتی، یعنی در زمانی که هیچ شناختی به‌جز اطلاعات صرف وجود ندارد، گسترش و رواج می‌یابند. گمانه‌زنی در مورد یافتن جسد صدام بعد از یک حمله جراحی‌گونه و نمونه‌گیری از دی.ان.ای[1] آن، بسیار زود بود.

عجیب آنکه، جراحی با موفقیت همراه نبود، ازاین‌رو بیمار جان سالم به در برده بود. تصویرهایی[2] از بازداشت‌شدگانی که مانند زندانیان جنگی با آنها رفتار می‌شد ولی هیچ جایگاه رسمی و حقوقی (وابستگی به دولتی خاص) نداشتند، تأثیر این آشناپنداری را تقویت می‌نمود. بعد از آنکه بازداشت‌شدگان امکان دفاع از خود را یافتند، دادگاه رأی صادر خواهد کرد که به‌عنوان زندانی جنگی آزاد شوند یا به‌عنوان پیکارجویان و رزمندگان غیرقانونی اعلام شوند. در نتیجه هیچ چیز جدیدی درباره سرنگونی یک رژیم جبار و رهبر مستبد دیده نمی‌شد.

وقتی عملیات آزادی عراق به‌عنوان شعار پدیدار شد و بر صفحات رسانه‌ها درج گردید و ماند، به یک واقعیت مبدل شد. دونالد رامسفلد وزیر دفاع آمریکا در ۲۱ مارس هشت هدف نظامی را برای حمله به عراق برشمرد. هدف اول، مانند جنگ در افغانستان، پایان دادن به رژیم استبدادی (صدام حسین)؛ هدف دوم، شناسایی، قرنطینه‌سازی و امحای تسلیحات کشتارجمعی عراق و هدف سوم، تعقیب، دستگیری و بیرون راندن تروریست‌ها از آن کشور بود. بااین‌حال، عبارت «عملیات آزادی عراق» نیز مشکل‌آفرین بود. اولاً، اگر آزادی با دمکراسی پیوند دارد، آزادسازی یک ملت نیز مدت زیادی طول می‌کشد. ثانیاً، آمریکا ناقوس جنگ را به صدا درنمی‌آورد. برخلاف عملیات «طوفان صحرا» در عملیات آزادی عراق، هیچ اشاره‌ای به چالش‌های جنگ واقعی نشده بود.

روایت‌ها درباره حرکت سربازان به داخل عراق[3] و گزارش‌ها در مورد اینکه واحدهای

---

1. DNA
2. Pictures
3. Sakewalk

ارتش عراق چگونه خود را به‌سرعت تسلیم خواهند کرد و شهروندان عراقی چگونه از آمریکایی‌ها و بریتانیایی‌ها به‌عنوان نیروهای آزادی‌بخش استقبال خواهند کرد شایع و گسترده بودند. حتی قبل از آنکه جنگ آغاز شود، آمریکا اراده‌ای قوی برای به راه انداختن و پیروزی در این جنگ داشت، قدرت شکست‌ناپذیر ارتش آمریکا نیز این تأثیر روانی را تشدید می‌کرد. همچنین، تأکید بر مفهوم «ضربه و وحشت»[1] که درست پیش از جنگ در شبکه‌های مجازی وجود دارد، این تأثیر را ایجاد کرد که اقدام نظامی علیه عراق با پرتاب ۴۰۰۰ موشک و بمب هدایت‌شونده و دقیق آغاز خواهد شد. اما بااین‌حال، شروع جنگ، ناامیدکننده بود. ازنظر نظامی، عملیاتی کوچک‌تر از توسل به زوری که بیل کلینتون علیه تروریست‌ها در افغانستان و سودان انجام داده بود، صورت گرفت (در آغاز عملیات، تنها ۵۰ موشک، شلیک شد). در مورد مدیریت برداشت،[2] نیز به‌علت توهمی که عامه مردم آمریکا در مورد «جنگ بدون انجام عملیات نظامی»، یا حداقل در مورد «جنگ تمیز»[3] داشتند، انتظارات آنها بسیار بالا بود.

اولین حملات و ضربه‌ها رسانه‌ها را به جنبش درآورد. پیتر آرنت[4] گزارشگر کهنه‌کار آمریکایی(۴) با هیجان فریاد زد: «یک منظره حیرت‌انگیز، مانند فیلم‌های سینمایی اکشن. اما این واقعی است». اریک سورنسون[5] گفت فناوری ـ به‌ویژه فناوری‌های نظامی و رسانه‌ای ـ در حد انفجار گسترش یافته است. وی این تحول را به تفاوت میان آتاری و پلی‌استیشن تشبیه کرد و افزود: «این وضعیت ممکن است حالتی باشد که در آن، توالی صحنه‌ها جذاب‌تر از نمونه‌های اصیل آنها (که توالی صحنه‌ها در آن دیده نمی‌شود) باشد» (Kakutani, 2003 , E1).

پوشش خبری تلویزیون، بینندگان را به تماشاگران ۲۴ ساعته تلویزیون مبدل ساخت. وبلاگ‌های اختصاصی[6] حتی آخرین اخبار و گزارش‌ها را به‌صورت به‌روز شده و دقیقه به دقیقه پخش می‌کردند. این نوع «پیشرفت»، مثل تماشای فیلم سینمایی واقعی در

---

1. Shock and Awe
2. Perception Management
3. Clean War
4. Peter Arnett
5. Erik Sorenson
6. Dedicated Blogges

سالن سینما بود. البته در این حالت، فرد ناگزیر نیست به سالن سینما برود و خط تمایز میان واقعیت و تخیل نیز بیش‌ازپیش مخدوش گردیده است. گویندگان اخبار، مدام به مخاطبین خود یادآوری می‌کردند «آن صحنه‌های زنده‌ای که آنها مشاهده می‌کنند، فیلم سینمایی نیست». آیا این میل شدید به تماشای صحنه‌های جنگ به‌قدری قوی است که بتواند خط تمایز میان امور واقعی و امور تخیلی را مخدوش سازد و درهم بریزد؟ حتی کالین پاول هشدار داد که «این، یک بازی ویدئویی نیست. این جنگ است، یک جنگ واقعی» (Powell, 2003a). عجیب آنکه وی راست گفته بود زیرا دشمن در میدان نبرد عراق عملاً با دشمنی که در بازی‌های رایانه‌ای جنگی وجود دارد تفاوت داشت.

اطلاعاتی که به‌سوی صفحه‌های تلویزیون سرازیر شد، با آنچه عامه مردم انتظار داشتند تفاوت داشت. فاز اول جنگ عملاً طولانیتر، وحشیانه‌تر، خسته‌کننده‌تر، وحشت‌انگیزتر و آکنده از معضلات و غافلگیری‌ها از کار درآمد. هلی‌کوپترهایی که سرنگون می‌شدند، بمب‌های دقیقی که اتوبوس غیرنظامیان را هدف قرار داده بودند، سربازان دشمن که خود را تسلیم می‌کردند، زندانیان جنگی که دستگیر و شکنجه می‌شدند، وقایعی که از مرگ و آتش گلوله حکایت داشتند و زنان و کودکانی که هدف تیراندازی قرار می‌گرفتند در صدر تیترهای خبری بودند. در اولین روزهای جنگ، اصلاً هیچ نشانه‌ای دال بر وجود تسلیحات کشتارجمعی یا حتی تسلیحات پیشرفته دشمن دیده نشد، اما با وجود این، باز هم دشمن به مقابله برخاسته بود.[1] اوضاع میدان نبرد، پرالتهاب و آکنده از آژیر خطرهای غلط و ترس و وحشت بسیار بود.(۵) حتی سربازانی که در میدان نبرد می‌جنگیدند، تصوراتی در مورد وقایع جنگی داشتند که شباهت زیادی به تصورات درباره صحنه‌های نبرد فیلم‌های سینمایی داشت.

ائتلاف کشورهای راغب[2] موفق عمل کرد و به‌سرعت در جبهه زمینی پیشروی نمود. این ائتلاف مایل بود اطلاعاتی را که از صحنه‌های نبرد برای عامه مردم پخش می‌شد به‌گونه‌ای دیگر ببینند. برای مثال، مایل بود گزارش‌هایی در مورد «جنگیدن برطبق برنامه‌های تعیین شده، عملیات شجاعانه نجات یک زندانی جنگی و امحای کامل

1. Shot Back
2. Coalition of the Willing (ائتلاف موافقان هم می‌گویند)

و مؤثر اهداف نظامی پخش شوند». حال باید این سؤال را پرسید که آیا این واقعیت‌های جنگی، واقعی‌تر از اموری که در پاراگراف قبل بدان‌ها اشاره شد، است؟ آنچه قطعی و مشخص است، نبود قطعیت جنگ و قطعیت اطلاعات جنگی، حتی در زمانی است که بهترین فناوری جنگی مورد استفاده قرار می‌گیرد.

جنگ، شکلی به خود گرفت که با واقعیت مطابقت نداشت و تصویری را ارائه داد که انظار عمومی[1] مایل نبود آن را ببیند؛ درواقع، شکلی از جنگ به نمایش درآمد که افکار عمومی در برابر آن ایستادند و با آن به مخالفت برخاستند. بسیار مشخص و آشکار است که جنگ مجازی برای ما تماشاگران عادی و معمولی جنگ، کفایت می‌کند. در اینجا گزیده‌ای از گزارش فرماندهی مرکزی ارتش آمریکا که ژنرال وینسنت کی. بروکس[2] در ۲۹ مارس به‌طور رسمی اعلام نمود، ذکر می‌شود: «آنچه دوست دارم بعداً به شما نشان دهم، مجموعه‌ای تصویری در مورد دوره قبل و بعد از حمله است که استودیوی تلویزیون دولتی رژیم بعث و تأسیسات پخش اخبار آن را نشان می‌دهد. این تأسیسات، مانند سایر تأسیسات، به‌عنوان بخشی از شبکه کنترل و فرماندهی مورد استفاده قرار می‌گرفتند. نیروهای ائتلاف، سه مورد از تأسیساتی را که در داخل این شبکه جای می‌گرفتند، هدف قرار دادند. تصویر پس از حمله خسارت‌های مورد نظر در این سه فلش را نشان می‌دهد. من با ماژیک روی بالاترین فلش خط کشیده‌ام. تصویری که روی آن خط کشیده‌ام، ساختمانی است که فرو ریخته بود» (Brooks and Renuart, 2003).

با وجود این، روزنامه‌های همان روز با تیترهای درشت، گزارش متفاوتی در مورد واقعه دیگری که رخ داده بود، نوشتند: گمان می‌رود حداقل پنجاه غیرنظامی در اثر یک حمله هوایی که بازار بغداد را هدف قرار داده بود، کُشته شده باشند. تصاویر گرافیکی تلویزیون، افرادی را نشان می‌داد که برای یافتن اجساد کشته‌شدگان و مجروحان خرابه‌های بازار «الناصر»، زیر پاره‌سنگ‌ها را می‌گشتند ... خبرنگاران مستقر در بغداد می‌گویند هنوز هیچ اطلاعات مشخصی در مورد اینکه چه کسی مسبب تخریب بازار بوده است، در دست نیست. بیشتر قسمت‌های زمین را خون کشته‌شدگان و مجروحان

---

1. Public Eye
2. General Vincent K. Brooks

پوشانده است ... فرماندهی مرکزی ... اظهار داشت ... این حادثه احتمالاً به‌دلیل انفجار موشک‌های عمل نکرده عراقی بوده است (BBC, 2003).

این گفته ژنرال بروکس، بیشتر با واقعیت تطابق دارد که «در سراسر این عملیات، قدرت اطلاعات، کلید موفقیت بوده است». ژنرال ریچارد مایر نیز در اول آوریل همان عبارت‌های ژنرال چارلز هارنر[1] را تکرار کرد: «قدرت اطلاعات، به این بستگی دارد که چه برداشتی از اطلاعات وجود دارد». این جمله، یک پرسش اساسی را در ذهن ما مطرح می‌سازد: اطلاعات چه کسی واقعی‌تر و ارزشمندتر است؟ این برداشت‌ها در مورد روزهای آغازین جنگ علیه عراق، از نسبیت[2] جنگ حکایت داشتند. اگر از دهکده امقصر به جنگ نگریسته شود، این نگاه به جنگ با نگاهی که از حومه لندن از محل مراکز فرماندهی مرکزی آمریکا در واشنگتن یا اروپا، از پشت صفحه تلویزیون و از درون یک گروه پیکارگر به جنگ انجام می‌گیرد، بسیار متفاوت خواهد بود، حتی اگر روزنامه‌نگاران در آن موقعیت حضور داشته باشند.

ائتلاف کشورهای راغب به رهبری آمریکا در سطح نظامی به پیروزی قاطعی دست یافتند. اما وضعیت امنیت به‌گونه دیگری است و برداشت‌های متفاوتی از آن وجود دارد، زیرا امنیت نوعی احساس است. وقتی ژنرال تامی فرانکس به همراه یکی از صمیمی‌ترین افسران تحت امر او در یک مکان نمادین، یعنی یکی از کاخ‌های صدام حسین در شانزدهم آوریل ۲۰۰۳ پیروزی نظامی آمریکا در عراق را تأیید کردند، رسانه‌ها هم در آنجا بودند. وقتی روزنامه‌نگاران یکی پس از دیگری به وطن خود بازمی‌گشتند، یک سبزی‌فروش ۳۳ ساله در بغداد به نام ولید الفرطوسی،[3] گفت که حالا دیگر مردم رفته‌رفته اعتمادشان را به آنها از دست می‌دهند: آمریکا به عراق قول داد که این حکومت استبدادی را سرنگون کند، اما حالا اوضاع حتی بدتر شده است. برخی از مردم عراق حتی رفته‌رفته آرزو می‌کنند که ای کاش صدام همچنان بر مسند قدرت باقی می‌ماند، زیرا به‌نظر آنها همه این مشکلات پس از خلع وی از قدرت بروز کرد ... تا به امروز، که ما در خانه‌هایمان نشسته‌ایم ... از شر قاتلان و غارتگران در امان نیستیم.

---

1. General Charles Harner
2. Relativity
3. Walid Al - fartousi

نیروهای آمریکایی فقط کنار ایستاده‌اند و تماشا می‌کنند و برای مقابله با آنها دست به هیچ کاری نمی‌زنند. هیچ نظم و امنیتی وجود ندارد. مردم احساس امنیت نمی‌کنند (Gordon and Kifner, 2003).

پرزیدنت بوش، پس از موفقیت در جنگ علیه عراق، اول می۲۰۰۳ اعلام کرد قسمت‌های اصلی عملیات‌های نبرد در عراق به پایان رسیده است. از آن زمان تاکنون امور متناقض‌نمای بسیاری روی داده که این اظهارنظر رسمی را به چالش کشیده است. در حال حاضر، در مقایسه با فاز اول «عملیات اصلی جنگ در عراق»، نه تنها هزاران نفر از مردم عراق، بلکه تعداد زیادی از سربازان آمریکایی کشته شده‌اند. رسوایی دیگری نیز در زندان ابوغریب، تالار پذیرایی و تشریفات[۱] صدام روی داد؛ اما این بار تنها پس از آن روی داد که فناوری اطلاعات توانست به شکل دوربین‌های دیجیتالی به این زندان رسوخ کند. این تصاویر فهم ماهیت جنگ را تقویت نکرد. جنگ به مساجد موصل، فلوجه و شهرک صدر در بغداد نیز کشیده شده است؛ حتی گفته شده بود که جنگ علیه تروریسم با مذهب ارتباط ندارد. اما ما شبکه‌هایی را به چشم خود دیده‌ایم که نیروهای ائتلاف به رهبری آمریکا با مجال دادن به آنها اماکن مقدسه را تخریب می‌کنند. ما اطلاع دقیقی در مورد علت این اقدام نداشته‌ایم. چرا که اصلاً مشخص نیست کدام‌یک از ۷۷ مسجدی که نیروهای ائتلاف و نیروهای عراقی در سطح فلوجه بدان‌ها یورش بردند، به‌عنوان انبار تسلیحات یا سنگری برای انجام حمله مورد استفاده قرار گرفته است (Washington Times, 2004, P.20).

به‌طورکلی، جنگ علیه عراق را می‌توان عقب‌نشینی از جنگ پیش‌دستانه واقعیت‌محور[۲] و تبدیل آن به جنگ اطلاعاتی عقیده‌محور[۳] توصیف کرد. گرایش دیگری که با ویژگی‌های خاص رسانه‌ها و نیز سرعت اطلاع‌رسانی پیوند دارد، این است که بسیاری از اقدامات مثبتی که در عراق انجام گرفته است هرگز گفته نخواهد شد؛ زیرا ازنظر بیشتر رسانه‌های خبری درباره عراق، خبر خوشی در کار نیست و اصلاً هیچ فرصتی هم برای پخش این‌گونه خبرهای مثبت وجود ندارد. بنابراین، وقتی «جنگ علیه عراق» نشان داده

---

۱. عبارتی طعنه‌آمیز و کنایه‌آلود.

2. Facts - based Preemptive War
3. Faith - based IW

شده است، بی‌آنکه هر دو طرف جنگ دیده شوند اخبار فوری و ساده شده و به‌عبارت بهتر، سرعت به‌جای واقعیت نشسته است، به‌این‌ترتیب، فناوری اطلاعات به ما کمک نکرده است تا آگاه‌تر و مطلع‌تر باشیم. درحقیقت، فناوری و رسانه از این توانایی برخوردارند که به فهم ما از جهان شکل دهند؛ ازاین‌رو، مبانی این دو در میدان تجربه بیش‌ازپیش سست می‌شود. این وضعیت، آکی هوتینن[1] را به این نتیجه‌گیری رهنمون می‌سازد که دست‌کاری در محیط نمادین می‌تواند رویدادهای مهمی را در زندگی سیاسی و میدان جنگ خلق کند (Huhtinen, 2004, P.104).

بعدها، بسیاری از مردم ایستارهای خود را در مورد «رفتن به جنگ» تغییر دادند. این تغییر در ایستارها نشان می‌دهد که ما در دورانی متناقض‌نما زندگی می‌کنیم، چرا که قضاوت در مورد حقانیت جنگ‌های پیش‌دستانه به موفقیت این جنگ‌ها بستگی دارد. اما درهرحال، قضاوت، بیش از آنچه در اینجا و هم‌اکنون فرصت است، زمان می‌برد. این سؤال که «اگر جنگ با موفقیت همراه باشد، آیا تمایزگذاری میان اطلاعات مجازی و واقعی برای توجیه آن ضرورت دارد»، پرسشی فقط فلسفی نیست؛ بلکه علاوه‌بر این، باید بررسی شود آمریکا که خود را ازنظر اخلاقی مسئول می‌داند چگونه می‌تواند راهی را برای تحقق وعده فضیلت‌مندانهٔ خود در جهت نیل به صلح دمکراتیک واقعی بیابد.

۷-۴ ابر مه‌آلود صلح

جنگ مجازی فضیلت‌مندانه، پدیده ساده‌ای نیست. آزادی، دمکراسی و صلح، در شرایط وجود «شر»، جنگ را توجیه می‌کند. آشکار است که همه بر سر اصل استراتژی «ضربه و وحشت» توافق دارند؛ پایه استراتژی ضربه و وحشت، این است که ما از آنها می‌خواهیم دست از شرارت بردارند و به ستیز علیه ما برنخیزند. این، هدفی کاملاً فضیلت‌مندانه و برای پیگیری خیر همگانی است. کسانی که در جنگ، به زور متوسل می‌شوند، می‌باید نحوه استفاده از آن زور را نیز در نظر بگیرند؛ به‌طوری‌که این اظهارنظر که «ما یک بن‌لادن نخواهیم داشت ما هزاران بن‌لادن خواهیم داشت»، درباره جنگ در عراق به حقیقت نپیوندد.

---

1. Aki Huhtinen

کسی که به زور متوسل می‌شود، به سیاست ماکیاولیایی روی آورده است. در این نگرش، سیاست نه براساس فضیلت ذاتی اقدام بلکه برحسب نتیجه‌ای که در پی دارد، تعریف می‌شود. جنگ تنها در صورتی می‌تواند فضیلت‌مندانه باشد که موفقیت‌آمیز باشد؛ موفقیت جنگ نیز به‌جای آنکه در گرو میزان مطابقت آن با حقوق بین‌الملل باشد، بیشتر به این بستگی دارد که برای شکست دادن دشمن تا چه اندازه باید به حمله پیش‌دستانه روی آورد.

در این مفهوم، نیت‌های فضیلت‌مندانه که به طرف‌داری از آزادی، عدالت و دمکراسی رخ می‌دهند ممکن است این احساس را در دل تماشاگران ایجاد کنند که اگر این ارزش‌ها نتوانند ریشه‌های تروریسم را هرچه زودتر از بیخ درآورند و همچنان به معاهدات بین‌المللی اعتنا نکنند، کسانی که این ارزش‌ها را ترویج می‌کنند خودشان نیز دیگر به آنها اعتقاد نخواهند داشت. پیگیری یک فضیلت برجسته و مهم می‌تواند حتی خطرناک باشد.

روایت کلان جنگ فضیلت‌مندانه در صورتی فریبنده است که روایت‌ها برای شکل دادن به یک داستان متجانس، هرچه بیشتر خلاصه شود. به معنای دقیق کلمه، روایت‌ها واژگان و تصاویر را در یک واحد منسجم و یکدست جمع می‌کنند. در چنین لحظه‌ای، این وحدت و یکدستی مجازی، در واقعیت‌های محلی مختلف مثلاً در میدان نبرد، آشفته‌تر از قبل می‌شود. اما واقعیت‌ها در جنگ، کافی نیستند. اراده و عزم جنگیدن نیز باید حفظ شود و تداوم یابد. در این حالت، به نام جنگ کارآمد و موفقیت‌آمیز، به افکار و نظرات متناقض اجازه داده نمی‌شود که در زمان جنگ اظهارنظر کنند. زبان جنگ فضیلت‌مندانه، سلاح نیرومندی است که آسان‌تر می‌تواند ما را به طرف جنگ‌هایی که نباید در آنها شرکت کنیم سوق دهد. به‌علت اینکه هیچ روایت کلان کلام‌محوری[1] غیر از آنچه بر صفحه‌های تلویزیون ظاهر می‌شود وجود ندارد، ابر مه‌آلود جنگ اطلاعاتی هر روز غلیظ‌تر می‌شود.

مجازیت به کمک فناوری است که توانمند شده است. براساس مفهوم تصادف[2] که ویریلیو ارائه داده است، فناوری اطلاعات، «واقعیت و مجاز، دوست و دشمن، دور و نزدیک و صلح و جنگ» را درهم می‌آمیزد. دیگر هیچ منازعه‌ای محلی نیست (البته اگر اطلاعات، همه قسمت‌های جهان را به هم پیوند نزده باشد، خلاف این مدعا امکان‌پذیر خواهد بود).

---

1. Logocentric
2. Accident

فضیلت‌مندانه به کمک فناوری اطلاعات در تمام اوقات و سراسر جهان در گرفته است. به‌ویژه اگر ابعاد مجازی و فضیلت‌مند این جنگ باهم ترکیب شوند، می‌توان آن را یک تصادف تمام‌عیار تعریف کرد. بعید است که این جنگ با استفاده از تقویت فناوری، «واقعیت» را تقویت کند، زیرا جنگ، سرشار از عناصر و عوامل انسانی و عدم قطعیت است. در جنگ اطلاعاتی، وقتی سرعت به قدرت مبدل می‌شود، دیگر مجالی برای تعمق و تفکر انسان باقی نمی‌ماند و از این رو خود سرعت، دیگر نمی‌تواند یک فضیلت خوانده شود. آنچه در جنگ مجازی فضیلت‌مند در میان ما باقی می‌ماند، پدیده متناقض‌نمای قطعات پاور پوینت است که از دانش محلی و واقعی، رهاست. جنگ می‌باید درگیرد ولی نمی‌تواند درگیرد. دیکتاتورها از قدرت خلع می‌شوند، اما نه با تسلیحات. تسلیحات کشتارجمعی می‌باید نابود شود، اما نمی‌توان آنها را یافت، به‌نظر می‌رسد که جنگ، دیگر یک کشمکش اجتماعی نیست. مرزهای فرهنگی، به احتمال زیاد، عملاً شکافی را ایجاد خواهند کرد که رفع آن با توسل به اطلاعات آمرانه،[1] غیرممکن است. اگر دشمن، غیرقابل مشاهده باشد و در درون جامعه و در ساختارها پنهان شود، حتی با پیشرفته‌ترین تسلیحات نیز نمی‌توان جنگ را با پیروزی بر دشمن خاتمه داد.

سرعت شتابنده رویدادها و بمباران مستمر و جهان‌گیرانه اطلاعات به یمن وجود کلیپ‌های ویدئویی و تصاویر، ماهیت جنگ را دگرگون ساخته است. ما می‌توانیم جنگ را ببینیم، اما درعین‌حال، نمی‌توانیم آن را درک کنیم. به‌طبع، ارتش و صنعت غرب در جنگ‌های دقیق همچنان از اعتبار برخوردارند، اما «آرمان‌شهر» انقلاب در امور نظامی، (همان وضعیتی که همگان انتظار آن را می‌کشند) با کمک رسانه‌ها و صنعت سرگرمی‌های رایانه‌ای می‌تواند به‌سمت منحرف‌سازی برداشت‌ها کشیده شود. یکی از دلایل این امر، این است که تصاویر جنگ جذاب‌تر، تأثیرگذارتر و قانع‌کننده‌تر از خود واقعیت‌اند. روایت جنگ فضیلت‌مندانه، ویژگی‌هایی از جمله «خسارت‌های جانبی» و خطاها در بمباران‌ها را نیز در خود دارد و همین ویژگی‌های نامطلوب است که سیاست‌مداران، نظامیان و شهروندان را آزار می‌دهد.

اگر واقعیتی که در شبکه‌های مجازی به نمایش درمی‌آید جایگزین خود واقعیت

---

1. Coercive Information

شود، زبانی که در جنگ مجازی فضیلت‌مندانه مورد استفاده قرار می‌گیرد معنای خود را از دست می‌دهد. شبکه «برنامه‌های سرگرمی رسانه‌ای براساس سناریوهای صنایع نظامی» و کسانی مثل جان رندان و سایر شرکت‌های تبلیغاتی که در این حوزه فعالیت دارند، وقتی می‌کوشند جنگ را با بهترین شکل و تصویر ممکن نشان دهند، با چالش عظیمی مواجه می‌شوند؛ ازاین‌رو واقعیت را به شیوه‌ای نمایش می‌دهند که ویریلیو آن را «نمایش‌نمایی مجازی[1] جهان واقعی» می‌نامد. بیل کلر،[2] ستون‌نویس روزنامه *نیویورک تایمز* درباره پیامدهای جنگ، فناوری و رسانه چنین می‌نویسد: «در سال ۱۹۹۱ بیشتر مردم حتی تصور هم نمی‌کردند که خودشان در جایی نزدیک خط مقدم باشند. اما حالا، خط مقدم در جایی است که ما زندگی می‌کنیم، ازاین‌رو ما در وحشت به‌سر می‌بریم (Keller, 2003, A17).

بروز جنگ مجازی فضیلت‌مندانه، مانند شمشیر دولبه است. بر کلاه یکی از سربازان آمریکایی که در ویتنام می‌جنگید شعار «جنگ جهنم است» نقش بسته بود، اما هم‌اکنون در جنگ اطلاعاتی علیه تروریسم چه‌بسا این خطر وجود دارد که شعار «جنگ، صلح است» در تصاویری که از جنگ مجازی فضیلت‌مندانه ارائه می‌شود انعکاس یابد.

بروز جنگ مدرن در عصر اطلاعات چه‌بسا می‌تواند به ظهور بحران‌های اطلاعاتی بیانجامد. جست‌وجوی جنگ تمام‌عیار به نام اهداف فضیلت‌مندانه توهم جنگ با کمک فناوری مجازی را ایجاد می‌کند. این بمباران اطلاعاتی گسترده به ما کمک نمی‌کند تا فراسوی صفحه‌های نمایشگر تلویزیونی و رایانه‌ای را ببینیم و پدیده جنگ را بفهمیم. وقتی جنگ با هدف نیل به مقاصد فضیلت‌مندانه درمی‌گیرد هیچ‌کس نمی‌خواهد واقعیت وحشت‌آفرین محلی جنگ را فراسوی منظره مجازی سرگرم‌کننده ببیند. فهم این موضوع، آسان است که «ابر مه‌آلود» همان واژه جنگ است. این وضعیت نیز برای جنگ‌هایی غیر از جنگ علیه تروریسم، جنگ علیه عراق و جنگ علیه افغانستان صدق می‌کند. کنگو جدیدترین نمونه رذیلت‌مندترین[3] جنگ‌های جهان است، اما ما نمی‌توانیم

---

1. Virtual Theatricalisation
2. Bill Keller
3. Vicious

آن را در این عصر متناقض‌نمای اطلاعات و فناوری مشاهده کنیم.[۶] اگر ما بی‌آنکه شناخت واقعیت‌محورانه در مورد ابعاد محلی اطلاعات داشته باشیم تنها با روند یک‌طرفه اطلاعات سروکار داشته باشیم، همین اطلاعات به‌آسانی می‌تواند ما را به تماشاگران تصادف و زندانیان جنگ دائمی مبدل سازد.

پی‌نوشت‌ها

۱. این فصل بر پایه اندیشه‌هایی است که پیش از این در یک فصلنامه چندرشته‌ای به نام *FUTURA* (۲۰۰۲/۴) به چاپ رسید. من این فصل را کاملاً به‌روز و بازنگری کرده‌ام به‌گونه‌ای که بتوانم وضعیت عراق را در چارچوب آن تبیین کنم و قالب کلی کتاب حاضر را نیز لحاظ نمایم.

۲. جان فرانیس لیوتار (Jean-Francois Lyotard) برای اولین بار، اصطلاح روایت کلان را مطرح کرد. این اصطلاح نوعی روایت را توصیف می‌کند؛ این روایت زیربنای انتخاب‌های خاصی را که یک فرهنگ، آنها را به‌عنوان روال احتمالی کنش تجویز می‌کند تشکیل می‌دهد، به آنها مشروعیت می‌بخشد و آنها را توجیه می‌کند. «مسیحیت»، «روشنگری»، «سرمایه‌داری» و «مارکسیسم» از جمله نمونه‌های بارز چنین روایت‌هایی محسوب می‌شوند. در این فصل، من مفهوم روایت کلان از لیوتار را در مورد مفهوم محدودتر «جنگ علیه تروریسم» به‌کار گرفتم.

۳. این دیدگاه در زمانی مورد تأیید قرار گرفت که «جان والکر» (John Walker)، طالبان آمریکایی و خوزه پادیلا (Jose Padilla) ابداع‌کننده بمب کثیف که به عبدالله المجاهری معروف است، دستگیر شدند. مورد دیگری که به تعریف «دشمن در درون» نزدیک بود در زمانی پدیدار شد که لی‌بوید مالوو (Lee Boyd Malvo) و جان آلن محمد (John Allen Muhammad) آمریکایی‌ها را به وحشت انداختند. آنها اذعان کرده‌اند که در پاییز گذشته در قضیه تیراندازی در کمین به طرف چند نفر در آمریکا تیراندازی کردند و آنها را به قتل رساندند. در فوریه ۲۰۰۳، دولت آمریکا حتی دستگیری تنها یک نفر از افرادی را که تهدید جدی علیه ایالات متحده معرفی شده بودند، یک پیروزی قلمداد می‌کرد. اما در دوران جنگ سرد، وضعیت به‌کلی فرق می‌کرد.

۴. آرنت (Arnett) یکی از کارکنان شرکت تلویزیونی ان.بی.سی، در ماه مارس، بعد از مصاحبه با تلویزیون عراق هدف گلوله قرار گرفت. در این مصاحبه، وی گفته بود که طرح نظامی نیروهای ائتلاف به رهبری ایالات متحده شکست خورده است.

۵. یکی از آژیرهای خطری که برای نیروهای آمریکایی در اوایل آوریل پخش شد، اطلاع داد که عراق از تسلیحات شیمیایی استفاده کرده است. این اعلام خطر، غلط بود. نیروهای آمریکایی در فاصله بیست کیلومتری هدف مورد نظر، زمین را کنده بودند. آنها در عملیات حفاری به یک کانتینر برخورده بودند؛ این کانتینر ماده‌ای را منتشر کرد که در ابتدا تصور می‌شد آن یک عامل عصبی است اما بعدها معلوم شد که آن ماده یک ماده شیمیایی و صنعتی بی‌ضرر است.

۶. براساس گزارش کمیته امداد و نجات بین‌المللی، که آوریل ۲۰۰۳ منتشر شد، بیش از ۳/۳ میلیون نفر پیش از آنکه جنگ در سال ۱۹۹۸ در کنگو درگیرد در این کشور کشته شده‌اند.

منابع و مآخذ

BBC, 'Many dead in Baghdad Blast', *BBC News*, Available on http://news,bbc.co.uk//2/hi/middle_east/2897117.stm, 29 March 2003.

Bush, G.W., (2001-2003). 'Speeches and Transcripts'. Available on www.whitehouse.gov.

Brooks, V. and V. Renuart, (2003). 'CENTCOM Operation Iraqi Freedom Briefing', CENTCOM Homepages. Available at www.centcom.mil, presented by Maj. Gen. Victor Renuart and Bris. Gen. Vincent Brooks.

Clark, W.K., (2001). Waging Modern War: Bosnia, Kosovo, and the Future of Combat, New York: Public Affairs.

Doa, J. and E. Schmitt, (2002). 'Pentagon Readies Efforts to Sway Sentiment Abroad', The *New York Times*, A1.

Der Derian, J. Virtuous War, (2001). Mapping the Military-industrial-Media-Entertainment Network, Boulder, CO: Westview Press.

Fleischer, A., (2001). 'Press Briefing by Ari Fleischer', Whitehouse.

Gordon, M.R. and J. Kifner, (2003). 'U.S. Generals Meet in Palace, Sealing Victory', *The New York Times*.

Harle, V., (2000). The Enemy with a Thousand Faces: The Tradition of the Other in Western Political Thought and History, Westport, CT: Praeger.

Hinsliff, G.M. Bright, P. Beaumont and E. Vulliamy, (2003). 'First Casualties in the Propaganda Firefight', The Observer. Available on http://www.observer.co.uk/waronterrosism/story/0, 1373, 892146,00.html.

Hoffman, D., (2002). 'Beyond public Diplomacy', *Foreign Affairs*, 81(2).

Huhtinen. A., (2004). 'Soldiership Without Existence-The Changing Socio-Psychological Culture and Environment of Military Decision-Makers', in J. Toiskallio (ed.), Identity, Ethics, and Soldiership, Helsinki: National Defence College, Department of Education. ACIE Publications, No. 1.

Huhtinen, A. and J. Rantapelkonen, (2002). 'Perception Management in the Art of War-A Review of Finnish War Propaganda and Present-day Information Warfare', *Journal of Information Warfare*, 2(1).

_____, (2001). Imagewars: Beyond the Mask of Information War, Saarjärvi: Marshal of Finland Mannerheim's War Studies Fund and Finnish Army Signals School.

Joint Chiefs of Staff, Joint Doctrine for Information Operatins, Joint pub 3-13 US Department of Defence, 9 October 1998.

Kakutani, M., (2003). 'Shock, Awe and Razmatazz in the Sequel', *The New York Times*, E1.

Kaplan, R.D., (2003). Warrior Politics: Whyleadership Demands a Pagan Ethos New York: Vintage Books.

Keller, B., (2003). 'Fear on the Home Front', *The New York Times*, A17.

Kellner, D. September 11, Terror War, and the New Barbarism, References to the 10 June 2002 Version while work was-in-progress on-line at http://www.gseis.ucla.edu/faculty/kellner/kellner.html published 2003 as From 9/11 to Terror War: The Dangers of the Bush Legacy, Maryland: Rowman & Lilltefield Publishers, Inc.).

_____, (2000).'Virilio, War, and Technology. Some Critical Reflections', in John Armitage (ed.), Paul Virilio: From Modernism to Hypermodernism and Beyond London: Sage.

Khalilzad, Z. and J.p. Whiten (eds), (1999). Strategic Appraisal: The Changing Role of Information Warfare, Santa Monica, CA: RAND.

Kurtz, H., (2001). The Fog of War: From the Ground Zero. A Spectral Patchwork of Sound and Fury', *Washington Post*, C1.

Luostarinen, H., (2002). 'Propaganda Analysis', in W. Kempf and H. Luostarinen (eds): Journalism and the New World Order: Studying War and the Media, Vol. II Gotherburg: Nordicom.

Lyotard, J-F., (1984). The Postmodern Condition: A Report on Knowledge, Minneapolis: University of Minnesota Press, Theory and History of Literature, Vol. 10.

McGeary, J., (2003). '6 Reasons Why So Many allies Want Bush To Slow Down', *Time*.

Miller, L. and S. Rampton, (2001). 'The Pentagon's Information Warrior: Rendon to the Rescue', *PR Watch*, 8(4), Fourth Quarter.

Myers, R.B., (2003). 'Speeches and transcripts', Available on www.defenselink.mil.

Rowell, C., (2003). 'Transcript: Secretary of State Colin Powell', *Fox News*, Available on www.foxnews.com/story/0.2933.82037,00.html.

Ricks, T.E., (2003). 'War Plan for Iraq Largely in Place. Quick, Simultaneous Attacks on Ground and From Air Envisioned', *Washington Post*, A01.

Rumsfeld, D., (2003). 'Speeches and Transcripts'. Available on www.defenselink.mil.

Susser, E.S., D.B. Herman and B. Aaron, (2002). 'Combating the Terror of Terrorism', Scientific American.

Virilio, P., (1988). 'Paul Virilio', Interview, Block.

Virilio, P., (1986). Speed and Politics: An Essay on Dromology, Trans. Mark Polizzoni, New York: Semiotext (e).

Virilio, P. and S. Lotringer, (1997). Pure War, Revised Edition, New York: Semiotext (e).

Walkom, T., (2003). 'Replays Show Powell Did Not Score', *Toronto Star*, 2003.

Washington Times, (29 November, 2004)'Zarqawi's City of Death', p.20.

Whitehead, Y., (1997). 'Informatin as a Weapon: Reality Versus Promises', *Air Power Journal*.

Wibben, A.T.R., (2001). 9.11: Images, Imaging, Imagination', InfoInterventions. Available on www.watsoninstitute.org/infopeace/911.

فصل پنجم خطرهای فناوری مرتبط با رایانه

پیتر جی. نیومن*

مقدمه

در این فصل، خطرهای فناوری مرتبط با رایانه را که با موضوعاتی از قبیل رفاه فردی، ثبات جهانی، اعتمادپذیری،[1] ایمنی، امنیت و حوزه خصوصی پیوند دارد، بررسی می‌کنیم و علاوه‌بر این، اقداماتی را که می‌توان برای مقابله با این خطرات انجام داد، مورد توجه قرار می‌دهیم. در بسیاری از موارد باید تلاش‌های پیگیرانه بسیار بیشتری برای کاهش این خطرات انجام گیرد. در برخی موارد برای مثال، رایانه نظامی ـ تخیلی «واکنش به برنامه عملیات جنگی» در فیلم سینمایی «بازی‌های جنگی»، تنها راهبردی که با پیروزی همراه است، بازی نکردن است.(۱) موضوع این فصل، خطراتی را که در «سیستم‌های کنترل پدافندی، هوایی و فضایی»، سیستم‌های ارتباطاتی، امور مالی ـ تجاری، مراقبت بهداشتی و امور درمانی و به‌طورکلی، سیستم‌های اطلاعاتی و غیره وجود دارد، دربرمی‌گیرد.(۲) از یک‌سو، آگاهی از تهدیدهایی که تروریسم ایجاد کرده است، در این اواخر افزایش یافته است؛ ازسوی‌دیگر، خطرهای ناشی از اختلال در سیستم‌ها و استفاده‌های نابجایی که به‌عمد یا به‌اشتباه از سیستم‌های رایانه‌ای انجام می‌گیرد، مدت‌هاست وجود دارد و تداوم یافته است. ازاین‌رو، طبیعی به‌نظر می‌رسد که فناوری‌های مرتبط با رایانه و روابط تنگاتنگ میان آنها در حوزه‌های اجتماعی، سیاسی، اقتصادی و زیست‌محیطی را بررسی کنیم. در این فصل مسائل و موضوعاتی از جمله امنیت سیستم‌ها، اعتمادپذیری سیستم‌ها، ایمنی انسانی، اعتبار برنامه‌های کاربردی،

---

* Peter G. Neumann

1. Reliability

جایگاه حریم خصوصی و بسیاری از موضوعات دیگر مورد بررسی قرار می‌گیرند.

با توجه به اینکه تقریباًهمه اقدامات ما، چه بخواهیم چه نخواهیم، به فناوری‌های رایانه‌ای وابسته شده است، برای فهم موضوعات مورد نظر می‌باید بر زمینه‌های پایه‌ای و حوزه‌های علمی زیادی اشراف داشته باشیم. بزرگ‌ترین دغدغه ما در اینجا این است که چگونه می‌توانیم بی‌آنکه در جزئیات کم‌اهمیت‌تر گم شویم، توجه خود را به این تصویر بزرگ معطوف نماییم.

ما می‌توانیم ابعاد بی‌شماری را برای بررسی مسئله‌ای که واقعاً بسیار چندبعدی است در نظر بگیریم. به‌طور بسیار خلاصه، برخی از گزینه‌های بررسی ابعاد موضوعات چندبعدی که به ذهن خطور می‌کنند، عبارت‌اند از:

- بین‌المللی‌گرایی در برابر انزواگرایی،
- چندجانبه‌گرایی در برابر یک‌جانبه‌گرایی،
- حکومت کرده با توافق در برابر حکومت کرده با زور،
- همکاری[1] در برابر ملی‌گرایی،
- حذف نظارت و مقررات‌زدایی در برابر نظارت و اعمال مقررات،
- هموارسازی زمینه‌های بازی اقتصادی در برابر جهانی شدن بر پایه سیطره شرکت‌های چندملیتی،
- بازارهای آزاد در برابر بازارهای کنترل شده (برای مثال کارتل‌های بین‌المللی)،
- توسعه منابع جایگزین تأمین انرژی در برابر وابستگی به سوخت‌های فسیلی.

بااین‌حال، چهار گزینه دیگر نیز وجود دارد که در اینجا اهمیت خاصی برای ما خواهند داشت:

- فهم خطرهای استفاده نابجا از فناوری در برابر بی‌توجهی به این خطرها،
- فناوری بیشتر در برابر فناوری کمتر (به‌عنوان راهی برای حل معضلات اجتماعی)،
- آزادی اطلاعات در برابر اختفا،
- حریم خصوصی در برابر نظارت.

بیشتر این ابعاد، معمولاً با نگرشی به‌نسبت ساده‌انگارانه، گزینه‌هایی سیاه و سفید تلقی می‌شوند که ایدئولوژی‌های مختلف، هریک از دو طرف وضعیت را یا خوب می‌دانند

---

1. Partnership

یا بد. در واقعیت، این امور درکل کاملاً سیاه یا کاملاً سفید نیستند و ما باید بپذیریم که سایه‌های خاکستری نیز در این میان وجود دارد. هریک از این گزینه‌هایی که «عناصر متباین»[1] به‌نظر می‌رسند، درواقع، خود، طیف گسترده‌ای از گزینه‌ها را دربرمی‌گیرند و بیشتر مواقع نیز در امتداد همان طیفی که چندان آشکار نیست، باز هم باید عناصر متعددی برای تحقق آنها وجود داشته باشد. هرگونه تلاش برای بررسی پدیده‌ها ازمنظری افراط‌گونه به شکست می‌انجامد و البته به‌نظر می‌رسد این‌گونه بررسی‌ها آشکارا نشانگر نبود عقل سلیم در عرصه تحقیق است. معمولاً هیچ پاسخی راحت و بدون دغدغه نیست. من همیشه از زبان آلبرت انیشتین نقل قول می‌کنم که می‌گفت: «هرچیزی باید تاحدامکان ساده شود». ازاین‌رو در جامعه نیز می‌کوشیم امور را بسیار ساده سازیم، سپس، راه‌حل‌های ساده‌انگارانه‌مان را مورد انتقاد قرار می‌دهیم.

بنابراین، اجازه دهید ابتدا به بررسی این موضوع بپردازیم که این ابعاد چهارگانه چگونه در مورد فناوری و به‌طور خاص فناوری اطلاعات صدق می‌کنند:

۱-۵ فناوری ارتباطات رایانه‌ای[2]

در بسیاری از برنامه‌های رایانه‌ای کاربردی، ما به سیستم‌هایی نیاز داریم که ایمن و قابل اعتماد باشند و قابلیت دسترسی به آنها بسیار بالا باشد. در مورد بسیاری از برنامه‌های کاربردی حساس نیز، ما به معنای واقعی کلمه به توانمندی نیازمندیم.

آنچه ما در عمل داریم، به معنای واقعی کلمه، نقطه‌ضعف است. سیستم‌ها و شبکه‌های اطلاعاتی آکنده از آسیب‌پذیری‌ها و پیوندهای ضعیف می‌باشند. وانگهی، مراکز تولید انبوه این محصولات با بهره‌مندی از بازارهای انبوه، درزمینه تولید مدل‌های پیشرفته سیستم‌های اطلاعاتی، بی‌نظیر و حیرت‌آور ظاهر شده‌اند، اما متأسفانه نتوانسته‌اند سیستم‌های مقاومی تولید کنند. هرگز نباید تصور کنیم «سیستم‌هایی که ما بدان‌ها وابسته‌ایم آسیب‌ناپذیرند یا کسانی که از این سیستم‌ها استفاده می‌کنند لغزش‌ناپذیرند. ما باید بیاموزیم سیستم‌ها را به‌گونه‌ای طراحی کنیم که استحکامات

---

1. Dichotonomy
2. Computer Communication Technology

ایمنی و حفاظتی آنها به‌مراتب بهتر از وضعیت کنونی باشد؛ علاوه‌بر این، ما باید نسبت به نیت‌های آن جماعت ساده‌انگار که می‌گویند می‌توانیم بازار را به حال خود واگذاریم تا راه‌حل‌هایی برای اعتمادپذیری و امنیت سیستم‌ها ارائه دهد، به دیده تردید بنگریم؛ چرا که این مسائل معمولاً با نیروی بازار حل نمی‌شوند.

۲-۵ اینترنت

اینترنت فرصت‌های جدید بی‌شماری را درزمینه‌های توسعه جهانی، گسترش تجارت در سراسر جهان، آموزش، روند سریع اطلاعات و غیره ایجاد کرده است، اما مقاومت بسیار اندکی در برابر حملات هماهنگ از خود نشان داده است. درواقع، آنچه ما تا به حال دیده‌ایم، در قیاس با آنچه می‌توانست اتفاق بیافتد، کم‌وبیش به یک بازی کودکانه شبیه بوده نه مقاومت و سیستم‌هایی هم که به آن متصل شده‌اند، در عمل بسیار آسیب‌پذیر بوده‌اند. اسب‌های تروا، ویروس‌ها، کرم‌ها، حملات به سرویس‌های اینترنتی و غیره جلوه‌هایی از تهدیدهای واقعی علیه اینترنت به‌شمار می‌آیند؛ علت این وضعیت نیز بیش از همه، نبود سیستم‌های مقاوم و ساختارهای شبکه‌ای قوی می‌باشد. زیبایی اینترنت، این است که پدیده‌ای، کاملاً بین‌المللی است. اما عواملی از قبیل نبود مدیریت روشن‌بینانه در این حوزه، تمایل دولت‌ها به کنترل آن، طمع‌ورزی شرکت‌های رایانه‌ای و بسیاری از عوامل دیگر، آینده آن را در معرض تهدیدهایی جدی قرار داده است. گروه‌های ویژه متعددی که در این حوزه فعالیت دارند، می‌کوشند روند تکاملی این فناوری را هدایت کنند. شرکت اینترنتی تعیین نام‌ها و ارقام،[1] منشوری به‌نسبت تنگ‌نظرانه دارد و حتی بحث و مجادله زیادی ایجاد کرده است. اما سازمان جدیدی به نام جامعه طرف‌داران مسئولیت در برابر اینترنت[2] (۳) می‌کوشد رویکردهای دمکراتیک‌تری را ترویج دهد که هم دسترسی واقعی همگان به اینترنت را تضمین نماید و هم به گروه‌های ذی‌نفع طمع‌کار، عرضه‌کنندگان پست‌های الکترونیکی نابهنجار، کلاهبرداران و ... اجازه ندهد این پدیده را به تباهی بکشانند؛ درعین‌حال، این سازمان از این موضوع که وضع مقررات نباید اینترنت را به‌طور کامل محدود سازد، حمایت می‌کند.

---

1. Internet Corporation for Assigned Names and Numbers
2. People For Internet Responsibility

۵-۳ آسیب‌پذیری

زیرساخت‌های حساس ما در هر دو سطح ملی و بین‌المللی، مملو از آسیب‌پذیری‌اند؛ در این زمینه می‌توان به آسیب‌پذیری‌های مرتبط با حوزه‌های امنیت، اعتمادپذیری، بقاپذیری سیستم‌ها[1] و ایمنی انسانی اشاره کرد. این موضوع در مورد حوزه‌های مخابرات، برق، آبرسانی، پخش نفت و گاز، حمل‌ونقل و حتی دوام دولت‌ها نیز صدق می‌کند. برای مثال، گزارش «کمیسیون حفاظت از زیرساخت‌های حساس» که زیرمجموعه نهاد ریاست جمهوری آمریکاست در زمان ریاست جمهوری بیل کلینتون[۴] به این نتیجه رسید که اساساً هر پدیده‌ای در برابر حملات داخلی و خارجی، آسیب‌پذیر است و درواقع بدون مداخله دیگران و بی‌آنکه مورد حمله قرار گیرد، از هم می‌پاشد. هرچند در گذشته، اقدامات بسیار کمی برای مقابله با این‌گونه خطرات انجام گرفته، اما سال‌هاست که بسیاری از این خطرات بر همگان آشکار بوده است.

۵-۴ باز بودن[2]

بحث‌ها و مجادلات زیادی در مورد این موضوع که «آیا محرمانه بودن می‌تواند امنیت را تقویت کند»، وجود دارد. در شمار اندکی از موارد، محرمانه بودن می‌تواند امنیت را تقویت کند. حماقت محض است که تصور شود با انکار وجود نارسایی‌های جدی امنیتی می‌توان از سوءاستفاده از این نارسایی‌ها جلوگیری به‌عمل آورد. ازاین‌گذشته، اگر ندانیم که چقدر آسیب‌پذیر هستیم، بعید است که بتوانیم تدابیر معقولی را برای ترمیم این آسیب‌پذیری‌ها انجام دهیم. این مسئله‌ای واقعاً جدی و بغرنج است. بحث‌ها بر سر همگانی بودن یا انحصاری بودن نرم‌افزارهایی که اشخاص حقوقی یا حقیقی بر آنها مالکیت دارند مهم‌اند. به خاطر داشته باشید وجود نرم‌افزار همگانی به‌خودی‌خود مشکل را حل نمی‌کند. وانگهی، پنهان شدن در پشت نرم‌افزار انحصاری نارسا و مخدوش به نهادینه شدن امنیت با توسل به ابهام[3] منتهی می‌شود و این طرح، ذاتاً طرح نامطلوبی است.

---

1. System Survivalability
2. Openness
3. Obscurity

۵-۵ حریم خصوصی، محرمانه بودن، مراقبت،[۱] کنترل،[۲] نظارت:[۳] چه کسی بر ناظران نظارت می‌کند؟

مسائل مرتبط با حریم خصوصی فوق‌العاده مهم است، بیشتر مردم به این مسائل توجه نمی‌کنند. هر فرد عادی معتقد است هیچ چیزی برای پنهان کردن ندارد، پس چرا حریم خصوصی برای او مهم است؟ در پاسخ به این سؤال می‌توان عواملی از جمله سرقت هویت،[۴] اطلاعات غلط، کنترل، مزاحت، اخاذی، حملات شخصی هدفمند و بسیاری از عوامل دیگر را برشمرد. وانگهی، بسیاری از مسائل مربوط به حریم خصوصی، نهادی‌اند[۵] نه فردی. به‌طورکلی، برخی از نظارت‌های مستقل، کاملاً ذاتی‌اند. به‌عنوان مثال، شرکت‌هایی از قبیل انرن،[۶] تقاطع جهانی،[۷] مدیریت ضایعات[۸] و ال ـ تایم وارنر[۹] نقطه‌ضعف‌هایی جدی درزمینه پاسخ‌گویی داشته‌اند. رویه‌های حسابداری شرکت اندرسون[۱۰] به درپوشی برای تبانی، سوءمدیریت و نبود حسابرسی مستقل تبدیل شده است.

در حوزه سیستم‌های رایانه‌ای، این وضع به‌مراتب بدتر است. حتی در جاهایی که نشانه‌هایی از حسابرسی مستقل وجود دارد، حسابرسی‌ها دست‌کاری و نادیده گرفته می‌شوند. هرچند در بیشتر مواقع، فرصت‌هایی برای بازسازی و احیای آن داده‌های حسابرسی که حذف شده‌اند، وجود دارد؛ اما بااین‌حال، معضلات فراروی تلاش برای اتکا به شواهد و اسناد دیجیتالی نیز بسیار جدی‌اند، زیرا این امکان وجود دارد که صحت و اعتبار فرایند تهیه اسناد و مدارک مورد تردید قرار گیرد. اگر شما ناگزیرید برای حفاظت از اطلاعات خود بر درستی یک سیستم رایانه‌ای اتکا کنید، دچار مشکل می‌شوید؛ زیرا مسائل امنیتی و نقض حریم خصوصی، پای افرادی را که به پایگاه‌های اطلاعاتی دسترسی دارند یا می‌توانند در پایگاه‌های اطلاعاتی نفوذ کنند، به میان می‌کشد. اگر

---

1. Surveillance
2. Control
3. Monitoring
4. Identity Theft
5. Institutional
6. Enron
7. Gobal Crossing
8. Waste Management
9. Aol-Time Warner
10. Anderson

شما ناچارید به کسانی اتکا کنید که غیرقابل اعتمادند، همه گزینه‌هایی که انتخاب می‌کنید، نامطلوب‌اند.

۶-۵ فرایند انتخابات

یکی از مواردی که معمولاً آن‌چنان حساس هم قلمداد نمی‌شود، فرایند انتخابات است. فرایند انتخابات به نوعی بسیاری از مشکلات حوزه فناوری از قبیل اعتمادپذیری، امنیت و حریم خصوصی را که پیش‌تر در مورد آنها بحث کردیم در قالب یک بافت[1] واحد جای می‌دهد. در دهه‌های گذشته، هشدارهای بسیاری در این زمینه داده شده است، اما این هشدارها عمدتاً مورد بی‌اعتنایی قرار گرفته‌اند. تجربه فلوریدا[2] در سال ۲۰۰۰ فقط ظاهر قضیه را که به چشم می‌آمد نشان داد. از همان آغاز فرایند ثبت‌نام رأی‌دهندگان، لیست‌های جعلی تبهکاران[3] در فلوریدا و عوامل دیگری از این قبیل ده‌ها هزار رأی‌دهنده را از شرکت در انتخابات محروم ساخت؛ به‌طوری‌که براساس بررسی‌های مشترک ام.آی.تی ـ کال تک،[4] بین چهار تا شش میلیون رأی در سال ۲۰۰۰ مفقود شد. در مورد ریختن برگه‌های رأی به صندوق‌ها و شمارش آرا نیز باید خاطرنشان کرد خطرات زیادی فرایند فهرست‌بندی برگه رأی و درواقع، پاسخ‌گویی مقامات درکل فرایند انتخابات را تهدید می‌کند. کارت‌های پانچ شده[5] نیز آشکارا مشکل‌آفرین‌اند.

بااین‌همه، سیستم‌های تمام ـ الکترونیک، بسیار پرخطرند. در سیستم‌های تمام ـ الکترونیک امروزی، واقعاً هیچ تضمینی وجود ندارد که «رأیی که شما به صندوق می‌اندازید به‌صورت درست شمارش شود» و درصورت تقلب آشکار در فرایند رأی‌گیری و شمارش آرا یا بروز اشتباه مرموز در داخل سیستم‌های رأی‌گیری نیز، معمولاً آن‌چنان‌که باید و شاید پاسخ‌گویی وجود ندارد. چنین سیستم‌هایی فرصت‌های زیادی را برای تقلب در فرایند انتخابات ایجاد می‌کنند. چند شرکت بزرگ، آماج اتهامات درزمینه تقلب در انتخابات بوده‌اند و در مواردی در دادگاه محکوم شده‌اند و به تخلفات آشکارا اخلاقی

---

1. Context
2. Florida
۳. در آمریکا افرادی که برخی از جرائم خاص را مرتکب می‌شوند، حق رأی ندارند ـ م.
4. Caltech-MIT Study
5. Punched Cards

اذعان کرده‌اند. تقریباً در همه موارد، رمز منبع داده‌ها اختصاصی و انحصاری است. در توجیه این وضعیت، این ادعای بی‌ربط و دروغین مطرح می‌شود که انحصاری بودن رمز منبع داده‌ها سیستم رأی‌گیری را ایمن‌تر می‌سازد. فروشندگان این سیستم‌ها تأکید می‌کنند که قابل اعتمادند و علاوه‌بر این، سیستم‌های رأی‌گیری نیز به‌طور کامل مورد آزمون قرار گرفته‌اند و تأیید شده‌اند. اما، فرایندهای آزمون و تأیید و ارائه مجوز، ذاتاً نارسا می‌باشند. ازآنجاکه برقراری دمکراسی حقیقی اساساً به‌درستی فرایند انتخابات بستگی دارد، این نقل قول قدیمی در اینجا فوق‌العاده موضوعیت دارد: مهم این نیست که آرای چه کسانی شمرده می‌شود، مهم این است که چه کسانی آرا را می‌شمارند.

سند ریسک‌های بارز،[1](۵) در بسیاری از صفحات خود، نمونه‌هایی را بیان می‌کند که از نارسایی‌های سیستم‌های رایانه‌ای در حوزه‌های امور دفاعی، هوا ـ فضا، حمل‌ونقل، برق، سیستم‌های بهداشت و درمان، سیستم‌های کنترل، محیط زیست، امور مالی و بازرگانی، مخابرات، انتخابات، سازوکار اجرای قوانین و شاید ناامیدکننده‌تر از همه، امنیت اطلاعاتی و حریم خصوصی حکایت دارند. در اینجا تنها موارد معدودی از نمونه‌های «ریسک‌های بارز» را برمی‌شماریم.[2]

۷-۵ مشکلات فراروی صنعت هواپیماسازی و هوانوردی تجاری

ـ هواپیمای لودا ایر[3] نقص فنی اختلال در فشار هوا را داشت و به‌طور تصادفی در میانه پرواز فرود آمد.

ـ در پرواز هواپیمایی در خطوط هوایی شمال غرب، سیستم هشداردهنده نتوانست مستقر شود زیرا مجهز نبود.

ـ موتور هواپیمای بریتیش میدلند ۷۳۷[4] دچار آتش‌سوزی شد و خلبان به اشتباه (به‌جای موتور سوخته) موتور سالمی را که در حال کار کردن بود از هواپیما جدا کرد و زمین انداخت. علت این اقدام نیز اشتباه علائم در کنار دکمه‌ها بود.(۶)

---

1. Illustrative Risks Ducument

۲. برای جزئیات بیشتر می‌توانید به سایت www.risks.org مراجعه کنید.

3. Lauda Air

4. British Midland 737

ـ به‌علت اشتباهات خلبان و مأمور برج کنترل، هواپیمایی از خطوط هوایی ایرومکزیکو[1] در نزدیکی فرودگاه لس‌آنجلس با هواپیمای دیگری برخورد کرد.
ـ سقوط چهار هواپیمای ایرباس ای ۳۲۰[2] را عمدتاً به اشتباه خلبان نسبت دادند، این در حالی بود که راهنمای خودکار هواپیما و خلبان باهم هماهنگ نبودند.
ـ یک هواپیما از شرکت مسافربری ایرونیوزلند[3] در کوهستان ارباس[4] در منطقه آنتارتیکا[5] سقوط کرد، زیرا مشخص شد داده‌هایی که درزمینه مسیر هواپیما ارائه شده بود غلط بوده؛ اما همین استدلال نیز ثابت نشده بود.
ـ یک هواپیمای روسی که با سیستم اتوماتیک جلوگیری از برخورد برای صعود به ارتفاعات بالاتر هدایت می‌شد، براساس فرمان‌های مأمور کنترل حمل‌ونقل هوایی سوئیس فرود آمد و در نتیجه به‌شدت در هنگام فرود با زمین برخورد کرد.

۸-۵ مسائل مرتبط با سیستم‌ها در حوزه‌های نظامی و غیرنظامی

ـ موشک‌انداز یورک تاون[6] در اثر عدم کنترل بخش‌های صفر و یکی نرم‌افزار برنامه رایانه‌ای، ظرف تقریباً سه ساعت در آب غرق شد. همین امر باعث شد سیستم عامل ویندوز کشتی نیز به هم بریزد. متأسفانه، این واقعه سبب شد موتورهای کشتی از کار بیافتند.
ـ سیستم دفاع موشکی پاتریوت[7] نتوانست موشک‌های جدید را به‌درستی هدف‌گیری کند زیرا تغییرات مفرط در نرم‌افزار ساعت رایانه، اشیا جدید را خارج از ناحیه هدف قرار می‌داد.
ـ سیستم ایجیس[8] در داخل ناو هواپیمابر یواس‌اس وینسنس[9] نتوانست هواپیمای تجاری را از جنگنده نظامی ایران متمایز سازد، و علاوه‌بر این، اخلالگری انسانی در آن سیستم نیز باعث شد به‌نحو نامناسبی طراحی گردد؛ در نتیجه ایرباس به اشتباه هدف قرار

---

1. Aeromexico
2. Airbus A320
3. Air New Zeland
4. Mount Erebus
5. Antartica
6. Yorktown
7. Patriot
8. The Aegis System
9. USS Vincennes

گرفت و در اثر آن بسیاری از سرنشینان غیرنظامی در آن جان باختند.[۱]

ـ هواپیمای هندلی ـ پیج ویکتور[۲] به‌ظاهر سه بار به‌طور جداگانه آزمایش شده بود و به‌نظر می‌رسید که این سه آزمایش وجود ثبات در سکان افقی هواپیما را توجیه خواهد کرد. اما، سه نقطه‌ضعف جداگانه در این آزمایش‌ها وجود داشت: طراحی مدل جداره داخلی بال‌های هواپیما در مدل‌سازی‌های مربوط به استحکامِ قدرت ارتعاش بالا دچار اشتباهاتی بود؛ آزمایش میزان پژواک صدا به اشتباه با معادله‌های آیرودینامیکی مطابقت داده شده بود؛ کیفیت پروازهای با سرعت بالا به غلط از روی آزمایش‌های پروازهای با سرعت پایین تخمین زده شد؛ و سکان افقی هواپیما در اولین آزمایش پرواز شکست و باعث کشته شدن خلبان و نابودی هواپیما شد.

ـ سیستم‌های کنترل رایانه‌ای بیش‌ازپیش در قطارها، خودروها، کشتی‌ها، تجهیزات و دستگاه‌های مربوط به این حوزه‌ها و ... مورد استفاده قرار می‌گیرد. بسیاری از نقطه‌ضعف‌ها و نارسایی‌های سیستم‌های خودکار تجربه شده‌اند. به‌علاوه، عوامل متعددی از قبیل اشتباهات انسانی، نقص‌های سخت‌افزارها و مشکلات نرم‌افزاری در بروز حوادثی که به پیدایش این همه لاشه‌های قطار انجامیده است نقش داشته‌اند.

۹-۵ برنامه‌های رایانه‌ای در امور پزشکی و درمانی

ـ دستگاه پرتوزایی تراک ۲۵[۳] چند نفر را به کام مرگ برد. علت این واقعه به معضل حیاتی زمان‌بندی رایانه آن نسبت داده شد. چرا که حالت تحقیقاتی پرتوهای پرشدت به‌جای حالتِ درمانی کم‌شدت در دستگاه تعبیه شده بود.

ـ سیم دستگاه کنترل ضربان قلب در بیمارستان اطفال سیاتل[۴] به اشتباه به پریز شبکه برق بیمارستان وصل شد و باعث برق‌گرفتگی و در نتیجه، مرگ یک دختر چهارساله در سال ۱۹۸۶ گردید. واقعه مشابهی نیز هفت سال بعد در شیکاگو روی داد. دست‌کاری در سیم‌های برق و شبکه‌های الکترومغناطیسی باعث بروز حوادث و مرگ بسیاری از کسانی که

---

۱. البته، روندهای عینی و واقعیاتی که به مرور زمان فاش گردید، کذب این مدعا را ثابت کردند ـ م.

2. Therac 25
3. Therac
4. Seattle

دستگاه تنظیم ضربان قلب بر آنها وصل بوده شده است، چرا که این‌گونه دستگاه‌ها مغناطیس‌هایی را در خود دارند که بر برنامه کنترل‌کننده ضربان قلب تأثیر می‌گذارند.
ـ مسائل بی‌شماری وجود دارد که از پایگاه‌های اطلاعاتی پزشکی و سیستم‌های کنترل بیمارستان‌ها سرچشمه می‌گیرد و امنیت و حریم خصوصی افراد را تهدید می‌کند.

۱۰-۵ مسئله سال ۲۰۰۰

ـ نبود پیش‌بینی و آینده‌نگری باعث بروز مسئله سال ۲۰۰۰ شد. این مسئله به سیستم‌هایی که از سال ۱۹۶۵ تولید و تأیید شده بودند، ولی به‌نحو نظام‌مندانه‌ای از طرح آن نیز خودداری شده برمی‌گردد. در ژانویه سال ۲۰۰۰، منابع عظیمی برای جلوگیری از بروز اختلاف‌های جدی در سیستم‌های رایانه‌ای هزینه شد. جالب آنکه، برخی از این سیستم‌های به‌اصطلاح نوسازی شده در ژانویه ۲۰۰۱ و بعد از آن دچار اختلال گردید.

هر روز بر تعداد سیستم‌هایی که صفت «حساس»[1] بر آنها اطلاق می‌گردد (برای مثال، سیستم ایمنی حساس، و سیستم بقاپذیری حساس) افزوده می‌شود؛ علت این وضعیت، آن است که ابعاد زندگی ما هر روز رایانه‌ای‌تر شده و ما به‌طور کامل به سیستم‌های رایانه‌ای وابسته شده‌ایم. بسیاری از خطرات جدید عبارت‌اند از: وابستگی به دانش زیست‌ـ سنجی[2] که با تأیید سندیت سروکار دارند و سیستم‌های فعال‌کننده صدا و فهم کلام که برای تشخیص گوشی‌های بومی، لهجه‌های خارجی، جعل‌کنندگان هویت، تقلیدکنندگان صدا و مداخله عابران در یک صحنه خاص به‌کار گرفته می‌شوند. قبل از آنکه به دنبال راه‌حل‌های احتمالی برای معضلات حوزه‌های فناوری باشیم، می‌باید شناخت بیشتری درزمینه تجربیات خود و دیگران کسب نماییم.

وب‌سایت پیتر نیومن پر از مطالبی است که تبیین می‌کند چگونه ما می‌توانیم این وضعیت را به‌نحو چشمگیری بهبود بخشیم. اما اعتقاد راسخ شخصی من این است که اگر راه‌حل‌ها مبتنی‌بر اصول دمکراتیک استوار نباشند، در درازمدت کارگر نخواهند افتاد.

---

1. Critical
2. Biometrics

وقتی ما وضعیت شبکه جهانی، اینترنت، تلویزیون، رادیو و سایر رسانه‌ها را ـ که تقریباًهمه افراد در جهان متمدن به‌نحوی و تاحدی سریع به‌وسیله آنها باهم ارتباط برقرار می‌کنند ـ بررسی کنیم، این وضعیت بسیار آشکار می‌شود.

شاید تعجب‌آور و جالب باشد که بگوییم کاریکاتوریست‌ها به‌ظاهر کار مثبتی را انجام می‌دهند چرا که واقعیت را به عامه مردم نشان می‌دهند. برای مثال، این گفته جرج اُرول[1] را که با لباس بازیگران داستان کمدی پشت قله قاف[2] در صفحات کمدی روزنامه آخر هفته ظاهر شده بود در نظر بگیرید: «اگر آزادی به معنای این است که هر کاری می‌توان انجام داد، پس این حق را هم دربرمی‌گیرد که به مردم آن چه را نمی‌خواهند بشنوند، بگوییم».

۱۱-۵ نقش‌های فناوری

ما معمولاً تمایل داریم مسائل را با استفاده از رویکردهای نامناسب[3] حل کنیم. به‌کارگیری رویکردهای فناورانه برای حل مسائل اجتماعی با خطرات چشمگیری همراه است. البته، به‌کارگیری راه‌حل‌های اجتماعی، حقوقی و اقتصادی برای رفع مشکلات فناورانه نیز خطراتی را به دنبال دارد. در این میان، باید در مورد کاربردهای فناوری نیز دقت کنیم. به‌طور مثال:

ـ تلاش‌هایی که با توسل به طرح‌ها و اقداماتی از قبیل دفاع موشکی ملی، کارت‌های شناسایی ملی، اسکن کردن چهره و بمباران غارها برای پیشگیری از تروریسم انجام می‌گیرد: کارت‌های شناسایی ملی را تنها می‌توان دنباله روند صدور گواهی‌نامه‌های رانندگی قلمداد کرد، اما تعمیم این کاربرد به کارت‌های شناسایی ملی، خطرات جدی در پایگاه‌های اطلاعاتی و زیرساخت‌ها به دنبال دارد؛ دراین‌باره می‌توان به مواردی از قبیل سرقت هویت، داخلی‌های (خودی‌های) غیرقابل اعتماد و غیره اشاره کرد.

ازاین‌گذشته، چنین کارتی از اقدامات تروریست‌های یازده سپتامبر، به‌ویژه کسانی که تغییر چهره دادند ولی در ظاهر، هویت‌های مشروعی داشتند، جلوگیری نکرده است.

---

1. George Orwell
2. Boondocks
3. Inappropriate

اسکن کردن چهره معمولاً نتایج مثبت زیادی را ارائه می‌دهد که البته جعلی‌اند، چرا که در زمان حمله یازده سپتامبر تنها چهره‌های معدودی اسکن شده بودند. احراز هویت با ابزارهای زیست‌ـ سنجی، در حال حاضر در برنامه‌های رایانه‌ای فوق‌العاده حساس در مقیاسی کوچک وجود دارد، اما به‌کارگیری این برنامه‌ها در مقیاسی عام، سؤال‌برانگیز به‌نظر می‌رسد. معمولاً ما این مسئله را داریم که درب جلویی منزل را قفل می‌زنیم و درب پشتی را باز می‌گذاریم. از اطمینان مفرط به این فناوری‌ها برحذر باشید، زیرا تهدیدهای بسیاری می‌توانند این فناوری‌ها را دور بزنند.

ـ تلاش‌ها برای کنترل مرزهای الکترونیکی از جمله تلفن‌ها، فکس‌ها، تلویزیون، رادیو و اینترنت.

ـ تلاش‌ها برای سانسور کردن تلاش‌هایی که برای مخالفت با برخی از انواع اطلاعات از قبیل فیلم‌های مستهجن با فیلترینگ انجام می‌گیرد، در این مقوله قابل بررسی است. برای مثال حکومت‌های ایالتی و دولتی فدرال آلمان توافق کردند که هرزه‌نگاری را به‌استثنای ساعات ۱۱ شب تا ۶ صبح در سراسر جهان ممنوع کنند.

ـ تلاش‌ها برای جلوگیری از نفوذ ویروس‌ها با فیلتر به‌جای طراحی سیستم‌هایی برای مقابله با آنها.

ـ تلاش‌ها برای جلوگیری از اسپم کردن[1] اطلاعات که بیشتر با اشتیاق بسیار برای مسدود کردن پست الکترونیک‌های مهم انجام می‌گیرد.

فناوری می‌تواند برای کل جهان معجزه کند، اما این تنها در صورتی است که بتوانیم خود را از منجلاب آزمندی منفعت‌جویانه و ساده‌انگارانه بیرون بکشیم. بازار و تجارت همه مشکلات ما را حل نخواهد کرد ما نمی‌توانیم بر جهان مسلط شویم و کنترل داشته باشیم. البته در توان ما هم نیست که به‌طور کامل انزواگرایی پیشه کنیم.

باید تبعات و الزاماتی را که رفتارهای ما در سطح جهان به بار می‌آورند، در نظر داشته باشیم. اقتصاد جهانی، محیط زیست جهانی و مبارزه با فقر و گرسنگی در سراسر جهان، موضوعات مطرح و مهمی به شمار می‌آیند. ما به‌ظاهر از بهبود وضعیت آموزش‌وپرورش طرف‌داری می‌کنیم اما به‌نظر می‌رسد که آموزش‌وپرورش فاقد شاخص‌های کمی و کیفی

1. Spamming

مناسب می‌باشد و بر یافته‌های ناچیز برگرفته از اینترنت تأکید می‌کند، همچنین، به‌نظر می‌رسد که تفکر خلاقانه در آموزش‌وپرورش بی‌مقدار شمرده می‌شود.

بهینه‌سازی‌هایی که بر پایه مجموعه‌ای تنگ‌نظرانه از مفروضات‌اند (برای مثال، چه چیزی به خیر و صلاح شخص من، یا خانواده‌ام، یا شرکتم، یا کشورم به‌نظر می‌رسد؟) نتایجی را به بار می‌آورند که با بهینه‌سازی‌های مبتنی‌بر ارزیابی واقع‌گرایانه از تبعات و پیامدهایی که در درازمدت پدیدار می‌شوند و در بیشتر مواقع نیز الزاماً ملی هم نیستند، بسیار فرق دارد. انرون نمونه بارزی از مؤسسه‌هایی است که نه براساس دیدگاه‌های کارگران و سهام‌داران خود یا حتی در سطحی وسیع‌تر، مطابق با خیر و صلاح ملت یا جهان، بلکه براساس دیدگاه‌های تعداد معدودی از افراد به بهینه‌سازی فعالیت‌های خود می‌پردازد.

سوخت فسیلی نمونه دیگری است. سیاست‌های بر پایه این اندیشه که نفت مهم‌ترین کالا در جهان است، با سیاست‌های انسان‌ـ محور (یعنی سیاست‌هایی که بر پایه مبتنی‌بر یافتن منابع جایگزین انرژی، حفظ منابع انرژی یا تعدیل مصرف انرژی می‌باشند) تفاوتی ریشه‌ای دارد. برای یک مرد چکش به‌دست، همه چیز شبیه میخ به‌نظر می‌رسد. برای کسی که در بخش نفت سرمایه‌گذاری می‌کند، همه چیز به اسکناس دلار شباهت دارد. برای کسی که به بقای سیاره زمین و انواع موجودات ساکن در آن علاقه‌مند است، حفاظت از محیط زیست، یک آرمان به‌شمار می‌آید.

تحقیقات آینده‌نگرانه در برابر منافع کوتاه‌مدت دو عامل انگیزشی افراطی‌اند که رویکردهای بسیاری در حد واسط این دو قرار می‌گیرند. در مورد تحقیقات آینده‌نگرانه که برای سیاره زمین کاملاً ضروری است، ما بسیار کوته‌نظر شده‌ایم. ما با وجود آنکه نمی‌توانیم آن‌چنان‌که باید و شاید از تحقیقات پایه‌ای حمایت کنیم، غلّات را به‌طور بی‌رویه مصرف می‌کنیم. تعداد تحقیقات آینده‌نگرانه برجسته‌ای که بسیار مفید باشند، اندک است؛ برای مثال، تحقیقات اندکی در حوزه‌های مخابرات، لیزر، سیستم‌های رایانه‌ای، بیوتکنولوژی، فهم بازشناسی کلام (که به‌عنوان یک منبع پول‌ساز عظیم برای صنعت تولید تلفن ظهور کرده است) انجام گرفته است. اما در حوزه رایانه و به‌ویژه تولید انبوه نرم‌افزار، مقدار زیادی از مهم‌ترین تحقیقات درزمینه سیستم‌های مقاوم مورد بی‌توجهی قرار گرفته است و در مقابل، تولید نرم‌افزارهایی که فقط بازارپسند باشند

تشدید شده است. البته، وقتی به سرگرمی‌های پرزرق و برق و شخصیت‌های تخیلی می‌رسیم، استعدادمان گل می‌کند. طراحان نرم‌افزار که هدفشان فروش انبوه در بازار است، مهارت بسیاری درزمینه خلق خوک‌های در حال رقص روی صفحه‌های نمایشگر شما دارند. ما دستگاه‌های تلویزیون و سایر رسانه‌های تصویری را به‌گونه‌ای تولید می‌کنیم که تصاویر سرگرم‌کننده‌ای را به نمایش بگذارند، اما توجه به محتوای این رسانه‌ها در بیشتر مواقع، در آخرین اولویت‌های تولیدکنندگان قرار دارد. تولید سیستم‌های حساس ـ که می‌باید بدون اشتباه، در فضایی مطمئن و قابل اعتماد عمل کنند ـ همواره در وضعیت بسیار بد و نامطلوب است.

به‌نظر می‌رسید که ما به‌عنوان یک جامعه، با پیمودن مسیری تکاملی وارد این قالب ذهنی شده‌ایم که «هرچیزی مادامی امکان‌پذیر است که شما بتوانید از آن فرار کنید». به‌نظر می‌رسد این وضعیت هم در مورد شرکت‌ها و هم در مورد افراد صدق می‌کند و تأثیراتی جدی بر محیط زیست و آینده تمدن در درازمدت دارد.

از قرار معلوم، ما از تاریخ، هیچ نمی‌آموزیم. بازمی‌گردیم به انرون در ژانویه ۲۰۰۲: *نیویورکر*[1] مقاله‌ای به قلم جیمز سورویکی[2] در مورد حقه‌ای شبیه حقه‌های انرون با عنوان «راه‌آهن پاسیفیک مرکزی»[3] به چاپ رسانید. به نوشته این مقاله، للاند استنفورد[4] و شرکای وی، یک شرکت تابعه پیمانکاری را تأسیس کردند و حداقل پنجاه میلیون دلار پول اضافی از دولت کلاهبرداری کردند. البته پس از این ماجرا همه اسناد ناپدید شدند.

هرچند به‌نظر می‌رسد که ما به‌عنوان یک جامعه درآوردن نوشدارو پس از مرگ سهراب، به‌نسبت خوب عمل می‌کنیم، ولی کارنامه بسیار بدی هم درزمینه انجام واکنش‌های فوری در برابر علائم هشداردهنده داریم. بااین‌حال، باید اعتراف کرد که زیرساخت‌های حساس و فناوری‌های ارتباطات رایانه‌ای که ما در اختیار داریم، بسیار سرشار از آسیب‌پذیری‌هاست. ازاین‌رو، در آینده باید به مراتب فعالانه‌تر و مؤثرتر عمل کنیم. متأسفانه به‌نظر می‌رسد بزرگ‌ترین مانع فراروی ما این است که ما هرگز به‌طور

---

1. The New Yorker
2. James Surowiecky
3. Central Pacific Railroad
4. Leland Stanford

عملی «مقابله با رویدادهای پرل‌هاربر[1] یا یازده سپتامبر با ابزارهای الکترونیکی» را تجربه نکرده‌ایم و ازاین‌رو، ناگزیر نبوده‌ایم که تدابیری همه‌جانبه و کافی برای محافظت از زیرساخت‌هایمان بیاندیشیم. این، معضلی برجسته و خاص درزمینه نحوه تأمین امنیت است؛ اگر شما در آتش این وقایع نسوخته‌اید، هیچ انگیزه‌ای برای انجام اقدام جدی ندارید.

ما باید بیاموزیم که آینده‌نگری به خرج دهیم، نگاه جهانی داشته باشیم و در این راستا بیشتر سرمایه‌گذاری کنیم؛ نه اینکه فقط نیازهای کوتاه‌مدت محلی را برآورده سازیم. بهره‌مندی از بینش آینده‌نگرانه، عاملی اساسی و ضروری است. تقریباًهمه کارهایی که ما انجام می‌دهیم از جمله سیاست‌های اقتصادی، سیاستگذاری‌ها در حوزه انرژی و سیاست‌های حوزه فناوری بیش‌ازپیش به هم پیوند خورده‌اند. به‌عبارت بهتر، نباید فقط به بهینه‌سازی امور در مقیاسی کوچک بپردازیم، بلکه باید همیشه این تصویر بزرگ را در نظر بگیریم و در راستای روشی که به ایثاری به‌مراتب بیشتر نیاز دارد، گام برداریم. نهادهای دمکراتیک به‌طور مسلم بهترین امیدها برای اصلاح رویه دولت ملت‌ها و بهبود سیاست‌ها در حوزه فناوری‌اند چرا که روند تکامل سازنده اینترنت را تضمین می‌کنند.[2]

بدیهی به‌نظر می‌رسد که تقریباً عوامل دیگری هم در پرورش تروریسم جهانی نقش دارند. اما باید خاطرنشان کرد که با لابی‌گری‌های فشرده به‌آسانی می‌توان بر رفتار دمکراسی‌ها تأثیر نهاد و آنها را به فساد کشاند. قضیه انرون نمودار پدیده‌ای است که می‌توان آن را «باج‌سبیل‌های ترش و شیرین» نامید.[3]

این وضعیت در مورد تروریسم که موضوع مورد علاقه شخصی من است و من آن را با استعاره درآمیخته‌ام، صدق می‌کند: «ما با عصر جدیدی روبه‌روایم که در آن، گریه پاندورا خارج از لانه است و اجنه نیز به آن تعفن‌گاه باز نخواهند گشت».

مدت‌ها پیش براندیس[4] قاضی دیوان عالی ایالات متحده اظهار داشت دولت‌ها با استناد به الگوهایی که در گذشته وجود داشته است، شهروندان را تعلیم می‌دهند.

---

1. Perl Harber

۲. Andora: در اساطیر یونان، اولین زنی که خلق شد ـ م.

۳. Pork Barrels: در آمریکا، به بودجه یا طرح عمرانی‌ای اطلاق می‌شود که به‌دلیل جلب آرای محلی به‌جای خاصی اختصاص می‌یابد ـ م.

4. Brandeis

ازاین‌رو، بجاست که شعار اقدامات ما این باشد که «فرض کنید دیگران، نـه آنچـه را کـه شما می‌گویید، بلکه آنچه را که شما انجام می‌دهید، انجام خواهند داد».[۷]

به همین جهت، نتیجه می‌گیریم که ما، به‌عنوان افـراد یـا ملـت‌هـا، بایـد الگوهـای استوار و منطقی ایجاد کنیم که هم به حقوق بشر و رفاه آدمیان در سـطح بـین‌المللـی و هم به سیاست‌های زیست‌محیطی که منطق اقتـصادی دارنـد، پایبنـدی عمیقـی داشـته باشند. در این میان، اگر فناوری به‌صورت منطقی مورد استفاده قرار گیرد، نقـش مهمـی در این زمینه می‌تواند ایفا کند. اما، این پدیـده در بیـشتر مواقـع، همـان مـسائلی را کـه می‌کوشد حل کند، تشدید می‌نماید و گاهی اوقات حتی معـضلات جدیـدی را بـه‌وجـود می‌آورد. برای مثال، در حال حاضر، این خطر جدی وجود دارد که شـکاف عظـیم میـان داراها و ندارها هر روز بیشتر می‌شود، زیرا فناوری در بیشتر مواقع، تنها بـه داراهـا سـود می‌رساند. فناوری، علاوه‌بر این، نوعی حرکت مارپیچی جاسوس در برابر جاسـوس ایجـاد می‌کند که در آن، مهاجمان، مزیتی به‌مراتب بیشتر از مـدافعان دارنـد. ایـن وضـعیت در مورد آن تدابیر امنیتـی کوتـه‌فکرانـه‌ای کـه جهـان را بـه‌عنـوان یـک سیـستم در نظـر نمی‌گیرند آشکارا صدق می‌کند. ثمربخشی راه‌حل‌ها در نهایت نه مستلزم توجـه محـض به ملاحظات داخلی، بلکه در گرو توجه فراگیر به امور بین‌المللی خواهد بود.

پی‌نوشت‌ها

1. L. Lasker and W.F. Parkes, War Games, USA, 1983.

2. For Extensive Background Information, See the Following: Peter Neumann website: http://www.csl.sri.com/neumann; The Illustrative Risks compendium indexes to Risks Cases: http://www.csl.sri.com/neumann/illustrative.html; and the archives of the Risks Forum: http://risks.org.

3. People for Internet Responsibility: http://pfir.org/.

4. Department of Justice, White Paper: The *Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision* Directive 63, 22 May 1998. Available at http://www.usdoj.gov/criminal /cybercrime/white_ Pr.htm.

5. Peter Neumann Website: http://www,csl.sri.com/neumann/illustrative.html.

6. For Example: N.G. Leveson, and C.S. Turner. 'An Investigation of the Threrac-25 Accidents', IEEE Computer, 26(7), July 1993, 18-41.

7. A. McGruder, 'The Boondocks', *San Francisco Chronicle*, 30 January 2002.

فصل ششم دفاع موشکی؛ نخستین گام‌ها به‌سوی جنگ در فضا

دیوید وب*

۱-۶ استفاده نظامی از فضا

اصطلاح انقلاب در امور نظامی[1] نمایانگر حرکتی در جهت گردهم آوردن فناوری‌ها به‌منظور کمک به پیشبرد و مدیریت جنگ است. در طول چند دهه گذشته، ارتش آمریکا، سیستم‌های فناورانه خود را به‌نحوی توسعه داده است که تا جایی که امکان دارد در هر میدان جنگی بتوانند شرایط آگاهی کامل نیروها از اوضاع جنگ را فراهم آورند. این سیستم‌های فرماندهی و کنترل و شبکه‌های رایانه‌ای با بهره‌برداری از فناوری فضایی در یکدیگر ادغام شده و به‌صورت یک سازوکار یکپارچه درآمده‌اند.

این فصل استدلال خواهد کرد که ایالات متحده آمریکا اتکای «انقلاب در امور نظامی» به فضا را لازمه استقرار سیستم دفاع فضایی فعال می‌داند. بیانیه‌های دولت‌ها و معاهدات بین‌المللی در عمل چنین سیستمی را غیرقانونی اعلام کرده‌اند؛ البته چنین سیستمی با روح حاکم بر معاهدات بین‌المللی و بیانیه‌های دولت‌ها منافات دارد. در این میان، رویدادهای یازده سپتامبر و جنگ علیه تروریسم فرصت مغتنمی را برای توسعه سیستم‌های دفاعی جنگ در فضا (در لباس دفاع موشکی) فراهم آورده‌اند؛ به‌طور قطع، توسعه این سیستم‌ها گامی به‌سوی اجرای سیستم‌های تهاجمی به‌شمار می‌آیند که درصورت نیاز برای حمله به کشورهای دیگر مورد استفاده قرار خواهند گرفت.

استفاده ارتش‌های جهان از فضا، امروزه به پدیده‌ای جاافتاده و متعارف مبدل شده است و برای آمریکا که تجربه‌های زیادی در طول جنگ‌های متعدد اندوخته است، ضرورت یافته است؛ این جنگ‌ها عبارت‌اند از:

---

* David Webb

1. Revolution in Military Affairs (RMA)

۱. عملیات طوفان صحرا، کویت، عراق، ۱۹۹۱،
۲. عملیات نیروهای متحدین، کوزوو، ۱۹۹۹،
۳. عملیات آزادی مستمر، افغانستان، ۲۰۰۲،
۴. عملیات آزادسازی عراق، عراق، ۲۰۰۳.

در طول عملیات آزادسازی عراق، اطلاعات ماهواره‌ای ایالات متحده باعث شد واکنش‌های نظامی در قبال حرکت نیروهای بعثی در کمتر از چند دقیقه انجام گیرد. این در حالی است که پیش از این، این واکنش‌ها ساعت‌ها و در برخی مواقع روزها طول می‌کشید. این کوتاه شدن به‌اصطلاح «زنجیره کشتن»[1] به این معناست که حالا دیگر، فضا به تعیین‌کننده‌ترین میدان و عرصه نظامی مبدل شده است.

هم‌اکنون، ارتش آمریکا حتی در هر جنگ متعارف نیز سیستم‌های فضایی پیش‌بینی هوا (برنامه دفاعی حمایت از طرح‌های هواشناسی)[2]، ماهواره‌های ارتباطات نظامی[3] (که بین مراکز فرماندهی نیروهای نظامی و نیز بین نیروهای نظامی ارتباط برقرار می‌کنند)، ماهواره‌های جاسوسی و مراقبت[4] (که برای رهگیری ارتباطات دشمن و گردآوری تصاویر تحرکات نیروها و جابه‌جایی تسلیحات مورد استفاده قرار می‌گیرند)، ماهواره‌های مجهز به سیستم هشدار سریع (که اطلاعاتی را درزمینه نحوه پرتاب موشک ارائه می‌دهند) و ماهواره‌های نظامی مجهز به سیستم موقعیت‌یابی جهانی (که به نیروها و نفربرهای نظامی کمک می‌کنند تا به‌صورت صحیح جهت‌یابی نمایند و اهداف را بادقت و سرعت هرچه تمام‌تر مشخص سازند و بمب‌های هوشمند و هواپیماهای بدون سرنشین را هدایت کنند) را در اختیار دارد.

ایالات متحده آمریکا در جنگ عراق ۶۶۰۰ دستگاه ادوات نظامی مجهز به سیستم موقعیت‌یابی جهانی و افزون‌بر ۱۰۰ هزار گیرنده دقیق و سبک ـ وزن سیستم موقعیت‌یابی جهانی مستقر ساخت.(۱) ارتش ایالات متحده در این جنگ، ده‌ها بار از همان امکانات ماهواره‌ای که در جنگ سال ۱۹۹۱ استفاده کرده بود، استفاده کرد. نه روز قبل از آغاز جنگ، سیستم ارتباطات ماهواره‌ای جدیدی را مستقر ساخت که می‌توانست همه نیروهای

---

1. Kill Chain
2. Defence Meteorological Support Program
3. Military Communications Satellites (MILSTAR)
4. Spionage and Surveillance Satellites

نظامی آمریکا را که در زمین، دریا و هوا عمل می‌کردند با پنتاگون، کاخ سفید، وزارت امور خارجه و فرماندهی فضایی آمریکا ارتباط دهد. افزون‌بر ۱۰۰ ماهواره نظامی از عملیات جنگی آمریکا و بریتانیا پشتیبانی می‌کردند، ۲۷ ماهواره مجهز به سیستم موقعیت‌یابی جهانی به‌منظور کمک به تعیین موقعیت گروه‌های عملیات ویژه و اهداف نظامی، فعال و در دسترس بودند و در حدود ۲۴ ماهواره ارتباطاتی، امور فرماندهی و کنترل را تسهیل می‌کردند و هشدارها درزمینه حملات موشکی را به اطلاع نیروهای نظامی می‌رساندند. تجهیزات پیش‌بینی هوا، سیستم‌های تلویزیونی و سایر سیستم‌های مرتبط با این حوزه نیز فعال بودند. پرواز ماهواره فضایی اندیور[1] در فوریه ۲۰۰۰ برای نقشه‌برداری سه‌بعدی از اهداف نظامی در عراق از تجهیزات راداری استفاده کرد.(۲) منابع انسانی نیز وسیع‌اند. سرلشکر جاد بلیسدل[2] مدیر عملیات فضایی[3] تخمین زد که ۳۳۶۰۰ نفر در ۳۶ پایگاه نظامی در سراسر جهان در فعالیت‌های «جنگ فضایی» درگیر بودند.(۳)

این رشد چشمگیر کاربرد فناوری فضایی در عملیات‌های جنگی بدون مشکل نیست. ساختار سیستم‌های تسلیحاتی مدرن به‌گونه‌ای است که ماهواره‌های ارتباطاتی می‌باید مقادیر عظیمی از اطلاعات این سیستم‌ها را به مقصدهای مورد نظر انتقال دهند. برای مثال، هواپیماهای بدون سرنشین گلوبال هاوک[4] تقریباً در هر ثانیه به ۵۱۰۰ مگابایت امواج اطلاعاتی نیاز دارد (این رقم پنج برابر کل حجم داده‌هایی است که کل ارتش آمریکا در روند عملیات طوفان صحرا بدان نیاز داشت). در سال ۲۰۰۲، روزنامه *وال استریت ژورنال*[5](۴) گزارش داد که آمریکا در طول عملیات آزادی مستمر، توانست چهار فروند، یعنی نیمی از هواپیماهای بدون سرنشین خود را در عملیات‌های جنگی به‌کار بگیرد؛ زیرا باند کافی برای پرواز همه آنها در اختیار نداشت. شرایط در آینده احتمالاً سخت خواهد بود؛ شورای علوم دفاعی[6] در بررسی‌های خود پیش‌بینی کرده است که تا سال ۲۰۱۰ پنتاگون برای انجام امور پشتیبانی یک جنگ بزرگ به ۱۶ گیگابایت امواج اطلاعاتی در هر ثانیه نیاز خواهد داشت.(۵)

---

1. Endeavour
2. Major General Judd Blaisdel
3. Space Operation
4. Global Hawk
5. WAll Street Journal
6. Defense Science Board

البته تنها ایالات متحده نیست که از فضا برای اهداف نظامی خود استفاده می‌کند. روسیه نیز چند برنامه ساخت ماهواره‌های نظامی در دست اجرا دارد. این کشور پنج مدل از ماهواره‌های شناسایی (که می‌توانند تصویربرداری‌های مقطعی انجام دهند و داده‌های توپوگرافیک و نقشه‌برداری را به‌روز نمایند) و دو سری از ماهواره‌های جاسوسی الکترونیک[1] را راه‌اندازی کرده است. البته، چهار مدل از ماهواره‌های ارتباطی نظامی اختصاصی نیز (که از سال ۱۹۹۷ تاکنون در حدود ۲۴ بار به فضا پرتاب شده‌اند ولی در حاضر برخی از آنها دیگر کاربرد عملیاتی ندارند) در اختیار دارد.(۶) علاوه‌بر این، روسیه تعدادی ماهواره که در صنعت هواپیمایی و امور جهت‌یابی به‌کار می‌روند و سیستم ماهواره ملی جهان‌گستر،[2] که کاربرد دوگانه دارد و به سیستم موقعیت‌یاب جهانی شبیه می‌باشد، بهره‌مند است.(۷) ازاین‌گذشته، قرار است نیروهای مسلح روسیه تا قبل از سال ۲۰۰۵ به گیرنده‌های سیستم ماهواره ملی جهان‌گستر مجهز شوند.(۸) ازاین‌رو، روسیه سیستم‌های کنترل فضا و هشدار اولیه را نیز در موشک‌های بالستیک خود نصب کرده است.

استفاده نظامی از فضا به‌سرعت رو به گسترش است. چین چند ماهواره نظامی به فضا پرتاب کرده است. هند ماهواره‌های تصویربرداری و ارتباطاتی در اختیار دارد که برای کاربردهای نظامی نیز مناسب‌اند. رژیم صهیونیستی هم از ماهواره‌های نظامی بهره‌مند است و هم طرح‌هایی برای پرتاب ماهواره‌های جدید ارتباطاتی، تصویربرداری و راداری به فضا در دست اجرا دارد؛ و در حال حاضر در نظر دارد سیستمی را عملیاتی سازد که می‌تواند درصورت ضرورت، ماهواره‌های کوچک را از درون هواپیمای جنگنده نظامی به فضا پرتاب نماید.(۹) کشورهای دیگر از جمله برزیل، پاکستان و اکراین توانمندی استفاده نظامی از فضا را به‌صورت بالقوه یا بالفعل در اختیار دارند.(۱۰) استرالیا دارای ماهواره‌ای است که کاربرد دوگانه نظامی ـ تجاری دارد.(۱۱) اما در اروپا، بریتانیا و ایتالیا به‌طور گسترده از ماهواره‌های نظامی برای تصویربرداری و تسهیل ارتباطات استفاده می‌شود. سازمان فضایی اروپا،[3] که سازمانی کاملاً مستقل به‌شمار می‌آید،[4] (۱۲) به‌تدریج رفته‌رفته سیاست‌زده شده است (کمیسیون اروپا هر روز بیش از گذشته کنترل

1. Electronic Intelligence (ELINET) Satellites
2. Global National Satellite System (GNSS)
3. European Space Agency (ESA)
4. Galileo GPS Systems

خود را بر این سازمان اعمال می‌کند)[۱۳] و حتی احتمال دارد که با پیوستن به سیستم‌های موقعیت‌یاب جهانی گالیله، بعد نظامی نیز به خود بگیرد.[۱۴]

۲-۶ برنامه‌های ضدماهواره‌ای

این اتکا به فضا در حوزه‌های فرماندهی، ارتباطات، رایانه، جاسوسی، مراقبت، کنترل و شناسایی، نقص جدی نیز دارد: سیستم‌های ماهواره‌ای مستقر در فضا در برابر حملات سیستم‌های ضدماهواره‌ای به‌شدت آسیب‌پذیرند. اندکی قبل از انتصاب خود به‌عنوان وزیر دفاع آمریکا دونالد رامسفلد ریاست کمیسیون ارزیابی امنیت ملی ایالات متحده در حوزه تشکیلات سازمانی و مدیریت فضا را برعهده داشت.[۱۵] این کمیسیون در ژانویه ۲۰۰۱ طی گزارشی اعلام کرد: «برای پیشگیری از وقوع یک پرل‌هاربر فضایی[1] در آینده باید موضوع احتمال حمله به سیستم‌های فضایی آمریکا را جدی گرفت».

درحقیقت، اولین حمله به سیستم ماهواره‌های نظامی آمریکا در سال ۲۰۰۳ به‌وقوع پیوست. در این سال، ارتش عراق کوشید سیستم موقعیت‌یاب جهانی آمریکا را از کار بیاندازد اما ناکام ماند.[۱۶] جیمز رشه[2] فرمانده نیروی هوایی آمریکا اظهار داشت این تلاش برای ایجاد اختلال در تسلیحاتی که به‌وسیله سیستم موقعیت‌یابی جهانی هدایت می‌شوند، آشکارا نشان داد که جهان به نقش مهم عامل فضا در ارتش آمریکا پی برده است. جالب اینکه در سال ۲۰۰۴، خود نیروی هوایی آمریکا نیز با هدف ارتقای آمادگی برای مقابله با این‌گونه حملات، چند سیستم ایجاد پارازیت را که قابل برگشت بود، راه‌اندازی کرد.[۱۷] اما سناریوی تهدیدآفرین‌تر همانا احتمال به‌کارگیری سیستم‌های تسلیحاتی علیه ماهواره‌هاست.

از آغاز ظهور عصر فضا، روسیه و ایالات متحده آمریکا به‌صورت علنی چندین طرح تحقیقاتی در مورد برنامه‌های ضدماهواره‌ای انجام داده‌اند. تلاش‌هایی که در دهه ۱۹۵۰ آغاز شد به آن فناوری‌های موشکی مربوط می‌شد که برد پرتاب آنها تا محدوده داخل جو بود، اما از آن تاریخ تاکنون، سیستم‌های پیشرفته‌تری گسترش یافته‌اند.

