مجله سیاست دفاعی
شماره ۳۳-۳۲، پاییز و زمستان ۱۳۷۹

جنگ اطلاعاتی و نقش آن در جنگ آینده

تاریخ ارائه: ۷۹/۷/۱۰ *تاریخ تصویب:* ۷۹/۹/۱۴

نویسنده : دکتر رضا کلهر*

کلیدواژه‌ها

جنگ اطلاعاتی، اطلاعات استراتژیک، انقلاب اطلاعاتی، هکرها، تصمیم‌گیری، تروریسم، سیستم اطلاعاتی، جاسوسی اقتصادی، ارزیابی اطلاعاتی، فرآیندهای اطلاعاتی، ارتباطات.

چکیده

تحولات در عرصه‌های گوناگون به عرصه جنگها نیز کشیده شده‌است. جنگ اطلاعاتی یکی از این پیامدهاست. تکنولوژی اطلاعات که حضور و ظهورش به حدود دو دهه بازمی‌گردد با سرعتی بیش از تصور ما حوزه‌های متفاوت بشری را متحول ساخت. سیستمهای دفاعی، طراحیهای استراتژیک، شبکه‌های اطلاعاتی همه و همه سخت تحت تأثیر این دگرگونیها قرار گرفتند. رهیافتهای نوین این جنگ، حوزه‌های درگیری و کشمکشهای، شیوه‌های تاکتیکی و عملیاتی رزمندگان این نوع جنگها، ادبیات وسیعی را در جهان شکل داده و در دسترس پژوهشگران قرار می‌دهد. مقاله حاضر به بررسی برخی از زوایای این نوع جنگ پرداخته و کوشیده‌است تا بعضی از ویژگیهای این نبرد و قلمروهای منازعاتی آن را به بحث بکشد.

*****

مقدمه

گسترش حوزه‌های تکنولوژیک در جهان در محورهای گوناگون عرصه تمدنی، بسیار چشمگیر و بارز است. تکنولوژیهای گوناگون همواره ادامه فعالیتهای اندام بشری

---

* دکتر رضا کلهر عضو هیأت علمی، محقق و پژوهشگر در زمینه مباحث شبکه‌های اطلاعاتی کامپیوتری و جنگهای شبکه‌ای است.

بوده‌اند. تکمیل پیچیدگیها و توانهای انسانی در عرصه‌های گوناگون، تکنولوژی را به وجود آورد، اما در اواخر قرن بیستم در این امر نیز تحولی برجسته رخ داد و نوعی تکنولوژی به جهانیان عرضه گردید که به جای تکمیل و تتمیم اندام بشری، دنباله ذهن و مغز انسانی بود؛ یعنی تکنولوژی اطلاعات*. ویژگیهای خاص این تکنولوژی آن را بر انواع تکنولوژیهای دیگر تفوق بخشید و آرام آرام در ظرف چندسالی، همه حوزه‌های فکری، فرهنگی و تمدنی انسان قرن بیستم را تحت‌الشعاع خود قرار داد.(۱)

بی‌شک یکی از این عرصه‌ها، عرصهٔ دفاعی ـ استراتژیک بوده‌است. تکنولوژی اطلاعات با ورود به این عرصه تحولات عظیمی را در آن به وجود آورد. ابعاد و زوایای تأثیر تکنولوژی اطلاعات بر سیستمهای دفاعی استراتژیک موضوع بحث و مقاله‌ای جداگانه است، اما در این مقاله بررسی شیوه‌های متفاوت چالش و مبارزه‌ای که تکنولوژی اطلاعات بسترساز اصلی آن بوده، موردنظراست.

بدون بحث از انقلاب اطلاعات** که در واقع نتیجه فرآیند تکنولوژی اطلاعات است ورود به این حوزه مقدور نیست. انقلاب اطلاعات چیست؟ ویژگیهای آن کدام است و پیامدهای آن بر حوزه‌های اطلاعات دفاعی و استراتژیک چه بوده‌است؟

انقلاب اطلاعات به مجموعه‌ای از دگرگونیهای اساسی در حوزه اطلاعات و اطلاع‌رسانی گفته می‌شود که سرعت فوق‌العاده، گستره وسیع و انتشار آزاد مطالب از مهمترین ویژگیهای آن است. سرعت فوق‌العاده پردازش اطلاعات و ایجاد ارتباطات منطقی میان میلیونها داده اطلاعاتی در گستره وسیع جهانی در حوزه‌های گوناگون سیاسی، اجتماعی، اقتصادی و فرهنگی و در دسترس قرار دادن آزاد این نوع اطلاعات از طریق شبکه‌های اطلاع‌رسانی جهانی موضوع ویژه‌ای را به نام انقلاب اطلاعات ایجاد کرده‌است. انقلاب اطلاعات با ارزش‌گذاری بر نفس اطلاعات به منزله یک سرمایه اصیل و ارزیابی تکنولوژیهای پردازش و گسترش، مجموعه‌ای از تواناییهای متفاوت را برای افراد، گروهها، سازمانها و واحدهای سیاسی ـ اقتصادی به وجود می‌آورد. این ویژگیها خود موجب به‌بار آوردن پیامدهای جدی در حوزه‌های متفاوت تفکر و تمدن بشری است. درحوزه‌های اطلاعات استراتژیک و دفاعی نیز این تأثیرات کاملاً چشمگیر است تا آنجا که گفته شده‌است: «انقلاب اطلاعات و نوآوریهای سازمانی مربوط، ماهیت جنگ و انواع ساختارهای نظامی، دکترینها و استراتژیهای مورد نیاز را تغییر