---

1. Space Perl Harbor
2. James Rocshe

۶-۲-۱ اتحاد شوروی و روسیه

در دهه ۱۹۶۰ اتحاد شوروی، مسکو را در موشک‌های بالستیک قاره‌پیما که به کلاهک‌های هسته‌ای مجهز بودند و نقش سیستم موشکی ضدبالستیک را ایفا می‌کردند، محصور کرد. این موشک‌ها توانمندی‌های ضدماهواره‌ای نیز داشتند، زیرا می‌توانستند همه سیستم‌های مستقر در فضا را که نزدیک محل انفجار آنها باشد نابود سازند. اما سیستم ضدموشکی اصلی‌ای که اتحاد شوروی توسعه داد، سیستم ضدماهواره‌ای هم‌مدار[۱] بود. توسعه موشک‌های جنگنده استریبتال اسپوتنیکف[۲] در اوایل دهه ۱۹۶۰ آغاز شد و اولین پروازهای آزمایشی این موشک‌ها در سال ۱۹۶۸ انجام گرفت. قرار بود این سیستم ضدماهواره‌ای در مداری نزدیک مدار هدف استقرار یابد و در درون یک یا دو مدار، هدف را نابود سازد. آزمایش‌های اولیه‌ای که در فاصله سال‌های ۱۹۶۳ تا ۱۹۷۲ انجام گرفت، نشان داد که این سیستم از ارتفاعات ۲۳۰ تا ۱۰۰۰ کیلومتری می‌تواند عمل کند و کارگر افتد. در آن برهه زمانی نیز اعلام شد که این سیستم عملیاتی شده است.

شوروی‌ها بعد از امضای معاهده موشک‌های ضدبالستیک در سال ۱۹۷۲، آزمایش این سیستم را به‌طور موقت متوقف ساختند، اما این آزمایش‌ها را بار دیگر در سال ۱۹۷۶ از سر گرفتند و تا سال ۱۹۸۲ نیز فعالیت‌های خود را ادامه دادند. در طول این دوره، برد مؤثر این سیستم‌ها از ارتفاع ۱۶۰ کیلومتر به ۱۶۰۰ کیلومتر افزایش یافت.(۱۸) در سال ۱۹۸۳، اتحاد شوروی اعلام کرد پرتاب این سیستم‌های ضدماهواره‌ای را به‌طور موقت تعلیق می‌کند به این شرط که هیچ کشور دیگری چنین سیستمی را مستقر نسازد. به‌نظر می‌رسد روسیه نیز همچنان این سیاست را اتخاذ کرده است.(۱۹) کتاب *راهنمای فضا* چاپ ۲۰۰۲-۲۰۰۱، برنامه روسیه درزمینه سیستم‌های ضدماهواره‌ای را «غیرفعال»[۳] توصیف می‌کند.

۶-۲-۲ ایالات متحده آمریکا

ایالات متحده آمریکا آزمایش‌های موشکی خود را در سال ۱۹۵۹ آغاز کرد، اما نتایج این آزمایش‌ها امیدوارکننده نبود، به‌طوری‌که این طرح[۴] در سال ۱۹۶۳ متوقف شد؛ ولی

---

۱. Co-orbital ASTA: موشکی که در جنگ جهانی دوم مورد استفاده قرار گرفت و مواد منفجره با خود حمل می‌کرد.

2. Istribital Sputnikov
3. Inactive
4. Project

بااین‌حال، طرح‌های مربوط به نیروی دریایی آمریکا همچنان تا اوایل دهه ۱۹۷۰ ادامه یافت. در دهه ۱۹۶۰، انهدام موشک‌ها با استفاده از انفجارهای هسته‌ای مورد توجه قرار گرفت. در سال ۱۹۵۸، یک آزمایش هسته‌ای ۱/۴ مگاتنی در ارتفاع ۴۰۰ کیلومتری بالاتر از اقیانوس آرام منفجر شد و سه موشک را منهدم ساخت. بااین‌همه، این احتمال وجود داشت که در اثر تشعشعات رادیواکتیو و ضربه‌های الکترومغناطیسی بر مناطق و سیستم‌های هدف‌گیری نشده[1] خسارت وارد شود؛ ازاین‌رو، این قبیل آزمایش‌های ضدماهواره‌ای نیز عملاً انجام نگرفت. با وجود این، از سال ۱۹۶۲ به بعد، سیستم‌ها و برنامه‌های موشک حامل کلاهک هسته‌ای به نام نایک زئوس[2] به‌گونه‌ای تعدیل شد که در حوزه سیستم‌های ضدموشکی کاربرد داشته باشد. تا سال ۱۹۶۶ سیستم ضدماهواره‌ای تک موشکی[3] براساس برنامه ۵۰۵ با اسم رمز «مادفلپ»[4] در جزیره «کواجالاین آتل»[5] واقع در اقیانوس آرام مستقر بود ولی از این تاریخ تا سال ۱۹۷۲، سیستم ضدماهواره‌ای ثر[6] که در اختیار نیروی هوایی آمریکا بود جایگزین آن گردید.(۲۰)

در سال ۱۹۷۶، گزارش‌ها حاکی از آن بود که ایالات متحده علاقه‌مند است فناوری ضدماهواره‌ای را تقویت کند و قصد دارد برنامه شاتل فضایی[7] خود را نیز گسترش دهد (چنین تلقی شد که این برنامه، توانمندی ضدماهواره‌ای را نیز در خود جای داده است). شوروی نیز در واکنش به این گزارش‌ها، در همان سال، آزمایش‌های ضدماهواره‌ای خود را ازسرگرفت. خود ایالات متحده نیز نگران گزارش‌های اغراق‌آمیز درزمینه فناوری لیزری و پرتوافکنی شوروی و کاربرد آنها در سیستم‌های ضدموشک‌های بالستیک بود و ازاین‌رو، برنامه ضدماهواره‌ای خود را با راه‌اندازی «سیستم کوچک پرتاب‌کننده موشک»[8] دوباره آغاز کرد. این سیستم از هواپیمای اف ۱۵ شلیک می‌شد، یک دستگاه هدف‌یاب حرارتی را با خود حمل می‌کرد و برای حمله به ماهواره‌هایی که در مدار پایین زمین قرار داشتند طراحی

---

1. Untargeted
2. Nike Zeus
3. Single-missile
4. Mudflap
5. Kwajalien Atoll
6. Thor
7. Space Shuttle
8. Air-launching Miniature Vehicle

شده بود. این موشک درواقع، متشکل از دو موشک بود: در مرحله اول، مدل جرح‌وتعدیل شده‌ای از موشک تهاجمیِ با بردِ کوتاه و در مرحله دوم، یک سیستم کوچک هدف‌یاب وات[1] این سیستم ضدموشکی را در ارتفاع بالا و یک هواپیمای اف ۱۵ در حالتی که با شیبی تند در حال صعود است، پرتاب می‌کرد. این حالت باعث می‌شد موشک در همان لحظهٔ شلیک، شتاب و سرعت مناسبی داشته باشد و با موفقیت به هدف خود در مدار اصابت نماید. بعد از مرحله اول، یعنی مرحله جدا شدن، در مرحله دوم، سیستم کوچک هدف‌یاب وات در مسیر اصابت به آن موشک هدف قرار خواهد گرفت به‌نحوی‌که اصابت با سرعتی بالا، ماهواره هدف‌گیری شده را منهدم خواهد کرد. ایالات متحده از سال ۱۹۸۴ تا سال ۱۹۸۶ پنج آزمایش موشکی انجام داد و در سپتامبر ۱۹۸۵، در اقدامی آزمایشی، با استفاده از این سیستم، یک ماهواره را هدف قرار داد.(۲۱) اما تخصیص بودجه چشمگیری برای توسعه بیشتر این سیستم‌ها به تدوین برنامه‌ای انجامید که در سال ۱۹۸۸ لغو شد. در همان سال، کنگره آمریکا با تمدید ممنوعیت یک‌جانبه درزمینه سیستم‌های موشکی ضدماهواره‌ای مخالفت کرد و توسعه سیستم‌های جدید ضدماهواره‌ای آغاز شد.

به‌موجب «ابتکار دفاع استراتژیک» که ریگان در سال ۱۹۸۳ به راه انداخت، پروژه‌های ضدماهواره‌ای به‌گونه‌ای اصلاح شدند که کاربرد آنها در موشک‌های ضدبالستیک و بالعکس امکان‌پذیر باشد. در همان ابتدا، در این طرح قرار بود از سیستم هدف‌یاب کوچک به‌عنوان مبنای تجمیع در ۴۰ ایستگاه فضایی که بیش از ۱۵۰۰ تجهیزات رهگیری را در خود جای داده بودند، استفاده شود. تا سال ۱۹۸۸، این پروژه در یک فرایند چهار مرحله‌ای، روند توسعه خود را پیموده بود. مرحله اول، سیستم سنگریزه‌های روشن[2] بود که تجهیزات رهگیری و سیستم‌های ردیابی متنوعی را دربرمی‌گرفت. مرحله دوم، ایستگاه‌های بزرگ‌تری را تعبیه می‌کرد و در مراحل بعدی نیز قرار بود تسلیحات لیزری و سلاح‌های پرتوافکنی نصب شود. چنین برنامه‌ریزی شده بود که این پروژه تا سال ۲۰۰۰ با صرف هزینه‌ای در حدود ۱۲۵ میلیارد دلار تکمیل شود.

تنها سلاح حرارتی که با موفقیت از درون پروژه ابتکار دفاع استراتژیک بیرون آمد،

---

1. Vought
2. Brillian Pebbles System

سلاح لیزری- شیمیایی پیشرفته نیمه مادون قرمز[1] بود. (۲۲) این سیستم در مدت تقریباً ۷۰ ثانیه می‌تواند یک مگاوات انرژی تولید کند. آمریکا این اقدام را عمدتاً در واکنش به اطلاعاتی که درزمینه فعالیت‌های اتحاد شوروی رسیده بود انجام داد؛ چرا که برمبنای آن اطلاعات جاسوسی، گفته می‌شد که اتحاد شوروی سیستمی شبیه به همین سیستم را راه‌اندازی کرده است. اما بعد از دیدار مقامات رسمی آمریکایی از آن کشور در سال ۱۹۸۹ معلوم شد که سیستم شوروی‌ها هیچ تهدیدی را در پی نداشت و تازه، مدت زمان زیادی تا تکمیل آن باقی‌مانده بود. کنگره نیز در سال ۱۹۹۱ استفاده از سلاح لیزری ـ شیمیایی پیشرفته نیمه مادون قرمز را ممنوع کرد. در سال ۱۹۹۳، توسعه سیستم ضدماهواره‌ای انرژی جنبشی که مقر آن در زمین بود و اجرای آن به نیروی زمینی ارتش واگذار شده بود، ممنوع گردید. اما توسعه این سیستم در سال ۱۹۹۶ با اختصاص بودجه‌ای ۴۵ میلیون دلاری که تا سال ۲۰۰۲ نیز ادامه داشت، از سر گرفته شد.

در سال ۱۹۹۶، ممنوعیت استفاده از سلاح لیزری- شیمیایی پیشرفته نیمه مادون قرمز پایان یافت و در سال بعد از آن، این سیستم با هدف قرار دادن یک ماهواره نیروی هوایی آمریکا که در ارتفاع ۴۲۰ کیلومتری بر فراز زمین در حرکت بود مورد آزمایش قرار گرفت. گویا هدف از آزمایش آن، بررسی این موضوع بوده است که آیا ماهواره آمریکا می‌تواند در برابر حمله لیزری مقاومت کند یا خیر. در حال حاضر، سیستم ضدماهواره‌ای انرژی جنبشی، پیش از رسیدن به مرحله عملیاتی به بودجه و آزمایش‌های بیشتری نیاز دارد. سیستم کوچک پرتاب‌کننده موشک نیز آزمایش نشده است و به‌نظر می‌رسد که هنوز نیز علاقه‌ای به احیای این سیستم وجود ندارد. بیش از همه، رژیم صهیونیستی به توسعه سیستم سلاح لیزری- شیمیایی پیشرفته نیمه مادون قرمز پرداخته است، ولی از سال ۱۹۹۷ تاکنون، آن را آزمایش نکرده و توانمندی‌های این سیستم نیز چندان مشخص نیست.

۳-۲-۶ چین

در حال حاضر، چین برنامه ضدماهواره‌ای که به‌صورت علنی اعلام کرده باشد ندارد؛ اما بااین‌حال، توانمندی فعلی چینی‌ها درزمینه پرتاب موشک را می‌توان دلیلی بر اقدام این

1. Mid- Infrared Advanced Chemical Laser (MIACL)

کشور درباره توسعه چنین سیستمی محسوب کرد.(۲۳) در سال ۱۹۸۰، چین برنامه‌ای را که درزمینه راه‌اندازی سیستم ضدماهواره‌ای کارآمد تدوین کرده بود لغو کرد؛ این سیستم از عناصری همچون دستگاه جنبشی کشتن افراد، سیستم لیزری قوی، سیستم تشخیص هدف و سیستم هشدار اولیه در فضا، تشکیل شده بود. از آن زمان تاکنون، تحقیقات مقدماتی درباره سیستم‌های ضدماهواره‌ای انجام گرفته است؛ و تا اندازه‌ای در قالب «برنامه توسعه فناوری‌های برتر»، بودجه‌ای بدان اختصاص یافته است.(۲۴)

در سال‌های ۲۰۰۳ و ۲۰۰۴، گزارش‌های سالیانه کنگره آمریکا در مورد قدرت نظامی چین به مقاله‌ای از روزنامه هنگ‌کنگی استناد کرد که گزارش داده بود چین، سیستم ضدماهواره‌ای به نام ماهواره کوچک انگلی[1] را توسعه داده و آزمایش کرده است. اما به‌نظر می‌رسد این اطلاعات از داده‌ای که در سال ۲۰۰۰، یک ماجراجوی خودشیفته و علاقه‌مند به مسائل نظامی به یک بولتن اینترنتی پست الکترونیک زده بود نشئت گرفته باشد.

۳-۶ تحولات اخیر در آمریکا

ایالات متحده آمریکا در این اواخر بودجه و پشتیبانی از برنامه‌های مرتبط با توسعه سیستم‌های ضدماهواره‌ای را تقویت کرده است. در سال ۲۰۰۴، پنتاگون ۱۶۸/۶ میلیون دلار برای توسعه فناوری تسلیحات فضایی و افزون‌بر دو میلیارد دلار برای برنامه‌های مرتبط با این‌گونه تسلیحات دریافت نمود.(۲۵) در آگوست ۲۰۰۴، نیروی هوایی ارتش آمریکا سندی را با عنوان *سند عملیات ضد ـ فضایی، دکترین نیروی هوایی ۲-۲.۱*[2] منتشر کرد. (۲۶) این سند، عملیات‌های آمریکا با استفاده از تسلیحات ضدماهواره‌ای و فضایی را برای اولین بار، به‌طور مبسوط تشریح می‌کند. ژنرال جان پی. جامپر،[3] رئیس ستاد نیروی هوایی ایالات متحده در مقدمه این سند بیان می‌کند که عملیات‌های ضد ـ فضایی نیروی دریایی آمریکا، روش‌ها و ابزارهایی می‌باشند که نیروی هوایی با آنها نه تنها برتری آمریکا در فضا را تحقق می‌بخشد بلکه تداوم این برتری را نیز تضمین می‌کنند. برتری آمریکا در فضا هم «آزادی در حمله» و هم «آزادی از حمله» را فراهم می‌نماید ... برتری فضایی و هوایی نخستین گام‌های

---

1. Parasitic Micro Satellite
2. Counterspace Operations, Air Force Doctrine Document 2-2.1.
3. General John P. Jumper

تعیین‌کننده در هر عملیات نظامی به‌شمار می‌آیند. «این سند به بحث در مورد موشک‌هایی که در هوا پرتاب می‌شوند، می‌پردازد و آن سیستم‌های ضدماهواره‌ای را که در مدار زمین قرار می‌گیرند یا در یک خط مستقیم برای هدف قرار دادن ماهواره‌های دشمن، فضا را می‌پیماند بررسی می‌کند؛ و در این راستا، این ادوات و تجهیزات را به‌عنوان سازوکارهایی احتمالی برای نابودسازی ماهواره‌ها معرفی می‌نماید».

بودجه‌ای که پنتاگون برای برنامه‌های مربوط به کنترل فضا و تأمین نیروی فضایی آمریکا در سال ۲۰۰۵ درخواست کرد، افزون‌بر سه میلیارد دلار بود؛ که در حدود ۲۱۷ میلیون دلار آن به پروژه‌های احتمالی درزمینه تسلیحات فضایی و ضدماهواره‌ای اختصاص می‌یافت. کمیته‌های تخصیص بودجه تقریباً یک میلیارد دلار از بودجه فضایی ـ نظامی را کسر کرد. (۲۷) بودجه توافقی کنگره و دولت ۱۰/۶ میلیون دلار به فعالیت‌های مقدماتی درزمینه استقرار سکوهای آزمایش ماهواره‌های رهگیری که در فضا مستقر بودند، اختصاص داده‌اند. (۲۸) متصدیان تخصیص بودجه در کنگره، برنامه به‌کارگیری نیروها و پرتاب موشک و ماهواره از قلمرو آمریکا[1] (۲۹) را در روندی حرکت دادند که در طول سال مالی ۲۰۰۵ به پیشبرد طرح‌های تسلیحاتی نپردازد و بودجه تجهیزات و دستگاه‌های هوایی مشترک[2] را به نصف (یعنی ۱۲/۵ میلیون دلار) کاهش دهد، (البته، هرگونه تلاش برای نصب سلاح بر این‌گونه دستگاه‌ها و تجهیزات یا اقدام به پرتاب آزمایشی آنها از روی موشک‌های بالستیک نیز ممنوع بود). سایر برنامه‌های فضایی نیز از قطع بودجه‌هایی که متصدیان تخصیص بودجه اعمال کرده بودند، رنج می‌بردند. از آن جمله، می‌توان به برنامه‌های رادار مستقیم در فضا، سیستم ارتباطات ماهواره‌ای گشتاری[3] و سیستم شناسایی ضد کنترل[4] اشاره کرد.

مقاله‌ای که اخیراً در مجله *گزارش دفاعی و روزمره هوا فضا*[5] به چاپ رسیده است،(۳۰) نقل قولی را از دانشمند عضو شرکت بین‌المللی برنامه‌های رایانه‌ای علمی و کاربردی[6] ذکر می‌کند. وی گفته است که این قطع بودجه‌ها تا حد زیادی به‌دلیل نگرانی در مورد استفاده

---

1. Force Application And Launch From The Continental US (FALCON)
2. Common Aero Vehicle (CAV)
3. Transformational Satellite Communications System (T-SAT)
4. Counter Surveillance Reconnaissance System (CSRS)
5. Aerospace Daily & Defense Report
6. Science Applications International Corporation (SAIC)

نامناسب از نیروها در فضا و جامعه پرسروصدای تسلیحات ضدفضایی است. آنها برای آنکه اعتبار خود را حفظ کنند فعال شده‌اند. افرادی که طرف‌دار تخصیص بودجه برای این برنامه‌های خاص هستند تاکنون آن‌چنان‌که باید و شاید در مناظره‌های مربوط به این حوزه نقش‌آفرینی نکرده‌اند. البته از پیتر هیوسی[1] عضو بنیاد دانشگاه دفاع ملی آمریکا نیز نقل قول آورده شده است. وی گفته است که لابی تسلیحات ضدفضایی تا اندازه‌ای به‌علت پشتوانه مالی قابل ملاحظه‌ای که دارند مؤثر بوده‌اند. به گفته هیوسی، متأسفانه نه تنها جامعه کنترل تسلیحات سنتی بلکه بنیادهای خاصی نیز ارائه کمک‌های مالی را (که به ۱۰۰ میلیون دلار در سال می‌رسید) به این لابی‌ها هدایت می‌کنند. این میزان کمک فراتر از مبالغی است که طرف‌داران آن هزینه کرده‌اند.

البته، موضوع تخصیص بودجه بیشتر به‌علت لابی‌گری شاید فقط در حد یک حرف و ادعا باشد و تردیدی نیست که این افزایش بودجه رخ خواهد داد، اما به‌نظر می‌رسد فعالیت‌های سازمان‌های غیردولتی از قبیل مرکز اطلاع‌رسانی دفاعی[2] (۳۱) مرکز مطالعات منع اشاعه تسلیحات کشتارجمعی[3] و مؤسسه مطالعات بین‌المللی مانتری[4] (۳۲) که کمک‌های سازمان‌های فعال ریشه‌دار از جمله شبکه بین‌المللی مهندسان و دانشمندان مخالف اشاعه،[5] (۳۳) شبکه جهانی مبارزه با قدرت تسلیحاتی و هسته‌ای در فضا[6] و سازمان حمایت از خلع سلاح هسته‌ای[7] را دریافت می‌کنند (۳۴) مؤثر بوده است.

پروژه دیگری که با مانع کمبود تخصیص بودجه مواجه شد، طرح مناقشه‌برانگیز «آزمایش مادون قرمز در میدان نزدیک»[8] است که آژانس دفاع موشکی[9] طراحی کرده است. اصلی‌ترین نقش این پروژه، گردآوری داده‌ها برای کمک به تفکیک میان موشک و لوله خروج گاز آن است. قرار بود این طرح، یک سکوی پرتاب به نام دستگاه قتل[10] را

---

1. Peter Huessy
2. Centre for Defense Information (CDI)
3. Centre for Non-Proliferation Studies
4. Monterey Institute of International Studies (CNS/MIIS)
5. International Network of Engineers and Scientists Against Proliferation (INESAP)
6. Global Network Against Weapons and Nuclear Power in Space
7. Compaign for Nucleawr Disarmament
8. Near Field Infrared Experiment (NFIRE)
9. Missile Defense Agency (MDA)
10. Kill Vehicle

راه‌اندازی کند. این سکوی پرتاب از توانمندی بالایی درزمینه از کار انداختن یا نابودسازی موشک‌هایی که مورد هدف قرار می‌گیرند یا ماهواره‌هایی که در مدار زمین قرار دارند برخوردار است و با استفاده از همین توانمندی با دقتی هرچه تمام‌تر موشک مورد نظر را هدف قرار می‌دهد. پروژه «آزمایش مادون قرمز در میدان نزدیک» در تابستان ۲۰۰۴ از موشک مینیاتوری پرتاب شد، ولی آژانس دفاع موشکی در مارس همان سال اعلام کرد به‌علت کمبود بودجه، عملیاتی شدن این پروژه به مدت یک سال به تعویق افتاده است؛ آژانس دفاع موشکی اعلام کرد تنها ۴۴/۵ میلیون دلار از بودجه ۸۲ میلیون دلاری را که برای سال ۲۰۰۴ درخواست کرده بود دریافت کرده است. پس از این، در جولای ۲۰۰۴، متصدیان تخصیص بودجه در کنگره، کل بودجه ۶۸ میلیون دلاری را که برای اتمام این پروژه درخواست شده بود، قطع کردند.

بااین‌حال کمیته تخصیص بودجه در مجلس سنا توصیه کرد که این برنامه باید همچنان تداوم یابد. در حال حاضر برنامه‌ریزی می‌شود که این پروژه در اواخر سال ۲۰۰۵ یا اوایل سال ۲۰۰۶ راه‌اندازی شود.(۳۵) مجله *اسپیس نیوز*[1] در اگوست ۲۰۰۴ گزارش داد که حسگر مناقشه‌برانگیز دستگاه قتل از این برنامه حذف خواهد شد. این گزارش اظهار داشت: «لورتا سانچز، عضو مجلس نمایندگان آمریکا از تلاش‌ها برای متقاعد کردن مقامات پنتاگون به بررسی بازسازی برنامه این پروژه و حذف دستگاه قتل حمایت کرده است». سانچز در هفته گذشته گفت: «بزرگ‌ترین دغدغه من این است که چه پیامی به سایر ملت‌ها می‌فرستیم».(۳۶)

یکی از حوزه‌های دیگر پیشرفت درزمینه توانمندی ضدماهواره‌ای، توسعه و آزمایش مدل‌های ماهواره‌های کوچک[2] است. دراین‌باره می‌توان به ماهواره‌های کوچک ۲۸ کیلوگرمی به نام «ایکس اس اس ـ ۱۰»[3] اشاره کرد که کار ویژه آنها عکس‌برداری از اشیا فضایی، نظارت و هدایت حرکت آنها می‌باشد.(۳۷) نیروی هوایی آمریکا اولین ماهواره در این مدل را در ژانویه ۲۰۰۳ به فضا پرتاب کرد. مدل بزرگ‌تری از این نوع ماهواره،

---

1. Space News
2. Micro - Satellite (MS)
3. XSS-10

ایکس اس اس ـ ۱۱[1] نام دارد که به مدت یک سال در مدار زمین باقی خواهد ماند و اطلاعات ویدئویی هم‌زمان به ایستگاه‌های مستقر در زمین ارسال خواهد کرد. گروه مطالعاتی بررسی پیش‌نیازها و فناوری ماهواره‌ای کوچک[2] که یک نهاد غیررسمی در نیروی هوایی ارتش آمریکا به‌شمار می‌آید، ـ در سال ۱۹۹۹ گزارشی را منتشر کرد. بارزترین توصیه این گزارش، این بود که نیروی هوایی آمریکا ماهواره‌های مدل ایکس اس اس ۱۰ را هرچه سریع‌تر در فضا مستقر سازد تا با آنها بتواند ماهواره‌های هدف را رهگیری و تصویربرداری نماید و درصورت لزوم علیه آنها اقدام کند.(۳۸)

بخش اعظم برنامه‌های فعلی آمریکا درزمینه توسعه فناوری‌ها و تسلیحات فضایی (از جمله، ادوات رهگیری در فضا(۳۹) و لیزرهای فضایی و هوایی زیر چتر دفاع موشکی قرار دارند و در قالب آن طراحی شده‌اند. همان‌گونه که دیوید وایت[3] و لورا جرج،[4] از اعضای اتحادیه دانشمندان نگران اظهار داشته‌اند: «توانمندی فعلی آمریکا درزمینه سیستم‌های ضدماهواره‌ای به‌نسبت محدود است و براساس سطوح فعلی تخصیص بودجه در این حوزه، به‌نظر می‌رسد که سیستم‌های ضدماهواره‌ای در استراتژی‌های آمریکا در اولویت‌های بالا قرار ندارند. اما برخی از سیستم‌های دفاع موشکی که پیش از این طراحی شده‌اند، توانمندی چشمگیری را در حوزه سیستم‌های ضدماهواره‌ای به زرادخانه ایالات متحده می‌بخشد و از پشتوانه مالی و پشتیبانی سیاسی چشمگیر و نیرومندی برخوردارند. در این راستا، وقتی توانمندی‌های ایالات متحده را تحلیل می‌کنیم و سیاست‌هایی را درزمینه محدودسازی سیستم‌های ضدماهواره‌ای پیشنهاد می‌کنیم می‌باید این واقعیت را نیز به یاد داشته باشیم».(۴۰)

به‌این‌ترتیب پروژه‌هایی که سیستم‌های ضدماهواره‌ای یا فضایی را آشکارا توسعه می‌دهند مشکلاتی را درزمینه جذب منابع مالی فراروی خود دارند و این وضعیت نیز بدیهی به‌نظر می‌رسد. اما شیوه‌های دیگری نیز برای جذب مقادیر هنگفتی منابع مالی در جهت توسعه این‌گونه سیستم‌ها وجود دارد. در این میان می‌توان به برنامه‌های فضایی مشابهی اشاره کرد که به‌ظاهر در لباس طرح‌ریزی سیستمی برای حفاظت از

---

1. XSS-11
2. MS Technology and Requirements Study
3. David Wright
4. Loura George

کشور در برابر حملات موشکی تروریست‌ها یا دولت‌های یاغی به اجرا درآمده‌اند.

۴-۶ دفاع موشکی

دولت ایالات متحده در توجیهی که در مورد علت استقرار سیستم دفاع موشکی برای مردم آمریکا و جهان ارائه داده است، آن را سپری در برابر حملات موشکی محدود معرفی کرده است، اما می‌توان آن را زمینه‌ساز توسعه تسلیحات فضایی نیز به‌شمار آورد. در گذشته، هر استراتژی‌ای در مورد دفاع موشکی بالستیک درست برخلاف دفاع موشکی نیمه‌استراتژیک[1] (که تسلیحات کوتاه‌برد و ویژه میدان جنگ را دربرمی‌گیرد) براساس نظریه سنتی بازدارندگی هسته‌ای میان دولت‌های هسته‌ای بزرگ و مفهوم انهدام قطعی متقابل[2] طرح‌ریزی شده است. اما در حال حاضر، آمریکا توسعه سیستم‌های دفاع موشکی بالستیک را با استناد به «تهدیدهای دولت‌های یاغی از قبیل ایران و کره شمالی، یا گروه‌های تروریستی» توجیه می‌کند. بااین‌حال، هیچ سند و مدرکی وجود ندارد که نشان دهد دولت‌های ذکر شده فناوری پرتاب موشک‌های دوربرد به‌سمت ایالات متحده (یا حتی نیت انجام چنین عملی) را داشته باشند ـ چرا که چنین اقدامی درواقع نوعی انتحار خواهد بود. ازاین‌گذشته، ابزارهای بدیل بی‌شماری در اختیار گروه‌های تروریستی است که با آنها می‌توانند سلاح هسته‌ای یا بمب کثیف پرتاب کنند (و این ابزارها چه‌بسا ارزان‌تر و سهل‌الوصول‌ترند).

دیدگاه بدیل دیگری نیز وجود دارد که تبیین می‌کند چرا ایالات متحده این‌قدر علاقه‌مند است فناوری‌هایی را که غیرقابل اعتماد، پرهزینه و مناقشه‌برانگیزند توسعه دهد. متقاعدسازی مردم در مورد ضرورت بهره‌مندی از تسلیحات فضایی، دشوار است. اما باید خاطرنشان کرد که ایجاد ترس از حمله تروریست‌ها یا دولت‌های یاغی به‌منظور توجیه توسعه فناوری‌های تسلیحات فضایی به‌مراتب آسان‌تر است. نمونه‌های متعددی از سیستم‌های فناورانه[3] وجود دارد که در راستای پیشبرد طرح دفاع موشکی توسعه‌یافته‌اند و به‌آسانی می‌توان آنها را با عملیات جنگی یا نقشه‌های ضدماهواره‌ای منطبق ساخت.

---

1. Theatre Missile Defemse
2. Mutually Assured Destruction
3. Technological Systems

توسعه تأسیسات ردگیری اشیای فضایی در روی زمین (از جمله ارتقا و بهسازی سیستم هشدار اولیه در موشک‌های بالستیک، رادارهای مستقر در فیلینگدیلز[۱] و تیول[۲] گرینلند و توسعه رادار ایکس‌ــ باند[۳]) و در فضا (از قبیل رادارهای مستقر در فضا، سیستم‌های ردگیری و کنترل فضایی،[۴] یا سیستم مادون قرمز مستقر در فضا[۵]) یکی از مؤلفه‌های ذاتی دفاع موشکی است، اما برای توانمندی‌های ضدماهواره‌ای نیز می‌تواند مورد استفاده قرار گیرد.(۴۱)

موشک‌های مخصوص ردگیری که یکی از ارکان دفاعی سیستم دفاع موشکی به‌شمار می‌آیند، در سطح زمین استقرار می‌یابند؛ هدف از طراحی این موشک‌ها هدف قرار دادن و رهگیری موشک‌هایی است که پرتاب شده‌اند. موشک‌های مخصوص ردگیری را می‌توان علیه ماهواره‌هایی که در مدار پایین زمین حرکت می‌کنند، به‌کار گرفت.(۴۲) هرچند برنامه لیزر فضایی کم‌وبیش لغو شده است، اما طرح لیزرهای مستقر در سطح زمین ـ که از یک سیستم آینه مانند در فضا استفاده می‌کنند ـ پیشنهاد شده است. این لیزرها نقش یک سیستم دفاع موشکی و یا سلاح فضایی را ایفا می‌کنند.

دلایلی نیز وجود دارد که تبیین می‌کند چرا پیگیری برنامه دفاع موشکی ملی را می‌توان زیر سؤال برد. البته در ابتدا باید این سؤال را بیان کرد که وقتی قاچاق یک وسیله به درون خاک آمریکا با قایق یا کامیون، ارزان‌تر، آسان‌تر و مطمئن‌تر است، پس چرا گروه یا کشوری می‌کوشد برای پرتاب سلاح هسته‌ای یا سلاح‌های مشابه آن، از موشک دوربرد گران و غیرقابل اطمینان استفاده کند؟

علاوه‌بر این، مدت‌ها پیش از این، یعنی در سال ۲۰۰۰، اتحادیه دانشمندان نگران(۴۳) علناً اعلام کردند هر گروهی که قادر باشد با استفاده از کلاهک هسته‌ای، موشک بالستیک قاره‌پیما پرتاب کند، قادر خواهد بود تدابیر متقابل[۶] کافی برای غلبه بر آن سیستم دفاع موشکی که پنتاگون پیشنهاد داده است انجام دهد. بااین‌حال، این

---

1. Fylingdales
2. Thule
3. X- Band
4. Space Tracking and Surveillance Systems (STSS)
5. Space Based Infra Red System (SBIRS).
6. Countermeasures

سؤال نیز همچنان باقی می‌ماند که چرا یک دولت یا گروه تروریستی چنین سلاحی را به‌طور مخفیانه (با کامیون یا کشتی) برای هدف قرار دادن دشمن، حمل نمی‌کند و در عوض، موشک‌های دوربرد پرهزینه و غیرقابل اطمینان را پرتاب می‌نماید؟

انجمن فیزیک آمریکا[1] نیز مطالعه علمی دیگری را در این زمینه انجام داد.(۴۴) این انجمن، رهگیری فاز بالا[2] را محور بررسی‌های خود قرار داد. بسیاری از استراتژیست‌های نظامی آمریکا به دلایل متعددی از این مدل سیستم موشک‌های ضدبالستیک حمایت می‌کنند. برای مثال، این سیستم قادر است رهگیری را قبل از استقرار طعمه‌ها با موفقیت به انجام برساند. این امر باعث می‌شود قطعات فولادی ناشی از عملیات رهگیری، به‌جای آنکه بر منطقه هدف فرو ریزند در همان ناحیه‌ای که موشک رهگیری پرتاب شده است، فرود آیند.

بررسی انجمن فیزیک آمریکا نشان داد که «رهگیری‌های مستقر در زمین یا هوا (حتی رهگیری‌های لیزری)، برای آنکه عملیاتی شوند، باید بسیار نزدیک به جایگاه‌های پرتاب قرار گیرند؛ و علاوه‌بر این، اگر بخواهیم از پوشش عملیاتی این رهگیری‌ها در سطح جهانی و در تمام زمان‌ها اطمینان حاصل کنیم، می‌باید در حدود ۱۶۰۰ دستگاه یا موشک رهگیری را در فضا مستقر سازیم. حتی اگر رهگیری در همان دقایق اولیه پرتاب (یعنی در زمان روشن شدن موتورهای احتراقی موشک) با موفقیت انجام شود، باز هم معلوم نیست برد موشکی که مثلاً از نقطه‌ای در خاورمیانه پرتاب شده است، به قاره آمریکا برسد.

در دسامبر ۲۰۰۲، جرج بوش برای اولین بار، دستور داد ده فروند موشک رهگیری دوربرد تا پایان سال ۲۰۰۴ راه‌اندازی شود. در حال حاضر شش فروند موشک رهگیری در فرت گریلی[3] (واقع در آلاسکا) مستقرند و چهار فروند موشک دیگر نیز قرار است در پایگاه نیروی هوایی واندنبرگ[4] در کالیفرنیا نصب شود. البته برنامه‌ریزی شده است که در سال ۲۰۰۵ ده فروند دیگر در برخی از نقاط آمریکا قرار گیرند و احتمالاً صد فروند دیگر نیز در سایر پایگاه‌ها (حتی شاید خارج از آمریکا) تا قبل از سال ۲۰۱۲ استقرار یابند. پنتاگون از همان ابتدا تاریخ ۳۰ سپتامبر ۲۰۰۴ را برای راه‌اندازی این سیستم تعیین کرد، ولی موانع

1. American Physical Society
2. Boost - phase
3. Fort Greely
4. Vandenberg

بی‌شمار و نگرانی‌های مستمری درزمینه اجرای بسیار شتاب‌زده این سیستم وجود داشت.

با وجود آنکه صدها میلیارد دلار صرف توسعه اجزای مرتبط با این سیستم شد، باز هم نگرانی‌های فزاینده‌ای در مورد میزان بالای کل این هزینه‌ها وجود دارد. برآورد شده است که هزینه‌های تحقیقات و توسعه در مقطع زمانی ۲۰۰۹-۲۰۰۴ تقریباً پنجاه میلیارد دلار خواهد بود؛ این در حالی است که تا سال ۲۰۳۵، مجموع هزینه‌های چرخه اجرای سیستم دفاع موشکی به‌حدود ۱/۲ تریلیون دلار خواهد رسید.(۴۵)

بااین‌حال، ایالات متحده آمریکا تمام تلاش خود را به‌کار گرفته است تا کشورهای بیشتری را با خود همراه سازد؛ در بخش ذیل، محورهای این تلاش‌ها تبیین می‌شود.

۱-۴-۶ واکنش بین‌المللی به دفاع موشکی ایالات متحده

در اروپا، سه کشور ـ بریتانیا، دانمارک و گرینلند ـ اجازه داده‌اند ایالات متحده رادارهای رهگیری و هشدار اولیه در پایگاه‌های فیلینگدیلز و تیول مستقر سازد ـ که البته به همین منظور، بهسازی و نوسازی نیز شده‌اند. این سه کشور با این اقدام خود، عملاً هم‌اکنون موافقت کرده‌اند که به بخشی از این سیستم دفاع موشکی تبدیل شوند. در جولای ۲۰۰۳ یک سیستم دفاع موشکی [1] در بریتانیا راه‌اندازی شد و دو ماه بعد از این تاریخ فاش گردید که قرار است دولت بریتانیا تا سال ۲۰۰۹، سالیانه پنج میلیون پوند درزمینه دفاع موشکی هزینه کند. سایر کشورهای اروپایی نیز وسوسه شده‌اند که به دنبال انعقاد قراردادهای تحقیقات و توسعه در این حوزه بروند. برای مثال، یک قرارداد سه میلیارد دلاری برای استقرار سیستم دفاع موشکی به نام «سیستم متوسط دفاع هوایی موسع» [2] منعقد شده است. این قرارداد درواقع سرمایه‌گذاری مشترک میان شرکت لاکهید مارتین، [3] شرکت دفاعی و فضایی هواپیماسازی اروپا، [4] شرکت فضایی ایتالیایی و شرکت آلمانی به نام لنک فلوگ کورپرسیستم [5] بود. علاوه‌بر این ایالات متحده درزمینه امکان استقرار ایستگاه‌های راداری و پایگاه‌های رهگیری موشکی در جمهوری چک و

---

1. Missile Defense System
2. Medium Expanded Air Defense System
3. Lockheed Martin Corp
4. European Aeronautic Defense and Space Company (EADS)
5. Lenkflugkorpersystem

لهستان با این دو کشور وارد مذاکره شده است. آمریکا رویکردهای مشابهی نیز در قبال کشورهای مجارستان، رومانی و بلغارستان در پیش گرفته است.

در هفتم جولای ۲۰۰۴ استرالیا یادداشت تفاهمی با ایالات متحده آمریکا امضا کرد. این یادداشت تفاهم درواقع چارچوب‌هایی است که محورهای مشارکت استرالیا با آمریکا درزمینه توسعه و آزمایش سیستم دفاع موشکی در ۲۵ سال آینده را مشخص می‌سازد. هدف از این موافقت‌نامه، این است که تلاش‌های مشترک جدیدی را به‌وجود آورد، ترتیبات خاصی را نیز برای مشارکت دو کشور درزمینه توسعه و آزمایش فناوری راداری پیشرفته ایجاد کند، عملیات شناسایی فوری موشک‌های بالستیک را بهبود بخشد و به‌طور بالقوه یک ناوشکن جدید استرالیایی را به توانمندی دفاع موشکی مجهز سازد.

اما کانادا هنوز مشارکت خود را در سیستم دفاع موشکی آمریکا اعلام نکرده است. بااین‌همه، اوتاوا در این اواخر با اصلاح موافقت‌نامه فرماندهی دفاعی آمریکای شمالی در حوزه هوا ـ فضا[1] (که میان این کشور و آمریکا منعقد شده بود) موافقت کرده است. اصلاح این موافقت‌نامه به‌گونه‌ای خواهد بود که کارویژه هشدار موشکی در این فرماندهی، در دسترس سیستم دفاع موشکی آمریکا قرار خواهد گرفت.

ژاپن به دلیل تهدیدی که از جانب کره شمالی احساس می‌کند، اولین کشوری است که همکاری با آمریکا را درزمینه استقرار سیستم دفاع موشکی در کشتی‌های خود پذیرفته است. در سال ۱۹۹۸، اقدام کره شمالی در پرتاب موشک بالستیک «چندمرحله‌ای»[2] بر فراز جزیره اصلی ژاپن، این کشور را شوکه کرد. هرچند در سال ۲۰۰۲ یونیشیرو کویزومی[3] نخست‌وزیر ژاپن از کره شمالی تعهد گرفت که آزمایش موشک‌های دوربرد را متوقف سازد، اما درهرحال این اقدام کره شمالی بی‌اعتمادی را تشدید کرده است و باعث شده توکیو با بهسازی ناوشکن‌های نظامی خود و تهیه سیستم‌های رهگیریِ ساخت آمریکا واکنش نشان دهد.

روسیه اعلام کرده است اگر موافقت‌نامه غیرنظامی‌سازی فضا به‌قوت خود باقی باشد، آماده همکاری با آمریکاست. اما این وضعیت، بعید است و بنابراین، روسیه با

---

1. North American Aerospace Defence Command (NORAD)
2. Multi-stage
3. Junichiro Koizumi

توسعه اقدامات متقابل و سیستم‌های دفاع موشکی خود همچنان به تنهایی عمل خواهد کرد. پوتین رئیس‌جمهور روسیه، در فوریه ۲۰۰۴ اعلام کرد روسیه یک موشک هسته‌ای مافوق صوت جدیدی را با موفقیت آزمایش کرده است که قادر است در هنگام نزدیک شدن به هدف تغییر مسیر دهد. این اظهارات آشکار نشان داد که این نوع جدید موشک‌ها با هدف غلبه بر سیستم‌های دفاع موشکی توسعه یافته است. طراحی این نوع موشک‌ها به‌نوبه خود، بر این انتقاد که دفاع موشکی به بروز مسابقه تسلیحاتی دیگری منجر خواهد شد صحه نهاد.

چین از اجرای دفاع موشکی ابراز نگرانی کرده است، این کشور به‌ویژه نگران است که کشورهای منطقه پاسیفیک از جمله تایوان، کره جنوبی و ژاپن سیستم‌های دفاع موشکی را در کشتی‌ها یا قلمرو خود مستقر سازند.

توسعه فراگیر سیستم‌های دفاع موشکی (از جمله سیستم دفاع موشکی با استفاده از موشک‌های نیمه‌استراتژیک) و احتمال استفاده از چنین سیستم‌هایی در جنگ‌هایی که در فضا درمی‌گیرد یا از فضا آغاز می‌شود، باعث شده است که همگان برای توصیف این فعالیت‌ها از اصطلاح رایج جنگ ستارگان استفاده کنند.

۶-۵ امکان کنترل تسلیحات فضایی

۶-۵-۱ سلاح فضایی چیست؟

در حال حاضر ایالات متحده به‌شدت علاقه‌مند است سیستم دفاع موشکی خود را راه‌اندازی کند و می‌کوشد آن را در سطح جهان توجیه کند. علاوه‌بر این، احتمال اوج‌گیری توسعه تسلیحات فضایی نیز وجود دارد. با این اوصاف، یافتن راه‌هایی برای پیشگیری از وقوع جنگ در فضا ضروری به‌نظر می‌رسد. مسئله مهم دیگری که در اینجا مطرح می‌باشد، تعریف سلاح فضایی است. سیستم‌های تسلیحاتی فضایی بسیاری وجود دارد که می‌توان آنها را برای اهداف غیرنظامی و مفید به‌کار گرفت یا فقط به‌آسانی به‌صورت توانمندی تهاجمی درآیند. برای مثال، می‌توان به ماهواره‌های کوچکی که در مانورها مورد استفاده قرار می‌گیرند یا فضاپیماهای کوچک اشاره کرد. سازه‌های دیگری از قبیل سیستم‌های ارتباطاتی یا نظارتی (یا آینه‌هایی برای هدایت لیزرهای مستقر در

زمین) نیز در فضا وجود دارد که هرچند در زمره تسلیحات قرار نمی‌گیرند، اما می‌توان آنها را بخشی از یک سیستم تسلیحاتی هدف‌گیری یا مدیریت نبرد محسوب کرد.

نیونک[1] و رتکیرچ[2] خاطرنشان کرده‌اند تعاریف تسلیحات فضایی چه‌بسا ممکن است فنی، جغرافیایی یا آمیخته با انگیزه‌های سیاسی باشد.(۴۶) چین در کنفرانس خلع سلاح در سال ۱۹۸۵ پیشنهاد داد تسلیحات فضایی به «همه وسایل یا تأسیسات مستقر در فضا (از جمله ابزارهای مستقر در کره ماه و سایر اجرام سماوی) که با هدف حمله یا وارد ساختن خسارت به اشیای موجود در جو، زمین یا دریا طراحی و ساخته می‌شوند»، اطلاق شود. با این اوصاف، آیا دست یافتن به تعریفی که مورد توافق همه باشد، بدون شک، چیزی ماورای عقل آدمی نیست؟

۲-۵-۶ معاهدات

معاهده فضایی ماورای جو (۱۹۶۷)(۴۷)، چارچوب‌های اساسی را برای تدوین حقوق بین‌الملل فضا[3] فراهم می‌کند. این معاهده موارد ذیل را به رسمیت می‌شناسد:

۱. کاوش و استفاده از فضای ماورای جو می‌باید برای منافع و علایق تمامی کشورها انجام گیرد و باید در قلمرو صلاحیت کل بشریت باشد.

۲. کاوش و استفاده تمام دولت‌ها از فضای ماورای جو باید آزاد باشد.

۳. هیچ کشوری نمی‌تواند با ادعای حاکمیت، با بهره‌برداری یا تصرف یا با هر وسیله دیگری، فضای ماورای جو را تابع حوزه صلاحیت اختصاصی و ملی خویش قرار دهد.

۴. دولت‌ها نباید تسلیحات هسته‌ای یا سایر تسلیحات کشتارجمعی را در مدار زمین قرار دهند یا بر اجرام سماوی نصب نمایند یا آنها را به هر شیوه دیگری در فضای ماورای جو مستقر سازند.

۵. کره ماه و سایر اجرام سماوی باید منحصراً برای مقاصد صلح‌آمیز مورد استفاده قرار گیرند.

معاهده‌های دیگری نیز درزمینه حقوق فضا وجود دارد. موافقت‌نامه حاکم بر

---

1. Neuneck
2. Rothkirch
3. International Space Law

فعالیت‌های دولت‌ها در کره ماه و سایر اجرام سماوی[1] (موافقت‌نامه کره ماه) در سال ۱۹۸۴ به اجرا درآمد. معاهده اتحادیه بین‌المللی مخابرات[2] نیز که در سال‌های ۱۹۹۲ و ۱۹۹۴ اصلاح گردید، از ماهواره‌های غیرنظامی در برابر هرگونه مزاحمت و مداخله حمایت می‌کند.

بنابراین دستیابی به توافقی بین‌المللی درزمینه بسیاری از موضوعاتی که به «استفاده از فضا» مربوط می‌شوند، امکان‌پذیر است. اما فعلاً هیچ معاهده‌ای وجود ندارد که از استقرار تسلیحات در فضا جلوگیری کند (البته در مورد تسلیحات کشتارجمعی، موافقت‌نامه‌هایی منعقد شده است) و هنوز مذاکره‌ای درزمینه جلوگیری از بروز مسابقه تسلیحاتی در فضای ماورای جو انجام نگرفته است.

در سازمان ملل متحد، اتفاق‌نظری همگانی، از جمله در میان همه کشورهای برخوردار از توانمندی فضایی، وجود دارد که باید از هرگونه مسابقه تسلیحاتی در فضای ماورای جو جلوگیری شود. کمیته کاربردهای صلح‌آمیز فضای ماورای جو[3] به کمیته چهارم مجمع عمومی (کمیته ویژه امور سیاسی و استعمارزدایی) ملحق شد. علاوه‌بر این، سازمان ملل متحد[4] اجلاس‌های ادواری برگزار می‌کند، اما در این اجلاس‌ها معمولاً «مسائل مربوط به کاوش در فضا» بحث می‌شود. کمیته اول (کمیته خلع سلاح و امنیت بین‌الملل) مسائل مرتبط با امور نظامی در فضا را بررسی می‌کند و مذاکرات در مورد این مسائل نیز در قالب کنفرانس خلع سلاح انجام می‌گیرد.

از سال ۲۰۰۲ تاکنون، ابتکارعمل‌های مهمی درزمینه کنترل تسلیحات فضایی در کنفرانس خلع سلاح مورد بحث و بررسی قرار گرفته؛ دراین‌باره می‌توان به معاهده ممنوعیت به‌کارگیری تسلیحات فضایی (به ابتکار چین و روسیه) و تأسیس کمیته موقت پیشگیری از مسابقه تسلیحاتی در فضای ماورای جو[5] اشاره کرد. در گذشته، چین اصرار داشته است که چنین کمیته‌ای باید انعقاد معاهده ممنوعیت تسلیحات فضایی را در

---

1. Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (The Moon Agreement)
2. International Telcommunication Union (LTU)
3. Committee On the Peaceful Uses of Outer Space (COPUOS)
4. United Nation (UN)
5. Prevention of an Arms Race in Outer Space

اختیارات خود بگنجاند و علاوه‌بر این، در این راستا موافقت خود درزمینه انجام مذاکرات برای انعقاد معاهده پیشگیری مواد شکاف‌پذیر[1] را به آغاز مذاکره در مورد انعقاد معاهده پیشگیری از مسابقه تسلیحاتی در فضای ماورای جو پیوند زده است. ازسوی‌دیگر، ایالات متحده آمریکا مخالف اصلی انعقاد معاهده‌ای درباره ممنوعیت تسلیحات فضایی است، اما از تشکیل کمیته موقت پیشگیری از مسابقه تسلیحاتی در فضای ماورای جو به شرط اینکه اختیارات کمیته مذکور گسترده باشد، حمایت می‌کند. هرچند در مورد ضرورت تشکیل این کمیته، اتفاق‌نظر وجود دارد، اما اختلاف‌نظرها بر سر میزان اختیارات آن، دستیابی به اجماع‌نظر در درون کنفرانس خلع سلاح را مدام به تأخیر انداخته است.

سال ۲۰۰۰، مجمع عمومی سازمان ملل متحد قطعنامه پیشگیری از مسابقه تسلیحاتی در فضای ماورای جو را با بیشترین آرا (۱۶۳ موافق، بدون رأی مخالف و با سه رأی ممتنع) تصویب کرد. سه دولتی که رأی ممتنع دادند میکرونزیا،[2] ایالات متحده آمریکا و رژیم صهیونیستی بودند(۴۸) در همین اواخر، یعنی در ۲۰ اکتبر ۲۰۰۴، در کمیته اول (کمیته خلع سلاح و امنیت بین‌الملل) در نیویورک، تعدادی از دولت‌ها بر اهمیت جلوگیری از استقرار تسلیحات در فضای ماورای جو تأکید کردند. یک روز قبل از این تاریخ، روسیه در یک نشست ویژه، سیاست جدید خود را درباره تسلیحات فضایی، تحت عنوان اولین استقرار، ممنوع[3] اعلام کرده بود. علاوه‌بر این، روسیه از پیش‌نویس معاهده‌ای که چین در مورد جلوگیری از نصب و استقرار تسلیحات در فضا تدوین کرده است، سخت حمایت کرده است. مصر و سریلانکا نیز قطعنامه سنتی پیشگیری از مسابقه تسلیحاتی در فضای ماورای جو را پیشنهاد داده‌اند. این قطع‌نامه، با بندهای کارآمد و مناسبی که در خود دارد، بر ضرورت انجام تدابیر بیشتر برای کنترل پیشگیری از مسابقه تسلیحاتی در فضا تأکید می‌کند و در نشست سال ۲۰۰۵ از کنفرانس خلع سلاح می‌خواهد کمیته‌ای موقت درزمینه پیشگیری از مسابقه تسلیحاتی در فضای ماورای جو تأسیس کند. تأسیس این کمیته با بیشترین آرا (۱۶۷ رأی موافق، بدون رأی مخالف و دو رأی ممتنع ـ آمریکا و رژیم صهیونیستی) به تصویب رسید.(۴۹)

---

1. Fissile-Material Cutoff Treaty (FMCT)
2. Micronesia
3. No First Deployment

موضوعات «سیاست» و «برتری نظامی یا صنعتی» معمولاً بیش از هر موضوع دیگری محور بحث‌ها و مناظرات بوده است. هیچ‌گاه استدلال اخلاقی وارد این مباحث نمی‌شود. هرچند می‌توان گفت موفق‌ترین معاهده درباره فضا (معاهده فضای ماورای جو)، که فضا را قلمرو همه ابنای بشر اعلام می‌کند، معاهده‌ای اساساً اخلاقی است، اما هیچ‌گاه تاکنون، استدلال اخلاقی وارد این قبیل مباحث نشده است. آیا زمان آن فرانرسیده است که برای یافتن طنین حس مشترک انسانی و راه‌های برون‌رفت از مسیر نفع شخصی، ترس و بی‌اعتمادی، به بررسی ملاحظات اخلاقی در حوزه بهره‌برداری از فضا نیز توجه کنیم؟

بهره‌برداری اخلاق‌مدارانه از فضا در کنفرانسی با عنوان بهره‌برداری از فضا و اخلاقیات[1] مورد بررسی قرار گرفت. کنفرانس معیارهای ارزیابی آینده فضا[2] در سال ۱۹۹۹ در دانشگاه فناوری دارمشتات[3] آلمان برگزار شد. در قرن بیست‌ویکم، فناوری فضایی می‌باید به شیوه‌ای پایدار به حل‌وفصل منازعات و مسائلی که روی کره زمین پدیدار می‌گردند، کمک کند.(۵۰)

یورگن شفران[4] موضوعاتی از جمله استفاده از فناوری فضایی، میزان پذیرش اجتماعی، هزینه‌ها و منابع، اهداف و فواید و پیامدهای نامطلوب و خطرات آن را ارزیابی کرد؛ وی در این راستا به هشت معیار عینی برای ارزیابی پروژه‌های فضایی در آینده اشاره کرد. معیارهایی که وی برمی‌شمارد به‌گونه‌ای است که می‌توان آنها را در سایر حوزه‌های فناوری نیز به‌کار گرفت. این معیارها عبارت‌اند از:

۱. از میان برداشتن احتمال وقوع فاجعه‌ای شدید،
۲. پرهیز از استفاده نظامی از فضا، منازعه خشونت‌آمیز و اشاعه تسلیحات فضایی،
۳. به حداقل رساندن اثرات سوءفناوری فضا بر بهداشت محیط زیست،
۴. تضمین کیفیت، اعتمادپذیری[5] و کارآمدی فناوری فضایی ازلحاظ فنی و علمی،
۵. حل‌وفصل مسائل و تأمین پایدار و به‌موقع نیازها،

---

1. Space Use and Ethics
2. Critieria for the Assessment of Future Space
3. Darmstadt University of Technology (DUT)
4. Jurgen Scheffran
5. Reliability

۶. جست‌وجوی بدیل‌هایی که بهترین کارآمدی و بیشترین بازدهی را دارند،

۷. تضمین سازگاری اجتماعی و تقویت همکاری،

۸. توجیه اجرای پروژه‌ها با برگزاری مناظرات و بحث‌های همگانی به‌گونه‌ای که همه طرف‌های ذی‌ربط در آنها شرکت داشته باشند.

در زمانی که از قضا به‌نظر می‌رسد فناوری‌های ماهواره‌ای و موشکی به‌سرعت و به شیوه‌ای به‌نسبت لجام‌گسیخته رشد می‌کنند، کشورهای جهان باید این مسائل را بسیار جدی بگیرند و در مورد نحوه پیشبرد شیوه‌ای که بتواند بقای انسان را به بهترین شکل تضمین کند به توافق برسند. سیستم دفاع موشکی که افزایش تسلیحات فضایی و دفاع موشکی را در پی دارد، نمی‌تواند شیوه‌ای خوش‌فرجام باشد.

پی‌نوشت‌ها

1. Jeffrey Lewis, 'What if Space Were Weaponized?, Center for Defense Information, Washington DC.

2. As reported in the *Colorado Springs Gazette*, 13 April 2003.

3. Michael Woods, 'Satellites Provide Vital Reconnaissance, Communications to war Effort, 'Post-Gazette, Available at http://www.post-gazette.com/nation /20030402 spacewar0402p4.asp.

4. Greg Jaffe, 'Military Feels Bandwidth Squeeze As the Satellite Industry Splutters, *Wall Street Journal*, 4 October 2002.

5. As reported in Lewis, 'What if Space Were Weaponized?'

6. See 'Current and Future Space Security-Russia: Military Programs' from the Center for Nonproliferation Studies, Monterey Institute of International Studies- http://cns.miis.edu/research/space/russia/mil.htm.

7. www.fas.org/spp/guide/russia/nav/glonass.htm.

8. Nikolay Poroskov, 'Platoon With a Satellite', *Vremya Novostey*, 21 August 2003; in 'Russian General Staff Approves Plan to Equip Troops With GLONASS Navig'ation Receivers', quoted in http://cns.miis.edu/research /space/russia/mil.htm.

9. Barbara Opall Rome, 'Israel Makes Plans for Broad Space Capabilities', Space News, 25 August 2003.

10. 'Countries with Advance-Launch Capabilities' from the Monterey Institute of International Studies-See: http://cns.miis.edu/research/ space/spfrnat.htm.

11. 'France Launches Australian MilSat Half Owned by Singtel', spacedaily.com, 11 June 2003, http://www.spacedaily.com/news/milspace-comms-03t.html.

12. See European Space Agency, www.esa.int, in particular, www.esa.int/esaCP /SEMFEPYVISD_index_0.html.

13. See, for Example, Regina Hagen, 'Europe-the Leading Space Power? INESAP Bulletin no. 23, April 2004, http://www.ineap.org/bulletin23/art04.htm.

14. 'An Evaluation of the Military Benefits of the Galileo System' by James Hasik and Michael Rip, GPS World, April 2003. Available at http://www. gpsworld .com/gpsworld/article/articleDetail.jsp?id=53279.

15. Available from: http://www.defenselink.mil/pubs/space20010111.html.

16. 'Jamming Incident Underscores Lessons About Space', Spacedaily.com. Available at http://www.spacedaily.com/news/gps-04zzzzb.html.

17. Jim Wolf, 'US Deploys Satellite Jamming System', Reuters, SanDiego.com, 29 October 2004.

18. Laura Grego, Union of Concerned Scientists', A History of US and Soviet ASAT Programs, 'April 2003. Available at http://www.ucsusa.org /global_ security/space_weapons/a-history-of-asat-programs.html.

19. Aleksandr Dolinin, Interview with Space Troops Commander Colonel-General Anatoliy Perminov, 'Outer Space and the Military Security of Russia', Krasnaya *Zvezda*, 27 April 2001, p. 1; in 'New Space Troos Commander Colonel-general Anatoliy Perminov Interviewed on Connection Between Space Troops' activities and Various areas of Country's Development.'

20. See http://www.paineless.id.au/missiles/Nikezeus.html and http://en.wikipedia .org/wiki /Anti-satellite_weapon.

21. The USA Tested the ALMV Against an Ageing Solwind Satellite in a 555km orbit on 13 September 1985.

22. For more Information, see: http://www.fas.org/spp/military/program/asat /miracl.htm.

23. 'Chinese Anti-satellite Capabilities', from Global Security.com at:

24. http://www.globalsecurity.org/space/world/china/asat.htm.

25. Ibid.

26. Jeffrey Lewis, 'Space Weapons Spending in the FY2005 Defense Budget'. Presented at the 9th PIIC Beijing Seminar on International Security, October 2004.

27. Available from: http://www.dtic.mil/doctrine/jet/service_Pubs/afdd2_2_1.pdf.

28. Ibid.

29. Jeffrey Lewis, 'Programs to Watch', in 'Weapons in Space, Arms Control Today', November 2004, available at:http://www.armscontrol.org/act/ 2004_11 /Krepon.asp.

30. Details of the FALCON Programme can be found in the 'US Air Force Transformation Flight Plan', November 2003 –see http://www.af.mil/library/ posture /AF_TRANS_FLIGHT_PLAN_2003.pdf.

31. Jefferson Morris, 'Space Weapon Proponents Need to make Better Case', Aviation Week's Aerospace Daily & Defense Report, 211 (25).

32. http://www.cdi.org.

33. www.cns.miis.edu.

34. www.space4peace.org.

35. www.cnduk.org.

36. 'US Might Intercept Target from Space in 2006', from *the Global Security Newswire*. Available at http://www.nti.org/d_newswire/issues /2004_4_29. html# DAE4AB71.

37. Jeremy Singer, Critics Land Laud Plan to Remove 'Kill Vehicle' From Satellite, space.com. Available at http://www.space.com/spacenews/ archive04/ nfirearch_082304.html.

38. Theresa Hitchens and Jeffrey Lewis, 'Arms Race in Space?' US Air/ Quietly Focuses on Space Control', *Defense News*, 1 September 2003.

39. Matt Bille, Robyn Kane, and Maj. Mel Nowlin, 'Military Microsatellites: Matching Requirements and Technology', presentd to the AAIA Space 2000 Conference and Exhibition, Long Beach, CA, 19-21 September 2000, p.9.

40. The US has Stated its Intent to Launch a Space-based Interceptor Test bed by 2008. See for example, Theresa Hitchens and Victoria Samson, 'Space-based Interceprots- still not a Good Idea', Center for Defense Information, Summer/Fall 2004-available at www.cdi,org/news/space-security/space-based -interceptors.pdf.

41. David Wright and Laura George, 'Anti-satellite Capabilities of Planned US Missile Defence Systems', *Disarmament Diplomacy*, Issue No. 68, December 2002-January 2003. Also at http://www.acronym.org.uk/dd/dd68/68op02.htm and from the Union of concerned scientists: http://www.ucsusa.org/global_ security/space_weapons/page.cfm?pageID=1152.

42. Ibid.

43. Ibid.

44. See:http://www.ucsusa.org/global_security/missile_defense/index.cfm

45. Boost-phase Intercept Systems for NMD', a Report by the American Physical Society Study Group, July 2003.

46. R.F. Kaufman (ed.), 'The Full Costs of Ballistic Missile Defense Ćenter for Arms Control and Non-proliferation, January 2003.

47. For a more Detailed Discussion see G. Neuneck and A. Rothkirch, 'Space as a New Medium of Warfare? Motivations, Technology and Consequences',

Institute for Peace Research and Security Policy, University of Hamburg.

48. See: http://www.oosa.unvienna.org/SpaceLaw/outerspt.html.

49. More Details in the UN Press Release GA/9829-available at http://www.un.org /News/Press/docs/2000/20001120.ga9829.doc.html; Rebecca Johnson, 'PAROS Discussions at the 2004 UN First Committee', The Acronym Institute, 20 October 2004. Available at http://www.acronym.org.uk /un /2004paro.htm.

50. See Reports from the Conference in INESAP Bulletin No.17. Available at http://www.inesap .org/bulletin17/bul17art19.htm.

فصل هفتم فناوری به‌عنوان منبع آشوب جهانی

استفان فریتش*

فناوری نه خوب است نه بد، خنثی و بی‌طرف هم نیست.(۱)

مقدمه

فناوری، که انباشت دانش و مصنوعات ساخت بشر به شیوه‌های مشخص و قابل بازتولید[1] برای تحقق اهداف انسان تعریف می‌شود،(۲) (اگر نگوییم نقش محوری)، همواره نقش تعیین‌کننده‌ای در توسعه رشته‌های روابط بین‌الملل یا اقتصاد سیاسی بین‌الملل ایفا کرده است، تاریخ نوع بشر، نمونه‌های بی‌شماری از تحولات نظامی، اقتصادی، اجتماعی و فرهنگی را به نمایش می‌گذارد.(۳) ژرف‌ترین تأثیر پیشرفت فناوری، به‌ویژه از قرن پانزدهم به بعد، افزایش حجم نظام بین‌الملل بوده است که در اثر افزایش حجم و شتاب تعاملات، پدیدار گشته است. در قرن بیستم، ظرفیت‌های تعامل در دو حوزه مهم ابداعات فناورانه به اوج خود رسید: ۱. تسلیحات کشتارجمعی هسته‌ای و سایر سیستم‌های موشکی که این‌گونه تسلیحات را حمل می‌کنند؛ ۲. فناوری‌های اطلاعاتی و ارتباطاتی الکتریکی و بعد از آن، الکترونیکی و توسعه فناوری‌های اطلاعاتی و ارتباطاتی در نیمه دوم قرن نوزدهم (تلگراف و تلفن) آغاز شد. از دهه ۱۹۴۰ به بعد، فناوری‌های اطلاعاتی و ارتباطاتی به حوزه‌هایی از جمله میکروالکترونیک و فناوری رایانه (سخت‌افزار) و به دنبال آن، توسعه نرم‌افزارها نیز کشیده شده‌اند. فرایندهای همگرایی[2] با فناوری‌های مخابراتی و آپتوالکترونیک[3] از دهه ۱۹۷۰، با بهره‌گیری از اصل اساسی

---

* Stefan Fritsch

1. Reproducible
2. Convergence
3. Optoelectronics

رمز دووجهی دیجیتالی، که به یمن پیشرفت فناوری ابداع شده است، به مبانی دگرگونی‌های بنیادین در حوزه‌های سیاست فراملی، ارتباطات، امور مالی و تجارت، تولید و فرهنگ شکل داده‌اند.

این دو نمونه نه تنها تأثیر چشمگیر فناوری بر تحولات نظامی، سیاسی، اقتصادی و اجتماعی را تبیین می‌کنند، بلکه ویژگی دیگر فناوری یعنی توانایی درنوردیدن مرزهای دولت را که حاکمیت و اقتدار سرزمینی دولت‌ها را تضعیف می‌سازد به نمایش می‌گذارد. از زمانی که نظام بین‌المللی دولت‌ـ ملت‌ها در دوران مدرن بعد از معاهده وستفالیا در سال ۱۶۴۸ شکل گرفت، حاکمیت و اقتدار سرزمینی دولت‌ها دو اصل اساسی این نظام بین‌المللی بوده است.

در دوران جنگ سرد، وجود تسلیحات هسته‌ای یکی از ویژگی‌های بارز نظام بین‌المللی بود.(۴) در حال حاضر، یعنی به‌اصطلاح در عصر جامعه اطلاعاتی، فناوری‌های اطلاعاتی و ارتباطاتی نقش تعیین‌کننده‌ای در نظام بین‌المللی ایفا می‌کنند. (۵) شمار زیادی مطالعات علمی وجود دارد که به موضوعات فناوری‌های خاص و تأثیر آنها بر سیاست‌های دولت و ظهور مسائل جدید سیاستگذاری در اثر تحولات فناورانه می‌پردازند.(۶) بااین‌همه، نظریه روابط بین‌الملل و اقتصاد سیاسی بین‌الملل تاکنون نتوانسته نظریه‌ای مشخص و فراگیر که اعتبار کافی به علم و فناوری و نقش آن در امور بین‌المللی بدهد، طراحی و تدوین کند. در مورد این شکاف، اسکلنیکف[1] نتیجه می‌گیرد حتی دانشمندانی که با مسائل نظری در روابط بین‌الملل سروکار دارند تمایل دارند علم و فناوری را اموری از پیش داده شده[2] و ایستا، یا برخاسته از جعبه‌های سیاه نفوذناپذیر در نظر بگیرند.(۷)

هدف این فصل کوتاه، این است که نشان دهد چگونه نظریه‌پردازان رشته‌های روابط بین‌الملل و اقتصاد سیاسی بین‌الملل در طول چند دهه گذشته کوشیده‌اند نقش فزاینده فناوری (به‌ویژه فناوری‌های اطلاعاتی و ارتباطاتی شبکه‌ـ محور) در شکل‌دهی به ساختارها و فرایندهای سیاسی و اقتصادی نظام بین‌الملل را توصیف و تحلیل کنند.

تحلیل همه رویکردهایی که در این حوزه وجود دارد، غیرممکن است. ازاین‌رو، فصل حاضر توجه خود را بر سه رویکرد نظری اصلی که در طول سه دهه گذشته، تأثیر

---

1. Skolnikoff
2. Givens

چشمگیری بر نظریه روابط بین‌الملل و اقتصاد سیاسی بین‌الملل داشته است متمرکز می‌سازد: واقع‌گرایی- نوواقع‌گرایی، جهان‌گرایی وابستگی متقابل[1] و سازه‌انگاری.[2] نویسنده در کل استدلال می‌کند که فناوری، در بیشتر موارد، هنوز در نظریه روابط بین‌الملل و اقتصاد سیاسی بین‌الملل، یک متغیر وابسته محسوب می‌شود و ارزش نقش آن نیز دست‌کم گرفته شده است. فصل حاضر سرانجام نتیجه می‌گیرد که اگر رشته‌های روابط بین‌الملل و اقتصاد سیاسی بین‌الملل بخواهد تأثیر پیشرفت فناوری بر روابط بین‌الملل را به‌نحو مؤثرتر و کارآمدتری تحلیل کند، باید برخی از مفروضات اساسی خود را تغییر دهد.

۱-۷ رویکردهای واقع‌گرا و نوواقع‌گرا به فناوری

واقع‌گرایی مفروضاتی اساسی در مورد نظام بین‌المللی دولت‌ها ارائه داده است (برای مثال، تنها دولت‌ها را بازیگر مهم در روابط بین‌الملل می‌داند). ازاین‌رو، این رویکرد روابط بین‌الملل را جنگ همه علیه همه تعریف می‌کند. براساس برداشت واقع‌گرایی، دولت‌ها بیش و پیش از هر چیز به تعقیب منافع ملی خود می‌پردازند. به‌عبارت بهتر، برای تضمین بقا و امنیت خود در نظام بین‌المللی بی‌سالار[3] (که ویژگی بارز آن، نبود حکمرانی جهان- گسترانه[4] است)، قدرت خود را بیشینه می‌سازند و برای فرار از افزایش قدرت دشمنان قوی‌تر، موازنه قدرت را تداوم می‌بخشند.(۸) در این برداشت‌های واقع‌گرایانه، فناوری درحقیقت یک «جعبه سیاه» به‌شمار می‌آید. از دیدگاه واقع‌گرایان، فناوری فقط ابزار قدرت برای تحقق اهداف دولت محسوب می‌شد و در بیشتر موارد نیز همچنان این‌گونه است.

واقع‌گرایی سنتی در تبیینی که درباره علت تداوم جنگ و ستیز میان دولت‌ها ارائه می‌دهد، بر میل بی‌وقفه انسان به کسب قدرت که در سرشت او نهفته است تأکید می‌کند، اما نوواقع‌گرایی بر ماهیت بی‌سالار جامعه جهانی که از حکمرانی جهان‌گسترانه

---

1. Interdependent Globalism
2. Constructivism
3. Anarchical System
4. Global Governance

بی‌بهره است، تأکید دارد. به همین دلیل، گاهی اوقات نوواقع‌گرایی را واقع‌گرایی ساختاری نیز می‌نامند، زیرا بر تأثیر ساختار قدرت جهانی بر رفتار دولت‌هایی که در درون آن عمل می‌کنند تأکید می‌ورزد. نوواقع‌گرایی درزمینه توجه به فناوری، بهتر از واقع‌گرایی عمل نکرد. کنت والتز،[1] یکی از تأثیرگذارترین نمایندگان نوواقع‌گرایی، توجه همه‌جانبه‌ای به توزیع قدرت میان دولت‌ها کرد و آن را عاملی اساسی برای تبیین سرشت نظام‌ها می‌دانست. به‌نظر وی نظریه نظام‌ها به مفهومی نیاز دارد تا ساختارها را براساس توزیع توانمندی‌ها میان واحدها تعریف کند. دولت‌ها، به علت آنکه در یک نظام خودیاری به‌سر می‌برند، برای تأمین منافع خود، ناگزیرند از توانمندی‌های خود استفاده کنند.

براساس رویکرد واقع‌گرایی، جایگاه دولت‌ها در نظام بین‌المللی به این بستگی دارد که چگونه آنها براساس همه اقلام ذیل امتیاز می‌گیرند: اندازه سرزمین و شمار جمعیت، مواهب و منابع، توانمندی اقتصادی، قدرت نظامی، ثبات سیاسی و کارآمدی سیاسی.(۹) هرچند فناوری در این رویکرد به صراحت مورد اشاره قرار نگرفته است، اما آشکار می‌شود که آن نوعی توانمندی ضمنی تلقی شده است.

اگر این مواضع را به خاطر بسپاریم، می‌توان گفت هم واقع‌گرایی و هم نوواقع‌گرایی فهم به‌نسبت ابزاری درباره فناوری ارائه می‌دهند. در این چارچوب، فناوری ابزار بی‌طرف به‌شمار می‌آید که باید در حوزه‌های ذیل از آن بهره گرفت: تأمین جایگاه قدرت یک دولت؛ یا کسب سودهای مطلق یا نسبی در رابطه با رقبا (در حوزه‌های امنیت، قدرت یا رفاه). این نبود ادراک[2] فناوری را در آثار (نو) واقع‌گرایان معاصر نیز می‌توان یافت.(۱۰) باید خاطرنشان کرد که برخی از فناوری‌های مدرن از جمله تسلیحات هسته‌ای یا فناوری‌های اطلاعاتی و ارتباطاتی می‌تواند قدرت (باز) ساختاردهی[3] خود را در سراسر نظام بین‌الملل و در سطح فراملی اعمال کند و البته اعمال می‌کند؛ این فناوری‌ها، ازاین‌رو، فضا را برای اقدام سیاسی و حاکمیت‌مدارانهٔ دولت‌ها تنگ می‌سازند و ویژگی‌هایی به نمایش می‌گذارند که نشان می‌دهد این فناوری‌ها حداقل، استقلال نسبی

---

1. Kenneth Waltz
2. Non-conception
3. (Re) Structuring

از دولت‌ها دارند. به‌محض اینکه نویسندگان واقع‌گراـ نوواقع‌گرا توجه خود را بـه بررسـی فرایندهای دگرگونی ناشی از پویش‌های فناوری معطـوف مـی‌سـازند، نـاگزیر مـی‌شـوند برخی از محوری‌ترین مفروضات خود را مورد تجدیدنظر قرار دهند.(۱۱)

۲-۷ جهان‌گرایی مبتنی‌بر وابستگی متقابل[1]

پایان جنگ سرد نه تنها به تشدید فرایندهای مبـادلات اقتـصادی و سیاسـی در گـستره جهـانی کمـک کـرد، بلکـه ظهـور بـازیگران قدرتمنـد جدیـدی از جملـه شـرکت‌هـای چندملیتی، سازمان‌های بینادولتی،[2] سازمان‌های غیردولتی[3] یا حتی افراد را تسهیل کرد. سلسله‌مراتب تعدیل شده در نظام بین‌الملـل و زوال تـدریجی قـدرت دولـت باعـث شـد بسیاری از نظریه‌پردازان روابط بین‌الملل/ اقتصاد سیاسی بین‌الملـل، رویکردهـای سـنتی روابط بین‌الملل / اقتصاد سیاسی بین‌الملل را زیر سؤال ببرند. حالا دیگر، دولت‌ها نه تنها یگانه بازیگران مطرح در صحنه جهانی به‌شمار نمی‌آینـد، بلکـه حتـی گـاهی اوقـات بـه موازات این وضعیت، قدرت‌گیری بازیگران غیردولتی را نیز فراروی خود می‌بینند.

بسیاری از نظریه‌پردازان، فناوری‌های اطلاعاتی و ارتباطی را یکی از نیروهای اصـلی این تغییرات بنیادین می‌دانند. ساختارهای جهانی نوظهور، روزنا[4] یکی از برجـسته‌تـرین نمایندگان این دیدگاه جدید در حوزه روابط بین‌الملل/ اقتصاد سیاسی بین‌الملل را بر آن داشت اصطلاح جدید «سیاست پسابین‌الملل» را برای اشاره به این تحـولات وضـع کنـد: «به‌نظر می‌رسد همین مفهوم «روابط بین‌الملل» نیز در برابر روند آشکاری کـه در جریـان آن، تعاملات تداوم‌بخش سیاست‌های جهانی رفته‌رفته بیش‌ازپـیش بـدون نقـش‌آفرینـی مستقیم ملت‌ها یا دولت‌ها انجام می‌گیرند، معنـا و مفهـوم خـود را از دسـت داده اسـت. «سیاست پسابین‌الملل» عنوان مناسبی است زیرا بی‌آنکه نشان دهد این تغییرات به کجـا ختم می‌شوند، آشکارا بر اضمحلال الگوهای دیرپا در نظام بـین‌الملـل اشـاره دارد. حتـی وقتی که سیاست پسابین‌المللی بر حضور و تداوم کـارکرد سـاختارهای باثبـات و پایـدار

1. Interdependent Globalism
2. Inter-Governmental Organizations (IGOS)
3. Nongavermental Organisations (NGOS)
4. Rosenau

تأکید می‌کند، به‌وجود تحول همیشگی و شرایط گذر[1] در امور جهانی نیز اشاره می‌نماید. این مفهوم خاطرنشان می‌سازد که موضوعات «بین‌المللی» دیگر بعد مسلط زندگی جهانی نیستند، یا حداقل نشان می‌دهد که ابعاد دیگری نیز سر برآورده‌اند و تعاملات دولت ـ ملت‌ها را به چالش کشیده‌اند یا جرح و تعدیل کرده‌اند.(۱۲)

مسبب این تغییر در درون نظام بین‌الملل چیست؟ به گفته روزنا، منابع این دگرگونی‌ها آشوب[2] است. براساس تعریفی که او ارائه می‌دهد، آشوب، یک وضعیت جهان‌گستر است؛ در این وضعیت، وجود پیچیدگی‌ها و ناپایداری‌های فراوان یکی از ویژگی‌های بارز به هم پیوستگی‌هایی[3] است که اصلی‌ترین عوامل مؤثر در سیاست جهانی را تداوم می‌بخشند.(۱۳) روزنا محدودیت‌های مدل خود را نیز برمی‌شمارد. دولت‌ها ممکن است پاره‌ای از قدرتی را که می‌توانند با به‌کارگیری آن در ساختارها و فرایندها نفوذ کنند از دست بدهند، اما آنها منسوخ نمی‌شوند: «دولت‌ها پیوسته در حال تغییر و دگرگونی‌اند، اما نابود نمی‌شوند. حاکمیت دولت تحلیل رفته است، اما با جدیّت بر آن اصرار می‌شود. دولت‌ها نسبت به گذشته، ضعیف‌ترند، اما هنوز هم می‌توانند از اعتبار خود حمایت و دفاع کنند. (...) مرزها هنوز نیز مانع ورود متجاوزان به داخل خاک دولت می‌شوند، اما نفوذپذیر نیز گردیده‌اند. چشم‌اندازهای سرزمینی[4] جای خود را به چشم‌اندازهای قومی،[5] چشم‌اندازهای رسانه‌ای،[6] چشم‌اندازهای عقیدتی،[7] چشم‌اندازهای فنی[8] و چشم‌اندازهای مالی[9] داده است، اما اصل سرزمینی بودن حاکمیت[10] همچنان دغدغه اصلی بسیاری از افراد است».(۱۴)

برطبق گفته‌های نویسندگانی که بر این دگرگونی‌های ساختاری در نظام بین‌الملل تأکید دارند، منابع این کاهش نسبی قدرت دولت‌ها کدام‌اند؟ تجزیه و تحلیل ادبیات و

---

1. Transitions
2. Turbulence
3. Interconnections
4. Landscape
5. Ethnoscape
6. Mediascape
7. Ideoscape
8. Technoscape
9. Finascape
10. Territoriality

آثار نویسندگانی که در این زمینه قلم‌فرسایی کرده‌اند آشکار می‌سازد چند عامل وجود دارد که درهم‌تنیده‌اند و یکدیگر را تقویت می‌نمایند و نقشی محوری در این زمینه ایفا می‌کنند. این عوامل عبارت‌اند از:

۱. افزایش کمی شمار بازیگران سنتی (دولت‌ها و بازیگران بینادولتی) و ظهور بازیگرانی جدید (سازمان‌های غیردولتی، شرکت‌های چندملیتی و افراد) که ازلحاظ کیفی با بازیگران سنتی فرق دارند،(۱۵)

۲. فرایندهای متعدد جهانی شدن، به‌ویژه در حوزه‌های نظامی، اقتصادی و اجتماعی ـ فرهنگی،(۱۶)

۳. فناوری به‌عنوان یکی از منابع محوری آشوب جهانی.(۱۷)

فرانسیس فوکویاما[1] شاید گسترده‌ترین دیدگاه جهان‌گرایانه[2] را که با فناوری ارتباط دارد بیان کرده است. ازنظر او، پیشرفت در حوزه فناوری، منبع دگرگونی بنیادینی است که به پایان تاریخ خواهد انجامید. بر همین اساس، وی روند پیروزی اشاعه دمکراسی و اقتصاد بازار لیبرالی در سراسر جهان را مسلم فرض می‌کند. اما درعین‌حال، این دو مفهوم نیز مؤثرترین نقطه عزیمت را برای ترویج این تحولات فنی و اقتصادی تعیین می‌کند.(۱۸) فوکویاما سخت معتقد است در آینده، تعداد پرشمارتری از دولت‌ها و جوامع آنها در مسیری که برای نیل به استانداردهای بالاتر زندگی می‌پیمایند، این الزامات را خواهند پذیرفت.(۱۹)

جهان‌گرایی وابستگی متقابل به‌دلیل ماهیت جبرگرایانه‌ای[3] که در خود دارد(۲۰) بیشتر مواقع مورد انتقاد قرار گرفته است. این رویکرد، به‌علت همین جبرگرایی، نیروهای جهانی شدن (عمدتاً فناوری) را منبع اصلی و مهم‌ترین عامل تحلیل رفتن ظرفیت‌های دولت‌ها در حوزه‌های تدوین و اجرای سیاست‌ها توصیف می‌نماید. اما با وجود این، بیشتر نمایندگان این رویکرد باز هم، همچنان فناوری را عاملی غیرجبرگرایانه[4] و خارجی[5] قلمداد می‌کنند: «پویش‌های دگرگونی که در حال حاضر جریان دارند، بدون

---

1. Francis Fokoyama
2. Globalistic
3. Deterministic
4. Nondeterministic
5. External

فناوری‌های جدید در عرصه ارتباطات و حمل‌ونقل، محلی از اعراب ندارند؛ اما این نوعی جبرگرایی نیست زیرا فناوری‌های جدید ابنای بشر را در «یک جهت واحد» سوق نمی‌دهند. این فناوری‌ها چندین روند علّی[1] را تسهیل می‌کنند و این پویش‌های افراد و اجتماعات است که تعیین می‌کند در وضعیت‌ها یا مناطق خاص، کدام روند دنبال خواهد شد».(۲۱)

۳-۷ فناوری و روابط بین‌الملل/ اقتصاد سیاسی بین‌الملل ازمنظر سازه‌انگاری

از اواسط دهه ۱۹۸۰، دیدگاه دیگری در مورد روابط بین‌الملل، بر غنای نظریه روابط بین‌الملل افزوده است. این دیدگاه از همان بدو ظهورش، بحث‌های زیادی را برانگیخته است: به بیان اونف،[2] «سازه‌انگاری، روش مطالعه روابط اجتماعی ـ هر نوع روابط اجتماعی ـ است».(۲۲) هرچند رویکردهای سازه‌انگارانه ازلحاظ برداشتی که در مورد روابط و فرایندهای اجتماعی دارند، در طیف گسترده‌ای قرار می‌گیرند، اما کوچک‌ترین مخرج مشترک آنها دو بعد را دربرمی‌گیرد:

۱. شناخت[3] و معنا،

۲. این ایده که واقعیت اجتماعی، نوعی برساخته اجتماعی[4] است.

همه سازه‌انگاران می‌کوشند»[...] از جهان اجتماعی طبیعت‌زدایی[5] کنند و به‌عبارت دقیق‌تر، با تجربه کشف کنند و آشکار سازند که چگونه نهادها، رویه‌ها و هویت‌هایی که افراد طبیعی، مفروض، یا واقعی می‌پندارند، درحقیقت محصول کارگزاری انسانی[6] و بر ساختگی اجتماعی‌اند.(۲۳)[7] سازه‌انگاران واقع‌گرایی/ نوواقع‌گرایی و جهان‌گرایی را نظریه‌هایی مادی‌گرا[8] می‌دانند و بدین‌سبب، آنها را به باد انتقاد می‌گیرند. ازنظر ونت،[9]

---

1. Causal Streams
2. Onuf
3. Knowledge
4. Socially Constructed
5. Denaturalise
6. Human Agency
7. Social Construction
8. Materialist
9. Wendt

یکی از نمایندگان اصلی و سازه‌انگار میانه‌رو، یک نظریه در زمانی شأن مادی‌گرایانه به خود می‌گیرد که [...] معلول‌های قدرت، منافع، یا نهادها را با رجوع به نیروهای مادی «خام»[1] (یعنی اموری از جمله سرشت انسان، محیط فیزیکی و شاید مصنوعات فناورانه،[2] مستقل از ایده‌ها وجود دارند و دارای قدرت‌های علی و معلولی می‌باشند) تبیین می‌کند.(۲۴)

ازنظر ونت، توانمندی‌های مادی به معنای دقیق کلمه، هیچ چیزی را توضیح نمی‌دهند، معلول‌های این توانمندی‌ها ساختارهای شناخت مشترک را که باهم فرق دارند و قابل تقلیل به توانمندی‌ها هم نیستند، پیش‌فرض می‌گیرند.(۲۵) فناوری بر رفتار اجتماعی و جوامع تأثیر می‌گذارد؛ واژه «تعامل» در اینجا مهم است، زیرا تعامل باعث می‌شود نیروهای مادی در برخی سطوح، مستقل از جامعه قوام یابند و به شیوه‌ای علّی بر جامعه تأثیر گذارند. نیروهای مادی فقط با معانی اجتماعی قوام نمی‌یابند و معانی اجتماعی نیز مصون از معلول‌های مادی نیستند.(۲۶) موضوع سازه‌انگاری در مورد فناوری را می‌توان بدین‌روش جمع‌بندی و ارزیابی کرد: فناوری به‌عنوان یک ساختار مادی بر فرایندهای سیاسی، اجتماعی و اقتصادی تأثیر می‌گذارد. همین صرف وجود فناوری، واقعیت اجتماعی را دگرگون می‌سازد، اما معنای واقعی[3] آن به بافت[4] اجتماعی بستگی دارد.(۲۷) با وجود این، سازه‌انگاران تمایل دارند قدرت ایده‌ها و هویت‌ها در روابط بین‌الملل را بیش از حد برآورد کنند و بیشتر مواقع نیز نقش و تأثیر تعیین‌کننده فناوری بر بازیگران در نظام بین‌الملل را می‌گیرند.

آن برداشت‌هایی که نظریه روابط بین‌الملل/ اقتصاد سیاسی بین‌الملل تا به حال در مورد فناوری ارائه داده‌اند، آشکارا نشان می‌دهند که نگرانی‌ها در مورد نقش فناوری در امور بین‌المللی افزایش یافته است. با وجود این، این برداشت‌ها کلاً کمتر از آنچه انتظار می‌رود به‌طور عمیق به تبیین رابطه اساسی میان فناوری و سیر تطور[5] امور بین‌المللی توجه می‌کند. بنابراین، تلفیق نظریه روابط بین‌الملل/ اقتصاد سیاسی بین‌الملل با سایر شیوه‌های تحقیقات اجتماعی ـ یعنی، تاریخ، جامعه‌شناسی و فلسفه فناوری ـ ضروری به‌نظر می‌رسد.

---

1. Brute
2. Technological Artefacts
3. Actual
4. Content
5. Evolution

۷-۴ بحث‌هایی در دفاع از ارائه دیدگاهی وسیع‌تر درباره فناوری

پرسش‌های مطرح در رشته‌های علمی هم‌جوار که بدان‌ها اشاره شد، عبارت‌اند از:

ـ آیا فناوری، ابزاری است که از پیش وجود داشته است و جامعه فقط آن را به مقتضای الزامات و نیازهای سیاسی و اقتصادی به‌کار می‌برده است؟

ـ آیا فناوری، منبع مستقل بروز تغییر است، به‌گونه‌ای که خود خصوصیات سیاسی را ایجاد می‌کند و از این رهگذر، شیوه‌هایی را که با آنها سیاست‌ها به ناگزیر واکنش نشان می‌دهند، اقتصادها تغییر ایجاد می‌کنند و جوامع نیز خود را با شرایط جدید منطبق می‌سازند، از پیش تعیین می‌نماید؟

اولین رویکردی که درباره فناوری وجود دارد، بر ویژگی انفعالی[1] آن تأکید دارد و در نتیجه، فرض را بر این می‌گذارد که جامعه می‌تواند براساس علایق و منافع خویش از آن استفاده کند. این رویکرد، برداشت «سازه‌انگاری اجتماعی»[2] از فناوری توصیف شده است.(۲۸) سازه‌انگاری اجتماعی، فهمی به‌نسبت ابزاری را در مورد فناوری به تصویر می‌کشد، چرا که برطبق این رویکرد، جامعه می‌تواند فناوری را براساس اهداف خود به‌کار ببرد، و قادر است همه تأثیرات جانبی مثبت و منفی آن را کنترل کند. در چنین برداشتی، فناوری به‌گونه‌ای درک نمی‌شود که به‌خودی‌خود ویژگی‌های سیاسی در خود دارد. در این رویکرد، فناوری اساساً وسیله‌ای بی‌طرف و خنثی و ابزاری برای نیل به هدف به‌شمار می‌آید.(۲۹) دیدگاه دوم درزمینه فناوری به‌طورکلی با جبرگرایی فناورانه[3] در پیوند بوده است. نویسندگانی مثل لویس مامفورد،[4] ژاک الول،[5] یا لانگدون وینر[6] کوشیدند نشان دهند که فناوری می‌تواند به‌صورت نیروی به‌نسبت مستقل عمل کند و ویژگی‌های سیاسی به خود بگیرد. جامعه می‌تواند گزینه‌های مرتبط با فناوری را فعالانه انتخاب کند، اما این گزینه‌ها نیز به‌نوبه خود فشارهایی را بر بازیگران مختلف تحمیل می‌کنند تا خود را با شرایط فناوری جدید منطبق سازند و ازاین‌رو، در حوزه‌های

---

1. Passive
2. Social Constructivism
3. Technological Determinism
4. Lewis Mumford
5. Jacques Ellul
6. Langdon Winner

سیاسی، اقتصادی و اجتماعی به فرایندهایی شکل می‌دهند که چه‌بسا همواره مورد انتظار نبوده‌اند یا آگاهانه انتخاب نشده‌اند.(۳۰)

این رویکردها در معرض انتقادات شدیدی قرار گرفته و به بیان مارکسیستی، «جبرگرایی فناورانه» توصیف شده‌اند؛ زیرا امکان بروز تحولات پیش‌بینی نشده و خلاف انتظار را که در اثر ارتقای فناوری‌ها پدید می‌آیند، از قلم انداخته‌اند. با وجود این، برخی از مفروضاتی که این رویکردها در خود دارند، باعث می‌شوند نظریه روابط بین‌الملل/ اقتصاد سیاسی بین‌الملل، فهم بهتری از شیوه‌های تعامل فناوری با سیاست بین‌الملل، اقتصاد و جامعه جهانی به‌دست دهد. در حال حاضر دولت‌ها دیگر نمی‌توانند تحولات فناورانه، اقتصادی و اجتماعی را مستقل از یکدیگر مدیریت کنند؛ ازاین‌رو، به‌نظر می‌رسد حداقل، برخی از استدلال‌های جبرگرایانه مورد تأیید قرار گرفته‌اند (برای مثال، گفته می‌شود که دولت‌ها نمی‌توانند مستقل از یکدیگر تصمیم بگیرند و تصمیمات خود را اجرا کنند و به‌عبارت بهتر، حاکمیت خود را در این حوزه از دست داده‌اند). بااین‌همه، تلاش‌های فزاینده‌ای که در سراسر جهان برای حل مسائل مرتبط با فناوری در درون نهادهای بین‌المللی انجام می‌گیرد، نشان می‌دهد که امکانات جدیدی برای کنترل و تأثیرگذاری بر تحولات جهانی سر برآورده‌اند. این وضعیت، عرصه را برای طرح استدلال‌های رویکرد سازه‌انگاری اجتماعی باز می‌کند. رویکرد سازه‌انگاری اجتماعی در این راستا اساساً امکان کنترل و تداوم تحولات فناورانه را، این بار در سطح جهانی، مفروض قرار می‌دهد.

۷-۵ تأثیرات چندبُعدی فناوری

۷-۵-۱ سطح فردی

در تحلیل‌هایی که درزمینه فرایندهای چندبعدی سیاست و اقتصاد جهانی و فرایندهای تعامل فرهنگی و اجتماعی ارائه می‌شوند، اصطلاح «انقلاب مهارت‌ها»[1] افزایش نقش مهارت‌های افراد را توصیف می‌کند. فناوری‌های اطلاعاتی و ارتباطاتی، اساس بهبود و

1. Skill Revolution

ارتقای ظرفیت «گردآوری و تحلیل اطلاعات» را تشکیل داده‌اند.(۳۱) توزیع جغرافیایی این فناوری‌ها در بخش‌های وسیعی از کره زمین و کاهش هزینه‌های خرید و استفاده از آنها به «دمکراتیزه شدن فناوری»[1] انجامیده است. این وضعیت، فناوری‌های بیان شده را در دسترس بیشتر افراد ـ حداقل در جهان صنعتی شده[2] ـ قرار داده است. وانگهی، افراد نیز آموخته‌اند که چگونه از فناوری‌های اطلاعاتی و ارتباطاتی از قبیل پست الکترونیک یا تلفن‌های همراه استفاده کنند تا بتوانند علایق خود را بیان کنند و با سایر افرادی که اندیشه‌ها، هویت‌ها، یا تصاویر مشترکی از دشمن دارند، با پیوندهای شبکه‌ای تعامل داشته باشند. این وضعیت، افراد را قادر می‌سازد برای بیان اندیشه‌ها و علایق یا اجرای آنها در سطح جهان اجتماعات جدیدی را تشکیل دهند.(۳۲) یکی از نمونه‌های این «انقلاب مهارت‌ها» مبارزه اطلاعاتی جنبش زاپاتیست‌ها[3] با فرایند آزادسازی تجاری در داخل منطقه تجارت آزاد آمریکای شمالی در سال ۱۹۹۲ با اینترنت بود.[4] اعضای این جنبش تصور می‌کردند اقدام دولت مکزیک به افزایش واردات غلات ارزان‌قیمت از خارج، سبک زندگی سنتی‌شان را به خطر انداخته است.(۳۳)

نمونه دیگر، جنبش گسترده مبارزه با جهانی شدن بود. یکی دیگر از نمونه‌های افزایش ظرفیت‌های هماهنگ‌سازی، که در اثر فناوری‌های اطلاعاتی و ارتباطاتی و فناوری‌های مدرن در عرصه حمل‌ونقل (مثل هواپیماها) پدید آمده است، حملات تروریستی به نیویورک و واشنگتن در یازده سپتامبر ۲۰۰۱ است. افزایش وابستگی جوامع مدرن به طیف وسیعی از فناوری‌ها، اهداف بالقوه جدیدی را برای همه انواع تروریسم ایجاد می‌کند.(۳۴) در حوزه اقتصاد، افراد با خرید و فروش اطلاعات از راه اینترنت می‌توانند استقلال بیشتری را در تصمیم‌گیری‌های خود به‌دست آورند (برای مثال، قیمت یک کالای خاص را در وب‌سایت‌های مختلف مقایسه کنید) و ازاین‌رو، بازدهی تصمیماتی را که درزمینه کالاهای مصرفی می‌گیرند، بالا می‌برند.(۳۵) براون و استودمیستر[5] درباره افزایش نفوذ افراد در روابط بین‌الملل به به این نتیجه‌گیری می‌رسند: تک‌تک دولت‌ها انجام

---

1. Democratisation of Technology
2. Industrialised World
3. Zapatista
4. Northern American Free Trade Area (NAFTA)
5. Studemeister

واکنش‌های مؤثر در برابر اقدامات اَبَرــ افـرادی[1] از قبیـل بیـل گیـتس،[2] جـرج سـوروس،[3] جیمی کارتر[4] یا اسامه‌بن‌لادن را اگر نگوییم غیرممکن، دشوار می‌دانند.(۳۶)

۲-۵-۷ ساختارهای جدید در سیاست جهانی

این موضوع به افول نسبی حاکمیت دولت در اثر فرایندهای جهـانی شـدن و یـا فراملـی شدن[5] اشاره دارد که بیش از هر چیز از فناوری‌های اطلاعاتی و ارتباطاتی و فناوری‌هـای حمل‌ونقل سرچشمه می‌گیرد. در قلمرو اقتصاد، فشاری که بازارهای مالی یا شرکت‌هـای چندملیتی برای انجام اقداماتی برای انطباق با الزامات سرمایه‌داری جهـانی بـر دولـت‌هـا وارد می‌کنند، برخی از نویسندگان را بر آن داشته است که از ظهور ویژگـی‌هـای جدیـد دولـت، از جملـه «دولـت تـاجر»،[6](۳۷) «دولـتِ رقابـت‌گـرا»،[7](۳۸) یـا خـصوصی‌سـازی و بازارمحوری[8] ساختارهای سیاسی و اقتصادی که دولت رفـاهی را در عـصر صـنعتی زیـر فشارهای شدید قرار می‌دهند ـ سخن به میان آورند.(۳۹) اگر دولت‌هـا بخواهنـد حـداقل، بخشی از قدرت خود را از افول نجات دهند می‌باید خود را با این شرایط جدید منطبق و سازگار کنند. در قلمرو اقتصادی، که توجه خاصی به فناوری‌های برتر اطلاعـاتــ بـر[9] و فناوری بسیار گران‌قیمت مبذول می‌گردد، این وضعیت به ارتقـای مـداوم سیـستم‌هـای آموزش‌وپرورش و تحقیقات در سطح ملی می‌انجامد و محـیط‌هـای پرجاذبـه‌ای را بـرای سرمایه‌گذاری مستقیم خارجی، ظهور نیروهای کار بسیار ماهر و انعطـاف‌پـذیر در سـطح ملی و استقرار زیرساخت‌های فنـاوری‌هـای بـه‌روز (از جملـه، فنـاوری‌هـای اطلاعـاتی و ارتباطاتی و فناوری‌های حمل‌ونقل) و غیره فراهم می‌کند.(۴۰)

البته، دولت‌ها هنوز هم می‌توانند بـر بازارهـا و تحـولات فناورانـه تـأثیر بگذارنـد و

---

1. Supra-Individuals
2. Bill Gates
3. George Soros
4. Jimmy Carter
5. Transnationalisation
6. Trading State
7. Competition State
8. Marketisation

۹. Information-intensive: به‌عبارت بهتر، نقش اطلاعات در این حوزه، چشمگیر است ـ م.

می‌کوشند جریان‌های اطلاعات را در کنترل خود درآورند. برای مثال، دولت آمریکا نقش مهمی در گسترش اینترنت به سراسر جهان ایفا کرد و با سازمان تجارت جهانی و در راستای تأمین منافع شرکت‌های چندملیتی خود، «انحصارهای ارتباطاتی» را که روزگاری در مالکیت دولت‌ها بود، آزادسازی کرد.[۴۱] اما نقش دولت در اینجا با تشکیل و حمایت از ساختارهای جهانی فراگیر با اقدام اقتصادی پیوند می‌خورد. این امر ایالات متحده آمریکا را (مانند سایر دولت‌های صنعتی شدهٔ غربی) از فرایندهایی از قبیل، «دسترسی به منابع و فعالیت‌های اقتصادی برون‌مرزی» ـ که در هنگام برگزاری آخرین انتخابات ریاست جمهوری، موضوعی بسیار مناقشه‌برانگیز در حوزه اقتصادی به‌شمار می‌آمد ـ محروم نمی‌سازد. کنترل روند اطلاعات هرگز کامل نخواهد بود. تروریست‌ها در واکنش به تقویت کنترل‌ها بر روند اطلاعات در اینترنت و ارتباطات سیار، با استفاده از شیوه‌های قدیمی‌تر برقراری ارتباط مثل نوارهای ویدئویی و پیک‌های نامه‌بر، این فناوری‌های اطلاعاتی و ارتباطاتی را دور زدند.

شرکت‌های چندملیتی، به‌ویژه شرکت‌هایی که در بخش فناوری‌های برتر فعالیت دارند، با تشدید رقابت جهان‌گستر بر سر رهبری در حوزه‌های فناوری و بازار مواجه‌اند. آنها پیوسته ناگزیرند خود را با تقاضاهای مصرف‌کنندگان و استانداردهای فناورانهٔ جدید منطبق سازند. چرخه‌های تولید کوچک و کوچک‌تر می‌گردند و تحقیقات و توسعه محصولات جدید نیز پرهزینه‌تر می‌شوند. ازاین‌رو، بسیاری از شرکت‌های چندملیتی به ابتکار عمل نوینی دست می‌زنند و به‌منظور کاستن از هزینه‌های تحقیقات و توسعه به همکاری‌های استراتژیک با رقبای خود روی می‌آورند یا برای جبران هزینه‌های تحقیقات و توسعه، فعالیت‌های خود را به بازارهای جدید گسترش می‌دهند.

یکی دیگر از جنبه‌های ساختاری بسیار مهم در بخش‌های مختلف فناوری در سطح جهان مسئله استانداردهای فناورانه بوده است. بهترین نمونه دراین‌باره، تحرک و جابه‌جایی آزادانه منابع در بخش نرم‌افزار است که در حال حاضر در حال ظهور است. بازیگران ریشه‌دار اصلی مثل مایکروسافت به‌شدت با این وضعیت به مخالفت برخاسته‌اند.[۴۲] نمونه دیگر درباره اهمیت روزافزون استانداردهای فناورانه، منازعه میان تولیدکنندگان تجهیزات ارتباطاتی در اروپا، شرق آسیا و ایالات متحده بر سر نحوه تعیین

استانداردهای فناورانه برای نسل بعدی ارتباطات سیار بی‌سیم است.(۴۳) فقط دولت‌ها، بازارها و شرکت‌های چندملیتی نیستند که در نظام بین‌المللی، توان بالقوه چشمگیری برای انجام اقداماتی در گستره‌ای جهانی به‌دست آورده‌اند؛ بلکه بازیگران اجتماعی جدیدی مثل سازمان‌های غیردولتی، جنبش‌های اجتماعی یا خرده‌گروه‌هایی که نمایندگان جامعه مدنی خوانده می‌شوند نیز مهارت‌های خود را گسترش داده‌اند. بسیاری از این بازیگران، خود، در سطحی گسترده از فناوری‌های اطلاعاتی و ارتباطاتی استفاده می‌کنند.

لیفین[1] نشان داده است آن سازمان‌های غیردولتی که با مسائل تخریب جنگل‌ها یا گرم شدن کره زمین سروکار دارند برای طرح نگرانی‌های خود در مورد این مسائل از عکس‌های پروضوحی که شرکت‌های ماهواره‌ای تجاری- غیرنظامی تهیه کرده‌اند استفاده می‌کنند و از این راه بر دستگاه‌ها و تشکیلات اداری دولت‌ها فشار وارد می‌کنند تا در برابر این مسائل واکنش نشان دهند. گروه‌های مخالف جهانی شدن، گروه‌های مخالف مین‌های زمینی و غیره با اینترنت و دستگاه‌های ارتباطات سیار، فعالیت‌های خود را باهم هماهنگ می‌کنند و به دنبال کسب پایگاه‌های حمایتی در سراسر جهان می‌روند.(۴۴) برخی از سازمان‌های غیردولتی از قبیل سازمان حریم خصوصی بین‌المللی[2] که موضوع «آزادی همیشگی خود اینترنت» را دنبال می‌کنند پیام‌های خود را با فضای سایبر اشاعه می‌دهند و می‌کوشند نگرانی‌های خود را درزمینه تجاری شدن اینترنت که شرکت‌های چندملیتی جدید قرن بیست‌ویکم با زور و با توسل به معیارهای حمایت از مالکیت فکری به‌وجود آورده‌اند ابراز نمایند.(۴۵)

۳-۵-۷ شیوه‌های جدید تعامل

همه فرایندهایی که در بالا توصیف شدند به ظهور شیوه‌های جدید حکمرانی[3] در نظام بین‌الملل می‌انجامند. دولت‌ها دیگر در موقعیتی نیستند که به‌طور انحصاری و به تنهایی قواعد بازی سیاسی و اقتصادی را دیکته کنند؛ ازاین‌رو دولت‌ها در برابر این وضعیت واکنش نشان می‌دهند: از یک‌سو همکاری‌ها میان خود را با نهادهای دولتی بین‌المللی

1. Liffin
2. Privacy International
3. Governance

(سازمان‌های بین‌المللی دولتی یا رژیم‌های بین‌المللی) افزایش داده‌اند و ازسوی‌دیگر، با روی آوردن به همگرایی در مناطق مختلف جهان، در جوامع بزرگ‌تری که مبنای آنها اقتصادی بوده است جای گرفته‌اند ـ در این زمینه، می‌توان به اتحادیه اروپایی اشاره کرد.(۴۶) این وضعیت امکان کسب قدرت جدیدی را به آنها می‌دهد، به‌طوری‌که با توسل به آن می‌توانند به شرایط اساسی اقتصادی و سیاسی که بر تحولات فناورانه در آینده تأثیر می‌گذارند، شکل دهند.(۴۷)

روزنا خاطرنشان کرده است دولت‌هایی که می‌خواهند به شبکه‌های جهان ـ گستر فناوری دسترسی داشته باشند، هیچ چاره‌ای جز پیوستن به آن نهادهای بین‌المللی که به نمایندگی از همه، مقررات فناوری‌های مورد نظر را تنظیم می‌نمایند، ندارند.(۴۸) اما درعین‌حال نیز، آنها باید همکاری با بازیگران غیردولتی مثل شرکت‌های چندملیتی، سازمان‌های غیردولتی یا سایر گروه‌های فرعی[1] را که حداقل در برخی از ابعاد روابط بین‌الملل/ اقتصاد سیاسی بین‌الملل با دولت‌ها رقابت می‌کنند، افزایش دهند.(۴۹) روزنا ظهور این حوزه‌های جدید تعامل میان بازیگران غیردولتی سیاسی، اجتماعی و اقتصادی را که اقتدار ـ خصوصی ـ خودشان را (براساس ارزش‌ها، هنجارها، منافع خاستگاه یا جهت‌گیری محلی) توسعه می‌دهند، «جهان چندمحور»[2] توصیف کرده است. به‌نظر او، این جهان چندمحور به‌نوبه خود، حوزه‌های جدید اقتدار[3] را نیز ایجاد کرده است.(۵۰) این جهان چندمحور اقتصاد جهانی به همراه جامعه مدنی جهانی، گروه‌های ذی‌نفع محلی بی‌شمار و غیره مدام با جهان دولت‌محور[4] سنتی که هنوز نیز وجود دارد، تعامل دارد. جهان چندمحور از جوامعی که اقتدار خود را از جهات بسیار گوناگون رو به زوال می‌بینند، تشکیل شده است. این وضعیت، شکل جدیدی از حکمرانی بدون حکومت[5] را ایجاد می‌کند که شبکه پیچیده‌ای از بازیگران مختلف و پرشمار را در خود دارد. این بازیگران برای کسب نفوذ در حوزه‌های موضوعی مختلف و نقش‌آفرینی در تنظیم مقررات در آن حوزه‌ها در سطوح مختلف با یکدیگر تعامل دارند.(۵۱)

---

1. Supgroup
2. Multicentric World
3. New Spheres of Authority
4. State-centric World
5. Governance Without Government

۶-۷ نتیجه‌گیری

به جمله آغازین فصل (فناوری نه خوب است نه بد، بی‌طرف و خنثی هم نیست) بازمی‌گردیم. مباحث این فصل نشان داده که فناوری در روابط بین‌الملل/ اقتصاد سیاسی بین‌الملل نمایانگر «ابزاری منفعل یا جعبه سیاهی از پیش موجود» بیش نیست، اما درعین‌حال، چندان هم خارج از کنترل کارگزاری انسان نمی‌باشد.(۵۲) فناوری نه تنها بر بازیگران، هویت‌ها و منافع آنها تأثیر عمیقی می‌گذارد، بلکه بر فرایندها و ساختارهای نظام بین‌الملل نیز به‌شدت تأثیر دارد. در سطح فردی، فناوری به شیوه‌های مختلفی مورد استفاده قرار می‌گیرد برای مثال، اینترنت می‌تواند برای انجام کارهای تجاری، برقراری ارتباط با دوستان، یا سازمان‌دهی و اجرای حملات تروریستی به‌کار گرفته شود. دولت‌ها و شرکت‌های چندملیتی نیز بی‌آنکه بتوانند همه تأثیرات جانبی و احتمالی سیاسی، اقتصادی و اجتماعی فناوری‌های جدید را ارزیابی کنند، در مورد توسعه و توزیع این فناوری‌ها تصمیم می‌گیرند.

سرانجام، در سطح جهانی، فناوری در بیشتر کاربردهای جدید آن در قالب سیستم‌های بزرگ[1] که بیشتر بخش‌های جهان را فرا گرفته‌اند و حداقل تا اندازه‌ای مستقل عمل می‌کنند، توسعه یافته است؛ (برای مثال، دراین‌باره می‌توان به تأثیرات جانبی منفی، محاسبه‌های قبلی در مورد تصمیمات آینده در حوزه فناوری و غیره اشاره کرد)(۵۳). در سطح جهانی است که سیستم‌های فناورانه ویژگی‌هایی به‌نسبت جبرگرایانه ایجاد می‌کنند؛ و ازاین‌رو، ما شاهد نوعی وابستگی ابنای بشر به فناوری هستیم. خواننده چه‌بسا ممکن است فقط تلاش کند که جهان را بدون حضور حمل‌ونقل عمومی، اتومبیل‌ها، هواپیماها، فناوری‌های اطلاعاتی و ارتباطاتی و غیره تصور کند. جلوه‌های این تلاش چه خواهند بود؟ در بسیاری موارد، توسعه فناوری در آینده، که تمایل دارد افراد بیشتر و بیشتری را منتفع سازد، تنها در سطح جهانی می‌تواند مدیریت گردد و مقررات جدید برای کنترل آن وضع شود. این امر تلاش‌های هماهنگ میان همه بازیگران نظام برای پیشبرد بهتر حکمرانی جهانی[2] را بیش‌ازپیش ضروری می‌سازد.

---

1. Mega-systems
2. Global Governance

نظریه‌های روابط بین‌الملل و اقتصاد سیاسی بین‌الملل تنها در یک صورت قادر خواهند بود بینش‌های بیشتری را در مورد شیوه‌های تأثیرگذاری فناوری بر نظام بین‌الملل و ساختارها، فرایندها و بازیگران آن به‌دست آورند؛ این امر در زمانی محقق می‌شود که این نظریه‌ها به بحث‌های مطرح در رشته‌های هم‌جوار علوم اجتماعی نیز بیشتر توجه کند. در جمع‌بندی این برداشت باید گفت: «در تاریخ نظریه روابط بین‌الملل/ اقتصاد سیاسی بین‌الملل، فناوری به‌تدریج به‌عنوان مقوله‌ای تحلیلی که تحولات سیاسی، اقتصادی و اجتماعی در نظام بین‌الملل را توصیف، تبیین و پیش‌بینی می‌کند اهمیت یافته است. با وجود این، هنوز هم به‌نظر می‌رسد فناوری در بیشتر چارچوب‌های نظری روند اصلی که در اینجا مطرح شدند عاملی منفعل، کم‌ارزش و برون‌زاد[1] می‌باشد. بسیاری از تحقیقات آینده در حوزه نظریه روابط بین‌الملل/ اقتصاد سیاسی بین‌الملل باید به‌گونه‌ای باشد که موضوع فناوری و نقش فزاینده آن در نظریه‌های بیان شده را به معنای دقیق کلمه در خود جای دهد.

1. Exnogeneous

پی‌نوشت‌ها

1. M. Kranzbert,'The Information Age: Evolution or Revolution in B.R. Guile (ed.), *Information Technologies and Social Transformation,* Washington DC: National Academy of Engineering, 1985, p.50.

2. H. Brooks, Technology, Evolution and Purpose in Modern Technology. Daedalus, 109 (1), 1980, 65-81.

3. M. Van Creveld, *Technology and War: From 2000 B.C. to the Present*, New York: The Free Press, 1989; W.H. Mcneill, The Pursuit of Power: *Technology, Armed Forces, and Society Since A.D. 1000*, Chicago: University of Chicago Press, 1982; and A. Pacey, *Technology in World Civilization: A Thousand-Year History*, Cambridge, MA: MIT Press, 1990. For the Role of Science and Technology in Western Economic Development, see N. Rosenberg and L.E. Birdzell, *How the West Grew Rich: The Economic Transformation of the Industrial World*, New York: Basic Books, 1986; and D. Landes, *The Wealth and Poverty of Nations: Why Some are so Rich and Some so Poor*, New York: w.w.Norton, 1998.

4. B. Brodie, 'The Atom Bomb as Policy Maker', *Foreign Affairs*, 27(1), 1948/49, 17-33. Also see R. Jervis, 'The Political Effects of Nuclear Weapons: A Comment', *International Security*, 13(2), 1988, PP.80-90; and C.S. Gray, The Geopolitics of the Nuclear Era: Heartlands, Rimlands, and the Technological Revolution, New York: Crane, Russak & Company Inc., 1977.

5. W. Wriston, 'Technology and Sovereignty', *Foreign Affairs*, 67 (2), 1988/89, 63-75.

6. For Probably one of the Earliest Attempts to Analyse Different Technologies and their Impact on IR see W.F. Ogburn (ed.), *Technology and International Relations, Chicago*: The University of Chicago Press, 1949.

7. E.B. Skolnikoff, *The Elusive Transformation: Science, Technology and the Evolution of International Politics*, Princeton, NJ: Princeton University Press, 1993, p.9.

8. H.J. Morgenthau, Politics among Nations, New York: Knopf, 1948; and R. Niebuhr, Moral Man and Immoral Society, New York: Scribner's, 1947.

9. K.N. Waltz, *Theory of International Politics*, New York: McGraw-Hill Inc., 1979.

10. Z. Brzezinski, *American Primary and Its Geostrategic Imperatives,* New York: Basic Books, 1997.

۱۱. سه نمونه، این فرض را به اثبات می‌رساند:

الف) در سال ۱۹۶۱، هانس مورگنتا دیدگاهی کم‌وبیش تعدیل شده را در مورد تسلیحات هسته‌ای ابراز داشت: «من فکر می‌کنم انقلابی رخ داده است. شاید این انقلاب، اولین انقلاب واقعی است که از زمان آغاز تاریخ یعنی از زمان ورود تسلیحات هسته‌ای به زرادخانه جنگ‌ها، در حوزه سیاست خارجی رخ داده است. زیرا از آغاز تاریخ تا پایان جنگ جهانی دوم، رابطه‌ای عقلایی میان خشونت به‌عنوان ابزار سیاست خارجی و اهداف سیاست خارجی وجود داشت، به‌عبارت‌دیگر یک دولتمرد می‌توانست از خودش سؤال کند ـ و همواره از خودش می‌پرسید ـ که آیا می‌تواند با ابزارهای دیپلماتیک مسالمت‌آمیز به آنچه برای ملت خود می‌خواست دست یابد یا ناگزیر است به جنگ متوسل شود. [...] آن دولتمرد در دوران پیش از ظهور تسلیحات هسته‌ای به معنای واقعی کلمه نقش یک قمارباز را ایفا می‌کرد [...] که حاضر است بخشی از منابع مادی و انسانی‌اش را به خطر بیاندازد. اگر وی برنده شود، پیروزی ریسک او را توجیه می‌کند و اگر بازنده شود، همه چیز را از دست نداده است. به‌عبارت‌دیگر، ضررهای او قابل تحمل بودند. اما احتمال بروز جنگ هسته‌ای تمام‌عیار، این رابطه عقلایی بین خشونت به‌عنوان ابزار سیاست خارجی و اهداف سیاست خارجی را از میان برده است». نگاه کنید به:

H. Morgentau, "Western Values and Total War", *Commentary*, 32(4)(1961), 4, p.280.

ب) در همین خصوص، رابرت گیلبین می‌گوید: «جنگ‌افزارها و موشک‌های اتمی درواقع، تأثیر چشمگیری بر ماهیت و ابزارهای کشورداری نهاده‌اند. [...] دلایلی هم برای خویش‌بینی محتاطانه وجود دارد، چرا که برای اولین بار در طول تاریخ، تهدید تسلیحات گرماهسته‌ای علیه بقای ملی، منفعتی مشترک، همه‌جانبه و نیرومند درزمینه پرهیز از جنگ را برای ملت‌ها فراهم می‌سازد. بنابراین، تعقیب این منفعت مشترک با نهادهای بین‌المللی و اصول رفتاری متناسب به یکی از مهم‌ترین چالش‌هایی مبدل می‌شود که فناوری مدرن برای کشورداری امروز ایجاد کرده است. نگاه کنید به:

R. Gilpin, *Has Modern Technology Changed International Politics*? In I.N. Rosenav, V Davis, M.A.East (eds), *The Analysis of International Politics: Essays in Honour of Harold and Margaret Sprout*, New York: The Free Press, 1972, p.173.

ج) باری بوزان و ریچارد لیتل که مفهوم «ظرفیت تعامل» را برای تمایز نهادن میان نظام‌های بین‌المللی باستان، کلاسیک و مدرن ارائه می‌دهند، دیدگاه نوواقع‌گرایانه تعدیل شده‌ای را مطرح

می‌کنند. براساس نظر آنها، پیشرفت‌های سریع درزمینه فناوری‌های مدرن نظامی، ارتباطاتی و حمل‌ونقل، ظرفیت‌های تعامل را بسیار افزایش داده‌اند و ازاین‌رو ـ برای نخستین بار در تاریخ بشر ـ یک نظام بین‌المللی به‌وجود آورده‌اند که به معنای واقعی کلمه «جهان‌گستر» است. وانگهی، پیشرفت در حوزه فناوری باعث ظهور بازیگران جدیدی شده است که تا حدودی با دولت‌ها (به‌عنوان بازیگران مسلط در نظام بین‌الملل) به رقابت می‌پردازند.

نگاه کنید به:

B. Buzan and R.Little, International Systems in World History: Remaking the Study of International Relations, Oxford: Oxford University Press, 2000.

اگر انصاف به خرج دهیم، می‌باید به آثار دیگری نیز اشاره کنیم که عموماً با واقع‌گرایی پیوند دارند و آشکارا به «فناوری و تأثیرات آن درزمینه ساختار بخشیدن به نظام بین‌المللی و بازیگران آن» توجه نموده‌اند. این آثار عبارت‌اند از:

R. Aron, *Peace and War: A Theory of International Relations*, New York: Doubleday & Co, 1966; R.Gilpin, *War and Change in World Politics*, Cambridge: Cambridge University Press, 1981; and R. Gilpin, *The Political Economy of International Relations*, Princeton: Princeton University Press, 1987.

12. J.N. Rosenau, *Turbulence in World Politics: A Theory of Change and Continuity*, New York and London: Harvester-Wheatsheaf, 1990, p.6.

13. Ibid., p. 78.

14. J.N. Rosenau, *Along the Domestic-foreign Frontier: Exploring Governance in a Turbulent World*, Cambridge: Cambridge University Press, 1997, P.4.

15. Rosenau, *Turbulence in World Politics*, p. 12f.

16. D. Held, and A McGrew, and D. Goldblatt, and Perration, *Global Transformations*. *Politics, Economics and Culture*, Cambridge: Policy Press, 1999.

17. R. Langhorne, The Coming of Globalization: Its Evolution and Contemporary Consequences, Basingstoke: Palgrave Macmillan, 2001, P.2.

18. F. Fukuyama, *The End of History and the last Man*, New York: Perennial, 1993, PP.71-108.

19. Ibid., p.108.

20. B.R.J. Jones, The World Turned Upside Down? Globalization and the Future

of the State, Manchester: Manchester University Press, 2000.

21. Rosenau, *Along the Domestic-foreign Frontier*, p.47. Emphasis Added by the author.

22. N. Onuf, 'Constructivism: A User's Manual', in V. Kubalkova, N. Onuf and P. Kowert (eds), International Relations in a Constructed World, Armonk, NY: M.E. Sharpe, 1998, S. 58.

23. T. Hopf, 'The Promise of Constructivism in International Relations Theory' *International Security*, 23(1), 1998, 182.

24. A. Wendt, *Social Theory of International Politics,* Cambridge: Cambridge University Press, 1999, p.92.

25. Ibid., p. 73.

26. Ibid., p. 111.

27. J. Checkel, 'The Constructivist Turn in International Relations Theory', *World Politics,* Vol. 50, 1998, No. 1, P.326.

28. P. Weingart (ed.), Technik als Sozialer Prozeeß (Frankfurt am Main: Fischer, 1989). W.E. Bijker, T.P. Hughes and T.J. Pinch, (eds), The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology, Cambridge, MA: MIT Press, 1987.

29. N.J. Vig, 'Technology, Philosophy, and the State: An Overview' in M. Kraft and N.J. Vig (eds), Technology and Politics, Durham and London: Duke University Press, 1988, PP.8-32; A recently Published Introductory Work to the Changing Philosophy of Technology is: D.M. Kaplan (ed.), Readings in the Philosophy of Technology, Lanham, Boulder and et. al.: Rowman & littlefield Publisihers Inc., 2004. See also U. Teusch, Freiheit und Sachzwang. Untersuchungen zum Verhältnis von Technik, Geselslchaft und Politik, Baden-Baden: Nomos Verlagsgesellschaft, 1993.

30. L. Mumford, Technics and Civilization, New York: Harcourt Brace & Company, 1934; J. Ellul, La Technicque ou L'enjeu du Sie'cle (Paris: Economica, 1990 [1964]; and L. Winner, Autonomous Technology. Technics-out-of-Control as a Theme in Political Thought, Cambridge, MA: MIT Press, 1977; L. Marx and M.R. Smith (eds), Does Technology drive History? The Dilemma of Technological Determinism, Cambridge, MA: MIT Press, 1994.

31. T.L Friedmann, The Lexus and the Olive Tree, New York: Farrar, Straus & Giroux, 1999.

32. J.N. Rosenau, and M.W. Fagen, 'A New Dynamism in World Politics. Increasingly Skillful Individuals?, International Studies Quarterly, 41(4),

1997, 655-86.

33. D. Ronfeldt and A. Martinez, 'A Comment on the Zapatista "Netwar", in J. Arquila and D. Ronfeldt (eds), in Athena's Camp: Preparing for Conflict in the Information Age, Rand: National Defence Research Institute, 1997, PP.369-391.

34. T. Homer-Dixon, 'The Rise of Complex Terrorism', *Foreign Policy*, 1 (2002), 52-62.

35. K. Ohmae, Der Unsichtbare Kontinent: Vier Strategische Imperative für die New Economy, Vienna: Ueberreuter Verlag, 2001.

36. S.J. Brown and M.S. Studemeister, Diffusion of Diplomacy. Net Diplomacy I. Beyond Foreign Ministries, Part III. United States Institute of Peace 2002. Available at www.usip.org/virtualdiplomacy/ publications /reports/14c. html.

37. R. Rosecrance, The Rise of the Trading State, New York: Basic Books, 1986.

38. P.G. Cerny, The Changing Architecture of Politics: Structure, Agency, and the Future of the State, London: Sage Publications, 1990.

39. Ibid., p. 339.

40. R. Palan, J. Abbott, and P. Deans, State Strategies in the Global Political Economy, London and New York: Pinter, 1996.

41. D. Schiller, Digital Capitalism: Networking the Global Market System, Cambridge, MA: MIT Press, 1999.

42. T. Baumgärtel, 'Am Anfang war alle Software frei. Microsoft, Linux und die Rache der Hacker', in A. Roesler and B. Stiegler (eds), Microsoft: Medien, Macht, Monopol, Frankfurt am Main: Edition Suhrkamp, 2002, PP. 103-29. See also K. Sanabae and J.A. Hart, 'The Global Political Economy of Wintelism: A New Mode of Power and Governance in the Global Computer Industry, ' in J.N. Rosenau, and J.P. Singh (eds), Information Technologies and Global Politics: The Changing Scope of Power and Governance, Albany: Stage University of New York Press, 2002, PP.143-68.

43. K. T. Litfin, 'public Eyes. Satellite Imagery, The Globalization of Transparency, and New Networks of Surveillance', in J.N. Rosenau and J.p. Singh (eds), Information Technologies and Global Politics: The Changing Scope of Power and Governance, Albany: State University of New York Press, 2002, PP.65-89.

44. For Some Detailed Examples of NGOs and their use of ICTs see C. Warkentin, Reshaping World Politics: NGOs, the Internet, and Global Civil

Society, Lanham, MD and Boulder, CO: Rowman & Littlefield publishers Inc., 2001.

45. L. Lessig, Code and Other Laws of Cyberspace, New York: Basic Books, 1999, and L. Lessig, The Future of Ideas: The Fate of the Commons in a Connected World, New York: Random House, 2001.

46. P.G. Cerny, 'Globalization and the Changing Logic of Collective Action', *International Organization*, 49(3) (1995), 595-625. For Economic Regionalization, see K. Ohmae, 'The Rise of the Region State', *Foreign Affairs*, 72(2), 1993, PP. 78-87.

۴۷. یکی از نمونه‌های (فوق ملی)، تلاش‌هایی است که در درون اتحادیه اروپایی برای تدوین استراتژی‌هایی برای مشارکت موفقیت‌آمیز در اقتصاد اطلاعاتی جهانی انجام گرفته‌اند. نگاه کنید به:

- European Union, eEurope 2002: An Information Society for All (Action Plan prepared by the Council and the European Commission for the Feira European Council, 19-20 June 2000).

نمونه دیگری از تلاش‌هایی که در درون سازمان‌های بین‌الدولی برای حل «معضلات جهانی ناشی ظهور جامعه اطلاعاتی جهانی» (برای مثال، تشدید شکاف دیجیتالی میان فقرای اطلاعاتی و اغنیای اطلاعاتی) انجام گرفته است، اجلاس جهانی جامعه اطلاعاتی است که اتحادیه بین‌المللی مخابرات (سازمان تخصصی ملل متحد که مقر آن در ژنو است) در اوایل سال ۲۰۰۳ و سال ۲۰۰۵ در ژنو و تونس برگزار شدند. هدف این فرایند، این است که بر روی شکاف دیجیتالی موجود میان شمال و جنوب پل بزند.

48. M. van Creveld, *The Rise and Decline of the State*, Cambridge: Cambridge University Press, 1999, p. 380.

۴۹. یک نمونه از همکاری میان شرکت‌های چندملیتی و دولت‌ها، کنسرسیوم اروپایی به رهبری شرکت اریکسون است که اتحادیه اروپایی را متقاعد ساخت استاندارد GSM را برای ارتباطات سیار به تصویب برساند. یک نمونه دیگر درزمینه این‌گونه اتحادها میان دولت‌ها و شرکت‌های چندملیتی مذاکرات در درون اتحادیه بین‌المللی مخابرات میان تولیدکنندگان تجهیزات مخابراتی، مؤسسات ارائه‌دهنده خدمات مخابراتی و دولت‌ها برای تدوین استانداردهای جدید در حوزه ارتباطات سیار است.

50. Rosenau, p. 15; Y.H. Ferguson and R.W. Mansbach, 'History's Revenge and Future Shocks, The Remapping of Global Politics', in M. Hewson and T.J.

Sinclair (eds), *Approaches to Global Governance Theory*, Albany: State University of New York Press, 1999, PP. 197-238; M. Castells, *The Information Age: Economy, Society and Culture* Vol. *1: The Rise of the Network Society*, Basic Books: New York, 2000.

51. J.N. Rosenau, 'Governance, Order, and Change in World Politics', in J.N. Rosenau, and E.O. Czempiel (eds), *Governance Without Government: Order and Change in World Politics*, Cambridge: Cambridge University Press, 1992, p. 4.

52. J.P. Singh, 'Introduction. Information Technologies and the Changing Scope of Global Power and Governance', in J.N. Rosenau and J.P. Singh (eds), Information Technologies and Global Politics: The Changing Scope of Power and Governance Albany: State University of New York Press, 2002, p. 11.

53. T.P. Hunghes, 'Technological Momentum', in L. Marx and M.R. Smith (eds), Does Technology Drive History? The Dilemma of Technological Determinism, Cambridge, MA: MIT Press, 1994, PP. 101-13.

فصل هشتم تسلیحات هسته‌ای و دورنمای فرماندهی و کنترل

بروس دی. لارکین*

واشنگتن در سال ۲۰۰۳ اشتباهی بزرگ مرتکب شد، خود را در باتلاق عراق گرفتار ساخت و با اقدامات نسنجیده و ناشیانه‌ای که پس از حمله به عراق انجام داد، نتوانست راه خروج از این بحران را پیدا کند. این «یگانه ابرقدرت»، این «قَدَرقدرت»[1] و این ارباب نظامی جهان، به همین سادگی این تصمیم اشتباه را گرفته است. وانگهی ناکامی‌هایش نیز به‌دست خودش به‌وقوع پیوست. کاخ سفید و رهبران غیرنظامی پنتاگون نیز خودشان را به وهم و خیالی بزرگ متقاعد ساختند. این نهادها مبانی اطلاعاتی را نادیده گرفتند، زیر پا نهادند، یا به‌کلی رد کردند و مدعی وجود حقایقی شدند که نمی‌توانستند به اثبات برسانند و ازاین‌رو فرض را بر این گذاشتند که همگان راهی را که آنها می‌خواستند خواهند پیمود و نیروهایشان را آزادی‌بخش خواهند خواند و از آنها استقبال خواهند کرد. آنها هیچ تردیدی نداشتند که قدرت نظامی ایالات متحده پیروز خواهد شد.

این فصل، نه جنگ عراق در سال ۲۰۰۳ و پیامدهای آن، بلکه موضوع تسلیحات هسته‌ای را بررسی می‌کند، اما در این میان به سؤالی که این جنگ مطرح کرد می‌پردازد. فرض می‌کنیم واشنگتن در تجاوز به عراق، اقدامی بسیار اشتباه انجام داد، آیا باز هم می‌توانیم مطمئن باشیم که ایالات متحده تسلیحات هسته‌ای را مدیریت کند؟

درست است که همگان امکان استفاده از تسلیحات هسته‌ای در این جنگ را نفی می‌کنند و آن را بحثی بی‌مورد می‌دانند، اما درهرحال باید پذیرفت که سیاست جنگی و سیاست هسته‌ای اموری غیرقابل تفکیک‌اند. فرمانده کل قوا که جنگ در عراق را انتخاب

---

* Bruce Larkin

1. Hyperpower

می‌کند فرمانده نیروهای هسته‌ای آمریکا نیز می‌باشد. او نیمی از مقام فرماندهی ملی[1] است که اصولاً باید مجوز استفاده از تسلیحات هسته‌ای را صادر کند و فرمانده کل ارتش نیز می‌باشد. نیم دیگر مقام فرماندهی ملی، یعنی وزیر دفاع، همان دونالد رامسفلد است که حمله به عراق را واکنشی مناسب به حملات یازده سپتامبر می‌دانست و از آن حمایت می‌کرد. وی همان کسی است که بر نحوه اداره جنگ عراق نظارت کرده است. گزارش موضع هسته‌ای[2] در ژانویه ۲۰۰۲ که خواستار تدوین طرح‌ها و برداشتن گام‌های جدید برای آسان‌تر ساختن ازسرگیری آزمایش‌های هسته‌ای می‌شود و گزارش استراتژی امنیت ملی[3] در سپتامبر ۲۰۰۲، که از پیش‌دستی[4] ایالات متحده درصورت مواجهه با «تهدیدهای قریب‌الوقوع»[5] به‌شدت حمایت می‌کند، استدلال‌های کاخ سفید و پنتاگون را در راستای طرف‌داری از توانمندی‌های نظامی جدید به پیش می‌برند و دو نهاد یاد شده نیز برای استفاده از این توانمندی‌ها ابراز آمادگی کرده‌اند.

البته در این فصل کوتاه من نمی‌توانم همه ابعاد مدیریت تسلیحات هسته‌ای را بررسی کنم. این فصل با تمرکز بر موضوع دسترسی رهبران و فرماندهان نظامی آمریکا به ارتباطات فوری، روشنگر و مطمئن می‌کوشد میزان دقت و قدرت تخریب تسلیحات هسته‌ای در ایالات متحده را بررسی کند.

مدیران تمایل دارند تسلیحات هسته‌ای را به‌خوبی و بدون بروز هیچ خطری مدیریت کنند و برای انجام این کار نیز رویه‌های اندیشمندانه و حساب شده‌ای در اختیار دارند. اما بااین‌حال، آنها با محدودیت‌هایی در حوزه فناوری روبه‌رو می‌شوند، در معرض قضاوت‌ها و محاسبات غلط قرار دارند و امکان خطا در برآوردهای آنها وجود دارد؛ ازاین‌گذشته، هم به سیستم‌های پیچیده‌ای که امکان اختلال در آنها وجود دارد، وابسته‌اند و هم از پیش‌فرض‌هایی که در مورد وفاداری‌ها و عملکرد پرسنل خود دارند تأثیر می‌پذیرند. آنچه در شرایط عادی زمان صلح به‌خوبی و بدون هیچ نقص و اختلالی عمل می‌کند، چه‌بسا ممکن است در هنگام مواجهه با شرایط غیرمنتظره بحران

---

1. National Command Authority (NCA)
2. Nuclear Posture Review
3. National Security Strategy
4. Preemption
5. Imminent Threats

تصمیم‌گیری و استفاده حساب شده از سلاح هسته‌ای مؤثر واقع نشود و به‌خوبی عمل نکند. این به این معناست که ما نمی‌توانیم به مدیریتی که در حال حاضر، ایالات متحده در رابطه با تسلیحات هسته‌ای خود پیش می‌برد اطمینان داشته باشیم. موضع بهتر، موضعی مبتنی‌بر شک‌ورزی در برابر این ادعاست که «هر سیستم فرماندهی و کنترل می‌تواند استانداردهای هم‌بستگی، استحکام، اعتمادپذیری و عملکرد مناسب را که مدیریت تسلیحات هسته‌ای در شرایط کنونی بدان‌ها نیاز دارد برآورده سازد».

۱-۸ کاخ سفید و وزارت دفاع

تسلیحات هسته‌ای الزامات جدیدی را تحمیل می‌کند. دولتی که از قدرت هسته‌ای بهره‌مند است همواره در پیوستاری بین «ضرورت خویشتن‌داری» و «ترس از حمله غافلگیرانه» حرکت می‌کند. این دولت که متعهد به بازدارندگی و منصرف‌سازی[1] است، نیروهای آماده‌باش مستقر می‌سازد. اما باید از کاربرد غیرعمدی و غیرمجاز سلاح هسته‌ای پیشگیری کند. اگر این دولت گزینه‌های «پرتاب وضعیت هشدار» و «پرتاب در وضعیت حمله» را باز بگذارد، آنگاه زمان بسیار کوتاهی میان دریافت هرگونه هشدار و دستور آتش را می‌پذیرد. هر مرحله ـ هشدار، احتیاط، خویشتن‌داری در هنگام بحران و پرتاب ـ به ارتباطات میان مقامات صلاحیت‌دار و پرسنل نظامی متکی است.

کاخ سفید نارسایی‌های ارتباطاتی بسیاری دارد، اما چشمگیرترین نقایص با ضرورت مدیریت کاربرد تسلیحات هسته‌ای ارتباط دارد. سازمان ارتباطات کاخ سفید[2] به‌عنوان بازوی وزارت دفاع (که پرسنل آن نظامی‌اند) این نیازها را برآورده می‌سازد. سازمان ارتباطات کاخ سفید وظیفه دارد تضمین دهد که رئیس‌جمهور و معاون رئیس‌جمهور، چه در واشنگتن باشند چه در سایر مناطق آمریکا، چه در حال عبور از قلمرو آمریکا باشند چه در خارج از مرزهای آمریکا، در همه زمان‌ها از ارتباطات مطمئن بهره‌مندند. نتیجه این مدل معیار، این است که بدون اجازه و رضایت رئیس‌جمهور (که با درج یک رمز ویژه، رضایت خود را به ثبت می‌رساند)، نمی‌توان از تسلیحات هسته‌ای استفاده کرد. حال،

---

1. Dissuation
2. White House Communication Agency (WHCA)

شرایطی را در نظر بگیرید که رئیس‌جمهور به‌علت مرگ یا نداشتن صلاحیت نتواند اقدامات مقتضی را انجام دهد، یا مثلاً تصور کنید اختیار اعطای مجوز استفاده از تسلیحات هسته‌ای «از پیش» به رده‌های پایین‌تر تفویض شده باشد، به‌گونه‌ای که رئیس‌جمهوری نتواند کارویژه خود را انجام دهد. در این حالت‌ها، چه ارتباطاتی باید انجام پذیرد؟

مقام فرماندهی ملی به رئیس‌جمهور و وزیر دفاع تفویض می‌شود. هنجار قاعده دو ـ تن[1] ایجاب می‌کند در هر سطحی از زنجیره فرماندهی، اتفاق‌نظری حداقل میان دو شخص صاحب‌مقام وجود داشته باشد به‌گونه‌ای که استفاده از تسلیحات هسته‌ای نیز امکان‌پذیر شود. در نتیجه در زیرمجموعه مقام فرماندهی ملی تأیید می‌گردد که فرمان هماهنگ صادر شده است و در بالاترین سطح نیز میان رئیس‌جمهور و وزیر دفاع، یا کسانی که در منصب خود مقام فرماندهی ملی را نیز برعهده دارند، درزمینه استفاده از تسلیحات هسته‌ای اتفاق‌نظر وجود دارد. بنابراین باید راهی وجود داشته باشد که از طریق آن، رئیس‌جمهور و وزیر دفاع، یا جانشینان آنها بتوانند باهم تبادل نظر کنند.(۱)

این امر مستلزم آن است که ارتباطات «مطمئن» و «دائمی» بین آنها وجود داشته باشد. در اینجا «مطمئن» به معنای آن است که پیام‌ها و مکالمات آنها یا اطلاعات همراه با آنها درصورت رهگیری ازسوی افراد نفوذی نه تنها قابل فهم نباشند، بلکه توجه افراد نفوذی را به‌سمت اموری غیرمرتبط معطوف سازند و درواقع، آنها را فریب دهند. اگر فرد جانشین به‌جای مقام فرماندهی عمل می‌کند، می‌باید این اطمینان وجود داشته باشد که جایگزینی، اقدامی مناسب است. امنیت کافی نیز از راه رمزگذاری و استفاده از واژگان رمزی ویژه دنبال می‌شود.

۲-۸ سازمان ارتباطات کاخ سفید

سازمان ارتباطات کاخ سفید نه تنها در کاخ سفید بلکه در هرجا که رئیس‌جمهور، معاون رئیس‌جمهور و همسر رئیس‌جمهور مسافرت می‌کنند، به انجام وظیفه می‌پردازد. فرماندهی ارتباطات ناحیه واشنگتن[2] [به‌عنوان زیرمجموعه این سازمان]، از فعالیت‌های

---

1. Two-man Rule
2. Encryption

دفتر نظامی کاخ سفید[1] و سرویس مخفی[2] در ناحیه کلمبیا نیز پشتیبانی می‌کنند. سه فرماندهی تمام مدت سفر، از ارتباطات پشتیبانی می‌کنند. علاوه‌بر این، فرماندهی دیگری نیز در استراحتگاه رئیس‌جمهور در کمپ دیوید وجود دارد.(۲)

سازمان ارتباطات کاخ سفید، شکل جدیدی است که مدام مورد بازنگری قرار گرفته، تشکیلات آن تغییر یافته و به ابزارها و سازوکارهای جدیدی مجهز شده است. در گذشته این سازمان، گروهان هشدار کاخ سفید[3] بوده است که در سال ۱۹۴۲ تشکیل شد. تا اواخر دهه ۱۹۹۰، این سازمان در حدود هشتصد پرسنل در اختیار داشت و مدت مأموریت آنها نیز چهار سال بود؛ در سال ۱۹۹۴ تشکیلات آن به‌سرعت گسترش یافت و در زمانی که وزارت دفاع بودجه و نیروهای خود را کم می‌کرد، همچنان خواستار جذب افراد بیشتری شد. تغییرات در ساختار داخلی سازمان به‌صورت حساب شده‌ای انجام گرفت و تا سال ۱۹۹۸ در حدود ۸۰ درصد آن به اتمام رسید.

سازمان ارتباطات کاخ سفید حالا دیگر با افزایش نیروهای خود مفاهیمی مبتنی‌بر مدیریت مشارکتی را دربرمی‌گرفت. البته این مفاهیم با سبک سنتی مدیریت نظامی سازگاری نداشت، اما باید اشاره کرد که مدیریت سنتی همچنان ویژگی اساسی فرهنگ این سازمان به‌شمار می‌آید.(۳)

حال این پرسش مطرح می‌شود که سازمان هنگام مواجهه با بحران واقعی تا چه میزان از آمادگی کامل برخوردار است؟ بعد از حملات اولیه به مرکز تجارت جهانی و پنتاگون، پرسنل کاخ سفید به موازات استفاده از خطوط ارتباطاتی مطمئن، به معنای واقعی کلمه دست روی دست گذاشتند.(۴) آیا کاخ سفید تجهیزات و توانمندی‌های بسیار پیشرفته در اختیار ندارد؟ افسری که ریاست فرماندهی ارتباطات ناحیه واشنگتن را برعهده داشت در اوایل سال ۲۰۰۳ نوشت: «بازنگری در سیستم‌های رایانه‌ای میراث نارسا و کهنه این سازمان، پروژه‌ای است که در حال انجام است و آنها با موفقیت توانستند کارت‌های رمزگذاری و سازمان‌های رایانه‌ای را برای ارسال برنامه‌های مطمئن طراحی پست الکترونیک به اعضای پرسنل سازمان ارتباطات کاخ سفید و دفتر نظامی

1. Washington Area Communication Agency
2. White House Miltary Office
3. Secret Service

کاخ سفید معرفی کنند. در ۱ سپتامبر ۲۰۰۲ آنها مرکز عملیات دایر کردند: این مرکز پس از آنکه مرکز عملیات و امنیت شبکه جهانی[1] (وابسته به سازمان سیستم‌های اطلاع‌رسانی دفاعی) امکان کنترل شبانه‌روزی تأسیسات و سیستم‌های مستقر را فراهم کرد، به‌صورت الگویی برای سازمان‌های دیگر درآمد. اما چنین ظرفیتی پیش از این به مرحله اجرایی نرسیده است.(۵)

برنامه فعلی برای ارتقای سطح توانمندی‌های سازمان ارتباطات کاخ سفید که یک طرح فراگیر درزمینه دگرگونی فناوری ـ محورانه[2] به‌شمار می‌آید، «پروژه ابتکاری»[3] نام گرفت.(۶) این پروژه در اظهارات جرج دبلیو بوش نیز انعکاس یافته است. وی گفت: «من متوجه می‌شوم ـ وقتی در کراوفورد[4] ناراحت هستم مدام با دولتمان تماس دارم. ما این ظرفیت مطمئن را در خود داشته‌ایم که رابطه «کنفرانس صوتی» از راه دور برقرار سازیم؛ و این خیلی خوب است. البته بهتر از این هم می‌تواند باشد. این وضعیت می‌تواند به‌صورت هم‌زمان و واقعی‌تر باشد».(۷)

در راستای همین هدف، برآورد بودجه سازمان سیستم‌های اطلاع‌رسانی دفاعی در سال مالی ۲۰۰۵ حکایت از آن داشت که توسعه عملیاتی توانمندی کنفرانس صوتی و ارتقای آن به سطح مطمئن و بادوام به‌منظور اطلاع‌رسانی به رهبران ملی و نظامی در روند بحران‌ها مورد حمایت قرار خواهند گرفت. عنوان این طرح کنفرانس صوتی ملی و ریاست جمهوری بود. بودجه‌ای که در سال مالی ۲۰۰۵ برای این طرح پیش‌بینی شد، ۹/۹۷۵ میلیون دلار بود. هدف از تخصیص این میزان بودجه: «کمک به برنامه‌هایی از قبیل مهندسی، برنامه‌ریزی، توسعه، ایجاد یکپارچگی، نصب و آزمایش تجهیزات جدید رمزنویسی و صدانگاری است که روی زمین نصب می‌شود و برای عرضه توانمندی کنفرانس صوتی با کیفیت صدای موجود در شبکه‌های تلفن ضرورت دارد. این توانمندی در اختیار رئیس‌جمهور و سایر رهبران ملی و نظامی قرار می‌گیرد. این پروژه هزینه‌های مهندسی اساسی و حساسی را که برای طراحی یک الگوریتم جدید درزمینه پردازش

---

1. Global Network Operations and Security Center
2. Defense Information Systems Agency
3. Pioneer Project
4. Crawford

صدا مورد نیاز خواهند بود برعهده می‌گیرد و منابع مالی ساخت تجهیزات جدید رمزنویسی و صدانگاری را تأمین می‌کند. البته باید خاطرنشان کرد برای تأمین این هزینه‌ها از سودهای حاصل از طرح‌های تحقیقات، توسعه، آزمایش و مهندسی[1] در سایر بخش‌های وزارت دفاع استفاده می‌شود. این دستگاه‌های مستقر در زمین توانمندی‌های فناوری جدید از قبیل رمزنویسی و صدانگاری چندسطحی[2] و توانمندی‌های فناوری اطلاع‌رسانی از جمله میانجی‌های اترنت[3] قابل نصب روی زمین را که پروتکل اینترنت شامل حال آنها می‌شود عملیاتی خواهند ساخت. این پروژه از پیش‌شرط ستاد مشترک برای اجرای کامل طرح پیشنهادی کمیته موقت نام‌گذاری ویروس‌ها[4] با عنوان سیستم فرکانس بسیار بالای پیشرفته[5] که در راستای بهبود وضعیت اعضای کمیته در ظرف کمتر از ده سالِ مالی طراحی شده است حمایت می‌کند».(۸)

روش دیگر تفسیر این پیام، چنین است که این توانمندی‌ها در خوش‌بینانه‌ترین حالت تا سال ۲۰۰۹ به اجرا در نخواهد آمد.

۳-۸ تجربه بحران: ترور نافرجام رونالد ریگان

۳۰ مارس ۱۹۸۱، رونالد ریگان رئیس‌جمهور آمریکا در واشنگتن هدف گلوله قرار گرفت و روانه بیمارستان شد. مقامات ارشد آمریکا در اتاق وضعیت[6] کاخ سفید گرد هم آمدند. در این اتاق ریچارد ای.آلن[7] مشاور امنیت ملی با اجازه حاضران در آن جلسه، فرایند تبادل نظرها میان شرکت‌کنندگان را ضبط کرد(۹) آلن قسمتی از آن نسخه ضبط شده را منتشر ساخته است. این نسخه بینش بسیاری را در مورد مسائل مربوط به ارتباطات، آشفتگی فکری و خطاهایی که در آن روز، فضا را به هم ریخته بود، نشان می‌دهد. کنترل تسلیحات هسته‌ای آمریکا از نگرانی‌های آشکار بعضی از شرکت‌کنندگان در آن نشست بود.

---

1. Research, Development, Test & Engineering (RDT&E)
2. Multi-stream
۳. Ethernet interfaces: مجموعه‌ای از فناوری‌های شبکه‌سازی رایانه‌ای که برای شبکه‌های محلی به‌کار برده می‌شود.
4. Provisional Committee on Nomenclature of Virus (PCNV)
5. Advanced Extremely High Frequency (AEHF)
6. Situation Room
7. Richard A Allen

یافته‌های آن روز زنگ بیدارباشی را برای کسانی که فرماندهی و کنترل تسلیحات هسته‌ای را برعهده می‌گیرند به صدا درآورده است، اما اگر تصور کنیم که ضعف‌هایی از نوع دیگر و به همان اندازه مختل‌ساز، هنوز هم سیستم امروز را می‌آزارند، به بیراهه نرفته‌ایم. چند نکته کلیدی از گزارش آلن به‌دست می‌آید:

۱. جرج بوش پدر، معاون وقت رئیس‌جمهور آمریکا که با هواپیما از ایالت تگزاس باز می‌گشت به‌اصطلاح «توپی» حامل سلاح هسته‌ای رمزدار با خود به همراه داشت. در آن زمان وی هیچ پیوند ارتباطاتی مطمئنی با کاخ سفید نداشت. اما به‌نظر می‌رسید الکساندر هایگ[1] وزیر خارجه دولت ریگان تصور کرده است که چون ریگان روی تخت عمل جراحی است، بوش این رمزها را فرماندهی می‌کند، وی گفته بود: توپ نزد معاون رئیس‌جمهور است ـ پس اوضاع عالی است.

۲. بااین‌حال، ممکن است آنها گمان کرده باشند که فرماندهی هسته‌ای نمی‌تواند در کاخ سفید مستقر باشد. آلن و هایگ پی بردند که مسئله مربوط به اتاق وضعیت نیست. آلن داوطلب شد و گفت: ما باید از شر این بمب در اینجا خلاص شویم. ما یک سلاح دومی را نیز در اینجا داریم. یک بمب نیز در دفتر مشاور نظامی وجود دارد. توپ در آن اتاق است.

۳. فرماندهی هوایی استراتژیک به حالت آماده‌باش درآمد اما بااین‌حال، سطح آمادگی دفاعی[2] بالا نرفت. هایگ و آلن توجه خود را به‌احتمال صدور فرمان استفاده از تسلیحات هسته‌ای معطوف ساختند: «هایگ: آیا ما در اینجا یک توپ داریم؟ آیا داریم؟ آلن: درست اینجاست».

۴. ادوین میسه،[3] مشاور حقوقی کاخ سفید از بیمارستان تماس گرفت و به غلط تصریح کرد که مقام فرماندهی ملی برعهده واینبرگر[4] است. واینبرگر معتقد بود که غیبت بوش در کاخ سفید، بوش را از زنجیره مقام فرماندهی ملی دور می‌سازد؛ واینبرگر: «... تا زمانی که معاون رئیس‌جمهور واقعاً به اینجا وارد شود، مقام فرماندهی در دست

---

1. Alenander Haig
2. DEFCON (Defense Readiness Condition)
3. Edwin Meese
4. Weinberger

من است». اما هایگ نظر دیگری داشت: «هایگ: شما بهتر است قانون اساسی را بخوانید». واینبرگر: چه؟ هایگ (با خنده): «شما هم بهتر است قانون اساسی را بخوانید، ما هر زمان‌که بخواهیم می‌توانیم رئیس‌جمهور شویم». [البته، قانون اساسی هیچ چیزی در مورد مقام فرماندهی ملی نمی‌گوید].

در این گیرودار، هیچ بحران هسته‌ای رخ نداد. اما، ما می‌آموزیم که سه توپ وجود داشت (یک توپ، همراه ریگان، یک توپ نزدیک بوش، یک توپ هم در یکی از اتاق‌های کاخ سفید در کنار مشاور نظامی). علاوه‌بر این، آشکار گردید که هیچ توپی همراه وزیر دفاع نبود. به‌نظر می‌رسد آلن و هایگ تصور کرده‌اند توپ واقع در آن اتاق رمزهایی را در خود داشتند.[1]

۸-۴ تجربه بحران: حمله یازده سپتامبر

وقتی حملات یازده سپتامبر ۲۰۰۱ به مرکز تجارت جهانی و پنتاگون اتفاق افتاد، رئیس‌جمهور و وزیر خارجه هر دو در خارج از واشنگتن بودند. کالین پاول وزیر خارجه آمریکا در لیما پایتخت پرو بود. وی برای شرکت در اجلاس سازمان کشورهای آمریکایی به این کشور سفر کرده بود؛ جرج دبلیو بوش در شهر ساراستا[2] واقع در ایالت فلوریدا به‌سر می‌برد. رئیس‌جمهور با خبر شد که هواپیمایی به مرکز تجارت جهانی برخورد کرده است. بوش در ساعت ۸:۵۵ بعدازظهر، یعنی اندکی قبل از آنکه وارد یکی از کلاس‌های مدرسه ابتدایی شود، با کاندولیزا رایس (مشاور وقت امنیت ملی) ــ که در کاخ سفید بود ـ صحبت کرد. در ساعت ۹:۰۳ بعدازظهر یک هواپیمای دیگر نیز به برج دوم برخورد کرد. واقعه دوم نشان داد که این برخوردها عمدی بوده‌اند.

کمیسیون یازده سپتامبر، گزارشی علنی را منتشر کرده است. بنابراین ما منبعی بسیار مفصل درباره واکنش‌های اخیر کاخ سفید و وزارت دفاع در برابر بحران در اختیار داریم.(۱۰)

اداره هواپیمایی فدرال،[3] کاخ سفید و وزارت دفاع، هریک پیش از ساعت ۹:۳۰ ارتباطات از راه دور میان خود را راه‌اندازی کردند. ازآنجاکه هیچ‌یک از این ارتباطات از

---

1. National Command Authority
2. Sarasota
3. Federal Aviation Administration

راه دور ـ حداقل قبل از ساعت ۱۰:۰۰ ـ مقام‌های مرتبط در وزارت دفاع و اداره هواپیمایی فدرال را پوشش ندادند، هیچ‌یک از این سه نهاد موفق نشدند واکنش‌های ارتش و اداره هواپیمایی فدرال در برابر این هواپیماربایی‌ها را به‌نحو معناداری باهم هماهنگ سازند.(۱۱)

حداقل یک ساعت از زمان وقوع حملات گذشته بود، اما هیچ‌کدام از اطلاعات موجود در ویدئو کنفرانس کاخ سفید به مرکز فرماندهی نظامی ملی[1] نرسیده بود. ازاین‌گذشته، کمیسیون نوشت: «ما نمی‌دانیم چه کسی در درون وزارت دفاع در این فعالیت‌ها مشارکت داشت، اما می‌دانیم که در یک ساعت نخست، هیچ‌یک از پرسنل در مدیریت این بحران مشارکت نداشت». یک شاهد به کمیسیون گفت که: «آن وضعیت تقریباً شبیه آن چیزی بود که فرایندهای موازی تصمیم‌گیری عمل می‌کردند، درواقع یک کنفرانس صوتی بود که مرکز فرماندهی نظامی ملی، آن را طراحی و سازمان‌دهی می‌کرد. علاوه‌بر این، یک ویدئو کنفرانس از راه دور نیز در کاخ سفید راه‌اندازی شده بود ... به‌نظر من، این افراد برای کسب جایگاه‌های فرماندهی کنترل و تصمیم‌گیری باهم رقابت می‌کردند».(۱۲)

مرکز فرماندهی نظامی ملی در ساعت ۹:۳۷ بعدازظهر پیامی را با کنفرانس صوتی مبنی‌بر وجود یک تهدید هوایی ارسال کرد. این ارسال پیام هشت ساعت طول کشید تا به رئیس‌جمهور، معاون رئیس‌جمهور و وزیر دفاع رسید. علاوه‌بر این، در ساعت ۹:۳۷ بعدازظهر، معاون رئیس‌جمهور که در تونلی در زیر کاخ سفید به‌سر می‌برد، با استفاده از یک ارتباط تلفنی مطمئن، درخواست کرد که با رئیس‌جمهور صحبت کند، اما برقراری این تماس نیز طول کشید. در آن زمان جرج دبلیو بوش در راه فرودگاه بود. آنها حدود ساعت ۹:۴۵ بعدازظهر باهم صحبت کردند.(۱۳) دونالد رامسفلد، وزیر دفاع در زمانی که هواپیمای سوم به پنتاگون برخورد کرد در یک جلسه توجیهی در وزارتخانه حضور داشت و از این جلسه به منطقه حادثه‌دیده رفت. تنها بعد از آن موقع، یعنی اندکی قبل از ساعت ۱۰:۳۰ بعدازظهر، وی به کنفرانس از راه دور[2] پیوست.

---

1. National Military Command Centre (NMCC)
2. Teleconference

در لیما، کالین پاول، وزیر امور خارجه، هنگام اطلاع یافتن از وقوع این حملات، دستور داد هواپیمایی را آماده کنند که با پروازی هفت‌ساعته وی را به واشنگتن رسانید و البته سیستم ارتباطات تلفنی این هواپیما نیز ضعیف بود.(۱۴) یکی از اعضای قانونی شورای امنیت ملی آمریکا اظهار داشت: «آن روز، روزی طولانی برای من بود، من سوار هواپیما شدم و تمام مسیر بازگشت از پرو را با هواپیما طی کردم. ازاین‌رو تا وقتی‌که وارد واشنگتن نشده بودم و با رئیس‌جمهور در کاخ سفید و سایر مشاوران امنیت ملی ملاقات نکرده بودم، نتوانستم با هیچ‌کس در واشنگتن ارتباط برقرار کنم».(۱۵)

قضیه یازده سپتامبر تأیید کرد که توانمندی‌های کنفرانس از راه دور وجود دارد و درصورتی‌که تجهیزات دقیق و کاملی مهیا باشد، مدیران دولتی می‌توانند به‌آسانی باهم صحبت کنند. اما بااین‌حال، مدیران در بیشتر مواقع از این توانمندی‌ها بهره‌برداری نکردند. ازاین‌گذشته، قضیه یازده سپتامبر، آشکار ساخت که در فاصله یک ساعت بعد از حمله دوم، کاخ سفید و وزارت دفاع اصلاً باهم در ارتباط نبودند و از ساعت ۹:۴۶ بعدازظهر، کارکنان پنتاگون «همچنان تلاش می‌کردند محل استقرار وزیر دفاع (رامسفلد) را ـ که یکی از اعضای قانونی شورای امنیت ملی است، پیدا کنند».(۱۶)

۵-۸ سیستم فرماندهی و کنترل جهان‌گستر (آن‌چنان‌که وزارت دفاع تعریف کرده است)

عملیات‌های پنتاگون، به‌شدت به مجموعه‌ای از فناوری‌های مخابراتی رایانه ـ محور اتکا دارند که امروزه در اصطلاح، «فناوری اطلاعات» نامیده می‌شود. در اواخر دهه ۱۹۹۰، وزارت دفاع آمریکا تغییرات در توانمندی‌ها و دکترین نظامی آمریکا را تحت عنوان «انقلاب در امور نظامی» معرفی کرد. انقلاب در امور نظامی بر فناوری اطلاعات و عملیات‌های مشترک (یعنی عملیات‌هایی که بیش از یک نیروی ارتش، مثلاً نیروی هوایی و نیروی زمینی به‌صورت مشترک در آنها حضور دارند) تأکید می‌کند.

ازاین‌رو، یک شبکه اطلاع‌رسانی نیز به‌منظور پشتیبانی از این عملیات‌ها راه‌اندازی شده است: سیستم فرماندهی و کنترل جهان‌گستر.[1] در اصل، این سیستم، سخت‌افزار،

1. Global Command and Control System (GCCS)

نرم‌افزار و رویه[1] را باهم تلفیق می‌کند. سخت‌افزار، ابزارهایی از جمله حسگرها، میزهای رایانه، سرورها، فیبر، دریافت‌کننده‌ها و فرستنده‌های ماهواره‌ای، حافظه رایانه و کار با رایانه را دربرمی‌گیرد. سیستم فرماندهی و کنترل جهان‌گستر، این توانمندی‌های جدید را جهت گردآوری و عرضه مفید اطلاعاتی که تاکنون غیرقابل دسترسی بوده‌اند سامان‌دهی می‌کند و در نتیجه، این امکان را به ارتش می‌دهد که اقدامات مناسب را شناسایی کند و نحوه اجرای آن اقدامات را باهم هماهنگ سازد و نظم بخشد. در حال حاضر، رایانه‌ها در همه جا وجود دارند و استفاده از آنها فراگیر شده است. کلمه اختصاری C3I (فرماندهی، کنترل، ارتباطات و اطلاعات)[2] حالا دیگر از دور خارج شده است: ستاد مشترک ارتش با تهوّری هرچه تمام‌تر می‌کوشد یکی از اهداف مهم وزارت دفاع را تحقق بخشد؛ وزارت دفاع قصد دارد سیستم‌های فرماندهی و کنترل، ارتباطات، رایانه‌ها، اطلاعات، نظارت و شناسایی را به‌گونه‌ای یکپارچه سازد که تا قبل از سال ۲۰۰۸، با به‌کارگیری یکی از این سیستم‌ها بتوان از سیستم یا سیستم‌های دیگر نیز بهره‌برداری کرد.(۱۷)

دولت ایالات متحده سیستم فرماندهی و کنترل جهان‌گستر را به سبک و سیاق اعلانیه‌های پنتاگون این‌گونه تبلیغ می‌کند:(۱۸) «سیستم فرماندهی و کنترل جهان‌گستر، بزرگ‌ترین و اولین سیستمی است که ایالات متحده درزمینه فرماندهی و کنترل نیروهای ائتلاف و مشترک راه‌اندازی کرده است. این سیستم حاوی برنامه‌های رایانه‌ای درزمینه ارزیابی، برنامه‌ریزی و آمادگی نیروهاست که فرماندهان نظامی در میدان نبرد برای طراحی و اجرای مؤثر عملیات‌های نظامی بدان‌ها نیاز دارند. تصویر عملیاتی مشترک[3] آن، داده‌های حسگرها و منابع اطلاعاتی متعدد را پردازش و تلفیق می‌کند و از این طریق، اطلاعات مربوط به وضعیت میدان نبرد را که برای انجام عمل و عکس‌العمل قاطعانه ضروری‌اند، در اختیار جنگنده‌ها قرار می‌دهد. علاوه‌بر این، تصویر عملیاتی مشترک مجموعه گسترده‌ای از خودکارسازی یکپارچهٔ سیستم‌های موجود در ادارات، ارسال پیام و برنامه‌های کاربردی مشارکتی را فراهم سازد».[4]

---

1. Practice
2. C3I (Command, Control, Communications, and Intelligence)
3. Common Operational Picture
4. Collaborative Applications

نیروهای ائتلاف نیروهایی از کشورهای خارجی‌اند که با ایالات متحده آمریکا همکاری می‌کنند، اما نحوه مساعدت آمریکا درزمینه دسترسی ارتش‌های غیرآمریکایی به سیستم فرماندهی و کنترل جهان‌گستر همچنان موضوعی مطرح باقی مانده است.

برنامه‌ریزان نظامی در دهه ۱۹۹۰ تصمیم گرفتند که توجه خود را به‌شدت بر محصولات تجاری شرکای خود که دارای کیفیت بیشتری نسبت به محصولات داخلی این کشورها بوده‌اند و دسترسی به آنها زمان کمتری نیاز دارد، متمرکز سازند. «سیستم فرماندهی و کنترل جهان‌گستر مبتنی‌بر شالوده‌ای است که محیط عملیاتی مشترک[1] پی‌ریزی می‌کند. این سیستم آخرین و جدیدترین نوآوری‌ها در حوزه فناوری سخت‌افزاری، نرم‌افزاری و ارتباطاتی رایانه‌های تجاری را در خود جای داده است. سیستم فرماندهی و کنترل جهان‌گستر به واسطه اتخاذ «استراتژی کسب تکاملی و نوآورانه اطلاعات» قادر است برنامه‌های رایانه‌ای کاربردی جدید را در زمانی که تولید تجهیزات، روند تکاملی خود را می‌پیماید و فناوری نیز پیشرفت می‌کند، به‌سرعت و با هزینه‌ای کمتر و بازدهی بیشتر وارد میدان نبرد سازد. سیستم فرماندهی و کنترل جهان‌گستر در بیش از ۶۲۵ پایگاه نظامی در سراسر جهان به اجرا درآمد. همه این پایگاه‌ها با اینترنت اختصاصی و طبقه‌بندی شده وزارت دفاع در قالب شبکه‌ای جهان‌شمول از این سیستم بهره‌برداری کردند. سیستم مذکور با این هدف طراحی و اجرا شد که زمینه برتری اطلاعاتی جنگنده‌های کشور ما بر سایر کشورها را فراهم نماید: برتری‌ای که برای حفظ سیطره خود در حال حاضر و در تمام قرن بیست‌ویکم بدان نیاز داریم».

به‌عبارت‌دیگر، سیستم فرماندهی و کنترل جهان‌گستر، یک اینترنت اختصاصی است. این اینترنت خصوصی، مانند شبکه‌های اینترنتی شرکت‌هایی است که گستره فعالیت‌ها آنها بسیار پراکنده است. ورود به این سیستم برای عموم مردم آزاد و باز نیست، چرا که به‌عنوان سیستمی مطمئن[2] و درواقع، سیستمی که مخصوص ارتباطات سری است، طراحی شده است.

مسئله فراروی سازندگان سیستم فرماندهی و کنترل جهان‌گستر این بود که آنها

---

1. Common Operating Environment (COE)
2. Secure

چگونه می‌توانند انبوهی از سیستم‌های رایانه‌ای ویژه‌ای را که خدمات ــ محورند، به‌کار گیرند و امکان دسترسی و استفاده همگانی از آنها را فراهم آورند. هریک از این سیستم‌ها باید بتوانند با یکدیگر تعامل داشته باشند، اما درعین‌حال باید قادر باشند تدابیر امنیتی اولیه خود را نیز تداوم بخشند و اطمینان دهند که دروازه‌های بین اجزای آنها ایمن باشند. محیط عملیاتی مشترک نقطه اتصال میان اجزا را مشخص می‌سازد.(۱۹) برای هریک از این اجزای جداگانه، «شبکه‌سازی[1] نرم‌افزار» رایت شده است. این شبکه از یک‌سو، خدماتی را که پیش‌تر موجود بوده‌اند دربرمی‌گیرد و ازسوی‌دیگر، داده‌ها را به محیط عملیاتی مشترک می‌فرستد و از این محیط به فضاهای دیگر انتقال می‌دهد. وانگهی، همان‌گونه که در ذیل تشریح خواهیم کرد، تعمیرات در سیستم‌های اجزا و خصایص سیستم فرماندهی و کنترل جهان‌گستر در حال وقوع بوده است. سخت‌افزار جدید رواج می‌یابد و نرم‌افزار قدیمی کنار می‌رود؛ ازاین‌رو آهنگ و حجم داده‌ها نیز افزایش می‌یابد. بنابراین دومین مسئله‌ای که فراروی طراحان سیستم فرماندهی و کنترل جهان‌گستر می‌باشد، این است که چگونه سیستم تولید پراطمینان[2] را در سطحی بالا و قابل دسترسی نگه دارند و درعین‌حال، «بهسازی سیستم‌ها» را با اجزا انطباق دهند و آن را درون نرم‌افزار یکپارچهٔ سیستم فرماندهی و کنترل جهان‌گستر وارد سازند.

سایت‌های سیستم فرماندهی و کنترل جهان‌گستر می‌باید قادر باشند در جهان واقعی باهم ارتباط برقرار کنند. چگونه می‌توان این کار را انجام داد و درعین‌حال اطمینان یافت که دشمن نمی‌تواند ارتباطات را استراق سمع کند، به آنها دستبرد بزند، یا در آنها اختلال ایجاد کند؟ پاسخ، ایجاد یک شبکه اختصاصی از «توانمندی‌های جاافتاده» می‌باشد که هریک از آنها از طریق آن، اقدامات احتیاطی و تدابیر امنیتی بیشتری را اجرا نماید. براساس گزارش‌های سازمان سیستم اطلاعات دفاعی،[3] این سیستم گسترده:

۱. یک شبکه سیستم اطلاعاتی دفاعی[4] به‌شمار می‌آید،

---

1. networking
2. High-reliability
3. Secret Internet Protocol Router Network (SIPNet)
4. Defence Information System Network (DISN)

۲. زیرمجموعه سازمان سیستم اطلاعات دفاعی (که سیستم فرماندهی و کنترل جهان‌گستر در درون آن عمل می‌کند)، شبکه سری مسیریاب پروتکل اینترنت[1] و یک شبکه پروتکل اینترنت به‌شمار می‌آید،

۳. زیرمجموعه شبکه سری مسیریاب پروتکل اینترنت است که سیستم رمزنویسی اضافی با عنوان مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر را در خود دارد.

۶-۸ مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر:[2] ایجاد آمادگی سری برای عملیات‌های هسته‌ای

پوشیده‌ترین و درعین‌حال ایمن‌ترین «شبکه خصوصی مجازی» با این هدف سفارش داده شد که برنامه‌ریزی، فرماندهی و کنترل تسلیحات هسته‌ای در چارچوب سیستم فرماندهی و کنترل جهان‌گستر قرار گیرد.

پیوند میان همه پایگاه‌های سیستم فرماندهی و کنترل جهان‌گستر با شبکه سیستم اطلاعات دفاعی فراهم می‌شود. ارتباط با سیستم فرماندهی و کنترل جهان‌گستر که در محیط امنیتی- فوق سری عمل می‌کند، با شبکه سری مسیریاب پروتکل اینترنت که زیرمجموعه شبکه سیستم اطلاعات دفاعی است، برقرار می‌شود. مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر نیز با شبکه سری مسیریاب پروتکل اینترنت ارتباط برقرار می‌کند، اما استفاده از سیستم رمزنویسی شبکه‌ای[3] در میان این گروه‌ها شبکه خصوصی مجازی را ایجاد می‌کند که به اطلاعات فوق سری اجازه می‌دهد شبکه سری را درنوردد.(۲۰)

در اوایل سال ۱۹۹۸، پنتاگون اعلام کرد که تا قبل از اواسط سال ۱۹۹۸، عملیات‌های هسته‌ای، طرح عملیاتی یکپارچه[4] و گزینه‌های مقام فرماندهی ملی برای اجرای حمله هسته‌ای را در قالب مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر باهم تلفیق خواهد کرد و یکپارچه خواهد ساخت: «فرماندهی و کنترل: سیستم‌های

1. Defence Information System Agency (DISA)
2. Top Secret (TS) Version of GCCS (GCCS-T)
3. Network Encryption System (NES)
4. Single Integrated Operational Plan (SIOP)

فرماندهی و کنترل، ابزارهایی را برای اجرای مؤثر عملیات‌های هسته‌ای متعارف و ویژه فراهم می‌آورند. مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر، زیرساخت‌های فوق سری را برای سیستم‌های فرماندهی و کنترل در سراسر چرخه استقرار نیروها[1] فراهم می‌سازد. درصورتی‌که ساخت مدل ۲/۲ فوق سری سیستم فرماندهی و کنترل جهان‌گستر، در اواسط سال ۱۹۹۸ به اتمام برسد، توانمندی هسته‌ای طرح عملیاتی کردن یکپارچه و توانمندی فوق سری تصویر عملیاتی مشترک (از جمله توانمندی جاسوسی ویژه) را نیز در خود خواهد داشت. پیشرفت‌ها درزمینه «سیستم فرماندهی و کنترل جهان‌گستر» و «فرمول فوق سری سیستم فرماندهی و کنترل جهان‌گستر» در سال ۱۹۹۹، اطلاعات بخش‌بندی شده حساس را دربرخواهند گرفت. پایگاه‌های کاربران را افزایش خواهند داد و عملکرد و اعتمادپذیری را نیز بهبود خواهند بخشید ...».[۲۱]

آیا این موضوع که «مدل ۲/۲ توانمندی‌های هسته‌ای طرح عملیاتی یکپارچه واحد را نیز در خود خواهد داشت»، یک شیوه بیان هنری بود، آیا منظور از این توانمندی‌ها در سال ۱۹۹۸، تنها بعضی توانمندی‌ها، از جمله دسترسی به نوسازترین طرح عملیاتی یکپارچه و نه ظرفیت بالفعل طراحی و اجرای عملیات بوده است؟

۸-۷ دگرگونی‌های نوظهور در عرصه سیستم‌های فرماندهی و کنترل

به‌دلیل پایان جنگ سرد و از بین رفتن نگرانی‌های آمریکا در مورد نیروهای هسته‌ای شوروی، ارتش ایالات متحده تا اواسط دهه ۱۹۹۰، فعالیت‌های خود را بر توسعه توانمندی‌های «کنترل، فرماندهی، ارتباطات و اطلاعات» که در حوزه تسلیحات متعارف کاربرد داشتند متمرکز ساخته بود. جنگ (از نوع نامتعارف)، دیگر رخ نمی‌داد چرا که در گذشته تجربه شده بود. از هم‌اکنون، جنگ از تحولات در عرصه فناوری و به‌ویژه فناوری اطلاعات بهره خواهد برد. وزارت دفاع آمریکا، در یک سری از اسناد، مسیرهایی را که فناوری اطلاعات، توانمندی‌های ایالات متحده را در راستای آنها پیش خواهد برد، برشمرد.[۲۲] برای مثال، گزارش سالیانه ایالات متحده در حوزه امور دفاعی در سال

1. Force Deployment Cycle

۱۹۹۸ هیچ شک و شبهه‌ای درزمینه تأکیدی که بر فناوری اطلاعات نهاده می‌شود، باقی نگذاشت.(۲۳)

از دهه ۱۹۷۰ تا ۳۰ آگوست سال ۱۹۹۶ سیستم جهان‌گستر فرماندهی و کنترل نظامی[1] توانمندی‌های ارتباطاتی ارتش آمریکا را به‌صورت شبکه‌ای درآورده بود. این سیستم لاجرم در وهله اول به تلفن، تلگراف و رادیو و با گذشت زمان، به ارتباطات ماهواره‌ای و امواج متکی بود.

گذر از سیستم جهان‌گستر فرماندهی و کنترل نظامی به سیستم فرماندهی و کنترل جهان‌گستر بی‌دردسر و سهل و آسان نبود. در گزارش سال ۱۹۹۷، اداره آزمایش و سنجش[2] وزارت دفاع نظرات خود را درباره نحوه انطباق سیستم جدید مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر با شرایط عملیات‌های هسته‌ای بیان کرد و به این نتیجه رسید که: «ستاد مشترک بعد از انجام آزمایش‌های امنیتی، به‌طور موقت این اختیار را به مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر بدهد که در سطح فوق سری فعالیت کند. سازمان تسلیحات ویژه دفاعی[3] آزمایش‌های موازی درزمینه توانمندی‌های تخصصی این سیستم‌ها را انجام داد ولی هیچ مشکل چشمگیری در آنها نیافت. اما این آزمایش‌ها ناهنجاری‌هایی نیز در حوزه توانمندی‌هایی که سازمان تسلیحات ویژه دفاعی در خود جای داده است، آشکار ساخت. این نارسایی‌ها به لحاظ تأثیر عملیاتی که دارند به‌ترتیب در ذیل می‌آیند: مشکلات و تأخیرهای متناوب درزمینه ورود به سیستم رایانه‌ها، پیامک‌های اشتباهی که از «پایگاه‌های اطلاعاتی» در روند آزمایش فشار گهگاه ارسال می‌شوند، ناتوانی در ارسال پیامک‌های اصلی (برنامه کاربردی امنیتی و تجاری) از دو سایت متفاوت و بروز اشتباهات جدی درباره فرمت کردن دستور پرینت در دو مورد از آزمایش‌هایی که از دو سایت انجام گرفته است. در آزمایش بعدی، مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر ثابت کرد می‌تواند از حجم کار مورد نظر خودش که طراحی کرده است، بهره‌برداری کند؛ البته همه مشکلات سابق به‌استثنای آن شرط اصلی که ستاد مشترک حذف کرد، رفع شدند».

---

1. World Wide Military Command and Control System (WWMCCS)
2. Office of Test and Evaluation
3. Defense Special Weapons Agency (DSWA)

۱-۷-۸ درس‌هایی که باید آموخت

«به‌طورکلی، فرایندهای نصب، شکل‌بندی و تنظیمات اولیه و مرحله گذار، هم در سیستم فرماندهی و کنترل جهان‌گستر و هم در مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر عملاً بسیار مشکل‌آفرین بوده‌اند. این فرایندها چه‌بسا از جمله مشکلاتی ذاتی در همه ساختارهای تجاری می‌باشند که محصولات بسیاری از فروشندگان و منابع دولتی را در یکجا در کنار هم می‌آورند. شکل‌بندی[1] نامناسب به عاملی چالش‌زا و یکی از علل اصلی آسیب‌پذیری در جنگ اطلاعاتی تبدیل می‌شود. بعد از انجام آزمایش، هیچ ابزار بسیار مؤثر و هیچ سیاست حمایتی برای نظارت و اجرای کنترل شکل‌بندی وجود ندارد».(۲۴)

ازآنجاکه سیستم فرماندهی و کنترل جهان‌گستر و اجزای آن مدام در حال توسعه‌اند، هیچ نظارت مشخصی درباره «کاربردپذیری متقابل»[2] (ظرفیت اجزای سیستم در انجام اموری به عنوان بخشی از یک طرح کلی) وجود ندارد.(۲۵)

از سال ۱۹۹۶، سیستم فرماندهی و کنترل جهان‌گستر چهار مدل[3] را تجربه کرده است:

در سال ۲۰۰۴ مدل x۳۰ رایج بود و در سال ۲۰۰۶، مدل x۴۰ پیش‌بینی شده است. در این راستا، قرار است به دنبال راه‌اندازی سیستم فرماندهی و کنترل جهان‌گستر، سیستم جدیدی به نام فرماندهی و کنترل مشترک[4] وارد عرصه شود که بخش‌های اولیه آن نیز در سال ۲۰۰۴ آماده بوده است.(۲۶) این نام‌های پرشمار آشنا نشان می‌دهد که تغییرات عمده‌ای در این‌گونه ساختارها رخ داده است، سیستم‌هایی که پیش‌تر وجود داشته به ناگزیر پذیرفته شوند و تغییرات نیز می‌باید براساس مقتضیات موجود طراحی و اجرا شوند. مدیر ارشد بخش فناوری‌های سازمان سیستم اطلاعات دفاعی در آوریل ۲۰۰۴ گفت که این سازمان از یازده سپتامبر ۲۰۰۱ تاکنون ۲۷ مدل به‌روز شدهٔ سیستم فرماندهی و کنترل جهان‌گستر را عرضه کرده است.(۲۷)

مقامات دولتی تعهد داده‌اند سیستم جدیدی را راه‌اندازی کنند اما بی‌پرده‌تر و صریح‌تر می‌توانند در مورد نارسایی‌ها و کمبودهای سیستم فرماندهی و کنترل

---

1. Configuration
2. Interoperability
3. Version
4. Joint Command and Control (JC2)

جهان‌گستر و نیز طرح‌های آینده صحبت کنند. هرگونه تغییر در این سیستم مستلزم «تنظیم و آزمایش مجدد کل سیستم» است. فرماندهی و کنترل مشترک انتقال داده‌ها، سرویس‌های سیستم‌های عامل و شبکه‌های تحت وب و برنامه‌های کاربردی و داده‌ها را از یکدیگر جدا خواهد ساخت و زمینه‌های به روزسازی مستقل سیستم‌ها را فراهم خواهد کرد.(۲۸) ازاین‌گذشته، وزارت دفاع خواهان تدارک پهنای باند به‌مراتب بیشتر و ارتباط گسترده‌تر میان بخش‌های ارتش می‌باشد. شبکه‌ای که طراحی شده است، شبکه اطلاع‌رسانی جهانی[1] نامیده می‌شود که مبنای جنگ «شبکه‌محور» به‌شمار می‌آید و پهنای باند وسیعی را در اختیار دارد. مدیر عامل شرکت لاکهید مارتین[2] طراحی یک «اینترنت بسیار مطمئن» را پیش‌بینی می‌کند که در آن، فعالیت‌های جاسوسی و نظامی باهم تلفیق می‌شوند.(۲۹)

۸-۸ تجربه جنگی: جنگ عراق (۲۰۰۳-۲۰۰۰)

آیا جلوه‌های فناوری اطلاعات و سیستم فرماندهی و کنترل جهان‌گستر در جنگ عراق، نقش چشمگیر ـ یا حتی مهمی ـ در موفقیت آمریکا و انگلیس در میدان نبرد ایفا کردند؟ به‌نظر می‌رسد که مقامات این کشورها و بعضی از صاحب‌نظران نیز چنین فکر می‌کنند. در ۹ آوریل ۲۰۰۳ ریچارد دیک چنی معاون رئیس‌جمهور آمریکا به انجمن سردبیران خبری آمریکا گفت: «من در زمان جنگ خلیج فارس در سال ۱۹۹۱ وزیر دفاع بودم و در آن زمان در برنامه‌ریزی و اجرای عملیات جنگی نقش داشته‌ام، اما با قاطعیت می‌توانم بگویم که این جنگ (جنگ ۲۰۰۳) توانمندی‌های بسیار پیشرفته‌ای را به نمایش گذاشته است و این توانمندی‌ها به‌مراتب برتر از توانمندی‌هایی است که ما در دوازده سال پیش به نمایش گذاشتیم. در عملیات طوفان صحرا تنها ۲۰ درصد جنگنده‌های هوا به زمین ما می‌توانستند بمب‌های لیزری را به‌سمت هدف هدایت کنند. اما امروز، همه جنگنده‌های هوا به زمین ما آن توانمندی را دارند. در عملیات طوفان صحرا، معمولاً بیش از دو روز طول می‌کشید تا برنامه‌ریزان حمله به اهداف، عکسی از

---

1. OS and Web Services
2. Lockheed Martin Corporation

«هدف» مأموریت حمله به هدف را برنامه‌ریزی کنند و برنامه هدف‌گیری را در اختیار گروه نظامی بمب‌افکن‌ها قرار دهند. اما در حال حاضر، ما تصویربرداری تقریباًهم‌زمان از اهداف داریم و عکس‌ها و مختصات جغرافیایی با پست الکترونیک به هواپیمایی که در همان لحظه در حال پرواز در منطقه جنگی است، ارسال می‌شود. در عملیات طوفان صحرا، فرماندهان تیپ، لشکر و گردان ناگزیر بودند برای رهگیری تحرکات نیروهای‌مان به نقشه‌ها، قلم‌های روغنی و گزارش‌های رادیویی اتکا کنند. اما امروز فرماندهان ما می‌توانند به‌طور هم‌زمان تصاویر نیروهایمان را روی صفحه‌های نمایشگر رایانه‌هایشان نمایش دهند. در عملیات طوفان صحرا، ما هنوز B-2 نداشتیم. اما این هواپیما در حال حاضر نقش تعیین‌کننده‌ای در عملیات‌های ما دارد. یک هواپیمای B-2 در یک سورتی پرواز برای بمباران اهداف، با استفاده از سلاح‌های ۲۰۰۰ پوندی دقیق و هدایت شونده‌ای که از اطلاعات ماهواره‌ای بهره می‌گیرد، می‌تواند ۱۶ هدف مجزا را نشانه‌گیری کند. آن فناوری برتر که ما اکنون در اختیار داریم، شاید آشکارترین تفاوت میان منازعه فعلی و جنگ خلیج فارس در سال ۱۹۹۱ است».[۳۰]

از سخنان دیک‌چنی معاون رئیس‌جمهور آمریکا که بگذریم، حالا دیگر، جنگ عراق به جنگی علیه چریک‌های شهری مبدل شده است؛ چریک‌هایی که مسلح به سلاح‌های سنگین‌اند و از قرار معلوم، انعطاف‌پذیر هم می‌باشند. توانمندی‌های جدید ایالات متحده در حوزه‌های نظارت و ارتباطات در این جنگ نیز به‌کار گرفته شده‌اند. بااین‌حال، اگر بخواهیم ببینیم که آیا این توانمندی‌ها می‌توانند برتری قاطعی را به‌وجود آورند، همچنان باید به انتظار بنشینیم. آنچه ما از گزارش‌های بی‌پایه و اساس جنگ‌های عراق و افغانستان می‌دانیم، این است که ارتش آمریکا هنوز هم اشتباهاتی را مرتکب می‌شود و در هیچ‌یک از این دو کشور، شرایط را برای تأمین امنیت خودش برقرار نساخته است. در همان اوایل جنگ عراق، یکی از یگان‌های نیروهای آمریکایی که با کردها در شمال عراق دست به عملیات می‌زد مورد حملهٔ هواپیمای آمریکایی قرار گرفت. علت این واقعه از دو احتمال خارج نیست: یا افسر آمریکایی به همراه آن عده‌ای که در بخش پشتیبانی هوایی باهم در تماس بودند مرتکب اشتباه شدند و به‌جای مختصات جغرافیایی هدف موردنظر، مختصات خودشان را به خلبان هواپیما دادند، یا اینکه خود خلبان هواپیما

اشتباه کرده است.(۳۱) در افغانستان، خلبان آمریکایی به گروهی از سربازانی که در سطح زمین حرکت می‌کردند حمله کرد؛ بعدها مشخص شد که این سربازان، نیروهای کانادایی بودند که به انجام رزمایش‌های آموزشی می‌پرداختند؛ در این هدف‌گیری اشتباه، چهار تن از این نیروها کشته و هشت تن دیگر زخمی شدند.(۳۲) در جریان نبردهای فلوجه در نوامبر ۲۰۰۴، یک گروه از تفنگداران دریایی، که در شب تاریک روی پشت‌بام خانه‌ای نشسته بودند، به‌سختی از خطر حمله هواپیماهای آمریکایی که آنها را به‌جای «شورشیان» اشتباه گرفته بودند، جُستند.(۳۳) تقریباً دو سال از آغاز جنگ عراق گذشته بود، اما نیروهای ایالات متحده عملاً نتوانسته بودند امنیت جاده‌هایی که شهر بغداد را به فرودگاه آن شهر متصل می‌کرد برقرار سازند و پرسنل آمریکایی ناگزیر بودند برای رفتن به فرودگاه از هلی‌کوپتر استفاده کنند.(۳۴)

مقامات آمریکایی به این تراژدی‌ها فکر نمی‌کنند. استیون کامبرن[1] رئیس اداره جاسوسی وزارت دفاع که در تدوین گزارش پروژه قرن جدید آمریکا[2] در سپتامبر ۲۰۰۰ با عنوان بازسازی استحکامات دفاعی آمریکا[3] مشارکت داشته است، به یک مصاحبه‌کننده گفت که ترکیب اطلاعات[4] و هنرهای عملیاتی چه‌بسا خودش حوزه مأموریت جدیدی را ایجاد کرده است.(۳۵) در آن روز، *نیویورک تایمز* مصاحبه کامبرن را چاپ کرد. این روزنامه در سرمقاله خود درج کرد که «مجموعه‌ای از هواپیماها و ماهواره‌های جاسوسی پیشرفته به همراه شبکه ارتباطاتی رایانه‌ای به متحدان آمریکا امکان داد آنچه را در میدان نبرد اتفاق می‌افتاد به‌مراتب آشکارتر و پروضوح‌تر از قبل مشاهده کنند».(۳۶)

۹-۸ آیا سیستم فرماندهی و کنترل جهان‌گستر به حد کافی برای انجام عملیات‌های هسته‌ای، قابل اطمینان است؟

آیا این توانمندی‌های رایانه‌ای و ارتباطاتی که از عملیات‌های هسته‌ای پشتیبانی

1. Steven Camborne
2. Project on New American Century
3. Rebuilding American's Defenses
4. Intelligence

می‌کنند، باثبات و مطمئن‌اند؟ در این بخش، ما مسئله اطمینان‌پذیری را بررسی خواهیم کرد. بعد از آن، به موضوع امنیت شبکه سری مسیریاب پروتکل اینترنت که عملیات‌های هسته‌ای آمریکا و مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر بدان متکی است، بازمی‌گردیم.

با توجه به اینکه زمان کافی برای ارتقای سطح سیستم‌های رایانه‌ای وجود دارد، سیستم‌های رایانه‌ای موجود نیز قاعدتاً زمانی منسوخ خواهند شد. در زمان نگارش این سطور، هیچ مدرکی دال بر نارسایی در سیستم فرماندهی و کنترل جهان‌گستر وجود ندارد، اما ما می‌دانیم که یک مقام مسئول در سال ۲۰۰۳، این سیستم‌ها را سیستم‌های قدیمی و نارسا نامید.(۳۷)

ما چیزهایی نیز در مورد سیستم جاسوسی بزرگ آمریکا ـ که ضعف‌ها و نارسایی‌های آن چه‌بسا پیامدهایی برای عملیات‌های نظامی و بازدارندگی هسته‌ای داشته است ـ می‌دانیم. در روزهای پایانی سال ۱۹۹۹ و بار دیگر یک ماه بعد از آن، سازمان امنیت ملی[1] توانایی پردازش داده‌های دریافتی از ماهواره‌ها را از دست داد. این نارسایی و اختلال در سازمان امنیت ملی چقدر شدید بود؟

در ۲۹ ژانویه ۲۰۰۰ خبرگزاری *رویترز* خبر تازه‌ای را درباره سازمان امنیت ملی منتشر کرد و گزارش داد که مراکز فرماندهی سازمان امنیت ملی در ساعت هفت بعدازظهر روز دوشنبه، ۲۴ ژانویه ۲۰۰۰ از یک مشکل حاد رایانه‌ای رنج می‌بردند.(۳۸) این سیستم بعد از ۷۲ ساعت یعنی در روز پنج‌شنبه دوباره راه‌اندازی شد.(۳۹) سازمان امنیت ملی کوشید تأکید کند که هیچ اطلاعات جاسوسی مهمی از بین نرفته است، اما در برآورد اهمیت فرصت مغتنم دسترسی به داده‌های جاسوسی و اطلاعاتی کوتاهی کرد: «این مسئله، که صرفاً به مجموعه مراکز فرماندهی سازمان امنیت ملی در فورد مید، ام. دی[2] مربوط می‌شد، بر عملیات‌های اطلاعاتی ـ جاسوسی تأثیر ننهاد، اما بر پردازش اطلاعات جاسوسی تأثیر نهاد ...».

«طرح‌های احتیاطی بلافاصله به اجرا درآمدند. این طرح‌ها مقرر ساختند که سایر

---

1. National Security Agency
2. Ford Meade, MD

بخش‌های سیستم سازمان امنیت ملی نیز مقداری از این مسئولیت را برعهده بگیرند. سازمان امنیت ملی اطمینان دارد که هیچ اطلاعات جاسوسی چشمگیر و مهمی از دست نرفته است».[۴۰]

خبرهای خوش همچنان این است که آزمایش سیستم‌ها در فهم کاربرد سیستم فرماندهی و کنترل جهان‌گستر و به‌ویژه درخصوص سیستم برنامه‌ریزی و اجرای طرح‌های هسته‌ای[1] به‌شدت جاافتاده است. برخی خبرهای «خوب و بد» هم حکایت از آن دارد که اصلاح و بهبود نرم‌افزارها و سخت‌افزارها یکی از ویژگی‌های بارز این سیستم است. اما اخبار بد این است که دقت، صحت و یکپارچگی، اطمینان‌پذیری و کاربردپذیری سیستم‌ها چه‌بسا در زمانی مشخص می‌شود که این سیستم‌ها به مخاطره افتاده و بی‌اعتبار شده‌اند. باید خاطرنشان ساخت که این حالت حتی بعد از مرحله آزمایش و تأییدِ به‌کارگیری سیستم‌ها نیز روی می‌دهد.

۱۰-۸ آیا شبکه سری مسیریاب پروتکل اینترنت به حد کافی برای انجام عملیات هسته‌ای امنیت دارد؟

شبکه سری مسیریاب پروتکل اینترنت شبیه شبکه اینترنت عادی است. اما ویژگی‌های خاصی را نیز دارد. تنها ایالات متحده است[۴۱] که این شبکه را در اختیار دارد و ازاین‌رو مشکلاتی را درزمینه همکاری آمریکا با نیروهای ائتلاف پدید آورده است.[۴۲] این معضلات به‌قدری شدید و حاد می‌باشد که در طرح‌های جدید برای حل آنها قید «تنها ایالات متحده» را سست ساخته‌اند.[۴۳] حداقل، آنچه در تلاش برای تضمین امنیت ارتباطات اهمیت دارد، تمرکز فعالیت‌های شبکه سری مسیریاب پروتکل اینترنت بر سخت‌افزار اختصاصی است: این سخت‌افزار به‌گونه‌ای طرح‌ریزی شده است که براساس آن، کاربر اینترنت همگانی به‌هیچ‌وجه نمی‌تواند به شبکه سری مسیریاب پروتکل اینترنت دسترسی داشته باشد.

یک شبکه، برای آنکه قابل اطمینان باشد می‌باید چند معیار را رعایت کند:

---

1. Nuclear Planning and Execution System

۱. سری بودن محتوا: پیام‌ها را نتوان خواند.
۲. یکپارچگی و درستی محتوا: پیام‌ها را نتوان تغییر داد.
۳. اطمینان از تحویل پیام: پیام‌ها را نتوان از بین برد.
۴. اطمینان از منبع تدوین پیام: پیام‌ها و منابع را نتوان کپی‌برداری کرد.
۵. امکان جریان یافتن پیام‌ها و داده‌ها: هیچ کارشکنی یا تأخیر چشمگیری وجود نداشته باشد.
۶. مصونیت از تحلیل حرکت داده‌ها در شبکه: منبع، زمان، حجم و مخاطبان پیام‌ها در دسترس افراد غیرمجاز قرار نگیرند.
۷. صحت و یکپارچگی ابزارهایی که در شبکه به‌کار رفته‌اند: غیرخودی‌ها نتوانند بدون مجوز به داده‌ها نگاه کنند و دستگاه‌های ازکارافتاده را نتوان به‌کار گرفت.

البته، اینها همان پیام‌ها در معنای روزمره نیستند و چه‌بسا ممکن است انتقال فایل‌ها، جریان یافتن جابه‌جایی داده‌ها، درخواست‌های موجود در صفحه‌های وب و هرگونه تبادل داده و اطلاعات را دربرگیرند.

سه‌گونه متفاوت اطمینان در مفهوم «شبکه مطمئن» مطرح می‌باشد: محتوا و منبع تولید داده از طریق رمزنویسی حفاظت می‌شود. ساختار سخت‌افزارها و نیز ساختار شبکه، این احتمال را تقویت می‌کند که سیستم به‌رغم وجود نارسایی‌ها و اختلال‌ها در آن کار خواهد کرد. آمیزه‌ای از سخت‌افزارهای سیم‌دار (از جمله فیبری) و بدون سیم می‌باید براساس اصول فیزیکی مبادله اطلاعات را هدایت کنند. مسئله سوم، که با تحلیل «تبادل داده‌ها» مرتبط است، در صورتی وجود ندارد که شبکه از یکپارچگی فیزیکی کاملی بهره‌مند باشد. اما اگر در هر نقطه بتوان از آن استراق‌سمع کرد، چه‌بسا برخی داده‌ها در دسترس سارقان و هکرها قرار گیرد. ازاین‌رو، نرم‌افزاری درزمینه کشف و شناسایی نفوذ به اینترنت با اهداف تجاری تعبیه شده است.

ما سیستم فرماندهی و کنترل جهان‌گستر را یک شبکه فرعی اجرایی توصیف کرده‌ایم که روی شبکه وسیع‌تر به نام شبکه سری مسیریاب پروتکل اینترنت نصب است و البته به‌شدت نیز به آن وابسته است.[۴۴] شبکه مسیریاب پروتکل اینترنت شیوه‌هایی در خود دارد که بهره‌برداری از شبکه را به کاربران مجاز، محدود می‌سازد و طبقه‌بندی

داده‌ها را نیز به اجرا درمی‌آورد. اسناد فقط برای آن کاربرانی قابل دسترسی خواهد بود که مجوز لازم را داشته باشند. همان‌گونه که در بالا اشاره شد، شبکه سری مسیریاب و پروتکل اینترنت شبکه‌ای است که تنها شهروندان آمریکایی می‌توانند از آن استفاده کنند. یک شبکه «مطمئن و امن» در این معنا هیچ «ارتباط دوجانبه»[1] مستقیمی با تلفن‌های همگانی یا شبکه‌های داده‌پراکنی نخواهد داشت. این شبکه با این هدف طراحی شده است که جدا از سایر شبکه‌ها باشد.(۴۵) اما، برای آنکه سودمند باشد، باید شیوه‌هایی به‌وجود آورد که افراد مجاز بتوانند از طریق آنها بدان دسترسی یابند. تمهیداتی نیز برای محدودسازی بهره‌برداری از شبکه به اشخاص مجاز اندیشیده شده است. سازمان سیستم اطلاعات دفاعی[2] (تأکید از من است) تبیین می‌کند که:

«شبکه سیستم اطلاعات دفاعی دو شبکه مسیریاب پروتکل اینترنت دارد که جدا از یکدیگرند: شبکه سری مسیریاب پروتکل اینترنت و نوعی شبکه پروتکل اینترنت که طبقه‌بندی نشده اما حساس است.

شبکه سری مسیریاب پروتکل اینترنت، شبکه‌ای دربرگیرنده حوزه‌ای وسیع است که هم ازنظر فیزیکی و هم ازلحاظ منطقی از سایر شبکه‌ها جداست. هر مدار دسترسی و استخوان‌بندی شبکه نیز برای تضمین یکپارچگی اطلاعات، رمزنویسی شده است.