---

* Information Technology

** Information Revolution (IR).

می‌دهند.»[۲] از سوی دیگر گفته شده‌است که حتی انقلاب اطلاعات و پیشرفتهای کامپیوتری و تکنولوژیهای اطلاعاتی و ارتباطاتی تأثیر خود را بر نظریه‌های مدیریتی و سازمانی نیز به طور وسیع به جای گذاشته است.[۳]

انقلاب اطلاعاتی در حوزه‌های نظامی با عرضه ویژگیهای نوین خود موجب گردیده‌است که مهمترین بحث در این قلمرو، ورود بحث انقلاب اطلاعات درحوزه‌های دفاعی و نظامی باشد.[۴] فرآیندهای اطلاعاتی، سیستمهای متحول و پیچیده اطلاعات، تحولات نوین در نگرشهای اساسی به وجود آمده در حوزه اطلاعات، جنگ و ارزیابی استراتژیک و تصویر و ترسیم جنگهای آینده را کاملاً متحول کرده‌است.

بهره‌برداری از این ابزار نوین، ورود به عرصه‌ای جدید از جنگ میان ارتشهای مدرن و پست مدرن را با یکدیگر و با گروهها، سازمانها و افراد به وجود آورده‌است که امروز تحت عنوان "جنگ اطلاعاتی"* شناخته می‌شود. جنگ اطلاعاتی به نوعی «از جنگ اطلاق می‌شود که در آن هدف از بین بردن اطلاعات و سیستمهای اطلاعاتی دشمن با حفظ اطلاعات و سیستم اطلاعاتی خودی است.»[۵] و به طور دقیقتر گفته شده‌است که جنگ اطلاعاتی «مجموعه‌ای از عملیاتها برای دستیابی به برتری اطلاعاتی از رهگذر تخریب اطلاعات دشمن، فرآیندهای اطلاعات پایه‌ای، سیستمهای اطلاعاتی و شبکه‌های کامپیوتری در ضمن حفظ سیستم و فرآیندهای اطلاعاتی خودی است».[۶]

در این نوع جنگ متخصصان و کارشناسان برجسته سیستمهای اطلاعاتی و شبکه‌های کامپیوتری جنگجویان اصلی به شمار می‌آیند و سخت‌افزارها و شبکه‌های آنها میدانهای نبرد و پیکار هستند. جنگ‌افزارهای این نوع از جنگ، نرم‌افزارهایی هستند که از سوی این جنگجویان به کار گرفته می‌شوند و هرچه این نرم‌افزارها دقیقتر و کارآمدتر طراحی گردند، شلیک آنها به مجموعه اطلاعاتی دشمن دقیقتر و کارآمدتر است.

با وجود گسترده شدن این نوع جنگ در عرصه‌های مهم حیات بشری، باید گفت هنوز یک اجماع کلی دربارهٔ مفهوم آن شکل نگرفته است. مفسران و کارشناسان برجسته این نوع جنگ در تعریف و شمول آن آرای متفاوتی دارند. برخی معتقدند که جنگ اطلاعاتی را باید یک پدیده نوین گسترده تلقی کرد ـ یعنی یک راه‌حل سحرآمیز نوین برای جبران منابع کاهش یافته کنونی ـ و برخی دیگر با تعریف اینکه جنگ اطلاعاتی چیزی بیش‌ازتلاشهای جنگ الکترونیک سنتی نیست، آن را کم ارزش جلوه می‌دهند.[۷]