شبکه سری مسیریاب پروتکل اینترنت برای اینکه به همه نوع تبادل اطلاعات اجازه عبور دهد، از چند پروتکلی که شبکه‌ها را به هم پیوند می‌دهد، استفاده می‌کند. این پروتکل‌ها عبارت‌اند از: پروتکل اینترنت، پروتکل کنترل انتقال،[3] پروتکل انتقال فایل،[4] پروتکل انتقال هایبرتکست،[5] تل نت،[6] پروتکل انتقال پستی ساده.[7]

سرورهای ارتباطاتی از دستگاه‌های مطمئن داده‌پردازی استفاده می‌کنند. از جمله این دستگاه‌ها، «واسط شماره‌گیر» است. این‌گونه دستگاه‌ها به مسیریاب‌های سازمان سیستم اطلاعات دفاعی متصل‌اند. مسیریاب‌های این سازمان به کاربران دستگاه‌های

---

1. Interconnections
2. Defernse Information System Agency
3. Transmissission Control Protocol (TCP)
4. File Transfer Protocol (FTP)
5. Hypernet Transfer Protocol (HTTP)
6. Telnet
7. Simple Mail Transfer Protocol (SMTP)

مطمئن داده‌پردازی اجازه می‌دهند به شبکه سری مسیریاب پروتکل اینترنت دسترسی داشته باشند. دستگاه‌های مطمئن داده‌پردازی با استفاده از «فهرست کنترل دسترسی»، دسترسی کاربران مجاز را محدود می‌سازند. برای آنکه کاربران اجازه یابند به سرور ارتباطاتی متصل شوند، باید کلید کاربری محرمانه‌ای داشته باشند. ابزار حفاظتی دیگر، استفاده از سیستم کنترل دسترسی به ترمینال خارجی[1] است که مستلزم کلمه عبور و ورود به سیستم[2] است. برای کسب اطلاعات در مورد چگونگی دسترسی به‌سرور ارتباطاتی به سایت "Network Information Home Rage" نگاه کنید.

شبکه مسیریاب سری پروتکل اینترنت از بسیاری از برنامه‌های مهم حمایت می‌کند. در این زمینه، می‌توان به این برنامه‌ها اشاره کرد: سیستم پیام دفاعی،[3] سیستم فرماندهی و کنترل جهان‌گستر و سیستم جهان‌گستر پشتیبانی از نبرد».(۴۶)

به خاطر داشته باشید که سیستم فوق سری فرماندهی و کنترل جهان‌گستر حتی معیارهای مشکل‌تری را درزمینه امکان دسترسی اعمال می‌کند و همان‌گونه که در مورد لزوم رمزنویسی مضاعف گفته شد می‌باید بسیار قوی‌تر از شبکه مسیریاب پروتکل اینترنت ـ که معمولی است ـ به رمزنگاری پرداخت وگرنه به‌محض اینکه شخص به شبکه سری مسیریاب پروتکل اینترنت به‌طور مجاز دسترسی داشته باشد، آن فرد چه‌بسا فرصت شیطنت خواهد داشت. شما قادر خواهید بود به هر کاربر دیگری که از این شبکه استفاده می‌کند پست الکترونیکی بزنید (۴۷) و با وی ارتباط برقرار کنید.

به‌طورقطع، طراحان این شبکه از احتمال انتقال رمزهای قابل اجرا با پست الکترونیکی آگاهی دارند. زیرا از چنین رمزی می‌توان برای به خطر انداختن و بی‌اعتبارسازی دستگاهی که کاربر دارد، استفاده کرد. البته اقداماتی هم برای جلوگیری از مداخله در شبکه انجام گرفته است. در برخی موارد، از همان نرم‌افزاری که من و شما می‌توانیم از بازار محلی خریداری کنیم استفاده می‌شود؛ اما بااین‌حال فایل‌های پیوست نامه‌های الکترونیکی به‌طور خاص هدف قرار می‌گیرند. «سرویس‌هایی که در آنها تأسیسات ساحلی و ناوگان دریایی به مشتریان عرضه می‌شوند، دو شبکه می‌باشند: یکی

---

1. External Terminal Aceess Control Access Control System (XTACACD)
2. Login
3. Defense Message System (DMS)

شبکه سری پروتکل اینترنت و دیگری، شبکه غیرطبقه‌بندی شده پروتکل اینترنت.[1] نرم‌افزار «طیف»[2] برای مدیریت شبکه مورد استفاده قرار می‌گیرد. حفاظت از طریق دیوار نسوز[3] نیز با استفاده از نرم‌افزار «گاونلت»[4] انجام می‌گیرد. یک رایانه با استفاده از آنتی‌ویروس نورتون،[5] اسکن‌هایی از ویروس تهیه می‌کند. نرم‌افزار آنتی‌ویروس فایل‌های پیوست پست الکترونیکی را از مشتریان خارج دیوار نسوز به مشتریان ناوگان دریایی در داخل دیوار نسوز انتقال می‌دهد».(۴۸) آیا فایل‌های پیوست که از داخل دیوار نسوز ارسال می‌شوند، مورد آزمایش قرار می‌گیرند؟ به‌ظاهر نه.

این منبع، برگرفته از مصاحبه‌ای با دی. بی. تامس،[6] مدیر وقت سیستم‌های اطلاعاتی در مرکز عملیات‌های شبکه منطقه آتلانتیک متحد[7] و وابسته نیروی دریایی آمریکاست. مصاحبه‌کننده موضوع امنیت شبکه، این‌گونه شرح می‌دهد: «به‌طور قطع، رهبران نظامی به‌احتمال افشای اطلاعات امنیتی توجه داشته‌اند. ازآنجاکه امنیت، دغدغه و نگرانی همه به‌شمار می‌آید، من از تامس سؤال کردم که در مورد ریسک‌هایی که در برابر منافع روحیه‌بخش وجود دارد، چه تدبیری اندیشیده است. وی در پاسخ می‌گوید: هر چیزی ریسک‌هایی دارد. مهم این است که ما چگونه آن ریسک‌هایی را که اهمیت دارد مدیریت کنیم. برای مثال، اداره مرکزی[8] این توانمندی را دارد که از روی کشتی، پست الکترونیک را کنترل کند و به آن دسترسی داشته باشد. علاوه‌بر این، ما نرم‌افزار آنتی‌ویروس نورتون را در خارج از دیوار نسوز نصب کرده‌ایم تا فایل‌های پیوست به پیام‌ها را پیش از آنکه به ناوگان دریایی برسند اسکن کند. اما این نرم‌افزار برای ویروس‌ها به‌کار می‌رود نه برای افشای اطلاعات طبقه‌بندی شده و صرفاً فایل‌های پیوست اسکن می‌شوند نه پست الکترونیک اصلی».

تامس شبکه سری مسیریاب پروتکل اینترنت را شبکه‌ای جدا می‌داند، اما به‌نظر

---

1. Non-Classified Internet Protocol Network (NIPRNET)
2. spectrun
3. Firewall Pratection
4. Gaunlet
5. Norton Anti-Virus
6. D.B. Thomas
7. Unified Atlantic Region Network Operations Cetre
8. Centre Organization (CO)

می‌رسد که اذعان کرده است احتمال دارد این شبکه وارد شود (تأکید از من است): «شبکه سری مسیریاب پروتکل اینترنت، داستان دیگری است. حفاظت از این شبکه همواره با استفاده از رمزنگاری انجام می‌گیرد. اگر کسی این شبکه را هک کند، مشکل بزرگی پیش می‌آید.

در سراسر تاریخ، افراد به‌صورت عمدی یا غیرعمدی به اطلاعات طبقه‌بندی شده دست یافته‌اند. افرادی مثل جانی واکر[1] در پیرامون ما وجود دارند در گذشته آنها را داریم. در حال حاضر نیز آنها را داشته‌ایم و باز در آینده نیز آنها را خواهیم داشت. اما اکثریت قاطع نظامیان ما صداقت فردی دارند و آموزش‌هایی دیده‌اند که آنها را از نقض قواعد امنیتی بازمی‌دارد.

اگر آنها ساعت کار داشتند، آیا مرکز عملیات‌های شبکه واقعاً می‌توانست محتوای پیام‌ها را بررسی کند؟ تامس می‌گوید: بله ما می‌توانیم هم محل پیام‌ها را کنترل کنیم و هم ببینیم این پیام‌ها به کجا می‌روند. پست الکترونیک‌های بسیار زیادی وجود دارد اما افرادی که به‌کار گردآوری آن داده‌ها گمارده شده‌اند به حد کافی می‌باشند. ما معیارهایی را برای افراد دریافت‌کننده داده‌ها در نظر گرفته‌ایم و به نتایج جالبی هم رسیده‌ایم. مرکز عملیات‌های شبکه در این اواخر کوشیده است بودجه کافی را مشخص سازد به‌گونه‌ای که این افراد بتوانند سرویس شماره‌گیری در خارج از دیوار نسوز را تهیه کنند. در این صورت، مرکز عملیات‌های شبکه قادر خواهد بود از سایر مراکز فرماندهی مستقر در سواحل آن ناحیه محلی نیز پشتیبانی به‌عمل آورد».

جانی واکر که از وی نام برده شد، همان جان ای واکر، یکی از خدمه زیردریایی‌های نیروی دریایی آمریکا و سازمان‌دهنده یک شبکه جاسوسی بود که اعضای آن دوستان و خویشاوندان وی بودند. این شبکه جاسوسی خارج از بندرگاه نیروی دریایی آمریکا در نورفولک[2] ویرجینیا فعالیت می‌کرد. واکر اطلاعات سری در مورد رمزنویسی نیروی دریایی و سایر موضوعات را گردآوری می‌کرد و آنها را در اختیار اتحاد شوروی قرار می‌داد.(۴۹)

به‌نظر می‌رسد گزارشی که در سال ۱۹۹۷ منتشر شد تأیید می‌کند که شبکه سری

---

1. Johnny Walker
2. Norfolk

مسیریاب پروتکل اینترنت در نیروی دریایی ایالات متحده آن زمان آسیب‌پذیر بوده است. برخلاف نیت‌هایی که طراحان این شبکه داشتند، در آزمایش امنیت شبکه: «یک افسر نیروی هوایی ایالات متحده موفق شد با اینترنت و اسپینت[1] (که شکل نظامی اینترنت به‌شمار می‌آید) به سیستم فرماندهی و کنترل یکی از کشتی‌های نیروی دریایی دسترسی پیدا کند (نقطه‌ضعفی که این امکان را فراهم آورده بود، از آن زمان به بعد رفع شده است)».(۵۰)

یکی از دغدغه‌های کاربران سیستم‌های نظامی، این است که چه‌بسا ممکن است بخش‌هایی از این سیستم در جریان نبرد خراب شود. این سیستم، هم برای انطباق شرایط خود با سکوهای در حال حرکت و هم برای جلوگیری از خسارت‌های نبرد، «سرورِ نام گستره»[2] را اضافه بر سازمان در خود جای داده است: «حوزه عملیات‌های «مرکز عملیات‌های شبکه»،[3] منطقه آتلانتیک است. اما گستره این عملیات‌ها به فراسوی این منطقه، یعنی دریای مدیترانه، اقیانوس هند و خلیج فارس کشیده شده است.

زمانی که «مرکز عملیات‌های شبکه» تردد یک کشتی در خارج ناحیه آتلانتیک را زیر نظر دارد، این عبور تقریباً آزادانه است. این نوع کنترل پدیده‌ای به نسبت جدید است. با تأسیس و راه‌اندازی کامل یوروسن[4] بخش زیادی از بار کنترل از روی مرکز عملیات‌های شبکه برداشته شده است. ما دیگر ناگزیر نیستیم همه کشتی‌هایی که از این منطقه تردد دارند پشتیبانی کنیم. علاوه‌بر این، پایگاهی نیز در بحرین وجود دارد. اما این پایگاه یک «مرکز عملیات‌های شبکه» که کامل و تمام‌عیار باشد، نیست. اما خدمات شبکه را در اختیار کشتی‌هایی که در خلیج فارس تردد می‌کنند، قرار می‌دهد.

برای مثال، «سیستم نام گستره» را در نظر بگیرید. مرکز عملیات‌های شبکه سرورهای ثانویه‌ای دارد که در سراسر جهان مستقراند. اگر سرور اولیهٔ «سیستم نام گستره» دچار اختلال شود، سرور دیگر به‌صورت خودکار کوک می‌شود و اداره شبکه را

---

1. Spinet
2. Domain Name Server
3. Network Operations Centre (NOC)
4. EUROCEN

به‌دست می‌گیرد. در محیط شبکه‌ای، پشتیبانی واقعی در همان سرورهای ثانویه‌ای است که جاهای دیگر استقرار یافته‌اند».

وانگهی، در زمان نگارش این گزارش، مرکز عملیات‌های شبکه، دیوار نسوز را بهسازی کرده بود و زمینه‌های نصب نترانگر[1] را که شبکه‌های اخلال‌گر و هکرها را کنترل می‌کند، فراهم ساخته بود.(۵۱)

اگر رایانه‌ای در اختیار داشته باشیم که دستگاه شبکه غیرطبقه‌بندی شده پروتکل اینترنت روی آن نصب است و در وب‌سایت «شبکه سری مسیریاب پروتکل اینترنت» نیز روی URK کلیک کنیم، صفحه‌ای باز خواهد شد که این جمله در آن درج شده است: لطفاً به خاطر داشته باشید که شما نمی‌توانید از دستگاه شبکه غیرطبقه‌بندی شده پروتکل اینترنت به وب‌سایت شبکه سری مسیریاب پروتکل اینترنت صدمه بزنید.(۵۲) یک فروشنده پیشنهاد داده است در ازای یک دوره پنج‌روزه برای آموزش کار با این دو شبکه مذکور به تکنیسین‌هایی که این سیستم‌ها را نصب خواهند کرد ۱۵۹۵ دلار دستمزد دریافت می‌کند و موضوعاتی از قبیل استقرار و نصب رمزها و عیب‌یابی از رمزها را آموزش می‌دهد.(۵۳)

تا زمانی که ظرفیت فوق سری دیگری به سیستم فرماندهی و کنترل جهان‌گستر اضافه نشده بود، برنامه عملیاتی یکپارچه واحد هسته‌ای وارد سیستم فرماندهی و کنترل جهان‌گستر نشد. سیستم جهان‌گستر فرماندهی و کنترل نظامی به‌عنوان شبکه‌ای فوق سری که ازنظر محرمانه بودن در سطح بالایی قرار دارد وارد فاز اجرایی شده است. در ۳۰ ژوئن ۱۹۹۷، این سیستم برچیده شده و به‌جای آن، مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر راه‌اندازی شد.(۵۴) چه چیزی سطح سری را از سطح فوق سری متمایز می‌سازد؟ به لحاظ فنی، مدل فوق سری سیستم فرماندهی و کنترل جهان‌گستر رمزنویسی دوگانه‌ای را به اجرا درمی‌آورد ـ سیستم عادی فرماندهی و کنترل جهان‌گستر از این ویژگی بی‌بهره است. کاربران ـ چه نظامی، چه غیرنظامی و چه کارکنان پیمانکار غیردولتی ـ می‌باید مجوزهای امنیتی مشابهی داشته باشند. تا جایی که به تسلیحات هسته‌ای مربوط می‌شود، این مجوز، مجوزی مرتبط با طرح عملیاتی یکپارچه واحد در

1. Netranger

مقوله‌ای متناسب خواهد بود. این وضعیت مستلزم آن است که نظارت‌ها و صدور مجوزها کافی و جدید باشند، به‌گونه‌ای که با نیاز کاربر نیز متناسب باشند.(۵۵)

در شبکه جهانی اینترنت، کاربران خطر تلاش‌های «افراد بد»[1] برای بی‌اعتبارسازی درستی و یکپارچگی رایانه‌ها و داده‌های قابل دسترسی را به جان می‌خرند. روش‌های شناخته شده‌ای وجود دارد که با آنها می‌توان از تلاش‌ها برای رخنه کردن، دانلود کردن و سوءاستفاده از اینترنت جلوگیری کرد. آیا این مسائل جهان روزمره نیز موضوعاتی درزمینه جهان «کار قابل اطمینان با رایانه» در سایه حمایت دولت‌اند؟ فوگنه اچ. اسپافورد[2] یکی از دانشمندان علوم رایانه به ظاهر چنین می‌اندیشد، چرا که وی از دولت ایالات متحده سخن به میان می‌آورد. «دولت آمریکا از سیستم رایانه‌ای تک‌فرهنگی استفاده می‌کند که یک سیستم ایمن (و برخی می‌گویند ناچیز و حداقلی) را در خود دارد. در حال حاضر، این سیستم برای هدایت تسلیحات هسته‌ای، امور دفاع ملی، دولت و ارتباطات مورد استفاده قرار می‌گیرد. بیشتر افراد در رایانه‌های شخصی و تجاری خود از همین سیستم استفاده می‌کنند. این سیستم، سیستمی است که امور اقتصادی، دفاعی و بسیاری از فعالیت‌های علمی‌مان را بر آن استوار می‌سازیم. این سیستم بیش‌ازپیش در معرض حملات نرم‌افزارهای بدخواهان و تبهکاران قرار دارد».(۵۶)

وی سپس به‌صورت تلویحی حمله‌ای شدید به سیستم‌های وینتل[3] می‌کند و خاطرنشان می‌سازد که: «نسل بعدی ناوهای هواپیمابر نیروی دریایی همه سیستم‌های تسلیحاتی وینتل، فرماندهی و کنترل را در خود خواهند داشت. همان سیستم‌هایی که شما مشابه آنها را در خانه مورد استفاده قرار می‌دهید، با آنها وارد اینترنت می‌شوید و به بازی‌های رایانه‌ای می‌پردازید، همه اینها را به‌کار می‌اندازند».(۵۷)

درمجموع، تدابیر عملی نیز برای تخمین درجه بالایی از امنیت در شبکه سری مسیریاب پروتکل اینترنت و سیستم فرماندهی و کنترل جهان‌گستر اندیشیده شده است؛ اما آسیب‌پذیری‌ها همچنان وجود دارد ـ برخی آسیب‌پذیری‌ها در نیاز افراد به

---

1. Bad -Guy
2. Fugene H. Spafford
3. Wintel

استفاده از سیستم نهفته‌اند و برخی دیگر نیز در واقعیات فنی مشاهده می‌شوند.

۱۱-۸ ارزیابی

بررسی‌ای که در این فصل انجام گرفته است بر سه مسئله‌ای که در درازمدت و به‌صورت پایدار برای مدیریت تسلیحات هسته‌ای پیش خواهد آمد، تأکید می‌کند. نخست، «فرماندهی و کنترل» فرض را بر این می‌گذارد که پرسنل اصلی و کلیدی در زمان وقوع بحران در دسترس‌اند و از اطلاعاتی که خردمندان برای تصمیم‌گیری نیاز دارند، برخوردار است، اما ما می‌دانیم که این نیاز در آنها وجود ندارد. دوم، «فرماندهی و کنترل» مستلزم وجود ساختار ارتباطاتی باثبات است تا با آن بتواند اطلاعات را در اختیار قرار دهد، مجال بحث و بررسی را فراهم کند و تصمیمات را به اجرا درآورد، اما ما می‌دانیم که سیستم‌های ارتباطاتی چه‌بسا ممکن است نتوانند این کارویژه‌ها را انجام دهند. سوم، کنترل نیروهای هسته‌ای و مدیریت کردن آنها در برابر خطای چشمگیر مستلزم آن است که رسانه‌های ارتباطاتی نیز ایمن باشند، اما اگر شیوه‌های منسوخ جاسوسی را هم در نظر نگیریم، ما از نقطه‌ضعف‌ها و نارسایی‌های امنیتی در فناوری‌های جدید نیز بی‌اطلاعیم، ازاین‌رو ما می‌توانیم برخی از شیوه‌هایی را که با آنها می‌توان امنیت سیستم‌ها را برهم زد، در ذهن خود مجسم کنیم.

البته این وضعیت باعث نمی‌شود که ما نتیجه بگیریم تلاش‌ها برای طراحی یک سیستم نظامی باثبات و مورد اعتماد درزمینه مدیریت فعالیت‌های جاسوسی و ارتباطاتی، فاقد جدیت، بی‌پایه و اساس و ناشیانه بوده‌اند بلکه بالعکس حتی با بهترین حسن‌نیت نیز نمی‌توان به امنیت کامل دست یافت. «جنگ سایبر»[1] خواه‌ناخواه بحث «دفاع سایبر»[2] را پیش می‌کشد. آسیب‌پذیری‌ها را باید به‌عنوان دغدغه‌های همیشگی در نظر گرفت و درک کرد. برای مثال، سیستم‌های نظامی فناوری اطلاعات هر روز پیچیده‌تر می‌شوند. ازاین‌رو ناگزیر از یک‌سو نوعی ساده‌سازی[3] را تحمیل خواهند کرد و ازسوی‌دیگر، رویه‌های امنیت‌زا را تداوم خواهند بخشید. در این راستا، یک مرکز فناوری

---

1. Cyber War
2. Cyber Dffence
3. Simplification

اطلاعات و عملیات[1] در آکادمی نظامی آمریکا (وست‌پوینت)[2] تأسیس شده است. دانشجویان وست پوینت باهمتایان خود در سایر آکادمی‌های آموزش نظامی آمریکا در عرصه فناوری اطلاعات، در رقابت‌هایی که برای آنها طراحی شده است وارد می‌شوند.

مانورهای دفاع سایبر[3] در سال‌های ۲۰۰۱ و ۲۰۰۲: «شبکه‌ای از سرورها و ایستگاه‌های رایانه‌ای مشابه در هریک از دانشکده‌های افسری راه‌اندازی شد. در مرحله اول، دانشجویان افسری و دانشجویان نیروی دریایی در هر سایت، مجموعه متنوعی از سرویس‌های مورد نیاز خود را نصب و تنظیم کردند. هدف هر گروه در طول این مرحله، تنظیم سرویس مورد نیاز و سیستم‌های عامل اصلی به مطمئن‌ترین وجه ممکن بود. در مرحله دوم، گروه نفوذی[4] به رهبری سازمان امنیت ملی[5] به هر سایت حمله کرد. این گروه، یعنی گروه قرمز، در یک مقطع زمانی پنج‌روزه، عملیات شناسایی مبسوط و حملات گسترده‌ای را انجام داد. این گروه رکوردهای دقیقی را در مورد همه نفوذهای موفقیت‌آمیزِ خود ثبت کرد. گروه سفید از تیم رایانه‌ای واکنش اضطراری[6] در دانشگاه کارنگی ملون این تمرین نظامی را انجام داد. آنها به‌خوبی نقش ناظر و کنترل‌کننده را ایفا کردند و براساس سیستم امتیازدهی که تعیین می‌کرد کدام دانشکده برنده شده است، نمره قابل قبولی گرفتند».(۵۸)

برنامه‌ریزانی که نگران یکپارچگی فرماندهی و کنترل هسته‌ای ایالات متحده می‌باشند. باید به این نکته نیز توجه کنند که ایالات متحده در تلاش برای کسب مزیت نظامی با «فناوری اطلاعات» و توسعه توانمندی «فرماندهی، کنترل، ارتباطات، کار با رایانه، فعالیت جاسوسی، نظارت و شناسایی»[7] تنها نخواهد بود. پیش‌نویس برنامه فعلی فرانسه که بر سیاست نظامی این کشور در فاصله سال‌های ۲۰۰۸-۲۰۰۳ حکم‌فرماست، تصریح می‌کند که: «بحران‌های اخیر بر اهمیت برتری تکنولوژیکی در حوزه‌های «فعالیت‌های

---

1. Information Technology and Operation Center (ITOU)
2. West Point
3. Cyber Defense Exercises (CDX)
4. Penetration Team
5. National Security Agency (NSA)
6. Computer Emergency Response Team (CERT)
7. Command, Control, Communications, Computing. Intelligence, Surveilence and Reconnaissance (C4ISR)

جاسوسی، فرماندهی و کنترل، سلاح‌های دقیق و اقدام نظامی در فاصله‌ای دور در تمام اشکال آن» مهر تأیید زده‌اند. ما با آگاهی از این وضعیت، می‌باید ظرفیت‌های جدیدی را به‌ویژه در حوزه‌های اطلاعات، ارتباطات و فرماندهی به‌دست آوریم».

دولت‌ها و گروه‌هایی هم که خود را دشمن آمریکا می‌دانند، می‌توانند اقداماتی را که متحدان سنتی آمریکا انجام می‌دهند، انجام دهند. آیا می‌توان از سیستم فرماندهی و کنترل جهان‌گستر کپی‌برداری کرد؟ اندیشه‌هایی که از فناوری اطلاعات بهره می‌گیرند، در دسترس‌اند و به‌آسانی می‌توان تصور کرد که ارتباطات گسترده‌ای میان ادارات «بسیار دور از هم» در دسترس همگان وجود دارد؛ اما بااین‌حال، در هر مقطع زمانی، شرایط سختی در حوزه فناوری باید تحقق یابد که این شرایط به‌نوبه خود، استقرار سیستم فرماندهی و کنترل جهان‌گستر را پرهزینه می‌سازد. یک سیستم کامل و تمام‌عیار می‌باید شرایط ذیل را داشته باشد:

۱. توانمندی کسب داده‌های اولیه،

۲. پردازش کارآمد داده‌ها در فرمت‌های متنوع و در زمان‌ها و مکان‌های مجزا،

۳. تحویل به‌موقع به فرماندهان و رزمندگان به شیوه‌ای که قابل کاربرد باشند.

چه‌بسا ممکن است جوامع دارای فناوری‌های برتر، کارهایی را انجام دهند که به سیستم فرماندهی و کنترل جهان‌گستر شکل می‌دهند و «انقلاب در امور نظامی» را به اجرا درمی‌آورند، اما هزینه انجام هریک از این کارها چشمگیر خواهد بود. (این وضعیت، موضوع سیاسی هزینه‌های «فرصت» را پیش می‌کشد)، البته ناگفته نماند که هزینه انجام بسیاری از این کارها ماهیتی بازدارنده و کمرشکن دارد.

سیستم فرماندهی و کنترل جهان‌گستر سه جنبه در خود دارد که محور انقلاب در امور نظامی را تشکیل می‌دهد:

۱. آگاهی از وضعیت،[1]

۲. انتخاب راهبردها و تاکتیک‌های نویدبخش‌تر،

۳. ارتقای هماهنگی.

این سه جنبه با شرایط و لوازم سنتی جنگ مطابقت دارند که عبارت‌اند از: شناخت

---

1. Situation Awareness

میدان نبرد، برنامه‌ریزی، دقت و اجرا. کیفیت نبردهای واقعی همواره بسته به شرایط غیرمنتظره، ابتکار عمل‌های دشمن و موفقیت یا شکست طرح‌های پیشبرد جنگ ناگزیر دچار جرح و تعدیل‌هایی شده است (به‌طوری که چه‌بسا ممکن است با الگوی بالا مطابقت کاملی نداشته باشد).

سیستم فرماندهی و کنترل جهان‌گستر به‌گونه‌ای طراحی شده است که ابزارهای بیشتری را در اختیار فرماندهان قرار می‌دهد، به‌گونه‌ای که براساس پیشبرد یک فرایند دقیق به‌نحو بهتری می‌توانند عملکرد خود را با واقعیت‌های نوظهور منطبق سازند و با انتخاب و انجام ابتکار عمل‌های جدید واکنش‌های مناسبی را به اجرا درآورند. به‌عبارت ساده‌تر، این سیستم راه‌های جدید و دقیق‌تری را برای تأمین نیازهای لجستیکی فراهم می‌سازد. در نتیجه، سیستم فرماندهی و کنترل جهان‌گستر به‌نوعی بیانگر فرماندهی صحنه جنگ است و بنابراین در قیاس با روش‌های پیشین، یک «انقلاب» را به راه می‌اندازد. سیستم فرماندهی و کنترل جهان‌گستر به‌کارگیری متمرکز فناوری اطلاعات است؛ این سیستم، کارویژه‌ای به‌مراتب وسیع‌تر از سازمان‌دهی داده‌هایی که در تک‌تک تسلیحات و برنامه‌های نظامی به‌کار می‌رود انجام می‌دهد.

هوشمندانه‌ترین طرحی که در سیستم فرماندهی و کنترل جهان‌گستر به اجرا درآمد، انطباق‌پذیری در حال تکوین[1] است. مسیر رو به رشد این سیستم را نمی‌توان مسدود کرد؛ زیرا حسگرها، نرم‌افزارها و واسطه‌های مصنوعی که برتری نظامی با آنها به‌دست می‌آید موضوعات «تغییر در حال تکوین» می‌باشند.

وقتی فناوری اطلاعات توسعه می‌یابد، ابزارهای سخت‌افزاری بدیع و آسیب‌پذیری‌های جدیدی مطرح می‌شود؛ ازاین‌رو، انطباق‌پذیری سیستم فرماندهی و کنترل جهان‌گستر بیش‌ازپیش به محور دکترین نظامی ایالات متحده مبدل می‌شود: تأکید بر ستاد مشترک ارتش با این هدف انجام می‌گیرد که این امر فرایند انطباق را آسان‌تر سازد. هم‌اکنون وزارت دفاع در حال حرکت به‌سوی «جنگ شبکه‌محور»[2] است.

آیا این تکنیک‌ها دستیابی ایالات متحده آمریکا به برتری راهبردی و تاکتیکی

---

1. Ongoing Adaptability
2. Network-centric Warfare

مطلق را نوید می‌دهد؟ پاسخ کوتاه به این پرسش و البته شاید همه آنچه امروز با اطمینان می‌توان گفت، این است که ایالات متحده آمریکا می‌تواند توانمندی‌های نظامی هر دولتی را که تسلیحات هسته‌ای در اختیار ندارد کمابیش به‌راحتی و بدون اینکه با اقدام متقابل مواجه شود نابود سازد، اما توانمندی‌های آمریکا در حوزه فناوری اطلاعات هیچ مزیتی را به این کشور نمی‌دهد که بتواند پیروزی در میدان نبرد را به‌دستاوردهای سیاسی «خودـ تداوم‌بخش» مبدل سازد. اگر ویژگی اصلی نیروهای مسلح (ارتش) در قرن بیست‌ویکم تأمین امنیت و ثبات بیشتر (که اساساً اهداف سیاسی به‌شمار می‌آیند) باشد، در این صورت نه فناوری اطلاعات و نه صحبت در مورد «انقلاب» یا «شبکه‌ها» نمی‌توانند این بار مسئولیت را بر دوش کشند. خطر فراروی ما این است که پیروزی‌های آسان در میدان نبرد، استراتژی‌پردازان نومحافظه‌کار آمریکا را فریب خواهد داد و به این باور خواهد رساند که فناوری اطلاعات، انقلاب در امور نظامی و جنگ شبکه‌محور مزیت و برتری یک‌جانبه و بلامنازع آمریکا را تضمین می‌کند، به‌گونه‌ای که این برتری را می‌توان «بدون توجه به هم‌بستگی منافع سیاسی مشترک بشریت و در خارج از ساختار امنیت دسته‌جمعی» اعمال کرد. «برخورداری از دانش و اطلاعات فراگیر»، امپراتوری را وسوسه می‌کند و شکست می‌خورد.

پی‌نوشت‌ها

1. Laura Hill, 'White House Communications Agency Transforms to Meet New Challenges', Army Communicator, Spring 2003, http://www.gordon.army.mil/ AC/ Spring/AC Spring 2003. pdf. Lieutenant Colonel Hill Headed the Washington Area Communications Command.

2. Ibid.

3. March Laree Jacques, 'Transformation and Redesign at the White House Communications Agency', *Quality Management Journal*, 6(3) 1999.

4.Hill, 'White House Communications Agency'.

5. Ibid.

6. Ibid.

7. G.W. Bush, Remarks to the 21st Century High Tech Forum, Washington, DC, 13 June 2002. http://www.whitehouse,gov/news/releases/2002/06/20020613-11.html.

۸. وزارت دفاع آمریکا، سازمان سیستم‌های اطلاعات دفاعی. برآورد بودجه سال مالی ۲۰۰۵، فوریه ۲۰۰۴. در:

http://www.defenselink/comptroller/defbudget/fy2005/budget

justification/pdfs/rdtande/DISA.pdf.

ازاین‌گذشته، این متن تبیین می‌کند که توانمندی عملیاتی اولیه (Initial Operational Capability) به‌صورت آزمایشی برای پایان سال مالی ۲۰۰۹ طراحی شده است. بخش دفاعی دیگر، سازمان امنیت ملی است که بیشتر امور مربوط به بودجه سال مالی ۲۰۰۵ را انجام خواهد داد.

9. Richard V. Allen, 'The Day Reagan Was Shot', The Atlantic Monthly, April 2001. Subscriber access: http://www.theatlantic.com/issues /2001/04/allen. html.

10. National Commission on Terrorist Attacks Upon the United States. The 9/11 Commission Report, New York: w.w. Norton & Co., 2004. Hereafter Cited as Report.

11. Report, p. 36.

12. Ibid.

13. Ibid. p.37.

14. Dan Balz and Bob Woodward, 'America's Chaotic Road to war. Bush's Global Strategy Began to Take Shape in First Frantic Hours After Attack', The *Washington Post*, 27 January 2002.

15. Colin L. Powell, Testimony Before the US Senate Foreign Relations Committee, 25 October 2001. http://www.state.gov/secretary/rm/2001/index.cfm? docid=5751.

16. Report, p. 38.

17. Rear Admiral Nancy Brown, USN, Vice-director of Command, Control, Communications and Computer Systems, Joint Staff. Testimony to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, House Armed Service Committee, US House of Representatives, 3 April 2003. Available at, http://www.house.gov/hasc/openingstatementsandpreereleases/108thcongress /03- 04- 03 brown.html.

۱۸. نگاه کنید به:

United States. Department of Defense. Defense Information System Agency, http://gccs.disa.mil/gccs, Revised 24 April 2002.

این صفحه با ذکر جزئیات بیشتری در مورد سیستم فرماندهی و کنترل جهان‌گستر، این‌گونه ادامه می‌دهد:

سیستم فرماندهی و کنترل جهان‌گستر، سیستم ثبت رایانه‌ای وزارت دفاع برای انجام کارویژه‌های فرماندهی و کنترل استراتژیک است. فرماندهان ستاد مشترک به کمک این سیستم می‌توانند در عملیات‌هایی که جابه‌جایی سریع نیروها نیاز است، واحدهای نظامی پراکنده در نقاط مختلف را باهم هماهنگ کنند، بازخورد صحیح را دریافت کنند و اقدامات دشوارتر و پردقت‌تری را که لازمه این‌گونه عملیات‌هاست انجام دهند.

طراحی سیستم فرماندهی و کنترل جهان‌گستر به‌عنوان سیستم ثبت فرماندهی و کنترل استراتژیک، از این امر حکایت دارد که تنها اعتبار و صحت داده‌ها (که دیدگاه‌ها، اعطای مجوزها و فرمان‌ها را دربرمی‌گیرند و در خود سیستم فرماندهی و کنترل جهان‌گستر وجود دارند یا به این سیستم متصل می‌شوند به‌گونه‌ای که فایل داده‌ها تنها در زمانی تغییر می‌کند که تغییراتی در داخل این سیستم انجام گیرد)، تضمین می‌شود.

سیستم فرماندهی و کنترل جهان‌گستر، منبع سهل‌الوصول و غالب را برای تولید، دریافت، توزیع و بهره‌برداری همراه با ایمنی از اطلاعات در اختیار فرماندهان جنگ قرار می‌دهد. این سیستم، امکان دستیابی به اطلاعات مربوط به عملیات‌های نظارت و شناسایی و دسترسی به منابع جاسوسی در سراسر جهان و داده‌های مربوط به موقعیت دقیق نیروهای نظامی دوست را که پراکنده باشند فراهم می‌کند.

سیستم فرماندهی و کنترل جهان‌گستر، نظامیان و رزمندگان را قادر می‌سازد عملیات‌های نظامی را طراحی، اجرا و مدیریت کنند. این سیستم به فرماندهان ستاد مشترک کمک می‌کند

اقدامات نیروهای هوایی، زمینی، دریایی، فضایی و نیروی عملیاتی ویژه را به‌صورت هم‌زمان زیرنظر داشته و هماهنگ سازند؛ وانگهی، این انعطاف‌پذیری را هم دارد که در طیف وسیعی از عملیات‌ها (از نبردهای واقعی گرفته تا کمک‌های بشردوستانه) مورد استفاده قرار گیرد. «سیستم طراحی و اجرای عملیات مشترک» نیز به این محیط منتقل شده است و در چارچوب آن عمل می‌کند. با استفاده از همین سیستم طراحی و اجرای عملیات مشترک، طرح‌های نظامی کشور در سراسر جهان تداوم می‌یابد و به‌روز می‌شود.

سیستم فرماندهی و کنترل جهان‌گستر، که مبتنی‌بر فناوری اطلاعاتی مدرن است، از سه جز تشکیل شده است: سرورهای پایگاه اطلاعاتی، سرورهای برنامه‌های رایانه‌ای کاربردی و مشتریان. این سیستم، یک سیستم فرماندهی، کنترل، ارتباطات، رایانه و جاسوسی است که در بهترین مدل «محیط عامل مشترک» کار می‌کند و امکان انعطاف، اعتمادپذیری و قابلیت بیشتری را درزمینه انجام کارویژه‌های مشترک با سایر سیستم‌های رایانه‌ای فراهم می‌کند. برای مثال، فرماندهان می‌توانند صفحه شخصی خودشان را در سطح محرمانه و سری ایجاد کنند و با اطمینان خاطر با پست الکترونیک با سایر همتایان خود در سراسر جهان ارتباط برقرار کنند. این سیستم، همان نوع از خدماتی را که در دسترس سیستم‌های عامل ویندوز در رایانه‌های خانگی است در اختیار پرسنل ارتش قرار می‌دهد.

سیستم فرماندهی و کنترل جهان‌گستر، برنامه‌های کاربردی پشتیبانی، از قبیل سیستم خودکار پاسخ‌گویی به پیام‌ها و برنامه‌های کاربردی درزمینه انجام مأموریت‌ها را نیز در خود جای داده است. برنامه‌های کاربردی درزمینه انجام مأموریت‌ها تمهیداتی از جمله یکپارچه‌سازی داده‌ها در یک تصویر تاکتیکی واحد، کپی‌برداری از داده‌های موجود در پایگاه‌های سیستم فرماندهی و کنترل جهان‌گستر و نمایش داده‌ها در فاصله‌ای تقریباًهم‌زمان بر یک قالب واحد، مجموعه بی‌نظیری از توانمندی‌ها و کارویژه‌ها را برای کمک به رزمندگان در اختیار آنها قرار می‌دهند. فیلترهای نمایش داده‌ها نیز می‌تواند برای ایجاد تصاویر مختلف در ویندوزهای متفاوت مورد استفاده قرار گیرد و لایه‌های پوششی نیز می‌تواند برای نمایش داده‌های مسیر هوا و کنترل هوا ـ فضا بهره‌برداری شود.

19. Carnegie Mellon Software Engineering Institute: http://www.seiie.cmu.edu/ activities/str/ descriptions/diicoe_body.html; and Defense Information Systems Agency: http://diicoe.disa.mil/coe.

20. DISA, above. http://gccs.disa.mil/gccs/.

21. 1998 Annual Defense Report, Above' Chapter8. On 30 August 1996 WWMCCS was Replaced by the Global Command and Control System (GCCS).

22. Recent Overview Documents Outlining US Defense Policy are: Quadrennial

Defense Review (QDR) (1997,2001); Nuclear Posture Review (NPR) (irregular: 1994, 2001/2002); and Annual Defense Report (each January Since 1995). Available at http://www.defenselink.mil/execsec/adr_intro. html.

23. United States: Department of Defense, Secretary of Defense, 1998 Annual Defense Report, Chapters 8. This is Spelt Out in Greater Detail in the Quadrennial Defense Review [1997], as follows

این گزارش با تفصیل بیشتری در مجله 1997 *Quadrennial Defense Review* این‌گونه توضیح می‌دهد:

پنج مؤلفه اصلی ساختار فرماندهی، رایانه، برای سال ۲۰۱۰ و بعد از آن عبارت‌اند از:

الف) یک شبکه اطلاعاتی چند حسگری مقاوم که آگاهی کامل فرماندهان و نیروهایمان در مورد نبرد فضایی را فراهم می‌نماید.

ب) توانمندی‌های پیشرفته درزمینه مدیریت نبرد که باعث می‌شود نیروهایمان را که در سراسر جهان مستقرند ـ سریع‌تر و انعطاف‌پذیرتر از استقرار نیروهای دشمنان بالقوه مستقر سازیم.

ج) توانمندی درزمینه انجام عملیات‌های اطلاعاتی که مجال «نفوذ و دست‌کاری در آگاهی دشمن از فضای نبرد و محروم‌سازی دشمن از این آگاهی یا استفاده آزادانه از نیروهای خودی» را فراهم می‌کند.

د) یک شبکه ارتباطاتی مشترک که از ظرفیت، انعطاف و توانمندی‌های کافی درزمینه مدیریت شبکه برخوردار باشد تا بتواند از توانمندی‌های فوق و طیف شرایط ارتباطاتی میان فرماندهان و نیروها پشتیبانی به‌عمل آورد.

ه) یک سیستم پدافند اطلاعاتی که بتواند شبکه ارتباطات و پردازش اطلاعات (که در سراسر جهان پخش شده است) را از گزند مداخله یا سوءاستفاده دشمن محفوظ نگه دارد.

24. United States: Department of Defense. Office of Test and Development, 1997 Annual Report Available at http://www.dote.sod.mil/reports/FY97 /97tocmain.html. Accessed 24 July 2002. At archive.org.

25. United States: Department of Defense. Defense Information Systems Agency. GCCS Interoperability Status chart. Available at. http://jitc.fhu.disa. mil/gccsiop/ and associated acronyms, http://Jitc.fhu.disa.mil /gccstot/iop _table. html.

26. Dawn C. Meyerriecks, Speaking to the Systems and Soffware Technology Conference, Salt Lake City, Utah. Global Computer News. 21 April 2004. Available at http://www.gcn,com/vo11_no1/daily-updated/25644-1.html.

27. Ibid.

28. Ibid.

29. Quoted in Tim Weiner, 'Pentagon Envisioning a Costly Internet for War', *The New York Times*, 13 November 2004.

30. United States, The White House, 9 April 2003. Available at http://www.whitehouse.gov/news/release/2003/04/20030409-4.html.,accessed 19 April 2003.

۳۱. نگاه کنید به:

http://www.ctv.ca/servlet/ArticleNews/story/CTVNews/20030406/iraq_friendly_fire_030406/World?s_name=&no_ads=0

32. CBC News, 19 April 2002, 'Canada Launches Inquiry into Afghanistan Bombing Deaths'. Available at http://www.cbc.ca/stories/2002/04/18/ cdndeaths 020418.

33. National Public Radio (Washington), 3 December 2004.

34. J.H. Cushman, Jr., and T. Shanker. 'War in Iraq Provides Model of New Way of Doing Battle', *The New York Times*, 10 April 2003.

35. *The New York Times*, Editorial, 11 April 2003.

36. Hill, 'White House Communications Agency Transforms to Meet New Challenges'.

37. Reuters, 29 January 2000.

38. Ibid. and Associated Press, 31 January 2000.

39. National Security Agency Statement. Quoted in Associated, 31 January 2000.

40. United States: United States Marine Corps. Available at www.quantico.usmc.mil/g6/ia/accessreq.doc, Acessed 20 April 2003.

۴۱. نگاه کنید به:

http://www.fcw.com/fcw/articles/2004/1115/news-siprnet-11-15-04.asp.

۴۲. نگاه کنید به:

R.W. Anthony, Institute for Defense Analyses, GCCS Evolution: Past, Present, and Futrue, (n,d.: 1998). Available at http://www.dodccrp.org/Preceedings/DOCS/wcd00000/wcd000fd.htm.

۴۳. یکی از نمونه‌های غیرهسته‌ای را تیم تحلیل برنامه‌ریزی ارتش پیشنهاد کرده است: تیم تحلیـل

برنامه‌ریزی ارتش برنامه‌ای است که امکان تغییر به‌موقع در برنامه‌ها و طراحی نرم‌افزار عملیاتی را در تجهیزات بقاپذیری هوایی فراهم می‌کند. به‌نظر می‌رسد که این تغییر در برنامه‌های نرم‌افزار عملیاتی زمینه تغییر دادن سریع شکل‌بندی ابزارآلات الکترونیکی پدافندی در هلی‌کوپترها، هواپیماها و کشتی‌ها را مهیا سازد. در راستای این بحث، ما توجه خود را به آن مسیرهای شماره‌گیری بدیلی معطوف می‌سازیم که در درون این سیستم تعبیه می‌شوند:

اگر شما رزمنده میدان جنگ هستید و دسترسی به سیستم دفاع موشکی، تاکتیک‌ها، تکنیک‌ها و رویه‌ها و سایر فایل‌های داده‌ای تهدیدزای مرتبط با آنها که تجهیزات بقاپذیری هوایی شما را به خطر می‌اندازند نیاز دارید، باید تجهیزات رمزداری را روی سیستم چندمنظوره توزیع داده‌های نبرد الکترونیک نصب کنید.

شما باید برای کسانی که به داده‌های جاسوسی اضافی نیاز دارند یا به دنبال شیوه‌ای قابل اتکاتر و سودمندتر برای دستیابی به این سیستم چندمنظوره‌اند، شبکه سری مسیریاب پروتکل اینترنت را نصب نمایید. این شبکه دقیقاً به مانند اینترنت است. البته تنها تفاوت آن، وجود رمزنویسی در یک سطح جانبی سری است. این شبکه مانند اینترنت، یک شبکه جهانی (world wide web (www)) معروف به INTELink-s دارد که امکان دسترسی به گزارش‌های جاسوسی و اطلاعاتی از طیف متنوع سازمان‌های ملی جامعه اطلاعاتی از قبیل سازمان ملی نقشه‌برداری و تصویربرداری، سازمان اطلاعات دفاعی و مرکز ملی اطلاعات جاسوسی زمینی را فراهم می‌نماید.

در این زمینه می‌توانید نگاه کنید به:

United States. US. Army. http://arat.icw.sed.monmouth.army. mil/ARAT. information /arat.services/arat-services.html.

44. United States: Department of Defense, Defense Information Systems Agency. [Internet], Page last Revised 14 May 2001. Available at http://www.pac. disa.mil/siprnet.html (Accessed 26 April 2003).

45. Ibid., Last Sentence Quoted IN Previous Note.

46. United States: US Navy. E. Smith, Email and Internet Services to the Fleet, a Report on the US Navy's Unified Atlantic Region Network Operations Centre (UARNOC) (n.d., Probably July 1998?). Available at: http://www.chips.navy.mil/ archives /98_jul/c_ews3.html (Accessed 26 April 2003).

47. United States: Office of the National Counterintelligence Executive. A Biographic sketch of J.A. Walker. Available at: http://www.ncix.gov/ pubs/ misc/screen_backgrounds/spy_bios/john_walker_bio.html (Accessed 18 April 2003).

48. Lord Lyell and L. Ibrügger. 'Information Warfare and the Millennjum

Bomb', AP 237 STC, (97)7, Draft General Report, 1 September 1997, p. 6, cited in NATO Parliamentary Assembly, Science and Technology Committee, Information Warfare and International Security, Draft General Report, 9 Ocober 1999, Publication AS285STC-E. Available at 1999. http://www.naa. be /archivedpub/comrep/1999/as285stc-e.asp [Accessed 20 April 2003].

49. NetRange'r is s CISCO Systems Intrusion Detection Software Product.

50. For Example, try visiting http://jto.eustis.army.smil.mil.

51. CACI International, Arlington, Virginia. Available at http://www.caci.com /netcom/pdf/IP Network Description.pdf (Accessed 26 April 2003).

52. Anthony, GCCS Evolution, 1.2.2.

53. That SIOP-ESI Categories Exist is Unclassified, and they are Referred to as Category 1 and so Forth, but Description of the Categories is Classified.

54. E.H. Spafford, 'One View of Protecting the National Information Infrastructure', in A.H. Teich, S.D. Nelson and S.J. Lita (eds), Science and Technology in a Vulnerable World, July 2002, Supplement to AAAS Science and Technology Policy Yearbook 2003, Committee on Science, Engineering, and Public Policy, American Association for the Advancement of Science. PP. 41-42.

55. Ibid., p. 46.

56. Lt. Col. D. Ragsdale (presenter), 14 March 2003, 2003 Capital Seminar on Information Assurance, UMBC Center for Information Security and Assurance, University of Maryland, Baltimore County [USA]. Available at http: //cisa.umbc.edu/(Accessed 18 April 2003).

57. France, Assemble'e Nationale, Profet de Loi Relative 'a la Progrmmation Militaire Pour les Ann'ees 2003 'a 2008, Submiteed to the Assembl'ee Nationale, 11 September 2002. Available at http://wwwassemblee-mat.fr/12/projets/ p10187-1.asp (Accessed 20 April 2003).

۵۸. لغت برگر نوعی نرم‌افزار برای شناسایی اختلال می‌باشد.

فصل نهم جنگ اطلاعاتی و قوانین جنگ

جفری دارنتون*

مقدمه

سیر توسعه نظام گسترده حقوق بین‌الملل در حوزه حقوق عمومی از روزگار گروسیوس(۱) آغاز شده است. افزایش حجم تجارت، مسافرت، مهاجرت، جهانی شدن و ازدواج‌های بین‌فرهنگی نیز ظهور حقوق بین‌الملل در حوزه خصوصی را به خود دیده‌اند.

چند دلیل مهم وجود دارد که نشان می‌دهد ظهور مجموعه حقوق بین‌الملل هنوز نیز همچنان دوران طفولیت خود را طی می‌کند. طرح واژه کلی حقوق بین‌الملل که از زمان گروسیوس توسعه یافته است بر فرض حاکمیت دولت‌ـ ملت‌ها استوار شده است و نظام حقوق بین‌الملل عمومی نیز تا حدی مبتنی‌بر برابری میان دولت‌های حاکمیت‌دار بوده است. در حوزه حقوق بین‌الملل عمومی، پیشرفت‌هایی درزمینه شناسایی[1] برخی اصول کلیدی وجود داشته است، اما نقطه‌ضعف عمده آن همچنان در حوزه اجرا می‌باشد. همین‌طور در حوزه حقوق بین‌الملل خصوصی، هیچ نهاد بین‌المللی برای رسیدگی به موارد اختلاف، صدور حکم و اجرای احکام وجود ندارد. حل‌وفصل اختلافات خصوصی همچنان به حوزه صلاحیت هریک از دولت‌ـ ملت‌های حاکمیت‌دار و نظام‌های حقوقی خود آنها وابسته است؛ بااین‌حال، در حوزه حقوق بین‌الملل عمومی، دولت‌ـ ملت‌ها طیفی از پیمان‌ها، معاهدات و پروتکل‌های ناظر بر موضوعات متنوع حقوق خصوصی و موافقت‌نامه‌های متقابل درزمینه صلاحیت‌های ملی را بین خود منعقد ساخته‌اند.

براساس این، ما در حال حاضر شاهد تکامل هم‌زمان دو بعد از حقوق بین‌الملل که پیوندهای خاص و نزدیکی با موضوعات مربوط به جنگ اطلاعاتی دارند، می‌باشیم: یکی

---

* Geoffrey Darnton

1. Recognition

قوانین جنگی؛ و دیگری رویکردهای حل‌وفصل تعارض قوانین در حوزه خصوصی.

در بعد فناوری، مهم‌ترین تحولی که سال‌های اخیر در هر دو حوزه «جنگ» و «جنگ اطلاعاتی» رخ داده است، استقرار و به‌کارگیری فناوری اطلاعات و ارتباطات رایانه‌محور می‌باشد. اما، در این بحبوحهٔ مناظره پرشور در مورد «فناوری اطلاعات و ارتباطات»، ما نباید این واقعیت را نادیده بگیریم که آنچه در پس برخی دستگاه‌ها و ابزارهای عملیات‌های اطلاعاتی قرار دارد به‌مراتب گسترده‌تر از فناوری رایانه‌محور اطلاعات و ارتباطات است و چه‌بسا حتی فناوری را در اموری فراتر از اطلاعات ـ پراکنی (برای مثال، عملیات‌های روانی، تبلیغات و فریبکاری) درگیر سازد.

یکی دیگر از مؤلفه‌های موجود در رابطه میان جنگ اطلاعاتی و حقوق بین‌الملل، مسئله جهانی‌شدن است. براساس این، هرچند ممکن است کانون بحث‌ها در مورد جهانی شدن، اقتصادی باشد، اما ما جهانی شدن را در معنای فقط تجاری در نظر نمی‌گیریم و آن را پدیده‌ای فقط تجاری نمی‌دانیم. در حال حاضر می‌بینیم جهانی شدن در سطح اشخاص نیز در حال رخ دادن است. ازاین‌رو هر روز بر شمار افرادی که مهاجرت می‌کنند افزوده می‌شود و بسیاری از قسمت‌های جهان بیش‌ازپیش چندفرهنگی شده‌اند. علاوه‌بر این، شاهد هستیم که در موضوعاتی از قبیل ازدواج، اقامت، محل سکونت، گروه‌های فشار، گروه‌های ذی‌نفوذ و تماس‌های شخصی نیز بسیاری از پیوندهای فرافرهنگی بیش‌ازپیش در سطح اشخاص انجام می‌گیرند.

جهانی شدن در هر دو حوزه تجاری و خصوصی از به‌کارگیری فناوری و اطلاعات و اطلاعات در رسانه‌های اطلاعاتی جهانی و سیستم‌های اطلاعاتی شخصی یا فردی تأثیر می‌پذیرد (Damton and Giaco letto, 1992).

جهانی شدن تنش‌ها در حوزه حقوق بین‌الملل را که مبتنی‌بر دولت‌های حاکمیت‌دار است افزایش داده است، چرا که حقوق بین‌الملل دولت ـ ملت‌محور معمولاً هیچ کمکی به موضوعات تبادلات بین‌مرزی در حوزه‌های خصوصی و تجاری ارائه نمی‌دهد. علاوه‌بر این، هر روز بیش از گذشته به‌نظر می‌رسد حقوق بین‌الملل ملت‌محور به‌مراتب بهتر می‌تواند نیازهای موجودیت‌های دسته‌جمعی و فردی را که در محیط چندملیتی عمل می‌کنند تأمین کند. اگر بنیادی‌تر به مسئله بنگریم، مشاهده خواهیم

کرد که چه‌بسا تغییرات سیاسی و فرهنگی عظیمی در حال اتفاق افتادن است. عمق احتمالی این تغییرات را نباید دست‌کم گرفت، در اینجا آنچه بیش‌ازپیش اهمیت یافته، ظهور «فرهنگ سایبر» است (Tofts and et. al., 2002). بخش اعظم حجم تجارت الکترونیک در حال حاضر مبادلات خارجی است که ارزشی برابر با میلیاردها دلار در روز دارد؛ این‌گونه مبادلات همچنان از هرگونه نظارتی در سطح بین‌المللی به دور می‌باشند و در حوزه خصوصی انجام می‌گیرند (کسانی که تجارت الکترونیکی را در معنای اینترنت[1] و برحسب آن به‌کار می‌برند می‌باید به خاطر داشته باشند که بخش اعظم تجارت الکترونیک از آن شبکه‌های ارتباطی که با اینترنت سروکار ندارند، استفاده می‌کنند).

موضوع رابطه میان فعالیت‌های نظامی و غیرنظامی، اهمیتی ویژه در بحث‌هایی که میان نظریه‌پردازان جنگ اطلاعاتی و صاحب‌نظران حقوق بین‌الملل درمی‌گیرد دارد. یک پیش‌فرض اساسی در حقوق بین‌الملل وجود دارد که مقرر می‌سازد این دو حوزه می‌باید تا جایی که امکان دارد از یکدیگر جدا نگه داشته شوند، دراین‌باره، به‌طور ویژه به اموال فیزیکی نظامی و اموال فیزیکی غیرنظامی اشاره می‌شود که توانمندی نظامی را تداوم می‌بخشد یا عملیات‌های نظامی را پیش می‌برند. اما این تفکیک‌ناپذیری فزایندهٔ فناوری و زیرساخت نظامی و غیرنظامی، روند در حال ظهور دیگری است (Virillio and Lotringen, 1983; Levidow and Robins, 1989). برخی افراد چه‌بسا اجرای «دیسیپلین[2] نظامی» در این حوزه‌ها را گامی مثبت قلمداد می‌کنند، اما جهان شمار زیادی از نمونه‌های تفکرات ضعیف و کم‌مایه‌ای را تجربه کرده است که هیچ توجهی به آن محدودیت‌های انسانی که سیطره استعاره‌های نظامی به‌وجود آورده‌اند ندارد. این هم‌گرایی میان زیرساخت نظامی و غیرنظامی و در نتیجه، هم‌گرایی میان منافع نظامی و اقتصادی چه‌بسا آشکارا چالشی است که رژیمِ فعلیِ حاکم بر قوانین جنگی را به نابودی می‌کشاند.

دلیل این وضعیت نیز بسیار واضح است. توسعه سازوکارهای اجرایی قوانین جنگی به‌قدری شکننده است که به دولت‌ـ ملت‌ها فرصت می‌دهد همین نظام شکننده حقوق بین‌الملل را نابود سازند.

---

1. World Wide Web
2. Dicipline

۱-۹ جنگ اطلاعاتی

آنچه در حال حاضر شاهدیم امکان دارد درهم‌آمیختگی عمیق جهان‌های نظامی و غیرنظامی باشد. تشریح این امکان یا احتمال در بخش اعظم ادبیاتی که در مورد جنگ اطلاعاتی وجود دارد، منعکس شده است. به‌نظر می‌رسد موازنه بحث به نفع موضوع جنگ اطلاعاتی که به‌مراتب گسترده‌تر از پیشبرد روابط میان دولت- ملت‌هاست به هم خواهد خورد. جنگ اطلاعاتی نیز به بافتارهای نظامی سنتی‌تر محدود نمی‌شود. آنچه امروز به چالش کشیده می‌شود، برداشت‌های سنتی از مقوله‌های «نظامی» و «جنگ» است (Darnton and Rattanaphol, 2003).

بعضی نویسندگان، دیدگاه‌های خود را درباره گستره جنگ اطلاعاتی تشریح کرده‌اند. برای مثال، جنگ اطلاعاتی ممکن است موارد ذیل را دربرگیرد:

۱. دریچه نرم‌افزاری کنترل شبکه‌های همگانی،
۲. حمله به شماره‌گیری‌های انبوه،
۳. کنترل الکترونیکی بر رادیو یا تلویزیون،
۴. نظارت با دوربین‌ها،
۵. بمب منطقی،
۶. تغییر فرمول‌های پزشکی ـ درمانی یا اطلاعات،
۷. حمله هماهنگ به پست‌های الکترونیکی،
۸. تغییر مسیر بودجه یا داده‌های بانک‌های فاسد،
۹. دستبرد زدن به اطلاعات شخصی و مسدودسازی آنها،
۱۰. ویروس‌ها یا کرم‌های رایانه‌ای،
۱۱. مسدودسازی اطلاعات،
۱۲. ایجاد اختلال در زیرساخت فرماندهی و کنترل نظامی یک کشور،
۱۳. دست‌کاری یا ایجاد اختلال در زیرساخت‌های غیرنظامی (مبادلات کالا یا سرمایه، برق، سیستم کنترل ترافیک، حمل‌ونقل هوایی).

هرچند این موارد، در نشریه‌ای که زیر نظر برنامه تحقیقاتی فرماندهی و کنترل وزارت دفاع آمریکاست درج شده، اما تقریباً همه آنها با پیمودن راهی طولانی از

عملیات‌های نظامی سنتی که به‌طور مستقیم جان افراد یا انهدام ساختارها و دارایی‌ها را هدف قرار می‌دهند، فاصله گرفته‌اند. این فهرست که گرنبرگ (1997، 6-3 .PP) برشمرده است، نمونه بارز آن چیزی است که بسیاری از نویسندگان در مورد گستره جنگ اطلاعاتی سخن به میان می‌آورند (Erbschloe, 2001).

علاوه‌بر این فهرست، انواع دیگری از فعالیت‌ها وجود دارد که در بالا ذکر نشده است، این فعالیت‌ها عبارت‌اند از:

۱. اقدامات پنهانی در دستگاه‌های سخت‌افزاری که همه افراد به آنها دسترسی دارند.

۲. اقدامات پنهانی با نفوذ به نرم‌افزارهایی که همه افراد به آنها دسترسی دارند.

۳. حمایت مالی و ارتباط یافتن با شبکه‌هایی که امکان نظارت و کنترل همه‌جانبه و فراگیر را فراهم می‌آورند.

۴. تمرکز و تسلط بر صنایع مربوط به رسانه‌ها.[1]

به‌این‌ترتیب، مفهوم «نبرد»[2] از دوره گروسیوس یک دور کامل زده و به نقطه اول بازگشته است. درگیرودار بحث‌های گیج‌کننده‌ای که مترجمان لاتین به انگلیسی در مورد ریشه‌شناسی واژه «جنگ»[3] مطرح می‌ساختند، گروسیوس این مفهوم را وضع و تشریح کرد (Grotius, 1682).[4] نبرد، مفهوم گسترده‌ای بود. این مفهوم درست در راستای همان مباحثی است که من در آنها چیزی شبیه آن را مطرح می‌سازم: «جنگ چیست؟ دعوا با توسل به زور است ... وضعیتی از امور است که همه جنگ‌ها با هر وصف و خصیصه‌ای را دربرمی‌گیرد ... جنگ‌های تن‌به‌تن[5] از شمول این تعریف خارج نمی‌شوند ... چرا که این نوع جنگ‌ها نیز بر وجود اختلاف میان دو شخص دلالت دارند». تحلیل ریشه‌شناسانه‌ای که گروسیوس ارائه داد، همان مسیر لاتین واژه جنگ را پی گرفت و واژه Bellum را از این ریشه‌شناسی استخراج کرد. عجیب آنکه، اگر گروسیوس در

---

1. High Industry Concentration Ratios For Media
2. Warfare
3. War

۴. واژه "War" در انگلیسی ترجمه واژه لاتین واژه "Bellum" است.

5. Single Combats

بررسی واژه War از تحلیل ریشه شناختی تبعیت کرده بود، شاید در این مورد نیز مفهوم گسترده‌ای را مطرح می‌کرد.

جنگ همان آشوب،[1] نفاق، زدوخورد و یا به آشوب یا نفاق کشاندن است. در انگلیسی قدیم، ترجمه واژه لاتین Bellum معمولاً «کشمکش»[3] و «زدوخورد»[4] بود (OED, 1989).

در زمانی که حقوق جنگ در میان دولت‌ـ ملت‌ها رواج یافت، دولت‌ـ ملت‌ها این کار گروسیوس را به‌عنوان بنیانی کلیدی در تدوین حقوق جنگ قلمداد کردند و جنبه عملیاتی بدان بخشیدند. ازاین‌رو، مدت‌هاست که مفهوم جنگ، گستره معنایی محدودی داشته است و همه تصور می‌کنند که «جنگ» معطوف به میدان نبرد است. اگر ما برای رسیدگی به امور بازیگران غیردولتی به حقوق بین‌الملل جدیدی نیاز داشته باشیم، گروسیوس نقطه عزیمتی را به‌دست می‌دهد که با شرایط آنها نیز تناسب دارد. دیدگاهی که به‌تازگی درمورد جنگ اطلاعاتی ارائه شده است ما را به معنای واقعی کلمه به یاد معنای اصیل واژه «جنگ» انداخته است.

غیرنظامی کردن نبرد[5] و موضوعات نظامی فقط در سطح فناوری روی نداده است. غیرنظامی‌سازی فناورانه‌ای وجود دارد که در ابتدا برآمده از مؤلفه‌های ذیل بوده است:

۱. **عوامل مرتبط با هزینه**: توسعه سخت‌افزارهای نظامی خاص به‌شدت هزینه‌بر و گران‌اند و اگر از این اقلام بتوان در مصارف عمومی بهره‌برداری کرد، آنگاه هزینه‌ها را می‌توان به‌نحو چشمگیری کاهش داد.

۲. **ایدئولوژی اقتصادی**: رقابت و نیروهای بازار بهترین شیوهٔ تخصیص اقتصادی را به‌وجود می‌آورند و استفاده از منابع نیز باعث می‌شود کسانی که آن سخت‌افزار نظامی خاص را تولید می‌کنند تمایل لگام‌گسیخته‌ای به مصرف بیشتر داشته باشند و برای کسب سود اقتصادی بیشتر، این تحولات را به‌سمت بازار غیرنظامی سوق دهند.

---

1. Confusion
3. Struggle
4. Strife
5. Civilianisation Of Warfare

به‌این‌ترتیب، ما نمونه‌های جذابی از تحولات نظامی را سراغ داریم که در ابتدا در امور نظامی کاربرد داشتند، ولی پس از مدتی به درون حوزه عمومی (غیرنظامی) راه یافتند. این نمونه‌ها عبارت‌اند از: رایانه‌های شخصی و کاهش چشمگیر در اندازه و وزن رایانه‌ها (ارتش برای پیشبرد برنامه‌های فضایی و موشکی خود ناگزیر بود قطعات سخت‌افزارهای رایانه‌ها را تاحدامکان کوچک‌تر و مینیاتوری سازد)؛ سیستم‌های اطلاعاتی جهانی (ارتش برای توسعه تسلیحات دقیق به سیستم موقعیت‌یاب جهان‌گستر نیاز داشت)؛ و اینترنت (ارتش برای انجام عملیات‌های نظامی ـ که فقط مرزهای ملی را دربرنمی‌گرفتند بلکه چه‌بسا گستره جهانی نیز داشتند ـ به یک سیستم ارتباطاتی جهانی نیاز داشت).

برخی حتی پا را فراتر می‌گذارند و معتقدند در تمامی سطوح فرهنگی، سیاسی، اقتصادی و سازمانی، پیوندهایی به‌مراتب عمیق‌تر میان جهان‌های نظامی و غیرنظامی وجود دارد: مدل‌های رایانه‌ـ محور جنگ، کار و یادگیری، حتی هنگامی‌که کاربر را به تفکر وامی‌دارد، می‌تواند ارزش‌های نظامی را ترویج و تبلیغ نماید. در تمامی آن شیوه‌ها، ما در حال حاضر به‌سمت یک جامعه اطلاعاتی نظامی حرکت می‌کنیم؛ این جامعه به‌مراتب بیش از آنچه بخواهیم اذعان کنیم، زندگی‌مان را احاطه کرده است ... در هر دو حوزه (ارتش و صنعت)، «تشکیلات روانی‌ـ فیزیکی آدمی به‌طور کامل، خود را با مقتضیات این جهان، ابزارها و ماشین‌های موجود در آن ـ و در یک کلام، با یک «کارویژه» فردی ـ انطباق می‌دهد. دیسیپلین به‌شدت به مشروط‌سازی عقلایی عملکردها و به تنظیم رفتارهای یکپارچه و پیش‌بینی‌پذیر گرایش دارد (Levidow and Robins, PP. 159-160).

این وضعیت، سناریویی از جنگیدن را نمایش می‌دهد که ناآگاهانه، ماهرانه و به‌طور بی‌وقفه، نقش اساسی هر شخصی را به «کارویژه‌ای» در درون یک سیستم بزرگ‌تر تقلیل می‌دهد؛ سیستمی که حداقل برای مشروعیت بخشیدن به تعقیب خودخواهانه قدرت و سود اقتصادی، از استعاره‌های نظامی (و در عمل، از پارادایم‌های نظامی) استفاده می‌کند. به‌این‌ترتیب ما چه‌بسا نوعی دگرگونی فرهنگی بنیادینی را تجربه می‌کنیم که فرهنگ‌های نظامی و انسانی را درهم می‌آمیزد و البته در این آمیزه، فرهنگ نظامی غلبه دارد (Virilio and Lotringer, 1983).

دیدگاه غربی دمکراسی مبتنی‌بر نمایندگی، پیامد جانبی ناخوشایندی نیز دارد. رهبرانی که (براساس اصول حقوق بین‌الملل) به فعالیت‌های سرکوبگرانه و غیرقانونی روی می‌آورند، می‌توانند ادعا کنند که به نمایندگی از آن رأی‌دهندگان غیرنظامی که آن دولت را انتخاب کردند یا امکان انتخاب آن دولت برایشان فراهم بود، اقدامات ذکر شده را انجام می‌دهند. بنابراین، سایر بازیگران غیردولتی می‌توانند عقب‌نشینی کنند و این استدلال را مطرح سازند که تمامی آن رأی‌دهندگان غیرنظامی به خاطر انتخاب دولت موردنظر مقصرند. این امر نشان می‌دهد بازیگران غیردولتی چندان هم مایل نیستند تصمیم‌گیری و اختیارات به کسانی که خواهان اعمال قدرت به نام انتخاب‌کنندگان هستند واگذار شود. این اصول به شهروندان هشدار می‌دهد که سخت مراقب اقدامات دولت‌هایشان باشند.

بنابراین، ما نباید تعجب کنیم که در حال حاضر شاهد تحولی چشمگیر و بزرگ در فعالیت‌های نظامی هستیم؛ به‌گونه‌ای که این‌گونه فعالیت‌ها، حوزه‌ها و فعالیت‌های غیرنظامی را نیز دربرمی‌گیرند. این موضوع درباره بازیگران دولتی که علیه اهدافی وسیع‌تر از عملیات‌ها و پرسنل نظامی دشمنان به انجام عملیات‌های روانی و اطلاعاتی مبادرت می‌ورزند، بسیار صدق می‌کند. «جنگ علیه تروریسم» که در حال حاضر جریان دارد، جنگی علیه مجموعه‌ای نامشخص و ابهام‌آلود از بازیگران غیردولتی است که گفته می‌شود هیچ تمایزی میان اهداف نظامی و غیرنظامی قائل نیستند و درواقع به‌علت تفکیک‌ناپذیری فزاینده حوزه‌های نظامی و غیرنظامی به پرهیز از این تمایزگذاری روی آورده‌اند.

تمامی این تحولات، چالش‌های دشواری را در سال‌های آینده برای حقوق بین‌الملل ایجاد می‌کند. حقوق بین‌الملل در مباحث خود درباره جنگ، بیش از هر چیز، توجه خود را به رفتار نظامی دولت معطوف ساخت، ازاین‌رو تنش میان وضعیت بالفعل[1] حقوق بین‌الملل و وضعیت آرمانی آن باعث شده است اصول عام قوانین جنگ که در سطح گسترده‌ای پذیرفته می‌شوند دائماً گسترش‌یابند.

اما درهرحال، افزایش چشمگیر گستره جنگ اطلاعاتی در این اواخر، موضوعات

1. Actual State

بسیار بیشتری را مطرح کرده که باید مورد توجه قرار گیرند. زیرا حقوق بین‌الملل به‌اقتضای ماهیتی که دارد، سخت به دنبال نیل به آرمانی است که برای خود تعریف کرده است. این تنش سخت میان «وضعیت موجود»، که مبتنی‌بر دولت ــ ملت‌های موجود و حاکمیت آنهاست، از یک‌سو و تغییرات در نظم بین‌المللی فعلی ازسوی‌دیگر، مشکلات سهمگینی را برای حقوق بین‌الملل و قوانین جنگ ایجاد می‌کند. جنگ اطلاعاتی و ظهور پیامدهای جهانی شدن تنها این تنش را تشدید می‌کند. توسل روزافزون بازیگران غیردولتی به خشونت چه‌بسا ممکن است فقط و فقط وضع موجود را تحکیم و تثبیت کند. فالک این تنش را این‌گونه بررسی کرده است: ما در دوره‌ای تاریخی زندگی می‌کنیم. در این دوره، همه به‌خوبی آگاه‌اند که بقا، رونق و امنیت به دگرگونی‌های اجتماعی و سیاسی اساسی بستگی دارد ... این دگرگونی‌ها دنیای بدون جنگ را ـ به‌عبارت بهتر، ... جهانی که توانمندی‌های گسترده جوامع تمامت‌خواه[1] را تقویت نمی‌کند ... جهانی که آسیب‌پذیری‌ها در برابر اشکال سرکوبگرانه دولت را افزایش نمی‌دهد ـ به‌وجود آورده‌اند ... یکی از موانع اصلی بر سر راه این دگرگونی، فرایند نامطلوبِ تثبیتِ «وضعِ موجودِ» سیاسی و اجتماعی است ... (Falk, 1966, P. 172).

۲-۹ قوانین جنگ

قوانین جنگ هیچ‌گاه مجموعه مشخصی از «تفکرات حقوقی پذیرفته شده» نبوده‌اند و البته افراد مختلف نیز معانی متفاوتی از آنها ارائه می‌دهند.

بااین‌حال تحلیل طیف وسیعی از آثاری که به دلایلی به موضوع قوانین جنگ می‌پردازند، مرا به این دیدگاه رهنمون می‌سازد که بحث در مورد معنای اصطلاح «قوانین جنگ» در سه بعد متفاوت صورت می‌گیرد؛ این استدلال در جدول ۱-۹ تشریح شده است.

---

1. Totalitarion

جدول ۱-۹ حقوق جنگ ـ ابعاد معنا

بعد	مسائل
منازعه مسلحانه در برابر منازعه غیرمسلحانه	● قواعد در مورد توسل به منازعه (مسلحانه) ● اداره و پیشبرد منازعه (مسلحانه).
بازیگران دولتی در برابر بازیگران غیردولتی	شرکت‌کنندگان یا رزمندگان چه کسانی‌اند؟ آیا قواعد حقوقی، صرفنظر از جایگاه رسمی شرکت‌کنندگان به اجرا درمی‌آیند؟
آسیب مادی به افراد یا اموال در برابرِ آسیب غیرمادی به افراد یا اموال	برخی معتقدند جنگ فقط با اقداماتی سروکار دارد که آسیب‌های مادی (فیزیکی) به افراد یا اموال را به بار می‌آورند

این دیدگاه که «محدودیت‌هایی فراروی پیشبرد جنگ وجود دارد»، دیدگاه جدیدی نیست و به دوران باستان بازمی‌گردد (Roberts and Guelff, 1983, PP.2-3). پس از اندیشه‌های دوران میانه (به‌ویژه دیدگاه‌های گروسیوس) اواخر قرن نوزدهم اولین نمونه‌های تدوین پیمان‌ها و معاهدات مهم را تجربه کرد. سَلَف اصلی کنوانسیون‌های ۱۹۴۹ ژنو، کنوانسیون ۱۸۶۴ ژنو بود (Pictect and et. al., 1952). این کنوانسیون به دنبال تأسیس صلیب سرخ، به‌طور خاص برای رسیدگی به امور کسانی که در میدان‌های جنگ مجروح می‌شوند، تنظیم گردید. ژنو شهر کوچکی است. در این شهر، افرادی فعالیت داشتند که به‌طور ویژه در مورد موضوع حقوق بین‌الملل و توسل به زور در روابط بین‌الملل مطالعه می‌کردند. البته، خود ژنو نیز از همان ابتدا یک جمهوری مستقل بود و پس از آنکه طی جنگ‌های ناپلئونی به اشغال درآمد، به سوئیس ملحق شد. ژنو مقر دفتر صلح بین‌الملل[1] نیز بود. این نهاد در سال ۱۸۹۲ تأسیس شد و نقش فعالانه‌ای در برگزاری کنفرانس اول صلح لاهه در سال ۱۸۹۹ و کنفرانس دوم صلح لاهه در سال ۱۹۰۷ (که چند سال بعد از کنفرانس اول تشکیل شد) و تنظیم اسناد آنها ایفا کرد (Darnton, 1989, PP.xiii-xiv). دفتر صلح بین‌الملل در سال‌های اخیر نیز همچنان به فعالیت‌های خود ادامه داده است. این نهاد به تشویق تلاش‌ها درزمینه طرح مسئله قانونی بودن سلاح‌های هسته‌ای در دیوان بین‌المللی دادگستری در لاهه کمک کرده است (Mothersson, 1992).

1. International Peace Bureau

آنچه درباره کاربست‌پذیری موضوع حقوق بین‌الملل درزمینه جنگ اطلاعاتی، اهمیتی تعیین‌کننده و حیاتی دارد این است که حقوق بین‌الملل موجود (که بیش از ۱۰۰ سال قدمت دارد) تا چه اندازه می‌تواند برای وضعیت جدیدی که در زمان انعقاد پیمان‌ها، معاهدات و پروتکل‌های متعدد اصلاً پیش‌بینی نشده بود کاربرد داشته باشد. احتمال بروز این وضعیت، از همان آغاز در اذهان تدوین‌کنندگان پیش‌نویس این موافقت‌نامه‌ها نقش بسته بود؛ زیرا قاعدتاً آنها از آهنگ شتابان وقوع تغییرات فناورانه و ابتکار و نبوغ انسان در طرح‌ریزی شیوه‌های جدید آسیب‌رسانی به دیگران به‌خوبی آگاه بودند. آشکارترین اقدام صریح در پذیرش یک اصل حقوقی در هنگام جنگ که در زمان‌های بعد از آن و حتی تا امروز نیز کاربرد یافت، همان «اصلی» است که به شرط مارتنز[1] معروف شده است و در مقدمهٔ کنوانسیون چهارم لاهه (۱۹۰۷) درزمینه احترام به قوانین و قواعد عرفی جنگ زمینی آمده است: تا زمانی که آیین‌نامه کامل‌تری درزمینه قوانین جنگ صادر نشده است، طرف‌های عالی‌رتبه متعاهد مقتضی می‌دانند اعلام کنند در مواردی که در شمولیت مقررات مصوب آنها قرار ندارد، سکنهٔ نواحی جنگی و طرف‌های متخاصم همچنان تحت حمایت باقی بمانند و براساس قاعده اصول حقوق ملل با آنها رفتار شود. زیرا این اصول از قوانین انسانی، نداهای وجدان عمومی و کاربردهایی که در میان ملل متمدن جاافتاده و تثبیت شده‌اند نشئت می‌گیرند.[2]

شرط مارتنز بی‌تردید خصیصه‌ای اساسی درزمینه اجرای حقوق بین‌الملل تبیین می‌نماید. برخی از حقوق‌دانان کاربست‌پذیری این شرط را زیر سؤال برده‌اند و استدلال کرده‌اند که این شرط «تنها» در مقدمه معاهده آمده است، اما باید گفت که شرط مارتنز مورد توجه قرار گرفته و دیوان دادگستری بین‌المللی نیز در قضایای حقوقی به‌طور کامل از این مقدمه استفاده کرده و بدان استناد نموده است (Singh and Mcwhinng, 1989, P. 47). برخی دولت‌گرایان افراطی[3] مفهوم حاکمیت دولت را به این معنا می‌دانند که اگر اقدامی در حقوق بین‌الملل به‌طور صریح ممنوع اعلام شد، این ممنوعیت، قانونی و مجاز است. گرینبرگ (1997، P.17) یکی از نمونه‌های دیدگاه دولت‌گرایی افراطی را این‌گونه بیان می‌کند: «شاید به‌علت جدید

---

1. De Martens Clause

۲. این دیدگاه در منابع بسیاری تکرار شده است، ولی آن را می‌توان در این اثر یافت: Darnton, 1989, PP.1-7

3. Ultra-statists

بودن بسیاری از مؤلفه‌های این فناوری‌ها هیچ قید و شرطی در حقوق بین‌الملل به‌طور صریح آنچه را ما در حال حاضر در جنگ اطلاعاتی می‌شناسیم، ممنوع اعلام نمی‌کند. این نبود ممنوعیت به نوعی معنادار نیز است، زیرا ازآنجاکه براساس قاعده‌ای کاملاً کلی، حقوق بین‌الملل نیز جنگ اطلاعاتی را منع نمی‌کند، جنگ اطلاعاتی مجاز است. اما این نبود ممنوعیت نیز حکم حقوقی[1] به‌شمار نمی‌آید، زیرا حتی در جایی که حقوق بین‌الملل مدعی رسیدگی به امور تسلیحات یا فناوری‌های خاص نیست، باز هم اصول کلی آن درزمینه استفاده از آن تسلیحات و فناوری‌ها موضوعیت خواهد داشت و قابل اجرا خواهد بود».

بعدها دیوان بین‌المللی دادگستری شرط مارتنز را مورد توجه قرار داده است. رأی دیوان در مورد قابلیت اجرای[2] حقوق بشردوستانه که به اتفاق‌آرا صادر شد، ضربه‌ای مهلک بر دولت‌گرایان افراطی وارد آورده است: «من محدودیت‌هایی را که در پاراگراف ۱(C) [از این رأی] مقرر گردیده‌اند، اموری می‌دانم که نباید به آنها اعتنا کرد» (ICJ, 1996, Dissenting Opinion of Judge Weeramantry, Priliminary Observations (C) (iv).

شرط مارتنز به شکلی نسبتاً متفاوت در پروتکل الحاقی به کنوانسیون ژنو (۱۲ آگوست ۱۹۴۹) و پروتکل اول سال ۱۹۷۷ درباره حمایت از قربانیان منازعات مسلحانه بین‌المللی عملاً بار دیگر درج شد. در ماده (۲) ۱ پروتکل حمایت از قربانیان منازعات مسلحانه بین‌المللی به‌طور خاص آمده است:

«در مواردی که مشمول این پروتکل یا سایر موافقت‌نامه‌های بین‌المللی نمی‌شوند، غیرنظامیان و نظامیان همچنان تحت حمایت و در لوای آن اصول حقوق بین‌الملل که برآمده از عرف جاافتادهٔ اصول انسانیت و نداهای وجدان عمومی هستند قرار دارند».

مسئلهٔ کاربردپذیری حقوق بین‌الملل برای اَشکال جدید جنگ، سال‌هاست درباره تسلیحات هسته‌ای مطرح بوده است. دولت‌های دارنده تسلیحات هسته‌ای، برخورداری از این تسلیحات و استفاده احتمالی از آنها را با این دیدگاه دولت‌گرایانه افراطی که تسلیحات هسته‌ای فی‌نفسه در حقوق بین‌الملل غیرقانونی اعلام نشده بلکه حقوق بین‌الملل با برقراری آنها موافقت داشته است ـ توجیه کرده‌اند. اگر حقوق بین‌الملل،

---

1. Dispositive
2. Applicatility

تسلیحات هسته‌ای را ممنوع اعلام نکرده است احتمالاً تا حدودی به این دلیل بوده که دولت‌های هسته‌ای قطعاً با هرگونه اقدام از این دست مخالفت می‌کنند. مجمع عمومی سازمان ملل متحد نیز این موضوع را به دیوان بین‌المللی دادگستری ارجاع داد و رأی مشورتی این نهاد را جویا شد؛ رأی مشورتی دیوان در مورد «قانونی بودن تهدید به استفاده از سلاح‌های هسته‌ای یا استفاده از سلاح‌های هسته‌ای» نیز به تاریخ ۸ جولای ۱۹۹۶ صادر گردید (ICJ, 1996). این رأی، دو پاراگراف مهم دارد که کاربردپذیری شرط مارتنز در حال حاضر را به‌خوبی نشان می‌دهد:

«... ۸۵. دیوان هم‌اکنون با توسل به کاربردپذیری اصول و قواعد حقوق بشردوستانه درزمینه تهدید احتمالی به استفاده از سلاح‌های هسته‌ای یا استفاده از سلاح‌های هسته‌ای، متذکر می‌شود که گاهی اوقات تردیدهایی در این‌باره با این توجیه ابراز شده‌اند که این اصول و قواعد در زمانی پیش از اختراع سلاح‌های هسته‌ای شکل گرفته‌اند و کنفرانس‌های ژنو در سال‌های ۱۹۴۹ و ۱۹۷۷-۱۹۷۴ که به‌ترتیب کنوانسیون‌های ۱۹۴۹ ژنو و دو پروتکل الحاقی به آنها را به تصویب رسانده‌اند به‌طور خاص به سلاح‌های هسته‌ای نمی‌پردازند. اما تنها اقلیتی کوچک چنین دیدگاهی را مطرح می‌سازد و از آن دفاع می‌کند. به‌نظر اکثریت غالب دولت‌ها و نویسندگان، هیچ تردیدی در مورد کاربردپذیری حقوق بشردوستانه درزمینه تسلیحات هسته‌ای نمی‌تواند وجود داشته باشد.

...

۸۷. سرانجام، دیوان به شرط مارتنز اشاره می‌کند، موجودیت و کاربردپذیری مستمر این شرط نباید مورد تردید و شبهه قرار گیرد. این شرط، درواقع یک اصل مسلمی به‌شمار می‌آید که براساس آن، اصول و قواعد حقوق بشردوستانه می‌توانند در حوزه سلاح‌های هسته‌ای اعمال شود».

به‌این‌ترتیب، به‌عنوان یک نقطه عزیمت مفید، دلایل موجهی وجود دارد که تصریح نماییم اگر جنگ اطلاعاتی واقعاً شکل جدیدی از نبرد به‌شمار می‌آید، پس حقوق بین‌الملل عرفی در ارتباط با این حوزه به‌صورت آنچه معمولاً حقوق بشردوستانه نامیده می‌شود، کاربردپذیر و قابل اعمال است. حقوق بین‌الملل عرفی سه جنبه بنیادی دارد که در شرط مارتنز بیان شده است:

۱. کاربردهای ریشه‌دار و جاافتاده آن در میان ملل متمدن جهان،
۲. برآمده از قوانین مبتنی‌بر انسانیت،
۳. برآمده از نداهای وجدان عمومی.

بنابراین، برخلاف دیدگاهی که گرینبرگ[1] ارائه داد، حتی اگر هیچ‌یک از اسناد فعلی حقوق بین‌الملل هم جنگ اطلاعاتی را فی‌نفسه غیرقانونی اعلام نکند، هیچ تردیدی درباره کاربردپذیری شرط مارتنز و سایر ارکان حقوق بشردوستانه از جمله نداهای وجدان عمومی، وجود ندارد.

البته، یک الزام حقوقی نیز وجود دارد چرا که امضاکنندگان پروتکل اول ۱۹۷۷ ژنو، به‌موجب ماده (۳۶)، موضوع کاربردپذیری حقوق بین‌الملل را مورد توجه قرار داده‌اند:

ماده (۳۶) سلاح‌های جدید. درزمینه «مطالعه، توسعه، کسب یا اقتباس از یک سلاح جدید و ابزار یا شیوه جدید نبرد»، طرف‌های متعاهد بلندپایه متعهد می‌گردند که مشخص سازند آیا این پروتکل یا هر قاعده دیگر حقوق بین‌الملل که برای طرف‌های متعاهد بلندپایه به اجرا درمی‌آید، استفاده از آن سلاح را در برخی شرایط یا در هر شرایطی ممنوع اعلام می‌کند یا خیر.(۲)

کاربردپذیری ذاتی حقوق بین‌الملل در حوزه جنگ اطلاعاتی، امری معقول و منطقی است و البته می‌تواند از جمله جلوه‌های اساسی «کاربردها میان ملل متمدن» و «نداهای وجدان عمومی» به‌شمار آید. این دیدگاه را در ابتدا تعداد زیادی از نویسندگانی که تعریف موسعی از مفهوم جنگ اطلاعاتی ارائه می‌دهند، مطرح کرده‌اند. تلاش‌های جدی چندانی برای ارزیابی معیار «نداهای وجدان عمومی در قبال یک موضوع حقوقی» انجام نگرفته است. یک نمونه از این تلاش‌های اندک، تأسیس نهادی به نام هیئت حل اختلاف جنگ هسته‌ای مستقر در لندن[2] در سال ۱۹۸۵ است که شواهد زیادی از شاهدان مختلف در این موضوع مشخص را جمع‌آوری کرده و آنها را در هیئت‌های تخصصی حقوقی مورد ارزیابی قرار داده است. تعدادی از منابع اطلاع‌رسانی درباره وجدان عمومی نیز مورد توجه قرار گرفت؛ به این معنا که این هیئت حل اختلاف

1. Greenberg and et. al.
2. London Nuclear Warfare Tribunal

رسیدگی به امور نمایندگان گروه‌های مذهبی، نمایندگان گروه‌های جنبش‌های توده‌ای و اعتراضی، دیدگاه‌های مربوط به مسئولیت کیفری افراد، و سایر تفاسیر موجود در پیمان‌های متعدد را در صلاحیت خود قرار داد. نمونه دیگر، دیوان بین‌المللی دادگستری بود که این دیوان، داده‌های چشمگیری را از مردم دریافت می‌کرد، اما رأی خودش را صادر می‌کرد (Grief, 1997, P. 681 at 684, note 24). «دیوان حدود دو میلیون امضا از سازمان‌ها و افراد متعدد از ۲۵ کشور دریافت کرده است. به‌علاوه، سایر محموله‌های امضاها به‌قدری حجیم بوده‌اند که دیوان به‌طور فیزیکی نمی‌تواند آنها را دریافت کند. ازاین‌رو، این امضاها در سایر «مراکز بایگانی و اسناد» نگهداری شده‌اند. متصدی امور بایگانی دیوان مجموع کل امضاها را افزون‌بر سه میلیون امضا تخمین زده است» ((JIC), 1996, Dissenting Judgement by Judge Weeramantry, I).

بررسی اجمالی برخی از مهم‌ترین هنجارهای عرفی در حقوق بین‌الملل نیز مفید به‌نظر می‌رسد که در ذیل می‌آیند:

۱. **اصل تمایزگذاری**:[1] تسلیحات و تاکتیک‌ها باید بین اهداف[2] نظامی و غیرنظامی آشکارا تمایز بگذارد. کاربرد آنها نیز باید به «اهداف نظامی» محدود شود. هرچند خسارت غیرمستقیم به غیرنظامیان و اهداف غیرنظامی لزوماً غیرقانونی نیست، اما نبردی که فاقد این تمایزگذاری باشد به‌خودی‌خود غیرقانونی است.

۲. **اصل تناسب**:[3] تسلیحات و تاکتیک‌ها باید متناسب با هدف نظامی‌شان باشند. تسلیحات و تاکتیک‌های نامتناسب، زائد و به معنای دقیق کلمه غیرقانونی‌اند.

۳. **اصل قانونمندی**:[4] تسلیحات و تاکتیک‌ها نباید هیچ‌یک از قواعد معاهده حقوق بین‌الملل را که برای هر دو طرف جنگ الزام‌آور است، نقض کنند.

۴. **اصل ضرورت**:[5] تسلیحات و تاکتیک‌هایی که در اقدام «توسل به زور» به‌کار گرفته می‌شوند به‌نحو معقولی می‌باید برای تحقق هدف نظامی‌شان ضروری باشند. هیچ کاربرد مفرط و غیرضروری

---

1. Principle of Discrimination
2. Targets
3. Principle of Proportionality
4. Principle of Lawfulness
5. Principle of Nesessity

زور، قانونمند نیست حتی اگر خساراتی که به بار می‌آورد محدود به محیط زیست باشد.

۵. **اصل انسانیت**:[1] هیچ سلاح یا تاکتیکی را نمی‌توان مبتنی‌بر حربه‌ای ساخت که چه با به بار آوردن مرگ دیرگذر یا زجرآور و چه به شکلی حساب شده با ایجاد ترس و وحشت شدید، رنج‌های غیرضروری بر قربانیانش تحمیل کند. به همین دلیل تسلیحات و تاکتیک‌هایی که سم می‌پراکنند یا بیماری اشاعه می‌دهند یا خسارت‌های ژنتیکی به بار می‌آورند کلاً به خودی خود غیرقانونی‌اند، زیرا این تسلیحات اثراتی دارد که به مکان و زمان خسارت در میدان نبرد محدود نمی‌شود. چنین ممنوعیتی، در شرایط جدید حتی به ایجاد اختلال در محیط زیست به هر شکلی که باشد کشیده شده است.

۶. **اصل بی‌طرفی**: هیچ سلاح یا تاکتیکی را نمی‌توان مبتنی‌بر حربه‌ای ساخت که به انسان‌ها، اموال و محیط زیست طبیعی کشورهای بی‌طرف آسیب وارد سازد. یک کشور در صورتی بی‌طرف است که دولت آن خودش اعلام بی‌طرفی کند و سیاست عدم جانب‌داری درخصوص با منازعه مسلحانه (از جمله پرهیز از هرگونه عضویت در اتحادها و ائتلاف‌ها) را در پیش گیرد (Darnton, 1989, PP.1-5 to 1-6).

حقوق بین‌الملل عرفی چارچوب‌های مفیدی را ارائه می‌دهد که براساس آنها می‌توان کاربردپذیری حقوق بین‌الملل در حوزه وسیع جنگ اطلاعاتی را مورد ارزیابی و قضاوت قرار داد. نبرد نظامی سنتی در شکل آرمانی آن به خسارت‌هایی محدود می‌شود که در میدان جنگ در زمان و مکان نبرد و خارج از مناطق غیرنظامی وارد می‌آمد. علاوه‌بر این، تحمیل حداقل رنج و درد رعایت می‌شد و دسترسی و امدادرسانی به مجروحان نیز امکان‌پذیر بود. هرگونه انحراف از آن سناریو، امکان نقض اصولی را که در بالا بیان شد، مهیا می‌سازد.

براساس این نوع تحلیل، واضح است که جنگ اطلاعاتی چالش‌های جدیدی را برای اصول حقوق بین‌الملل ایجاد می‌کند. اگر به فهرستی که از گرینبرگ در بالا آورده شد بنگریم، می‌توان مشاهده کرد که تفاوت آشکاری میان نبردهای سنتی و جنگ اطلاعاتی وجود دارد؛ به‌عبارت دقیق‌تر، گذشته از برخی عملیات‌های اطلاعاتی خاص، آنچه جنگ اطلاعاتی در ذهن مجسم می‌سازد، عملیات‌هایی است که اساساً بر زمان عاجل و مکان

1. Principle of Humanity

نزدیک یک میدان نبرد تمرکز و تأکید دارند. عملیات‌های جنگ اطلاعاتی به‌گونه‌ای حساب شده با این هدف طراحی می‌شود که در اجرای سیستم‌های عملیاتی طرف مقابل تأخیر ایجاد کند. در این میان، می‌توان به تأثیرات ذیل اشاره کرد: ایجاد اختلال در زنجیره‌های تدارکات و لجستیک، اشاعه اطلاعات غلط و ایجاد تغییر در عقاید، ایستارها و رفتار. ازاین‌گذشته، بسیار آشکار است که بسیاری از عملیات‌های اطلاعاتی زیرساخت‌ها را هدف قرار می‌دهند. آیا این نوع عملیات می‌تواند مرگبار باشد، یا آیا می‌تواند خساراتی جدی بر افراد و دارایی‌ها وارد سازد؟ در بسیاری از موارد این تأثیر در همان موعد نبرد بروز نمی‌کند بلکه چه‌بسا ممکن است در یک مقطع زمانی طولانیتر و حتی مدت‌ها پس از نبرد، خود را نشان دهد. تا آنجا که من اطلاع دارم، این مسئله به شکل رسمی و در قالب حقوقی مورد بررسی و توجه قرار نگرفته است. ازاین‌رو، گمانه‌زنی در این زمینه تنها براساس روایت‌های نامعتبر امکان‌پذیر خواهد بود.

سال ۱۹۹۰، در ایالات متحده آمریکا، بروز یک اشتباه نرم‌افزاری شمار زیادی از خطوط تلفن‌هایی را که فاصله‌های طولانی از هم داشتند از کار انداخت (Lee, 1991). این وضعیت به گسترش تغییرات جزئی در حوزه نرم‌افزارهای آزمون نشده انجامید. اما یکی دیگر از تغییرات چشمگیرتر این بود که به‌منظور کاهش هزینه‌ها (و در نتیجه، افزایش سود)، شبکه‌های مخابراتی جدیدتری طراحی شد که میزان بار اضافی در آن سیستم‌ها کمتر بود و به‌این‌ترتیب، این اقدام، آستانه آسیب‌پذیری شبکه را ارتقا داد. یکی از ویژگی‌های مشترک تحولات اخیر در به‌کارگیری فناوری اطلاعات و ارتباطات، ایجاد زنجیره‌های عرضه و خطوط ارتباطی طولانیتر و درعین‌حال ظریف‌تر بوده است که آستانه آسیب‌پذیری را بالا برده‌اند. بنابراین، جنگ اطلاعاتی به موضوعی جدی‌تر برای اقتصاد مبدل می‌گردد، زیرا نصب و به‌کارگیری فناوری اطلاعات و ارتباطات، هر روز مدرن‌تر می‌شود. این رویداد منحصربه‌فرد در حوزه مدارهای مخابراتی و تلفنی، برخی از پیامدهای جنگ اطلاعاتی را که به‌طور بالقوه حاد و جدی نیز می‌باشد برجسته ساخت. به‌طور قطع نمونه‌های آشکار دیگری نیز در تجربیات ما زیاد دیده شده که از وجود اشتباه‌ها و نارسایی‌ها در رایانه‌ها و نرم‌افزارها حکایت دارد (Lee, 1991; Neumann, 1995).

وقتی خطوط عرضه در تأسیسات غیرنظامی نظیر سوپرمارکت‌ها و سوخت‌رسانی،

طولانی و ظریف‌اند[1] و افراد نیز «سبک‌های زندگی»ای مبتنی‌بر مدگرایی دارند، اختلال در بخش فناوری ارتباطات می‌تواند به بروز شورش داخلی جدی در یک مقطع زمانی به نسبت کوتاه منتهی شود. این نوع اقدام حساب شده و عمدی، تعدادی از اصول حقوق بشردوستانه را آشکارا نقض می‌کند.

جدول ۲-۹ برخی از شیوه‌هایی را که جنگ اطلاعاتی با به‌کارگیری آنها می‌تواند اصول بشردوستانهٔ مندرج در حقوق بین‌الملل درزمینه جنگ را نقض کند برمی‌شمارد.

جدول ۲-۹ اصول حقوق بشردوستانه و جنگ اطلاعاتی

اصل	نقض‌هایی که احتمال می‌رود جنگ اطلاعاتی به بار آورد
تمایزگذاری	بسیاری از سناریوهایی که برای «جنگ اطلاعاتی» فرض گرفته می‌شوند، به‌طور مستقیم این اصل را نقض می‌کنند. زیرا سناریوها دقیقاً معطوف به غیرنظامیان و زیرساخت‌های غیرنظامی‌اند
تناسب	بسیاری از اشکال جنگ اطلاعاتی هیچ هدف نظامی مشخصی ندارند. ازاین‌رو، آنها با هیچ چیزی نمی‌توانند تناسب داشته باشند.
قانونمندی	بسیاری از اشکال پیشنهادی جنگ اطلاعاتی به‌خودی‌خود تمامی قوانین جنگی را نقض نمی‌کنند، اما طیف وسیعی از قواعد حقوق بین‌الملل درزمینه اموری نظیر ایجاد اختلال و منحرف‌سازی ارتباطات را نقض می‌کنند.
ضرورت	بسیاری از اشکال جنگ اطلاعاتی معطوف به اهداف نظامی نیستند، ازاین‌رو، آنها ضروری هم نیستند.
انسانیت	بسیاری از اشکال جنگ اطلاعاتی در میدان نبرد به اجرا درنمی‌آیند و با اختلال‌هایی که به بار می‌آورند چه‌بسا می‌توانند وحشت و ترس فراگیر را ایجاد کنند و باعث ایجاد اختلال در عرضه کالاهای اساسی و کمک‌های بشردوستانه شوند.
بی‌طرفی	با توجه به ماهیت ابهام‌آلود اطلاعات و جنگ اطلاعاتی، به‌سختی می‌توان اطمینان حاصل کرد که عملیات‌های اطلاعاتی از تأسیسات کشورهای بی‌طرف استفاده نمی‌کنند و خطرات و زیان‌های جانبی را در کشورهای بی‌طرف به بار نمی‌آورند.