---

* Information Warfare

دیگرانی نیز هستند که به جنگ اطلاعاتی همچون تجسم نوین دیدگاههای قدیمی سون‌تزو در مورد تأثیرگذاری بر استراتژی دشمن، می‌نگرند.[۸] اما از این تفاوت و نگرشها در مفاهیم و تعاریف نمی‌توان چنین نتیجه گرفت که اندیشمندان این حوزه در قدر مشترکی از مفهوم جنگ اطلاعاتی هیچ دیدگاه نزدیک به یکدیگری ندارد؛ همگی پذیرفته‌اند که درک جنگ اطلاعاتی مستلزم آن است که ما به پیامدهای تعاریف متفاوت و معانی گوناگون خود اطلاعات، اهداف متفاوت برای به‌کارگیری جنگ اطلاعاتی، تأثیرات سطوح متفاوت و فازهای متنوع جنگ، مجموعه‌ای از بازیگران بالقوه (و دشمنان بالقوه)، که جنگ اطلاعاتی را به کار می‌گیرند و حوزه وسیعی از ارتباطات، فرماندهی، کنترل و اطلاعات، که به طور بالقوه از جنگ اطلاعاتی متأثر می‌شوند، بپردازیم.[۹]

درک فقرات پیش‌گفته، ارکان فهم جنگ اطلاعاتی را فراهم می‌آورد. به همین سبب باید دانست که جنگ اطلاعاتی دارای شمول آنچنانی است که تقسیم و مرزبندی موضوعات اصلی و اساسی آن بسیار مشکل می‌نماید.[۱۰] اما به طور کلی می‌توان گفت که امروزه در عرصه جهانی جنگ اطلاعاتی سه حوزه اصلی قابل بحث است که عبارت‌اند از: ۱) جنگ اطلاعاتی استراتژیک؛ ۲) جنگ اطلاعاتی دفاعی؛ و ۳) جنگ اطلاعاتی تروریستی.

جنگ اطلاعاتی استراتژیک

تعریف این نوع جنگ و ویژگیهای اصلی آن یکی از مهمترین مباحث مربوط به جنگ اطلاعاتی را رقم می‌زند. در چند دهه گذشته که شیوه‌های نبرد مستقیم با دشمن و استراتژیهای تصرف نشان‌دهندهٔ شکستها و پیروزیها بود، تحمل تلفات سنگین، واردآوردن آسیبهای جدی به سرمایه‌ها و تأسیسات حیاتی و... از عواملی بود که می‌توانست هر ارتشی را به زانو در آورد و ارتش دیگری را پیروزمند سازد. پس از آن ورود تسلیحات هسته‌ای به عرصه نبرد و بهره‌برداری از قدرت اتمی در یکسره ساختن سرنوشت هر جنگ، هرچند به صورت رسمی پیروزی به بار می‌آورد ولی تا مدتهای مدیدی سایه یک شکست سنگین اخلاقی و شریرانه را بر قدرت پیروز می‌انداخت. پناه‌بردن به بمبارانهای استراتژیک در جنگ جهانی دوم نیز کمتر از این شرمندگی جهانی نداشت و هرچند نمی‌توانست سرنوشت جنگها را به طور قاطع تعیین کند خسارتهای

جنبی فراوانی را وارد می‌ساخت که دیگر امروز در جهان از نظر سیاسی پذیرفته نیست. از سوی دیگر، ورود عرصه تکنولوژی اطلاعات به جنگها و پدیدار شدن نوعی جنگ اطلاعاتی استراتژیک که به «مجموعه‌ای از عملیاتهای اطلاعاتی و کامپیوتری اطلاق می‌شود و بدون واردکردن آسیبهای جدی انسانی، تأسیسات و شبکه‌های استراتژیک را از کار می‌اندازد و بلااستفاده می‌سازد» چهره جنگها تغییر کرد و بسیاری از پیامدهای آن را برای جنگنده‌های این میدان نبرد قابل تحمل ساخت. امریکاییها (که خود از پیشقراولان جنگهای اطلاعاتی استراتژیک هستند) در برابر این نوع جنگ با ابهامات جدّی روبه‌رو هستند و با وجود آنکه یکی از "شبکه شده‌ترین" کشورهای جهان می‌باشند، جنگ اطلاعات استراتژیک ابهامات فراوانی را در برابر استراتژیهای نظامی آنان ترسیم کرده‌است.(۱۱)

حوزه‌بندیهای جنگ اطلاعاتی استراتژیک

قلمروهای گوناگون، میدان نبردهای جنگ اطلاعات استراتژیک هستند.(۱۲) نخست باید مفهوم "اطلاعات استراتژیک" را تبیین کرد تا سپس با شناخت این حوزه اساسی، تقسیمات آن، به طور جزئی‌تر قابل بیان باشد.