چالش بزرگ‌تری که فراروی حقوق بین‌الملل است، ورود بازیگران و

1. Thin

مشارکت‌کنندگان غیردولتی به آن چارچوبه حقوقی است که اصول حقوق بشردوستانه به‌وسیله آن اعمال می‌شود. بعضی از گروه‌ها یا افراد ازآنجاکه ذاتاً بازیگر دولتی نیستند، معتقدند اصول کلی اخلاق و نداهای وجدان عمومی در اقداماتشان کاربرد ندارد؛ اما این دیدگاه، ادعایی مزورانه است. البته بازیگران دولتی نیز ناگزیرند در برابر اقدامات خشونت‌آمیز و سرکوبگرانهٔ خود علیه دیگران به‌مراتب پاسخ‌گوتر باشند. این همان تزویری است که بازیگران غیردولتی در بیشتر موارد برای توجیه رفتارهایی که نداهای وجدان عمومی قاعدتاً آنها را وحشیگرانه قلمداد می‌کند به‌کار می‌برند. معقول نیست که اقدامات وحشیگرانهٔ بازیگر غیردولتی را تروریسم قلمداد نکنیم؛ اما همگان به این وضعیت ناخوشایند یقین دارند که امروز تروریسم دولتی گسترده‌تر از تروریسم غیردولتی است.

درمورد حقوق بین‌الملل خصوصی باید گفت، افراد و شرکت‌هایی که به دلایل متعدد از جمله تشکیل جماعت‌های سایبر یا اجتماعات سایبر در سطح بین‌المللی فعالیت می‌کنند و هر روز بر شمار آنها افزوده می‌شود، در عرصه‌های تدوین، اعمال صلاحیت و اجرای معاهدات در حوزه فعالیت‌هایشان کلاً با خلأ مواجه‌اند. بعضی از بازیگران تجاری غیردولتی از جمله شرکت‌ها و بانک‌ها این خلأ را با به‌کارگیری کارت‌های اعتباری تا حدودی پر کرده‌اند.

۳-۹ مسائل اساسی

این فصل برخی از مسائل بنیادی در مورد رابطه میان حقوق بین‌الملل و جنگ اطلاعاتی را بیان کرده است. بی‌تردید، اصول فعلی و کاربردپذیری آنها حقوق بین‌الملل موجود را به چالش می‌کشد.

دستاوردهای بارزی وجود دارد که برای توسعه چارچوب‌های حقوقی در سطح بین‌المللی و توجه آن به جنگ اطلاعاتی ضرورت داشته‌اند:

۱. بازیگران دولتی، این مسئولیت اولیه را برعهده می‌گیرند که تضمین دهند خودشان برطبق «قاعده اصول حقوق ملل» عمل می‌کنند، چرا که این اصول از رویه‌های ملل متمدن، قوانین انسانیت و نداهای وجدان عمومی سرچشمه می‌گیرند.

۲. دستاوردهای جدید، بازیگران غیردولتی را در چارچوب همان اصول قوانین انسانیت قرار می‌دهند.

۳. دستاوردهای جدید، حقوق بین‌الملل را به‌گونه‌ای تقویت می‌کند که بسیاری از عملیات‌های جدیدِ جنگ اطلاعاتی را پوشش دهد.

۴. دستاوردهای جدید، نهادهای بین‌المللی را در دسترس عموم قرار می‌دهد («در دسترس عموم» بدین‌معناست که امکان دسترسی، مستقل از اجازه دولت‌های حاکمیت‌دار است) تا حقوق بین‌الملل را اجرا کنند (در این برهه به‌نظر می‌رسد که بسیاری از جنبه‌های جنگ اطلاعاتی صرفاً با نظام‌های حقوقی ملی یا سازوکارهای معاهده‌ایِ[1] خصوصی کنترل می‌شود).

۵. ظهور جنگ اطلاعاتی به شکل گسترده به این معنا خواهد بود که تعامل میان حقوق بین‌الملل و حقوق داخلی حتی بیشتر خواهد شد. یکی از الگوهای مفید درزمینه مدیریت این تعامل که از بررسی قانونیت تسلیحات هسته‌ای و نقش‌آفرینی حقوق داخلی نیز به‌دست می‌آید، گسترش رویه رسیدگی به پرونده‌های حقوقی داخلی در بریتانیاست که در آنها به حقوق داخلی و حقوق بین‌الملل به موازات یکدیگر استناد می‌شود (Manson, 1995).

بااین‌حال، با وجود آنکه حقوق بین‌الملل فعلی درزمینهٔ مقابله با تهدیدهای جنگ اطلاعاتی با ضعف‌هایی جدی روبه‌روست، تحلیلی که در بالا ارائه شد، نشان می‌دهد که مجموعه حقوقی ریشه‌دار و جاافتاده‌ای وجود دارد که می‌توان آن را در مورد جنگ اطلاعاتی به اجرا درآورد. نگران‌کننده‌ترین شکاف‌ها به دو دلیل ایجاد می‌شود: اولاً، بسیاری از انواع عملیات‌های جنگ اطلاعاتی صبغه غیرنظامی دارند؛ ثانیاً، به‌طور بالقوه مشکلات انسانی فراگیر و جدی‌ای را به بار می‌آورند.

---

1. Contractual

پی‌نوشت‌ها

۱. بسیاری هوگو گروسیوس (۱۶۴۵-۱۵۸۳) را آغازگر تفکر مدرن در مورد قوانین جنگ می‌دانند. اثر بزرگ او، با عنوان *در مورد حقوق جنگ و صلح* (On the Law of War and Peace) نخستین بار در سال ۱۶۲۵ به زبان لاتین در پاریس منتشر شد. امکان دسترسی به این اثر به زبان انگلیسی به اشاعه هرچه بیشتر و گسترده‌تر اندیشه‌های وی کمک کرده است. نگاه کنید به: Grotius, 1682.

۲. اندیشه‌هایی که در این فصل مطرح شدند، در دومین کنفرانس «جنگ اطلاعاتی» اروپا در جولای ۲۰۰۳ مورد بحث قرار گرفت. در طول بحث‌ها، آشکار شد که حداقل دو کشور (بریتانیا و ایالات متحده آمریکا) احتمالاً چنین ارزیابی‌هایی را از ماده سی‌وششم انجام داده‌اند، اما نتایج ارزیابی‌های آنها محرمانه‌اند!

منابع و مآخذ

Darnton, G (ed), (1989). *The Bomb and the Law: London Nuclear Warfare Tribunal Evidence, Commentary and Judgment*, Stockholm: Alva and Gunnar Myrdal Foundation.

Darnton, G and S. Giacoletto, (1992). Information in the Enterprise: It's More Than Technology Burlington, MA: Digital Press.

Darnton, G. and J. Rattanaphol, (2003). RMA Applied to Thailand: European Conference on Information Warfare, 2nd edition, Reading, England: MCIL, June.

Dixon, N.F., (1976). On the Psychology of Military Incompetence, London: Jonathan Cape.

Erbschloe, M., (2001). Information Warfare: How to Survive Cyber Attacks, New York: Osborne/ Mc Graw-Hill.

Falk, R.A., (1966). 'Historical Tendencies, Modernizing and Revolutionary Nations, and the International Legal Order', in R.A, Falk and S.H. Mendlovitz (eds), The Strategy of World Order, New York: New York Law Fund, Vol. 2, PP. 172-88.

Greenberg, L.T., S.E., (1997). Coodman, and K.J Soo Hoo, Information Warfare and International Law, Washington, DC: National Defense University Press.

Grief, N., (1997). 'Legality of the Threat or Use of Nuclear Weapons', *International and Comparative Law Quarterly*, 46.

Grotius, H., (1982). The Most Excellent Hugo Grotius. His Three Books Treating of the Rights of War and Peace, London: Thomas Basset, Text Readily available on line. See, for example. http://www.ecn.bris.ac. uk/het /grotius/law 2.pdf.

ICJ, (1996). Advisory Opinion on the Legality of the Threat or Use of Nuclear weapons, Hague: International Court of Justice.

Lee, L., (1991). The Day the phones Stopped: the Computer Crisis – the What and Why of It, and How we can Beat It, New York: Donald I. Fine, Inc.

levidow, L. And K, Robbins, (1989). 'Towards a Military Information Society?' in L. Levidow and K. Robbins (eds), Cyborg Worlds: the Military Information Society, London: Free Association Books.

Manson, R., (1995). The Pax Legalis Papers: Nuclear Conspiracy and the Law, Oxford: Jon Carpenter.

Mothersson, K., (1992). From Hiroshima to the Hague : a Guide to the World Court Project, Geneva: International Peace Bureau.

Neumann, P., (1995). Computer-related Risks, London: Addison-Wesley Publishing Company.

OED, (1989). Oxford English Dictionary, 2nd edn, Oxford: Oxford University Press.

Pictet, J.S., F. Siordet, C. Pilloud, J.P. Schoenholzer, R.J. Wilhelm and O.H. Uhler (eds), (1952). Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field: Commentary, Geneva: Information Committee of the Red Cross. (This Set is What is Usually Supplied on Asking for a Copy of the 'Geneva Conventions'.)

Roberts. A and R. Guelff (eds), (1989). Documents on the Laws of War, Oxford: Clarendon Press.

Singh, N and E. McWhinney, (1989). Nuclear Weapons and Contemporary International law, 2nd Revised Edition, Dordrecht: Marinus Nijhoff Publishers.

Tofts, D. A. Jonson and A. Cavallaro (eds), (2002). Prefiguring Cyberculture: an Intellectual History, Cambridge, MA: MIT Press

Virilio, P. And S. Lotringer, (1983). Pure War, New York: Semiotext(e).

بخش سوم

دیدگاه‌های کشورها

فصل دهم انقلاب در امور نظامی، شیوه روسی

فانوریوس پانت‌لگیانیس*

۱-۱۰ بررسی تاریخی

در اواسط دهه ۱۹۷۰، به‌ویژه بعد از آنکه ایالات متحده بـه دنبـال تجربـهٔ نـاگوار جنـگ ویتنام سیاستی انزواطلبانه‌تر در پیش گرفـت، ارتـش شـوروی سـابق بـه قدرتمنـدترین ماشین نظامی در جهان مبدل شده بـود. امـا از ایـن تـاریخ بـه بعـد، یعنـی زمـانی کـه کشورهای غربی وارد عصر تسلیحات هوشـمند و فـوق دقیـق گردیدنـد، ارتـش شـوروی به‌نسبت ضعیف‌تر شد. تا قبل از نیمه دوم دهـه ۱۹۸۰، واضـح بـود کـه ارتـش شـوروی موقعیت برتر خود را از دست داده بود؛ برای مثال، در افغانستان، ارتش شوروی نتوانست عملیات مؤثری را برای مقابله با موشک‌های ضدهوایی استینگر[1] آمریکا بیابد.

در این فضا بود که نیروی نظامی «جدید» فدراسیون روسیه (سـال ۱۹۹۲) تأسـیس شد و جانشین قوای مسلح متحد[2] کشورهای مستقل مـشترک‌المنـافع گردیـد. از دسـت رفتن برخی از مناطق مرزی اتحاد شوروی سابق به از دست رفتن بخـش چـشمگیری از مدرن‌ترین سخت‌افزارهای نظامی، زیرساخت‌ها و بخش‌هـایی از سیـستم پدافنـد هـوایی اتحاد شوروی منتهی شد.

در حال حاضر، آمادگاه‌های نظامی در سراسر روسیه هنـوز زرادخانـه‌هـای عظیمـی دارند، اما تعداد تسلیحات جدید و به‌روز رو به کاهش است و نیروهای نظامی نیز آموزش چندانی نمی‌بینند. برای مثال، به‌علت کمبود سوخت، خلبانان روسی به‌طور متوسـط ۲۵ ساعت در سال پرواز می‌کنند، این در حالی است که خلبانـان کـشورهای غربـی حـداقل

---

* Fanourios Pantelogiannis

1. Stinger
2. Unified Armed Forces

سالیانه ۲۰۰ ساعت تمرین پرواز دارند. تنها در حدود ۷-۵ درصد از سازوبرگ نظامی ارتش روسیه، تجهیزاتی است که به‌عنوان ادوات جدید طبقه‌بندی می‌شوند (عمر آنها کمتر از ده سال است)؛ علاوه‌بر این، تنها کمتر از یک‌چهارم این تجهیزات و سخت‌افزارهای نظامی می‌توانند در میدان نبرد مورد استفاده قرار گیرند.(۱)

مدل‌های مدرن این تجهیزات، اقلام ذیل را دربرمی‌گیرند: ۴۰ درصد تانک‌ها و ادوات جنگی پیاده‌نظام، ۳۰ درصد موشک‌های زمین به هوا و سیستم‌های توپخانه‌ای و ۲ درصد هلی‌کوپترها. برای مثال، خلبان‌های روسی هنوز هم با هلی‌کوپترهای قدیمی Mi-8 و Mi-24 پرواز می‌کنند.

بنابراین، ارتش روسیه، تا حد زیادی همچنان محصول نیمه اول قرن بیستم بود. بااین‌حال هرچند روسیه به‌خوبی نتوانسته است خود را با واقعیت‌های فنی مدرن انطباق دهد، ولی به‌نظر نمی‌رسد این وضعیت مانع از آن شود که روس‌ها به فکر احتمال وقوع جنگ در آینده و یا جنگ اطلاعاتی نباشند. از همان دهه ۱۹۶۰، متفکران شوروی در زمره اولین کسانی بودند که پیامدهای آنچه را انقلاب در امور نظامی یا انقلاب علمی‌ــ فنی، یا به زبان روسی، ان.تی.آر[1] نامیدند، امری مسلم انگاشتند و به تحلیل آن پرداختند.(۲) درواقع، این نویسندگان روسی بودند که اصطلاح انقلاب در امور نظامی را وضع کردند و این مفهوم را پیش از آنکه نویسندگان و افسران آمریکایی به‌کار ببرند، بسط و گسترش دادند.(۳) در تعریف روس‌ها، سلاح‌های جدید تسلیحات بیولوژیکی یا روان‌پریشگر، اشکال صرفاً نوآورانه اطلاعات و سایر فناوری‌هایی را که با هدف «بی‌ثبات‌سازی جامعه مورد نظر از درون» طراحی شده بودند دربرمی‌گرفت. درواقع، نویسندگان فعلی روسیه که در این زمینه قلم‌فرسایی می‌کنند به همان اندازه که پیشینیانشان در دهه‌های ۱۹۷۰ و ۱۹۸۰ به تفکر می‌پرداختند، ژرف‌اندیش‌اند.

با وجود این، انقلاب در امور نظامی روسیه در حد یک تأمل صرفاً نظری متوقف نشد. جنگ‌های اخیر، به‌ویژه منازعات در کوزوو و افغانستان و عملیات «آزادی عراق» نشان دادند که بهره‌مندی و حفظ ارتش‌های بزرگ در حال حاضر، دیگر کاربرد و استفاده چندانی ندارد. انقلاب در امور نظامی که با هدف آماده‌سازی نیروهای نظامی

---

1. N.T.R.

برای شرایط بسیار دشوار طراحی شده بود، خود را در عملیات‌های سریع و سرنوشت‌ساز استقرار نیرو نشان داد و از میزان آسیب‌پذیری نیروها کاست. الکساندر گلتز،[1] یکی از کارشناسان نظامی در گفت‌وگو با هفته‌نامه *اژندلنی ژورنال*[2] اظهار می‌دارد: «یکی از افسران ارشد نظامی آمریکا گفت عملیات بمبارانی که آمریکا در افغانستان انجام می‌دهد هیچ نتیجه‌ای به بار نخواهد آورد؛ سربرآوردن ناگهانی طالبان آمریکایی‌ها را شوکه کرد». آناتولی مدتسکی[3] می‌افزائد: «توانایی آمریکا در انجام علمیات جنگی به روش کنترل از راه دور، به‌گونه‌ای که بدون روی آوردن به اقدامات پرهزینه اشغال سرزمین بتواند دشمنان خود را نابود سازد، برای رهبران نظامی ما بسیار عبرت‌انگیز بوده است».(۴)

براساس‌این، مقامات روسی پی بردند که در جنگ‌های آینده روسیه، قلمرو سرزمینی نقش تعیین‌کننده‌ای در آرایش وسیع نیروهای زرهی ایفا نخواهد کرد و در نتیجه، «سیستم فرماندهی، کنترل، ارتباطات، رایانه‌ها، عملیات جاسوسی، نظارت و شناسایی» و «سیستم‌های جنگ الکترونیک»، نحوه تخصیص منابع دفاعی را که کمیاب هم می‌باشند تعیین خواهند کرد. عصر جنگ‌های فراگیر و در نتیجه، ارتش‌های بزرگ برای روسیه در شرف به‌سر آمدن است.

اتخاذ این استراتژی به‌طورقطع مستلزم تغییرات گسترده‌ای بود. پس از سال‌ها اجرای اصلاحات نظامی در حوزه امور مجازی، کارشناسان می‌گویند که کرملین هم‌اکنون در نیل به اهداف خود جدی است. امور نظامی پایه دفاع از سرزمین قرار گرفت و توجه ارتش از کمیت نفرات و تسلیحات به کیفیت نیروها و تجهیزات معطوف شد. در همین چارچوب، این فصل پیشنهاد می‌کند که وضعیت فعلی انقلاب در امور نظامی روسیه، عوامل تأثیرگذار بر آن و پیامدهای منطقه‌ای و بین‌المللی آن به‌طور اجمالی بررسی شود. ارزیابی وضعیت فعلی و فرایند تاریخی این موضوع به ما کمک خواهد کرد تا تناقضات موجود در تفکر ستاد کل ارتش روسیه را درک کنیم و برآوردی از روندهای احتمالی در آینده ارائه دهیم. انجام اصلاحات در وزارت دفاع ـ با این هدف که وضعیت

---

1. Alexander Goltz
2. Ezhenedelng Journal
3. Anatoly Medetsky.

ارتش فعلی بهبود یابد ـ غیرممکن است. مشکل از خود وزارتخانه نیست. بلکه دلیل اصلی، این است که این وزارتخانه به‌منظور تعقیب اهداف دیگری تأسیس شد. ارتش فعلی روسیه، میراث ارتش قرن گذشته را که همه منابع ملی را بسیج می‌کرد بر دوش می‌کشد. آنچه در حال حاضر وجود خارجی ندارد، یک ارتش مدرن برخوردار از فناوری‌های برتر است که آن منابع را به خدمت گیرد و همه آنها را زیر پوشش قرار دهد. تنها یک راه برای برون‌رفت از این وضعیت وجود دارد: ایجاد تحول در ارتش و تبدیل آن به یک ارتش کاملاً حرفه‌ای، این ارتش می‌باید براساس شالوده‌ای جدید ایجاد شود و اهداف جدیدی را برای خود تعریف کند، به‌گونه‌ای که با مقتضیات قرن جدید نیز هماهنگ باشد. آیا روسیه شهامت سیاسی و منابع مالی کافی و قابل توجه برای تحقق این مقصود را خواهد داشت؟ جان کلام همین است.(۵)

۲-۱۰ وضعیت فعلی روسیه در حوزه انقلاب در امور نظامی و پیامدهای بین‌المللی آن

البته، سؤالی که می‌توان مطرح کرد این است که چرا دیدگاه‌های روسیه درباره انقلاب در امور نظامی را باید مطالعه کرد؟ اولاً، در چند سال اخیر، ما شاهد دگرگونی‌های چشمگیری در ماهیت جنگ‌ها و نبردها بوده‌ایم. همان‌طور که انگلس[1] خاطرنشان کرد، تقویت توان نظامی هر کشور وابسته به شرایط مادی (اقتصادی)، منابع انسانی و تسلیحاتی است که این عوامل به‌نوبه خود، به کیفیت و اندازه جمعیت مورد نظر و به فناوری‌هایی که در اختیار دارد، بستگی دارد.(۶) بدون بررسی این عوامل به‌هیچ‌وجه نمی‌توان شناخت دقیقی درخصوص سازمان‌دهی و نفرات نیروهای مسلح یک کشور و سیاست و استراتژی نظامی آن کسب کرد. این سؤال که کشوری مثل روسیه به چه جنبه‌های خاصی از انقلاب در امور نظامی می‌تواند دست یابد، تأثیر ژرفی بر روندهای آینده جنگ و صلح در سطح جهان خواهد داشت. روس‌ها اظهار می‌دارند که در آینده نزدیک، اصلی‌ترین رقبا در حوزه انقلاب در امور نظامی، کشورهای آمریکا، روسیه، ژاپن و شاید چین خواهند بود و به احتمال زیاد، در این میان آمریکا در مقام نخست قرار خواهد

1. Engles

گرفت و سه کشور دیگر به‌ترتیب جایگاه‌های بعدی را به خود اختصاص خواهند داد.(۷)

بسیاری از اولین درخواست‌ها برای ایجاد تحولات بنیادین در امور نظامی از جانب نظریه‌پردازان نظامی شوروی مطرح شد. این نظریه‌پردازان در آن زمان، تأثیر به‌اصطلاح «انقلاب نظامی ـ فنی» را بررسی می‌کردند. افسرانی از قبیل ارتشبد اُرگاکف[1] از افسران بلندپایه اتحاد شوروی، توجه همگان را به آن فناوری‌های تسلیحاتی که در آغاز قرن جدید در دسترس قرار می‌گرفتند جلب کرد و در این راستا استدلال می‌کرد که این فناوری‌های جدید درمجموع باعث بروز دگرگونی در نبردهای نظامی خواهند شد و این دگرگونی‌ها به‌قدری وسیع و همه‌جانبه خواهند بود که می‌توان آنها را با رویداد رواج کاربرد تسلیحات هسته‌ای در میدان جنگ مقایسه کرد. در نوامبر ۱۹۹۷، آندری نیکلایف[2] نماینده دومای دولتی و یکی از ژنرال‌های ارتش روسیه در مجله *راشا جورنال*[3] نوشت: «درصورتی‌که تصویر مشخصی از کلیت جنگ مدرن در اختیار نداشته باشیم، چگونه می‌توانیم توان نظامی‌مان را بهبود بخشیم؟» دو سال بعد، با تدوین پیش‌نویس دکترین نظامی روسیه در سال ۱۹۹۹ پاسخ به این پرسش داده شد: «ویژگی‌های بارز جنگ منطقه‌ای در آینده عبارت خواهد بود از: نبرد نظامی در تمامی حوزه‌ها، عملیات‌های ائتلافی، استفاده انبوه از تسلیحات هدایت‌شونده دقیق و اشکال الکترونیک و غیرالکترونیک نبرد، حملات گسترده به‌سراسر قلمرو طرف‌های مخالف برای برآورده‌سازی نیازهای ارتش، به‌ویژه درزمینه تولید نسل جدیدی از جنگ‌افزارها. علاوه‌بر این، می‌باید پایگاه مستقل تولید علم و فناوری در حوزه امور نظامی تأسیس شود. اولویت‌ها در این حوزه عبارت‌اند از: ارتقای کیفی تسلیحات استراتژیک، توسعه سیستم‌های کنترل آتش و سیستم فرماندهی، کنترل، ارتباطات و اطلاعات، تقویت سیستم هشدار استراتژیک، جنگ الکترونیک، تسلیحات غیرهسته‌ای دقیق و متحرک و پشتیبانی اطلاعاتی از آنها، کاهش و استانداردسازی تعداد تسلیحات و تجهیزات گوناگون».

---

1. Marshal Orgakov
2. Andrea Nikolayov
3. The Russia Journal

چند سال بعد، کاپیتان ولادیمیر بارینوف[1] دستیار ارشد نماینده نظامی روسیه در سازمان آتلانتیک شمالی (ناتو) در کمیته مشترک ناتو و روسیه اعلام کرد: «ویژگی‌های بارز توسعه تسلیحات تاکتیکی که نیروهای نظامی روسیه، سخت دنبال می‌کنند، بدین‌قرار است: راه‌اندازی سیستم‌های تسلیحاتی بسیار دقیق، ... تولید تجهیزات پیشرفته مخصوص سربازان که عناصری از سیستم‌های جنگی و لجستیکی نسل جدید را در خود دارند، توسعه جنگنده پیشرفته‌ای که در خط مقدم کاربرد دارد و توانمندی آن به‌حدی گسترش یافته که قادر است با اهداف مستقر در زمین نیز درگیر شود. روندهای اصلی در توسعه کلی نیروی دریایی در ده سال آینده عبارت‌اند از: تولید زیردریایی‌های چندمنظورهٔ نسل جدید، طراحی و تولید انبوه کشتی‌های دارای کاربرد دوگانه که می‌توانند حملات بسیار دقیقی را اجرا کنند و تسلیحات ضد زیردریایی را با خود حمل کنند، تولید هواپیماهای جنگی که قابلیت فرود بر روی زمین و کشتی را دارا باشند، توسعه بیشتر تجهیزات فرماندهی، کنترل و ارتباطات».

متأسفانه تعداد دقیق، ظرفیت و توانایی رزمی ارتش روسیه همچنان موضوعی رازآلود و پرابهام به‌شمار می‌آید و جزء اسرار نظامی روسیه باقی‌مانده است؛ ازاین‌رو، ما تنها به‌وسیله برآوردها و آمارها می‌توانیم به آنها استناد کنیم و اطلاع یابیم. اما همه پذیرفته‌اند که ارتش روسیه به اصلاحات فوری احتیاج دارد. برای مثال، روسیه برای مقابله با چالش‌های امنیتی در آسیای میانه و سایر مناطق به یک نیروی نظامی پرتحرک و مجهز به فناوری‌های برتر نیاز دارد به‌گونه‌ای که این نیرو بتواند در مناطق و نواحی متعدد به‌طور هم‌زمان بجنگد و در ظرف مدتی کوتاه و به‌محض صدور فرمان جنگ، سربازان خود را در منطقه مورد نظر مستقر سازد. سامان‌دهی و ایجاد این نوع نیروی نظامی، دقیقاً همان وعده‌ای است که پوتین رئیس‌جمهور روسیه در نوامبر ۲۰۰۱ به ژنرال‌های خشمگین از وضعیت موجود قول داد عملی سازد.

اما در حال حاضر، وضعیت نیروهای مسلح روسیه چندان آرمانی نیست و با شرایط مطلوب فاصله دارد. هم‌اکنون هزینه‌های تسلیحاتی ۶ درصد کل بودجه دفاعی روسیه را تشکیل می‌دهد. این در حالی است که در کشورهای عضو ناتو این رقم، حداقل ۲۰

1. Captain Vladimir Barinov

درصد است. از زمان فروپاشی اتحاد شوروی، نیروهای مسلح روسیه به‌غیراز تعداد معدودی هواپیمای IL-765 هیچ هواپیمای ترابری نظامی خریداری نکرده‌اند. علاوه‌بر این، در حوزه فناوری‌های جدید از قبیل هلی‌کوپترهای KA-52 نیز هیچ تولید انبوهی انجام نگرفته است. بخش اعظم بودجه‌ای که ارتش دریافت کرده، صرف نگهداری و ارتقای سطح تسلیحات و فناوری‌های قدیمی شده است و بودجه اندکی به توسعه مدل‌های اصلی و نخستین[1] تسلیحات اختصاص یافته است. «اگر این وضعیت به مدت پنج یا شش سال دیگر نیز ادامه یابد، ارتش روسیه دیگر ارتشی نخواهد بود که بتواند از کشور دفاع کند، بلکه به یک موزه تبدیل خواهد شد».(۸)

تعداد ماهواره‌هایی که نیروهای فضایی روسیه در اختیار دارند، نصف ماهواره‌های فرماندهی فضایی ایالات متحده است.(۹) تعداد ماهواره‌هایی که روسیه هرساله از دور خارج می‌کند بیش از ماهواره‌هایی است که به فضا پرتاب می‌کند.(۱۰) وانگهی، ۷۰ درصد ماهواره‌های روسیه نیز در حال حاضر مدت مأموریت خدمت خود را افزایش داده‌اند و بنابراین مشخص نیست که آنها بتوانند وظایف اصلی خود از قبیل جاسوسی استراتژیک، اعلام هشدارهای اولیهٔ حملات موشکی و کارویژه‌های ارتباطاتی را انجام دهند. البته این وضعیت طبعاً ناشی از این واقعیت است که برنامه فضایی شوروی در دهه‌های ۱۹۶۰ و ۱۹۷۰ به نقطه کمال خود رسیده بود.

ازاین‌گذشته، بیشتر موشک‌های سنگین روسیه، که مدت‌هاست زمان کارکرد مطلوب و تضمین شدهٔ آنها سپری شده است، تا قبل از سال ۲۰۰۸ از رده خارج خواهند شد. موشک اس اس ۱۹ اس (استیلتو)[2] بعد از سال ۲۰۰۷ به‌سرعت به پایان دوران عملیاتی‌اش خواهد رسید.(۱۱) مدت زمان کارکرد موشک اس اس ـ ۲۴ (اسکالپل)[3] تا سال ۲۰۰۷ پیش‌بینی شده است و تعداد اندکی از موشک‌های اس اس ـ ۱۸ اس[4] و اس اس ـ ۲۵ اس[5] تا پایان سال ۲۰۱۰ برقرار خواهند ماند. تعداد موشک‌های بالستیک با قابلیت پرتاب

---

1. Proctotypes
2. SS-19s (Stileto)
3. SS-24 (Scalpel)
4. SS-18 (Scalpel)
5. SS-25s (Satan)

از دریا[1] طی دهه‌های آینده کاهش خواهد یافت زیرا عمر زیردریایی‌های حامل موشک‌های بالستیک روسی ـ که با سوخت هسته‌ای تغذیه می‌شوند ـ[2] به‌سر خواهد آمد.(۱۲) درمجموع، ۶۰ درصد موشک‌های بالستیک قاره‌پیمای روسیه عمر تضمین شدهٔ خود را سپری کرده‌اند. نیمی از زیردریایی‌های حامل موشک‌های بالستیک[3] (۷۵ درصد موشک‌های آنها) و بیشتر کلاهک‌های موشک‌های بالستیک قاره‌پیما حداکثر تا سال ۲۰۰۵ باید تعویض شوند. بعید است که روسیه بتواند موشک‌های جدیدی در این سطح تولید کند. این وضعیت باعث شده است که این کشور به تولید مدرن‌ترین سیستم‌های تسلیحاتی از قبیل موشک (Toplo-M SS-28s) روی آورد.(۱۳) رهبران روسیه امیدوار بودند که مسکو خواهد توانست هرساله ۳۰ فروند از این موشک‌های جدید را تولید کند، اما واقعیت این است که بیش از ۱۰ فروند در سال نمی‌تواند تولید کند.(۱۴) زیرساخت‌ها از نواقص بسیاری رنج می‌برند و تجهیزات و قطعات آنها نیز نیاز به تعمیر دارند.

در نیروی هوایی تا سال ۲۰۰۵ هیچ دورنمای مثبتی درزمینه جذب بودجه برای تأمین هواپیماهای جدید وجود نداشت.(۱۵) در نتیجه، روس‌ها توجه خود را به ارتقای سطح مدل‌های موجود معطوف ساختند. بر همین اساس، روس‌ها که سخت به دنبال افزایش توانمندی‌های هواپیماهای جنگی هوا به زمین خود بودند، کوشیدند جنگنده‌های MIG-29 را به صورتی درآورند که با استانداردهای Mig-29 UBT و Mig ـ ۲۹ Smt منطبق شوند. همین‌طور، بعد از این تدابیر، تعدادی از هواپیماهای Su-27 نیز به مدل "SU۲۷ IB" ارتقا خواهند یافت، به‌گونه‌ای که به‌عنوان هواپیماهای مخصوص عملیات‌های پرواز شناسایی و تهاجم به‌کار خواهند آمد. بعد از این پروژه، مقامات روسیه به فکر بهبود مدل‌های قدیمی هواپیماهای Su-24، Su-25 و MiG 31 افتادند. این پروژه‌ها نیز لاجرم راه‌حل‌هایی موقتی بیش نیستند. برطبق گفته‌های مقامات روسی، راه‌حل‌های واقعی در حال حاضر مطرح شده‌اند و آغاز اجرای پروژه‌های مربوط به آنها فقط به منابع مالی نیاز دارد. به‌موجب اصل به حداقل رساندن شمار مدل‌های هواپیمای مورد نظر، روس‌ها توجه خود را به تولید هواپیمای چندکارکردی

1. Sea- Launched Ballistic Missiles (SLBMs)
2. Ballistic Missile Submarines
3. SSBNs

Su-34 معطوف خواهند ساخت. این هواپیماها ساخته شده و مورد آزمایش نیز قرار گرفته‌اند و البته هواپیماهای اصلی نیروی هوایی روسیه خواهند بود. اگر دفاتر طراحی هواپیماهای MiG و یاکولف ـ دندوکف[1] به توافق برسند، یک هواپیمای آموزشی نیز به‌طور مشترک تولید خواهند کرد.(۱۶) در وهله بعد، احتمالاً مطالعات پژوهشی ـ علمی درزمینه تعیین توانمندی‌های بالقوه هواپیماهای جنگنده چندکارکردی ـ که پیشرفته‌ترین هواپیماهای اوایل قرن بیست‌ویکم به‌شمار می‌آیند و پشتیبانی از نیروهای نظامی (در میدان جنگ) را انجام می‌دهند ـ صورت خواهد گرفت. البته ناگفته نماند انجام این‌گونه مطالعات در چارچوب امکانات مالی موجود روسیه خواهد بود.(۱۷)

بااین‌همه، روسیه امروز فاقد نیروهایی است که بتواند با استفاده از تسلیحات متعارف برای مثال در برابر حمله فرضی چین در شرق دور از سرزمین‌اش دفاع کند. در پی انتقال فناوری نظامی از روسیه به چین، برخی از صاحب‌نظران روسی، از قبیل الکساندر شاراوین،[2] مدیر مؤسسه تحلیل‌های سیاسی و استراتژیک،(۱۸) هشدار می‌دهند که ارتش آزادی بخش خلق(۱۹) با شتابی هرچه تمام‌تر به نیرویی آماده‌تر از ارتش به‌روز نشده روسیه مبدل می‌شود. ازاین‌گذشته، تقریباً تمامی شهرهای اصلی روسیه و مراکز فرماندهی نظامی آن در مجاورت منطقه‌ای قرار دارد که با چین هم‌مرز است. ازاین‌رو، روسیه در حال حاضر، استفاده از زرادخانه تسلیحات هسته‌ای تاکتیکی را حتی درصورتی‌که وارد منازعه نظامی بزرگ با چین شود، بسیار بعید می‌داند. استفاده از نیروهای هسته‌ای غیراستراتژیک تنها در صورتی محتمل خواهد بود که مسکو با استفاده از تسلیحات هسته‌ای تاکتیکی دوربردتر، قلب سرزمین چین و شهرهای بزرگ این کشور را که دورتر از مرزهای مشترک دو کشور واقع شده‌اند تهدید کند. روسیه که به‌وجود این معضلات دفاعی در جبهه شرقی خود اذعان دارد چه‌بسا ممکن است نسل جدیدی از تسلیحات و تجهیزات هسته‌ای تاکتیکی کم‌خرج را تولید کند و با استفاده از سیستم‌های تاکتیکی و استراتژیک پرتاب موشک از جمله موشکِ با برد کوتاه و چهارصد کیلوگرمی اسکندر[3] ـ که جدیداً تولید کرده است ـ به‌سمت اهداف پرتاب کند.(۲۰)

---

1. Yavkovle-dondukov
2. Alexander Sharavin
3. Iskander

روسیه، علاوه‌بر تسلیحات متعارف، فناوری موشکی و هسته‌ای نیز صادر می‌کند. این موضوع مدت‌هاست که منشأ اختلاف‌نظر میان ایالات متحده آمریکا و روسیه بوده است، چرا که کاخ سفید بیش از همه به‌دلیل وضعیت فعلی موضوع هسته‌ای ایران، سیاست روسیه درزمینه انتقال فناوری را با نگرانی‌های بیشتری دنبال می‌کند. ایالات متحده آمریکا مدام در مورد خطرات تقویت توانمندی‌های نظامی چین نیز به روسیه هشدار داده است. اما روسیه در حال حاضر چین را بیش از همه فقط به‌عنوان یکی از منابع درآمد ارزی خود قلمداد می‌کند.

روی‌هم‌رفته، مجتمع نظامی صنعتی روسیه،[1] این توانمندی را دارد که با فروش زیرقیمت محصولات خود، عرضه‌کنندگان غربی را تضعیف کند؛ زیرا قیمت‌های فناوری تسلیحاتی روسیه، مانند دوران اتحاد جماهیر شوری سابق، ارتباطی با هزینه‌های واقعی تولید ندارد. هیچ آمار و ارقام دقیقی در مورد میزان یارانه‌های مستقیمی که به حدود ۱۷۰۰ شرکت دفاعی وابسته به دولت پرداخت می‌شود، وجود ندارد. گذشته از یارانه‌های غیرمستقیم از قبیل بهای نازل انرژی و اجاره که دولت با ارائه آنها قیمت تمام شده محصولات را به شکل تصنعی پایین می‌آورد، هزینه واقعی تولید چه‌بسا در عمل بالاتر از میزان سودی است که عاید این کشور می‌شود. همچنین، روس‌ها بی‌میل هم نیستند که حتی برخی از پیشرفته‌ترین تسلیحاتشان را (که بسیاری از آنها کیفیتی بسیار بالا دارند) صادر کنند. آنها در دفاع از این سیاست، استدلال می‌کنند که تداوم این فروش‌ها تنها راه تأمین مالی توسعه نسل بعدی جنگ‌افزارهای روسی را در پیش روی آنها می‌گذارد.(۲۱)

مجتمع نظامی صنعتی روسیه در عمل، ظرفیت مازاد زیادی دارد؛ اما هیچ فعالیت تولیدی انجام نداده است. حتی تولیدات مجتمع نظامی صنعتی برای بخش غیرنظامی نیز افت کرده است؛ زیرا کالاهایی که تولید می‌کند، آن‌چنان‌که باید و شاید کیفیتی ندارند که بتوانند با محصولات وارداتی مشابه رقابت کنند. پاول فلگنگاور[2] در مقاله‌ای که هفتم اکتبر ۱۹۹۸ در روزنامه *سگدنیا*[3] نوشت، استدلال کرد که مجتمع نظامی صنعتی

1. Military -Industrial Complex (MIC)
2. Pavel Felgengauer
3. Segodnya

روسیه تنها به‌صورت یک بخش کوچک، مجزا و با گسترهٔ تخصصی محدود می‌تواند به حیات خود ادامه دهد. اگر روسیه همچنان بر ادامه سنت شوروی‌ها مبنی‌بر تلفیق توسعه و تولید دستگاه‌های تلویزیون و دستگاه‌های هدایت پرواز از راه دور در قالب یک شرکت یکپارچه اصرار ورزد، آنگاه تلویزیون‌ها در هنگام استفاده به‌خودیخود منفجر خواهند شد و نیمی از بمب‌ها نیز به اهداف مورد نظر اصابت نخواهند کرد.

تجربه نشان می‌دهد که کارخانه‌های روسیه در وضعیتی نیستند که بتوانند تولید محصول جدیدی را با هدف رقابت در بازارهای غیرنظامی آغاز کنند. اما بااین‌حال، لوازم اصلی ابزارهای ماشینی به مقدار کافی موجود است و در چندین مورد حتی در عالی‌ترین سطوح دولتی نیز مدیران، مهندسان و دست‌اندرکارانی که اصلاً قصد ندارند نظام اداری کهنه شوروی و تأکید مفرط بر تحقیقات و توسعه را کنار بگذارند، مؤسسات و کارخانجات را طراحی می‌کنند.

درست برخلاف این دیدگاه‌های کهنه‌باورانه، دولت پوتین، درمجموع وضعیتی کاملاً متفاوت را به تصویر می‌کشد. سیاست نظامی‌ـ فنی دولت پوتین بر تحقیقات، توسعه، طراحی و اجرای مدل‌های جدیدی از سخت‌افزارهای نظامی تمرکز دارد و وضعیتی را مجسم می‌سازد که «ساختارهای علمی و طراحی» ناگزیر خواهند بود هزینه‌های حفظ تأسیسات بی‌ثمر را از جیب خود بپردازند. درحقیقت، ازآنجاکه توانمندی‌های روسیه در حوزه فناوری ممکن است به‌علت نبود سرمایه نتوانند از عهده تولید تسلیحات جدید برآیند[۲۲] این احتمال وجود دارد که (حداقل تا زمانی که منابع مالی لازم تأمین می‌شود) بازار طرح‌ها[1] و دانش فنی جایگزین بازار سخت‌افزارهای نظامی شود.[۲۳]

با وجود همه عواملی که در بالا ذکر شد، نباید تصور کرد که نیروهای روسیه در زمینه «انقلاب در امور نظامی» توفیق نیافته‌اند. نیروهای شوروی تلاش می‌کردند گوی سبقت را از همتایان آمریکایی‌شان بربایند و در بعضی موارد حتی پیشتاز نیز بوده‌اند. این کشور پس از سپری کردن دهه طاقت‌فرسای ۱۹۹۰ یک بار دیگر خیز برداشت. برای مثال، روسیه با اجرای دکترین نظامی پوتین توانست سیستم‌های تسلیحاتی از جمله موشک‌های بالستیک قاره‌پیمای Topol-M2 یا موشک‌های SS-27 را (که ایالات

1. Ideas

متحده آمریکا آنها را در اختیار ندارد یا هنوز بودجه لازم را برای توسعه آنها تخصیص نداده است) توسعه دهد.

ولادیمیر پوتین، پنج سال بعد از به قدرت رسیدنش، یعنی در ۱۷ نوامبر ۲۰۰۴، گفت روسیه به‌زودی سیستم‌های موشک‌های هسته‌ای جدیدی را مستقر خواهد ساخت که بر موشک‌های هر قدرت هسته‌ای دیگر برتری دارد. وی خاطرنشان کرد که «ما صرفاً به تحقیقات نمی‌پردازیم و جدیدترین سیستم‌های موشک‌های هسته‌ای را با موفقیت آزمایش می‌کنیم. من مطمئن هستم که در همین سال‌های آینده، ما به این تسلیحات مجهز خواهیم شد. این همان پیشرفت‌ها و سیستم‌هایی است که سایر دولت‌های هسته‌ای از آنها بی‌بهره‌اند و در چند سال آینده نیز به آنها دست نخواهند یافت».

مدل سیستمی که در دست بررسی بود، فاش نشد، اما بنابر بعضی گزارش‌ها، ارتش روسیه تلاش کرده است که مراحل تولید موشک توپول اسکندر ـ ام[1] یا بولاوا[2] را به پایان برساند. برخی‌ها می‌گویند که Topli ـ M می‌تواند تا قبل از سال ۲۰۰۶ به مرحله عملیاتی برسد.(۲۴)

روس‌ها همچنین مشغول تولید نسل جدیدی از کلاهک‌های هسته‌ای یک بمب‌افکن ضد رادار جدید و موشک‌های با برد ۵۰۰۰ کیلومتری که برای پرتاب‌های دوربرد به‌کار می‌رود می‌باشند. علاوه‌بر این، این کشور در حال حاضر، زیردریایی‌های با قابلیت حمل و پرتاب موشک‌های بالستیک مدل بری[3] (این زیردریایی‌ها در زمره زیردریایی‌های نسل پنجم قرار دارند)، موشک‌های بالستیک قاره‌پیمای جدیدی که روی زیردریایی‌ها مستقر می‌شوند، زیردریایی‌های مخصوص حملات هسته‌ای [مدل آکولای ۲][4] و بسیاری از سیستم‌های تسلیحاتی دیگر را توسعه داده است.(۲۵) روسیه جنگ‌افزارهای هدایت‌شونده و دقیق هوا به زمین را نیز به این منظور توسعه داده است که بر کارآمدی پشتیبانی هوایی از نیروهای زمینی بیافزائد. در حال حاضر، این جنگ‌افزارها توانمندی عملیاتی در تمام شرایط آب و هوایی را ندارند و درعین‌حال، بهای آنها نیز زیاد است.

---

1. Topol Iskander-M
2. Boulava
3. Borei
4. Acula-2-Class

این عوامل، کاربرد آنها برای انجام حملات علیه اهداف بسیار مهم را محدود می‌سازد.(۲۶) اما به‌نظر می‌رسد کارشناسان روسی سخت می‌کوشند راه‌حلی برای این معضل بیابند، زیرا آنها می‌دانند که برتری در حوزه انقلاب در امور نظامی عمدتاً از برتری در تسلیحات اطلاعاتی (سیستم‌های شناسایی، کنترل، هدف‌یابی و سیستم‌های هوشمند «فرماندهی، کنترل، ارتباطات و جاسوسی») آغاز می‌شود.

در نتیجه، زمان نگارش این سطور، یعنی از سال ۲۰۰۱ تاکنون، بیش از سی مأموریت موفقیت‌آمیز، ناوگان کهنه ماهواره‌های روسی را تقویت کرده‌اند. سه عملیات اول، یعنی پرتاب ماهواره‌ها در برنامه فضایی جدید دولت پوتین، اقداماتی کاملاً نمادین بود: ماهواره تصویربرداری کبالت،[1] ماهواره‌ای متعلق به شبکه ارتباطاتی هواپیمایی تسیکلن ـ بی[2] (که اطلاعات حساس را برای انجام نبردهای فوق‌العاده دقیق ارائه می‌دهد) و ماهواره ملنیا ـ ۳ کی[3] (که برای تقویت ارتباطات نظامی طراحی شده است). این ماهواره‌ها براساس برنامه فضایی جدید دولت پوتین، پرتاب شدند. مأموریت‌های بعدی چند مدل از ماهواره‌های دیگر را نیز با موفقیت پرتاب کرده‌اند. این ماهواره‌ها عبارت‌اند از: تعدادی رادوگای یک[4] (ارتباطات)، US ـ PV (که به‌منظور انجام جاسوسی‌های الکترونیک و هدایت موشک‌ها برای نیروی هوایی روسیه طراحی شده است)، گنتس دی[5] (بخش‌هایی از یک شبکه ارتباطات مدار پایین)، یانتار[6] (ماهواره شناسایی و تصویربرداری)، ماهواره اکوتایپ[7] (هشدار اولیه)، تسیکادا[8] (امور هوانوردی)، آراکس و ملنیا[9] (دیدبانی و ارتباطات)، نمان و دن‌ـ تایپ[10] (کنترل تصویربرداری) و تعدادی کُندر ــ ای[11] (کنترل و نظارت). گذشته از موارد بالا، سیستم گلناس[12] نیز بودجه چشمگیری را جذب کرده است و بسیار مورد توجه

---

1. Kobalt
2. Tsyklon-B
3. Molniya-3K
4. Raduga1
5. Gonets D1
6. Yantar
7. Oko-type
8. Tsikada
9. Araks and Molniya
10. Neman and Don’t-type
11. Kondor-E
12. Glonass System

قرار گرفته است. در همین چارچوب، تعدادی ماهواره اُراگان و اراگان ـ ام[1] پرتاب شده‌اند. شبکه گلناس از همان ابتدا با این هدف طراحی شده که بتواند ۲۴ ماهواره را (که روی سه فضاپیمای مداری مستقر شده‌اند) پوشش دهد. استفاده هدفمندانه از منابع مالی، این امکان را فراهم خواهد ساخت که پارامترهای این سیستم نیز ازلحاظ کیفی به‌گونه‌ای تغییر یابند که از طریق آن، اشیا و اجرام متعددی با دقتی بالا در نقاط مختلف جهان مستقر شود.(۲۷) به‌علت کمبود منابع مالی لازم، تنها هشت فروند از این ماهواره‌ها تا پایان سال ۲۰۰۳ عملیاتی شده‌اند. در نتیجه، شبکه گلناس قادر بود در عملیات‌های هوانوردی و فضانوردی، کم‌دقت‌تر از سیستم تکمیل شده عمل کند. اما ماهواره‌های گلناس ــ ام نسل جدید نیز در این اواخر به فضا پرتاب شده‌اند. برای مثال، گلناس ام- ۱۲- ال در ۲۴ نوامبر ۲۰۰۴ و ماهواره‌ای دیگر از همین مدل نیز در اواسط سال ۲۰۰۵ به فضا پرتاب شده است.

اما، درزمینه تأسیسات مستقر در روی زمین، چند مدل از رادارهای کنترل، هدایت و ردگیری توسعه‌یافته‌اند و به‌روز شده‌اند. کاستا ـ ۲ ای ۲[2] که یک هدایتگر جهانی به‌شمار می‌آید تنها یکی از این نمونه‌هاست. نمونه‌های دیگر عبارت‌اند از: GAMMA ـ DE، LEML 76N6، S- 300PMU/PMU1، PMU2 Favorit (SA-10e)، TOR ـ M1 و NEBO. درخصوص تأسیسات زیر دریا نیز باید گفت تأسیسات MG و MGK (که به Sonar تعلق دارند) و شکوال ترپدو[3] این طیف گستردهٔ سیستم‌های «شناسایی، کنترل و هدف‌یابی» روسیه را تکمیل می‌کند.

جدای از سیستم‌های شناسایی، کنترل و هدف‌یابی، ارتش روسیه مدت‌هاست بر این باور بوده که جنگ الکترونیک به شکلی از دفاع در برابر تسلیحات دقیق و سیستم‌های پیشرفته «فرماندهی، کنترل، ارتباطات و جاسوسی» مبدل شده است، زیرا قادر است پهنه دیده‌بانی تجهیزات الکترونیک سیستم‌های شناسایی و پدافند هوایی طرف مقابل را کور کند. ازاین‌رو، جنگ الکترونیک به یکی از ارکان ضروری در همه سطوح هنر نظامی مبدل شده است. روسیه نیز در پاسخ به این ضرورت، سیستم‌های

1. Uragan-M
2. Kasta-2 E2
3. Shkval Torpedo

متعددی را در حوزه جنگ الکترونیک توسعه داده است. ایستگاه‌های زمینی پرقدرت SPN-4 و SPN-2 و مجتمع فرماندهی و کنترل AKUP-1 در زمره چشمگیرترین نمونه‌های این سیستم‌ها به‌شمار می‌آیند.

گذشته از تولید محصولات سخت‌افزاری جدید، پیشرفت‌های سریع در عرصه فناوری باعث شد روسیه بپذیرد که می‌باید بیش‌ازپیش سرعت تغییرات در عرصه فناوری اطلاعات را به کنترل خود درآورد. ازنظر روس‌ها، مهم‌ترین و اصلی‌ترین دغدغه درزمینه فناوری اطلاعات، همانا تأثیر احتمالی این فناوری بر جامعه و بر راهبردها و تاکتیک‌های نیروهای مسلح بوده است. دیری نپایید جایگاه فناوری اطلاعات به‌قدری ارتقا یافت که در صدر فهرست اولویت‌های استراتژیک روسیه قرار گرفت، زیرا مقامات این کشور پی بردند که نه تنها مؤلفه‌های کَمّی بلکه مؤلفه‌های کیفی نیروهای مسلح نیز نقش تعیین‌کننده‌ای در قدرت نظامی واقعی کشورها در آینده ایفا خواهد کرد. این برداشت‌های جدید باعث شد فناوری اطلاعات در برنامه‌ریزی‌ها وارد میدان شود، سیستم‌های فنی را ـ که پشتیبانی از کارویژه‌های لجستیکی و فرماندهی و کنترل را برعهده دارند ـ یکپارچه سازد و از اقدامات غیرمستقیمی که مکمل استراتژی‌های مستقیم و آرایش مستقیم نیروها به‌شمار می‌آیند به‌نحو احسن بهره‌برداری کند.(۲۸)

یکی از مؤلفه‌هایی که روس‌ها به‌راحتی آن را دریافتند، این واقعیت بود که فناوری اطلاعات می‌تواند کارآمدی نظامی سیستم‌های تسلیحاتی را افزایش دهد چرا که پربازده‌ترین شیوه «افزایش توانمندی‌های رزمی بدون افزایش کمّی تسلیحات» به‌شمار می‌آید. برای مثال، فناوری اطلاعات، پتانسیل رزمی تسلیحات دقیق را افزایش می‌دهد و بر محاسبات درزمینه هم‌بستگی نیروها تأثیر می‌گذارد، زیرا این نوع فناوری به ارتش‌ها کمک می‌کند تا بتوانند از هر نقطه‌ای به‌وسیله موشک‌های کروز به اهداف استراتژیک حمله‌ور شوند [و آنها را منهدم سازند]. این توانایی بیش‌ازپیش آشکار می‌سازد معیار میزان «اطلاعاتی شدن»[1] که یک سلاح در خود دارد، جایگزین شاخص‌های کمّی و کیفی کارآمدی تسلیحاتی شده است. ازاین‌گذشته، فناوری اطلاعات «عدم قطعیت در جنگ» را از میان برمی‌دارد و غافلگیری‌ها را محدود می‌سازد؛ همین واقعیت نیز به‌خودی‌خود، هنر جنگ را دگرگون می‌سازد.

---

1. Informatisation

شورای امنیت روسیه به‌منظور مقابله با این معضلات در سپتامبر ۱۹۹۷ نسخه پیش‌نویس «سیاست امنیت اطلاعاتی» این کشور را مورد بحث و بررسی قرار داد. نیروهای مسلح روسیه نیز بلافاصله بعد از آن، کار روی تلفیق «فناوری اطلاعات» با مفاهیم روان‌شناختی قدیمی‌تر از قبیل کنترل انعکاسی[۱] (۲۹) و استفاده از فناوری اطلاعات در شکل‌دهی به واقعیت‌های هنجاری و ایجاد محیط‌های ترکیبی[۲] در امور نظامی را آغاز کردند. تقریباً بلافاصله بعد از این اقدام، دانشمندان روسی حوزهٔ فناوری اطلاعات روسیه، تحقیقات خود را بر نحوه کاربرد فناوری اطلاعات متمرکز ساختند، هدف آنها از این تحقیقات این بود که به ادغام سیستم‌های تسلیحاتی جدید در رویه‌های روزمره نظامی کمک کنند. دو مورد از کاربردهای عمده‌ای که گسترش یافت، یکی آموزش واقعیت مجازی به افسران روسی و دیگری تأکید بر آزمایش سیستم‌های تسلیحاتی با ابزارهای واقعیت مجازی (البته قبل از دستیابی به آنها) بود. سرانجام رهبران نظامی روسیه نیز به‌منظور کمک به بهبود دکترین نظامی، آزمون پرسنل و آزمایش ضعف‌های تجهیزات در شرایط متفاوت جوی، ساعات مختلف روز و سطوح گوناگون آمادگی، رفته‌رفته استفاده از واقعیت مجازی را آغاز کردند.

اما جنگ اطلاعاتی همواره اهمیتی دوگانه[۳] برای روس‌ها داشته، زیرا گذشته از اهمیت فنی ـ اطلاعاتی آن، جنبه اطلاعاتی ـ روانی جنگ اطلاعاتی نیز هرگز کنار گذاشته نشده است. تأسیس سازمان فدرال ارتباطات و اطلاعات دولتی،[۴] این دوگانگی[۵] را نشان داد. این کشور به‌طور عمده در دو حوزه از جنگ اطلاعاتی، یعنی ویروس‌های رایانه‌ای (۳۰) و عملیات روانی، تبحر خاصی داشت. دیری نگذشت که سازمان فدرال ارتباطات و اطلاعات دولتی به یکی از اصلی‌ترین اپراتورهای سیستم SOUD (که برخی آن را آشلن روسی[۶] می‌نامند) مبدل شد. در سپتامبر ۲۰۰۰، پوتین دکترین امنیت اطلاعاتی فدراسیون روسیه را تصویب کرد و سه سال بعد از آن، با صدور حکم

---

1. Refletive Control
2. Synthetic Environononents
3. Dual
4. Federal Agency for Government Communication and Information (FAPCI)
5. Duality
6. Russian Echelon

ریاست جمهوری، سازمان فدرال ارتباطات و اطلاعات دولتی را منحل کرد و وظایف آن را بین سرویس امنیت فدرال[1] و وزارت دفاع تقسیم کرد. همه این عناصر نشان‌دهنده اهمیت فزاینده دستیابی به فناوری اطلاعات در اذهان مقامات روسیه است.

در حال حاضر، تعداد اندکی از قرارگاه‌های رایانه‌ای کنترل نیرو و تسلیحات در ارتش روسیه به‌کار گرفته شده‌اند. کاربران نهایی یعنی همان پرسنل گردان‌ها یا تک‌تک سربازانی که در میدان نبرد می‌جنگند، حالا دیگر این امکان را دارند که از چنین فناوری‌ای استفاده کنند. در حال حاضر، دو حوزه است که به میزان بیشتری توسعه یافته است. حوزه اول، تسلیحات غیرمرگبار است. این تسلیحات مختص نیروهایی است که در این اواخر در عملیات‌های صلح به‌کار گرفته شده‌اند. اما حوزه دوم، تسلیحاتی است که از طریق آنها ابزارهایی کارکردی برای انهدام اهداف به‌کار گرفته می‌شوند و می‌توانند به‌عنوان عاملی بازدارنده در برابر سلاح‌های بسیار دقیق به‌کار آیند.

بالاخره، گردآوری و بهره‌برداریِ به‌موقعِ اطلاعات، امری بیش‌ازپیش بااهمیت به‌شمار می‌آید. یکپارچه‌سازی اطلاعاتی که به کمک تجهیزات شناسایی، فرماندهی و کنترل گردآوری می‌شوند یکی از ارکان حیاتی نظریه سیستم‌های رزمی روسیه است. هم‌اکنون هدف این ارتش توسعه آن عواملی است که امکان جای دادن اطلاعات گردآوری شده در درون سیستم‌ها را فراهم می‌سازد؛ سیستم‌هایی که برای انجام واکنش‌های صحیح و دقیق به برقراری پیوند مستمر میان داده‌ها سخت نیاز دارند. «از صفر شروع کردن» و تولید درون‌زاد تنها شیوه‌ای نیست که مقامات روسیه در پیش گرفته‌اند و پیش می‌برند. کسب فناوری اطلاعات از خارج نیز رویکردی پذیرفتنی است؛ زیرا سریع‌ترین روشی به‌شمار می‌آید که با آن می‌توان عقب‌ماندگی‌ها در برابر غرب را جبران و توانمندی‌های رزمی را تقویت کرد.

۳-۱۰ نتیجه‌گیری و ارزیابی

بوریس یلتسین اولین کسی بود که ایده «گذر به ارتش حرفه‌ای» را مطرح کرد. در پاییز ۲۰۰۱، پوتین خواستار دگرگونی‌های عمده در ارتش روسیه شد که براساس برنامه‌های او

1. Federal Security Service (FSS)

می‌باید تا سال ۲۰۱۰ تحقق یابد. بسیاری از کارشناسان در مورد واقع‌بینانه بودن این جدول زمانی تردید دارند، زیرا احتمال پیشرفت‌های مورد نظر به دو چالشی بستگی دارد که می‌باید بر آنها فائق آمد: سطوح نازل بودجه‌های موجود در این حوزه و مقاومت ارتش با اصلاحات. نظامیان و به‌ویژه ژنرال‌های ارشد ارتش، معضلات موجود در نیروهای مسلح را تشدید می‌کنند. آنها با طرح‌های پیشنهادی درزمینه انجام اصلاحات در ارتش به مخالفت برمی‌خیزند؛ زیرا براساس برداشت‌های آنها، پیشنهاد هر طرحی در این زمینه لاجرم باعث می‌شود که قدرت ارتش کاهش یابد. پاول فلگنهاور[1] می‌گوید: «ژنرال‌های ما در دوران شوروی تعلیم دیدند و فکر می‌کنند ارتش شوروی بزرگ‌ترین ارتش جهان بوده است. هدف آنها احیای همان ارتش است نه حرکت به‌سمت ایجاد نوع جدیدی از نیروی نظامی».(۳۱)

در آوریل ۲۰۰۲، مارشال سرگیف،[2] مشاور پوتین، اظهار داشت گذر به یک ارتش جمع‌وجور به‌عنوان برنامه‌ای برای نوسازی ارتش، به‌ویژه در حوزه‌های ارتباطات، عملیات‌های جاسوسی، نیروهای استراتژیک هسته‌ای و توسعه ارتش فضایی می‌باید درهرحال رخ دهد. واقعیت این است که زمینه‌سازی‌های بودجه‌های ارتش و نیروهای رسمی نظامی چندان زیاد نبوده‌اند. تخصیص بودجه‌های دفاعی و تدارکاتی در عمل به سناریوهای جنگ هسته‌ای و حمایت از افزایش طرح‌های تحقیقات و توسعه برای بهره‌برداری از انقلاب در امور نظامی معطوف شد. برای مثال، دراین‌باره می‌توان به موشک‌های بالستیک قاره‌پیمایی که از روی حامل‌های در حال حرکت پرتاب می‌شوند، موشک‌های بالستیک با قابلیت پرتاب از دریا، سرمایه‌گذاری‌ها درزمینه سلاح‌های ضدزیردریایی استراتژیک، تحقیقات و توسعه درزمینه سیستم‌های استراتژیک و متعارف «فرماندهی، کنترل، ارتباطات و جاسوسی» و جنگنده‌های جدید اشاره کرد.

براساس‌این، ازآنجاکه تأمین هزینه‌ها از منابع داخلی تاکنون امکان‌پذیر نبوده است، مجتمع نظامی صنعتی روسیه اجازه یافته است عملاً فارغ از محدودیت‌های دولتی، حتی پیشرفته‌ترین تسلیحات را صادر کند. ازاین‌رو، رقبای شناخته شده روسیه، یا رقبای منطقه‌ای این کشور (چین، هند، کره جنوبی، اندونزی و ایران) نیز می‌توانند تسلیحات و

---

1. Pavel Felgenhauer
2. Marshal Sergeev

سیستم‌های مدل بالا را به‌نسبت ارزان به‌دست آورند. ازاین‌گذشته، این کشورها می‌توانند مسکو و سایر عرضه‌کنندگان تسلیحات را ناگزیر سازند نمونه‌های ساخت را در اختیارشان قرار دهند تا با کپی‌برداری از آنها سلاح‌های خودشان را بسازند و از این روش، بیش‌ازپیش از فشار فروشندگان تسلیحات بکاهند. هرچند بسیاری از این کشورها دشمنان بالقوه روسیه به‌شمار می‌آیند، اما دولت روسیه حداقل طی دهه آینده هیچ تهدید متعارف یا هسته‌ای را که در عالی‌ترین سطح نبرد روی دهد فراروی خود نمی‌بیند.

به‌ظاهر در همین چارچوب نیز، پوتین در شانزدهم اکتبر ۲۰۰۱ پایگاه لوردز[1] (مجتمع نظامی کوبا که بزرگ‌ترین پایگاه نظامی و ایستگاه شنود الکترونیک روسیه در نیم کره غربی به‌شمار می‌آید) را تعطیل اعلام کرد. این پایگاه در سال ۱۹۶۴ تأسیس شد. تأسیسات آن ۲۸ مایل مربع وسعت داشت و ۱۵۰۰ تا ۱۶۰۰ نفر به‌صورت پرسنل نیز به‌صورت تمام‌وقت در آنجا کار می‌کردند؛ علاوه‌بر این دو نهاد روسیه، یعنی اداره ششم سازمان جاسوسی نظامی و سازمان فدرال ارتباطات و اطلاعات دولتی به‌طور مشترک این پایگاه را اداره می‌کردند.(۳۲) هزینه اجاره این پایگاه، جدای از دستمزدهای پرسنل آن، هرساله حدود بیست میلیون دلار (۳ درصد بودجه مستقیم دفاعی) بوده است.

به گفته مقامات روسیه، ارتش باهمین مبلغ می‌توانست بیست فروند ماهواره شناسایی یا ۱۰۰ ایستگاه راداری پیشرفته خریداری کند. در همان روز، پوتین گفت روسیه ایستگاه‌های شنود و پایگاه نیروی دریایی خود در کام ران بای[2] ویتنام را که از سال ۱۹۷۹ دایر شده بود، برخواهد چید. درهرصورت، این دو رویداد، در راستای شرایط جدیدی که پیش از یازده سپتامبر در عرصه بین‌المللی پدیدار گشت، نشان‌دهنده دو تغییر در جهت‌گیری سیاسی دولت روسیه و افزایش درک رهبران روسیه از اولویت‌های اقتصادی و فنی این کشور است.

در مورد نیروهای زمینی، ساختارهای زائد و دوباره‌کاری در سازوکارهای فرماندهی و کنترل کاهش یافته‌اند. این تدابیر با این هدف انجام گرفته‌اند که مدت زمان تصمیم‌گیری به حداقل برسد و پاسخ سریع‌تری به وضعیت‌هایی که به‌سرعت به‌وقوع می‌پیوندند، داده شود.

---

1. Lurdes
2. Cam Rahn Bay

اما به گفته بعضی از تحلیلگران، تحقیقات و توسعه در روسیه به شیوه عملی، علمی و جامعی انجام نمی‌گیرد بلکه روسیه در این زمینه، چند دستورالعمل محدودگرانه و تخصصی را به اجرا درمی‌آورد و این دستورالعمل‌ها نیز ارتباط چندانی با توانمندی‌های رزمی یا مأموریت‌هایی که از نیروهای مسلح روسیه درخواست می‌شود انجام دهند، ندارند. مقامات روسیه برای حل این معضل، قصد دارند ساختار ارکان «فرماندهی، کنترل، ارتباطات و جاسوسی» را حفظ کنند و آن را با «ملزومات مدرن» هماهنگ سازند. در این خصوص، طول زمان بهره‌برداری از فناوری‌هایی که در این ارکان به‌کار رفته است افزایش داده‌اند و آنها را با ملزومات تأسیسات پیشرفته منطبق ساخته‌اند و به موازات آن، منابع مالی لازم برای پیشبرد تحقیقات و توسعه را به‌منظور بهبود این زیرساخت فراهم ساخته‌اند. در برنامه‌های نوسازی ضروری است نه تنها دستیابی به سیستم‌های تسلیحاتی جدید[۳۳] بلکه «ارتقای سیستم‌های فرماندهی، کنترل، ارتباطات و جاسوسی و سرمایه‌گذاری در این زیرساخت اساسی» نیز هدف قرار گیرد.[۳۴]

در نتیجه‌گیری باید گفت ستاد کل نیروهای مسلح روسیه همچنان جنگ‌های آینده را براساس انقلاب در امور نظامی طرح‌ریزی می‌کند. به‌نظر می‌رسد مقامات روسیه در کوتاه‌مدت رویکرد عمل‌گرایانه‌ای را در پیش گیرند و به دنبال راه‌حل‌های موقتی و تدابیر عملیاتی برای مقابله با چالش‌ها باشند (در این راستاست که به تولید تسلیحات غیرسنتی روی آورده‌اند).[۳۵] اما در درازمدت به‌نظر می‌رسد آنها درصدد برآیند زیرساختی را ایجاد کنند که امکان تولید سریع پیشرفته‌ترین تسلیحات بدیع را فراهم آورد. به‌نظر می‌رسد در دوره‌گذاری که میان این دو دورنما وجود دارد، آنها به زرادخانه هسته‌ای‌شان اتکا خواهند کرد.

۴-۱۰ دیدگاه‌ها

پس از فروپاشی اتحاد شوروی، ارتش روسیه، در اثر محدودیت‌هایی که در تخصیص بودجه دفاعی داشته و بسیاری از معضلات دیگری که فراروی خود دیده است، دوره‌ای سرشار از آشفتگی را در نیروها و تجهیزات خود تجربه کرده است. آیا تأمین بودجه در نهایت، عاملی تعیین‌کننده برای پیشبرد انقلاب در امور نظامی روسیه به‌شمار می‌آید؟

در طول چند سال اخیر، بودجه ارتش روسیه حدود ۲/۶ درصد تولید ناخالص داخلی ۳۰۸ میلیارد دلاری این کشور را تشکیل داده است.(۳۶) این مبلغ ناچیز برای حفظ ارتشی که توانایی نبرد در میدان جنگ را داشته باشد آشکارا ناکافی بود، چه رسد به اینکه بتواند مخارج پروژه‌های پرهزینه‌ای که برای انجام اصلاحات در نیروهای مسلح لازم است (به‌ویژه، پروژه‌های تحقیقات و توسعه) تأمین کند. اما تغییرات اخیر در سیاست غرب در قبال روسیه و روابط نزدیک آن کشور با ایالات متحده فرصت بی‌سابقه‌ای را در اختیار مسکو قرار داد تا بتواند هزینه‌ها را کاهش دهد و بودجه‌هایی را برای «تجدیدساختار»[1] ارتش روسیه اختصاص دهد. به‌نظر می‌رسد این امتیازهای سیاسی و اقتصادی که به‌تازگی در اثر روابط نزدیک با غرب عاید روسیه شده است، به آن امکان می‌دهد تا انجام اصلاحات در ارتش را با جدیت دنبال کند، نیروهای زمینی‌اش را از مشکلات فعلی برهاند و به یک ارتش مدرن مبدل سازد. درعین‌حال، درآمدهای حاصل از فروش تسلیحات و افزایش درآمدهای نفتی نیز صنایع دفاعی این کشور را سرزنده و فعال نگاه خواهد داشت و نیازهای مالی تحقیقات و توسعه را تأمین خواهد کرد.

سرگئی ایوانف[2] وزیر دفاع روسیه، که نزدیک‌ترین فرد معتمد پوتین در دولت روسیه محسوب می‌شود، گفت که میزان بودجه نظامی، از جمله در حوزه تولید اقلام گران‌بهایی همچون زیردریایی‌های هسته‌ای و جنگنده‌های جت در چند سال آینده افزایش نخواهد یافت. در عوض، دولت خواهد کوشید شبکه نارسای ماهواره‌های اطلاعاتی روسیه را تعمیر کند، ضریب امنیت و ایمنی تأسیسات هسته‌ای را افزایش دهد، ناوگان‌های موجود هواپیمای جنگی به موتورهای جدید مجهز سازد و تا جایی که در توان دارد، ارتش را با تجهیزات هدایت‌شونده دقیق و سیستم‌های جنگ اطلاعاتی نوسازی کند.

برخلاف این شعارها، بودجه دفاعی مستقیم روسیه در همان سال به‌نحو چشمگیری افزایش یافت، حتی تقریباً تمام منابع مالی‌ای که علاوه‌بر بودجه در اختیار داشت، صرف خرید تجهیزات جدید شد. این میزان تخصیص بودجه، بیشترین میزان بودجه‌ای بود که روسیه در طول دهه اخیر به‌طور مستقیم به تهیه تسلیحات جدید و

1. Restructure
2. Sergei Ivanov

تأمین مالی فعالیت‌های تحقیقات و توسعه اختصاص می‌داد. پوتین در مورد دلیل آغاز این تدابیر فوری برای تجهیز ارتش به تسلیحات جدید گفت: «شرایط فعلی در جهان، ما را ناگزیر ساخته است به این اقدام روی آوریم».

در این میان، تخصیص بودجه جدید برای تهیه تجهیزات بر «نوسازی و ارتقای تسلیحات هوایی و دریایی و به‌ویژه، ماهواره‌ها، سیستم‌های تسلیحاتی بسیار دقیق و مجتمع ویژه عملیات شناسایی ـ حمله» متمرکز شد. اما تولید این تجهیزات احتمالاً تا پس از سال ۲۰۰۶ یا حتی سال‌های بعد از آن آغاز نخواهد شد.[۳۷]

البته، گذشته از پول، عامل دیگری که تحقق آن ضرورت دارد، بهبود همکاری فنی‌ـ نظامی در درون وزارت دفاع روسیه است. چه‌بسا روسیه به فناوری‌های جدید دست یافته است، اما به‌کارگیری آنها در ارتش هنوز مشخص نیست. یک انقلاب در امور نظامی تنها به مدد وجود استراتژی می‌تواند روی دهد و استراتژی‌ای که از همان سطوح بالای مقامات دولتی آغاز می‌شود، باید تمامی بخش‌های اجرایی را در نظر گیرد و همه مسیرهای منتهی به آخرین سرباز را نیز بپیماید. سیستم‌های تسلیحاتی پیشرفته باید تنها بعد از تصویب رئیس‌جمهور، دولت و وزارت دفاع خریداری شوند. جلوگیری از صادرات غیرقانونی فناوری‌های دفاعی و عرضه لجام‌گسیخته تسلیحات انفرادی به سایر کشورها نیز از جمله وظایف این نهادهاست. نهادهای مذکور باید منافع روسیه درزمینه همکاری‌های فنی‌ـ نظامی را در نظر گیرند و به این موضوع توجه کنند که هرگونه موافقت‌نامه‌ای درباره چنین همکاری‌هایی بر روابط این کشور با سایر کشورها در عرصه بین‌المللی تأثیر خواهد گذاشت.

حجم تکان‌دهندهٔ هدر رفتن منابع مالی نیز می‌باید مورد توجه قرار گیرد. بودجه رسمی دفاعی روسیه مانند دوران شوروی تنها بخشی از آن پولی است که مسکو در ارتش هزینه می‌کند. بودجه‌های هنگفتی نیز صرف اموری از قبیل احداث تأسیسات نظامی و تولید تسلیحات می‌شود که در بودجه‌های وزارتخانه‌های مختلف، کمیته‌های دولتی و شبکه گسترده‌ای از پیمانکاران شبه‌خصوصی جای می‌گیرند که به ظاهر مشخص نیستند و در بودجه رسمی دفاعی نیز ذکر نمی‌شوند. این تسلیحات نیز به

صورتی که استفن بلنک،[1] استاد دانشگاه جنگ ارتش آمریکا طرح‌های هرمی شکل می‌نامد، به سایر کشورها فروخته می‌شود. به‌موجب این طرح‌ها، مبالغی که از یک منبع در یک بخش به‌دست می‌آید برای تأدیه بدهی‌های کوتاه‌مدت در سایر بخش‌ها مورد استفاده قرار می‌گیرد. کل بودجه نظامی روسیه ـ البته فقط اقلام تسلیحاتی سری مستثناست ـ باید در دوما به‌صورت علنی مورد بحث و بررسی قرار گیرد. همچنین، به‌محض اینکه بودجه به تصویب رسید، همه مقامات دولتی و نظامی می‌باید بودجه را به‌طور کامل و دقیق رعایت کنند. البته دومای دولتی و شورای فدراسیون [روسیه] نیز حق خواهند داشت شیوه‌های صرف بودجه «براساس فهرست اقلام مورد نظر» را بررسی و بر حسن اجرای آن نظارت کنند. درصورتی‌که این امر تحقق یابد، مقررات امور دفاعی به اجرا درخواهد آمد، مخارج فعالیت‌های تحقیقات و توسعه به‌موقع تأمین خواهد شد، تجهیزات جدید در اختیار نیروهای مسلح قرار خواهد گرفت و درعین‌حال، افسران نیز حقوق خود را دریافت خواهند کرد.

واقعیت‌های موجود نشان می‌دهد که بعید است روسیهٔ جدید در آینده منابع اقتصادی و فناورانه‌ای را که برای رقابت با آمریکا در حوزه فناوری‌های نظامی پیشرفته ضروری است، در اختیار داشته باشد. این ضعف چه‌بسا ممکن است ستاد کل نیروهای مسلح روسیه را ناگزیر سازد که همچنان بر راه‌حل‌های سرزمین‌محورانه‌تر[2] و ددمنشانه‌تر به‌ویژه به‌کارگیری تسلیحات هسته‌ای تکیه کند. راه‌حل موقت دیگر، این است که توانمندی‌های نامتقارن یا «فناوری دنج»(۳۸) ـ که می‌توانند پرل‌هاربر الکترونیکی ایجاد کنند ـ توسعه یابند، یا تسلیحات بیولوژیکی ـ که محیط زیستی انسان را هدف قرار می‌دهند ـ تولید شود.(۳۹) سرانجام، سومین راه‌حل کوتاه‌مدت، توسعه پیوندهای چین و روسیه خواهد بود، البته به‌گونه‌ای که این پیوندها از معامله‌های ساده «پول نقد در برابر تسلیحات» (که در گذشته انجام می‌گرفته است) فراتر رود و اساس یک اتحاد به‌مراتب پیش‌بینی‌ناپذیرتر در آینده را شکل دهد؛ اما، یک مسئله روشن است: روس‌ها با وجود رخوت اقتصادی‌ای که از آن رنج می‌برند، فکر و ذهن خود را به هدف رقابتگری نظامی

1. Stephen Blank
2. Territorial

در آینده مانند آنچه در گذشته نیز تجربه کرده‌اند، معطوف ساخته‌اند. به‌نظر می‌رسد تفاوتی که وجود دارد این است که آنها در حال حاضر مشغول تدوین اولویت‌ها می‌باشند، درحالی‌که دهه‌های ۱۹۶۰ و ۱۹۷۰، همه برنامه‌ها در همه بخش‌ها و سازمان‌های دولتی اولویت یافته بودند.

تجهیز ارتش به تسلیحات جدید از سال ۲۰۰۵ آغاز شده است؛ هدف دولت این است که هرساله پنج درصد تسلیحات ارتش را به‌روز کند و تا قبل از سال ۲۰۲۵، برنامه تجهیز ارتش به تسلیحات جدید را به پایان رساند. در این برنامه، تأکید بر آن حوزه‌هایی است که روسیه در آنها توانایی رقابت با سایر کشورها را بازمی‌یابد.[۴۰] ابزار تأمین این هدف نیز مشخص است: برای مثال، بودجه نظامی روسیه در سال ۲۰۰۵ نسبت به بودجه نظامی سال قبل از آن سه برابر شده است.

مقامات نظامی روسیه، برای دستیابی به آن اهداف بین‌المللی که ترسیم کرده‌اند، از همین حالا هر دو استراتژی‌های موقت و بلندمدت را پیش برده‌اند. آیا آنها قادر خواهند بود اهداف خود را عملی سازند؟ در گذشته که توانستند.

پی‌نوشت‌ها

1. Shurygin Vadim, 'Generals' Wars, *Novaya Gazeta*, 30 April 2002.

2. Nauchnaya-Tekhnicheskaya Revoliutsiya.

3. Col, General N.A. Lomov, *The Revolution in Military Affairs: A Soviet View*, Translated and Published Under the Auspices of the United States Air Force, Washington, DC: USGPO, 1973; John Erckson , Edward L. Crowley and Nikolay Galay (eds)., *The Military-Technical Revolution*, New York: Frederick A. Praeger Publishers, 1966; William R, Kintner and Harriet Fast Scott Trans. and ed, *The Nuclear Revolution in Soviet Military Affairs,* Norman, OK: University of Oklahoma Press, 1968.

4. Anatoly Medetsky, 'Putin OK's Plan to Cancel Conscription' *Vladivostok News*, 4 December 2001.

5. Anonymous, 'Deserters go on a Shooting Spree', Izvestia, 6 February 2002.

۶. روس‌ها به مانند اسلاف خود در دوران شوروی، استدلال می‌کنند که پیشرفت‌های علمی در یک کشور نه به وضعیت سیاسی یا اقتصادی آن، بلکه به مغزهای دانشمندان آن بستگی دارد. دانشمندان روسیه مدعی‌اند هنوز در بسیاری از حوزه‌ها در سراسر سیاره زمین، پیشرو هستند و همچنان در حوزه‌هایی از قبیل فیزیک هسته‌ای و تولید تسلیحات ترموهسته‌ای به تحقیقات و توسعه می‌پردازند.

7. Fitzgerald C. Mary, The New Revolution in Russian Military Affairs London: RUSI, Whithall Paper Series, 1994.

8. Aleksey Arbatov, Quote selected by Johnson's Russia List no. 5262 (AVN Military News Agency, 18 May 2001.

9. See, for more details, Baltic Defence Review, 6, 2001. Available at www.bdcol.ee/pages/bdr-archive.

10. Yakovlev, Interviewed by Ludmila Averina, Trud, 13 May 2000, p. 2.

۱۱. در پایان سال ۲۰۰۰، نیروهای موشکی استراتژیک روسیه موشک SS-19 را آزمایش کردند. برطبق گزارش‌ها، این موشک از ایستگاه فضایی بایکنور (Baikonur) در قزاقستان به هدف خود در منطقه کامچاتکا اصابت کرد. موشک SS-19 بخشی از زرادخانه این نیروها در طول ۲۵ سال اخیر بوده است. یک روز قبل از انجام آزمایش سخن‌گوی این نیروها به *رویترز* گفت که این موشک در آینده از سرویس‌دهی خارج می‌شود و سیستم و تجهیزات آن با مدل موشک SS-18 که مختص ماهواره‌های تجاری است منطبق می‌گردد. به‌موجب پیمان استارت ۲ قرار است

موشک‌های SS-18 و SS-19 دیگر در مأموریت‌های نظامی به‌کار نروند.

12. Staus Report: Nuclear Weapons, Fissile Material and Export Controls in the Former Soviet Union, CNS Print Publicatin, 2001. Available at http://cns.miis.edu/pubs/print/nsr2.htm,p. 14-17, 19.

۱۳. در اکتبر ۲۰۰۰، یک موشک بالستیک توپل شانزده‌ساله نیز با موفقیت آزمایش شد. سخن‌گوی نیروهای موشکی استراتژیکی نیز گفت که روسیه در حال ارتقای توپل به مدل جدیدتری به نام Topol-m است. اما درعین‌حال، توپل‌های قدیمی را نیز در مرحله ارائه خدمات نگاه خواهد داشت و توسعه خواهد داد.

14. A Golts, 'Kremlin Moves to Rekindle Cold War Missile Plan', *The Russia Journal*, 28 June 2001.

۱۵. برنامه‌ریزی نظامی ۱۹۹۷ از سه مرحله تشکیل شده است: مرحله اول، مرحله اجرایی (۲۰۰۰-۱۹۹۷) است که کاهش ۳۰ درصدی نیروهای مسلح را پیش‌بینی کرده است. مرحله دوم (۲۰۰۵-۲۰۰۰) به تغییرات ساختاری در مابقی نیروهای مسلح اختصاص می‌یابد. در این مرحله هیچ تسلیحات و فنون نظامی از خارج خریداری نمی‌شود و صرفاً تمرکز ارتش بر تحقیقات و توسعه است. این برنامه‌ریزی خرید نسل بعدی تسلیحات درصورتی‌که شرایط مالی فراهم باشد، پیش‌بینی می‌کند. مرحله سوم به بعد از سال ۲۰۰۵ اختصاص می‌یابد. در این مرحله است که نیروهای مسلح عرضه تسلیحات جدیدی را که در طول ده سال قبل طراحی کرده بودند، آغاز می‌کنند.

۱۶. این هشدار که هیچ تسلیحات جدیدی تا قبل از سال ۲۰۰۵ وارد عرصه نخواهد شد، به‌وسیله ایگور ایوانف وزیر دفاع روسیه در مصاحبه با *اینترفاکس* در تاریخ ۸ فوریه ۱۹۹۹ داده شد.

17. Kornukov, in Another Interfax Interview, 11 March 1999.

۱۸. چینی‌ها بزرگ‌ترین خریداران تسلیحات روسی می‌باشند، این خریدها که در چند سال اخیر افزون‌بر شش میلیارد دلار رسیده است، این اختیار را به چینی‌ها داد که برخی از تسلیحات را خودشان تولید کنند. این تجارت ممکن است در کوتاه‌مدت رشد یابد اما دیر یا زود منافع مالی روسیه را کاهش خواهد داد. هند نیز مانند چین یکی از خریداران بزرگ تسلیحات روسیه است.

19. Alexei G. Arbatov. The Transformation of Russian Military Doctrine: Lessons Learned from Kossovo and Chechenya, George C. Marshall: European Centre for Security Studies, July 2000, p. 18.

۲۰. ایران (بعد از چین و هند) سومین مصرف‌کننده بزرگ تسلیحات روسیه است؛ موافقت‌نامه خرید تسلیحات که در سال ۲۰۰۱ به امضای دو کشور رسید، سالیانه در حدود ۳۰۰ میلیون دلار را

عاید روسیه می‌ساخت که در سال‌های بعد از آن نیز به ۱/۵ میلیارد دلار رسید؛ این مبلغ بخش مهمی از هزینه‌های مجتمع نظامی صنعتی روسیه را تأمین می‌کند.

۲۱. شرکت سوخوی (Sukhoi) بودجه برنامه تولید سیستم S-37 را از طریق فروش هواپیمای SU-27/Su -30 به چین و هند تأمین می‌کند.

۲۲. یکی از اهداف عمده سیاست فنی ـ نظامی روسیه، تشکیل یک نیروی ذخیره فنی ـ علمی است که به صنایع دفاعی اجازه می‌دهد که توجه خود را بر توسعه مدل‌های نخستین تسلیحات متمرکز سازند و از تولید هزینه‌بردار مدل‌های ارتقایافته بپرهیزند.

23. Alexei Alexandrov, 'Restructuring and Privatisation', *Rossiiskie Esti*, 14-20 March 2002, p. 10.

24. Lee Myers Steven, 'Putin Touts New Missile Advances', *The New York Times*, 18 November 2004.

25. Colonel Stanislav Lunev in Maxnews.com on 4 October 2002.

26. Colonel General A.M. Kornukov,'Win, Suppress. Support?' Armeyskiy Sbornik, December 1998.

27. Dubovoi Alexander, Segodnashnaya Gazeta (Krasnoyarsk), 20 March 2002.

28. Thomas L. Timothy Information Technology: US/Russian Perspectives and Potential for Military – Political Cooperation in Global Security Beyond the Millennium, Basingstoke: Macmillan – new Palgrave Macmillan, 1999.

۲۹. یکی از ابزارها یا شیوه‌هایی است که برای انتقال اطلاعات به شخص یا کشور به‌کار می‌رود و بر اتخاذ تصمیمی که از پیش گرفته شده است و برای عامل کنش نیز مطلوب است تأثیر می‌گذارد.

۳۰. از همان آغاز، ویروس‌های رایانه‌ای به‌عنوان یکی از عوامل توان‌افزا تلقی شده‌اند که می‌توانند ابعاد جدیدی به اصل غافلگیری بیافزایند.

31. The Christian Science Monitor, 30 September 2002.

۳۲. بر پایه برخی گزارش‌ها، لوردس (Lurdes)، علاوه‌بر گردآوری و تحلیل ارتباطات آمریکا، جاسوسان روسی در آمریکای شمالی را هدایت می‌کرد، امکان پیوندها با شبکه جاسوسی ماهواره‌ای روسیه را فراهم می‌نمود، دستورات را به کشتی‌ها و زیردریایی‌ها ارسال می‌کرد و فعالیت‌هایِ ناوگان دریایی آمریکا در دریای کارائیب را رهگیری می‌نمود.

33. D.Yu. Bukreyev,'Ground Forces and Military Reform', Military Thought, 10(5) (2001), p. 1.

34. Baev Pavel, 'Putin's Military Reform', *Security Policy Library*, No. 6 (2001).

۳۵. در حال حاضر، تحقیقات گسترده‌ای درزمینه تسلیحات لیزری، تسلیحات مافوق صوت و با فرکانس بالا و نبرد الکترونیک و اطلاعاتی انجام می‌گیرد.

36. 'Problems of the Russian Armed Forces Must Be Addressed', CSIS Prospectus, 3(3), Fall 2002.

37. 'No Big Changes Planned in Size of Russian Arms Budget', *Jamestown Foundation Monitor*, 23 January 2002; and Alexander Golts, 'The Shadow that Lags Behind' *Yezhenedelnyy Zhurnal*, 25 July 2002.

۳۸. سیستم‌های فضایی، جنگ اطلاعاتی و تسلیحات ضدماهواره‌ای.

۳۹. به گفته یکی از دانشمندان روسیه که نقش عمده‌ای در پروژه تسلیحات بیولوژیکی روسیه ایفا کرد، شواهدی وجود دارد که نشان می‌دهد حداقل تا سال ۱۹۹۷ دانشمندان روسی کار بر روی توسعه عاملان ژنتیک در جنگ‌ها را ادامه دادند.

40. FitzGerald C. Mary, Russian Military Policy and International Objectives: Interim Strategies and Plans for Long Term Systemic Change, Project on Eurasian Security, Washington, DC: Hudosn Institute, 2001.

فصل یازدهم مروری اجمالی بر تحقیقات و توسعه درزمینه جنگ اطلاعاتی در چین

کریس وو*

مقدمه

چین جنگ اطلاعاتی را سیستم عصبی[1] (چشم‌ها و گوش‌های) سیستم‌های عملیات نظامی نهادهای نظامی تعریف می‌کند. جنگ اطلاعاتی مورد نظر چین حوزه‌های «فرماندهی و کنترل، ارتباطات، امور رایانه‌ای، جاسوسی، نظارت و شناسایی»، جنگ الکترونیک، جنگ شبکه‌ای و سایر موضوعات مرتبط با این حوزه‌ها را دربرمی‌گیرد. برطبق آثار و ادبیات، شن وی کوان،[2] یکی از افسران رده پایین ارتش آزادی‌بخش خلق[3] در سال ۱۹۸۵ مفهوم جنگ اطلاعاتی را برای اولین بار مطرح ساخت. اما در آن زمان، چین از زیرساخت لازم در حوزه فناوری برخوردار نبود و هیچ پژوهش عمیقی هم در مورد معماری[4] جنگ اطلاعاتی انجام نداده بود تا بتواند در حوزه تحقیقات و توسعهٔ این نظریه و فناوری علمی ـ نظامی جدید پیش‌قدم شود. علاوه‌بر این، نظام اجتماعی سنتی و ایدئولوژی ـ رژیم حاکم بر چین نمی‌توانست خود را با آن اندیشه‌های جدید جنگ اطلاعاتی که در درون فرهنگ آمریکایی لیبرال نضج گرفته بود وفق دهد.

در سال ۱۹۹۱، یعنی در زمان عملیات طوفان صحرا، نیروهای مسلح آمریکا مفهوم جنگ اطلاعاتی را به‌کار بردند و مجموعه تمام‌عیار جدیدی از مفاهیم نظری و تاکتیکی را

---

* Chris Wu

1. Neuro-system
2. Shen Wei Kuan
3. The Poople's Liberation Army
4. Architecture

در مورد جنگ و جنگیدن مطرح ساختند که فناوری اطلاعات و توسعه انواع جدیدی از تسلیحات هوشمند را دربرمی‌گرفت. این وضعیت، رهبران ارتش آزادی‌بخش خلق را متوجه این واقعیت ساخت که چین برای تقویت نیروی زمینی، ارتقای توانمندی‌های نیروی هوایی و قابلیت‌های دریایی و فضایی خود می‌باید ساختار نظامی‌اش را متحول کند.

طی دهه گذشته، چین تحقیقات درزمینه «نظریه جنگ اطلاعاتی و سخت‌افزارها و نرم‌افزارهای مرتبط با آن» را از سر گرفته است و به لحاظ توانمندی‌های فنی در حوزه‌های ماهواره، رادار، ارتباطات، فناوری اینترنت، پیشرفت‌های چشمگیری کرده است. دستیابی به اطلاعات دقیق و به‌روز در مورد سیستم‌های جنگ اطلاعاتی چین به‌علت آنکه بسیار محرمانه به‌شمار می‌آید، دشوار می‌باشد. ازاین‌رو، آنچه در ذیل می‌آید، تحلیلی از دستاوردهای تحولات فعلی و آینده چین براساس اطلاعاتی است که در دسترس همگان است.

۱-۱۱ تحقیقات نظری درخصوص جنگ اطلاعاتی در چین

تحقیقاتی که چین در مورد نظریه جنگ اطلاعاتی انجام داده است، از دو منبع سرچشمه می‌گیرد: یکی، کشورهای خارجی به‌ویژه ایالات متحده آمریکا و دیگری، آمیزه‌ای از فلسفه چین باستان و تجربیات جنگی این کشور. اما مهم‌ترین بعد جنگ اطلاعاتی، پخش گسترده[1] و بهره‌برداری کامل از اطلاعات است. دولت چین در حال حاضر به‌علت ترس و وحشتی که از بروز بی‌ثباتی اجتماعی دارد، بیشتر تمایل به محدود کردن اطلاعات دارد. ازاین‌رو، در مقطع کنونی، استقرار آن سیستم‌های جنگ اطلاعاتی که مستلزم روند آزاد اطلاعات باشد، آسان نیست.

از سال ۱۹۹۱ تاکنون، تعدادی از نهادهای تحقیقات و توسعهٔ چین تحقیقاتی را در مورد نظریه و فناوری جنگ اطلاعاتی انجام داده‌اند. در این خصوص می‌توان به نهادهای تحقیقاتی ذیل اشاره کرد:

۱. مرکز تحقیقات استراتژی نظامی[2] در مؤسسه علوم[3] ارتش آزادی‌بخش خلق (که مهم‌ترین مرکز تحقیقات جنگ اطلاعاتی در چین به‌شمار می‌آید). برنامه تحقیقاتی در

---

1. Wide Distribution
2. Military Strategy Researeh Gentre
3. PLA Institute of Science

این نهاد، موارد ذیل را دربرمی‌گیرد: توسعه نظریه استراتژیک جنگ اطلاعاتی، جای دادن جنگ اطلاعاتی در درون تمامی سیستم‌های نظامی، ارائه و تدوین تاکتیک‌های مختلف برای پیشبرد موفقیت‌آمیز جنگ اطلاعاتی، مشارکت و سازمان‌دهی فناوری اطلاعات در جامعه بین‌المللی.

۲. مؤسسه فناوری الکترونیک،[1] وابسته به ارتش آزادی‌بخش خلق؛ این مؤسسه جنبه‌های فناورانه توسعه جنگ اطلاعاتی را محور مطالعات خود قرار داده است و انواع مختلف فناوری‌های جدید، دستگاه‌های جدید و سازه‌های جدید را بررسی و مطالعه می‌کند.

۳. ستاد مشترک ارتش آزادی‌بخش خلق، پژوهشکده شصت‌ویکم[2] و دانشکده مهندسی اطلاعات[3] نیز مطالعاتی را در مورد جنگ اطلاعاتی انجام داده‌اند. این دو نهاد، زیرمجموعه‌های ستاد مشترک ارتش آزادی‌بخش خلق‌اند.

۴. پژوهشکده مالکیت اطلاعات جاسوسی و سیستم رایانه‌ای ملی.[4]

۵. دانشگاه علوم و فناوری الکترونیک چنگ دُ.[5]

۶. گروه فناوری و فیزیک واقع در شانگهای،[6] وابسته به *مؤسسه* علوم چین.[7](۱)

۱-۱-۱۱ تحقیقات اولیه چین در مورد نظریه جنگ اطلاعاتی

گرچه شن وی کوآن اولین شخصی بود که مفهوم جنگ اطلاعاتی را در چین مطرح کرد، ولی وی یک ساختاربندی نظری فراگیر در این زمینه ارائه نداد. درحقیقت، این افسران بلندپایه ارتش بودند که چارچوب نظری جنگ اطلاعاتی چین را پس از عملیات طوفان صحرا ارائه دادند.

چینی‌ها تحقیقات درزمینه جنگ اطلاعاتی را با مطالعه مقالات خارجی و تحلیل

---

1. Electronic Technoligy
2. The 61th Research Centre
3. Information Engineering School
4. National Intelligence Property and Computer System Research Centre
5. Cheng-Do University of Electronic Seience and Technoligy
6. Shangheai Technology and Physics Department
7. China Institute of Science

پوشش تلویزیونی عملیات طوفان صحرا آغاز کردند. ازآنجاکه نیروهای مسلح چین هیچ تجربه‌ای درزمینه جنگ اطلاعاتی نداشتند، محال بود که دانشمندان نظامی چین به تنهایی بتوانند چارچوب‌هایی را در مورد جنگ اطلاعاتی طراحی کنند. ازاین‌رو، آنها از مفهوم و نظریه جنگ اطلاعاتی در آمریکا کپی‌برداری کردند. اما تفاوت‌ها میان جامعه و فرهنگ آمریکا و چین به‌قدری زیاد است که چینی‌ها نمی‌توانند هر چیزی را عیناً کپی‌برداری کنند و ازهمین‌رو، نظریه چینی‌ها در مورد جنگ اطلاعاتی ناقص و ناتمام است.

جنگ اطلاعاتی، به‌عنوان یک مفهوم در حوزه «جنگ و جنگیدن»، هنوز در مرحله تکاملی خود قرار دارد و رو به توسعه است. در نتیجه، تعریف جنگ اطلاعاتی در وضعیتی است که مدام در حال دگرگونی است و به‌موازات تحولات علمی و فناورانه تغییر خواهد کرد. چین درزمینه برداشتی که از جنگ اطلاعاتی دارد از ایالات متحده آمریکا تقلید می‌کند، اما این تقلید نمی‌تواند به طراحی نظریه‌ای در مورد جنگ اطلاعاتی در چین منتهی شود. تا سال ۲۰۰۱، وضعیت جنگ اطلاعاتی در چین آشفته بود و هیچ دستورالعمل یا طبقه‌بندی هوشمندانه‌ای به‌طور رسمی و در سطح ملی وجود نداشت که تصویر کلی جنگ اطلاعاتی در چین را به‌طور دقیق توصیف کند.

۲-۱-۱۱ تحلیل مختصر تعریف ایالات متحده از جنگ اطلاعاتی

تعریف موسعی که دانشگاهیان و نظامیان درباره جنگ اطلاعاتی در ایالات متحده آمریکا به‌کار می‌برند به قرار ذیل است:

۱. اطلاعات می‌تواند تصمیم‌گیری در مورد استقرار استراتژیک نیروهای نظامی و رزمایش‌های تاکتیکی را چه در زمان صلح و چه در زمان جنگ تسهیل کند.

۲. هدف از انجام جنگ اطلاعاتی، تأثیرگذاری بر فرایند تصمیم‌گیری طرف مقابل و سود بردن از آن است.

۳. نتیجه جنگ اطلاعاتی این است که باعث می‌شود دشمن تصمیمات غلط اتخاذ کند، تصمیمات را به تأخیر بیاندازد یا اصلاً هیچ تصمیمی اتخاذ نکند.

۴. هدف جنگ اطلاعاتی موفقیت‌آمیز، دستیابی به برتری اطلاعاتی بر طرف مقابل است.

۵. توانمندی عملیات اطلاعاتی به توانایی گردآوری، پردازش و پخش[1] بی‌وقفه اطلاعات و محروم‌سازی دشمن از دستیابی به چنین توانمندی‌ای اطلاق می‌شود.(۲)

به‌طور خلاصه، توانمندی عملیات اطلاعاتی، عمق استراتژیک در حوزه اطلاعات را مشخص می‌سازد.

اما تعریف محدودتر جنگ اطلاعاتی برحسب تاکتیک‌هایی که به‌کار گرفته می‌شوند انجام می‌گیرد که به قرار ذیل است:

۱. حمله الکترومغناطیسی به تأسیسات الکترونیکی و منهدم ساختن آنها،

۲. حمله به شبکه‌های رایانه‌ای،

۳. فریب دادن، کنترل کردن، تحریف و ارائه اطلاعات غلط به‌منظور گمراه کردن دشمن،

۴. گمراه‌سازی روانی،

۵. حفاظت از مرزها و گشودن رمزها.[2]

در ایالات متحده، جنگ اطلاعاتی در حال حاضر بعد از یازده سپتامبر به سطح پیشرفته‌تری رسیده است. در جنگ افغانستان، سیستم اطلاعاتی مرکز فرماندهی ایالات متحده ۶۵۰ هزار کیلومتر مربع قلمرو افغانستان را به ۱۰۰۰ ناحیهٔ جنگی کوچک برای انجام عملیات جنگ اطلاعاتی تقسیم کرد. پس از آن، ارتش آمریکا از ماهواره‌های شناسایی استفاده نمود.