در ادبیات استراتژیک جهان، تعاریف گوناگونی از اطلاعات استراتژیک وجود دارد. اما شاید بتوان به عنوان مهمترین تعریف، اطلاعاتی را استراتژیک تلقی کرد که به طور اساسی در اندازه توان یک کشور یا واحد سیاسی در حالت جنگ، صلح و بحران مؤثر باشد. این تعریف هرچند فراگیری کامل و صددرصدی از خود نشان نمی‌دهد ولی می‌تواند تا اندازه زیادی معرّف خود را توضیح دهد و تبیین کند. اطلاعات استراتژیک که به اطلاعات راهبردی نیز ترجمه گردیده است (و شاید این معادل‌گذاری بیشتر ریشه ترجمه‌ای داشته باشد) حوزه‌ای از اطلاعات را فرا می‌گیرد که در آن ضریب اهمیت هر موضوع در حالات گوناگون می‌تواند استراتژیک بودن آن موضوع را تعیین کند. لغت‌نامه جدید و بستر تعاریف ذیل را برای صفت استراتژیک پیشنهاد و ارائه می‌کند: «امری که دارای اهمیت فراوان در یک مجموعه یکپارچه است» و یا «در منابع قدرت سیاسی، نظامی یا اقتصادی دشمن چشمگیر باشد» استراتژیک نامیده می‌شود. در لغت‌نامه اکسفورد به نحو جالبتری این واژه تعریف گردیده‌است: "امر اساسی در جنگ" یا «چیزی که برای مختل کردن اقتصاد داخلی دشمن و تخریب روحیه او طراحی

شده‌است» موضوعی استراتژیک است.[۱۳]

با توجه به تعاریف گفته شده در مفهوم لغوی واژه استراتژی می‌توان دریافت که چرا اطلاعات استراتژیک بیشتر به اموری اطلاق می‌شود که به حوزه‌های امنیت ملی و حیاتی یک کشور ارتباط دارند. از این رو جنگ در حوزه‌های اطلاعات استراتژیک نیز اهمیتی صدچندان می‌یابد و مرزبندی و تعریف و تبیین این نوع جنگ ضرورتی غیرقابل انکار است. در گذشته جنگهای حوزه‌های غیرمتعارف مانند جنگهایی که با تسلیحات هسته‌ای، شیمیایی، بیولوژیک و غیرمتعارف صورت می‌گرفت جنگهای حوزه استراتژی تلقی می‌گردید ولی با ظهور تکنولوژیهای اطلاعاتی نوین نسل دوم، جنگهای اطلاعات و استراتژیک فقط آن حوزه از جنگها را دربرمی‌گیرد که موضوع مورد چالش؛ جنگ اطلاعات استراتژیک باشد.[۱۴] جنگ اطلاعات استراتژیک با تعریفهای گفته شده در باب ویژگان آن به به‌کارگیری ابزار و فنون موجود در انقلاب اطلاعات به منظور به مخاطره انداختن سرمایه‌ها و داراییهای پراهمیت اصلی یک کشور مانند بخشهای اصلی تأسیسات حیاتی ملی از قبیل حمل و نقل، انرژی و ارتباطات، اطلاق می‌گردد.[۱۵]

با این وصف می‌توان گفت که در واقع جنگ اطلاعات استراتژیک در دو حوزه عمده تواناییهای اقتصادی و صنعتی و حوزه‌های نظامی و دفاعی قابل طرح و بحث است. حوزه نخست شامل تمام امکانات و تسهیلات بخش غیررزمی می‌گردد که جنگ اطلاعات استراتژیک حتی در زمان صلح نیز می‌تواند آثار ویرانگر خود را بر آن برجای گذارد؛ و حوزه دوم در زمان جنگ و بحران ممکن است یک کشور را به نابودی و یا شکست در برابر دشمن وادار سازد.

تأثیر انقلاب اطلاعات در این نوع جنگ هم بسیار بسزا، و هم بسیار گسترده است و در این مقال مختصر جای بحث و بررسی این مقوله وجود ندارد ولی ذکر این نکته لازم است که چون جنگ اطلاعاتی اصولاً هم در حوزه اطلاعات فی‌نفسه و هم در حوزه سیستمها صورت می‌گیرد، تبیین جنگ اطلاعاتی استراتژیک می‌تواند در آن حوزه از تصمیم‌گیریهای استراتژیک نیز نقشی اساسی ایفا کند. به نظر می‌رسد که اگر خسارتهای مادی حاصل از جنگهای اطلاعات استراتژیک در سیستمهای اطلاعاتی مشهود باشد ولی آن حوزه غیرمشهودی که می‌تواند مورد بحث قرار گیرد موضوعات استراتژیک کلیدی و اصلی است که در تصمیم‌سازی نقش بسزایی بازی می‌کند؛ هرچند ادبیات این حوزه بسیار محدود و مختصر است ولی پرداختن به آن می‌تواند این بعد از مسائل

مربوط به جنگ اطلاعات استراتژیک را روشنتر کند.

شکل‌دهی تصمیم‌گیریها

یکی از مهمترین مباحث در جنگ اطلاعات استراتژیک، شکل‌دهی اذهان تصمیم‌گیرنده در امور استراتژیک است. این نوع از جنگهای اطلاعاتی استراتژیک جنگهایی است که هم صبغه تهاجمی دارد و هم صبغه تدافعی؛ در وجه تهاجمی آن سیستم جنگنده اطلاعات استراتژیک می‌کوشد تا با شکل‌دهی اذهان تصمیم‌گیرندگان در سیستم اطلاعاتی دشمن ضمن حفظ سیستم اطلاعاتی خودی و حفظ اذهان تصمیم‌گیرنده در شبکه اطلاعاتی خودی، دشمن را ناخواسته وادار به نوعی از تصمیم‌گیری کند که در پایان آسیب‌پذیریهای او افزایش یابد و بستر تهاجم اطلاعاتی و حتی تهاجم رزمی تاکتیکی را فراهم آورد. این نوع از دخالت در تصمیم‌سازیها از شبکه‌های اطلاعاتی رقبا و دشمنان به صورت باز و آزاد هنوز در همه سیستمهای اطلاع‌رسانی جهانی نشت نکرده‌است ولی بخشهای تئوریک و نظری درباب آن گاه‌گاهی در برخی از متون و ادبیات موجود به چشم می‌خورد.

به نظر نگارنده این سطور این بخش از جنگ اطلاعات استراتژیک مهمترین بخش آن است و در تهاجم فراگیر شبکه‌ای و هجوم اطلاعات انبوه، خطر شکل دهی اذهان تصمیم گیرندگان و دخالت دشمن در تصمیم‌سازیها بر اساس عنصر اطلاعات بسیار قابل توجه است. به همین سبب جایگاه این نوع جنگ را در شیوه‌های غیرمتقارن قرار داده و در تقسیم‌بندی میان تهدیدات و جنگهای متقارن آن را در عداد تهدیدات غیرمتقارن برشمرده‌اند. دلیل اصلی این امر در آن است که دخالت در تصمیم‌سازیها از طریق سیستمهای اطلاعاتی* و تخریب اطلاعات صحیح دشمن و جایگزین کردن آن با اطلاعات نادرست و ایجاد فریبهای اطلاعاتی** به منظور ساخت تصمیمات نادرست همه و همه می‌تواند همان اندازه که از سوی قدرتهای بزرگ صورت پذیرد به وسیله واحدهای کوچکتر نیز امکان‌پذیر باشد.(۱۶) اما برخی از قدرتها، به‌کارگیری آشکار جنگ اطلاعات استراتژیک را پیروزی بزرگ خود می‌دانند و به‌کارگیری فوری و کارآمد آن را برای پیروز شدن در جنگ به منظور جلوگیری از یک بحران بزرگتر با استفاده از تسلیحات هسته‌ای علیه ژاپن در جنگ جهانی دوم مقایسه می‌کنند.(۱۷) اگرچه آنها در

---

* Information Systems

** Intelligence deceptions

ادبیات بجا مانده از خود این نوع جنگ را در حوزه‌های پیش‌گفته اطلاعات استراتژیک به رخ می‌کشند ولی باید به یادداشت که غافلگیریهای استراتژیک* از فریبهای اصلی در اطلاعات استراتژیک و ارزیابیهای استراتژیک** ناشی می‌شود که حاصل جنگ اطلاعات استراتژیک موفق است. البته باید یادآور گردید که این نوع غافلگیرییها اکنون در حوزه جنگهای نامتقارن که زاییده جنگهای اطلاعاتی درجهان است، بسیار فراگیرتر، وسیع‌تر و کارآمدتر است، جای می‌گیرد.

جنگ اطلاعاتی دفاعی (۱)

جنگ آینده به هر شکل و به هر شیوه‌ای که رویارویی خاص قدرتها و یا بلوکها را تجلی بخشد از پایه جنگ اطلاعاتی بی‌بهره نیست و آنها همواره آن را به عنوان یکی از اساسیترین محورها در این صحنه ملحوظ خواهند کرد. جنگ اطلاعاتی که قواعد و شکلهای ویژه خود را دارد، از حوزه یک جنگ اختیاری خارج شده و آنچنان به طور وسیع دامنگیر سیستمهای اطلاعاتی جهان شده‌است که ورود در این کارزار،به امری الزامی و ناگزیر بدل گردیده است.(۱۸)

توانایی کشورها در ورود به این کارزار و ادامه حضور موفقیت‌آمیز در آن، در گرو وقوف کامل به شیوه‌های این جنگ نوین و پیامدهای استراتژیهای اطلاعاتی در آن است. تعریف این جنگ آن گونه که به صورت تقریباً یکپارچه مورد قبول همگان قرار گرفته، عبارت است از: "مجموعه‌ای از عملیات که برای دستیابی به برتری اطلاعات با تخریب اطلاعات دشمن، فرآیندهای اطلاعات پایه‌ای ، سیستمهای اطلاعاتی و شبکه‌های کامپیوتری در ضمن حفظ سیستم و فرآیندهای اطلاعات خودی صورت می‌پذیرد».(۱۹)