این ماهواره‌ها، اطلاعات هر ناحیه را گردآوری و تحلیل و سپس آنها را به فرماندهی مرکزی نواحی نظامی در فلوریدا[3] ارسال می‌کردند؛ ازاین‌گذشته قادر بودند در هر شرایط آب‌وهوایی، عملیات کنترل و نظارت را در سراسر افغانستان انجام دهند. یکی از نمونه‌های بارز تصمیم‌گیری از فاصله یک هزار مایلی، این بود که هواپیماهای شناسایی بدون‌سرنشین عکس‌هایی را از سراسر افغانستان می‌گرفتند و آنها را به فرماندهی مرکزی نواحی نظامی می‌فرستادند. این فرماندهی نیز پس از بررسی عکس‌ها و تصاویر، با به‌کارگیری هواپیماهای بدون‌سرنشین به موشک‌های هدایت‌شونده به اهداف شناسایی شده حمله می‌کرد.

---

1. Distribution
2. Protect And Decipher Encryption
3. Central Military Area Command in Florida

بعد از عملیات طوفان صحرا و جنگ کوزوو، ارتش آمریکا مفهوم «نبرد شبکه‌محور» را بیان کرد. ارتش آمریکا با طرح این مفهوم به دنبال آن بود که همه انواع سیستم‌های تسلیحاتی یا مقرهای پرتاب تسلیحات را با شبکه رایانه‌ای یکپارچه سازد تا بتواند همه واحدهای ارتش را از داخل مرکز شبکه، فرماندهی و کنترل کند. نبرد شبکه‌محور کارایی عملیات‌ها را بسیار بهبود بخشیده و عملیات جنگی را به سطح بالاتری ارتقا داده است. کارشناسان نظامی آمریکا سه مزیت نبرد شبکه‌محور را مورد توجه قرار داده‌اند:

اولاً، نبرد شبکه‌محور نیروهای عملیاتی پراکنده را یکپارچه می‌سازد و از این طریق باعث می‌شود این نیروها توانایی هجومی خود را متوازن و تقویت کنند و کارکردهای نظامی چندجانبه‌ای انجام دهند. در جنگ سنتی، ارتباطات و امکان گردآوری نیروها و تسلیحات، محدود است و ازاین‌رو همه نیروهای لجستیکی فعالیت‌های خود را بر ارائه خدمات در خط مقدم متمرکز می‌کنند و در اطراف اهداف حفاظت شده مستقر می‌شوند. این وضعیت، نیروهای پراکنده لجستیکی را در شرایط نامطلوبی قرار می‌دهد؛ زیرا متمرکزسازی سریع نیروهای لجستیکی و اجرای برنامه حمله در این وضعیت امکان‌پذیر نیست. در عصر جنگ اطلاعاتی، گسترش کارآمدی حسگرها در فواصل طولانی، افزایش برد تسلیحات و تقویت توانایی انتقال اطلاعات باعث شده‌اند خدمات تدارکاتی ـ لجستیکی لازم را در اختیار هریک از واحدهای نظامی که پراکنده‌اند قرار گیرند.

دیگر ضرورتی ندارد که برای متمرکزسازی توان جنگیدن در میدان نبرد، نیروهای رزمی نیز متمرکز شوند ـ در این حالت است که انقلاب در امور نظامی می‌تواند روی دهد، چرا که، مزیت‌های نظامی واضح‌اند. تعریف توان جنگیدن از «متمرکزسازی نیروهای رزمی در جلو نیروهای دشمن» به «متمرکزسازی قدرت آتش و اطلاعات» تغییر کرده است، در نتیجه، خطرات[1] جنگیدن نیز کاهش می‌یابد. علاوه‌بر این، حجم کار بخش لجستیک نیز کاهش می‌یابد زیرا واحدهای نظامی پشت جبهه نبرد مدام در حال حرکت نخواهند بود. حجم کار، مراقبت‌های بهداشتی و حمل‌ونقل، عرضه کالاها و تجهیزاتی از قبیل سوخت، مهمات نظامی و غیره، پخش و پراکندن کارآمد نیروها و تسلیحات را امکان‌پذیر می‌سازد و زمینه حمله هم‌زمان به چند هدف متفاوت را فراهم می‌کند.

---

1. Risks

ثانیاً، به کمک نبرد شبکه‌محور، هر سرباز می‌تواند کل میدان نبرد را مشاهده کند و می‌تواند مقصود و هدف فرمانده را درک کند. در این وضعیت، با کمک سیستم فرماندهی و کنترل می‌توان حرکت و جابه‌جایی نیروها را محدود و هماهنگ کرد و عملیات‌های انفرادی و مشترک را به‌نحوی مؤثر اجرا کرد.

ثالثاً، هر برنامه عملیات جنگی کلاً شبکه‌ای می‌شود. بعد از آنکه یگان‌های متعدد رزمی به کمک شبکه‌ها در فضای نبرد به یکدیگر متصل شدند، نیروها و تسلیحات پراکنده را می‌توان هماهنگ کرد و اقدام مؤثری را انجام داد. شیوه جنگیدن نیز متحول می‌شود، به‌طوری‌که به‌سرعت می‌توان شرایط نیروها و تسلیحات را با وضعیت‌های جدید میدان نبرد منطبق و سازگار کرد. کارآمدی به استحکام و کیفیت بالای زیرساخت اطلاعاتی بستگی خواهد داشت. دو نوع شبکه وجود دارد:

۱. شبکه سخت[1] و فیزیکی که موجودیت‌های نظامی را به یکدیگر پیوند می‌دهد.

۲. شبکه نرم،[2] رویه‌مند[3] و مجازی.

هر دو شبکه درمجموع، یک سیستم رزمی را تشکیل می‌دهند که فرایندها و روندها را به یکدیگر متصل می‌سازند. کیفیت اتصال نرم[4] عاملی مهم در تعیین چگونگی همکاری هماهنگ نیروها با یکدیگر و کلید شکل‌دهی به توان جنگی[5] نیروها و تسلیحات به‌شمار می‌آید. اما، نه میزان پیوندهای شبکه‌ای و نزدیک و درهم‌تنیده این دو نوع شبکه، بلکه میزان تناسب آنها با یکدیگر است که کارآمدی آنها را تعیین می‌کند.

چین این دیدگاه‌ها را مطالعه کرده و کانون توجه خود را از «نبرد سایبر»[6] به نبرد مقرمحور[7] تغییر داده است. جنگ سایبر ایستگاه‌های راداری، سیستم‌های اطلاعاتی، شبکه‌های رایانه‌ای و وب‌سایت‌های رایانه‌ای دشمن را نابود می‌سازد. اهداف جنگ سایبر، رایانه‌ها و شبکه‌هایی‌اند که این نوع جنگ را اداره می‌کنند. تاکتیک‌های اساسی‌ای که در

---

1. Hard Network
2. Soft Network
3. Proeedual
4. Soft Connection
5. Fighting Capacity
6. Cyber Wafdare
7. Platform Centric Warfare

این نوع جنگ به‌کار برده می‌شود عبارت‌اند از: حمله به شبکه‌های رایانه‌ای، ارسال ویروس‌های الکترونیک، هک کردن‌های ویرانگر و غیره. نبرد مقرمحور، درست عکس نبرد شبکه‌محور است. «نبرد مقرمحور» باعث می‌شود روند «نظارت، برآورد، دقت و تصمیم» کُند و ناکارآمد به‌نظر برسد و هدردهنده منابع نبرد جلوه‌گر شود. عملیات‌های نبرد مقرمحور نه بر شبکه‌ها و رایانه‌ها بلکه بر مقرها و پیوندهای میان مقرها استوار است.

در ارتش آمریکا، تمایزاتی اساسی میان نبرد سایبر و نبرد شبکه‌محور وجود دارد. نبرد سایبر، رایانه‌ها و شبکه‌ها را ابزارهای اصلی اطلاعات قلمداد می‌کند. در مدل جدید جنگ، حمله و دفاع برحسب وضعیت شبکه‌ها و حوزه فرماندهی تعریف می‌شوند. نبرد سایبر، عرصهٔ آزمایش میزان قابلیت‌های نظامی در یک میدان نبرد نامرئی است. این نوع نبرد، تلفیق ویژگی‌های زمان جنگ و زمان صلح را در خود دارد و نه تنها در میدان نبرد در زمان جنگ بلکه در هر زمان دیگری نیز شیوه‌ای مهم برای پیشبرد همکاری به‌شمار می‌آید.

در نبرد مقرمحور، عمدتاً مقرهای تسلیحاتی، محور اقدامات است. هر مقر، اطلاعات میدان نبرد را دریافت و ارسال می‌کند، اما تبادل هم‌زمان اطلاعات میان مقرهای فرادست و فرودست به‌هیچ‌وجه صورت نمی‌گیرد و روندی که انجام می‌گیرد، کُند است. علاوه‌بر این، پخش و تسهیم اطلاعات میان مقرها بسیار محدود است و این وضعیت باعث می‌شود که افسران فرماندهی، خود به میدان نبرد بروند و به کمک فرایند مشاهده، قضاوت و تصمیم‌گیری، شخصاً اقدامات را هماهنگ سازند. این شیوه ناکارآمد است چرا که وقت را هدر می‌دهد، به توسعه یک سیستم یکپارچه برای پیشبرد جنگ کمک نمی‌کند و توان جنگی را نیز می‌کاهد.

همان‌گونه که در بالا نیز شرح داده شد، هرچند نبرد شبکه‌محور از فناوری شبکه رایانه‌ای به‌طور کامل بهره‌برداری کرده است، اما این نوع جنگ، رزم را به درون شبکه رایانه‌ای نمی‌کشاند. نبرد شبکه‌محور شبکه‌های رایانه‌ای را محور و بنیان جنگیدن قلمداد می‌کند و میدان نبرد، نیروها و هر مقر تسلیحاتی را به‌عنوان یک مجموعه در نظر می‌گیرد و یک کل ارگانیک تلقی می‌کند؛ و از این روش است که به ارتقای کارآمدی رزم کمک می‌کند. بنابراین، نبرد شبکه‌محور، مدل جدیدی برای رزم است. این جنگ باعث می‌شود تسهیم اطلاعات در همه سطوح و در همه جهات زمینه انجام

عملیات‌های مرکب[۱] را فراهم سازد و ازسوی‌دیگر نیز کارایی رزم را ارتقا می‌دهد.[۳]

در این خصوص می‌توان گفت که «نبرد شبکه‌محور» جلوه‌ای از جنگ اطلاعاتی پیشرفته‌تر است و آشکارا نشان می‌دهد که جنگ اطلاعاتی آمریکا چگونه جهان را رهبری می‌کند. نظریه و فناوری جنگ اطلاعاتی مدام رو به توسعه است. ازاین‌رو، استراتژی جنگ اطلاعاتی باعث می‌شود که آمادگی به‌کارگیری تاکتیک‌ها و نیز ابزارهای فناورانه در گستره‌ای که ظاهراً پایانی ندارد شکل گیرد.

۳-۱-۱۱ ترویج تحقیقات درزمینه جنگ اطلاعاتی در چین

بعد از عملیات طوفان صحرا در سال ۱۹۹۱، چین رفته‌رفته به اهمیت فناوری برتر و قدرت اطلاعاتی در عصر جهانی شدن و وابستگی متقابل اذعان کرد. چین می‌خواهد به یک مشارکت‌کننده سیاسی و اقتصادی بزرگ در جامعه جهانی مبدل شود؛ چرا که اقدامات اطلاعاتی در حال حاضر نقش مهمی در روابط بین‌الملل ایفا می‌کند. چین در سال‌های اخیر، رشد چشمگیری را ازلحاظ قدرت اقتصادی و ملی تجربه کرده است. به دنبال این رشد چشمگیر، چین معتقد است که جامعه بین‌المللی به‌صورت جهان چندقطبی در خواهد آمد. چین ازمنظر استراتژیک و نظامی به جنگ اطلاعاتی می‌نگرد و در این راستا، جنگ اطلاعاتی چاره‌ای برای علاج ضعف‌های موجود در سیستم نظامی کهنه چین قلمداد می‌شود، زیرا شیوه‌های کم‌هزینه و ساده‌ای را ارائه می‌دهد که به کشورهای ضعیف‌تر مجال می‌بخشد تا با سیطره نظامی کشورهایی از قبیل آمریکا و ژاپن مقابله کنند. در مورد توان نظامی قاطع ایالات متحده آمریکا، جنگ اطلاعاتی می‌تواند راه‌حلی کم‌هزینه برای «ضرورت بازسازی سریع توان نظامی چین بعد از حمله» ارائه دهد. استراتژی‌پردازان چینی امیدوارند که به‌کارگیری فناوری اطلاعات در تجهیزات نظامی بتواند نیاز به بودجه‌های هنگفت نظامی را کاهش دهد.

در تمام مدت بیست سال گذشته، توانایی پردازش اطلاعات به‌سرعت رشد کرده است اما هزینه‌های انجام این کار هر روز کاهش یافته است. بااین‌همه، این رخداد، فقط جنبه‌ای از وضعیت موجود است. اگر به شیوه‌ای دیگر محاسبه کنیم، هزینه‌های جنگ

---

۱. Combined Operations: عملیات‌هایی که هر سه نیروی زمینی، هوایی و دریایی در آنها مشارکت دارند ـ م.

اطلاعاتی بسیار بالاست. هزینه‌های فناوری نظامی و سیستم‌های زیرساختی سنتی به‌نحو چشمگیری افزایش یافته است. هرچند هزینه پردازش یک قطعه از اطلاعات به‌علت ظهور «عامل ده» در سی سال گذشته کاهش یافته است اما هزینه سیستم فرماندهی به حدی رو به افزایش است که کل بودجه دفاعی چین را خواهد بلعید.

بنابراین، سرعت توسعه جنگ اطلاعاتی در چین به مقدار بودجه‌ای که می‌توان تخصیص داد و نیز به گستره اهتمام چین به توسعه جنگ اطلاعاتی بستگی خواهد داشت. برخی از پروژه‌ها و سیستم‌ها پشتیبانی مالی عظیمی را می‌طلبند. برای مثال، سیستم‌های زیربنایی شناسایی در فضا و سایر سیستم‌های مرتبط، به‌ویژه استقرار شبکه ماهواره‌ای چندمنظوره و با قابلیت پوشش‌دهی جهات شش‌گانه با وجود آنکه به گردآوری اطلاعات می‌پردازند، به بودجه‌ای هنگفت نیاز دارند که پوشش مالی هزینه‌های گسترده و بلندمدت آنها را به‌طور مستمر تضمین کند.

دانشمندان و کارشناسان چینی که درزمینه جنگ اطلاعاتی چین قلم‌فرسایی کرده‌اند، فلسفه‌های سنتی‌تر چین در مورد جنگیدن را که مبتنی‌بر کتاب *هنر جنگ*[1] سون‌تسو و کتاب‌های *جنگ خلق*[2] و *۳۶ استراتژی*[3] مائوتسه‌دنگ[4] است، به نظریه جنگ اطلاعاتی وارد ساخته‌اند. توانمندی مالی و فنی چین در حدی نیست که بتواند از شیوه‌ای که ایالات متحده در عملیات‌های جنگ اطلاعاتی به‌کار می‌برد، به‌طور کامل کپی‌برداری کند؛ ازاین‌رو، طبیعی و قابل فهم است که این کشور توجه خود را به طراحی و بسط نظریه جنگ اطلاعاتی به سبک چینی معطوف خواهد ساخت.

محورهای اصلی این سبک به قرار ذیل‌اند:

۱. در جنگ اطلاعاتی تدافعی برای رفع ضعف‌هایی که در حوزه فناوری وجود دارد می‌توان از شیوه‌های غیرفناورانه از قبیل ظاهرسازی، پنهان کاری و انتشار اطلاعات گمراه‌کننده استفاده کرد. اما این رویکرد چه‌بسا ممکن است در عمل ثمربخش نباشد. برای مثال، در قضیه عملیات طوفان صحرا، نیروهای عراقی نتوانستند خود را از تیررس

---

1. The Art of War
2. People War
3. 36 Strategies
4. Mao Tze Dong

حملات موشکی[۱] و بمباران‌هایی که ماهواره‌های شناسایی آمریکا آنها را هدایت می‌کردند پنهان سازند و بگریزند.

۲. در جنگ اطلاعاتی تهاجمی کارشناسان چینی از «به‌کارگیری نیروی ضعیف برای مقابله با نیروی قوی» حمایت می‌کنند و پیشنهاد می‌دهند که در حملات پیش‌دستانه به «مراکز فرماندهی» و «سیستم کنترل و شناسایی» دشمن نه از استراتژی‌های تدافعی بلکه از استراتژی‌های تهاجمی استفاده شود. این پیشنهاد به این علت مطرح شده است که چین در حال حاضر فقط می‌تواند نبرد سایبر انجام دهد و فاقد توانمندی نبرد شبکه‌محور است.

کارشناسان و دانشمندان جنگ اطلاعاتی چین که در بخش‌های نظامی و دانشگاهی فعالیت دارند، مباحث عمیقی را در مورد ماهیت، جایگاه، کارویژه، رهنمودها،[۲] اصول، روش‌ها و رویه‌های[۳] جنگ اطلاعاتی مطرح کرده‌اند. در دسامبر ۱۹۹۴، چین یک سلسله اجلاس‌های سطح بالا و سمینارهای بزرگی را در مورد «تحلیل سیستم پدافند ملی» و انقلاب فنی ـ نظامی برگزار کرد؛ مسئول سازمان‌دهی این اجلاس‌ها و سمینارها کمیسیون علوم چین[۴] بود. به دنبال این اجلاس‌ها و سمینارها، سازمان فناوری و صنعت برای دفاع مالی[۵] نیز در اکتبر ۱۹۹۵، سمیناری را در مورد «نتایج انقلاب در امور نظامی» برگزار کرد. شاخص‌ترین نویسندگانی که درخصوص موضوعات مرتبط با «جنگ اطلاعاتی در سطوح داخلی و بین‌المللی» در چین قلم‌فرسایی می‌کنند، افرادی از قبیل دکتر ویگوآنگ شن،[۶] ژنرال پوفنگ وانگ،[۷] سرهنگ باووگان وانگ[۸] و ژنرال بانگای یوآن[۹] هستند.

در سال ۱۹۹۵، ژنرال پوفنگ وانگ، یکی از کارشناسان جنگ اطلاعاتی برای نخستین بار پیشنهاد داد که کتاب *جنگ خلق* مائوتسه‌دنگ وارد ادبیات جنگ اطلاعاتی شود. به‌نظر وی، کارشناسان امور برق و الکترونیک، رایانه و اطلاعات، محور و نقطه اتکای

---

۱. منظور، موشک‌های کروز است.

2. Guidlines
3. Practices
4. Commission on Science
5. Technology and Industry for National Defence
6. Weiguang Shen
7. General Pu Feng Wang
8. Baocun Wang
9. General Banggai Yuan

جنگ *خلق* جدید می‌باشند و نقشی هم‌تراز با افسران رزمنده در میدان نبرد در جنگ‌های گذشته را ایفا می‌کنند. در اذهان مردم، جنگ اطلاعاتی باید با جنگ پیوند داده شود ـ جنگی که بتوان روی رایانه‌های خانگی نیز انجام داد و صدها و بلکه هزاران نفر را برای حمله به سیستم‌های رایانه‌ای دشمن بسیج کرد. چین تعداد زیادی کارشناس کارکشته نرم‌افزار در اختیار دارد که پتانسیل عظیمی در حوزه جنگ اطلاعاتی دارند.

کارشناس دیگری که جنگ اطلاعاتی را محور مطالعات خود قرار داد دکتر ویگوآنگ‌شن است. وی نوشته است که: «کل جامعه جایگزین میدان نبرد سنتی خواهد شد. اقشار مردم و سازمان‌های دولتی مختلف در فعالیت‌های سیاسی کشور خود یا سایر کشورها مشارکت خواهند کرد». وی تشکیل «ارتش محافظ اطلاعات» را پیشنهاد می‌دهد. این ارتش، متشکل از دانشمندان، افسران پلیس، سربازان و کارشناسان دیگری است که جنگ اطلاعاتی را می‌فهمند؛ به‌نظر وی، کارویژه اصلی این ارتش، دفاع از امنیت قلمرو اطلاعاتی ملی در برابر متجاوزان احتمالی خواهد بود.

در سال ۱۹۹۶، دکتر شن برای اولین بار پیشنهاد داد که «جنگ اطلاعاتی» به‌عنوان جنگی تعریف شود که در آن، طرفین با کنترل اطلاعات و افکار عمومی می‌کوشند ابتکار عمل را در میدان جنگ به‌دست گیرند. مانند آنچه در ایالات متحده وجود دارد، تأکید دکتر شن از «حفاظت از خود و کنترل دشمن» به «دفاع از خود و حمله به دشمن» تغییر کرده است. ژنرال وانگ نیز معتقد است که کلید پیروزی در جنگ اطلاعاتی، کنترل اطلاعات است.

در سال ۱۹۹۷، باووکان وانگ ماهیت، جایگاه و ویژگی‌های جنگ اطلاعاتی را توصیف کرد. وی معتقد بود که جنگ اطلاعاتی را می‌توان براساس سه معیار تقسیم‌بندی کرد: نوع، سطح، ویژگی. نوع جنگ اطلاعاتی با آزمایش قدرت میان حمله‌کننده و دفاع‌کننده طی دوره‌های صلح، تنش و جنگ مشخص می‌شود. جنگ اطلاعاتی در سه سطح روی می‌دهد: عقلایی، تاکتیکی و استراتژیک. ویژگی‌های جنگ اطلاعاتی عبارت‌اند از: فرماندهی و کنترل عملیات هوشمند، جنگ الکترونیک، جنگ روانی، کنترل فضا، جنگ رایانه‌ای با به‌کارگیری هکرها، نبرد مجازی و نبرد اقتصادی. جنبه‌های خاص جنگ اطلاعاتی عبارت‌اند از: پیچیدگی، شفافیت، محدودسازی هدف، مدت زمان کوتاه، تخریب‌کنندگی اندک، انسجام قوی و فرمانده قدرتمند. رویه‌هایی که

در جنگ اطلاعاتی به‌کار گرفته می‌شوند، تمهیداتی است که برای از میان بردن، فریب دادن، پنهان ساختن، تسریع، بهبود و تقویت امکان بقا و غیره انجام می‌گیرند. تحلیل وانگ سهم چشمگیری در ارتقای فهم مردم از جنگ اطلاعاتی در چین داشته است.

نویسنده دیگری که در مورد تعریف جنگ اطلاعاتی در چین قلم‌فرسایی کرده ژنرال یوآن است که در مراکز فرماندهی ستاد کل ارتش آزادی‌بخش خلق اشتغال دارد. وی دیدگاه خود را در مورد جنگ اطلاعاتی در سال ۱۹۹۹ بیان کرد: «جنگ اطلاعاتی، کشمکشی است که برای به چنگ آوردن و حفظ کنترل بر اطلاعات درمی‌گیرد؛ این جنگ، کشمکشی است که در آن، طرف‌های متخاصم می‌کوشند درزمینه کسب، کنترل و بهره‌برداری از اطلاعات، ابتکار عمل را به‌دست گیرند. جنگ اطلاعاتی، وضعیتی است که در آن، هریک از طرف‌های متخاصم می‌کوشند از یک‌سو، منابع اطلاعاتی، سیستم اطلاعاتی و سیستم‌های تسلیحاتی اطلاعات- محور دشمن را مختل سازند و از آنها به نفع خود بهره‌برداری کنند و ازسوی‌دیگر، از منابع اطلاعاتی، سیستم‌های اطلاعاتی و سیستم‌های تسلیحاتی اطلاعات- محور خودشان نیز بهره‌برداری و حفاظت کنند».(۴)

در سال ۲۰۰۰، ژنرال پوفنگ وانگ تبیین عمیق‌تر و جامع‌تری از «جنگ اطلاعاتی» ارائه داد و آن را از «ستیزه اطلاعاتی»[۱] متمایز کند. ژنرال وانگ معتقد بود که جنگ اطلاعاتی نوعی جنگ است و علاوه‌بر این یک نوع «روش‌شناسی جنگ»[۲] نیز به‌شمار می‌آید؛ حال آنکه ستیزه اطلاعاتی شیوه «جنگیدن»[۳] و «روش‌شناسی جنگیدن»[۴] است. این وجه جنگیدن در عرصه شبکه رایانه‌ای انجام می‌گیرد. ستیزه اطلاعاتی، مؤلفه‌هایی از قبیل سیستم‌های کشف و انتقال اطلاعات، به‌کارگیری اطلاعات در سیستم‌های تسلیحاتی و سیستم‌های پردازش و به‌کارگیری اطلاعات را در خود جای می‌دهد. اما جنگ اطلاعاتی، پدیده‌ای فراگیرتر است و ستیزه اطلاعاتی را نیز دربرمی‌گیرد و دو عنصر را باهم تلفیق می‌کند: از یک‌سو، اطلاعات و توانایی بهره‌برداری از آن در درون میدان نبرد و ازسوی‌دیگر، شبکه اطلاعاتی به‌عنوان یک

---

۱. در این کتاب، جنگ اطلاعاتی را در برابر Information Warfare قرار داده‌ام و برای Information War نیز برابر نهاد ستیزه اطلاعاتی را برگزیده‌ام ـ م.

2. War Methodology
3. Fighting
4. Fighting Methodology

زمین بازی. تعریفی که پوفنگ وانگ ارائه داده است به مفهوم نبرد شبکه‌محور، که ایالات متحده آمریکا به‌کار می‌برد، بسیار نزدیک است.(۵)

دانشمندان و کارشناسان چینی نبرد اطلاعاتی را به‌گونه‌ای تعریف کرده‌اند که چهار بعد ذیل را دربرمی‌گیرد:

۱. هدف‌گیری دقیق و امحای فیزیکی. حمله به مراکز فرماندهی کل، قرارگاه‌های فرماندهی، تجهیزات «فرماندهی، کنترل، ارتباطات، رایانه و جاسوسی» دشمن؛ استفاده از حملات هوشمند و مخفیانه و تسلیحات جنگی افقی برای اجرای حملات دقیق و حساب شده؛ بهره‌گیری از سیستم‌های حمل تسلیحات و تجهیزات که بتوانند بمب‌ها و توپ‌های هوشمند و موشک‌های کروز و غیره را حمل کنند.

۲. جنگ الکترونیک و کنترل طیف الکترومغناطیسی. مبارزه برای کنترل طیف الکترومغناطیسی یکی از ابعاد مهم پیروزی در میدان نبرد جنگ اطلاعاتی است.

۳. جنگ شبکه‌ای.[1] شبکه‌های رایانه‌ای می‌توانند شفافیت فرماندهی در میدان نبرد، ارائه داده‌های هم‌زمان و استفاده از ماهواره‌های شناسایی، سیستم‌های هوایی موقعیت‌یاب جهانی،[2] هواپیماهای شناسایی بدون سرنشین و سیستم‌های جهان‌گستر انتقال اطلاعات را امکان‌پذیر سازند.

۴. فرماندهی و کنترل عملیات ضریب و جنگ روانی. از جمله انتشار اطلاعات درست یا غلط برای تأثیرگذاری بر روحیه و رفتار دریافت‌کننده اطلاعات ابزارهای اصلی در این زمینه، تبلیغات رسانه‌ای (در رادیو و تلویزیون)، انتشار اعلامیه‌ها، ایمیل (پست الکترونیکی) و سایر ابزارهای ارتباطی.(۶)

همان‌گونه که پیش‌تر گفته شد، تعریفی که چین از جنگ اطلاعاتی ارائه می‌دهد به تعریفی که ایالات متحده آمریکا به‌کار می‌گیرد بسیار شبیه است. تفاوت عمده این است که چین فلسفه نظامی کهن خود را نیز که در کتاب *هنر جنگ* سون‌تسه و مفاهیم نظامی مندرج در کتاب *جنگ خلق* مائوتسه‌دنگ بیان شده‌اند، در درون نظریه جنگ اطلاعاتی خود گنجانده است.

---

1. Network Warfare
2. GPS

آیا چین می‌تواند اندیشه فلسفی ـ فرهنگی‌اش را براساس سنت‌های ملی و وضعیت نظامی خودش طرح‌ریزی کند و از این روش موفق شود سبک متمایز خاص خود را در حوزه نظریه جنگ اطلاعاتی ایجاد کند؟ در زمان نوشتن این سطور، این پرسش هنوز مسئله‌ای است که پاسخ دادن به آن دشوار است. به‌طور قطع روند جنگ اطلاعاتی در چین در حال حاضر شبیه وضعیت چهل یا پنجاه سال پیش است که این کشور توسعه تسلیحات هسته‌ای خود را آغاز کرد. در آن زمان، چین همان مسیری را طی کرد که اتحاد شوروی پیش از آن پیموده بود؛ چین ابتدا نظریه‌های اساسی و ساختارهای فناورانه اتحاد شوروی را برگرفت و پس از آن، نیم‌نگاهی نیز به فناوری هسته‌ای ایالات متحده انداخت؛ اما با وجود این، چارچوبه اساسی تأسیسات هسته‌ای این کشور همچنان روسی باقی ماند. این روش‌شناسی باعث نشد که چین در خط مقدم توسعه فناوری هسته‌ای قرار گیرد.

از همان ابتدا، چین نظریه‌های جنگ اطلاعاتی خود را از مدل‌های آمریکا برگرفت و از فناوری و تجهیزات آمریکایی استفاده کرد. ازاین‌رو، چین دریافته است که پیشی گرفتن از ایالات متحده آمریکا درزمینه توسعه جنگ اطلاعاتی در حال حاضر بسیار دشوار است. ایالات متحده آمریکا نخستین کشوری است که نظریه جنگ اطلاعاتی را طراحی کرده و «تحقیقات و توسعه» را در مورد آن انجام داده است و ازسوی‌دیگر، تسلیحات جنگ اطلاعاتی را تولید نموده و در چندین جنگ نیز در طول نبردها از آنها استفاده کرده است. ازاین‌رو، این کشور درزمینه جنگ اطلاعاتی در میان کشورهای جهان همچنان در مقام اول قرار می‌گیرد.

این احتمال وجود دارد که گرایش فعلی چین به توسعه نظریه و فناوری جنگ اطلاعاتی به‌سمت پیشبرد سبک چینی باشد. اما درعین‌حال، چین نظریه و فناوری اساسی آمریکایی‌ها را نیز به‌کار خواهد گرفت. این شیوه به آن معنا خواهد بود که چین از روندهای کشورهای دیگر پیروی خواهد کرد و در نتیجه، چینی‌ها جبران عقب‌ماندگی‌ها و پیشی گرفتن از دیگران را دشوار خواهند یافت. در حال حاضر، همچنان شکاف عظیمی میان تحقیقات در مورد نظریه جنگ اطلاعاتی و به‌کارگیری عملی آنها در چین وجود دارد.

در قرن بیست‌ویکم، به یمن وجود مقر قدرتمند شبکه اطلاعاتی، «استفاده گسترده از ماهواره‌های شناسایی با قطعیت بالا و سیستم‌های هشدار اولیه درزمینه زمان حمله در هدایت موشک‌های کروز» و نیز «به‌کارگیری بسیاری از انواع هواپیماهای جنگنده و شناسایی بدون سرنشین، سیستم‌های جنگی پردقت و پرسرعت و انواع و اقسام تسلیحاتی که کارکردهای متعددی در میدان جنگ دارند»، مؤلفه‌های مهمی خواهند بود که به جنگ اطلاعاتی و نبرد شبکه‌محور شکل خواهند داد. اما این مؤلفه‌ها همان جنبه‌هایی می‌باشند که نیروهای مسلح چین، در این زمینه‌ها کمترین پیشرفت را داشته‌اند. هرچند تلاش‌هایی که در دهه گذشته انجام گرفته است به تولید برخی سیستم‌های جنگ اطلاعاتی و تسلیحاتی جدید برای نیروهای مسلح چین انجامیده‌اند، اما این تلاش‌ها نه ازلحاظ عملکردی و نه ازلحاظ کمی، نیازهایی را که جنگ‌های آینده تحمیل خواهند کرد برآورده نمی‌سازند. علاوه‌بر این، نیروهای مسلح چین در حال حاضر، توانایی نبرد شبکه‌محور را در اختیار ندارند.

۱۱-۲ روند فعلی توسعه جنگ اطلاعاتی در چین

چین تعریف خاص خود را از جنگ اطلاعاتی مشخص ساخت و آن را به‌عنوان محور برنامه‌های خود پذیرفت؛ پس از این مرحله، این کشور، چه ازنظر نیروی انسانی و چه ازنظر منابع مالی، سرمایه‌گذاری سنگینی را برای توسعه هرچه بیشتر آن انجام داده و به دستاوردهای چشمگیری در زمینه‌های توسعه تسلیحات جدید، تأسیس شبکه برای ارتش و آموزش نیروهای ارتش دست یافته است.

۱۱-۲-۱ سیستم و ایجاد سیستم

در سال ۱۹۹۹، دانشکده مهندسی اطلاعات،[1] دانشکده اوزان و مقادیر[2] و دانشکده مهندسی برق[3] با دانشگاه مهندسی اطلاعات ارتش آزادی‌بخش خلق[4] ادغام شدند. این

1. The Information Engineering College
2. Metrology College
3. Etectronic Engieering College
4. PLA Information Engineering University

دانشگاه عهده‌دار توسعه فنی جنگ اطلاعاتی شد و سیزده استاد دانشگاه را به‌عنوان «مغزهای مورد اعتماد» به خدمت گرفت. سطح ساختار آکادمیک تیم آموزشی دانشگاه نیز ارتقا یافته است؛ برای مثال، آن افسر فن‌آموزی که در حوزه فناوری‌های اصلی مؤثر در جنگ اطلاعاتی مدرن آموزش می‌بیند، از توانمندی‌های خاصی در حوزه‌های ایمنی اطلاعات، مهندسی ارتباطات، اطلاعات فضایی و ساختاربندی فضایی و غیره برخوردار می‌شود. دوره‌هایی که در این دانشگاه ارائه می‌شود حوزه‌های موضوعی تخصصی از قبیل مهندسی برق، مهندسی اطلاعات، مهندسی شبکه، مهندسی کنترل و جنگ الکترونیک را دربرمی‌گیرد. یک گروه تحقیقاتی چندرشته‌ای درجهٔ یک نیز تشکیل شده و مأموریت یافته است که فعالیت‌های علمی پیشتازانه‌ای را درزمینه «توسعه علمی ـ فنی اطلاعات در دوران معاصر» انجام دهد.(۷)

در مه ۱۹۹۷، مراکز فرماندهی ستاد کل ارتش آزادی‌بخش خلق (به ریاست یوکای ژانک)[1] به همراه چهار کمیته رسمی رهبری اطلاعات، سمیناری درباره «جنگ اطلاعاتی و جنگ الکترونیک» برگزار کردند. در این سمینار، پیشنهاد شد که اطلاعات به معنای ظرفیت رزم به‌کار رود و مفهوم جنگ اطلاعاتی نیز به دو مفهوم «جنگ اطلاعاتی استراتژیک» و «جنگ اطلاعاتی برای دفاع ملی» تقسیم شود. یک گروه پیشتاز درزمینه پیشبرد جنگ اطلاعاتی نیز تشکیل شد تا به هدایت امور تحقیقات و توسعه در ارتش آزادی‌بخش خلق بپردازد.(۸)

برای توسعه تأسیسات تحقیقات نظامی از منابع غیرنظامی نیز استفاده شد. هی‌لی‌لین،[2] تحلیلگر ارشد *بی‌بی‌سی* درزمینه مسائل چین، مقاله‌ای منتشر ساخت و در این مقاله، اظهار داشت که دولت چین برای پیشبرد نوسازی ارتش و تقویت قدرت نظامی خود، مؤسسه تحقیقات نظامی در پکن تأسیس کرده است. یک منبع خبری دیپلماتیک نیز از پکن گزارش داد که جیانگ زمین رئیس‌جمهور سابق پکن، در دوران ریاست جمهوری خود، دستور تأسیس سازمانی جدای از وزارتخانه‌ها را صادر کرد؛ این سازمان وظیفه داشت از سال ۲۰۰۲ تحقیقات و توسعه درزمینه علوم و فناوری نظامی

1. Youcia Zhang
2. He Li Lin

در بخش‌های مختلف را باهم هماهنگ سازد. سازمان مذکور متشکل از افسران و کارشناسانی بود که در نهادهایی از قبیل کمیسیون علوم، فناوری و صنعت برای دفاع ملی،[1] آکادمی علوم چین و آکادمی مهندسی چین فعالیت می‌کردند. این مؤسسه تحقیقاتی با هدف توسعه فناوری و سخت‌افزارهای پیشرفته، با اداره جنگ‌افزارهای عمومی ارتش آزادی‌بخش خلق چین و سایر سازمان‌های مشابه همکاری خواهد کرد.

این سیر توسعه جنگ اطلاعاتی در چین چند بعد دارد. آکادمی علوم چین و آکادمی مهندسی چین در زمره واحدهای نظامی جای نمی‌گیرند بلکه، سازمان‌های غیرنظامی‌اند. هرچند بیشتر فعالیت‌های کمیسیون علوم، فناوری و صنعت برای دفاع ملی در حیطه امور و کارکردهای ارتش آزادی‌بخش خلق جای می‌گیرد، اما بااین‌حال، این سازمان یکی از ادارات زیرمجموعه شورای دولتی چین به‌شمار می‌آید. براساس این، ارتش آزادی‌بخش خلق برای ارائه خدمات به نظامیان در بلندمدت به منابع سازمان‌های غیرنظامی متکی خواهد بود. کار ویژه و جایگاه آکادمی علوم چین و آکادمی مهندسی چین با انجام یک سلسله انتصابات جدید بهبود یافته است. جوآنگ دی‌زو[2] شهردار سابق شانگهای به ریاست آکادمی مهندسی چین منصوب شد.

همه می‌دانند که در سال ۲۰۰۲، بودجه ۱۶۶ میلیارد یوآنی ارتش آزادی‌بخش خلق چین فقط در حدود یک‌سوم میزان واقعی هزینه‌های نظامی چین را تأمین می‌کرد. گرچه یکی از مقامات وزارت اقتصاد و امور دارایی در کنگره خلق ملی اظهار داشت که چین بودجه نظامی ویژه یا مخفی ندارد، اما تحلیلگران امور دفاعی در غرب معتقدند که بودجه تحقیقات و توسعه سیستم‌های تسلیحاتی پیشرفته گاهی اوقات عملاً از پژوهشکده‌های علمی یا سایر بودجه‌های غیرنظامی شورای دولتی منحرف و در مجاری مخفیانه هزینه می‌شوند.

در اکتبر ۱۹۹۸، منطقه نظامی شنیانگ[3] سمیناری در مورد «تعریفی که ارتش آزادی‌بخش خلق از جنگ اطلاعاتی ارائه داده است» برگزار کرد. در این سمینار، موضوعاتی از قبیل مختصات، جایگاه، کار ویژه، دستورالعمل‌ها، اصول، سبک، فرماندهی، امور هماهنگ‌سازی، لجستیک، مدیریت میدان نبرد و آموزش در حوزه جنگ اطلاعاتی

1. Commission of Sciences, Technology and Industry for National Defense
2. Guang Di Xu
3. Shenyang

مورد بحث و تبادل نظر قرار گرفت. کارشناسان لشکر پیاده نظام مکانیزهٔ ارتش آزادی‌بخش خلق پیش‌بینی کرده‌اند که «حمله اطلاعاتی» و «پدافند اطلاعاتی» در آینده احتمالاً باهم تلفیق خواهند شد. حمله اطلاعاتی، «حملات الکترونیک و شبکه‌ای، تخریب ارکان اطلاعاتی، حمله روانی و ارائه اطلاعات گمراه‌کننده در مورد امور نظامی» را دربرمی‌گیرد. پدافند اطلاعاتی مشتمل بر اقدام تلافی‌جویانه اطلاعاتی، حفاظت از اطلاعات و بازفراوری[1] اطلاعات خواهد بود.(۹)

چین توجه ویژه‌ای به جنگ‌های کوزوو و خلیج فارس داشته و اسنادی را که آمریکا درخصوص این دو جنگ منتشر کرده است، از جمله اسناد پنتاگون درزمینه «نبرد اطلاعاتی FM100-6[2]» و کتاب درسی *نبرد اطلاعاتی JP31-3*[3] را که از منابع آموزشی استاندارد درباره جنگ اطلاعاتی به‌شمار می‌آیند ترجمه کرده است.(۱۰)

ارتش آزادی‌بخش خلق، اولین «دستورالعمل درزمینه تضمین اطلاعات و رایانه‌ها» را منتشر و کمیته نظامی مرکزی حزب کمونیست چین[4] نیز آن را تصویب و امضا کرده است. این سند تازه انتشاریافته دربرگیرنده ۴۱ دستورالعمل است و بر همان مبنای اسناد «مقررات امنیتی ارتش آزادی‌بخش خلق چین» و «دستورالعمل ایمنی ـ امنیتی فناوری در ارتش آزادی‌بخش خلق چین» تنظیم شده است.(۱۱)

دانشگاه دفاع ملی چین، سیستم آفندی و پدافندی جنگ اطلاعاتی چین را توسعه داده و با موفقیت برآورد کرده است. سیستم پدافند و آفند شبکه‌ای، که در حال حاضر در مطالعات نظامی بین‌المللی به موضوعی شایع مبدل گشته، فناوری‌ای کلیدی به‌شمار می‌آید که کنترل پایگاه قدرت اطلاعاتی را به‌دست می‌گیرد و در آینده نیز در جنگ‌هایی که با فناوری‌های برتر سروکار دارند، نقشی اساسی ایفا خواهد کرد. برطبق گزارشی که روزنامه *ارتش آزادی‌بخش*[5] به چاپ رسانده، «یک گروه تحقیقاتی در دانشگاه دفاع ملی

---

1. Resumption
2. FM100-6 Information Combat
3. JP31-3 Information Combat
4. CPC Central Military Committee
5. Liberation Army Daily

چین پس از چهار سال فعالیت پژوهشی طاقت‌فرسا موفق شده است آخرین مدل تئوریک در مورد بخش‌های آفندی و پدافندی سیستم‌های شبکه‌ای را توسعه دهد».(۱۲)

چین هفتادویکمین عضو بین‌المللی اینترنت بود و در زمان نگارش این سطور، پنج شبکه رایانه‌ای اساسی را در داخل قلمرو خود راه‌اندازی کرده است. این شبکه‌ها عبارت‌اند از:

۱. شبکه سی.اس.تی چین،[1]
۲. شبکه رایانه‌ای آموزش تحقیقات علمی چین،[2]
۳. شبکه اطلاعاتی پل طلایی چین،[3]
۴. شبکه چاینایونین اینترنت،[4]
۵. شبکه اینترنتی رایانه‌های همگانی چین.[5](۱۳)

در ۱۶ ژانویه ۲۰۰۳، مرکز اطلاع‌رسانی شبکه اینترنتی چین[6] یازدهمین گزارش «آماری درباره وضعیت اینترنت در چین» را منتشر کرد. این گزارش نشان می‌داد که در ۳۱ دسامبر ۲۰۰۲، تعداد کاربران اینترنت در سرزمین اصلی چین با ۷۵/۴ درصد افزایش نسبت به سال قبل از آن به ۵۹،۱۰۰،۰۰۰ نفر رسیده است. این تعداد کاربر، تنها معادل نیمی از کاربران در ایالات متحده آمریکاست. این گزارش همچنین پیش‌بینی کرد که این رقم تا پایان سال ۲۰۰۴ به ۸۶،۳۰۰،۰۰۰ نفر افزایش خواهد یافت. برطبق این گزارش، کاربران شبکه اینترنت در چین تنها ۹ درصد کل کاربران در جهان و ۴/۶ درصد کل جمعیت این سرزمین را تشکیل می‌دهند؛ این بدان معناست که هنوز جا برای افزایش چشمگیر شمار کاربران در چین وجود دارد.(۱۴)

مؤسسه رایانه دانشگاه ووهان،[7] رشته «ایمنی اطلاعات» را در مقطع کارشناسی راه‌اندازی کرد و به‌طور رسمی در پاییز ۲۰۰۱ از دانشجویان جدید در این رشته نام‌نویسی کرد. وزیر آموزش‌وپرورش چین نیز این رشته را به تصویب رساند و در زمان

---

1. CSTNet
2. The Chinese Education and Scientific Research Computer Net
3. Chinese Golden Bridge Information Net
4. CHINAUNION Internet
5. Chinese Public Computer Internet
6. China Internet Network Information Centre (CINNIC)
7. Wuhan University

نگارش این سطور، این دانشگاه، تنها دانشگاه در کل چین است که در رشته ایمنی اطلاعات در مقطع کارشناسی دانشجو می‌پذیرد. رئیس دانشگاه ووهان می‌گوید گروه رایانه‌اش از سال ۱۹۸۴ دوره‌ای را در حوزه ایمنی و امور خصوصی رایانه ارائه کرده است. علاوه‌بر این، یک گروه تحقیقاتی نیز تشکیل شده است که به‌صورت تخصصی در مورد این زمینه و حوزه‌های موضوعی مرتبط با آن کار می‌کند. یکی از اعضای مؤسسه رایانه دانشگاه ووهان ادعا کرد که دانشگاه قصد دارد برای برگزاری این دوره در پاییز ۲۰۰۱، ۵۰ دانشجو جذب کند و در سال ۲۰۰۲ نیز این تعداد را به ۱۰۰ نفر افزایش خواهد داد.(۱۵)

۲-۲-۱۱ توسعه تسلیحات جدید برای بهره‌برداری در جنگ اطلاعاتی

پروژه‌های ذیل نشان می‌دهند که چین رفته‌رفته به توسعه تسلیحات جدید در حوزه جنگ اطلاعاتی نزدیک‌تر می‌شود:

«۱. رادارهای روزنه‌ای ترکیبی-[1] چین در تولید سیستم‌های حسگر از راه دور و چندمدلی مایکروویو[2] که می‌تواند در همه شرایط آب‌وهوایی حتی در زمانی که ۶۰ الی ۷۰ درصد آسمان را ابرها فراگرفته باشد، عمل‌کند، پیشتاز بوده است و رادارهای روزنه‌ای ترکیبی برای ارائه تصاویر پروضوح که هیچ محدودیتی ازنظر نور و شرایط جوی ندارند، از مختصات انتشار دوربرد سیگنال‌های راداری و توانمندی پردازش اطلاعات پیچیده مدارهای الکترونیکی و دیجیتالی مدرن استفاده می‌کند. یک سیستم شناسایی و تصویربرداری که توانمندی انجام عملیات در همه شرایط آب‌وهوایی را دارد و متشکل از رادیوسنج موج کوتاه، ارتفاع‌سنج راداری و موج‌یاب راداری است، با چهارمین فضاپیمای چین که «قایق الهی»نام داشت، پرتاب شد. دستگاه حسگر از راه دور، شش ماه پس از آنکه در مدار قرار گرفت، باز هم خوب کار می‌کرد و داده‌هایی که انباشته می‌شدند، بنیان فناورانه لازم را برای ماهواره‌های مخصوص نظارت بر اقیانوس‌ها فراهم می‌آوردند. به‌نظر می‌رسد استفاده ارتش آزادی‌بخش خلق از این نوع سیستم

1. Synthetic Aperture Radar (SAR)
2. Microwave

راداری در ماهواره‌ها تنش‌ها با تایوان و ایالات متحده را افزایش خواهد داد.(۱۶)

۲. آکادمی علوم چین، وابسته به مؤسسه علم فیزیک فنی شانگهای ــ[1] در حال حاضر، شش ماهواره چینی در فضا مستقراند که آکادمی علوم چین، مؤسسه علم فیزیک فنی شانگهای ساخته است. در ۲۵ مارس ۲۰۰۲، چین سومین فضاپیمای خود را با استفاده از پنج ابزار علمی به فضا پرتاب کرد. این فضاپیما حاوی یک طیف‌نگار مقایسه‌کننده[2] تصویربرداری با وضوح متوسط است که با کیفیتی بالا، از اهداف تصویربرداری می‌کند. تجهیزات تصویربرداری از رنگ آب دریاها و ثبت درجه حرارت، که بر روی اولین ماهواره دریاکاو چین نصب شده‌اند، نه تنها می‌توانند غلظت گل‌ولای معلق بر روی دریا، رنگ آب و غیره را زیر نظر بگیرند، بلکه قادرند درجه حرارت دریا را نیز محاسبه کنند.(۱۷)

۳. چین سومین کشوری است که سیستم جهت‌یابی ماهواره‌ای را در اختیار دارد ـ در پایان سال ۲۰۰۱، چین دومین ماهواره فضانوردی خود به نام «دب اکبر» را از مرکز پرتاب ماهواره‌های زیچانگ[3] پرتاب کرد و سومین کشوری شد که پس از آمریکا و روسیه سیستم هدایت ماهواره در اختیار دارد. این سیستم از دو ماهواره تشکیل شده است که همه قلمرو سرزمین چین را پوشش می‌دهد و اطلاعات ناوبری دقیق در اختیار شبکه‌های حمل‌ونقل ریلی و جاده‌ای قرار می‌دهد؛ علاوه‌بر اینکه نه تنها خدمات ناوبری را به کشتی‌های تجاری چین که در اقیانوس آرام تردد دارند ارائه می‌دهد بلکه، با هدایت ناوگان دریایی و حمل‌ونقل زمینی از طریق ماهواره‌ها می‌تواند نقش مهمی را در دفاع ملی ایفا کند. برطبق گزارش‌ها، در زمان نگارش این سطور، سیستم ناوبری نسل دوم چین در مرحله برنامه‌ریزی و طراحی قرار دارد.(۱۸)

۴. ماهواره‌های شکارچی کوچک ـ[4] چین در سال‌های اخیر با طراحی و اجرای مأموریت‌هایی با استفاده از ماهواره‌های بدون سرنشین و توسعه سیستم‌های ماهواره‌ای شناسایی، ارتباطات و ناوبری به ارتقای توانمندی‌های فضایی خود ادامه داده است.

---

1. Chinese Academy of Siences, Shaghai Institute of Technical Physics
2. Specrtocomparator
3. Xichang
4. Small Killer Satellites

تمامی سیستم‌های مستقر در فضا در برابر حملات آسیب‌پذیرند و ایالات متحده آمریکا، روسیه و چین، همه تولید سیستم‌های ضدماهواره‌ای را مورد توجه قرار داده‌اند و در برخی موارد نیز حتی این سیستم‌ها را آزمایش کرده‌اند. مقاله‌ای در روزنامه *سنگتائودیلی*،[1] چاپ هنگ‌کنگ در سال ۲۰۰۱ گزارش داد که پکن نوعی خرده ماهوارهٔ انگل‌وار را تولید کرده است که می‌تواند به ماهواره‌های بزرگ بچسبد و آنها را نابود کند.(۱۹)

۵. توپ بزرگ الکتریکی فوق سریع-[2] یکی از تسلیحات جدیدی که چین ساخته است، توپ بزرگ الکتریکی فوق سریع است که از انرژی گرمایی استفاده می‌کند و در حال حاضر به مرحله نهایی توسعه خود رسیده است و علاوه‌بر این، قرار است در سال ۲۰۰۵ آزمایش شود. دو نوع توپ بزرگ الکتریکی وجود دارد: توپ بزرگ الکترومغناطیسی و توپ بزرگ الکتروترمال.[3] با توجه به کاربردهای غیرنظامی‌ای که این دو نوع توپ دارند پرتابگرهای الکترومغناطیسی نیز نامیده می‌شوند. توپ بزرگ الکترومغناطیسی، یک سلاح استراتژیک است که برای پرتاب یک کلاهک به‌سمت هدف از نیروی الکترومغناطیسی استفاده می‌کند به‌طوری‌که آن کلاهک با سرعتی بسیار بالا هر ثانیه پانصد کیلومتر را می‌پیماید؛ در این خصوص باید خاطرنشان ساخت تسلیحات متعارف به‌قدری کند و کم‌سرعت‌اند که به پای این نوع سلاح نمی‌رسند. توپ بزرگ الکتروترمال برای پرتاب کلاهک به‌سمت هدف، که مسیر خود را با سرعتی در حدود سه کیلومتر در ثانیه می‌پیماید، از انرژی گرمایی ـ الکتریکی استفاده می‌کند و می‌توان از آن به‌عنوان سلاحی تاکتیکی سود جست. توپ‌های بزرگ الکتریکی می‌توانند از انواع و اقسام گلوله‌های چند گرمی کوچک گرفته تا کلاهک‌های چندتنی را که میزان نفوذ و قدرت حملهٔ سلاح را تا حد زیادی تقویت می‌کنند، شلیک کنند. این توپ‌ها علاوه‌بر این می‌توانند در آن واحد، بیش از یک کلاهک را در پرتابگرهای چندمرحله‌ای نصب کنند و بدین‌سان، کارآمدی رزمی آنها را به میزان زیادی افزایش دهند. در گزارش‌ها آمده است که توپ بزرگ الکتریکی بر روی زمین، در سطح دریا، در جو زمین، یا در فضا نصب خواهد شد. براساس برخی از گزارش‌های خبری، تحقیقات درزمینه تأثیر عوامل

1. Tsingtao Daily
2. Ultra Fast Electric Big Gun
3. Electro Thermal

مغناطیسی فضا بر توپ بزرگ نیز پیشرفت‌های مطلوبی داشته است.(۲۰)

۶. «ویندوز» چینی‌ـ[1] برآوردی که چنگ وی وانگ،[2] یکی از اعضای کمیته علوم و فناوری گروه جنگ‌افزارهای عمومی ارتش آزادی‌بخش خلق،[3] و هی کوآن وو،[4] معاون آکادمی مهندسی چین در ۱۱ ژانویه ۲۰۰۳ در مورد وضعیت فناوری تسلیحاتی در چین ارائه دادند نمایانگر پیشرفتی مهم و تعیین‌کننده در برنامه تحقیقاتی تولید واحد پردازشگر مرکزی به نام «مغز اژدها»[5] بود.(۲۱)

۷. توسعه ابررایانه‌ها ـ اطلاعیه رسمی‌ای که گروه افسانه چین[6] در ۳۰ آگوست ۲۰۰۲ منتشر کردند طراحی و ساخت سیستم ابررایانه‌ای به نام «افسانه سن‌تنگ ۱۸۰۰»[7] در پکن را اعلام کرد. در نتیجه، چین پس از ایالات متحده و ژاپن به سومین کشوری مبدل شد که ابررایانه می‌سازد.(۲۲) این ابررایانه، سازه‌ای مهم در سیستم شبکه فضایی ارتش چین به‌شمار می‌آید. آخرین ابررایانه، داون ـ۴۰۰۰ ـ ای ـ ۱۵ ـ اس[8] نام دارد که در شانگهای مستقر است و یک مسیریاب فوق پیشرفته به‌شمار می‌آید و دهمین ابررایانه سریع جهان است.

۸. توسعه سیستم‌های عامل ـ در ۲۸ سپتامبر ۲۰۰۲، مؤسسه فنی علوم رایانه‌ای آکادمی علوم چین جدیدترین نسخه ویرایش شده «واحد پردازشگر مرکزی» خود را که عملکرد بسیار نیز دارد، منتشر کرد.(۲۳) هفت گروه بزرگ که در حوزه فناوری اطلاعات فعالیت داشتند برای ساخت «مغز اژدها» به‌نحوی هماهنگ با یکدیگر همکاری کردند و اولین زنجیره صنعت فناوری اطلاعات را در چین تشکیل دادند. این شرکت‌ها عبارت بودند از: مؤسسه فناوری رایانه[9] وابسته به آکادمی علوم چین، گروه هایر،[10] گروه گریت

---

1. Chinese Windows
2. Cheng Wei Wang
3. The Science and Technology Committee of PLA General Armament Department
4. He Quan Wu
5. Dragon - Core
6. Chinese Legend Group
7. Legend Senteng 1800
8. Dawn - 4000 - A15s
9. Institute of Computing Technology
10. Haier Group

وال وابسته به شرکت نرم‌افزار گریت وال،[1] شرکت سی.اس.آند.اس،[2] شرکت کاس‌رد فلگ،[3] گروه داون[4] و گروه مغز اژدهای «قایق الهی».[۵(۲۴)]

۹. توسعه موشک‌های کروز ـ در ۱۲ ژانویه ۲۰۰۰، هفته‌نامه *دفاعی جونز*[6] گزارشی را در مورد توسعه موشک‌های کروز در چین منتشر کرد. در این گزارش، عکسی از موشک کروز چین به‌شمارهٔ سریال X-600 درج شده بود. چین در سال ۱۹۸۵ موشک کروز توربین‌دار خود را (که پرنده سرخ نام داشت و شکل و شمایل آن شبیه موشک روسی KH-55 است) آزمایش کرد.[(۲۵)]

پروژه‌هایی که در بالا بیان شدند، نشان می‌دهند که چین سیستم‌هایی را توسعه داده است که می‌توان آنها را در جنگ اطلاعاتی به‌کار برد. اما بااین‌حال، هرچند چین زمان و هزینه زیادی را صرف کرده و به دستاوردهای چشمگیری دست یافته است، اما هنوز راهی طولانی در پیش دارد تا به ایالات متحده آمریکا برسد.

۱۱-۲-۳ ایجاد نیروهای شبکه‌ای

چین پایگاه‌های جنگ اطلاعاتی تأسیس کرده است، ارتش ایالات متحده پنج پایگاه جنگ اطلاعاتی را شناسایی کرده است که تعداد زیادی از افراد مستعد درزمینه فناوری‌های برتر را گردهم آورده‌اند و نیروهای جنگ اطلاعاتی چین را آموزش می‌دهند. تحقیقاتی که انجام گرفته است، نشان می‌دهد که این ارتش الکترونیک ذخیره در حال حاضر، به‌قدری پرشمار است که می‌تواند به نیرویی بزرگ و بهره‌مند از توانایی جنگاوری مبدل شود و در سراسر قاره‌های جهان به انجام عملیات‌های جنگی دست زند.[(۲۶)]

۱۱-۲-۴ استراتژی جنگ اطلاعاتی

ارتش ایالات متحده ادعا می‌کند که استراتژی جنگ اطلاعاتی چین از پنج ترفند اول

---

1. Great Wall Software Company Of Great Wall Group
2. CS&S Ltd
3. CAS Red Flag Ltd
4. Dawn Group
5. "Divine Boat" Dragon Core
6. Jane's Defence Weekly

شگردهای سی‌وشش‌گانهٔ سنتی چین بهره می‌گیرد. این ترفندها عبارت‌اند از:

۱. **عبور از دریا با استتار، کاستن از هوشیاری دشمن با عملیات فریب**: برای مثال، ویروس‌هایی را در سرویس‌های معمولی شبکه‌ای یا پست الکترونیک مخفی کنید.

۲. **محاصره کردن یک دولت برای نجات دادن دولت دیگر**: با سلاح‌های هسته‌ای به دشمن حمله نکنید زیرا امکان دارد با عملیات تلافی‌جویانه شما را نابود سازد. در عوض، به گنجینه دشمن ـ از قبیل سیستم مالی، نهادهای دولتی و غیره ـ حمله کنید.

۳. **کشتن با استفاده از چاقوی قرضی**: حتی اگر شما آن‌قدر قوی نیستید که به‌طور مستقیم به دشمن حمله کنید می‌توانید از قدرت دیگران (به نفع خود) بهره‌برداری کنید. برای مثال به‌وسیله شخص ثالث، ویروس به شبکه‌های دشمن وارد کنید یا اطلاعات غلط برای دشمن ارسال کنید.

۴. **به انتظار اقدام دشمن نشستن**: تحلیل بردن توان رزمی دشمن و سپس حمله کردن. نظریه‌ای که در کتاب *جنگ خلق* آمده است می‌گوید: «حملات پرشماری به راه بیاندازید اما نیروهای اصلی خود را گسیل ندارید، بلکه فقط مدام دشمن را بگریزانید؛ پس از این اقدامات است که نیروهای اصلی را می‌توان به میدان سرنوشت‌ساز نبرد نهایی گسیل داشت».

۵. **غارت خانه‌ای که در آتش می‌سوزد**: برای مثال، هکری که وانمود می‌کند دانشجو یا تاجر است می‌تواند بی‌سروصدا به سیستم‌های رایانه‌ای دشمن وارد شود، آنها را تخریب نماید و منابع اطلاعاتی را نیز سرقت کند.[۲۷]

۵-۲-۱۱ دشواری‌های فراروی توسعه جنگ اطلاعاتی

هرچند چین توانسته است در عرصه‌های نظریه، استراتژی، تاکتیک، تسلیحات و رایانه‌های مرتبط با جنگ اطلاعاتی به پیشرفت‌های مهمی دست یابد، اما برخی نقطه‌ضعف‌های اساسی وجود دارد که تأثیری تعیین‌کننده بر روند توسعه جنگ اطلاعاتی در چین خواهد گذاشت. این نقطه‌ضعف‌ها عبارت‌اند از:

۱. چین فاقد خلاقیت در حوزه‌های نرم‌افزار و سخت‌افزار برای توسعه جنگ اطلاعاتی است، بیشتر نرم‌افزارها و سخت‌افزارهای رایانه‌ای چین وارداتی‌اند. هسته اصلی فناوری اطلاعات در کنترل غرب قرار دارد؛ ۸۰ درصد منابع اطلاعاتی که به‌صورت آن‌لاین در شبکه

اینترنت وجود دارد، به زبان انگلیسی است و تنها کمتر از ۴ درصد آنها به زبان چینی‌اند.

۲. سخت‌افزارهای کلیدی و فناوری‌های اصلی در این حوزه همچنان در کنترل کشورهای بیگانه است. شرکت‌های اینتل و مایکروسافت[1] در گزارشی که در مارس سال ۲۰۰۰ منتشر کردند اعلام داشتند که پنتیوم و ویندوز ۹۸[2] حاوی نرم‌افزاری مخفی شده‌اند که می‌تواند به داده‌های خصوصی کاربران آن‌لاین دسترسی یابند.

تدابیری که چین برای مقابله با این وضعیت اندیشید، ممنوع کردن آن رایانه‌های شخصی‌ای بود که در هنگام اتصال به شبکه اینترنت در ادارات دولتی از پردازشگرهای پنتیوم استفاده می‌کردند.

۳. چین نرم‌افزار سیستم عامل خاص خودش را ندارد، مایکروسافت بیش از ۹۰ درصد سیستم‌های عامل رایانه‌هایی را که در دولت، ارتش و مؤسسات علمی، مالی و تجاری به‌کار برده می‌شوند، عرضه می‌کند.

۴. عرضه استعدادها در عرصه فناوری اطلاعات، بی‌اندازه اندک‌اند، مقدار زیادی از عرضه بهترین ظرفیت‌ها و استعدادهای چینی به دره سیلیکان[3] رفته‌اند. زمان نگارش این سطور، حدود سه هزار نفر در چین در بخش توسعه فناوری اطلاعات فعالیت دارند. حال آنکه در ایالات متحده آمریکا این تعداد به چهارصد هزار نفر می‌رسد که هرساله هفتاد هزار نفر دیگر نیز به این جرگه می‌پیوندند. ارتباطات چین با سایر نقاط جهان در حوزه اینترنت با شبکه کابلی فیبر نوری (که در بستر دریا نصب می‌شود و به‌وسیله شرکت ماهواره‌ای ارتباطاتی[4] که یک شرکت مخابراتی آمریکایی به‌شمار می‌آید و گستره فعالیت‌های آن، حوزه اقیانوس‌های آرام و اطلس است) انجام می‌گیرد. ۱۰ سرور از سیزده سرور مشهور در جهان، آمریکایی‌اند و تحت کنترل ارتش ایالات متحده قرار دارند.(۲۸)

۶-۲-۱۱ تهدیدهای فراروی امنیت اطلاعاتی

در این عصر اطلاعاتی شدن جهان، انواع و اقسام مختلف سیستم‌های اطلاعات‌محور،

---

1. Intel and Microsoft
2. Pentium and Windows 98
3. Silicon Valley
4. Communication Satelilte Corporation (Comsat)

نقش‌هایی کلیدی برای دولت و مؤسسات خصوصی و تجاری در چین ایفا می‌کنند. سازوکارهای ایمنی اطلاعات مؤلفه‌های تعیین‌کننده‌ای برای توسعه مطمئن فناوری اطلاعات و جلوگیری از حمله به تأسیسات اطلاعاتی به‌شمار می‌آیند. وزیر صنایع اطلاعاتی چین به شش تهدید عمده‌ای که امنیت اطلاعاتی این کشور را به خطر می‌اندازد اشاره کرده است:

۱. **نارسایی و ناکافی بودن تأسیسات امنیتی و حفاظتی شبکه‌ها و اطلاعات**: این مسئله معضلی ویژه در حوزه فعالیت‌های مالی به‌شمار می‌آید. در چین نرخ جرائم مرتبط با فناوری‌های برتر به‌شدت افزایش یافته است و جرائم رایانه‌ای، معضلی است که هر روز حادتر می‌شود.

۲. **نداشتن توانایی کنترل، نظارت و سنجش فناوری و تجهیزات وارداتی**: چین هیچ روشی برای ارزیابی ایمنی تجهیزات اصلی محمل‌های پنهان شده در اختیار ندارد.

۳. **اتکای بیش از حد صنعت اطلاعات به تجهیزات خارجی**: هرچند صنعت تولید رایانه چین بسیار بهبود یافته است اما بسیاری از قطعات اصلی رایانه‌های چینی را شرکت‌هایی تولید می‌کنند که ظرفیت تولیدشان پایین است و هیچ اهتمامی به حوزه تحقیقات و توسعه ندارند.

۴. **نبود اقتدار در مدیریت ایمنی اطلاعات**: چین سازمان ملی یکپارچه‌ای را که اقتدار کاملی برای پیشبرد و اجرای موضوعات مرتبط با ایمنی اطلاعات داشته باشد تأسیس نکرده است.

۵. **رشد سریع و روزافزون شمار جرائم اطلاعاتی**: می‌توان اطلاعات را سرقت کرد و به‌نحو آسان‌تری از فواصل طولانی منتقل کرد. جرائم رایانه‌ای در حوزه‌های امور مالی و بانکداری در چین به‌سرعت رو به افزایش است.

۶. **ناآگاهی جامعه چین از اهمیت ایمنی اطلاعات**: به‌نظر می‌رسد مردم چین احساس می‌کنند درجه اطلاعاتی شدن[1] در چین در حدی نیست که در مورد ایمنی اطلاعات نگران باشند. ازاین‌رو، تصور می‌کنند که ایمنی اطلاعات در آینده به یک دغدغه تبدیل خواهد شد نه حالا.

ایمنی اطلاعات مسئله‌ای است که چینی‌ها در سطح ملی به‌وجود آن اذعان کرده‌اند. اگر این معضلات را نتوان به‌صورت جدی و ریشه‌ای حل کرد، چه‌بسا ممکن است امنیت اطلاعات در چین با تهدید جدی مواجه شود.(۲۹)

---

1. Degree of Informatisation

۳-۱۱ تاکتیک‌های جنگ اطلاعاتی که پکن می‌تواند برای حمله بـه تـایوان از آنها استفاده کند

تایوان یکی از توسعه‌یافته‌ترین مناطق ازلحاظ تأسیسات اینترنتی است. درجه اطلاعـاتی شدن در تایوان بسیار بالاست. بیش از ۶،۰۰۰ سرور شـبکه جهـانی اینترنـت در تـایوان وجود دارد و بیشتر این سرورها نیز با فعالیـت‌هـای تجـاری سـروکار دارنـد. بـالغ بـر دو میلیون کاربر اینترنت[1] در تـایوان وجـود دارد. اینترنـت کـاربرد وسـیعی در حـوزه‌هـای سیاست، اقتصاد، علم و فناوری، ارتش، فرهنگ و زندگی روزمره افراد مقـیم دارد. شـبکه اینترنت در حال حاضر به یکی از مؤلفه‌های مهم جامعه تایوان مبدل شده است. ازاین‌رو، اگر جنگ اطلاعاتی در گیرد، کل جامعه تایوان به‌شدت تحت تأثیر قـرار خواهـد گرفـت. توسعهٔ بیشتر شبکه اطلاعاتی در تایوان باعث می‌شود که کل جامعه در همه ابعاد به این شبکه وابسته باشد. در این خصوص، اگر دشـمن، جنـگ اطلاعـاتی علیـه تـایوان بـه راه بیاندازد، این کشور خسارت‌های اقتصادی بیشتری را متحمّل خواهد شد و با تهدیدهـای افزون‌تری روبه‌رو خواهد شد. در این صورت، امنیت شبکه و بقـای موجودیـت تـایوان بـا فشارهای عظیمی مواجه خواهد شد.

مساحت کل جزیره تایوان حـدود ۳۶۰۰۰ کیلـومتر مربـع اسـت و از طرفـی هـم در نزدیکی سرزمین اصلی چین واقع شده است. تایوان توانایی پدافندی پـایینی دارد و زمـانی هم که درصورت مواجهه با حمله نظامی برای واکنش و هشدار اولیه در اختیار دارد، کوتـاه است. محدودیت‌های فراروی این منطقه (جزیـره تـایوان) بـر میـزان مقاومـت آن در برابـر حملات خارجی به زیربناهای صنعتی و سیستم‌های جنگ‌افزاری تأثیر می‌گذارند.

در حال حاضر، چهار «سیستم فرماندهی، کنترل، ارتباطات و جاسوسـی» در ارتـش تایوان وجود دارد؛ این سیستم‌ها عبـارت‌انـد از: هنـگ‌شـان،[2] سیـستم لـوزی،[3] سیـستم داچنگ[4] و سیستم کیانگ وانگ،[5] در میان این چهار سیستم، کیانگ وانگ، پیشرفته‌تـرین

---

1. Netizen
2. Heng Shan
3. Lu Zi
4. Da Cheng
5. Qiang Wang

سیستم است که گسترهٔ عملیاتی آن تا سرزمین اصلی چین امتداد دارد. سیستم کیانگ وانگ از ایستگاه راداری زمینی، سیستم‌های فرماندهی و کنترل خودکار و سیستم هواپیمایی هشدار اولیه تشکیل شده است و برای یکپارچه‌سازی سیستم موقعیت‌یاب راداری، پایگاه هوایی و اطلاعات ضدهوایی از سیستم‌های رایانه‌ای پیشرفته‌ای بهره می‌گیرد.

تاکنون تایوان مراکز کنترل نظامی را هم در زیرزمین و هم در فضای جو تأسیس کرده است، تأسیسات شبکه‌ای خود را به یک «سیستم فرماندهی، کنترل، ارتباطات و جاسوسی» مجهز ساخته و سیستم رادارهای ضدهوایی آمریکایی پیشرفته خود را به‌گونه‌ای با شرایط جدید منطبق کرده است که بتوانند همه اهداف را در سراسر حریم هوایی جزیره تایوان و منطقه ساحلی سرزمین اصلی چین تا برد ۴۶۳ کیلومتری کنترل کنند. کیانگ وانگ می‌تواند بیش از ۶۰۰ هدف را به‌صورت هم‌زمان نشان دهد و می‌تواند ۱۵۰ هواپیمای نظامی را برای انجام عملیات‌های رهگیری هوایی آرایش دهد. در این راستا فرایند رزم، از ارائه طرح‌های دقیق گرفته تا اجرای قاطعانه آنها در میدان نبرد را به‌صورت کاملاً خودکار پیش می‌برد، آرایش رزمی را تعیین و رهگیری ضدهوایی اهداف را رهبری و فرماندهی می‌کند. سیستم کیانگ وانگ برای تسهیل روند فرماندهی رزم و کوتاه کردن مدت زمان واکنش می‌تواند با سیستم‌های هنگ‌شان، لوزی و داچنگ تلفیق شود.

کل سیستم اطلاعات رزمی هنگ‌شان در تایپه مستقر است. این سیستم هسته اصلی سیستم فرماندهی، کنترل، ارتباط و جاسوسی را تشکیل می‌دهد که مرکز گردآوری اطلاعات و فرماندهی نیروهای رزمی قوای سه‌گانه (زمینی، هوایی و دریایی) را در خود دارد. این سیستم در اوایل دهه ۱۹۸۰ تأسیس شد و در جولای ۱۹۹۰ فعالیت خود را آغاز کرد؛ سیستم هنگ‌شان از بخش‌های رزم، منابع انسانی و لجستیک و برخی سیستم‌های فرعی دیگر تشکیل شده است. این سیستم با یک رایانه اختصاصی و دستگاه پردازش و نمایش داده‌ها بین افسر بخش پدافندی و جنگ‌افزارها در منطقه جنگی و مراکز فرماندهی پدافندی ارتباط برقرار می‌کند و باعث می‌شود که انتقال اطلاعات به تسهیل فرماندهی و هماهنگ‌سازی نیروها در سراسر قلمرو تایوان بیانجامد.

سیستم لوزی در ژوئن ۱۹۹۶ فعالیت خود را آغاز کرد. این سیستم شیوه‌ای را

به‌کار می‌گیرد که تمرکز و تمرکززدایی را باهم تلفیق می‌کند. گره[1] این سیستم به مراکز فرماندهی ارتش و فرماندهی لشکری و پدافندی اتکا دارد. این سیستم به‌منظور پخش اطلاعات رزم، همه یگان‌ها را به یکدیگر پیوند می‌دهد. در حال حاضر، سیستم لوزی یک پایگاه اطلاع‌رسانی بزرگ به‌شمار می‌آید و در آینده نیز توسعه خواهد یافت و به سیستم پشتیبانی و سیاستگذاری خودکار مبدل خواهد شد.

نکته دیگری که در مورد جنگ اطلاعاتی می‌توان گفت این است که ویروس‌های رایانه‌ای می‌توانند سیستم‌های فرماندهی را تخریب کنند و از کار بیاندازند. ازاین‌رو تایوان به‌منظور کاهش احتمال حمله‌های ویروس‌ها و تقویت توانایی‌های خود درزمینه سیستم هشدار اولیه تدابیر مقتضی را اندیشیده است.

این سیستم برای پیشگیری از وارد آمدن خسارت بر توانایی فرماندهی و کنترل از شیوه متفرق‌سازی[2] بهره می‌گیرد. شبکه نظامی تایوان به‌منظور انجام اقدامات احتیاطی برای مقابله با هکرها یا حملات ویروسی در حال حاضر شیوه کارآمد منزوی‌سازی موجودیت[3] را برگزیده است. علاوه‌بر این، ارتش تایوان برای انجام اقدامات احتیاطی جهت مقابله با حملات هکرها و ویروس‌های رایانه‌ای، مقدمات ایجاد سازوکارهای کشف حملات را فراهم کرده است.(۳۰)

ازآنجاکه بیشتر سرورها و کاربران خطوط شبکه اینترنت در شهرهای تایپه و هینچو[4] متمرکزاند، سیستم‌های هنگ‌شان و داچنگ نیز در تایپه استقرار یافته‌اند. اگر پکن حمله «جنگ اطلاعاتی» علیه تایوان انجام دهد، اولین هدف آن شهرهای تایپه و هینچو خواهد بود و در این راستا از رویه‌های تاکتیکی ذیل استفاده خواهد کرد:

۱. حملات گسترده و پرشدت با استفاده از هکرهای رایانه‌ای به سبک *جنگ خلق*،

۲. حملات موشکی به شبکه توزیع و انتقال برق شمال و جنوب تایوان به‌منظور قطع برق شمال تایوان و پس از آن، قطع کل شبکه برق تایوان،

۳. پرتاب بمب‌های نوترونی در هوای شمال، جنوب و مرکز تایوان در این تاکتیک،

---

1. Node
2. Dispersion
3. Entity Isolation
4. Hsinchu

با به‌کارگیری پالس الکترومغناطیسی پرشدت، حملاتی علیه تجهیزات شبکه مخابراتی و الکترونیکی انجام می‌گیرد و این تأسیسات از کار می‌افتد،

۴. استفاده از موشک‌های کروز با انجام حملات دقیق و حساب شده به سیستم‌های «فرماندهی، کنترل، ارتباطات و جاسوسی» تایوان،

۵. حمله به «ماهواره‌های شناسایی» تایوان یا منهدم ساختن آنها،

۶. استفاده از ماهواره‌های مستقر در مدار زمین، ماهواره‌های کوچک و فضاپیماهای «قایق الهی» به‌منظور جاسوسی در مورد تحرکات ناوهای هواپیمابر آمریکا. با توجه به اینکه ارتش آمریکا (درصورت حمله چین به تایوان) در عملیات نظامی در تایوان درگیر می‌شود، پکن نیز با استفاده از موشک‌های کروز یا موشک‌های تاکتیکی، میان‌برد و کوتاه‌برد به نیروهای نظامی آمریکا حمله خواهد کرد.

در حال حاضر، توانمندی پکن درزمینه جنگ اطلاعاتی، بیشتر از تایوان است. اما، اگر ایالات متحده آمریکا در جنگ اطلاعاتی در تایوان درگیر شود، پکن چه‌بسا ممکن است پیروز میدان نباشد؛ ازاین‌رو، پکن ناگزیر است حداکثر تا پایان دهه حاضر، سیستم «فرماندهی، کنترل، ارتباطات، رایانه، جاسوسی، نظارت و شناسایی» خود را با شتاب بیشتری تقویت کند، روند توسعه ماهواره «دب اکبر» و ماهواره‌های شناسایی کوچک را شتاب بخشد و تدابیری را که برای تأمین ایمنی شبکه و حفاظت از سایت‌های محرمانه خود می‌اندیشد، تقویت کند.

۴-۱۱ مقاومت یکپارچه آمریکا و تایوان در برابر جنگ اطلاعاتی پکن

برای تایوان دشوار است که در برابر جنگ اطلاعاتی‌ای که پکن علیه این کشور به راه اندازد از خود دفاع کند. اگر ایالات متحده آمریکا و تایوان درصورت وقوع جنگ اطلاعاتی با یکدیگر متحد شوند، این دو کشور تاکتیک‌های ذیل را به اجرا در خواهند آورد:

۱. حملات به سیستم‌های رایانه‌ای با هکرها،

۲. ایجاد اختلال، نابودسازی و حمله به تأسیسات مخابراتی، ماهواره‌های شناسایی و نظامی، که در نتیجه، سیستم فرماندهی، کنترل، ارتباطات، رایانه، نظارت و جاسوسی چین از کار خواهد افتاد (اواخر اکتبر ۲۰۰۴ نیروی هوایی ایالات متحده به‌طور مخفیانه

سلاح جدیدی را تولید کرد که می‌تواند برای ایجاد اختلال در ارتباطات مخابراتی ماهواره‌های دشمن مورد استفاده قرار گیرد).[۳۱]

۳. وارد ساختن ویروس به درون رایانه‌های چین به‌منظور انهدام سیستم‌های رایانه‌ای که در درون آنها نصب شده‌اند،

۴. مختل ساختن نرم‌افزار رایانه با سیستم‌های عامل ویندوز مایکروسافت،

۵. تحقیق و بررسی حوزه‌های اقتصادی، تجاری و مالی چین به‌منظور کشف و بهره‌برداری از ضعف‌های موجود در شبکه‌های چین و پس از آن، منهدم‌سازی آنها،

۶. جمع‌آوری اطلاعات نظامی، اقتصادی، مالی و سیاسی از روی همه وب‌سایت‌های احتمالی در چین،

۷. ایجاد اختلال در آن شبکه‌های واسط که در خارج از شبکه چین فعالیت دارند،

۸. نصب شبکه ردیاب صوتی برای شناسایی زیردریایی‌های چینی در بستر دریا مبادی ورودی کانال‌های مهمی که دریاهای جنوب و شرق چین را به اقیانوس آرام متصل می‌کنند.

۱۱-۵ احتمال جنگ اطلاعاتی میان چین و ایالات متحده آمریکا

۱۱-۵-۱ جنگ اطلاعاتی چین و ایالات متحده در پس وقایع برخورد هواپیماهای دو کشور

فعالیت‌های جاسوسی و ضدجاسوسی چین علیه ایالات متحده آمریکا تنها ظاهر اقداماتی است که چین در حوزه جنگ اطلاعاتی انجام می‌دهد. سقوط هواپیماهای جاسوسی EP-3 سال ۲۰۰۱ در خاک چین، این موضوع را آشکارا نشان داد. این‌گونه فعالیت‌ها از گسترش رقابت اطلاعاتی میان دو کشور در آینده حکایت دارد.

اگر به پرسنل جنگ اطلاعاتی آمریکا بنگریم، درمی‌یابیم که جنگ اطلاعاتی فقط نبرد ویروسی نیست، بلکه کل نبرد اطلاعاتی نظامی را دربرمی‌گیرد و ازاین‌رو، نه تنها جنگ الکترونیک و رزم‌های پنهان را دربرخواهد گرفت بلکه شامل شکل سنتی جنگ روانی نیز خواهد بود. در الگوی آرمانی جنگ اطلاعاتی، هرگونه اطلاعات کارآمد در جنگ اطلاعاتی، هماهنگی تعامل‌گونه‌ای با سیستم‌های تسلیحاتی سنتی دارد. نتیجه

منطقی این تعامل آن است که سرعت واکنش ایالات متحده بیش از دشمنانش خواهد بود و آمریکا قادر خواهد بود طرح‌های نظامی دشمن را زیر نظر بگیرد.

نظامیان ایالات متحده معتقدند که هدف نهایی و غایی جنگ اطلاعاتی فقط شکست دادن دشمنان نیست، بلکه سوق دادن دشمنان و ناگزیر کردن آنها به انجام اقداماتی مطابق با اراده ایالات متحده آمریکا را نیز دربرمی‌گیرد. علاوه‌بر این، جنگ اطلاعاتی باید همه استراتژی‌های نظامی را بادقت هرچه تمام‌تر باهم تلفیق کند و همکاری و تعامل نزدیکی با روابط عمومی و دیپلماتیک داشته باشد.

هرچند آمریکایی‌ها در حال حاضر چین را چالشگر ـ و رقیب ـ اصلی هژمونی خود در حوزه جنگ اطلاعاتی می‌دانند، اما واقعیت این است که جنگ اطلاعاتی در چین در نخستین مراحل توسعه خود قرار دارد. نظامیان ایالات متحده معتقدند «چین مدل جدیدی از ابرشاهراه اطلاعاتی نظامیان را براساس یک شبکه فیبر نوری که در مانورهای نظامی سال ۱۹۹۸ راه‌اندازی کرده بود، تولید کرده است و راه‌اندازی این شبکه نیز دشوارتر از مایکروویوها و رادیو است». ایالات متحده آمریکا بر این باور است که، در پرتو آنچه در بالا ذکر شد، چین در حال حاضر یکی از پیشرفته‌ترین کشورهای جهان ازنظر توانمندی‌های ضدجاسوسی است. نظامیان آمریکایی معتقدند که چینی‌ها آمادگی خود درزمینه جنگ اطلاعاتی را با مشاهده «جنگ بدون تماس» در حملات هوایی ناتو به کوزوو تقویت کرده‌اند.

ایالات متحده آمریکا بعضی از نقطه‌ضعف‌های جنگ اطلاعاتی چین را نیز شناسایی کرده است. مسئله کلیدی این است که بیشتر سیستم‌های رایانه‌ای در چین از ویندوزهای شرکت مایکروسافت استفاده می‌کنند. یکی از مقامات عالی‌رتبه ارتش آمریکا گفت: «همه کشورهایی که می‌توانند تهدید جنگ اطلاعاتی علیه آمریکا ایجاد کنند، از نرم‌افزارهای آمریکایی استفاده می‌کنند. برای مثال، ۹۰ درصد سیستم‌های رایانه‌ای ارتش چین از ویندوزهای شرکت مایکروسافت و تراشه‌های شرکت اینتل[1] استفاده می‌کنند. این کشورها می‌دانند اگر به ما حمله کنند، ما توانمندی بیشتری برای انجام اقدامات تلافی‌جویانه داریم. ما قوی‌ترین و پرتجربه‌ترین کشور در حوزه جنگ اطلاعاتی هستیم».(۳۲)

1. Intel

۲-۵-۱۱ جنگ خلق و جنگ شبکه‌ای[1]

۱-۲-۵-۱۱ سازمان شبه‌نظامی اطلاعاتی چین می‌کوشد با انجام حمله‌ای غافلگیرانه ضربه‌ای کاری بر دشمن وارد آورد

ارتش آزادی‌بخش خلق چین به‌منظور بهره‌گیری از استراتژی خلق، ایجاد یک شبکه جنگ اطلاعاتی را آغاز کرده است. در آینده، اگر چین و ایالات متحده آمریکا رودرروی یکدیگر قرار گیرند، یک سازمان شبه‌نظامی اطلاعاتی متشکل از توده مردم به ایجاد یک اتحاد جنگ اطلاعاتی با سازمان شبه‌نظامی اطلاعاتی رسمی[3] دست خواهد زد. چینی‌ها از اتباع خارجی چینیتبار که در آن سوی اقیانوس آرام زندگی می‌کنند کمک‌های اطلاعاتی دریافت خواهند کرد. این تنها نقطه قوت و مزیتی است که چین درزمینه جنگ اطلاعاتی دارد.

۲-۲-۵-۱۱ هدف قرار دادن سیستم‌های مالی و نظامی ایالات متحده

ارتش آزادی‌بخش خلق چین در این اواخر یگان‌های «سربازان رایانه» و «سربازان شبکه» را ایجاد کرده است که به زبان‌های بیگانه کاملاً مسلطاند و سیستم‌های شبکه دشمن را به‌خوبی می‌شناسند. این سربازان با انواع و اقسام فنون حمله آشنایی دارند. کارآمدی آنها در هنگام رزم به‌مراتب بیشتر از افراد پیش‌کسوتی است که در حال حاضر نقش فعالانه‌ای در پیشبرد رقابت شبکه‌ای میان چین و آمریکا ایفا می‌کنند. در جنگ‌های آینده، از جمله وظایفی که «سربازان رایانه» در ارتش آزادی‌بخش خلق احتمالاً برعهده خواهند گرفت، موارد ذیل خواهد بود:

۱. سد کردن شبکه‌های ارتباطی دشمن،

۲. نفوذ در سیستم شبکه‌ای پنتاگون به‌منظور سرقت اطلاعات مورد نظر.

این سربازان نیروهای شبه‌نظامی اطلاعاتی جنگ خلق اطلاعاتی قلمداد می‌شوند که ارتش آزادی‌بخش خلق چین به‌منظور تخریب سیستم شبکه مالی دشمن از آنها استفاده خواهد کرد و خسارت‌های سنگینی را بر نظام اقتصادی دشمن وارد خواهد ساخت.

---

1. Network Warfare
3. Official Information Militia

دانشمندان علوم استراتژیک ایالات متحده آمریکا معتقدند حمله جنگ اطلاعاتی چین به آمریکا را می‌توان به دو سطح عمده تقسیم کرد. ابتدا شبکه‌های ارتش آمریکا مورد حمله قرار خواهد گرفت. در این سطح، هکرهای چینی به سیستم‌های شبکه خدمات عمومی که امور لجستیکی و سیستم‌های ارتباطات و حمل‌ونقل را تنظیم و کنترل می‌کنند، حمله خواهند کرد. در سطح دوم، حملات چینی‌ها بر مراکز مالی، شبکه‌های مخابراتی، شبکه‌های برق‌رسانی و ... متمرکز خواهند شد و سیستم‌های ارتباطی رهبران سیاسی تأثیرگذار آمریکا را مختل خواهد کرد. اگر چین به تایوان حمله کند احتمالاً از موشک‌های بالستیک استفاده خواهد کرد و علاوه‌بر این از فنون جنگ اطلاعاتی نیز برای حمله به تأسیسات نظامی حیاتی تایوان سود خواهد جست. «جنگ شبکه‌ها» که هم‌اکنون میان چین و ایالات متحده درگرفته است، می‌تواند پیش‌زمینه بروز جنگ اطلاعاتی در آینده میان آنها به‌شمار آید.[۳۳]

۶-۱۱ نتیجه‌گیری

اولین میدان نبرد جنگ اطلاعاتی که چینی‌ها در آن درگیر خواهند شد، شاید تنگه‌های تایوان خواهد بود و این محتمل‌ترین دلیلی است که نشان می‌دهد چرا چین اکنون در حال تشکیل نیروهای رزمی جنگ اطلاعاتی خود است. چینی‌ها قبل از آنکه حمله گسترده و پیاده کردن نیروهای خود در تایوان را آغاز کنند به‌طور هم‌زمان از دو جهت، جنگ اطلاعاتی را به راه خواهند انداخت. حمله موج اول علیه شبکه‌های رایانه‌ای و سیستم‌های الکترومغناطیسی سازوکارهای سیاسی، تأسیسات نظامی و مراکز تأمین انرژی و حمل‌ونقل خواهد بود. هدف از این حمله، این است که ارتش و دولت در تمامی سطوح فلج و مختل شوند. بعد از حمله موج اول، چین با موشک‌های کروز و موشک‌های بالستیک میان‌برد به اهداف حمله خواهد کرد.

در این میان، ارتش آزادی‌بخش خلق به‌منظور پیشگیری از هرگونه تأخیر در عملیات و نیز حمله به نیروهای کمکی‌ای که ارتش آمریکا (مستقر در پایگاه‌های گوام، اکیناوا، ژاپن و کره جنوبی) در اختیار تایوان قرار می‌دهد، با نفوذ در شبکه‌های رایانه‌ای به سیستم‌های پشتیبانی هوایی ایالات متحده در منطقه حمله خواهد کرد. ارتش

آمریکا نیز به ناگزیر با تمام توان خود به دو شیوه به این حمله پاسخ خواهد داد. نخست اینکه، به آن شبکه کابلی فیبر نوری که در بستر دریا قرار دارد و چین برای برقراری ارتباط با سایر نقاط جهان از آن استفاده می‌کند و نیز به شبکه رایانه‌ای چین حمله خواهد کرد و دوم اینکه، به حمله‌ای همه‌جانبه علیه سیستم‌های رایانه‌ای جنگ اطلاعاتی چین دست خواهد زد. فرماندهی ناحیه نظمی فوژو[1] در منطقه نانیچینگ،[2] سیستم‌های رایانه‌ای کمیسیون نظامی پکن،[3] همه فرودگاه‌های نظامی، شبکه رایانه پایگاه‌های نیروی دریایی، انبارهای مهمات نظامی، مخازن نفت، ایستگاه‌های راه‌آهن و فرودگاه‌ها آماج این حملات قرار خواهند گرفت.

ایالات متحده آمریکا احتمالاً از مدلی از موشک‌های کروز استفاده خواهد کرد که با حمل دستگاه‌های تولید پالس الکترومغناطیسی قوی می‌توانند به سیستم‌های رایانه‌ای جنگ اطلاعاتی چین حمله کنند و آنها را نابود سازند و پیش از آن، ماهواره‌های شناسایی و مجهز به سیستم موقعیت‌یاب جهانی را آماج حملات گسترده قرار دهند؛ در این خصوص ایالات متحده آمریکا نابودسازی کامل چشم‌ها و گوش‌های «جنگ اطلاعاتی» چین را سرلوحه اهداف خود قرار خواهد داد. براساس این، جنگ اطلاعاتی نقطه آغاز جنگ تمام‌عیار میان چین و ایالات متحده آمریکا خواهد بود. هرچند هنوز چنین ارتشی با قابلیت جنگ اطلاعاتی در چین به‌طور کامل شکل نگرفته است، اما باید گفت جنگ گسترده‌ای در این حوزه بین آمریکا و چین آغاز خواهد شد. در حال حاضر، توانایی تکنولوژیکی چین برای انجام جنگ اطلاعاتی به‌نسبت ضعیف است؛ با وجود این، احتمال می‌رود چین در آینده چنین جنگی را به راه بیاندازد.

این فصل تصویری کلی در مورد اقداماتی که ارتش آزادی‌بخش خلق چین در سال‌های اخیر برای آمادگی در صورت وقوع جنگ اطلاعاتی انجام داده، عرضه کرده است. دراین‌باره، نابرابری شدید در عرصه موازنه نیروها میان چین و تایوان را تبیین کرده است؛ حال این سؤال بیان می‌شود که برای حراست از امنیت تایوان چگونه می‌توان این نابرابری

---

1. Fuzhou
2. Nanijing
۳. این کمیسیون، وابسته به مراکز فرماندهی کمیته مرکزی حزب کمونیست چین در ستاد کل نیروهای مسلح چین است.

شدید را کاهش داد؟ از دیدگاه نویسنده، دو پیشنهاد را می‌توان مورد توجه قرار داد:

نخست اینکه «سیستم فرماندهی، کنترل، ارتباطات، رایانه، جاسوسی، نظارت و شناسایی» توان آن برای مصون ماندن در برابر حملات باید تا آن حد که امکان دارد تقویت شود و آموزش ارتش و قابلیت‌های کیفی آن باید بسیار برتر از آموزش‌ها و قابلیت‌های کیفی موجود در ارتش جمهوری خلق چین باشد. دوم اینکه، تایوان باید عملیات‌های فرماندهی، کنترل، ارتباطات، رایانه، جاسوسی، نظارت و شناسایی خود را با (رویکردهای) ایالات متحده آمریکا و به‌ویژه با سیستم‌های ضدماهواره‌ای این کشور تلفیق کند تا بتواند سیستم‌های ارتباطات، هوانوردی و شناسایی ماهواره‌ای جمهوری خلق چین را مختل، فلج و منهدم کند. در این صورت، وضعیت فعلی در تنگه‌های تایوان حفظ خواهد شد و تداوم خواهد یافت.

پی‌نوشت‌ها

1. James Mulvenon, *The PLA and Information Warfare* (Santa Monica, CA: Rand), p.179.
2. Toshi Yoshihara, 'Chinese Information Warfare: A Phantom Menace of Emerging Threat? Rand, November 2001, PP.3-5.
3. Baocun Wang, Meiyu Wang, Yansheng Shi, "Network Centric Warfare" of American Army in My Eyes', Liberation Army Daily, 11 October 2001.
4. Y. Banggen, On IW, Digital Battlefields (Beijing Zhongguo Junshi Kexue, 20 February 1999), PP. 46-51 as Translated and Downloaded from the FBIS Website on 17 July 1999 – quoted by T. Thomas, Like Adding Wings to the Tiger: Chinese Information War Theory and Practice (Fort Leavenworth: Foreign Military Studies Office). Available from: http://www.jwar.org.uk/jwar/ resources /china/iw/chinaiw.htm.
5. Zhanliang Wang. 'Characteristics of Chinese Information Warfare: The Point of View from Foreign Military Export', 31 December 2001.
6. Yoshinhara, 'Chinese Information Warfare', PP.16-17.
7. People's Daily, 8 April 2002.
8. Liberation Army Daily, 16 February 2000.
9. Kove Ping, 'The New People's War of China-America Network's, *Asia Weekly*, 9 May 2001.
10. Ibid.
11. Voice of Overseas Chinese, 11 February 2001.
12. 26 August 2002.
13. Xuewen Zhou and Xiangcheng Luo, 'The Legislation Analysis of China's Information Security in Internet Environment', Voice of Overseas Chinese, San Francisco: Overseas Chinese Cultural Society, 26 August 2002.

۱۴. در زمان نگارش این سطور، ۵/۹۱ میلیون نفر کاربر اینترنت در چین به‌سر می‌بردند؛ براساس این، چین از این نظر مقام دوم را در جهان به خود اختصاص داده است:

Daily of the World, 17 January 2003.

۱۵. برای اولین بار، یکی از دانشگاه‌های چین در مقطع کارشناسی در رشته ایمنی اطلاعات در پاییز ۲۰۰۱، دانشجو پذیرفت. نگاه کنید به: www.people.com.cn.9May ۲۰۰۱.

۱۶. سه آزمایش علمی بزرگ نیز درمورد چهارمین نسل «قایق الهی» چین انجام گرفتـه اسـت. ایـن گزارش را شبکه خبری چین در ۱۶ژانویه ۲۰۰۳ منتشر کرد.

17. Chinese Academy of Sciences, 'Shanghai Institute of Technical Physics Aims at International Advanced Technology', www.people.com.cn, 23 October 2002.

۱۸. چین به سومین کشور دارندهٔ سیستم جهت‌یابی ماهواره‌ای در جهان مبدل گردیده است.

19. Gregory Kulacki and David Wright, 'A Military Intelligence Failure? The Case of the Parasite Satellite', Union of Concerned Scientists, 16 August 2004. Available at http://www.iucsusa. Org/global_security/china/page.cfm? pageID= 1479.

20. 'The Ultrafast Electric Big Gun of China Will come out', Knowledge of the Naval Vessel, 25 March 2002.

21. 'Chinese Military Will Develop Advanced Domestic "Windows", Science and Technology Daily, 21 January 2003.

22. 'Legend Group of China Introduces the Super Computer', *Central News Agency*, 30 August 2002.

23. 'China First Piece High Performance General CPU-"Dragon Core" Came out', Beijing Evening, 14 October 2002.

24. Zhang Xuguang, 'Seven Major IT Industry Group League to Make "the Dragon Core"-The First IT Industry Chain of China Takes Shape', Beijing Morning, 26 December 2002.

25. 'China Cruises Missile Plan is Exposed', Jean's Defence Weekly', 12 January 2000.

26. 'China Has Set Up Five Major Information Warfares Base', China.com, 26 May 2001.

27. Ibid.

28. 'China is Losing The Power of Network Control', eNet Silicon Valley Power', 3 October 2000.

29. 'China Faces Six Major Respects Situation for Information Safety', CEInet, 9 November 2000.

30. 'Painstakingly Build Up with Limited Ability-can Taiwan Afford to Make Information Warfare? Hua Xia Transit Network, 17 May 2004. Available at http://jczs.sina.com.cn/2004-05-17/1643198436.html.

31. 'Great Era: New American Space Weapon System Has Started in Order to Paralyse Enemy's Communication Satellite', 23 November 2004. Available at http://www.chinaaffairs.org/gb/detail.asp?id=49285.

32. Luming You, 'The Information Warfare Behind the Collision Incidents of China and America Airplane', *China News Service*. 23 August 2001.

33. Kove Ping, 'The "People War" of Network Between China and America', *Asia Weekly*, 9 May 2001.

بخش چهارم

چه اقداماتی در دست انجام است ـ یا چه باید انجام داد؟

فصل دوازدهم پلی بسیار دوردست؟

مایک مور*

در حوالی ظهر روز هفتم آوریل سال ۲۰۰۳، در جنگ دوم خلیج فارس، نیروی‌های آمریکایی تلاش کردند با انجام عملیات بمباران از ارتفاع بالا، صدام حسین، دیکتاتور عراق را بکُشند. یک هواپیمای مافوق صوت بمب‌افکن B-1 که در ارتفاع سی هزار پایی برفراز آسمان پوشیده از ابر بغداد به پرواز درآمده بود، این بمب‌ها را فرو می‌ریخت. گفته می‌شد نیروهای عملیات‌های ویژهٔ مستقر در زمین، صدام حسین و مشاوران ارشد او را شناسایی کرده‌اند؛ همچنین، گفته می‌شد آنها در ضیافت ناهاری در ساختمان بزرگ در یکی از نواحی مسکونی شیک بغداد گردهم آمده‌اند.