همان گونه که از این تعریف برمی‌آید، جنگ اطلاعاتی صرفاً محدود به دستیابی به اطلاعات دشمن نیست، بلکه تخریب سیستمهای اطلاعاتی و فرآیندهای پردازشی اطلاعات پایه‌ای از مهمترین ارکان این جنگ است. چون شبکه‌های اطلاعاتی کنونی در سیستمهای کامپیوتری به یکدیگر مربوط می‌شوند ، اکنون حفظ شبکه از ورود کاربرهای غیرمجاز و حضور آنها در شبکه‌های اطلاعاتی به یک معضل جدی در تکنولوژی اطلاعات و حفظ سیستمهای اطلاعاتی بدل گردیده است. این کاربرهای

---

* Strategic Surprising

** Strategic Assesment

غیرمجاز که امروز، در سیستمهای اطلاعاتی و کامپیوتری به "هکرها"* معروف‌اند به دو بخش عمده تقسیم می‌گردند؛ هکرهای آماتور و هکرهای حرفه‌ای.

هکرهای آماتور بنا به تعریف بیشتر به منظور بهره‌برداری در پی تهاجمات الکترونیک به سمت سیستمهای اطلاع‌رسانی و اطلاعاتی پنهان هستند و سعی می‌کنند تخریب سیستمها و فرآیندهای اطلاعاتی را هدف قرار دهند و کوشش دارند که به نحو پنهان دستیابی خود را به سیستمهای اطلاعاتی، محفوظ نگهدارند. آنها می‌کوشند تا با ورود به سیستمها و تخریب فعالیتهای اطلاعاتی دولتها و سیستمهای تجاری، اهداف منفعت‌طلبانه خود را پیگیری کنند. این اعمال در اصطلاح ویژه خود به "جرایم کامپیوتری و ارتباطاتی" معروف‌اند.(۲۰)

هکرهای حرفه‌ای، هم در انگیزه و هم در نوع فعالیتها با هکرهای آماتور تفاوت دارند. هکرهای حرفه‌ای که بیشتر در سیستمهای حکومتی یا گروهها و سازمانهای پنهان تعریف می‌شوند این نوع فعالیت را جنگ تلقی می‌کنند و در ارتکاب به آن، اهداف وسیعتر و بزرگتری را می‌بینند. این هکرها بجز دستیابی به اطلاعات و سیستمهای اطلاعاتی دشمن، علاقه وافری به نحوه سیستمهای پردازشی در مجموعه اطلاعات آشکار و پنهان دشمن دارند. حوزه فعالیت این نوع از هکرها اغلب موضوعات امنیتی و دفاعی را دربرمی‌گیرد.

در مرحله اول جنگ اطلاعاتی دفاعی دسترسی به اطلاعات تصمیم‌گیرندگان حوزه دفاع از طریق شبکه‌های اطلاعاتی پنهان صورت نمی‌گیرد. اصولاً دست یازیدن به جنگ اطلاعاتی خود در مرحله اول در سطح اطلاعات آشکار است که ایجاد ارتباط در آن حوزه، دستیابی به اطلاعات از طرق مختلف آن، نوعی غافلگیری استراتژیک پدید می‌آورد. سؤال جدی این است که آیا برای دستیابی به اطلاعات و سیستمهای اطلاعاتی تصمیم‌گیرندگان صرفاً دستیابی به اجزای اطلاعات کافی است. فرآیند اصلی پس از این دستیابی چیست؟ آیا شیوه‌های این دستیابی اطلاعاتی خود ایمن و از ردیابی مصون‌اند؟ آیا گروههای سیاسی و سازمانهای اطلاعاتی از طریق حضور در این فرآیند خود را در صحنه یک ریسک جدی قرار نمی‌دهند؟ سؤالاتی از این دست هرچند نسبت به این اقدام هشدار دهنده و تحریک‌کننده احتیاطهای چندجانبه است، از حلاوت دستیابی به اطلاعات بیشتر نیز نمی‌کاهد.

---

* Hackers

هکرهای فردی و سازمانی به منظور دستیابی به اطلاعات تصمیم‌گیرندگان از طریق شناسایی شبکه‌های اطلاعاتی پیوسته می‌کوشند تا مدار مصرف و تولید اطلاعاتی را کشف کنند. این مدار خود می‌تواند موجب کشف یک ارتباط سازمانی نیز شود و متغیرهای زیر را دراختیار هکرها قرار می‌دهد:

۱ـ نیازهای اطلاعاتی تصمیم‌گیرندگان؛

۲ـ شیوه‌های کشف دسترسی به رفع این نیازها؛

۳ـ ارتباط ارگانیک و سیستماتیک تولید، مصرف اطلاعاتی.