گروه عملیات‌های ویژه بلافاصله مختصات دقیق جغرافیایی ساختمان مذکور را از طریق ارتباط مخابراتی ماهواره‌ای برای یکی از مراکز فرماندهی آمریکا فرستاد. این مختصات جغرافیایی به کمک دسته‌ای از ماهواره‌های مجهز به سیستم موقعیت‌یاب جهانی که به فاصله تقریباً ۱۲۵۰۰ مایلی در مدار می‌چرخیدند تعیین می‌شود. مدت زمان ارسال سیگنال‌های زمان‌بندی‌ای که ماهواره‌های مجهز به سیستم موقعیت‌یاب جهانی می‌فرستند، یک میلیونیم یک ثانیه است، که با استفاده از مدل «عصر فضایی» مثلث‌بندی سنتی با دقتی هرچه تمام‌تر موقعیت هدف را تعیین می‌کنند.

یک دسته هواپیمای بمب‌افکن B-1، که تازه سوخت‌گیری خود را در فراز آسمان مناطق غربی عراق از یک هواپیمای سوخت‌رسان به پایان رسانده بودند، هدف اصلی (پناهگاه رهبران رژیم بعث) را ظرف چند دقیقه پس از آنکه در بغداد رؤیت شده بودند، دریافت کردند. حدود ۱۲ دقیقه بعد، این بمب‌افکن‌ها چهار بمب فرورونده انفجاری

---

* Mike Moore

۲۰۰۰ پوندی را در فاصله ۵۰ تا ۱۰۰ پایی دو «نقطه هدف» اصلی خود فروریختند. ابتدا به هریک از «نقاط هدف»، یک بمب اصابت کرد. سه ثانیه بعد از اصابت دو بمب اول، دو بمب دیگر نیز به «نقاط هدف» خوردند. طولی نکشید مقاومت سازمان یافته ارتش عراق بعد از این بمباران از هم پاشید.

ساختمان مذکور به تلی از خاک مبدل شد و تعداد نامعلومی از افراد داخل آن کشته شدند. البته تعدادی غیرنظامی نیز میان این افراد در ساختمان حضور داشتند. صدام حسین در میان کشته‌شدگان بود؟ هیچ‌کس واقعاً نمی‌دانست. تخریب ساختمان به‌قدری کوبنده و کامل بود که هیچ‌کس در آن زمان نمی‌دانست آیا صدام حسین کشته شده است یا خیر یا آیا اصلاً وی در آن روز در آنجا بوده است یا نه؟ جهانیان در سیزدهم دسامبر پاسخ سؤال اول را گرفتند؛ در آن روز، صدام حسین در دخمه‌ای نزدیک تکریت پنهان شده بود شناسایی و دستگیر شد.

بمب‌های فرورونده انفجاری که در این حملات مورد استفاده قرار گرفتند، جزء خانواده بمب‌هایی به نام مهمات حمله مستقیم مشترک[1] (حتی از ارتفاع ۴۰ هزار پایی پرتاب می‌شوند)، بودند. مهمات حمله مستقیم مشترک تقریباًهمیشه در فاصله چند متری «نقاط هدف» خود منجر می‌شوند. البته دقت هدف‌گیری در ارتفاع‌های بالاتر از این نیز رفته‌رفته بهبود می‌یابد. رایانه‌ای که با بمب در حال سقوط در ارتباط است و دستورالعمل به آن می‌دهد به‌طور پیوسته داده‌هایی را از سیستم موقعیت‌یاب جهانی دریافت می‌کند. این ارتباط مستمر باعث می‌شود رایانه بتواند مسیر بمب را تا لحظه برخورد به هدف به‌دقت تنظیم کند. بمب‌هایی که به کمک سیستم موقعیت‌یاب جهانی هدایت می‌شوند ازلحاظ دقت در هدف‌گیری نیز متفاوت‌اند اما دقت این بمب‌ها به حدی است که تفاوت انواع مختلف آنها به‌لحاظ دقت هدف‌گیری، تنها چند متر است. در اوایل جنگ علیه طالبان و نیروهای القاعده در افغانستان، نیروهای زمینی آمریکا اهداف مورد نظر را ۲۵ متر دورتر از آن موقعیت‌هایی که واقع شده بودند، بمباران می‌کردند.

شیوه جدیدی که آمریکا در حوزه نبرد دقیق به‌کار گرفته است تا حد زیادی ـ اما نه کاملاً ـ به «برقراری ارتباط میان سیستم‌های اطلاعاتی مستقر در زمین و تعداد زیادی

---

1. Joint Direct Attack Munitions (JDAM)

تجهیزات و ادوات فضایی ویژه که در مدار زمین می‌چرخند» وابسته است. این تجهیزات و ادوات فضایی ویژه عبارت‌اند از: پرنده‌های جاسوسی، کنترلی و شناسایی؛ ماهواره‌های ارتباطاتی (نظامی و تجاری)، ماهواره‌های اندازه‌گیر[1] و البته، ماهواره‌های مخصوص تعیین زمان و مجهز به سیستم موقعیت‌یاب جهانی.[2]

در ارتش آمریکا، این شیوه نبرد، «نبرد نت‌ــ محور»[3] نامیده می‌شود و در زمان نگارش این سطور، ایالات متحده آمریکا تنها کشوری است که توانمندی مستقرسازی کامل چنین سیستمی را در اختیار دارد.

این تعامل میان سیستم‌های اطلاعاتی مستقر در زمین و تجهیزات و ادوات فضایی این امکان را به آمریکا می‌دهد که نیروی مرگباری را باسرعت و قاطعیتی هرچه تمام‌تر به‌کار گیرد؛ علاوه‌بر این، به نیروهای نظامی آمریکا اجازه می‌دهد به شیوه‌ای انسانی وارد جنگ (با دیگران) شوند ـ البته «اقدام به شیوه‌ای انسانی» را می‌توان برای واژه «نبرد» نیز به‌کار برد. اگر سیستم هدف‌گیری خوب و مطلوب باشد، که همیشه هم این‌گونه نیست، ارتش آمریکا، چه در روی زمین، چه در دریا و چه در هوا، قادر است به اهداف نظامی یا آنکه ازنظر نظامی اهمیت دارند (ولی لزوماً نظامی نیستند) بادقتی بالا حمله کند و به آنها ضربه وارد کند و بر همین اساس، اطمینان حاصل نماید که شمار کشته‌شدگان یا مجروحان غیرنظامی که در جنگ مشارکت ندارند، به حداقل خواهد رسید. به‌عبارت دقیق‌تر، اگر طرف مقابل اهداف نظامی را با اهداف غیرنظامی درهم نیامیزد، همان اقدامی که رژیم صدام حسین انجام داده بود، نیروهای ایالات متحده می‌توانند از کشتن غیرنظامیان درگذرند.

در جنگ جهانی دوم، آمریکایی‌ها و بریتانیایی‌ها برای شکست آلمان نازی و ژاپن، به‌شدت بر دکترین بمباران استراتژیک، دقیق و معطوف به اهداف نظامی تأکید داشتند. متأسفانه، آن دقتی که ما امروز در نظر داریم و می‌فهمیم، با توجه به فناوری‌هایی که در آن زمان در دسترس بود، امکان‌پذیر نبود. در طول نیم قرن گذشته، میلیون‌ها واژه در مورد «چگونگی استحاله دکترین بمباران دقیق (که بریتانیا و آمریکا طراحی کرده بودند) به تجربه‌ای دهشت‌بار برای غیرنظامیان آلمانی و ژاپنی در جنگ جهانی دوم» بر روی

---

1. Meteorologieal Satellites
2. Global Positioning and Timing Satellites
3. Net - centrie Warfare

کاغذ آمده است و البته، بیشتر این واژگان نیز مورد بی‌اعتنایی قرار گرفته‌اند، زیرا اساساً دقت واقعی و همه‌جانبه در آن زمان، غیرممکن بود. تعداد غیرنظامیان آلمانی و ژاپنی را که در اثر عملیات‌های «بمباران دقیق» ازسوی آمریکا و بریتانیا به کام مرگ رفتند نمی‌توان با قطعیت محاسبه و برآورد کرد. پایین‌ترین برآوردهایی که در این زمینه ارائه شده است، از ارقام صدها هزار نفری حکایت دارد؛ اما برآوردهای دیگر، که چه‌بسا برخی از آنها به اغراض سیاسی یا ایدئولوژی آلوده شده و مخدوش هستند، رقم‌های بالای یک میلیون نفر را می‌آورند. این برآوردها شمار کسانی را که در اثر بمباران اتمی شهرهای هیروشیما[1] و ناکازاکی[2] کشته شدند، در محاسبات وارد نکرده‌اند. برای مثال، منبع رسمی پیمایش بمباران استراتژیک ایالات متحده[3] برآورد کرد که حداقل ۳۰۵ هزار غیرنظامی آلمانی کشته و ۷۸۰ نفر دیگر نیز مجروح شده‌اند. (عجیب آنکه هرچند تجربه آلمان آشکارا در اذهان باقی مانده بود، اما جایگاه دکترین بمباران دقیق در دهه‌های ۱۹۴۰ و ۱۹۳۰ در آمریکا و بریتانیا ارتقا یافت).

بعد از جنگ، مارشال سرآرتور هاریس[4] که ریاست فرماندهی بمب‌افکن‌های نیروی هوایی سلطنتی بریتانیا را برعهده داشت، از استراتژی «هدف قرار دادن شهرها با حملات متمرکز بمب‌افکن‌ها» دفاع کرد. وی گفت: «مانند بسیاری از افراد دیگر، هرگز از یاد نمی‌برم که در همه جنگ‌های معمولی گذشته و در همه جنگ‌هایی که در گذشته‌ای نه‌چندان دور رخ داده‌اند، محاصره شهرها رویه‌ای مرسوم بوده است و اگر نیروهای مسلح در هنگام صدور فرمان محاصره شهرها ازسوی فرمانده که با تشریفات خاصی انجام می‌گرفت، از محاصره شهرها خودداری می‌کردند، هر جنبده و موجود زنده‌ای در آن شهرها سرانجام شمشیر به‌دست می‌گرفت و به مبارزه برمی‌خاست ...» (Harris, 1990, P.177).

آن آمریکایی که فرماندهی عملیات اصلی تهاجم هوایی ایالات متحده به خاک ژاپن را برعهده داشت ژنرال کورتیس لمی[5] بود که بعدها رئیس ستاد کل نیروی هوایی ایالات متحده شد. وی گفته‌های سر آرتور در مورد انهدام نظام‌مند شهرهای ژاپن را این‌گونه

---

1. Hiroshima
2. Nagasaki
3. US Strategic Bombing Survey
4. Marshal sir Arthur Harris
5. General Curtis Lemay

بازگو کرد: «این قتل‌عام مردم غیرنظامی، پدیده جدیدی نیست. در دوران باستان، یعنی در روزگاری که ارتش‌ها شهرها را محاصره می‌کردند، همه افراد چه نظامی چه غیرنظامی، در جنگ بودند و زمانی که شهر سقوط می‌کرد و غارت می‌شد، همواره همه افرادی که در شهر حضور داشتند، کشته می‌شدند» (Lemay, 1965, P.384).

اگر کسی بر این باور باشد که شیوه آمریکا درزمینه نبرد دقیق در قرن بیست‌ویکم، که تا حد زیادی مبتنی‌بر استفاده از ماهواره‌های فضایی ایالات متحده است، نابخشودنی و وحشیانه است، اجازه دهید لحظه‌ای و قدری در مورد گفته‌های سرآرتور و کوریس لمن تأمل کنیم. اما با وجود این، شیوه جدید آمریکا در زمینه جنگیدن، نیمه‌پنهان هم دارد. توانایی آمریکا در رفتن به جنگ دقیق در نهایت می‌تواند باعث شود که در مسیر خطرناک نئوامپریالیسم بیافتد، که با بهره‌برداری از توانمندی کنترل فضا و احتمالاً به‌کارگیری تسلیحات در فضا به اوج خود خواهد رسید. نئوامپریالیسم نخستین تجربه‌ای است که آدمی به خود خواهد دید. هیچ کشوری تاکنون در پی آن نبوده است که توانمندی کنترل فضا را به‌دست آورد و هیچ کشوری تاکنون تسلیحات در فضا مستقر نساخته است. البته، یکی از معاهدات بین‌المللی که در سال ۱۹۶۰ پس از مذاکره کشورهای مختلف به تصویب رسید، اعلام کرده است که فضا باید فقط برای مقاصد صلح‌آمیز مورد بهره‌برداری قرار گیرد.

اما این فصل در ابتدا باید یک موضوع را مشخص سازد. درست است که شیوه جدید ایالات متحده برای جنگیدن تا حد زیادی به سخت‌افزارهای مستقر در فضا وابسته است، اما آمریکا در حال حاضر هیچ سلاحی در فضا مستقر نساخته است؛ به‌عبارت بهتر، هیچ ادوات تیراندازی و پرتاب در میدان نبرد فضا نصب نکرده است. درواقع، هیچ کشوری ادوات تیراندازی و پرتاب در فضا ندارد. در مدت چهل سال اخیر، فضای مجاور زمین نظامی شده است و عمدتاً ایالات متحده آمریکا و اتحاد شوروی باعث بروز این وضعیت در فضای مجاور زمین شده‌اند، اما فضا هرگز تاکنون عرصه استقرار جنگ‌افزارها نشده است.

هرچند بخش زیادی از ماهواره‌های نظامی، جاسوسی و حتی تجاری ایالات متحده آمریکا شالوده عملیاتی‌سازی سیستم‌های تسلیحاتی آمریکا روی زمین، در دریا و هوا را تشکیل می‌دهند اما این ماهواره‌ها ذاتاً تسلیحات به‌شمار نمی‌آیند. بااین‌حال باید گفت

چه‌بسا ممکن است این وضعیت تغییر کند. بسیاری از افراد پرنفوذ در وزارت دفاع و اندیشه‌گاه‌های افراطی[1] درصورتی‌که ضروری تشخیص دهند، احتمالاً توسعه توانمندی آمریکا در کنترل و استقرار تسلیحات در فضا را مدنظر قرار خواهند داد.

۱-۱۲ مشارکت جهانی[2]

از زمانی که اولین ماهواره نظامی در مدار زمین قرار گرفت، استفاده ارتش آمریکا از توانمندی‌های فضایی تحول چشمگیری یافته است. پیشرفت‌هایی که به‌طور مستمر در حوزه فناوری فضایی صورت گرفته به توسعه سیستم‌های فضایی پیشرفته‌تری انجامیده است. توانمندی‌های فضایی مخصوصاً زمانی که در عملیات‌های مشترک (با مشارکت هر سه نیروی زمینی، هوایی و دریایی) به‌کار گرفته می‌شوند، عملاً به نیرویی چشمگیر مبدل می‌شوند که عملیات‌ها را تقویت می‌کنند. بخش‌های نظامی، غیرنظامی و تجاری ایالات متحده بیش‌ازپیش به توانمندی‌های فضایی وابسته‌اند و دشمنان نیز چه‌بسا ممکن است این وابستگی را آسیب‌پذیری بالقوه تلقی کنند. ایالات متحده آمریکا باید قادر باشد از ادوات و تجهیزات فضایی خود (و درصورتی‌که عملی منفعت‌زا باشد، از ادوات و تجهیزات متحدانش) حفاظت کند و استفاده دشمنان از تجهیزات و ادوات فضایی جلوگیری به‌عمل آورد (JCS, 2002, P.vii).

واژه کلیدی در نثر پرتکلف بالا که به نقل از رؤسای ستاد مشترک ارتش آمریکا آورده شده است، «جلوگیری به‌عمل آوردن»[3] است. حداقل به مدت یک نسل است که مقامات عالی‌رتبه کاخ سفید و وزارت دفاع و پژوهشگران بسیاری از اندیشه‌گاه‌های افراطی بر این باور بوده‌اند که کشورهای دشمن خواهند کوشید ادوات و تجهیزات فضایی ایالات متحده را مختل کنند یا منهدم سازند و ازاین‌طریق، قدرت نظامی ایالات متحده در حوزه فناوری‌های برتر را تعدیل و متوازن نمایند. این افراد تصریح می‌کنند که منازعات آینده به زمین، هوا و دریا محدود نخواهد بود. فضا نیز لاجرم به «چهارمین محیط نبرد»[4] مبدل خواهد شد. نبردها «در» فضا و «از» فضا اتفاق خواهند افتاد. ایالات

1. Hard-line Think-tanks
2. Global Engagement
3. To Deny
4. Fourth Medium of Warfare

متحده آمریکا به این واقعیت پی‌برده و احساس تکلیف کرده است. آمریکا باید با «اتخاذ» رویکرد پیش‌دستانه همه ابزارهای جلوگیری از استفاده «افراد بد»[1] از فضا را توسعه دهد. ازاین‌رو باید توانمندی کنترل فضا را در اختیار داشته باشد.

در سال ۱۹۹۷، فرماندهی فضایی ایالات متحده که در آن زمان یک سازمان فراگیر و دارای مراکز فرماندهی متعدد در کلرادو اسپرینگز[2] به‌شمار می‌آمد، سندی شانزده صفحه‌ای با عنوان چشم‌انداز سال ۲۰۲۰[3] را منتشر کرد. این سند که بر روی کاغذهای پر زرق‌وبرق، ضخیم و مملو از تصاویر رنگارنگ به چاپ رسید، به‌نظر می‌رسد تا حدی شبیه بروشور و دفترچه راهنما برای جامعه بازنشستگان فلوریداست و آکنده از پاراگراف‌های طویل و مطالب خسته‌کننده‌ای است که مطلوبیت‌های بی‌بدیل توسعه تسلیحات فضایی را تشریح می‌کند.

سند چشم‌انداز به‌جای آنکه زمین مسابقات قهرمانی گلف، زمین‌های تنیس، استخرها و باشگاه‌های ورزشی را تشریح کند، رویاهایی در مورد قدرت فضایی نامحدود را به ذهن خواننده متبادر می‌سازد. ما در اولین صفحه این سند که با فونت درشت و پس‌زمینه مشکی چاپ شده است، می‌خوانیم: «فرماندهی فضایی ایالات متحده ـ سیطره بر بعد فضایی عملیات‌های نظامی برای حراست از منافع و سرمایه‌گذاری‌های ایالات متحده. تزریق نیروهای فضایی به توانمندی‌های جنگی در انواع و اقسام منازعات». به‌نظر می‌رسد که این نوشته رابطه خود را با خواننده قطع کرده است و شباهت بسیاری به ابتدای فیلم سینمایی جنگ‌های ستارگان ساخته جرج لوکاس[4] دارد. این فیلم سینمایی با این جملات آغاز می‌شود: مدت‌ها پیش در کهکشانی در دوردست، بسیار دوردست ... تصویری که در پشت جلد مشکی این سند درج شده است، موضوع جنگ‌های ستارگان را برجسته ساخته است. چشم‌انداز مورد نظر ما فضای مجاور زمین و به عبارتی تا صد مایل بر فراز سطح زمین است.

در پایین صفحه، بخشی از کره زمین به‌صورت یک قاچ، منتزع شده است و

---

1. Bad Guys
2. Colorado Springs
3. Vision for 2020
4. George Lucas

چشم‌اندازی از بیابان به رنگ قهوه‌ای تیره به تصویر کشیده شده است. ما نوک منتهی‌الیه شرق دریای مدیترانه و در زیر آن دریای سرخ را مشاهده می‌کنیم و می‌بینیم که ابرهای تیره تا حدی باعث تیرگی سطح این دریاها شده است. در این تصویر، در بالای دریای مدیترانه، دریای سیاه واقع شده است و در سمت راست دریای سیاه، دریای خزر و در زیر آن خلیج فارس نقش بسته است. بقیه تصویر، فضایی آبی‌رنگ متمایل به مشکی است که لکه‌هایی از نقطه‌های سفیدرنگ که نشانگر ستارگان است، در آن دیده می‌شود و به‌عنوان پیش‌زمینه تصویر درج شده است. آیا انفجار ناشی از اشعهٔ لیزر، انهدام یک موشک در حال اوج‌گیری بر فراز آسمان را نشان می‌دهد؟ شاید. آیا انهدام مخزن مهمات زیرزمینی را در پی داشته است؟ شاید. این سند که به‌نحوی هنرمندانه نگاشته شده است، ابهام‌آلود است. اما نکته آموزنده، این نیست؛ اگر کاخ سفید با طرح فرماندهی فضایی موافقت کند، فرماندهی فضایی به‌معنای سیطره بر فضاست.

سند چشم‌انداز ۲۰۲۰ به نوعی یک پیش‌گزارش محسوب می‌شد. یک سال پس از انتشار این سند، فرماندهی فضایی آمریکا سندی ۹۰ صفحه‌ای با عنوان طرح درازمدت منتشر کرد. انتشار این سند مهم در داخل ایالات متحده چندان مورد توجه قرار نگرفت. بااین‌حال می‌توان حدس زد که این طرح در اکثر پایتخت‌های کشورهای جهان با شور و اشتیاق مطالعه شده است. مقامات دولتی و افسران نظامی در سراسر جهان با علاقه‌ای شدید می‌خواهند بدانند ایالات متحده در آینده با قدرت نظامی خود که از فناوری‌های برتر بهره‌مند است چه خواهد کرد.

فرماندهی فضایی، مانند نیروهای نظامی سایر نقاط جهان، تا مدت‌ها به قالب‌بندی‌های سخت‌گیرانهٔ تحلیل‌های مبتنی‌بر «بدترین وضعیت» خوگرفته بود. همیشه نصف لیوان، خالی بود و شاید ترک برداشته بود. به گفته فرماندهی فضایی، در آینده‌ای نه‌چندان دور، انواع و اقسام دشمنان آمریکا ـ نیروهای نظامی ملی، واحدهای شبه‌نظامی و تروریست‌ها ـ به توانمندی‌های فضایی پیشرفته دست خواهند یافت. دشمنان در آینده نزدیک چه‌بسا از نحوه آرایش همه نیروهای آمریکا به‌خوبی آگاه خواهند شد. این دشمنان می‌توانند فوراً به تجهیزات جهت‌یابی دقیق (از جمله ادوات مکان‌یابی و تعیین زمان)، تصاویر دقیق و پروضوح، داده‌های بسیار دقیق در مورد تغییرات آب‌وهوایی و

سیستم‌های هشدار به‌موقع درزمینه حملات موشکی و ارتباطات قومی دسترسی پیدا کنند و با بهره‌گیری از این توانمندی‌ها نیروهای خود را فرماندهی و کنترل خواهند کرد. نیروهای دشمن همان گستره‌ای را که آمریکا و متحدانش قلمرو اقدام خود قرار داده‌اند، در اختیار خواهند داشت.

این طرح بیان کرد که فناوری‌های موجود در بازار جهانی به بازیگران «بد» کمک خواهد کرد تسلیحات ضدماهواره‌ای را گسترش دهند. دولت‌های ثروتمند برای آنکه بتوانند ادوات و تجهیزات فضایی آمریکا را از کار بیاندازند احتمالاً به تسلیحاتی که از فناوری‌هایی از قبیل فناوری لیزر استفاده می‌کنند روی خواهند آورد. قدرت‌های لیزری چه‌بسا ترجیح خواهند داد روی سیگنال‌ها، پارازیت بیاندازند یا سیستم‌های فرماندهی و کنترل را از کار بیاندازند و با انجام حملات سایبر به سیستم‌های رایانه‌ای آمریکا عملیات‌های جاسوسی این کشور را مختل کنند.

نویسندگان این طرح، گوی بلورین خود را مورد بررسی دقیق قرار دادند و در همه جا نوعی ابهام را مشاهده کردند. آنها مدعی شدند که استفاده نکردن از فضا در منازعات آینده، تحمل‌ناپذیر خواهد بود. توسعه و استقرار توانمندی کنترل فضا در زمان اوج‌گیری تنش‌ها و حتی منازعات مستلزم تلاش پیگیرانه و نظام‌مند و سرمایه‌گذاری سنگین خواهد بود؛ نیل به این هدف نه آسان است و نه ارزان به‌دست می‌آید، اما درهرحال ضرورت دارد. تا سال ۲۰۲۰، ایالات متحده هم در فضا و هم در زمین، مجموعه مستحکم و کاملاً منسجم و یکپارچه‌ای از توانمندی‌ها را در اختیار خواهد داشت و به هدف خود که همانا «سیطره بر فضاست» دست پیدا خواهد کرد و به‌این‌ترتیب، حفاظت و حراست از منافع نظامی و تجاری خود در فضا را تضمین خواهد کرد.

این طرح خاطرنشان ساخت که ایالات متحده آمریکا در برهۀ «درنگ استراتژیک»[1] به‌سر می‌برد. جنگ سرد به تاریخ پیوست. حداقل در بیست سال آینده نیز هیچ رقیب هم‌ترازی فراروی ایالات متحده آمریکا قد علم نخواهد کرد. ازاین‌رو هم‌اکنون فرصتی مغتنم است که آمریکا در پی توانمندی‌ها و مفاهیم نوآورانه در حوزه جنگ و جنگیدن باشد. قدرت فضایی مانند قدرت هوایی، مسیر تکاملی خود را خواهد پیمود و حامی

1. Strategic Pause

رزمندگان در میدان نبرد به‌صورت ابزار اجرای عملیات‌های رزم هوایی در خواهد آمد. سرانجام، وقتی قدرت فضایی رفته‌رفته به مرحله کمال خود برسد، نیروی نظامی را از فضا به زمین خواهد آورد. به‌عبارت‌دیگر، اهداف زمینی را از فضا مورد حمله قرار خواهد داد.

۲-۱۲ پلیس فضا

توجه به قابلیت‌های بالای فضا و استقرار تسلیحات در فضا اصلاً ایده جدیدی به‌شمار نمی‌آید. شماره ۲۲ مارس ۱۹۵۲ *مجله کلیرز*[1] را که آن زمان یکی از نشریات پرخواننده و تأثیرگذار در ایالات متحده آمریکا بود، بررسی کنید. روی جلد این مجله، فضاپیمای بالدار با موتورهای پر سروصدا و مشتعل نقش بسته بود که به یک‌باره از درون ظلمات فضا به فاصله مایل‌ها بر فراز سطح زمین ظاهر می‌شود. سرمقاله این مجله نوشته‌ای به قلم ورنهر فون براون[2] دانشمند نازی است که موشک‌های وی ـ دوی (V_2) ساخت وی، لندن و آنتورپ[3] را در طول جنگ جهانی دوم به وحشت انداخته بود (Ryan, 1952, PP.12-70).

در سال ۱۹۵۲، فون براون به برجسته‌ترین موشک‌ساز آمریکا مبدل شده بود. وی در مجله *کلیزر* پیشنهاد داد آمریکایی‌ها ماهواره‌ای بسازند که به آرامی می‌چرخد و به شکل چرخ است. وی توصیه کرد قطر مدارِ آن به‌گونه‌ای باشد که در ارتفاع ۱۰۷۵ مایلی زمین هر دو ساعت یک بار به دور زمین بچرخد. به نوشته براون، اگر این پیشنهاد را یک سکوی پرش برای برنامه‌های دیگر در نظر بگیریم، سفر به کره ماه تنها یک گام از این برنامه‌ها خواهد بود.

اما ماهواره مذکور کاری بیش از ارتقای علم موشک‌سازی و سفر به فضا را انجام خواهد داد؛ این ماهواره صلح جهانی را تضمین خواهد کرد. آن متخصصان آمریکایی که از تلسکوپ‌های قوی، ظریف و متصل به دوربین‌ها، دستگاه‌های راداری و صفحه‌های نمایشگر بزرگ استفاده می‌کنند، در هر اقیانوس، قاره، کشور و شهری به‌طور مداوم مورد بازرسی قرار خواهند گرفت. عملاً غیرممکن است که کشوری بتواند تمهیداتی را که برای جنگ فراهم می‌کند، به مدت طولانی پنهان سازد.

---

1. Collier's Magazine
2. Wernher Von Braun
3. Antewerp

ایالات متحده آمریکا با بهره‌مندی از این سکوی فضایی به پلیس فضا مبدل خواهد شد که نه به چماق‌های ضدشورش بلکه به بمب‌های اتم مسلح خواهد بود. اگر کشوری صلح جهانی را تهدید کرد، موشک‌های بالدار کوچکی که دارای کلاهک‌های هسته‌ای می‌باشند از این ایستگاه به‌گونه‌ای پرتاب خواهند شد که با سرعت مافوق صوت به اهداف مورد نظر ضربه وارد سازند. این موشک‌های دارای کلاهک هسته‌ای می‌توانند به‌طور هم‌زمان هم موشک و هم هدف را ردگیری کنند و با بهره‌گیری از این توانمندی به‌نحوی دقیق به هر نقطه از زمین هدایت شوند.

چه کشوری به جنگ با آمریکا با دولت یا متحد آمریکا خواهد آمد و در نتیجه، خطر عملیات تلافی‌جویانهٔ گشت فضایی ۲۴ ساعته عموسام[1] را به جان خواهد خرید؟

فقط فون براون این دیدگاه را نداشت. در برخی محافل نظامی، مدت‌ها بود که فضا به‌عنوان عرصه غایی و نهایی نبرد تلقی می‌شد. چند ماه بعد از جنگ جهانی دوم و مدت‌ها قبل از مقاله فون براون، هنری هاپ آرنولد[2] فرمانده پنج‌ستارهٔ نیروی هوایی ارتش آمریکا گفت: «در آینده‌ای نه‌چندان دور آمریکا باید توانمندی پرتاب موشک‌های اتمی از فضاپیمای واقعی در مدار زمین را توسعه دهد» (Emme, 1959, P.310).

هرچند در آن زمان، هدف ایالات متحده آمریکا این بود که هرچه سریع‌تر اتحاد شوروی را با بمب‌افکن‌های دوربرد متعارف محاصره کند، اما ایده نیروی فضایی هیچ‌گاه کاملاً از اذهان پاک نشد. در فوریه ۱۹۵۷ ژنرال برنارد شریور،[3] مدیر برنامه موشکی نیروی هوایی آمریکا علناً تصریح کرد که ایالات متحده باید به تفوق فضایی[4] در حوزه نظامی دست یابد. وی خاطرنشان کرد در دهه‌های آینده، نبردهای مهم، نبردهای هوایی یا نبردهای دریایی نخواهند بود، بلکه نبردهای فضایی اهمیت خواهند یافت (Futrell, 1989, P.549).

به دنبال پرتاب سفینه فضایی اسپوتنیک،[5] تامس.دی.وایت[6] فرمانده ستاد کل

---

۱. نماد آمریکاست ـ م.

2. Henry Hap Arnold
3. General Bernald Schriever
4. space superiority
5. Sputnik
6. Thomas D. White

نیروی هوایی آمریکا «برای متقاعدسازی آیزنهاور به صدور فرمان ورود نیروی هوایی به فضا» به مبارزه‌ای پرشور و پیگیر دست زد. وایت در یک سخنرانی اظهار داشت: «ایالات متحده آمریکا به‌منظور تضمین پیشرفت و برتری ملل آزاد در جهان باید توانمندی کنترل فضا را به‌دست آورد، حفظ کند و تداوم بخشد». وی افزود: «... کنترل فضا ... باید هدف همه آمریکایی‌ها باشد» (AFM, 1959, PP.17-22 به نقل از: Lord, 2003).

آیزنهاور رئیس‌جمهور وقت با این درخواست موافقت نکرد. وی گفت جهان مکانی پر دردسر و خطرناک است؛ و مسابقه تسلیحاتی در فضا آخرین حربه‌ای است که ایالات متحده باید به آن روی آورد (نه اصلی‌ترین حربه). آیزنهاور علناً اعلام کرد فضا باید فقط برای مقاصد صلح‌آمیز مورد بهره‌برداری قرار گیرد، اما وی در محافل خصوصی می‌گفت به‌کارگیری ماهواره‌های جاسوسی، اقدامی عالی و حتی ضروری است. این ماهواره‌ها پنجره‌ای را به روی یک جامعه بسیار بسته به‌شدت نظامی شده خواهند گشود و به‌این‌ترتیب به حفظ صلح کمک خواهند کرد. وجود تردید و نبود قطعیت در مورد نیات طرف مقابل باعث بروز جنگ‌های پیشگیرانه می‌شد. در مقابل، داده‌های دقیق قطعیت را تقویت می‌کند.

آیزنهاور سیاست «فضا برای مقاصد صلح‌آمیز» را اتخاذ کرد، اما امروزه آمریکا این سیاست را چندان رعایت نمی‌کند. وی همچنین سلسله‌ای از رویدادها را به جریان انداخت که به امضای «پیمان فضای ماورای جو در سال ۱۹۶۷»[1] انجامید. این پیمان به‌کارگیری تسلیحات هسته‌ای و سایر تسلیحات کشتارجمعی در فضا را ممنوع ساخت. متأسفانه، این پیمان تسلیحات دقیقی را که در مدار زمین قرار دارند و رزمندگان فضاییِ[2] امروز از آنها سخن به میان می‌آورند، ممنوع نکرد. در دهه‌های ۱۹۶۰ و ۱۹۵۰ حتی تصور تسلیحات دقیق دوربرد وجود نداشت (McDougall, 1985, Chapter 8).

جهان آیزنهاور و ژنرال وایت مدت‌هاست که سپری شده است و دیگر بازنمی‌گردد. چهار دهه پیش، اتحاد جماهیر شوروی و ایالات متحده آمریکا قدرت‌های هسته‌ای محسوب می‌شدند و شوروی‌ها مهارت بسیاری در راهیابی به فضا و بهره‌برداری از آن از خود نشان داده بودند. در آن وضعیت، بروز مسابقه تسلیحاتی هسته‌ای در فضا دیوانگی

---

1. The Outer Space Treaty of 1967
2. Space Warriors

محض بود. اما امروز، جنگ سرد خاطره‌ای است که به‌سرعت در حال فراموش شدن است و ایالات متحده آمریکا تنها ابرقدرت جهان می‌باشد. تاریخ تحولات جهانی نیز نشان می‌دهد که آمریکا ابرقدرتی نسبتاً ملایم[1] است.

با توجه به این شرایط، چرا آمریکا اگر درصدد برآید برای تضمین پیشرفت و برتری ملل آزاد، کنترل فضا را به‌دست بگیرد، به بیراهه رفته است؟

۳-۱۲ معمای امنیت

بیش از یک دهه از پایان جنگ سرد گذشته است، اما جهان همچنان پیش‌بینی‌ناپذیر و خطرناک است. این وضعیت برای آمریکایی‌ها پدیده جدیدی نیست. ایالات متحده آمریکا برای کمک به تضمین امنیت خود به نیروهای نظامی بسیار مجرب و مجهز نیاز دارد. به‌هرحال، ایالات متحده آمریکا همچنان قدرت نظامی مسلط جهان باقی خواهد ماند. به‌نظر بعضی، قدرت آمریکا در دنیای پرآشوب پس از جنگ سرد، غیرقابل انکار و لازم است (Clinton, 1997). اما سیطره نظامی آمریکا چقدر باید باشد؟ تمایل آمریکا به کسب برتری نظامی قاطع در جهان در چه حدی باعث ترس و نفرت سایر کشورها خواهد شد و آنها را به واکنش واخواهد داشت؟ واقع‌گرایان معتقدند معمای امنیت پایانی ندارد؛ در وضعیت معمای امنیت، بازی با حاصل جمع صفر باعث می‌شود سایر دولت‌ها تصور کنند دولتی که بسیار قدرتمند شده امنیت نسبی‌شان را تحلیل برده و بدین‌سان آزادی عمل‌شان را به خطر انداخته است.

هرچند معمای امنیت دگردیسی‌های زیادی را به خود دیده است اما به‌نظر می‌رسد این مفهوم در تجربه عالم واقع ریشه دارد. بیش از دو هزار سال پیش، اسپارت به آتن حمله کرد. حمله اسپارت به آتن حداقل تا حدودی به این علت بود که «امپراتوری آتن به‌قدری قدرتمند شده بود که موازنه قدرت در میان دولت شهرهای یونان را تهدید می‌کرد». جنگ سرد نیز خود یکی از نمونه‌های بارز معمای امنیت بود، جنگ سرد درواقع یک پویش کنش ـ واکنش بود که در آن، شرق و غرب می‌کوشیدند اطمینان حاصل کنند که طرف مقابل «برتری نظامی خطرناکی» به‌دست نخواهد آورد. همان‌گونه

---

1. Benign

که واقع‌گرایان استدلال می‌کردند «هیچ رویارویی نهایی» بین دو طرف رخ نمی‌داد، زیرا قدرت‌های هسته‌ای در موازنه کامل قرار داشتند.

در دنیای پس از جنگ سرد، برتری نامتوازن و یک‌جانبه آمریکا در حوزه «فناوری‌های برتر نظامی» نگرانی‌های فزاینده‌ای در سطح جهان پدید آورده است. برای مثال، فرانسه که متحد آمریکاست، آن را به یک «قدر قدرت» لجام‌گسیخته[1] متهم کرده است و چین نیز تأکید کرده که آمریکا قصد دارد به جایگاه «هژمونی جهانی» دست یابد. بسیاری از این ادعاها و شعارها مورد تردید است؛ اما این میزان از قدرت نظامی آمریکا نیز نگران‌کننده می‌باشد. تیمثی گارتن آش،[2] یکی از دوستداران قدیمی و دیرینه آمریکا و عضو ارشد مؤسسه محافظه‌کار هوور[3] در دانشگاه استنفورد کالیفرنیا، نگرانی خود را در قالب عبارات زیر، این‌گونه بیان کرد:

«حتی اگر یک فرشته هم این همه قدرت در اختیار داشته باشد، خطرناک است. نویسندگان قانون اساسی آمریکا مدبرانه مقرر کردند که هیچ‌یک از قوای مجریه، قضائیه و مقننه، هرچند بی‌خطر باشد، نباید بر سایر قوا مسلط شود؛ تا مبادا حتی به وسوسه بیافتد که بر قوای دیگر استیلا یابد. بنابراین، هریک از قوا حداقل به‌وسیله یکی از دو قوه دیگر کنترل خواهد شد؛ شیوه نظارت و توازن میان قوای سه‌گانه حکومتی در نظام‌های سیاسی داخلی در سیاست جهانی نیز کاربرد دارد» (*New York Times*, 9 April 2002).

تلاش ایالات متحده آمریکا برای کنترل یک‌جانبه بر فضا تمام دنیا و شاید به‌ویژه، خود شهروندان آمریکایی را به دردسر خواهد انداخت. هرگونه تلاش آمریکا برای سیطره بر فضا بی‌تردید به‌صورت یکی از نمونه‌های گستردگی بیش از حد امپریالیسم آمریکا[4] درخواهد آمد و این وضعیت، در نهایت می‌تواند باعث رویدادها و اقداماتی شود که امنیت آمریکا را بیش‌ازپیش به خطر می‌اندازد.

تمایل به بهره‌مندی از آزادی عمل در امور جهانی، آرمانی صرفاً آمریکایی به‌شمار نمی‌آید. این آرمان، هدف جهان‌شمولانه تمامی دولت‌هاست ولو آنکه دولت‌ها به‌ندرت بدان

---

1. Loose-cannon Hyperpower
2. Timothy Garten Ash
3. Hoover Institute
4. Imperial Overstertch

دست یابند. همه دولت‌ها، چه دمکراتیک چه استبدادی و چه تمامیت‌خواه،[1] و نیز صرف‌نظر از اینکه دینی باشند یا سلطنتی، می‌کوشند آزادی عمل خود را در برابر دولت‌های دیگر به حداکثر برسانند. همان‌گونه که ورزشکاران در رختکن یکدیگر را ارزیابی می‌کنند، قدرت‌های منطقه‌ای و جهانی نیز همواره به ارزیابی رقبای خود می‌پردازند. در حال حاضر ایالات متحده آمریکا نیرومندترین ورزشکار در رختکن به‌شمار می‌آید.

منظور آمریکا از سیطره تمام‌عیار و همه‌جانبه[2] بر فضای نبرد[3] که در بیانیه‌های چشم‌انداز وزارت دفاع به‌طور مکرر آمده است، چیست؟ با توجه به اینکه وزارت دفاع ایالات متحده هر نقطه بر روی این کره خاکی را فضای نبرد بالقوه قلمداد می‌کند، این عبارت چه‌بسا ممکن است برای شهروندان سایر کشورهای بزرگ و کوچک جهان نیز وحشت‌برانگیز به‌نظر آید.

رهبران کشورها همواره تهدیدهایی را که رقبای بالقوه یا موجود علیه آنها ایجاد می‌کنند ارزیابی می‌کنند؛ ازاین‌رو، توجه خود را بیشتر به توانمندی‌های (فرضی و ثابت شده)[4] معطوف می‌سازند نه به نیت‌ها. همه تصور می‌کنند که توانمندی‌ها کاملاً قابل اندازه‌گیری‌اند. در مقابل حدس زدن نیت‌های هیئت حاکمه کشور دیگر نوعی هنر گمانه‌زنی است که به‌هرحال، معمولاً نتیجه‌ای در پی ندارد و بیهوده است. نیت‌ها نیز مانند دولت‌ها می‌توانند به‌سرعت تغییر یابند.

بعضی از ما که به ارزشمندی همکاری و تفاهم بین‌المللی باور داریم همیشه واقع‌گرایی مفرط را نکوهش می‌کنیم؛ واقع‌گرایی جو بین‌المللی را مسموم می‌سازد؛ برای درک نارسایی‌های واقع‌گرایی، کافی است به تحلیل آن در مورد تحولات جنگ سرد بنگریم. اگر فقط رهبران ایالات متحده آمریکا و اتحاد شوروی این‌قدر کوته‌بین نبودند، اگر فقط آنها مشترکات جامعه بشری را درک کرده بودند، اگر فقط آنها پی برده بودند که کره زمین تنها زیستگاهی است که ما آدمیان خواهیم داشت ... اصلاً مسابقه تسلیحاتی هسته‌ای روی نمی‌داد و هیچ‌گاه سایه تهدید نبرد نهایی[5] بر سر بشر سنگینی نمی‌کرد.

---

1. Totalitarian
2. Full Spectrum Dominance
3. Battle Space
4. Presumed And Demonstrated
5. Armageddon

متأسفانه، قدیسان و فرشتگان در میان ما کم‌اند یا حداقل کسانی که سلوک قدسیان و فرشتگان را دارند، رئیس‌جمهور، نخست‌وزیر یا حاکم نمی‌شوند. وقتی موضوع امنیت ملی مطرح می‌شود، رهبران کشورهای جهان به یکدیگر بسیار سوءظن دارند. آنها در اجلاس‌های دوجانبه، منطقه‌ای و بین‌المللی به سلامتی یکدیگر نوشیدنی می‌خورند ولی با احتیاط رفتار می‌کنند و به دیده تردید و نگرانی به یکدیگر می‌نگرند. لبخندها و تعارفات نقل محافل دیپلماتیک است، اما شرکت‌کنندگان واقعاً چندان اعتمادی به یکدیگر ندارند. خون‌ها و اشک‌ها تاریخ جهان را نگاشته‌اند و رهبران کشورها این واقعیت را از یاد نمی‌برند.

ارزیابی توانمندی‌های نظامی سایر دولت‌ها یکی از واقعیت‌های بنیادین سیاست جهانی است. هرچند این ارزیابی، فرایندی همواره ذهنی است، اما اقدامی ضروری و حزم‌اندیشانه به‌شمار می‌آید. در این ارزیابی، واقعیت‌ها و رویدادها به دور از هرگونه محدودیتی باهم تلفیق می‌شوند و از ابعاد مختلف و برحسب شرایط متفاوت مورد سنجش قرار می‌گیرند. دو واقعیت در مورد جهان امروز بر همگان مسلم و محرز است. ایالات متحده آمریکا توانمندترین کشور نظامی در طول تاریخ جهان است و مانند همه قدرت‌های بزرگ گذشته، علاقه شدیدی به انجام اقدام یک‌جانبه از خود نشان داده است. با توجه به این واقعیت‌ها، ایالات متحده آمریکا در بسیاری از بخش‌های جهان، قدرتی استکباری و پیش‌بینی‌ناپذیر و تهدیدی بالقوه قلمداد می‌شود.

«چرا آنها از ما نفرت دارند؟» پرسشی متداول در ایالات متحده آمریکاست. آیا ما آدم‌های خوبی نیستیم؟ یافتن پاسخ برای این‌گونه پرسش‌ها دشوار نیست. توانمندی‌های نظامی حیرت‌آور ایالات متحده آمریکا در جنگ اول خلیج فارس، در آسمان‌های کوزوو و صربستان، افغانستان و سرانجام در عراق آشکارا به اثبات رسیده است. همگان ایالات متحده آمریکا را دولتی تلقی می‌کنند که به یمن بهره‌مندی از امکانات تکنولوژیکی می‌تواند دقیقاً هر آنچه دلش بخواهد انجام دهد.

ایالات متحده آمریکا قصد دارد چند هزار تسلیحات هسته‌ای برای انجام عملیات‌های سریع حفظ کند و هزاران سلاح هسته‌ای دیگر را برای اطمینان به‌عنوان ذخیره در زرادخانه‌های خود نگه دارد. این کشور تعداد زیادی تسلیحات متعارف در اختیار دارد که

قادرند با استتار و دقتی بی‌سابقه از ارتفاع بالا به اهداف حمله کنند. آمریکا مجرب‌ترین و مجهزترین نیروهای نظامی جهان را در اختیار دارد؛ علاوه‌بر این، این توان را در خود دارد که تعداد قابل ملاحظه‌ای از نیروهای آماده نبرد را ظرف چند روز یا چند هفته به هر نقطه از کره زمین که بخواهد اعزام کند. دامنه برتری آمریکا بر سایر کشورها درزمینه فناوری‌های برتر در تمام حوزه‌های نظامی، هر روز وسیع‌تر می‌شود و این کشور هم‌اکنون با توجیه «قرار گرفتن در وضعیت اضطراری» از ضرورت تسخیر گستره وسیعی از فضا، کنترل فضا و احتمالاً استقرار تسلیحات در فضا سخن به میان می‌آورد.

این وضعیت، مسائل جدید و عمیقی را درزمینه حاکمیت ملی کشورها ایجاد می‌کند. اگر دولتی تا به این اندازه در سطح جهان قدرتمند شود، این سؤال مطرح می‌شود که سایر دولت‌ها چگونه حاکمیت کامل خود را حفظ می‌کنند؟

۴-۱۲ یک آزمایش ذهنی[1]

ما باید با لفاظی‌های طرف‌داران قدرت فضایی آمریکا با احتیاط برخورد کنیم. بسیاری از طرح‌هایی که آنها مطرح می‌کنند، به‌ویژه زمانی که آنها به بحث‌های مربوط به «به‌کارگیری زور» و «توانمندی حمله به اهداف زمینی از فضا» می‌رسند، به‌قدری پرهزینه، باور نکردنی و به لحاظ فنی ناممکن‌اند که عملاً ارزش و اعتبار خود را از دست می‌دهند. قاعده تجربی حکم می‌کند که: «اگر به کمک سیستمی که بر روی زمین مستقر است می‌توانید مأموریت نظامی مورد نظر را انجام دهید، درنگ کنید» مستقر ساختن سخت‌افزارهای رصدگری، هشدار، ارتباطاتی، اندازه‌گیری،[2] و جهت‌یابی در فضا مزیت‌های آشکاری دارد، اما فضا قلمرویی پردردسر و کنترل آن نیز هزینه‌بردار است و باید مخاطراتی را که در خود دارد در نظر گرفت.

جنگاوران[3] فضایی امروز، در تدوین پیش‌نویس اعلامیه‌های چشم‌انداز و دکترین‌های نظامی، ملاحظات مربوط به هزینه‌ها را در نظر نمی‌گیرند. آنها افرادی کلان‌نگرند. این دیدگاه که ایالات متحده آمریکا حق دارد به‌طور یک‌جانبه کنترل فضا را

---

1. Mind Experiment
2. Meteorological
3. Warriors

به‌دست گیرد، در بعضی از محافل نیروی هوایی، در محافل پشت پرده پنتاگون، در برخی از اندیشه‌گاه‌های[1] خاص و چه‌بسا در اتاق بیضی شکل کاخ سفید[2] مورد پذیرش قرار گرفته است. استدلال طرف‌داران این دیدگاه، این است که «ما آدم‌های خوبی هستیم». چرا همه باید نگران کنترل آمریکا بر فضا باشند؟ یک آزمایش ذهنی می‌تواند به این پرسش پاسخ دهد.

برای لحظه‌ای تصور کنید دولت دیگری اسنادی را تهیه و تدوین کرده بود که نشان می‌داد چرا و چگونه می‌تواند کنترل فضا را به‌طور یک‌جانبه به‌دست گیرد (ستاد مشترک نیروهای مسلح، فرماندهی فضایی نیروهای هوایی و مأمور اجرایی پنتاگون در امور فضا در این اواخر پیش‌نویس‌هایی از چنین اسنادی را تنظیم کرده‌اند). فرض کنید چین یا روسیه اعلام کرده بود که قصد دارد تا قبل از سال ۲۰۲۰، به سیطره همه‌جانبه و فراگیر در حوزه نظامی و از جمله فضا دست یابد. از این هم فراتر، فرض کنید رئیس ستاد کل ارتش روسیه یا رئیس ستاد کل ارتش چین گفته بود که «ارتش ما به‌گونه‌ای سازمان‌دهی شده است که می‌تواند بر همه مراحل و محیط‌های رزم[3] اشراف و سیطره داشته باشد. ما باید اذعان کنیم که راهبرد جنگی‌مان تفوق در همه محیط‌های منازعه و از جمله فضا را دربرمی‌گیرد. بر همین اساس، ما باید به‌گونه‌ای برنامه‌ریزی کنیم و برنامه‌هایمان را به‌گونه‌ای عملیاتی سازیم که بتوانیم تفوق نظامی در فضا را به‌دست آوریم». ریچارد بی. مایر[4] فرمانده فضایی ایالات متحده در اول ژانویه ۲۰۰۰ این دیدگاه را مطرح کرد. وی در دوران ریاست جمهوری جرج دبلیو بوش به ریاست ستاد کل نیروهای مسلح آمریکا منصوب شد.

یا اینکه فرض کنید ایران، سوریه یا کره شمالی به جهانیان گفته بودند که توانمندی اشراف بر «بعد فضایی عملیات‌های نظامی» را به‌دست خواهند آورد. اگر بریتانیا، فرانسه، آلمان یا ژاپن اعلام کرده بود که قصد دارند کنترل فضا را به‌گونه‌ای به دست گیرند که درصورت لزوم از دستیابی و استفاده سایر کشورها از فضا جلوگیری به‌عمل آورند، چه

---

1. Think Tanks
2. Oval Office
3. Combat
4. Richard B. Mayer

اتفاقی می‌افتاد. اگر سوئیس یا سوئد، اتریش یا استرالیا و هند یا اندونزی سند «چشم‌انداز ۲۰۲۰» را همراه با تصاویری رنگارنگ «در مورد نابودی اهداف مستقر در زمین در اثر حملات تسلیحات لیزری مستقر در فضا» تقریر کرده بودند، چه می‌شد؟

کشور مورد نظرتان را انتخاب کنید، دوست یا دشمن، گستاخ یا رام، پادشاهی، دمکراسی، یا دیکتاتوری. حالا تصور کنید کشور مورد نظرتان عملاً منابع فنی، عملی و مالی لازم برای نیل به اهداف خود را «در اختیار دارد». مطمئناً آخرین شرط لازم برای نیل به اهداف، «زمان» است. ایالات متحده آمریکا تنها کشوری است که می‌تواند حتی آرزوی کنترل فضا را در سر بپروراند. ما در اینجا ناباوری‌تان به این مدعا را موقتاً مسکوت می‌گذاریم. یکی از این گزینه‌ها را انتخاب کنید. اگر روسیه یا چین یا هر کشور دیگری اعلام کرد که قصد دارد ظرف ۲۰ سال آینده فضا را در کنترل خود درآورد، واکنش شما چه خواهد بود؟ غافلگیر می‌شوید؟ نگران می‌شوید؟ خشمگین می‌شوید؟ یا به هراس می‌افتید؟

همه این پرسش‌ها را کنار می‌گذاریم. اگر هر کشور دیگری بخواهد توانمندی کنترل فضا و جلوگیری از دسترسی سایر کشورها به فضا را به‌طور یک‌جانبه توسعه دهد، این کشور چه حقی برای روی آوردن به این اقدام دارد؟ اگر بریتانیا، فرانسه یا ژاپن چنین برنامه‌هایی داشتند، آمریکایی‌ها از دولت خود می‌خواستند آن‌چنان فشاری بر کشور مشکل‌آفرین وارد سازد که او را به دست کشیدن از آن اقدام وادارد. اگر هند یا اندونزی شعار کنترل فضا را سر می‌دادند ایالات متحده آمریکا خواستار محکومیت آنها در مجامع بین‌المللی و اعمال تحریم‌های اقتصادی شدید علیه آنها می‌شد.

اما اگر چنین تمهیداتی با شکست مواجه شود، جهان زیر سایه یک مسابقه فضایی جدید قرار می‌گیرد. در این میان، باید خاطرنشان کرد که با این اوصاف، هدف اصلی کشورها سیطره نظامی بر فضای نزدیک جو زمین خواهد بود نه اعزام مردان و زنان به کره ماه. مسابقه فضایی جدید بسیار پرهزینه خواهد بود؛ این مسابقه منابع فکری و سرمایه‌های کمیاب را به درون سیاه‌چاله‌های سوءظن متقابل خواهد کشید؛ و در نتیجه توانایی کشورها برای تأمین نیازهای روزمره انسان را به مخاطره خواهد انداخت؛ و بدتر از این، همکاری ثمربخش درزمینه مسائل حاد جهانی را کمتر فراهم خواهد ساخت.

بااین‌حال، بگذارید این مسابقه شروع شود. ایالات متحده نمی‌تواند به کشور X یا

ملت Y اجازه دهد کنترل فضا را به‌دست گیرند. مردم عاقل و منطقی ساکن بوستون یا شیکاگو یا سیاتل از وجود ماهواره‌های روسی یا چینی که در بالای سر آنها به‌گونه‌ای غیرقابل مشاهده و بدون هیچ صدایی در حال حرکت‌اند، نگران نیستند. دهه‌هاست که وضعیت به همین صورت بوده است. اما لیزرهای مستقر در زمین که می‌تواند ماهواره‌های ایالات متحده آمریکا را از کار بیاندازد، چطور؟ این تجهیزات، غیرقابل تحمل خواهند بود. دراین‌میان، تسلیحات مستقر در فضا یا تسلیحاتی که گلوله‌های آنها خط سیر مستقیمی را به‌سمت هدف طی می‌کنند و می‌توانند ماهواره‌های آمریکایی را از کار بیاندازند، چطور؟ این تسلیحات، غیرقابل قبول‌اند.

چه می‌شد اگر با گذشت چند سال، کشور X یا ملت Y عملاً تسلیحات کارآمدی را در فضا مستقر می‌ساخت؟ اگر تسلیحاتی که از انرژی جنبشی بهره می‌گیرند و می‌توانند کاخ سفید، ساختمان کنگره آمریکا و مجسمه آزادی را تخریب کنند یا فضاپیماهای بمب‌افکن بدون سرنشین که می‌توانند بدون ارائه هشدار بر سر ساختمان پنتاگون فرود آیند، یا لیزرهایی که در مدار زمین قرار دارند و می‌توانند یک نیروی هوایی را در حال انجام عملیات نابود سازند، در فضا استقرار می‌یافتند، چه اتفاقی می‌افتاد؟ این دورنما به‌قدری وحشت‌بار و ترسناک می‌بود که اقدام فوری را ضروری می‌ساخت.

آمریکا ممکن است بهترین نیت‌ها را داشته باشد و شاید هیچ‌گاه قصد نداشته باشد کشوری دیگر را به‌جز در شرایط حاد از دسترسی به فضا محروم سازد؛ اگر جنگی در کار نباشد ممکن است مایل هم نباشد که ماهواره‌های سایر ملل را نابود کند یا تأسیسات سایر کشورها را با تسلیحات انرژی ـ جنبشی مستقر در فضا تخریب کند؛ یا اگر کشوری ابتدا حمله نکند، شاید اصولاً نخواهد با پرتوهای لیزری هواپیماهای کشورهای دیگر را سرنگون سازد.

اما کدام ملت می‌تواند به حسن نیت‌های ملتی دیگر حتی ایالات متحده آمریکا اتکا کند؟

۵-۱۲ دستکش مخملین، مشت آهنین

استراتژی‌پردازان فضایی ایالات متحده استدلال می‌کنند که کنترل فضا چندان شوم‌تر از

سازمان‌دهی نیروی دریایی برای کنترل دریاها یا ایجاد نیروی هوایی برای به کنترل درآوردن فضای جو زمین نیست. این قیاس، اشتباه است. هرچند قدرت هوایی و دریایی آمریکا قاطع و کوبنده است اما نمی‌تواند بلافاصله در هر جایی صف‌آرایی کند و آرایش داده شود. در مقابل، اگر تسلیحات فضایی توسعه یابند، مانند اجل معلق خواهند بود؛ چرا که در هفت روزِ هفته و در ۲۴ ساعت شبانه‌روز چه در زمان جنگ و چه در زمان صلح به‌صورت ماشین‌های جنگی در مدار زمین و بر فراز اهداف خواهند چرخید.

ما به درون آینده‌ای سحرآمیز پا نهاده‌ایم و وارد یک سرزمین عجایب شده‌ایم که واژگان و عبارات در آن معناهایی که استراتژی‌پردازان جنگ فضایی می‌خواهند به‌کار می‌روند. آنها می‌گویند برنامه‌های قدرت فضایی آمریکا نباید هیچ‌کس را نگران کند. نیات آمریکا غیرتجاوزگرانه‌اند و خواهند بود؛ ازاین‌رو قدرت فضایی آمریکا عاملی بازدارنده در برابر بازیگران بد است و هیچ‌کس دیگر را تهدید نمی‌کند.

اورت سی دلمان[1] استاد دانشکده مطالعات قدرت هوایی نیروی هوایی آمریکا[2] که مرکز زایش و نشوونمو دکترین قدرت نیروی هوایی و قدرت فضایی به‌شمار می‌آید، است. وی در مجله *سیاست فضایی* (۲۰۰۱) استدلال می‌کند که ایالات متحده آمریکا باید هرچه سریع‌تر تلاش کند که کنترل نظامی فضای مجاور جو زمین را به‌دست گیرد. آمریکا تنها کشور قابل اعتمادی است که می‌تواند امور فضا را در راستای منافع و مصالح همه ابنای بشر تنظیم کند. کنترل نظامی بر فضای مجاور جو کره زمین درواقع، محاصره پلیسی همه نقاط ورود به فضا و کنترل و نظارت بر همه رفت‌وآمدها میان فضا و کره زمین خواهد بود ... حال، سایر کشورهای جهان می‌توانند کنترل آمریکا بر فضای مجاور جو زمین را موهبتی برای تمام مردم جهان و یک کالای همگانی قلمداد کنند؟(Dolman, 2002, PP. 147-9)

این فرض که سایر ملت‌ها با طرحی کاملاً ناسازگار با علایقشان آرامش و آسایش خواهند داشت عجیب و غریب و باور نکردنی است. چند کشور می‌توانند در تفسیر نیات آمریکا بلندنظری از خود نشان دهند و مثبت‌نگر باشند؟ ایالات متحده آمریکا درخصوص امنیت ملی، این کار را می‌کند؟ کدام‌یک از کشورها حاضر خواهند بود تابع اهداف

---

1. Everett C. Dolman
2. The Air force School of Advanced Airpower Studies

ژئوپلیتیک و هوس‌های متغیر ایالات متحده قرار گیرند؟ طبعاً ملتی که می‌تواند فضا را در زمان بروز منازعه به‌خوبی کنترل کند قادر خواهد بود هر زمانی که بخواهد هر ملتی را از دسترسی به فضا محروم سازد. کنترل آمریکا بر فضا برای استراتژی‌پردازان جنگ فضایی آمریکا قابل فهم و ضروری به‌نظر می‌رسد، اما سایر دولت‌ها کنترل آمریکا بر فضا را نوعی هژمونی دستکش مخملین[1] می‌دانند که می‌تواند به مشت آهنین مبدل شود.

استراتژی امنیت ملی آمریکا که سپتامبر ۲۰۰۲ منتشر شد، هیچ راه‌حل تسلی‌بخشی برای رفع نگرانی‌های موجود ارائه نمی‌دهد. با وجود این، این سند اعلام می‌کند که آمریکا سیاست «پیش‌دستی» را در پیش می‌گیرد. براساس این سیاست، قبل از آنکه آدم‌های بد به ما حمله کنند ما باید به آنها حمله کنیم. این سیاست، سیاستی است که جنگ پیشگیرانه را نیز توجیه می‌کند. طرح سیاست پیش‌دستی، بازی با الفاظ نیست. در حقوق بین‌الملل و در رویه‌های بین‌المللی تفاوتی چشمگیر میان جنگ پیش‌دستانه و جنگ پیشگیرانه وجود دارد. جنگ پیش‌دستانه در بیشتر مواقع موجه و پذیرفتنی است؛ اما جنگ پیشگیرانه شایسته و برازنده ملتی که خود را ملتزم به قانون می‌داند، نیست. اگر کسی می‌خواهد بداند که چگونه کنترل فضا سیاست «سیطره تمام‌عیار» و جنگ پیشگیرانه را تقویت می‌کند، نیازی نیست که جراح مغز و اعصاب یا درواقع امر، دانشمند موشک باشد.

۱۲-۶ پیامدهای ناخواسته

تلاش آمریکا برای کسب کنترل یک‌جانبه و مستقرسازی تسلیحات در فضا عالی‌ترین لحظه‌ای که آمریکا تجربه کند نخواهد بود؛ این تلاش آمریکا طبعاً بر همه افرادی که روی این سیاره زندگی می‌کنند تأثیر خواهد گذاشت. معاهده فضای ماورای جو[2] فضا را حریم عاری از تسلیحات به قلمداد می‌کند و در این راستا استقرار تسلیحات هسته‌ای و سایر تسلیحات کشتارجمعی در فضا را ممنوع کرده است. اما این معاهده نقطه‌ضعفی دارد که استراتژی‌پردازان جنگ فضایی آمریکا امیدوارند از آن بهره‌برداری کنند. در دهه

1. Velvet-glove Hegemony
2. The Outer Space Treaty of 1967

۱۹۶۰ طرف‌های مذاکره‌کننده برای تصویب این معاهده هرگز تصور نمی‌کردند که هر ملتی تمایل خواهد داشت تسلیحات متعارف و به‌عبارت دقیق‌تر، تسلیحاتی که تأثیرگذاری دقیقی برجای نمی‌گذارد در فضا مستقر سازد. فقط و فقط ایالات متحده آمریکاست که از انجام این کار سخن به میان می‌آورد. فقط و فقط اوست که در مورد توسعه و استقرار توانمندی «کنترل فضایی» فراگیر صحبت می‌کند.

کنترل فضا، علی‌الظاهر ایده بدی نیست. اگر قرار است بشریت راه خود را به‌سوی آینده‌ای انسانیتر بپیماید، کنترل فضا ضروری است؛ اما این هدف می‌باید براساس پیمانی بین‌المللی که بندهای اجرایی جدی داشته باشد، تعقیب شود. چنین پیمانی تحقق‌یافتنی و قابل حصول خواهد بود. فعالیت‌های مربوط به ساخت انواع و اقسام سیستم‌های تسلیحاتی به‌ویژه تسلیحات بیولوژیکی را به‌آسانی می‌توان با پنهان‌کاری و در قالب برنامه‌های دیگر انجام داد، اما این موضوع در مورد ساخت تسلیحات ضدماهواره‌ای که به فناوری پیشرفته‌تری نیاز دارد صدق نمی‌کند؛ چرا که مراحل پایانی توسعه این‌گونه تسلیحات می‌باید در محیطی باز یعنی در فضا انجام پذیرد.

با توجه به اینکه تسلیحات ضدماهواره‌ای در معرض دید قرار می‌گیرند، طراحی رویه‌ها و فناوری‌های نظارتی قابل اتکا که هم از رقابت تسلیحاتی در فضا جلوگیری کند و هم مانع مسابقه تسلیحاتی میان کشورها درزمینه تسلیحات ضدماهواره‌ای مستقر در زمین شود، دشوار و ناممکن نخواهد بود. اما تا به حال، ایالات متحده آمریکا هیچ علامتی از خود بروز نداده است که نشان دهد این کشور در آن جهت حرکت خواهد کرد. انعقاد معاهده‌ای برای جلوگیری از بروز مسابقه تسلیحاتی در فضا حداقل تا وقتی‌که آمریکا با آن موافق نیست، امکان‌پذیر نیست. هرساله این موضوع در کنفرانس خلع سلاح در ژنو مطرح می‌شود اما ایالات متحده آمریکا از بررسی بنیادین و انعقاد چنین معاهده‌ای جلوگیری می‌کند.

برای مثال، رابرت تی گری، نماینده وقت آمریکا در کنفرانس ژنو در سپتامبر ۲۰۰۰ این دیدگاه سنتی را ارائه داد: «ایالات متحده می‌پذیرد که بررسی این موضوع در این کنفرانس مناسب و بجاست، اما بسیار خاطرنشان کرده‌ایم که هیچ مسابقه تسلیحاتی در فضای ماورای جو وجود ندارد. علاوه‌بر این، براساس شواهد موجود نیز انتظار نمی‌رود که مسابقه تسلیحاتی در فضای ماورای جو در آینده رخ دهد» (Grey, 2000).

البته حداقل بخش اول اظهارات گری درست بود. در زمانی که وی صحبت می‌کرد هیچ مسابقه تسلیحاتی در فضا وجود نداشت، زیرا تنها یکی از طرف‌های مسابقه (یعنی ایالات متحده) در آن زمان از توانمندی استقرار تسلیحات در فضا برخوردار بود.

اما ارزیابی دلیل تلاش احتمالی آمریکا برای کنترل فضا در قرن بیست‌ویکم آسان نیست. شیفتگان کنترل فضا راست می‌گویند که از منافع حیاتی آمریکا باید قاطعانه دفاع کرد. آنها راست می‌گویند که آمریکا برای پیشبرد برنامه‌های جنگی خود در هنگام نبرد با دشمن و تداوم رونق اقتصادی خود، بیش از هر کشور دیگری به تأسیسات فضایی ـ نظامی و تجاری خود وابسته است. اما این گفته استراتژی‌پردازان جنگ فضایی اشتباه است که آمریکا برای تضمین امنیت خود باید به‌طور یک‌جانبه به کنترل فضا دست یابد. در دنیای مبتنی‌بر اصل حاکمیت ملت‌ها کنترل یک‌جانبه و استقرار انحصاری تسلیحات در فضا مسائل بسیار دردسرسازی را درزمینه حاکمیت ملی کشورها پدید خواهد آورد. به احتمال زیاد، سایر کشورها این اقدام آمریکا را نقض تحمل‌ناپذیر هنجارهای جهانی قلمداد خواهند کرد.

بسیاری از ملت‌ها در حال حاضر از آمریکا می‌ترسند یا نفرت دارند. این وضعیت تا حدودی به‌دلیل سیطره آمریکا در حوزه فناوری است. در حال حاضر به‌نظر نمی‌رسد بیشتر کشورها با این واقعیت کنار بیایند که ایالات متحده آمریکا تا آینده‌ای غیرقابل پیش‌بینی همچنان قدرتمندترین دولتی خواهد بود که جهان تاکنون در عرصه‌های اقتصادی، نظامی و فرهنگی به خود دیده است. آیا یک نقطه‌نظر کارگشا، یا درواقع پلی در دوردست[1] و به‌عبارت بهتر، معیاری وجود دارد که حتی کشوری مثل آمریکا نیز نتواند بدون برانگیختن واکنش‌ها فراسوی آن گام بردارد؟

طرف‌داران قدرت فضایی آمریکا کنترل فضا را «برخورداری از توانمندی تدارک امکان دسترسی آدم‌های خوب به فضا و جلوگیری از دسترسی آدم‌های بد به فضا» تعریف می‌کنند. مدافعان قدرت فضایی آمریکا این توانمندی را به زبان بازدارندگی بیان می‌کنند ـ یعنی، قدرتی نهفته که «تنها» در زمان ضرورت، اعمال خواهد شد. آنها آن پیامدهای سیاسی را که این قدرت به‌طور منطقی با خود به همراه دارد به‌سادگی نادیده

1. A Bridge Too Far

می‌گیرند. ایالات متحده آمریکا می‌تواند قاضی و هیئت منصفه شود و در مورد دسترسی سایر کشورها به فضا حکم صادر کند. چرا هر کشوری، حتی دوستان آمریکا از این وضعیت خرسند خواهند بود؟

اگر ایالات متحده آمریکا تصمیم بگیرد که برنامه کنترل فضا را دنبال کند، پیامدهای آن نیز پیش‌بینی‌ناپذیر خواهد بود. بسیاری از کشورها قاعدتاً آمریکا را همراهی خواهند کرد: این کشورها یا دوستان و متحدان قدیمی آمریکا می‌باشند یا به‌قدری ضعیف‌اند که چاره‌ای جز این ندارند.

تعداد محدودی از کشورها هستند که برای ایجاد موازنه در برابر افزایش قدرت فضایی آمریکا به واکنش‌های نامتقارن روی خواهند آورد. در حال حاضر، شواهد بسیاری وجود دارد که نشان می‌دهد برتری نظامی آمریکا در حوزه فناوری‌های برتر رفته‌رفته الهام‌بخش تدوین چنین استراتژی‌ها و برنامه‌هایی شده است.[1] آن تسلیحات هسته‌ای که از فناوری‌های نازلی بهره می‌برند، احتمالاً در صدر این فهرست قرار می‌گیرند. فناوری‌هایی که در این تسلیحات به‌کار رفته‌اند چه‌بسا ممکن است به‌قدری نازل باشند که برای پرتاب آنها به‌جای موشک از کامیون استفاده شود. تسلیحات بیولوژیکی و رادیولوژیکی ممکن است بلافاصله در اولویت‌های بعدی نباشند. البته، گذشته از این، در حال حاضر انواع و اقسام جنگ سایبر می‌تواند رخ دهد، همان‌گونه که سایر نویسندگان این کتاب خاطر نشان کرده‌اند تروریسم امکانات بی‌پایانی دارد که با استفاده از آنها می‌تواند هیچ ردی از خود برجای نگذارد.

تلاش آمریکا برای کنترل فضا ورود عاملی پیش‌بینی‌ناپذیر و جدید به بازی قدرت جهانی خواهد بود. تأثیر این اقدام بر سایر کشورها پیش‌بینی‌ناپذیر خواهد بود اما قطعاً بعضی از دولت‌هایی که پیش‌تر بی‌طرف بودند و خود را از این بازی کنار کشیده بودند به‌قدری به وحشت خواهند افتاد که اقدام خواهند کرد.

بسیاری از صاحب‌نظران واقع‌بین درزمینهٔ امور نظامی، برنامه‌های کنترل فضا را بسیار غیرمنطقی می‌دانند و معتقدند استقرار احتمالی تسلیحات در فضا غیرضروری، تحریک‌برانگیز و بسیار هزینه‌بر است. یکی از نقدهای کوبنده در مورد کنترل و استقرار

---

۱. برای مثال، در این زمینه می‌توان به انبوه تحلیل‌هایی که سازمان کاهش تهدیدات دفاعی در پایگاه اینترنتی www.dtra.mil ارائه داده است، اشاره کرد.

تسلیحات در فضا در یکی از فصلنامه‌های بسیار معتبر به نام *امنیت بین‌الملل* به چاپ رسید. نویسندگان اصلی این نوشتار نقادانه، ریچارد ال.گاروین[1] (یکی از برجسته‌ترین فیزیک‌دان‌های جهان و مشاور علمی رؤسای جمهور آمریکا از آیزنهاور گرفته تا کارتر) و بروس ام.د بلویس[2] (یکی از افسران بازنشسته نیروی هوایی آمریکا که کتاب *فراسوی راه‌های ورود به آسمان: ظهور اندیشه قدرت فضایی*[3] را گردآوری و تدوین کرد و یکی از کتب درسی مقدماتی درخصوص قدرت فضایی به‌شمار می‌آید و دانشکده مطالعات قدرت هوایی پیشرفته وابسته به نیروی هوایی آمریکا به چاپ رسانده است) بودند.

آنها در مقاله خود با عنوان «تسلیحات فضایی: دل به دریا زدن آمریکا»[4] به تجزیه و تحلیل مشکلات فنی و هزینه‌های سرسام‌آور طرح‌های استراتژی‌پردازان جنگ فضایی پرداختند و روشن ساختند که طرح‌هایی که استراتژی‌پردازان جنگ فضایی تدوین کرده بودند، به‌ندرت منطقی و معقول از کار درمی‌آیند. در همه مواردی که آنها ارائه دادند، سیستم‌های مستقر در زمین بهتر از سیستم‌های مستقر در فضا می‌توانستند مأموریت نظامی را به انجام برسانند و به‌مراتب ارزان‌تر هم بودند. این دو نویسنده در نتیجه‌گیری، اظهار داشتند بهترین شیوه تضمین امنیت فضایی ایالات متحده در درازمدت ترویج غیرتسلیحاتی کردن[5] فضا است: رویکرد تهاجمی (ایالات متحده) در جلوگیری از روی آوردن سایر کشورها به استقرار تسلیحات (در فضا) می‌تواند به‌نحو احسن به اجرا درآید؛ این اقدام آمریکا نشان خواهد داد که ایالات متحده خود را متعهد می‌داند که برای استقرار و آزمایش تسلیحات فضایی یا آزمایش تسلیحات ضدماهواره‌ای ویرانگر پیش‌قدم نمی‌شود. ابتکار عمل آمریکا در تدوین چنین قاعده‌ای پشتیبان اعلامیه یک‌جانبه آمریکا درزمینه پرهیز از استفاده نظامی از فضا خواهد بود؛ در این میان این اعلامیهٔ یک‌جانبه آمریکا ابتدا با اقدامات مشابه سایر کشورها و پس از آن شاید با توسل به تحریم‌ها یا زور علیه اقداماتی که ماهواره‌های هر دولتی را به مخاطره بیاندازند مورد حمایت قرار خواهد گرفت.

---

1. Richard L. Garwin
2. Bruce M. De Blois
3. Beyond the Paths of Heaven: the Emergence of Space Power Thought
4. Space Weapons: Crossing the US Rubicon
5. Non-weaponisation

سال‌هاست که مردان و زنان آگاه و فهمیده‌ای همچون گاروین و دلبلویس (De Blois and Garwin, 2004, P. 84). چنین دیدگاه‌هایی را مطرح کرده‌اند. اما با وجود این، قطار کنترل بر فضا همچنان راه خود را می‌پیماید. استراتژی‌پردازان عالی‌رتبه جنگ فضایی مدام اظهار می‌دارند که ایالات متحده باید پیش‌دستی کند و توانمندی کنترل فضا را توسعه دهد، زیرا اگر آمریکا این اقدام را انجام ندهد، دولت دیگری پیش‌قدم خواهد شد. پیتر بی. تیتس،[1] معاون فرمانده نیروی هوایی آمریکا سال ۲۰۰۳ این دیدگاه را در قالب عبارات ذیل بیان کرد: «و اگر ما به کنترل فضا روی نیاوریم، آنگاه دولت دیگری این کار را انجام خواهد داد. اگر ما در تمام اشکال جنگ و نبرد از بیشترین ظرفیت‌ها و مزیت‌های فضا بهره‌برداری نکنیم، آنگاه دیگران چنین خواهند کرد و ما با قبول خطر، این اجازه را به دیگران خواهیم داد. اگر ما متخصصان فضایی، شکل جدیدی از رزمندگان و جنگاوران را پرورش ندهیم، آنگاه دیگران در این کار پیش‌قدم خواهند شد و البته پیامدهای ناگواری را برای ما خواهد داشت ... موفقیت ما در بهره‌برداری از قدرت هوایی در این واقعیت نهفته است که ما باید قبل و بهتر از هرکس دیگری از این قدرت بهره‌برداری کنیم. اجازه بدهید همین سیاست را در مورد فضا نیز در پیش گیریم».

۷-۱۲ آخرین و بهترین مایه امید[2]

به گفته پروفسور دلمان، کنترل آمریکا بر فضا خوش‌رفتارترین[3] دولتی را که تاکنون هژمونی خود را بر بخش وسیع‌تری از جهان گسترانده است پاسبان فضا قرار خواهد داد. این اقدام، عملی سرنوشت‌ساز و متهورانه و دست‌کم از نقطه‌نظر هژمون به لحاظ اخلاقی عادلانه خواهد بود (Doman, 2002, P.158). عبارت کلیدی در اینجا «از نقطه‌نظر هژمون» است. چرا که احتمال دارد بعضی از دولت‌های دیگر، این اقدام هژمون را بسیار متفاوت از آنچه هژمون می‌انگارد، تلقی کنند.

---

1. Peter B. Teets
2. Last Best Hope
3. Benign

آبراهام لینکلن،[1] در دومین پیام سالیانه خود به کنگره در سال ۱۸۶۲ در بحبوحه جنگ داخلی آمریکا، در مورد معنای آزادی و اهمیت نمادین آمریکا برای جهانیان صحبت کرد. وی گفت بدانید جنگ داخلی تعیین خواهد کرد که آیا مردم آمریکا آخرین و بهترین مایه امیدواری زمین را با ازخودگذشتگی نجات خواهند داد یا با فرومایگی از کف خواهند داد.

باور به‌استثنا بودن[2] آمریکا در میان ملل جهان که لینکلن با ظرافت خاصی بر آن تأکید دارد، هم فضیلت بوده است هم رذیلت. این باور به ایالات متحده آمریکا کمک کرده است به ملتی بزرگ و پویا مبدل شود، اما در طول این سال‌ها مشکلات و دردسرهای عدیده‌ای را به ایالات متحده آمریکا تحمیل کرده است. جنگ ویتنام که طی آن بیش از ۸۵ هزار آمریکایی و بیش از یک میلیون ویتنامی کشته شدند، نشان می‌دهد که آمریکا چقدر می‌تواند در سیاست‌ها و اقدامات خود به‌نحو وحشتناکی به بیراهه رود.

هرچند این ایده آمریکا در تصور همچنان بزرگ باقی مانده است، اما در صحنه عمل همیشه چنین نبوده است. قدرت اقتصادی، سیاسی، فرهنگی و نظامی ایالات متحده بسیار زیاد است. از چنین قدرتی نباید سوءاستفاده کرد. هرگونه تلاش آمریکا برای به‌دست گرفتن کنترل یک‌جانبه بر فضا و ایفای نقش پاسبان فضا بر کل جهان، جلوه غایی و نهایی استکبار نئوامپریالیستی خواهد بود.

سال‌های پیش‌رو بسیار حساس و تعیین‌کننده‌اند. ایالات متحده آمریکا می‌تواند در تدوین پیش‌نویس معاهده‌ای درزمینه جلوگیری از مسابقهٔ تسلیحاتی در فضای ماورای جو با سایر دولت‌ها همکاری کند و به‌این‌ترتیب به بازسازی و بهبود اقتدار اخلاقی خود کمک کند. اما اگر به کنترل یک‌جانبه بر فضا روی آورد و تسلیحات مستقر سازد (تسلیحاتی که نه تنها بالای سر دشمنانش بلکه بالای سر همه ابنای بشر در مدار زمین خواهد چرخید)، آن اقتدار اخلاقی باقی‌مانده خود را نیز از دست خواهد داد.

---

1. Abraham Lincoln
2. Exceptionalism

منابع و مآخذ

AW&ST, *Aviation Week and Space Technology*. Accessed online at www.awstonline.com.Clinton , President W.J., *The Second Inaugural Address of President William J. Clinton*. Available at http: //www.law.ou.edu/hist/ clinton2.html.

Crane, C.C. *Bombs, Cities, and Civilians,* Lawrence, KS: University Press of Kansas, 1993.

DeBliois, B.M. *Beyond the Paths of Heaven*, Mawell Air Force Base, AL: Air University Press, 1999.

DeBlois, B.M.R.L. Garwin, R.S. Kemp and J.C. Mawell, 'Space Weapons: Crossing the US Rubicon', *International Security*, 29(2) 2004, 50-84.

Dolman, E.C. *Astropolitik: Classical Geopolitics in the Space Age,* London: Frank Cass, 2002.

Emme, E.M. *The Impact of Air Power*, Princeton, NJ: D. Van Nostrand, 1959.

Futrell, R.F. *Ideas, Concepts Doctrine: Basic Thinking in the United States Air Force.* 1907-1960, Vol. 1, Maxwell Air Force Base, AL: Air University Press, 1989.

Garrett, S.A. Ethics and Airpower in World War II, New York: St Martin's Press, 1993.

Grey, R.T. U.S. Mission Geneva. Press Releases 2000, (2000). Available at www.us-Mission.ch/Press2000/0915Grey.htm.

Harris, A. *Bomber Offensive,* London: Greenhill Books, 1990. The 1990 Edition is a Facsimile of the Original, Published in 1947, With a new Introduction by RAF Historian Denis Richards.

Irving, D. Apocalypse 1945: the Destruction of Dresden, Cranbrook, WA, Veritas Publishing, 1995.

JCS, Joint Publication 3-14 Joint Doctrine for Space Operations, 9 August 2002. Available at www.dtic.mil/doctrine/ipoperationsseriespubs.htm. For other Documents, Including the National Security Strategy of the United States of America, as well as Joint Vision 2020 (which Explores the role of Information Dominance and Space Assets), go to: www.dtic.mil/jcs.

LeMay, C.E. with Mackinlay Kantor, Mission with LeMay: My Story, Garden City, NY: Doubleday, 1965.

Lord, L. Air Force Command at 21, 19 September 2003. Available at:

http://www.peterson. af. mil/hqafspc/News/News-Asp/nws-tmp.asp?/storyid= 03-180.

Markusen, E. and David Kopf, The Holocaust and Strategic Bombing, Boulder, CO:Westview Press, 1995.

McDougall, W.A. The Heavens and the Earth: A Political History of the Space Age, New York: Basic Books, 1985. The Role of President Eisenhower in Establishing the 'space-for-peaceful-purposes' Policy is Widely Documented. However, McDougall's Book is Perhaps The basic text of the Space Age.

NYT. Available at www.nytimes.com/ 2002/04/09/opinion/09GART.html.

Rumsfeld, D. and et. al., Commission to Assess United States National Security Space Management and Organization, 2001. Paper Copies of the 'Space Commission' Report are Exceedingly Rare, but it is Widely Available Online, for Instance, www.space.gov.

Ryan, C. (ed.), Across the Space Frontierm New York: Viking Press, 1952.

M.Sherry, The Rise of American Air Power: the Creation of Armageddon, New Haven, CT: Yale University Press, 1987. The Previous Five Books Cited Explore the Dark Side of the Anglo-American Strategic Bombing Campaigns in World War II. It is Not Possible to Properly Evaluate America's New Way of Precision War, Based in Large Measure on Information Dominance and Assets in Space, Without a Clear Understanding of that History.

Space Com. Most, if not all, US Space Command Documents are no Longer Easily Accessible online. However, Extensive Commentary on Vision for 2020 as well as the Long-Range Plan Remains. A Particularly Helpful Search Engine is www.SearchMil.com.

Teets, P.B. 'Developing Space Power: Building on the Airpower Legacy', *Air and Space Power Journal,* 17(1), Spring 2003, 11-15.

White, General T.D., Air Force Chief of Staff, Control of Space, 1955. Available at http://www.fas.org/spp/military/docops/usspac/Irp/ch05a.htm.

فصل سیزدهم برآورد تهدید و تمهیدات حفاظتی: گسترش «نتایج چهارمین اجلاس اروپا و آسیا درزمینه مبارزه با تروریسم بین‌المللی و سایر اسناد» به تروریسم سایبر

ماسیمو مائورو*

مقدمه

این فصل به توصیف چارچوب همکاری و گفت‌وگوی اجلاس آسیا و اروپا[1] می‌پردازد، تروریسم سایبر را تعریف می‌کند و تأثیری که این پدیده در حال حاضر برجای گذاشته را تشریح می‌نماید. علاوه‌بر این، برخی از انواع تهدیدهای سایبر، تمهیدات حفاظتی و گزینه‌های سیاستگذاری که برای دستیابی به همکاری درزمینه مبارزه با تروریسم سایبر و سایر تهدیدهای سایبر در منطقه آسیا طراحی شده‌اند، تبیین می‌شوند.

۱-۱۳ چارچوب اجلاس آسیا و اروپا

اجلاس آسیا و اروپا یک فرایند غیررسمی گفت‌وگو و همکاری است که پانزده دولت عضو اتحادیه اروپا و کمیسیون اروپا و نیز ده کشور آسیایی، از جمله ژاپن و ویتنام را گردهم می‌آورد. گفت‌وگوی اجلاس آسیا و اروپا، با هدف تقویت رابطه میان این دو منطقه براساس احترام متقابل و مشارکت برابر، مسائل سیاسی، اقتصادی و فرهنگی را مورد توجه قرار می‌دهد و درصدد حل آنها برمی‌آید.

دومین سمینار اجلاس آسیا و اروپا درباره تجارت الکترونیک که ۲۳ سپتامبر ۲۰۰۲ در هلسینکی فنلاند برگزار شد، به این نتیجه رسید که امنیت سایبر یکی از

---

* Massimo Mauro

1. Asia-Europe Meeting

حوزه‌هایی است که توجه به آن باید در اولویت قرار گیرد. به دنبال دومین اجلاس، طرح ضربتی تسهیل تجارت درباره تجارت الکترونیک فردای آن روز در همان‌جا برگزار شد و پیشنهادهایی به سیاستگذاران توصیه شد.

۱-۱-۱۳ امنیت سایبر

کشورهای شرکت‌کننده در اجلاس آسیا و اروپا به پیروی از اصول کلی، باید بکوشند با بهره‌گیری از تلفیق متناسب فعالیت‌های بخش‌های خصوصی و دولتی، امور ذیل را انجام دهند:

۱. پیروی از بهترین رویه‌های پذیرفته شده بین‌المللی درزمینه امنیت اطلاعات و شبکه‌ها از قبیل رهنمودهای «سازمان همکاری و توسعه اقتصادی» درزمینه تأمین امنیت سیستم‌ها و شبکه‌های اطلاعاتی،

۲. حفاظت مناسب و شایسته از زیرساخت اطلاعاتی حساس،

۳. ایجاد توازن مناسب میان «ضرورت‌های محرمانه بودن فعالیت‌های تجاری و اطلاعات مصرف‌کنندگان» از یک‌سو و «اجرای قانون و اهداف امنیت ملی» ازسوی‌دیگر به‌ویژه با رعایت اصولی که در بهترین رویه‌های بین‌المللی از جمله «رهنمودهای سازمان همکاری و توسعه اقتصادی درزمینه رمزنگاری»[1] و «شورای کنوانسیون جرائم سایبر در اروپا آمده‌اند»،[2]

۴. فراهم کردن امکان دسترسی گسترده به سازوکارهای مناسب تأیید و امضا به‌منظور ترویج تجارت و بازرگانی باز و ایمن، به‌ویژه با رجوع به «کمیسیون سازمان ملل متحد در مورد حقوق تجارت بین‌الملل» که یکی از الگوهای قانونگذاری درزمینه امضاهای الکترونیک به‌شمار می‌آید.

براساس برنامه همکاری درزمینه مبارزه با تروریسم بین‌المللی که در چهارمین اجلاس آسیا و اروپا (۲۲-۴ سپتامبر ۲۰۰۲، کپنهاگ دانمارک) مورد موافقت قرار گرفت، قبل از آنکه پنجمین نشست وزرای خارجه اجلاس آسیا و اروپا در اندونزی

---

1. OECD Cryptography Policy Guidelines
2. Council of Europe Convention on Cybercrime

برگزار شود، سمینار اجلاس آسیا و اروپا در مورد مبارزه با تروریسم سال ۲۰۰۳ برگزار شد. سمینار مذکور با این هدف برگزار شد که چگونگی تقویت نقش پیشتازانه سازمان ملل متحد و همکاری اجلاس آسیا و اروپا با سازمان ملل متحد درزمینه مبارزه با تروریسم مورد بحث و بررسی قرار گیرد. اما تا به حال، اجلاس آسیا و اروپا توجه ویژه‌ای به تروریسم سایبر نداشته است.

۲-۱۳ تروریسم سایبر: اسطوره شهری

درتی دنینگ[1] (۲۰۰۰) تروریسم سایبر را این‌گونه تعریف کرده است: «حمله» یا «تهدید به حمله» به رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آنها که به‌طور غیرقانونی و به‌منظور ارعاب یا اجبار یک دولت یا مردم آن به پیشبرد اهداف اجتماعی و سیاسی انجام می‌گیرد.(۱) تعریفی که پیش‌نویس معاهده استنفورد[2] ارائه داده است اندکی با تعریف بالا تفاوت دارد: تروریسم سایبر به معنای استفاده یا تهدید به استفاده عامدانه از خشونت، اخلالگری و مداخله در سیستم‌های سایبر است که بدون مجوز قانونی صورت می‌گیرد، چه‌بسا به کشته یا زخمی شدن یک یا چند نفر می‌انجامد، خسارت‌های عظیمی بر املاک و ساختمان‌ها به بار می‌آورد، باعث نابسامانی مدنی[3] می‌شود یا زیان اقتصادی جدی وارد می‌سازد.(۲)

هرچند مطبوعات و برخی از سازمان‌های دولتی ادعا کرده‌اند که گروه‌های تروریستی به حملات سایبر دست زده‌اند یا در حال فراهم کردن مقدمات انجام چنین حملاتی هستند، اما هیچ مدرک مستند و قابل قبولی که این ادعاها را به اثبات برساند ارائه نشده است و تنها آنچه وجود دارد داستان‌پردازی‌های بی‌پایه و اساس است. به‌جز ویروس‌ها یا کرم‌ها، به‌نظر می‌رسد که سه گروه، حملات سایبر را طراحی و اجرا می‌کنند:

۱. **بچه‌های شرور و اهل شیطنت**: این افراد نوشتارها و برنامه‌هایی را که دیگران نوشته‌اند، بدون آنکه متوجه شوند، دست‌کاری می‌کنند.(۳)

۲. **تبهکاران مالی**: برخلاف گروه پیشین، این گروه می‌کوشند به‌نحوی خزنده و پنهانی در

---

1. Dorothy Denning
2. Stanford Draft Treaty
3. Civil Disorder

سیستم‌های مالی نفوذ کنند به این امید که به‌سرعت بـه نفـع مـالی برسـند؛ ایـن گـروه می‌کوشند هویت خود را مخفی نگه دارند تا رسوا نشوند. برآورد میزان حملاتی کـه ایـن گروه علیه سیستم‌های مؤسسات مالی انجام می‌دهند، دشـوار اسـت؛ زیـرا سـازمان‌هـای مالی (برای مثال، بانک‌ها) برای حفظ منافع خود، از اعلام مستند وقوع چنـین حملاتـی آشکارا طفره می‌روند. ریشه بیشتر این حملات در درون خود همان سـازمانی اسـت کـه مورد حمله قرار می‌گیرد.

۳. **مخالفان سیاسی**: بسیاری از نمونه‌های حملات سایبر عملاً در زمـان اوج یـک بحـران سیاسی یا منازعه بین‌المللی رخ داده است. مخالفان سیاسـی، وب‌سـایت‌هـای دولـت یـا سازمان هدف را مخدوش می‌سازند یا به‌گونه‌ای در آنها دست‌کاری می‌کنند کـه نتواننـد خدمات ارائه دهند و کاربران نیز از وصل شدن به آنها محروم شوند.

هیچ‌یک از گروه‌های بالا نمونه اعلای آن تعاریف تروریسم سایبر که تا به حال مورد بررسی قرار داده‌ایم نیستند. نتیجه‌ای که به‌طور موقـت از مباحـث ذکـر شـده مـی‌تـوان گرفت این است که در زمان نگارش این سطور، به‌نظر می‌رسد هیچ تهدید قریب‌الوقـوعی را از جانب «تروریسم سایبر» پیش‌رو نخواهیم داشت.

اینترنت پدیده جدیدی است و پدیده‌های جدید چه‌بسا ممکن اسـت هولنـاک‌تـر از آنچه واقعاً هستند به‌نظر برسند. به‌نظر بیایند بسیاری از تحلیل‌هایی کـه ابتـدا در مـورد تهدیدهای سایبر و امنیت سایبر ارائه شده‌اند، بسیار بدبینانه‌اند. اما چنـین تحلیـل‌هـایی چندان معتبر نیستند و به‌نظر می‌آید تسلیحات سایبر نیز ارزش محـدودی در حملـه بـه توانمندی کشورها یا به وحشت انداختن شهروندان دارد. نمونه‌هایی کـه در ایـن نوشـتار ارائه شد نشان می‌دهد کشورها مقاوم‌تر و ترمیم‌پذیرتر از آنچه نظریه‌های اولیه در مـورد تروریسم سایبر می‌انگاشتند می‌باشند. برای فهم آسیب‌پذیری زیرساخت‌های حساس در برابر حملات سایبر، ما می‌باید برآوردی به‌مراتب مفصل‌تر را در مورد «خدمات زائد، نـرخ معمول نقض‌ها و واکنش در برابـر نقـص‌هـا، میـزان دسترسـی شـبکه‌هـای عمـومی بـه کارویژه‌های حساس و سطح کنترل، نظارت و مداخله انـسان در عملیـات‌هـای حـساس» هریک از زیرساخت‌های حساس ارائه دهـیم. ایـن بـرآورد اساسـی نـشان مـی‌دهـد کـه زیرساخت‌ها در کشورهای بزرگ صنعتی در برابر حملات سایبر، مقاومند.[۴]

۱۳-۳ رده‌بندی تهدیدهای سایبر واقعی

اجازه دهید در اینجا رده‌بندی‌ای از تهدیدهای واقعی ارائه دهیم. یکی از رده‌بندی‌هایی که به‌طور آزمایشی از این نوع تهدیدها می‌توان ارائه داد به شرح ذیل است:

۱. تهدیدها علیه زیرساخت اینترنت،

۲. تهدیدها علیه تک‌تک شبکه‌ها یا سرورها،

۳. تهدیدها علیه زیرساخت‌های حساس.

در این میان، می‌توان گفت زیرساخت اینترنت، ترمیم‌پذیر است. حتی حمله‌ای که در اکتبر ۲۰۰۲ علیه سرور کلیدی DNS انجام گرفته بود[۵] و شکل روند نه‌چندان پیشرفته سیستم رد پراکنده خدمات[1] را به خود گرفت، اصلاً مورد توجه کاربران اینترنت نبود. نصب سیستم پروتکل اینترنت مدل ۶، که کمیسیون اروپا آن را تأیید و حمایت می‌کند،[۶] می‌تواند برخی از نواقص امنیتی مدل چهارم پروتکل اینترنت را رفع کند، اما با وجود این، تنها نصب این سیستم در مقیاس وسیع می‌تواند زمینه دستیابی به این منافع و سودها را فراهم نماید. حملاتی که با استفاده از سیستم‌های مسیریاب انجام می‌گیرند، به‌دلیل نارسایی‌هایی که در خود این مسیریاب‌ها نهفته است به‌وقوع می‌پیوندند و فروشندگان سیستم‌ها به‌محض اینکه این نارسایی‌ها را تشخیص دادند می‌توانند آنها را رفع کنند.

تک‌تک شبکه‌ها با توجه به سیستم‌های دفاعی متفاوتی که در خود دارند، به درجات مختلف در برابر این‌گونه حمله‌ها حساس‌اند. حملاتی که پیش‌تر کاربرد عملی به‌نسبت محدودی داشتند، معمولاً ازلحاظ تمهیدات ایمنی و امنیتی، ضعیف‌اند. در این خصوص می‌توان به حملاتی که از طرق ذیل انجام می‌گیرد اشاره کرد: مسموم‌سازی مواد غذایی،[۷] شکلی از حمله بلاگردان معرکه است که تنها می‌توان در سطح زیرمجموعه‌های شبکه اینترنت از آن سود جست و به‌علت رشد بسیار شبکه‌های بی‌سیم و کاربردهای چندگانه جایگاه‌های دسترسی به سیستم‌های بی‌سیم، بسیار مورد اقبال و توجه قرار گرفته است.

این روزها حملاتی که به ناقل‌های خصمانه (کرم‌ها، ویروس‌ها و غیره) متکی‌اند،

---

1. Distributed Denial of Services

یکی از اولویت‌های اصلی تک‌تک مدیران شبکه‌ها (چه خصوصی و چه دولتی) به‌شمار می‌آیند.

«زیرساخت حساس»، مفهومی ذاتاً نسبی و بسته به بافت مکانی و زمانی خود است؛ ازاین‌رو، معنای آن ابهام‌آفرین است. در ایالات متحده آمریکا، دولت کلینتون، زیرساخت‌های حساس را این‌گونه توصیف کرده است: «زیرساخت‌های حساس، آن سیستم‌های فیزیکی و «سایبر ـ محور»اند که یکی از مؤلفه‌های ذاتی و اساسی کمترین حد فعالیت‌های بخش‌های اقتصاد و حکومت‌داری به‌شمار می‌آیند، اما چه در بخش دولتی و چه در بخش خصوصی به حوزه‌های مخابراتی، انرژی، بانکداری و امور مالی، حمل و نقل، سیستم‌های آبرسانی و خدمات اضطراری محدود نمی‌شوند».(۸)

البته، خاطرنشان خواهیم ساخت که واژه «سایبرـ محور»[1] تا حدی ابهام‌آلود است؛ و اصطلاح «کمترین حد فعالیت‌های»[2] نیز چندان مشخص نیست. دولت بوش زیرساخت حساس را این‌گونه تعریف می‌کند: «انقلاب در فناوری اطلاعات، شیوه «معاملات تجاری، عملکرد دولت و پیشبرد دفاع ملی» را دگرگون ساخته است. هم‌اکنون، این سه کارویژه به «شبکه درهم‌تنیده و به هم وابسته‌ای از زیرساخت‌های اطلاعاتی حساس» وابسته‌اند. برنامه حفاظت از این زیرساخت‌ها ـ که به‌موجب این فرمان، مجوز آنها صادر شد ـ باید براساس تلاش‌هایی باشد که به‌طور مستمر برای تأمین امنیت سیستم‌های اطلاعاتی زیرساخت حساس انجام می‌گیرند. در این راستا می‌توان به آمادگی سیستم‌های ارتباطاتی در مواقع اضطراری و نصب تجهیزات فیزیکی که از چنین سیستم‌هایی پشتیبانی می‌کنند، اشاره کرد. حفاظت از این سیستم‌ها یکی از مؤلفه‌های لازم و اساسی در بقای بخش‌های مخابرات، انرژی، خدمات بهداشتی ــ درمانی و خدمات اضطراری به‌شمار می‌آیند».(۹)

این تغییر جهت سیاست‌ها به‌سمت توجه شدید به سیستم‌های دفاعی به دنبال حملات یازده سپتامبر مشهود است؛ اما بااین‌حال، آشکار است که سیستم‌های دفاعی

---

1. Cyber - based.
2. Minimum Operations.

استراتژیک آمریکا به اینترنت متصل نشده‌اند و به فضای اینترنت وارد نگردیده‌اند. دولت آمریکا در عوض از شبکه اختصاصی و انحصاری مقاوم «پالس الکترومغناطیسی»[1] استفاده می‌کند. تسلیحات شبکه مقاوم پالس الکترومغناطیسی یا «مایکروویو پرقدرت»[2] در حال حاضر، واقعیت‌هایی‌اند که مستقل از تسلیحات هسته‌ای عمل می‌کنند.(۱۰)

در اروپا، وضع به‌گونه‌ای دیگر است: سیستم‌های ارتباطاتی و شبکه‌ها به عاملی کلیدی در توسعه اقتصادی و اجتماعی مبدل شده‌اند و اعتبار و قابلیت دسترسی به آنها نقش تعیین‌کننده‌ای در زیرساخت‌های اساسی و بیشتر خدمات عمومی و خصوصی و در کل اقتصاد کشورهای اروپایی ایفا می‌کند. علاوه‌بر این، «امنیت مبادلات و داده‌ها نیز به یکی از مؤلفه‌های اساسی عرضه خدمات و الکترونیک، از جمله تجارت الکترونیک و خدمات عمومی آنلاین مبدل شده است و با این روند، احتمالاً کم‌اعتمادی به اشاعه گستردهٔ چنین خدماتی کاهش خواهد یافت».(۱۱) به‌عبارت‌دیگر، محور تأکیدگذاری در اروپا، حفاظت از خدمات شبکه‌ای و ارتباطاتی و خدمات دولت الکترونیک یا تجارت الکترونیک می‌باشد.