نیازهای اطلاعاتی تصمیم‌گیرندگان خود نشان از دلمشغولیهای آنان دارد و می‌تواند تا اندازه‌ای نشان‌دهندهٔ حوزهٔ فعالیتی آنها و علاقه‌مندیهایشان باشد. تصمیم‌گیرندگان به عنوان مصرف‌کنندگان اطلاعاتی می‌کوشند، مستقیم‌ترین اطلاعات مربوط به طرحها و جزئیات و تفصیلات آنها را در دست داشته باشند. اکنون که سیستمهای حفاظتی اطلاعات شبکه‌ای گسترش یافته است، این پدیده را به عنوان خطرناکترین مرحله کشف طرحهای سری مورد نظر قرار می‌دهند. اما ناگزیری از جمع‌آوریهای اطلاعاتی، همیشه آسیب‌پذیریهای متفاوتی را در سطوح گوناگون موجب می‌گردد.

سیر و سفرهای اطلاعاتی در شبکه‌ها و سیستمهای ارتباطی و جمع‌آوری اجزای اطلاعات، خود شیوه‌های وسیعتری را در منابع جهت رفع نیاز تصمیم‌گیرندگان دربرخواهد داشت. ردیابان این تصمیم‌گیرندگان علاقهٔ وافر دارند تا از طریق شیوه سیر و سفرهای اطلاعاتی در شبکه‌ها بتوانند نوع برآورد کردن نیازهای اطلاعاتی تصمیم‌گیرندگان را دریابند. این شیوه‌ها در حوزه‌های جنگ اطلاعاتی دفاعی چیست؟ تصمیم‌گیرندگان حوزه‌های دفاعی تا چه اندازه به شبکه‌های آشکار اطلاعات متوسل می‌شوند؟ آیا فریبهای اطلاعاتی در ایجاد ردپاهای مصنوعی بدیل نمی‌تواند از دسترسی به این شیوه‌ها بکاهد؟ چنین سؤالاتی هم جدّی‌اند و هم تاکنون درحوزه دفاع و امنیت در سیستمهای اطلاعاتی آشکار مورد بحث قرار گرفته‌اند. اما در اینجا پرداختن به این پرسشها مورد نظر نیست؛ بلکه هدف، ایجاد چارچوبی برای بحث در حوزه جنگ اطلاعاتی دفاعی است.[۲۱]

سومین متغیری که می‌تواند در شبکهٔ آشکار اطلاعاتی در اختیار هکرهای حرفه‌ای قرار گیرد کشف ارتباطات منطقی و سیستماتیک در مدار تولید، مصرف اطلاعاتی است. اصولاً ارزیابی اطلاعات خام در جمع‌آوریهای آشکار اطلاعاتی همواره از مهمترین

مراحل بوده‌است. در این مرحله هکر خود دیگر به تنهایی نمی‌تواند ارتباط سیستم تیک میان تولید و مصرف را براحتی پیش‌بینی و ارزیابی کند. بلکه هکر با دراختیار گذاشتن این ارتباط از بررسی‌کننده اطلاعات کمک می‌گیرد تا ارزیابی دقیقی را از این ارتباط به دست دهد. کشف ارتباط منطقی میان این اجزا در موارد اطلاعاتی هر چند که به ارزیابی اطلاعاتی جزئی‌تر بستگی تام دارد اما از دیگر مزایای وجود شبکه‌های آشکار نیز براحتی استفاده می‌کند. در حوزه دفاعی، مباحث مربوط به خریدهای تسلیحاتی، صنایع نظری، توان تجهیزاتی علاقه‌مندیهای مطالعاتی و بررسیهای تحقیقاتی می‌توانند مورد ارزیابی اطلاعات خام* قرار گیرند و به کشف سیستماتیک مدار مصرف، تولید تا اندازهٔ زیاد کمک کنند. گاه این هکرها در سطوح بالاتری قرار می‌گیرند به‌گونه‌ای که خود می‌توانند بجز یافتن شیوه‌هایی برای کسب اطلاعات نظیر اطلاعات جزئی‌تر، به کشف ارتباطات سیستماتیک نیز نایل شوند. این افراد را به جنگجویان حرفه‌ای کامپیوتری، یا سربازان مزدور کامپیوتری**، تعبیر می‌نمایند چه صرفاً به منظور دسترسی به پول بیشتر، تجربیات و تخصص خود را در اختیار سازمانها، دولتها و گروههای تروریستی قرار می‌دهند.(۲۲) این سربازان مزدور کامپیوتری که دارای تخصصهای گوناگون هستند با ایجاد یک شبکه تخصصی می‌توانند به یک سیستم ارزیابی نسبتاً دقیق تبدیل گردند. عمده این افراد از کنار گذاشته‌شدگان سیستمهای اطلاعاتی در جهان یا مؤسسات علمی هستند و بسیاری از آنها از متخصصان کامپیوتری در کشورهایی مانند روسیه، بلغارستان و... بوده‌اند که امتیازات ویژه خود را از دست داده‌اند.