به‌علاوه، چون اینترنت مسیرهای متفاوتی را در روند توسعه تاریخی اروپا و ایالات متحده آمریکا به‌بار آورده است، ازاین‌رو، اولویتی که اروپا و ایالات متحده آمریکا درزمینه حفاظت از زیرساخت اینترنت قائل شده‌اند، متفاوت است. در ایالات متحده آمریکا وجود بنیاد ملی علوم که پیشینه آن به قبل از پیدایش اینترنت بازمی‌گردد، زمینه توسعه پیگیر نظام‌مندانه و منطقی اینترنت و به دنبال آن، انطباق‌پذیری اینترنت با رشد بی‌وقفه تبادل اطلاعات را فراهم ساخت. به‌این‌ترتیب، آمریکایی‌ها وجود یک ستون فقرات اینترنتی مقاوم را حقیقت مسلم و بدیهی می‌دانند.

چنین ستون فقراتی در این روند تکاملی بی‌سالارانهٔ اینترنت هرگز وجود نداشت. در اروپا هر مرکز ارائه‌دهندهٔ خدمات اینترنتی ناگزیر بود شبکهٔ خودش را نصب کند و برای تبادل اطلاعات به انعقاد موافقت‌نامه خیره‌کنندهٔ دوجانبه با سایر ارائه‌دهندگان خدمات اینترنتی متکی باشد. این وضعیت به توسعه یک ساختار چهل‌تکهٔ تبادل پرحجم اطلاعات انجامیده است که نظارت و حفاظت از آنها بسیار دشوار است. نبود یک ساختار

---

1. EMP (Electromagnetic Pulse) Hardened.
2. High Power Microwave (HPM)

منسجم به‌عنوان ستون فقرات شبکه اینترنت و به دنبال آن، وابستگی به تجهیزات آمریکایی برای کشف مسیر تبادل اطلاعات در خارج از کشورهای اروپایی باعث می‌شود که اروپایی‌ها بیشتر به‌ضرورت تأسیس شبکه اینترنت مقاوم‌تر پی ببرند.

اما، از زمانی که «تیم رایانه‌ای واکنش اضطراری»[1] شروع به ثبت وقایع کرد، تا به حال هیچ حمله‌ای به خود زیرساخت اینترنت انجام نگرفته است که بتواند اختلالات چشمگیری در شبکه اینترنتی ایجاد نماید. حملاتی از قبیل «گرم نیمدا»[2] اثرات ناچیزی بر اینترنت گذاشتند، زیرا حجم بالای اسکن کردن گرم نیمدا شرایط «رد خدمات»[3] را بر شبکه‌هایی که با این ویروس مختل شده بودند، تحمیل می‌کرد.

۱۳-۴ روش‌های تدافعی پیشرفته و اولویت‌های منطقه‌ای متفاوت

در ایالات متحده آمریکا توجه بسیاری به مطالعات «بقاپذیری»[4] شده است. یکی از تعریف‌هایی که اخیراً در مورد بقاپذیری ارائه شده است، «توانمندی سیستم در اجرای به‌موقع مأموریت خود درصورت وقوع حمله، نارسایی، اختلال، یا پیشامد» می‌باشد.(۱۲) فنون بقاپذیری معمولاً به روش‌شناسی‌هایی متکی‌اند که در راستای سیاست‌های احداث و توسعه شبکه‌ها قرار می‌گیرند و گستره وسیعی را پوشش می‌دهند. هدف اصلی آنها فراهم آوردن زمینه فعالیت «سیستم‌های عاملی» است که در اثر حملات به‌راحتی متلاشی می‌شوند.

به‌نظر می‌رسد روش‌های ملهم از زیست‌شناسی که برای مقابله با نفوذ یا تکثیر ناقل‌های دشمن به شبکه به‌کار گرفته می‌شوند راه‌های نویدبخشی را در ایالات متحده آمریکا و اروپا گشوده‌اند. مدل‌های کشف ایمنی شناختی نفوذها به شبکه اینترنت (که از تکنیک‌های واکسیناسیون الهام گرفته‌اند) به‌نحو گسترده‌ای مجدداً مورد تحقیق و بررسی قرار گرفته‌اند و به‌نظر می‌رسد که کارآمدتر و مؤثر از تکنیک‌های انعطاف‌ناپذیر متعارف‌اند.(۱۳)

شیوه‌های کاهش پخش سرایت (مشابه روش‌های پیشگیری از سرایت در آلودگی‌های

---

1. Computer Emergency Response Team (CERT)
2. Nimda Worm
3. Denial of Service
4. Revivability

زیستی) نیز طراحی شده‌اند. برای مثال، روش خفه کردن[۱۴] عملاً در کاهش انتشار ویروس‌ها و برخی از انواع کرم‌ها مؤثر افتاده‌اند. برخلاف ویروس‌های چند ـ شکلی،[۱۵] که در این اواخر، کشف آنها سخت‌تر از کشف و شناسایی ویروس‌های دیگر است، تلفیق شیوه آزمایشگاهی و روش اکتشافی، به‌نظر می‌رسد نسبتاً کارآمد و مؤثر باشد.[۱۶]

در ایالات متحده آمریکا روش‌هایی که در هر محیطی برای دفاع از سیستم‌های زیرساخت‌های حساس برابر هر نوع تهدیدی به‌کار برده می‌شوند و درصورت لزوم، اجازه می‌دهند این سیستم‌ها به آرامی و بدون دردسر متلاشی شوند، بیش از سایر روش‌ها مورد تأکید قرار می‌گیرند.[۱۷] اما در اروپا به‌نظر می‌رسد ابتدا بر حفظ همین زیرساخت موجود اینترنت و در وهله بعد بر حفظ کل سرورهای مطمئن و کارآمد شبکه تأکید می‌شود چه [این سرورها] برای تجارت الکترونیک به‌کار روند، چه خدمات دولتی ارائه دهند.

احتمال می‌رود کشورهای آسیایی، که با برخی تنش‌های منطقه‌ای دست به گریبان‌اند و حضور اینترنت در آنها رو به افزایش است، علاقه بیشتری به دفاع از زیرساخت‌های اطلاعاتی و ارتباطاتی از خود نشان دهند.

۱۳-۵ همکاری منطقه‌ای و بین‌المللی درزمینه مبارزه با تروریسم سایبر

در مارس ۲۰۰۴ اتحادیه اروپا نهاد امنیت شبکه‌ای و اطلاعاتی[1] را تأسیس کرد[۱۸] و وظایف ذیل را به این نهاد محول نمود:

۱. گردآوری و تحلیل داده‌ها از جمله اطلاعات در مورد خطرات فعلی و آینده به‌ویژه خطراتی که بر ترمیم‌پذیری شبکه‌های ارتباطاتی حساس و اطلاعات موجود در آنها تأثیر خواهند گذاشت،

۲. ارائه کمک یا نظرات مشورتی به کمیسیون و سایر نهادهای صلاحیت‌دار در چارچوب اهدافی که برای آن مقرر شده است،

۳. تقویت همکاری میان بازیگران مختلفی که در حوزه امنیت شبکه‌ای و اطلاعاتی فعالیت دارند؛ البته، ازاین‌رو نهاد امنیت شبکه‌ای و اطلاعاتی نیز شبکه‌ای متناسب با کارکرد نهادهای ملی و اروپایی راه‌اندازی می‌کند،

---

1. Network and Information Security Agency

۴. کمک به دسترسی همه کاربران بـه اطلاعـات سـریع، عینـی و جـامع درزمینـه موضوعات امنیت شبکه‌ای و اطلاعاتی با ترویج بهترین رویه‌های تبادل داده‌هـا درزمینـه شیوه‌های هشدار به کاربران، از جمله شیوه‌های مربوط به «سیستم‌های هشدار حمله بـه رایانه» و تلاش برای اشاعه تعامل میان ابتکارات بخش‌های دولتی و خصوصی،

۵. کمک به کمیسیون و مراجع قانونگذاری ملی درزمینـه تجزیـه و تحلیـل اجـرای شرایط و ضرورت‌های امنیت شبکه‌ای و اطلاعاتی برای کاربران و ارائه‌دهندگان خـدمات؛ برای مثال شرایط و ضرورت‌هایی که درزمینه حفاظت از داده‌ها وجـود دارد و در قـوانین جامعه اروپا درج شده‌اند،

۶. کمک به ارزیابی استانداردهای امنیت شبکه‌ای و اطلاعاتی،

۷. ترویج فعالیت‌های مربوط به ارزیابی ریسک و تشویق راه‌حل‌های مکمل درزمینـه مدیریت ریسک در درون سازمان‌ها،

۸. کمک به رویکرد اتحادیه اروپا درزمینه همکـاری بـا کـشورهای ثالـث، از جملـه تسهیل تماس‌ها با مجامع بین‌المللی،

۹. انجام هر وظیفه دیگری که کمیسیون در چارچوب اهداف این نهاد به آن محـول کرده است.[۱۹]

برای مثال، بعضی از این وظایف ۲، ۸ و ۹ احتمالاً ارتباط چندانی با مباحث مطـرح در این فصل ندارند؛ اما سایر وظایف را می‌توان به یک سازمان آسیایی مشابه نیز که قرار است تشکیل شود، محول کرد. این وظـایف، درواقـع، اجـرای عملیـاتی مـصوبه دومـین اجلاس آسیا و اروپا با عنوان طرح ضربتی تـسهیل تجـارت خواهـد بـود و مـی‌توانـد بـه افزایش اعتماد میان کشورهای مشارکت‌کننده، البته در راستای نیل به هـدف مـشترکی که دارند، کمک کند.

ازاین‌گذشته، گفتنی است آن چارچوبه حقوقی[1] کـه اسـنادی از قبیـل کنوانـسیون شورای اروپا در مورد جرائم سـایبر مقـرر داشـته اسـت، بـه‌موجـب مـاده پـنجم همـین کنوانسیون، آن‌چنان‌که باید و شاید نمی‌توانـد بـا تروریـسم سـایبر یـا سـایر تهدیـدهای فراروی زیرساخت اطلاعاتی و ارتباطاتی بـه مقابلـه برخیـزد.[۲۰] ازایـن‌رو، بایـد معاهـده

1. Segal Framework

چندجانبه جدیدی (برای مثال، متن پیش‌نویس معاهده استنفورد)[1] به تصویب برسد تا بتواند چارچوبه حقوقی جامعی را درزمینه کمک‌های متقابل در حوزه‌های مرتبط با تهدیدهای سایبر فراهم کند و به مقامات هریک از کشورها تضمین دهد که با استناد به آن قادرند در تعقیب مجرمان سایبر به اقدامات قانونی دست زنند.

۶-۱۳ نتیجه‌گیری

در حال حاضر، تروریسم سایبر، تنها یک چارچوبه تئوریک به‌شمار می‌آید که می‌توان از آن بهره گرفت و اصلاً نیازی هم نیست که با دستپاچگی به تسلیحات تدافعی برای مقابله با آن روی آوریم. روش‌های دفاع در برابر سایر تهدیدهای سایبر را در اختیار داریم. این روش‌ها به‌طور پیوسته رو به توسعه‌اند. البته این امکان وجود دارد که برخی از مدل‌های همکاری بین‌المللی درزمینه مبارزه با تهدیدهای سایبر در هنگام مواجهه با واقعیت‌های متنوع مناطق مختلف جهان تعدیل شوند.

---

1. Stanford Draft Treaty

پی‌نوشت‌ها

1. D. Denning, 23 May 2000. Available at http: //www.terrorism.com/documents/ denning-testimony.shtml.

2. A.D. Sofaer, S.E. Goodman, M.F. Cuéllar, E.A. Drozdova and et. al., 'A Proposal for an International Convention on Cyber Crime and Terrorism', *The Information Warfare Site* 2000, Available at http://www.iwar.org.uk/ law/ resources/ cybercrime/stanford/cisac-draft.htm.

3. The New Hackers Dictionary. Available at http://www.hack.gr/jargon/html /S/script-kiddies.html.

4. J.A. Lewis, 'Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats', *Centre for Strategic and International Studies,* December 2002. Available at http://www.csis.org/tech/0211-lewis.pdf.

5. R. Naraine, 'Massive DDos Attack Hit DNS Root Servers', *Enterprise.* 23 October 2002. Available at http://www.internetnews.com/ent-news/article.php/ 1486981.

6. European Commission, *European Commission IPV6 Task Force,* Available at http://www.ecipv6tf.org/in/i-index.php.

7. B. Fleck and J.Dimov, *Wireless Access Points and ARP Poisoning: Wireless Vulnerabilities that Expose the Wired Network,* 2001. Available at http://www.cigitallabs.com/resources/papers/download/arppoison.pdf.

8. US Department of Homeland Security, 'White Paper. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63', *Information Analysis and Infrastructure Protection,* May 1998. Available at http://www.ciao.gov/publicaffairs/pdd63.html.

9. The White House, Presidential Executive Order on Critical Infrastructure Protection, 16 October 2001. Available at http://www.whitehouse.gov/news/ releases/2001/10/20011016-12.html.

10. R.A. Kehs, 'The Radio Frequency Weapons Threat and Prolifera of Radio Frequency Weapons', *Statement Before the US Congress Joint Economic Committee,* 25 February 1998. Available at http://www.house.gov/jec/ hearings /02-25-8h.htm.

11. The Council of The European Union, 'Council Resolution of 28 January 2002', *Official Journal of the European Communities,* 28 January 2002. Available at http://europa.eu.int/eur-lex.pri/en/oj/dat/2002/c_043/c-432002026en 00020004.pdf.

12. N.R. Mead, R.J. Ellison, R.C. Linger, T. Longstaff and J. MCHugh, 'Survivable Network Analysis Method', *Carnegie Mellon Software Engineering Institute,* September 2000. Available at http://www.sei. cmu.edu/publications/ documents/00t.reports/00tr013/00r013chap02.html.

13. See, for Example, Anchor and et. al., The University of Wales, (2002). Available at http://www.aber.ac.uk/~icawww/Proceeding/paper-32/Anchor-ICARIS-2002. pdf.

14. M.M. Williamson, *Throttling Viruses: Restricting Propagation to Defeat Malicious Mobile Code,* 17 June 2002. Available at http://www.hpl.hp. com/techreports/2002/ HPL-2002-172.pdf.

15. M. Landesman, *Antivirus Software*. Available at http://antivirus.about. com/library/ glossary/ bldef-poly.htm.

16. Symantec, "Understanding and Managing Polymorphic Viruses", The Symantec Enterprise, Vol. XXX (1996).

17. The White House, "Information Analysis and Infrastructure Protection Centre, Department of Homeland Security, June 2002, http://www.whitehouse.gov/ dept of homeland/sec6.html.

18. The European Network and Information Security Agency website, http://www. episa.eu.int.

19. The European Commission "Proposal for a Regulation of the European Parliament and of the Council, at http://europa.eu.int/information-society/ eeurope/news/library/documents/nisa-en-pdf.

20. Council of European Convention, Convention on Cybercrime, 29 Novomber 2001, http://connevantions.coe.int/treaty/en/Treaties/html/185.htm.

فصل چهاردهم تطهیر سیاست و سایر پویش‌های سیاستگذاری

گاس حسین*

مقدمه

قوانین و سیاست‌ها معمولاً اموری ملی قلمداد می‌شوند، چرا که در گفتمان‌های سیاستگذاری ملی جای می‌گیرند؛ اما این فصل استدلال می‌کند که ما باید پویش‌های سیر تطور سیاستگذاری مدرن را در پرتو فعالیت‌های بین‌المللی مطالعه کنیم. من معتقدم در این راستا ما باید به سه بعد مجزای فرایند سیاستگذاری توجه کنیم: تطهیر سیاست،[1] مدل‌سازی،[2] و تغییر محل ابراز مواضع در سازمان‌های بین‌المللی.[3] تطهیر سیاست رویه‌ای است که در آن، سیاستگذاران از سایر حوزه‌های صلاحیت برای پیشبرد اهداف‌شان استفاده می‌کنند و با این اقدام، فرایندهای مشورتی ملی را دور می‌زنند؛ مدل‌سازی در زمانی اتفاق می‌افتد که دولت‌ها، چه به‌صورت آشکار با فراخوان‌های همگون‌سازی و چه به‌صورت ناآشکار با اعمال نفوذ بی‌سروصدا و مخفیانه و بیان مفاهیم به شیوه‌ای جدید، قوانین‌شان را براساس قوانینی که در سایر «حوزه‌های صلاحیت»[4] مطرح می‌شوند، شکل دهند. تغییر محل ابراز مواضع در زمانی اتفاق می‌افتد که بازیگران، قواعد مورد نظر خود را در آن سازمان‌های بین‌الدولی که اهداف و منافع‌شان را تأمین می‌کند دنبال کنند و هنگامی‌که با مخالفت‌ها و چالش‌هایی مواجه شدند، قواعد مورد نظر خود را در سایر سازمان‌های غیردولتی یا ساختارهای موافقت‌نامه‌ای پی‌گیرند. این فصل این پویش‌ها را بررسی خواهد کرد و ابتکار عمل‌هایی را در مورد جرائم سایبر

---

* Gus Hosein

1. Policy Laundering
2. Modelling
3. Forum Shifting
4. Jurisdictions

ارائه خواهد داد و در این میان، از تجربیات گروه هشت کشور بزرگ صنعتی (گروه هشت) و شورای اروپا بهره خواهد گرفت.

ما می‌توانیم تطهیر سیاست را بسط طبیعی قدرت دولت‌ها قلمداد کنیم. در دهه ۱۹۸۰، به‌ویژه در دهه ۱۹۹۰، ما شاهد افزایش چشمگیر شمار سازمان‌های بین‌الدولی و تعداد معاهدات بودیم. به ادعای دولت‌ها، این وضعیت، محصول عصر جهانی شدن و وابستگی متقابل جهانی است. در حال حاضر، پیشبرد احکام بین‌المللی با شکلی از اجماع جهانی، وضعیتی اجتناب‌ناپذیر است. هنجارها و سیاست‌ها در نهادهای بین‌المللی با این هدف دنبال می‌شوند که معاهدات بین‌المللی را پی‌ریزی کنند و هنجارهای جهانی را دگرگون سازند. این دیدگاه، برداشتی خوش‌بینانه در مورد قدرت و روابط بین‌الملل ارائه می‌دهد. اما در این میان، دیدگاه بدبینانه‌ای نیز وجود دارد: براساس این دیدگاه، با افزایش شمار سازمان‌های بین‌الدولی، دولت‌ها لاجرم از این نهادها به نفع خود بهره‌برداری خواهند کرد ـ درست همان‌گونه در گذشته نیز از همه نهادهای دیگر بهره‌برداری کرده‌اند. بر همین اساس، هنجارهای جهانی و معاهدات بین‌المللی منافع دولت‌هایی را که بیشترین سلطه و نفوذ را دارند، یا حداقل، منافع کشورهایی را که از این هنجارها و معاهدات پیروی می‌کنند، نمایندگی می‌کنند. درهرحال، صرف‌نظر از اینکه چه دیدگاهی درخصوص قدرت و منافع ملایم داشته باشید، این نهادهای بین‌المللی به‌عنوان محفل سیاستگذاری مورد بهره‌برداری قرار می‌گیرند و پویش‌های مطرح در این نهادها نیز شایان توجه و بررسی‌اند.

این پویش‌های جدید در عرصه سیاستگذاری، دو پیامد مستقیم برجای می‌گذارد: نخست اینکه، فرایندهای مشورتی ملی نابود یا تضعیف می‌شود، چرا که تصمیم‌گیری‌های مهم در عرصه سیاستگذاری‌ها خارج از نهادهای دمکراتیک سنتی انجام می‌گیرد. از یک‌سو، «درخواست‌های مکرر برای همگونی‌سازی از راه تصویب معاهده» و «تعهدات بین‌المللی» امکان‌پذیری و کارآمدی رایزنی سنتی در سطح ملی را منتفی می‌سازد و ازسوی‌دیگر، مذاکرات در مورد این معاهدات در پشت درهای بسته انجام می‌پذیرد.

پیامد دوم این است که منافع خارجی و فرایندهای خارجی به سیاست‌ها شکل

می‌دهد. برای مثال، رویه‌های محرمانه و مخفیانه اتحادیه اروپا به‌دلیل نفوذ قوانین جدید آمریکا در مورد اسناد و تشریفات مسافرت مورد بازنگری قرار گرفته‌اند. در حال حاضر، اروپایی‌ها مذاکرات جدیدی را در مورد قواعد جریان اطلاعات در فراسوی مرزها و جمع‌آوری اثر انگشت انجام داده‌اند. این قواعد به کمک موافقت‌نامه‌ای بین‌المللی که مبتنی‌بر قوانین قابل اعمال در یک حوزه صلاحیت دیگر می‌باشد پی‌ریزی شده است.

البته من در زمره کسانی نیستم که اعتقاد دارند این وضعیت برایند گریزناپذیر جهانی شدن و موازنه قدرت و منافع است. بعضی استدلال می‌کنند که دولت‌ــ ملت‌ها قدرت و اختیارات خود را از دست می‌دهند. آنها وابستگی متقابل و مذاکره بین‌المللی از طریق سازمان‌های بین‌المللی را تصوری آرمانی می‌دانند. اما دیدگاهی که من به آن اعتقاد دارم هم محتاطانه‌تر با این وضعیت برخورد می‌کند و هم دغدغه بیشتری در مورد آن از خود نشان می‌دهد. برخی از منافع دولت‌ها تأمین شده است، اما درعین‌حال، جایگاه تصمیم‌گیری‌ها و رایزنی‌ها نیز تغییر یافته است؛ دولت‌ها قدرت خود را از دست نمی‌دهند. همگون‌سازی و استاندارد کردن سیاست‌ها که در این فصل مطرح می‌شود پیشنهادهایی‌اند که با هدف افزایش قدرت نهادهای مجری قانون ارائه می‌شوند. استقلال دولت در معرض تهدید قرار ندارد؛ این ظرفیت گفتمان دمکراتیک است که تحت شعاع قرار می‌گیرد.

دولت‌های ملی معمولاً حق دارند قوانینی را در درون حوزه صلاحیت خود وضع و اجرا کنند. بااین‌همه، حق حاکمیت آنهاست که این اجازه را به آنها می‌دهد. البته در برخی شرایط این حق حاکمیت زیر سؤال می‌رود یا تعارضات پدیدار می‌شود. تعارض در زمانی روی می‌دهد که «فعالیت فرامرزی» وجود داشته باشد؛ این نوع فعالیت در خارج از آن حوزه صلاحیتی است که بر «توانایی اعمال صلاحیت اجرای قوانین براساس حاکمیت» تأثیر می‌گذارد. این وضعیت، قابلیت اجرای قوانین مربوط به حل همین مسئله را با تردید مواجه می‌سازد. موضوع «قابلیت اجرا» بلافاصله مسئله‌ساز می‌شود؛ فعالیت ممکن است در خارج از حوزه صلاحیت قوانین ملی روی دهد و در این صورت، تنظیم مقررات درزمینه فعالیت‌های ملی نیز اقدامی عبث و ازلحاظ اقتصادی پرمخاطره است (Sun and Palkmans, 1998).

هرچند داده‌ها در درون شبکه‌های دیجیتالی فراملی جریان می‌یابند و محصولات و خدمات دیجیتالی نیز به این صورت عرضه می‌شوند، اما باید پذیرفت که در مورد معضلات فرامرزی مبالغه شده است. یک اقدام ممکن است در فاصله‌ای دوردست انجام گیرد، برای مثال، حجم زیادی از فعالیت‌ها می‌توانند در جایی رخ دهند که حتی فرد نیز ناگزیر نباشد به‌صورت فیزیکی وارد محدوده صلاحیت دیگری شود. نفوذ رایانه‌ها یا دانلود شدن تصاویر مستهجن می‌توانند در خارج از مرزهای سرزمینی انجام گیرد و در این وضعیت، مانع از آن شود که سازمان‌های مجری قانون (که به‌طور سنتی، حوزه‌های صلاحیتشان مبتنی‌بر مرزهای سرزمینی است) به این فعالیت‌ها رسیدگی کنند و به تحقیقات و جمع‌آوری اسناد بپردازند.

پی‌ریزی سیاست‌های ملی در بحبوحهٔ شبکه‌ها و روندهای اطلاعاتی در فراسوی مرزهای ملی، موضوعی حیاتی در عرصهٔ سیاستگذاری‌های مربوط به فناوری به‌شمار می‌آید. این وضعیت، پدیده جدیدی نیست و آن‌قدری که در بیشتر مواقع پیش‌فرض قرار می‌گیرد یا ازمنظر حقوقی استدلال می‌شود، عملی و امکان‌پذیر نیست (Johnson and Post, 1996). نظریه و عمل حقوقی در برابر این پیش‌فرض‌ها و استدلالات واکنش نشان داده است. ازلحاظ نظری، در حال حاضر چنین استدلال می‌شود که استدلال‌های مبتنی‌بر «عدم امکان‌پذیری» در مورد معضلات و وعده‌های جریان‌های داده‌ها اغراق کردند (Goldsmith, 1998, P. 1130). در این میان، این استدلال‌ها نتوانستند تشخیص دهند که بسیاری از مسائل و معضلات مربوط به تعدد حوزه‌های صلاحیت در تنظیم قوانین، مبادلات فراملی در سایر قلمروهای قانون را نیز دربرمی‌گیرند (Ibid., P. 1200-01).

اما مدت‌هاست که این بحث و مجادله از محافل دانشگاهی نیز فراتر رفته است. همواره درخواست‌های زیادی برای یافتن راه‌حل‌هایی جهت مقابله با چالش‌های روند داده‌ها در فراسوی مرزها، فعالیت تبهکاری در فراسوی مرزها و فعالیتِ تروریستیِ فرامرزی مطرح می‌شود. راه‌حل‌هایی که ترجیح داده می‌شود، با قوانین ظاهراً ملی که در پاسخ به سیاست‌های ملی در حوزه اطلاعات (برای مثال، حفاظت از داده‌ها و حراست از ویژگی محرمانه بودن داده‌ها و تجارت الکترونیک)، سیاست‌های مقابله با جرائم (برای مثال، اختیارات و ظرفیت‌های تحقیق و تفحص) و سیاست‌های مبارزه با تروریسم (برای

مثال، تشریفات قانونی درزمینه مهاجرت و کنترل و نظارت همه‌جانبه) طرح‌ریزی شده و فرق دارند. روابط میان راه‌حل‌های ملی و بین‌المللی لزوماً آشکار و قطعی نیست. بخش بعدی برخی از این راه‌حل‌ها را بررسی می‌کند.

۱-۱۴ در سطح بین‌المللی: شورای اروپا و گروه هشت

به‌نظر می‌رسد فعالیت سازمان‌های بین‌الدولی در بسیاری موارد، راهنمای تدوین سیاست‌ها در عصر جهانی شدن است. اگر چالش‌های فراروی ما در عرصه سیاستگذاری‌ها، ماهیت بین‌المللی داشته باشند و زیرساخت تجارت و ارتباطات نیز جهان‌گستر باشند، آنگاه این منطق صحت دارد و ما به راه‌حل‌هایی نیاز داریم که جهان‌شمول باشند و از طریق مجامع بین‌المللی ارائه شوند. این مجامع بین‌المللی سخت به دنبال آن‌اند که فعال و مطرح باشند. در چند سال پیش، دو نهاد بین‌المللی موافقت‌نامه‌هایی را درزمینه همکاری بین‌المللی در حوزه‌های فناوری‌های برتر و جرائم سایبر تنظیم کردند. از سال ۱۹۹۵ تاکنون، گروه هشت کشور صنعتی (گروه هشت) به‌طور منظم اجلاس‌های رسمی را برگزار کرده و به بحث و تبادل نظر در مورد هماهنگ‌سازی شیوه‌ها، ایجاد ابزارهای نوین همکاری و تعیین اختیارات جدید در عرصه تحقیق و رسیدگی به این‌گونه جرائم پرداخته است. به همین ترتیب، شورای اروپا نیز، که نهاد بین‌المللی تنظیم‌کننده معاهدات به‌شمار می‌آید، ۳۴ دولت اروپایی عضو دارد و از سال ۱۹۹۷ تاکنون کوشیده است کنوانسیون جرائم سایبر[1] را تدوین کند.

خدمات شورای اروپا درزمینه جرائم سایبر و گروه هشت و جرائم مرتبط با فناوری‌های برتر، تحلیل عمیق‌تری را می‌طلبد که در آثار و نوشته‌های دیگر به آن پرداخته شده است. در اینجا به بررسی مختصر عملکرد این دو نهاد بسنده می‌کنیم. کنوانسیون شورای اروپا در مورد جرائم سایبر شامل سه بخش است:

۱. مجموعه‌ای از جرائم جوهری[2] که به‌طور عام در قانون ذکر شده‌اند؛ جرائمی از جمله هک کردن، هرزه‌نگاری از اطفال و نقض حقوق انحصاری مؤلفین و مصنفین (کپی رایت) در این بخش جای می‌گیرد،

---

1. Convention on Cybercrime
2. Substantive

۲. مجموعه‌ای از قابلیت‌های کنترل و نظارت که از کشورهای تصویب‌کننده انتظار می‌رود مجال استفاده مقامات و مراجع مجری قانون از این قابلیت‌ها را فراهم سازد،

۳. تدوین یک رژیم حقوقی درزمینه کمک حقوقی متقابل استرداد مجرمان میان کشورهای تصویب‌کننده.

هشداردهنده‌ترین بخش کنوانسیون شورای اروپا بخش سوم آن است که بر انعقاد موافقت‌نامه‌ای گسترده درزمینه کمک حقوقی متقابل میان کشورهای تصویب‌کننده کنوانسیون تأکید دارد. همکاری بسیار مشکل‌آفرین است؛ زیرا این کنوانسیون سعی دارد دغدغه‌های سنتی درباره جرائمی که ماهیتی دوگانه دارند،[1] نادیده بگیرد؛ درحقیقت، این کنوانسیون کشورها را از خودداری کمک به کشور دیگر در وضعیت‌های دوگانه منصرف می‌سازد و در گاهی اوقات بازمی‌دارد؛ علاوه‌بر این، کنوانسیون چه‌بسا شرایطی را به‌وجود خواهد آورد که یک کشور ناگزیر خواهد بود بی‌آنکه حقوق داخلی خودش را نقض کند به جمع‌آوری اسناد و مدارک در مورد یک فرد بپردازد.

گروهی از نمایندگان وزارتخانه‌های کشور و دادگستری کشورهایی از قبیل کانادا، فرانسه، آلمان، انگلستان و ایالات متحده آمریکا پیش‌نویس این کنوانسیون را تنظیم کردند. گفتنی است که دو کشور از میان این کشورها (یعنی کانادا و آمریکا) فقط اعضای ناظر شورای اروپا می‌باشند. درهرحال، این کنوانسیون فرایندهای تدوین و رایزنی را طی کرده است و منافع و علایق سازمان‌های مجری قانون را نمایندگی می‌کند، اما با وجود این، موضوع حراست از حریم خصوصی و آزادی‌های مدنی را تقریباً نادیده می‌گیرد.

پیش‌نویس معاهده به شکلی نسبتاً محرمانه در سال‌های ۱۹۹۷ تا ۲۰۰۰ تدوین شد، اما فرایند رایزنی در آوریل ۲۰۰۰ آغاز شد. بااین‌حال، با وجود فعالیت‌ها و تلاش‌های نمایندگان جامعه مدنی و بخش خصوصی، تغییرات اندکی در مرحله رایزنی انجام گرفت. هم سازمان‌های بخش خصوصی و هم سازمان‌های جامعه مدنی به دلایل متعددی از جمله فرایند تدوین، تعدی به سایر حیطه‌ها،[2] تحمیل هزینه‌ها و فشارها، نبود تمهیدات مناسب فرایند تدوین و رایزنی و وجود زبان ابهام‌آلود در بدنه اصلی متن کنوانسیون، مخالفت شدید خود را با این کنوانسیون ابراز داشتند.

---

1. Dual Criminality
2. Invasiveness

شورای اروپا به این درخواست‌ها پاسخ و مدام وعده داد که در زمان امضا و تصویب فرصت رایزنی و مشارکت دمکراتیک به‌صورت موردبه‌مورد در سطح ملی داده خواهد شد.

اما هم‌زمان با فرایند مذاکرات در مورد این کنوانسیون، گروه لیون در مورد جرائم سازمان یافته فراملی[1] ـ که گروه هشت، آن را تشکیل داده بود ـ در مورد مسئله جرائم مرتبط با فناوری‌های برتر کار می‌کرد. این گروه برای رایزنی با بخش خصوصی کشورهای عضو گروه هشت در مورد پیشنهادهای مربوط به اختیاراتی که برای تحقیق درزمینه این‌گونه جرائم در نظر گرفته بود، در سال ۲۰۰۰ یک سلسله اجلاس‌هایی را برگزار کرد. نتایج اولین اجلاس، که در ماه می ۲۰۰۰ در پاریس برگزار شد، نامشخص بود زیرا علایق و مواضع دولت‌ها و بخش خصوصی باهم تعارض داشت. اعلامیه نهایی، برخی از این نگرانی‌ها، از جمله موضوع آزادی‌های مدنی و حریم خصوصی، حفظ اختیارات سازمان‌های مجری قانون، تعیین رژیم حقوقی مشخص و شفاف برای مبارزه با جرائم سایبر و تضمین توسعه آزادانه و منصفانه بازار در راستای تأمین شرایط مطلوب برای فعالیت بخش خصوصی را بیان کرد و درعین‌حال به ارزیابی کارآمدی و پیامدهای این سیاست‌ها پرداخت (G8 Lyon Group, 2000).

در اکتبر ۲۰۰۰، اجلاس برلین با پیشنهاد بعضی از اصلاحات دیگر پایان یافت، اما دوباره همه شرکت‌کنندگان توافق داشتند که همچنان کار بیشتری باید در این مورد انجام گیرد. در این راستا، دغدغه‌ها درزمینه جرم و تعدیل هزینه‌های تمهیدات پیشنهادی، الزامات توسعه فناوری، تداوم نگرانی‌های مجریان قانون در مورد دسترسی به داده‌ها، سیر تکاملی تعاریف در مورد انواع مختلف خدمات و ارائه‌دهندگان خدمات مطرح شد و مسائل مربوط به فرایند و تشریفات قانونی اجرای طرح کمک حقوقی متقابل، صحت و اطمینان به داده‌ها، حریم خصوصی و آزادی‌های مدنی نیز همچنان به قوت خود باقی بود. نتایج اجلاس برلین به پیش‌زمینه‌ای برای اجلاس توکیو که در می ۲۰۰۱ برگزار شد مبدل گردید چرا که بررسی‌ها و تحقیقات بیشتری باید انجام می‌گرفت.

---

1. Lyon Group on Transnational Organised Crime

اجلاس سران توکیو نتایج بسیاری در پی نداشت؛ درحقیقت، تداوم ناتوانی در رسیدن به توافق، آیندهٔ گفت‌وگوهای میان بخش خصوصی و دولت در چارچوب چنین اجلاس‌هایی را مورد تردید قرار داد. گزارش مختصری که وزارت امور خارجه و تجارت بین‌الملل کانادا در مورد اجلاس توکیو منتشر کرد پیچیدگی موضوعات به‌عنوان یکی از موانع حصول پیشرفت در همه این اجلاس‌ها معرفی شد: کنفرانس توکیو، که نوعی پیشرفت و موفقیت به‌شمار می‌آید، برخی از نارسایی‌های موجود در فرایند گفت‌وگوی بخش خصوصی و دولت‌های گروه هشت را برجسته می‌سازد که البته قبل از برگزاری اجلاس‌های آینده رفع خواهند شد (Purdy, 2001).

حوادث یازده سپتامبر ۲۰۰۱، این برداشت اولیه را که انجام مذاکرات بیشتر با بخش خصوصی ضرورت دارد، تصحیح کرد. در بحبوحه اظهاراتی که درزمینه «فوریت بیشتر این کار» مطرح می‌شد (G8 Lyon Group, 2001) واکنش‌های پیش‌نویس مقدماتی گروه هشت در برابر حملات تروریستی به آمریکا در نوامبر ۲۰۰۱ انتشار یافت. در این پیش‌نویس، مقرر شده بود که «قوانین حریم خصوصی باید به‌گونه‌ای تغییر یابد که زمینه تأمین امنیت عمومی و سایر ارزش‌های اجتماعی فراهم شود». در این راستا، پیشنهاد شده بود که سازمان‌های داخلی مجری قانون اجازه یابند اولاً، دستورالعمل‌هایی درزمینه دسترسی فوری به داده‌ها و حراست از آنها در برابر نفوذ بیگانگان در اختیار ارائه‌دهندگان داخلی این‌گونه خدمات (البته بعد از آنکه مورد تأیید قرار گرفتند) قرار دهند، ثانیاً، تضمین دهند که زمینه دسترسی فوری به داده‌ها و صیانت از آنها را فراهم می‌کنند، ثالثاً، حتی اگر قوانین داخلی دولت درخواست‌کنندهٔ کمک نقض نشده باشد، کمک حقوقی متقابل به آن کشور را تسریع بخشند و رابعاً، دولت‌های عضو را به صدور گواهی‌نامه‌های سطح ـ کاربر برای کاربردهای مورد نظر تشویق نمایند. با این اوصاف، مخالفت‌هایی که در آغاز ابراز می‌شد، از یاد رفتند.

این توصیه‌ها در اسناد رسمی اجلاس وزرای دادگستری و کشور گروه هشت، که می ۲۰۰۲ در شهر مونت ترمبلنت[1] برگزار شد، گنجانده شد. اسنادی که در این اجلاس به تصویب رسید از دولت‌ها خواستند که مشخص سازند چه اطلاعاتی برای اهداف

1. Mont-tremblant

امنیت عمومی مفید است (G8 Justice and Interior Ministers, 2002). توصیه‌ها به‌طور مستقیم از اسناد «کارگاه دولت ـ بخش خصوصی» که انواع و اقسام اختیارات و رویه‌های اجرای قانون را به‌طور مبسوط تشریح کرده‌اند (.Ibid) و یکی از بیانیه‌های رسمی که تأثیر مخرب رژیم‌های حراست از حریم خصوصی و حفاظت از داده‌ها بر امنیت عمومی را خاطرنشان می‌سازد، (.Ibid). برگرفته شده‌اند. رهبران این اجلاس، معاهدات بین‌المللی، از جمله کنوانسیون شورای اروپا را نیز مورد توجه قرار دادند.

۲-۱۴ سطح ملی

سیاستگذاری‌هایی که در سطح ملی در مورد جرائم مرتبط با فناوری‌های برتر انجام می‌گیرد، پویش‌ها شایان توجه‌اند. اتهام تطهیر سیاست به دفعات علیه آمریکا مطرح شد. کسانی که این اتهام را مطرح کردند، مدعی بودند حتی در زمانی که آمریکا خودش کنوانسیون شورای اروپا را تصویب نمی‌کند، بر سایر کشورها فشار وارد می‌آورد که این کنوانسیون را تصویب کنند. فرایند تصویب معاهدات در آمریکا بسیار طولانی و پرشاخ و برگ است؛ زیرا تصویب نهایی معاهدات در این کشور در گرو تصویب آنها ازسوی مجلس سناست ـ این رویه در آمریکا درست برخلاف رویهٔ کشورهای دیگری است که در آنها نیروی اجرایی دولت، نفوذ بیشتری بر روند تصویب دارد.

بعضی از کشورها در حال حاضر تصمیم گرفته‌اند این کنوانسیون را تصویب کنند و از آن به‌عنوان الگویی برای سایر حوزه‌ها استفاده نمایند. جالب آنکه برخی از کشورهایی که این کنوانسیون را به تصویب رسانده‌اند، عضو شورای اروپا نیستند. در زمان نگارش این سطور، تنها کشورهای استونی، کرواسی، مقدونیه، لیتوانی، مجارستان، آلبانی، رومانی و اسلونی کنوانسیون را تصویب کرده‌اند. بحث‌هایی نیز برای تصویب این کنوانسیون در کشورهای بلغارستان، کانادا و ژاپن وجود داشته و تصویب آن در استرالیا وارد گفتمان سیاسی و حقوقی شده است. در جولای ۲۰۰۱، دولت استرالیا اعلام کرد که قرار است لایحه «جرائم رایانه‌ای»، که به پارلمان ارسال شده است و کاربران را ملزم می‌سازد کلیدهای رمزنگاری ایجاد کنند، مبتنی‌بر این کنوانسیون باشد، (Attorney General, 2001) گفتنی است این کنوانسیون حاوی چنین شرطی نیست.

نمایندگان پارلمان و جامعه مدنی ژاپن ابراز نگرانی کرده‌اند که رایزنی ملی در مورد تصویب کنوانسیون شورای اروپا در شرایطی که دولت‌های خارجی فشار وارد می‌آورند، با موفقیت همراه نخواهد بود. در اجلاس مشترک آمریکا و ژاپن در مورد سیستم‌های اطلاعاتی و امنیت شبکه‌ای که سپتامبر ۲۰۰۳ برگزار شد، بیانیه مشترکی منتشر شد که بخشی از آن در ذیل می‌آید:

ایالات متحده آمریکا و ژاپن اهمیت همکاری چندجانبه درزمینه امنیت سایبر، از جمله تصویب کنوانسیون شورای اروپا در مورد جرائم سایبر را تأیید می‌کنند (United States and Japan, 2003).

و تصریح کردند که:

دولت‌ها تشویق می‌شوند برای اجرای توصیه‌ها و طرح‌هایی که در مجامع بین‌المللی از قبیل گروه هشت، سازمان همکاری و توسعه اقتصادی و اوپک به تصویب می‌رسند، در درون این مجامع باهم همکاری کنند (Ibid.).

در همین فضاست که گفتمان ملی در مورد این کنوانسیون ظاهراً در حال شکل‌گیری است. در کانادا، دولت پس از چند سال بررسی سیاست‌های سایر دولت‌ها در مورد ردگیری قانونمند، در سال ۲۰۰۲ بالاخره رایزنی در مورد دسترسی قانونمند را آغاز کرد. سند رایزنی آشکار می‌سازد که مقدار زیادی از این رایزنی در پاسخ به شرایطی است که کنوانسیون شورای اروپا مقرر کرده است:

کنوانسیون خواستار «جرم قلمداد کردن» برخی از خلاف‌های مرتبط با رایانه‌ها، تصویب اختیارات رسیدگی به جرائم به‌منظور تحقیق و تحت پیگرد قانونی قرار دادن جرم سایبر و ترویج همکاری بین‌المللی با کمک حقوقی متقابل و استرداد مجرمان در قلمرو جرم‌خیزی است که هیچ مرزی را نمی‌شناسد. کنواسیون به کانادا و شرکای این کشور کمک خواهد کرد با جرائمی که اعتبار و دسترسی به ابعاد سرّی و محرمانه سیستم‌های رایانه‌ای و شبکه‌های ارتباطاتی را به خطر می‌اندازند و نیز با فعالیت‌های مجرمانه‌ای از قبیل کلاهبرداری آن‌لاین یا پخش هرزه‌نگاری اطفال در اینترنت که از چنین شبکه‌هایی برای ارتکاب خلاف‌های سنتی استفاده می‌کنند، مبارزه نمایند (Department of Justice, Industry Canada and et. al., 2002).

جالب اینکه، این سند تنها به بحث درباره برخی از توانمندی‌های نظارتی و جرم‌انگاری‌ها می‌پردازد و همکاری بین‌المللی و کمک حقوقی متقابل را مورد بحث و بررسی قرار نمی‌دهد. به‌نوعی می‌توان گفت دولت کانادا از کنوانسیون شورای اروپا به‌عنوان مبنای افزایش اختیارات در حوزه تحقیق و رسیدگی به جرائم سایبر بهره‌برداری کرد؛ اما به‌ظاهر این کشور مایل نیست این کنوانسیون را تصویب کند و نمی‌خواهد به شرایطی که سایر کشورها درزمینه همکاری ایجاد می‌کنند، متعهد و وفادار باشد.

این اواخر، وقتی کنوانسیون شورای اروپا درباره جرائم سایبر به کمیته روابط خارجی سنا ارسال شد، رئیس این کمیته بلافاصله اعلام کرد که: «در این جلسه، سه معاهده بین‌المللی دیگر نیز مورد بررسی قرار می‌گیرد. من رئیس آن مقامات آمریکایی هستم که روی این موافقت‌نامه‌ها، که پشتوانه وسیعی دارند، کار کرده‌اند. برخی از این موافقت‌نامه‌ها و اسناد، محصول سال‌ها صرف وقت، نیرو و مذاکرات صبورانه‌اند. تصویب فوری این موافقت‌نامه‌ها به ایالات متحده کمک خواهد کرد همچنان نقش رهبری را درزمینه اجرای قواعد حقوق بین‌المللی ایفا کند و علاوه‌بر این، امنیت آمریکایی‌ها را در داخل و خارج از کشور تأمین خواهد کرد» (Lugar, 2004).

این کنوانسیون، چه خوب چه بد، درهرحال موافقت‌نامه‌ای است که هم سازمان‌های غیردولتی و هم بخش خصوصی، به‌ویژه در مورد نبود رایزنی در فرایند تدوین آن، شک و تردیدهای فراگیری دارند؛ البته ایالات متحده آمریکا نیز از این وضعیت به‌خوبی آگاه است. این وضعیت، همان چیزی است که اظهارات سناتور لوگار (Ibid.) را به نمونه بارز تبیین این پویش‌ها مبدل می‌سازد: «حتی در طول فرایند مذاکرات نیز ایالات متحده آمریکا تلاش کرده بود مذاکرات به‌صورت علنی باشد (و تا آنجا که معلومات من قد می‌دهد، آمریکا تنها کشوری بود که چنین کرد)، اما پس از آن در طول فرایند تصویب، یعنی درست در زمانی که رویه تصویب دولت آمریکا دشوارترین و طولانیترین رویه بود، رئیس کمیته خواستار تصویب «فوری» کنوانسیون شد و این کنوانسیون را به‌صورت فله‌ای و با شتابزدگی به همراه دو موافقت‌نامه بین‌المللی دیگر به تصویب رسانید. موافقت‌نامه‌های بین‌المللی و رهبری بین‌المللی هم‌اکنون زبان بررسی موضوعات در سطح ملی است که به این دو مفهوم تقلیل داده شده است» (Ibid.).

۳-۱۴ رقص بین‌المللی ـ ملی: نگهداری جریان داده‌ها

نگهداری داده‌ها یکی از نمونه‌های جالب همکاری میان سیاستگذاری ملی و بین‌المللی است. این فرایند تا حدودی در بریتانیا آغاز شد و به‌مرور زمان، گروه هشت و اتحادیه اروپا نیز آن را به‌کار گرفتند و به‌صورت زنجیره‌ای درآمد که دوباره به شبکه‌های بریتانیا ملحق شد. اما این مسیر پیامدهای پیش‌بینی نشدهٔ بسیاری را در پی دارد.

در آگوست ۲۰۰۰، تعدادی از نهادهای مجری قانون بریتانیا طرحی را به وزارت کشور پیشنهاد کردند. در این طرح پیشنهاد شده بود که یک نهاد دولتی مرکزی تمامی داده‌های تردد ارتباطات را به مدت حداقل هفت سال نگهداری کند (Gasper, 2000).

در آن زمان، این نگهداری اطلاعات حساس از جمله، داده‌های مکالمات تلفنی، داده‌های ارتباطات اینترنتی با پست الکترونیک و حتی داده‌های دیدار از وب‌سایت‌ها در دولت با مقاومت چشمگیری مواجه شد. به‌ویژه اینکه، این سیاست نگهداری، به‌موجب دستورالعمل اتحادیه اروپا درزمینه حفاظت از داده‌ها که سال ۱۹۹۵ به تصویب رسید با اصول حفاظت از داده‌ها مغایرت دارد. این دستورالعمل خواهان نابودسازی تمامی داده‌های حساس در زمانی که دیگر بدان‌ها نیاز نیست می‌باشد و جالب آنکه همان قانون بریتانیا را با عنوان قانون حفاظت از داده‌ها (۱۹۹۸) اجرا کرد (European Union, 1995).

تقریباً در همان مواقع، اتحادیه اروپا مشغول به‌روز کردن دستورالعمل‌های خود درباره حفاظت از داده‌ها بود تا بتواند امکانات لازم را برای تسهیل تجارت و تبادلات الکترونیک فراهم کند. در گردهمای کشورهای اروپایی، بریتانیا در همان ابتدا خواهان تغییر در محتوای دستورالعمل حفاظت از داده‌ها درزمینه ارتباطات الکترونیکی بود؛ این نوع تغییر به دولت‌های عضو اجازه می‌داد زمینه‌های نگهداری داده‌ها را فراهم کنند. اما هیچ پیشرفتی حاصل نشد. یکی از ملاحظاتی که مطرح شد این بود که موضوع نگهداری داده‌ها در کنوانسیون شورای اروپا گنجانده شود، اما شورای اروپا آن را نپذیرفت. گروه هشت نیز موضوع نگهداری داده‌ها را مورد بحث و بررسی قرار داد اما چنان‌که در بالا اشاره شد، بخش خصوصی این طرح‌های پیشنهادی را از ریشه رد کرد.

اکتبر سال ۲۰۰۱، جرج دبلیو بوش، رئیس‌جمهور آمریکا نامه‌ای به رئیس کمیسیون اروپا نوشت. در این نامه، وی پیشنهاد کرده بود که تغییراتی در سیاست اروپا

انجام گیرد؛ به‌گونه‌ای که این سیاست، موضوعات مرتبط با نگهداری داده‌ها را در چارچوب الزامات مبارزه با تروریسم و اجرای قانون مدنظر قرار دهد و در نتیجه، در پیش‌نویس دستورالعمل‌های اتحادیه اروپا در مورد حریم خصوصی که خواهان نابودسازی الزامی برای تسهیل نگهداری داده‌های حساس[1] می‌باشند، بازنگری کند (Bush, 2001). این توصیه برآمده از ابراز نگرانی‌هایی بود که پیش‌تر نیز آمریکا به اروپایی‌ها خاطر نشان کرده بود. آمریکا معتقد بود تشریفات و رویه‌های نگهداری داده‌ها و نیز اطلاعات اجرای قانون می‌باید به روش‌هایی تدوین و طراحی شود که همکاری بین‌المللی را تضعیف نکند (United States Government, 2001).

هرچند اجلاس‌های متعدد میان دولت‌ها و بخش‌های خصوصی در کشورهای گروه هشت نیز پیش‌تر، برای مثال، در دوران قبل از یازده سپتامبر، این قبیل نگرانی‌ها را رد کرده بود، اما همین نگرانی‌ها بعد از اظهارات بوش، در اسناد اجلاس سران گروه هشت که ماه می ۲۰۰۲ برگزار شد، مطرح شدند. تضمین وضع قانون درزمینه حفاظت از داده‌ها، در نظر گرفتن امنیت عمومی و سایر ارزش‌های اجتماعی، به‌ویژه با تسهیل نگهداری و صیانت از داده‌هایی که برای الزامات امنیت شبکه‌ای یا فرایندهای بازپرسی و تعقیب مجرمان در عرصه اجرای قانون و به‌خصوص، در حوزه‌های اینترنت و سایر فناوری‌های نوظهور اهمیت دارد (G8 Justice and Interior Ministers, 2002).

ظرف چند ماه بعد از این توصیه، قانون اتحادیه اروپا به‌گونه‌ای تغییر داده شد که مجال نگهداری داده‌ها را فراهم کرد. دسامبر ۲۰۰۱ موضوع نگهداری داده‌ها در واکنش به رویدادهای یازده سپتامبر مطرح شد و براساس قانون بریتانیا درزمینه مبارزه با تروریسم به تصویب رسید. از آن زمان به بعد، تعداد چشمگیری از سایر دولت‌های عضو نیز قوانین مشابهی را درزمینه نگهداری داده‌ها به تصویب رساندند.

هم‌اکنون، بحثی که در اتحادیه اروپا مطرح است اینکه این دستورالعمل چندان هم کافی نبوده است. دستورالعمل سال ۲۰۰۲ به کشورها اجازه می‌داد قوانین نگهداری را به تصویب برسانند. اما در زمان نگارش این سطور، وضعیت نگهداری داده‌ها کمی به‌هم ریخته است، بعضی از کشورها مجال نگهداری داده‌ها را فراهم می‌آورند و برخی دیگر چنین نمی‌کنند.

---

1. Critical Data

وزرای دادگستری و کشور کشورهای عضو به اتحادیه اروپا فشار می‌آورند تصمیم مبنایی[1] درباره نگهداری داده‌ها را که براساس آن، همه دولت‌های عضو باید سیاست‌هایی را درزمینه تسهیل نگهداری داده‌ها داشته باشند، نهایی کند.

این تغییر محل ابزار مواضع به دلایل متعددی که در این مقال نمی‌گنجد نگران‌کننده است. اما یکی از دغدغه‌های خاصی که در این میان وجود دارد، این است که خود آمریکا نیز هیچ سیاستی در مورد حفاظت از داده‌ها و به‌موازات آن هیچ سیاستی درباره نگهداری داده‌ها در اختیار ندارد؛ اما درعین‌حال، از اتحادیه اروپا خواست که رویه‌های خود را درزمینه سازوکارهای دسترسی به حریم خصوصی تغییر دهد.

در این میان، بریتانیا با سیاست اصلی که در سطح ملی طرح‌ریزی کرده بود، شکست خورد و باز هم برای اینکه بتواند چنین قوانینی را به تصویب برساند توجه خود را به اتحادیه اروپا معطوف ساخت. حالا که اتحادیه اروپا مجال نگهداری از داده‌ها را فراهم کرده است درخواست‌هایی برای استاندارد کردن و هماهنگ‌سازی قوانین در سراسر اروپا مطرح شده است تا اطمینان حاصل شود که سایر کشورها نیز قوانین مشابهی را تصویب می‌کنند. واقعیت گیج‌کننده‌ای که در اینجا مطرح است اینکه تطهیر سیاست در حال روی دادن است، اما پی بردن به اینکه دقیقاً چه کسی عمل تطهیر را انجام می‌دهد دشوار است.

۱۴-۴ چالش‌های دمکراتیک و فرصت‌های بین‌المللی

گاهی اوقات می‌توان گفت که سیاست‌ها همانا مایحتاج نهادهای مجری قانون و سایر سازمان‌های حکومتی هستند که ماهیتی داخلی دارند و از طریق مذاکره و با بررسی و سنجش دقیق تدوین می‌شوند. اما این برداشت، دیدگاهی ساده‌انگارانه در مورد سیاست ارائه می‌دهد. حالا دیگر، در مجامع بین‌المللی درباره سیاست‌ها تصمیم‌گیری می‌شود. در حال حاضر، آشکار است که بازیگران سیاسی داخلی به فهم روشن‌تری از فعالیت‌های بین‌المللی نیاز دارند. بنابراین، برای آنکه فهم صحیحی از پویش‌های سیاستگذاری ملی داشته باشیم، باید فعالیت‌های سازمان‌های بین‌المللی و شیوه عمل دولت‌های ملی و

1. Framework Decision

درعین‌حال شیوه مذاکره درزمینه موافقت‌نامه‌ها را نیز مورد توجه قرار دهیم.

سازمان‌های بین‌الدولی، به‌ویژه سازمان‌هایی که به موضوعات مرتبط با سیاست‌های مبارزه با تروریسم و تنظیم فعالیت‌های دیجیتالی می‌پردازند پرشمار بوده‌اند. اما اکثریت قاطع این اجلاس‌ها و سازمان‌های بین‌الدولی منحصر به طرف‌های دولتی می‌باشند که در آنها به مشارکت و رایزنی و بررسی امور می‌پردازند. اما در ماه‌ها و سال‌های آینده، فعالیت‌ها، دستاوردها، توافقات و معاهدات برآمده از آنها احتمالاً بر گفتمان سیاستگذاری ملی تأثیر خواهند گذاشت.

این تأثیرگذاری در مورد اتحادیه اروپا و بیش از همه، در حوزه برون‌دادهای شورای اتحادیه اروپایی که از یک‌سو، فقط دولت‌های ملی در آن نمایندگی دارند و ازسوی‌دیگر، شرایط الزامی متعددی برای وضع سیاست‌ها در سطح ملی وجود دارد، بسیار محتمل خواهد بود.

۱-۴-۱۴ چاره‌های احتمالی

حالا دیگر باید توجه بیشتری به فعالیت‌های مجامع بین‌الدولی مبذول داشت. ابتدا در مورد سیاست‌ها تصمیم‌گیری می‌شود، سپس این سیاست‌ها در سطح ملی به تصویب می‌رسد و این فرایند به‌صورت گزینشی انجام می‌گیرد. این سیاست‌ها فقط به موضوعات جرائم سایبر محدود نمی‌شود. برای مثال، بریتانیا، براساس بحث‌هایی که در اجلاس‌های گروه هشت و سازمان بین‌المللی هواپیمایی کشوری انجام گرفته است به‌سمت تدوین اسناد مطمئنی درزمینه «تعیین و تشخیص هویت» حرکت می‌کند؛ این رویه به درون گفتمان ملی وارد نشده است، اما بریتانیا هم‌اکنون تصمیم گرفته است از این گذرنامه‌ها به‌عنوان ابزارهایی به‌جای کارت ملی تعیین هویت استفاده کند. سیاست‌های دیگری از قبیل انتقال داده‌های مسافران به کشورهای ثالث و حتی سیاست مبارزه با تروریسم در خارج از فرایندهای رایزنی ملی تدوین می‌شوند.

وقتی کشورها به‌سمت تصویب و اجرای سیاست‌هایی که در سازمان‌های بین‌المللی مورد توافق قرار گرفته‌اند حرکت می‌کنند، نقش سازمان‌های غیردولتی ملی بیش‌ازپیش زیر سؤال می‌رود. سازمان‌های غیردولتی تا حد زیادی توجه خود را بر تحولات و روندهای سیاستگذاری ملی متمرکز می‌سازند و تعداد آنها در سطح ملی بسیار زیاد

است. حالا دیگر آنها نیز ناگزیرند بر آن فرایندها و برون‌دادهای سازمان‌های بین‌الدولی که همواره به‌صورت آشکار عمل نمی‌کنند نظارت کنند. در زمان تدوین کنوانسیون جرائم سایبر، شورای اروپا استدلال کرد که انجام رایزنی به شکل آرمانی آن، فرایندی ملی است و وظیفه‌ای نیست که شورای اروپا برعهده گرفته باشد. این ادعا چه‌بسا با توجه به اختیاراتی که این نهاد در حال حاضر دارد، درست است.

انطباق‌دهی و هماهنگ‌سازی کنوانسیون با قوانین ملی ضروری به‌نظر می‌رسد. ازاین‌رو، زمان تصویب کنوانسیون، زمان مناسبی برای بررسی مسائل جدی فراروی کنوانسیون براساس گفتمان‌های سیاستگذاری ملی نخواهد بود. سازمان‌های بین‌الدولی باید گستره اختیارات خود را به‌گونه‌ای تغییر دهند که رایزنی در سطح ملی را نیز در زمانی پیش از مذاکره در مورد منشورها، موافقت‌نامه‌ها و معاهدات لحاظ کنند؛ از این هم که بگذریم، تصور وجود صداقت در گفتمان سیاسی نیز بسیار سؤال‌برانگیز است.

مهم‌تر از همه اینکه، جامعه مدنی و سایر بازیگران می‌توانند این اسناد را ازمنظر لیبرالی تفسیر کنند. به‌طورکلی، این اسناد بین‌المللی به زبانی مبهم نگاشته شده‌اند و تأویل بردارند. هرچند این زبان مبهم به‌گونه‌ای است که منافع تنظیم‌کنندگان و دولت‌های عضو تصویب‌کننده این اسناد را تأمین می‌کند (در این راستا، اسناد به زبانی بسیار قالب‌مند به‌گونه‌ای که پارلمان‌های نافرمان را قانع سازند تدوین نمی‌شوند)، اما این «ابهام‌آلودگی» چه‌بسا ممکن است به نفع بازیگران کوچک‌تر مورد استفاده قرار گیرد. کنوانسیون شورای اروپا قیودی را به‌صورت واضح و مصرح بیان می‌کند که به شیوه‌ای خلاقانه بتوان از آنها تبعیت کرد. اگر تعهدات بین‌المللی دوباره مورد تفسیر قرار گیرند، کنترل دولت در درون چارچوب‌هایی که هیچ گفتمان ملی در اثر افزایش بی‌مورد و غیرضروری اختیارات دولت به بهانهٔ ادعای ضرورت نمی‌تواند محلی از اعراب داشته باشد امکان‌پذیر خواهد بود.

۲-۴-۱۴ تفسیر انعطاف‌پذیر و تبعیت خلاقانه

از یک‌سو، کنوانسیون تعاریف و اصطلاحات مبهمی را در خود جای داده است و ازسوی‌دیگر، براساس مادهٔ نخست آن، دولت‌های تصویب‌کننده ملزم نیستند که به‌طور

مستقیم از این تعاریف رونویسی و تقلید کنند. درمجموع، بسیاری از مفاهیم اساسی در این کنوانسیون فاقد تعریف می‌باشند. این کنوانسیون آشکارا در معرض سوءاستفاده است؛ برای مثال، تعریف «داده‌های در حال آمدوشد»، را می‌توان در قالبی که خاص فناوری است و با این هدف که آسیب‌های وارد بر آزادی‌های مدنی را به حداقل برساند، به‌کار برد. تعریف‌های آرمانی باید بپذیرند که برخی از داده‌های در حال آمدوشد، بسیار حساس‌اند و به داده‌های مربوط به موقعیت، وب‌سایت‌هایی که مورد بازدید قرار گرفته‌اند، نام‌های رایانه‌ای، داده‌های مکالمه‌ای در جایگاه‌های چت کردن و عوامل جست‌وجوگر، محدود نمی‌شود. چه‌بسا این تمایل وجود دارد که «داده‌های در حال آمدوشد» در اینترنت به شیوه‌ای مشابه «داده‌های در حال آمدوشد» در سیستم‌های تلفن تعریف شوند. ما در مورد چنین تمایز شکننده‌ای که میان فناوری‌ها نهاده می‌شود هشدار می‌دهیم؛ برای مثال، داده‌های تلفن همان داده‌های مربوط به موقعیت نیستند. همین که انواع و اقسام داده‌های حساس مورد توجه قرار می‌گیرند، سیاست‌های دسترسی قانونمند درزمینه صیانت از داده‌ها، تولید داده‌ها و نظارت فوری و هم‌زمان بر روند داده‌ها بسته به داده‌هایی که دریافت و تولید می‌شوند متفاوت خواهند بود. تفاسیر ممکن است ناهماهنگی‌های حقوقی در فراسوی مرزها ایجاد کنند و حتی آشفتگی‌هایی را در میان کشورهایی که نظام‌های حقوقی مشابهی دارند، برای مثال در کانادا، ایالات متحده و بریتانیا، به‌وجود آورند، اما همین تعریف‌هایی که در حال حاضر درزمینه مفاهیم و واژگان ارائه شده‌اند، تفاوت‌های چشمگیری باهم دارند (Escudero-Pascual and Hosein, 2003).

البته ممکن است وجود انعطاف در تفسیر کنوانسیون به بروز موانع و دشواری‌هایی نیز بیانجامد. برای مثال، ماده پانزدهم کنوانسیون تصریح می‌کند که «کشورها تضمین می‌کنند اختیارات و رویه‌هایی که به‌موجب این کنوانسیون به اجرا درمی‌آیند، تابع شرایط و تدابیر مندرج در حقوق داخلی می‌باشند تا از حقوق بشر و آزادی‌های انسانی به‌نحو شایسته‌ای حراست شود». این قید، موارد زیر را نیز دربرمی‌گیرد:

۱. گنجاندن اصول «خاص بودن» و «تناسب»،

۲. تضمین نظارت قضایی مناسب،

۳. تضمین اینکه با تمهیداتی از قبیل ارائه ادله کافی قابل اعمال اختیارات، فرایند مناسبی دنبال می‌شود،

۴. محدودسازی گستره مکانی و مدت زمان اعمال اختیارات.

بنابراین ما می‌توانیم توصیه کنیم که دولت تصویب‌کننده، «گفت‌وگویی صریح در مورد تعرض‌آمیز بودن همه این رویه‌ها و ضرورت ارتقا و تقویت حمایت از حقوق بشر در پرتو تحولات فناورانه جدید و برطبق قیدها و شرایط مندرج در این کنوانسیون» انجام دهد. زیرساخت‌های فناورانه گوناگون، تأثیرات گوناگونی بر حقوق، مسئولیت‌ها و منافع مشروع طرف‌های ثالث می‌گذارد. این کنوانسیون از کشورها می‌خواهد موضوعات مندرج در بند سوم مادهٔ پانزدهم را مدنظر قرار دهند. بالاخره اینکه این کنوانسیون را می‌توان با نگاهی موسع مورد تفسیر قرار داد و چنین استدلال کرد که برای دسترسی به داده‌های حساس، مجوز قوه قضائیه ضروری است. در بعضی کشورها، مخصوصاً بریتانیا، این رویه رویکردی انقلابی خواهد بود چرا که سیاست‌مداران و نهادهای پلیسی در حال حاضر نیز مجوز چنین دسترسی‌هایی را صادر می‌کنند.

همین‌طور، در حوزه همکاری‌های بین‌المللی نیز کنوانسیون به‌طور خزنده‌ای محدودیت‌های شرایط دسترسی را بیان می‌دارد. براساس ماده بیست‌وسوم، به‌نظر می‌رسد که کنوانسیون خواستار همکاری میان دولت‌ها در حوزه‌های تحقیق و تفحص درباره جرائم و جمع‌آوری اسناد و مدارک است. اما چند مبنا در این کنوانسیون وجود دارد که به یک کشور اجازه می‌دهد ماده بیست‌وسوم را رد کند و حق تحفّظ برای آن قائل شود. در مورد استرداد مجرمان براساس ماده بیست‌وچهارم، اگر یک دولت متقاعد نشود که همه شرایط و موجبات استرداد به‌قدر کفایت وجود دارد، آن دولت می‌تواند از استرداد فرد مورد نظر استنکاف ورزد. به‌موجب ماده بیست‌وهشتم، طرفی که از وی درخواست استرداد مجرم شده است می‌تواند با این شرط که داده‌هایش برای تحقیقات یا دعاوی‌ای غیر از آنهایی که در درخواست بیان شده مورد استفاده قرار نگیرند همکاری را محدود کند. سازمان‌های غیردولتی و سایر بازیگران کوچک‌تر می‌توانند در فرایند مذاکره درزمینهٔ این شرایط به ایفای نقش بپردازند.

سرانجام اینکه، اگر یک دولت معتقد باشد جرم مورد نظر جرمی سیاسی است یا با یک جرم سیاسی پیوند دارد، یا با حاکمیت یا نظم عمومی یا منافع ذاتی‌اش منافات دارد، می‌تواند درخواست‌ها برای همکاری را رد کند. جامعه مدنی ممکن است فرصت را غنیمت شمارد و از این موقعیت برای ترویج گفت‌وگویی ملی در مورد آنچه جرم سیاسی، نظم عمومی و منافع ذاتی توصیف می‌کند و نیز در مورد رویه‌هایی که چنین وقایعی به کمک آنها به‌صورت موردبه‌مورد بررسی و سنجش می‌شوند، استفاده کند. به‌ویژه اینکه به‌آسانی می‌توان استدلال کرد به‌موجب شرط «جرم سیاسی» باید از هر فردی که حقوق سیاسی‌اش را اعمال می‌کند حمایت کرد.

هدف ما می‌باید این باشد که «به تعاریف دقیقی که در سطح ملی مورد بحث و مذاکره قرار گرفته‌اند رجوع کنیم» تا بتوانیم اولاً، از ابهام‌های موجود در متن کنوانسیون بهره‌برداری کنیم، ثانیاً، اجرای تدابیر کنترل و نظارت را به حداقل برسانیم، ثالثاً، به فرایندهای مشخصی درزمینه اعطای مجوز و کنترل استفاده از فنون نظارت تعرض‌آمیز دست یابیم و رابعاً، پیش از به‌کار گرفتن هریک از این اختیارات از شرط «مجرمیت دوگانه» نیز بهره‌برداری کنیم. اگر ما این تمهیدات را انجام ندهیم، آنگاه قانونگذاران البته در راستای منافع خودشان چنین خواهند کرد.

۳-۴-۱۴ اقدام در حوزه‌های سیاستگذاری متمرکز

استراتژی دیگر این است که این سیاست‌ها را در نقطه‌ای که تمرکز می‌یابند به اجرا درآوریم. شورای اروپا، گروه هشت و حتی اتحادیه اروپا نهادهای خاص فرایندهای رایزنی نیستند. اما باز هم می‌توان فعالیت‌هایی را که در این حوزه انجام داده‌اند مورد توجه قرار داد. در شورای اروپا، جامعه مدنی که به‌نحوی فعالانه با دبیرخانه شورای اروپا نامه‌نگاری داشت، توجه رسانه‌ها را به این امر جلب کرد که شورای اروپا فاقد چنین فرایندی بوده است. در رایزنی گروه هشت، تعدادی از نمایندگان سازمان‌های غیردولتی با دولت آمریکا موفق شدند برای شرکت در اجلاس‌های سران دعوت‌نامه‌هایی را دریافت کنند. سایر کشورها نیز چه‌بسا ناگزیر خواهند شد مانند آنچه هیئت نمایندگی ایالات متحده عمل کرد عمل کنند.

در سطح اتحادیه اروپا نیز درخواست‌هایی برای بازنگری در اسناد حقوقی انجام گرفته است. ممکن است چنین استدلال شود که ابتکارعمل‌های اتحادیه اروپا درزمینه نگهداری داده‌ها، حتی از حیث شیوه تدوین پیش‌نویس این ابتکارعمل‌ها، ازلحاظ حقوقی مشکل‌آفرین‌اند. به‌عبارت دقیق‌تر، به‌موجب برخی از مواد کنوانسیون درزمینه حقوق بشر، نگهداری داده‌ها در ملأ عام غیرقانونی است. رأی حقوقی که برای استفاده در سطح اتحادیه اروپا تنظیم شد، می‌تواند این سیاست را در نقطه‌ای که تمرکز یافته است به اجرا درآورد حتی اگر چنین استراتژی (اقدام در حوزه سیاستگذاری متمرکز) در سطح اتحادیه اروپا با شکست مواجه شود. ازآنجاکه بسیاری از قوانین ملی در اروپا بسیار به یکدیگر شبیه‌اند و همه دولت‌های اروپایی نیز ناگزیر شدند از دیوان اروپایی حقوق بشر تبعیت کنند، یک چالش حقوقی را می‌توان تفسیر و جرح و تعدیل کرد و در سطح محلی به‌کار گرفت.

۱۴-۵ نتیجه‌گیری

با وجود همه تغییراتی که در طول بیست سال اخیر در نظام‌های سیاسی ما رخ داده‌اند، مشکلاتی که ما هم‌اکنون با آنها دست به گریبانیم بسیار طبیعی به‌نظر می‌رسند. جهانی شدن و فناوری‌ها و تهدیدهای بین‌المللی راه‌حل‌های بین‌المللی را می‌طلبند. افزایش شمار سازمان‌های بین‌الدولی که به بررسی و تدوین سیاست‌ها می‌پردازند، شاید برآیندهای گریزناپذیری باشند.

این همان دیدگاهی است که من می‌خواهم آن را رد کنم؛ البته نه به آن علت که نادرست است، بلکه بالعکس به این دلیل که بسیار خطرناک است. در عوض، من در این فصل تأکید کرده‌ام پویش‌هایی در کارند که برای فهم نیمهٔ پنهان و تاریک همکاری بین‌المللی و سایر امور اجتناب‌ناپذیری از این قبیل، درخور توجه و بررسی‌اند. وقتی این مجامع بین‌المللی برای بررسی و تدوین سیاست‌ها مورد استفاده قرار می‌گیرند، فرایندها و رویه‌های دمکراتیک متحول می‌شوند. از همین رو، چندجانبه‌گرایی فی‌نفسه خوب نیست، بلکه جلوه دیگری از «سیاست قدرت» و توازن بخشیدن به منافع است. آنهایی که در مجامع بین‌المللی دارای قدرت و نفوذند و آنهایی که در این اجلاس‌ها پشت میز مذاکرات می‌نشینند، اختیارات بی‌سابقه‌ای در سطح ملی دارند.

بر همین اساس، چشم‌انداز سیاستگذاری متحول می‌شود؛ البته، این تحول به شکلی مطلوب و در قالب رایزنی ملی نیست. تطهیر سیاست برای ترویج سیاست‌ها در مجامع بین‌المللی مورد استفاده قرار می‌گیرد. در این راستا تنها این سیاست‌ها برای «تصویب» یا «هماهنگ‌سازی» به همراه مقدار ناچیزی از بحث‌هایی که در سطح ملی انجام می‌گیرد به قلمرو صلاحیت ملی بازگردانده می‌شود. هم آمریکا و هم بریتانیا را می‌توان به ترویج ایده‌های انحصاری خود در مجامع بین‌المللی متهم کرد. در این صورت می‌توان دید که آنها این سیاست‌ها را در سطح ملی نیز دنبال می‌کنند بی‌آنکه در وهله اول مسئولیت عواقب سیاست‌ها را نیز برعهده بگیرند. مدل‌سازی برای رونویسی از قوانین و معاهدات و موافقت‌نامه‌های بین‌المللی مورد استفاده قرار می‌گیرند که زبان مورد استفاده در خارج از یک کشور را بی‌آنکه بررسی کافی در مورد آن انجام بگیرد در حقوق داخلی آن کشور می‌گنجانند. کپی‌برداری از زبان «داده‌های در حال آمدوشد» در کنوانسیون شورای اروپا در مورد جرائم سایبر می‌تواند بحث در مورد بررسی مجدد ریشه‌ای قوانین داخلی براساس طراحی متناسب فرایند اجرای قانون و تدوین مناسب اختیارات در این زمینه را به میان بکشد، اما این امر هرگز روی نخواهد داد. بالاخره، تغییر محل ابراز مواضع برای تعقیب سیاست‌ها از طریق رسانه‌های بین‌الدولی رخ می‌دهد؛ البته این وضعیت تا زمانی است که جایگاه مناسبی علاوه‌بر این‌گونه سازمان‌ها یافت نشود. بحث نگهداری داده‌ها در گروه هشت دنبال شد و پس از آن به اتحادیه اروپا آورده شد، دولت‌های عضو اتحادیه اروپا که می‌خواستند مسیری با کمترین مقاومت را درزمینه تصویب قوانین داخلی خود بیابند، جایگاه طبیعی «تصویب قانون درزمینه نگهداری داده‌ها» را در این نهاد نیافتند.

اگر ظرفیت‌ها توسعه نیابند، این پویش‌ها ظرفیت اقدام ما را تحلیل خواهند برد. بازیگران غیردولتی باید گنجینهٔ بهتری از استراتژی‌ها را برای مقابله با ماهیت بستهٔ این مجامع و زبان بین‌المللی‌گرایانهٔ اقناعی آنها طرح‌ریزی کنند. این شکل از فعالیت، رو به گسترش و افزایش است و هر معاهده و موافقت‌نامه بین‌المللی، قانون مدل‌واره و توصیه و پیشنهاد جدیدی هم که برآمده از همه این سازمان‌های بین‌الدولی باشد، این شکل از فعالیت را در خود دارد.

ردگیری همه این فعالیت‌ها آسان نیست. هدف، همچنان تغییر محل ابزار مواضع است و این سیاست‌ها همچنان مبتنی‌بر جابه‌جا شدن است و درخواست‌ها برای هماهنگ‌سازی و همکاری بین‌المللی افزایش یافته است. اما هنوز هم به‌نظر نمی‌رسد که ما این مسابقه را با دقت هرچه تمام‌تر دنبال می‌کنیم. برای آنکه بفهمیم بازی در کجا انجام می‌گیرد باید به این پویش‌ها توجه کنیم. در این صورت است که ما می‌توانیم ساختارهای جدید پاسخ‌گویی را برای بازیگران ایجاد کنیم؛ البته فرصت‌هایی نیز وجود دارد؛ ما می‌توانیم از بعضی تمهیدات متقابل[1] بهره‌برداری کنیم. برای تحقق این امر باید بار دیگر توجه خود را بر این قبیل موضوعات متمرکز سازیم.

1. Counter-measures

منابع و مآخذ

Attorney General *Cybercrime Bill 2001 Second Reading Speech by the Attorney General,* The Parliament of the Commonwealth of Australia, 2001.

Bush, G.W, 'Letter from President George W. Bush to Mr Romano Prodi, President, Commission of the European Communities. Brussels', Forwarded by the Deputy Chief of Mission to the European Communities. Brussels' Forwarded by the Deputy Chief of Mission to the European Union, 16 October 2001.

Canadian Delegation Discussion Paper for Workshop 1: *Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers.* Tokyo, G8 Government-Industry Workshop on Safety and Security In Cyber-space, 2001.

Department of Justice, Industry Canada, and et. al. *Lawful Access-Consultation Document.* Ottawa, Government of Canada, 2002, p.21.

Escudero-Pascual, A., and I.Hosein the Hazards of Technology-neutral Policy: Questioning Lawful Access to Traffic Data. *Communications of the ACM.* 2003. Accepted for publication 24 October 2002.

European Union Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals With regard to the Processing of Personal Data and on the Free Movement of Such data: 0031-0050(1995).

G8 Justice and Interior Minister *Data Preservation Checklists,* Mont-Tremblant, G8 Summit, 2002a.

G8 Justice and Interior Minsters *G8 Statement on Data Protiction Regimes.* Mont Tremblant, G8 Summit, 2002b.

G8 Justice and Interior Ministers *Principles on the Availability of Data Essential to Protecting Public Safety.* Mont-Tremblant, G8 summit, 2002c.

G8 Justice and Interior Ministers *Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigation.* Mont-Tremblant, Quebec, Group of 8, 2002d.

G8 Lyon Group 'Un Dialogue Entre les Pouvoirs Publics et le Secteur Prive'sur la Se'curite' et la Confiance dans le Cyberespace', Communique' du G8 (Groupe de Lyon) (Paris: G8, 2000).

G8 Lyon *Group Recommendations for Tracing Networked Communications Across National Borders in Terrorist and Criminal Investigations* (Draft), G8, 2001.

Gaspar, R. Looking to the Future: *Clarity on Communications Data Retention Law*. A submission to the Home Office for Legislation on Data Retention, On Behalf of ACPO and ACPO(S); HM Customs & Excise; Security Service; Secret Intelligence Service; and GCHQ, 2000.

Goldsmith, J.L. 'Against Cyberanarchy', *University of Chicago Law Review,* 65 1998, 1199-1250.

Goldsmith, J.L. 'Symposium on the Internet and Legal Theory: Regulation of the Internet: Three Persistent Fallacies', *Chicago-Kent Law Review,* 73, 1998, 1119-1131.

Johnson, D.R. and D.G. Post 'Law and Borders-The Rise of Law in Cyberspace', *Stanford Law Review,* 48, 1996, 1369.

Lugar, Serator R.G.' Chairman. Opening Statement for Hearing on Law Enforcement Treaties, 17 June 2004. Available at http://foreign.serate.gov /testimony /2004 /LugarStatement040617.pdf.

Purdy, D. Report of the G8 Government/Private Sector High Level Meeting on High-tech Crime, Tokyo, Japan: Department of Foreign Affairs and International Trade, 2001.

Sun, J.-M. and J.Pelkmans 'Regulatory competition in the Single Market', in C. Hood (ed.), A Reader on Regulation, Oxford: Oxford University Press, 1998, PP.443-67.

United States and Japan, 2003 United States-Japan Joint Statement on Promoting Global Cyber Security.

United States Government Comments of the United States Government on the European Commission Communication on Combating Computer Crime, Brussels, 2001.

فصل پانزدهم نتیجه‌گیری

استیو رایت*، فیلیپا ترورو،**
دیوید وب* و ادوارد هالپین****

بزرگ‌ترین تهدید سایبر در سال‌های پرتلاطم پیش‌رو چیست؟ از دیدگاه عامه‌پسندانه‌ای که رسانه‌ها آن را به‌شدت ترویج و تبلیغ می‌کنند، بزرگ‌ترین تهدید سایبر از جانب یک گروه متعصّب تروریستی یا یک فرد نابغه و باهوش خودسر است. این دو عامل تهدیدآفرین با جدیتی هرچه تمام‌تر می‌کوشند با رخنه کردن در درون موقعیت‌های شبکه‌های حساس از قبیل سیستم فرماندهی عالی ناتو یا سیستم کنترل حمل‌ونقل هوایی آمریکا تمدن غرب را سرنگون سازند. قضیهٔ گری مک کینن[1] این دیدگاه کلیشه‌ای عامه‌پسندانه را برجسته می‌سازد.(۱) مأموران قضایی آمریکا این واقعه را بزرگ‌ترین سرقت اطلاعات از رایانه‌های ارتش همه اعضا می‌دانند.(۲) وی به جرم رخنه و سرقت اطلاعات از سازمان‌های دولتی آمریکا از جمله فرماندهی قضایی آمریکا و آژانش پروژه‌های تحقیقاتی پیشرفته دفاعی[2] به هفتاد سال حبس محکوم شده است.(۳)

آیا این واقع‌گرانه‌ترین تهدید است؟ سایر صاحب‌نظران بر تلاش‌های گسترده تحقیقات نظامی مخفیانه‌تری که بعضی از دولت‌ها (چه در اتحادیه اروپایی به دلایل و با توجیهات تجاری، چه در چین با هدف ردگیری دگراندیشان سیاسی مظنون) برای کنترل و نظارت بر تبادل اطلاعات در اینترنت انجام می‌دهند، تأکید دارند.

---

* Steve Wright

** Philippa Trevorrow

*** David Webb

**** Edward Halpin

1. Gary Mckinnon
2. Defence Advanced Resaearch Projects Agency

همان‌گونه که در مقدمه این کتاب نیز اشاره شد، در عصر جنگ اطلاعاتی اصلاً تعجب‌برانگیز نخواهد بود که نظامیان، اینترنت را فقط نوعی ابزار قلمداد کنند و بسیاری از افراد، گروه‌ها و سازمان‌ها وابستگی جامعه مدرن به زیرساخت مخابرات را نوعی «آسیب‌پذیری» در نظر آورند که مورد بهره‌برداری قرار می‌گیرد.

پیدایش نانوتکنولوژی‌ها(۴) لاجرم شیوه‌ای را که چنین تسلیحات و داده‌هایی برای هدف‌گیری و منهدم‌سازی مؤثرتر اهداف گردآوری و سازمان‌دهی می‌شوند، دگرگون خواهد ساخت. «مینیاتوری کردن تمام‌عیار»،[1] تک‌تک سربازان را قادر خواهد ساخت به بخشی از میدان نبرد کارآمدتر مبدل شوند به‌طوری‌که فرماندهان می‌توانند همه کلاه‌خودهای سربازان خود را ببینند و عملکرد آنها را به‌خوبی تحت نظر بگیرند. نصب ریزتراشه‌های الکترونیکی روی افراد، دوست را از دشمن تمیز خواهد داد و هویت دوست و دشمن را مشخص خواهد نمود و از خسارت‌های ناشی از آتش سلاح‌های دوستان جلوگیری خواهد کرد، اما فناوری‌های نظارت و کنترل، ماهیت «اهداف» را در جوامع وابسته به اطلاعات تغییر خواهد داد.

البته، جنگ اطلاعاتی بخشی از طیف گسترده اشکال جدید استراتژی‌های نوظهور حمله در زمان جنگ است. مدرن‌ترین دولت‌ها به زیرساخت مخابرات وابسته‌اند. حتی بسیاری از اعضای محافل نظامی این سؤال را مطرح می‌کنند که اگر سیستم‌های عصبی یک کشور را می‌توان از کار انداخت نابودسازی زیرساخت غیرنظامی چه ضرورتی دارد؟ به‌نظر ژنرال فگلمن،[2] رئیس ستاد کل نیروی هوایی ایالات متحده، «سیطره بر پهنه اطلاعات در منازعات کنونی به اندازه تصرف سرزمین یا کنترل هوا که در گذشته تعیین‌کننده بوده است، مهم و سرنوشت‌ساز است».(۵)

این بعد جنگ نیز به‌سرعت رو به تغییر و دگرگونی است، اما رسانه‌ها هیچ توجهی به آن ندارند. برخی از اساتید دانشگاهی، از قبیل پروفسور استفن گراهام[3] از دانشگاه دورهام[4] موضوع «طراحی عملیات‌های نظامی برای حمله به زیرساخت شهری» را بررسی

---

1. Super Miniaturisation
2. General Fogoleman
3. Stephen Graham
4. Durham

کرده‌اند. پدیده‌های زیرساخت شهری که جنبه آشکاری به خود گرفته‌اند در حال حاضر به جزئی از تاکتیک‌های نبرد مدرن[۶] مبدل شده‌اند. گراهام معتقد است بسیاری از دولت‌ها در نظر دارند دشمنانی را که از سپر شهری (غیرنظامی شده) بهره می‌گیرند از وضعیت مدرن خارج سازند. وی با آوردن نقل قولی از تامس فریدمن، روزنامه‌نگار *نیویورک تایمز*، این شکل نبرد را با هژمونی آمریکا پیوند می‌دهد و درعین‌حال، خاطرنشان می‌سازد که چین نیز دکترین جنگی مشابهی دارد. همه وسایل روشنایی در بلگراد خاموش خواهند بود: شبکه‌های برق‌رسانی، لوله‌های آب، جاده‌ها، کارخانجات جنگ‌افزارسازی و سایر کارخانه‌های مرتبط با صنایع جنگی باید هدف قرار گیرند ... ما با درهم کوبیدن شما کشورتان را چندین سال به عقب برخواهیم گرداند. آیا شما سال ۱۹۵۰ را می‌خواهید؟ ما می‌توانیم آن سال را برایتان به ارمغان بیاوریم. آیا شما سال ۱۹۸۹ را می‌خواهید؟ ما می‌توانیم این کار را هم بکنیم.[۷]

تحلیل گراهام، هم تأثیرات اولیه (نابودسازی وسایل روشنایی و ساختمان‌ها)، هم تأثیرات ثانویه (معضلات بهداشتی، کمبود آب آشامیدنی، ناتوانی در تدارک و تأمین برخی مواد غذایی)، و هم تأثیرات ثالثه را (افزایش شمار غیرنظامیان نیازمند کمک) را پوشش می‌دهد. هرچند این نوع فناوری علناً تدبیری مبتنی‌بر محروم‌سازی غیرمرگ‌بار دشمن از منابع معرفی می‌شود، ولی جوامع محارب را به‌صورت یک کل یکپارچه قلمداد می‌کند. پیامدهای این وضعیت را می‌توان در یک عبارت خلاصه کرد: «حالا بمباران کن و بعداً بکش».[۸]

«فناوری نظارت» مدرن به بخشی از این زیرساخت مبدل شده است. در حال حاضر، تسلیحات، سیستم‌های نظارت و کنترل در خود دارند، اما می‌توان از زیرساخت مخابرات (مثلاً شبکه تلفن همراه که ماهیتی خنثی دارد) نه تنها برای عملیات نظارت و کنترل بلکه برای تعیین هدف و هدف‌گیری افراد و گروه‌های مورد نظر استفاده کرد. آنها از طریق اهداف براساس مختصاتی که دارند مشخص می‌شوند؛ ازاین‌رو، ما می‌توانیم داده‌های دیجیتالی درزمینه موقعیت‌ها را برای طرح‌ریزی گزینش هدف با سیستم‌های تسلیحاتی مورد استفاده قرار دهیم (چرا که داده‌های دیجیتالی درزمینه موقعیت‌ها در حال حاضر به یمن وجود «تلفن‌های همراه یا کارت‌های هوشمند تعیین هویت» سهل‌الوصول شده‌اند.

این کتاب دو هدف اصلی و مهم را دنبال کرد: نخست کوشید بررسی کند که چگونه انقلاب در امور نظامی باعث پیدایش فناوری‌های جدیدی شده است، به‌گونه‌ای که این فناوری‌ها هم به پیشرفت زیرساخت نظارت کمک کرده‌اند و هم هدف قرار دادن آن را تسهیل نموده‌اند. اما ازسوی‌دیگر درصدد برآمد تبیین کند که چگونه دکترین‌های نظامی «دسترسی به تمامی نقاط کور» رفته‌رفته به حریم زندگی شهرنشینان در آینده رخنه خواهد کرد. الزامات تشدید بحران در سطح بین‌المللی نیز باعث خواهد شد فعالیت‌های نظارتی از نظارت انبوه و همه‌جانبه فراتر روند و بهره‌گیری از سیستم‌های دقیق‌تر هدف‌گیری نقاط ریز را نیز دربرگیرند. برای مثال، ما باید توجه ویژه و همه‌جانبه‌ای به این موضوع داشته باشیم که برخی از انواع فناوری‌های جدید درزمینه کنترل مرزها تا چه اندازه‌ای می‌توانند سازوکارهای تنبیه و مجازات را نیز در خود جای دهند.

برای مثال، مقاله‌ای با عنوان «دکترین، تحقیقات و آموزش در ایالات متحده» که در دانشکده علوم هوا ـ فضا ارائه شده است فناوری‌های نوظهوری همچون رایانه‌های کوانتومی، نرم‌افزار هوشمند، واقعیت مجازی، داده‌های هوشمند، سلاح‌هایی که با بهره‌گیری از انرژی هدایت می‌شوند، میکروتکنولوژی، بیوتکنولوژی، واسط‌های انسانی ـ رایانه‌ای، کنترل اذهان، دستگاه‌های ویدئویی دوربین‌های دارای امواج میلیمتری را برمی‌شمارد. بسیاری از این فناوری‌ها ـ چه به‌منظور هدف‌گیری طراحی شده باشند، چه برای کنترل هدایت شده به‌وجود آیند و چه هدف از ابداع آنها بررسی بازخورد کارآمدی باشد، بعد نظارتی دارند.(۹)

چنین فناوری‌هایی در حال حاضر از مرحله «الگوی نخستین» فراتر رفته‌اند و سرمایه‌گذاری‌های تجاری هنگفتی برای تولید انبوه آنها انجام می‌گیرد. شرکت‌های تجاری از قبیل شرکت مختلط نظامی میکروسیستم‌های دل[1] از آلمان گزارش داده‌اند که طیف وسیعی از آنچه سیستم‌های فرماندهی، کنترل، ارتباطات، رایانه‌ها و جاسوسی می‌نامند و در تسلیحات با فرکانس رادیویی بالا به‌کار می‌روند تولید می‌کنند. این سیستم‌ها عبارت‌اند از:

۱. جنگ‌افزارهای تک‌تیر[2] که تأسیسات الکترونیکی سلاح‌ها را نابود می‌سازد،

---

1. Diehl Microsysems
2. Single - shot

۲. سیستم‌های تکراری و یکنواختی که سایر کارکردهای مهمات و جنگ‌افزارها را می‌توانند متوقف سازند،

۳. موشک‌هایی که تأسیسات مخابراتی در میدان نبرد تا شعاع ۳۰۰۰ متر مربع را می‌توانند نابود سازند و می‌توانند پایگاه‌های پدافند هوایی، دوربین‌های دارای شارژ کابلی[1] و تأسیسات برق‌رسانی در مراکز فرماندهی را هدف قرار دهند.

شرکت دل، کارویژه‌های فناوری خود را حفاظت از کشتی‌ها در بندرگاه‌ها، نابود کردن تأسیسات الکترونیکی در مخفیگاه‌های تروریست‌ها و حتی تخریب مین‌ها می‌بیند. مدل‌های پیشرفتهٔ چمدانی این نوع فناوری‌ها می‌توانند دوربین‌های نظارت و کنترل، تلفن‌ها، رایانه‌ها و حتی تجهیزات الکترونیکی را که در خودروها نصب می‌شوند تا شعاع یک کیلومتری منهدم سازد. (۱۰) این فناوری‌ها توانمندی‌های اعجاب‌انگیزی نیز برای نجات گروگان‌ها در اختیار دارند ـ اما اگر این فناوری‌ها به‌دست گروه‌های تروریستی بیافتد یا این گروه‌ها به ابداع مدل‌های جدیدی از آنها روی آورند، چنین توانمندی‌ای چه کابوسی را پدید خواهد آورد؟

پژوهشگران آینده باید به تلاش ارتش در به‌کارگیری فناوری نظارت، اطلاعات و رایانه که به‌منظور پیشبرد عملیات‌های ضدتروریستی، کنترل قلمرو داخلی و مقابله با انقلابیون انجام می‌گیرد توجه ویژه‌ای داشته باشند. اما در بسیاری از ابعاد، طیف موضوعات متنوعی که در این زمینه مطرح می‌شوند، بسیار وسیع است و از پرندگان مکانیکی(۱۱) که نقش جاسوسان خُرد نظامی را ایفا می‌کنند گرفته تا سیستم ارتباطات و نظارت جهان‌گستر اشلن[2] را که سیستم هوا فضای ملی آمریکا[3] آن را هدایت می‌کند دربرمی‌گیرند.(۱۲)

اشلن یک شر ضروری در مبارزه با جرائم بین‌المللی و پیگیری جنگ علیه تروریسم به‌شمار می‌آید، اما بااین‌حال پارلمان اروپا در اواخر دهه ۱۹۹۰ با توجه به دستورکار خاصی که درزمینه کنترل سیاسی و اقتصادی افراد و فعالیت‌ها دارد، بازیگران کلیدی در این بازی نظارت بسیار وسیع و همه‌جانبه در سطح بین‌المللی را به چالش کشید.(۱۳)

---

1. Charge-Coubled Deveive
2. Eshelon
3. National Airspace System

پروژه آمریکا در راه‌اندازی اشلن نتوانست جلو حملات یازده سپتامبر را بگیرد ولی هزینه‌ها و بودجه‌های سازمان‌های ذی‌ربط از قبیل سیستم هوا فضای ملی آمریکا افزایش یافته است و وظایف سیاسی آنها که تعرض بیشتر در حریم خصوصی افراد را در پی دارد، افزون‌تر شده‌اند.

مطالعات بسیار اندکی درزمینه بررسی چگونگی تأثیرگذاری این شبکه‌های نظامی نظارت و کنترل جهان‌گستر بر جامعه مدنی انجام گرفته است. ما می‌دانیم که بعد از یازده سپتامبر، سازمان‌های دیگری برای پردازش اطلاعاتی چنین داده‌هایی طراحی می‌شوند ولی آن‌چنان‌که باید و شاید هیچ نظارتی بر عملکرد آنها انجام نمی‌گیرد. ازاین‌رو این تشکیلات قادرند حریم‌هایی را که حقوق داخلی مقرر کرده است و نظارت و کنترل همه‌جانبه بر حریم خصوصی زندگی افراد را نفی می‌کند نقض کنند. برای مثال، در گذشته، ردگیری و شنود مکالمات تلفنی فقط درصورت اخذ مجوز قانونی و حکم قضایی امکان‌پذیر بود. ازاین‌رو، تحقیق و تفحص فراگیر و همه‌جانبه غیرقانونی از افراد که در حال حاضر وجود دارد، روا نبود.

وقتی بحران بین‌المللی تشدید می‌شود، گروه‌هایی که نقش و کارویژه چنین سازمان‌هایی را زیر سؤال می‌برند، منافع و علایق افرادی را که اهداف چنین سازمان‌هایی به‌شمار می‌آیند برجسته‌تر خواهند ساخت. این نتیجه‌گیری یک سؤال ساده را مطرح می‌کند: ما چگونه در مورد موجودیت‌های غول‌پیکر کنترل‌گر و نظارت‌کننده در هنگامی‌که سر برآورند تحقیق خواهیم کرد؟ تعداد معدودی از افراد و سازمان‌های غیردولتی توانسته‌اند فعالیت‌های چشمگیری درزمینه گردآوری فهرست این قبیل ابتکار عمل‌های فراملی براساس منابع موجود و آشکار انجام دهند.[۱۴] در عصر تروریسم، پژوهشگران آینده تا چه حدی این آزادی عمل را خواهند داشت که درباره ساختارهای دولتی به تحقیق و پژوهش بپردازند و خوانندگان کتاب‌هایی مثل این کتاب تا چه اندازه از این فعالیت فکری دفاع خواهند کرد؟ این وضعیت، فقط نوعی اخترشناسی اجتماعی است (مشاهده بدون مسئولیت).

پی‌نوشت‌ها

1. 'Game Over', *The Guardian*, 9 July 2005.

2. Ibid.

3. See interview with J. Ronson, 'Game Over', *The Guardian Weekend*, 9 July 2005, PP. 26-31.

4. J. Altmann, 'Military Uses of Microsystem Technologies', *Series Science, Disarmament and International Security,* Germany: FOANS 2.

5. General Fogelman, 'Information Operations', *US Air Force Doctrine Document, 2-5*. August, 1998. Available at http://www.dtic.mil/doctine /jel/ service_Pubs/afd2_5.pdf.

6. See S. Graham, 'Switching Cities Off', City, 9(2), July 2005, 169-93.

7. *New York Times Columnist* T.Friedman, 23 April 1999, Cited by Graham, 2005.

8. 'Bomb Now, Die Later', *Washington Post*, 1998, p.1. Available online at http://www.washingtonpost.com.wp-srv/inatl/longterm/forgofwar/vignettes/v10.htm.

9. W.A. Stanmeyer, *Emerging Technologies* IW-270 (College of Aerospace: Doctrine Research & Education). Available online at http://www.afrl.af.mil.

10. See R. Stark, M. Sporer, G. Staines (DIEHL Munitonssysteme), 'Non-Lethal Capabilities: Facing Emerging Threats', *Compact High Power RF Sources, for Non-Lethal Applications, presentation,* 2nd European Symposium on Non-Lethal Weapons, 13-14 May 2003, Ettlingen, Germany, Section 19-19.

11. 'Mechanical "Roboflie" Lend Wings to Defence', *Financial Times,* 22 November *2001*, p.15. See also http://www.newswise.com /articles/ view/ 502903/

12. See http://www.jya.com/stoa-atpc.htm.

13. D. Campbell, *Interception Capabilities,* 2000. Available online at http://www. iptvreports. mcmail.com/stoa_cover.htm.

14. See: http://www.statewatch.org.