محققان بررسیهای اطلاعاتی این افراد را از جمله افرادی به شمار می‌آورند که تهدیدی جدی برای امنیت ملی محسوب می‌شوند.(۲۳) عمق نفوذ این افراد و دسترسی آنها به اطلاعات تصمیم‌گیرندگان حوزه دفاع، حد و حصر معینی ندارد و به یک جنگ ذهنی اطلاعاتی وابسته است. از سوی دیگر، دستیابی به اطلاعات و تحلیل و ارزیابی تنها تهدیدی نیست که در حوزه دفاع در همان مرحله مذکور وجود داشته‌باشد. بلکه تخریب سیستمهای اطلاعاتی و اطلاعات تصمیم‌گیرندگان نیز از تهدیدهای جدید و جدّی به شمار می‌آید. کشف و سپس تخریب یک سیستم اطلاعاتی که پیوسته در حال جمع‌آوری و ارزیابی اطلاعات است امروزه به یک جنگ جدی مبدل گردیده است. این سربازان مزدور کامپیوتری خود پیشقراولان این نوع جنگ هستند. این جنگها که بیشتر

---

* Assessment of raw information ** Cyber - Mercenaries

در حوزه نرم‌افزاری مورد بررسی قرار می‌گیرند موضوعی را موسوم به "جنگ اطلاعاتی نرم‌افزاری"* به وجود آورده‌اند که خود مجالی دیگر را برای بحث می‌طلبند ولی در تعریف گفته شده‌است که این نوع جنگ، شامل فعالیتهایی است که جنگجویان اطلاعاتی برای هجوم یا نفوذ به شبکه‌های خاص اطلاعاتی به منظور تخریب سیستمها و کارکردهای نرم‌افزاری آنها انجام می‌دهند.(۲۴)

تهاجم به فرآیندهای اطلاعاتی و دفاع در برابر آن

"تهاجم به فرآیندهای اطلاعاتی پایه‌ای" یکی از تعاملهای صورت گرفته در جنگ اطلاعاتی دفاعی است. این فرآیندها را با ویژگیهایی که در جریانات اطلاعاتی پایه‌ای در هر حوزه‌ای توصیف می‌کنند، تعریف می‌نمایند. این ویژگیها به مبانی اطلاعات هر حوزه باز می‌گردد. اطلاعات پایه‌ای در هر حوزه، اطلاعاتی را دربر می‌گیرد که مبانی اطلاعات تحلیلی آن حوزه را شامل می‌شود. این مبانی در حوزه دفاعی بیشتر به اطلاعات پرسنلی، تجهیزات ، توان و امکانات دفاعی هر کشور مربوط می‌گردد. در منابع آشکار اطلاعاتی گاه می‌توان بسیاری از این مبانی را به صورت آشکار، و از برآیند برخوردهای این منابع به دست آورد. حضور در سیستمهای شبکه‌ای اطلاعات در مجموعه‌های دفاعی را از طریق هکرها و متخصصان رایانه‌ای که قبلاً ذکری از آنها به میان آمد، تأمین می‌کنند. تقریباً، همه سیستمهای اطلاعاتی شبکه‌ای در جهان در معرض این خطر عمده قرار دارند. بنا به گزارش ارائه شده از سوی گائو(۲۵)، شبکه‌های اطلاعاتی وزارت دفاع آمریکا در هر سال حدود دویست و پنجاه هزار بار از سوی هکرها و متخصصان گوناگون شبکه‌های جهانی مورد حمله قرار می‌گیرند.(۲۶) اهداف اطلاعاتی جنگجویان شبکه‌ای، غیر از دستیابی به اطلاعات یا تخریب سیستمها، به فرآیندهای اطلاعاتی پایه‌ای نیز تسرّی می‌یابد.

شبکه‌های موجود در سیستم دفاعی کشوری مانند آمریکا دربرگیرنده دو میلیون و یکصد هزار رایانه، و یکصد شبکه طویل‌الاتصال است که می‌تواند حوزه وسیعی را در اختیار نمایندگان و کشف کنندگان فرآیندهای اطلاعاتی پایه‌ای قرار دهد. این فرآیندها ارتباط دهندگان مستقیم و غیرمستقیم اجرا و ارکانی هستند که پایه تحلیل اطلاعات قرار می‌گیرند. کسب صحیح برآورد توان، بدون دستیابی به این فرآیندها امکان‌پذیر نیست.

---

* Software information warfare

این تهاجم، ابزار خاص خود و جنگ افزارهای متناسب با این مأموریت را می طلبد. در این میان نقش جنگ‌افزارهای نرم‌افزاری کاملاً مشهود است. طراحی نرم‌افزارهایی که می‌تواند فرآیندهای اطلاعاتی پایه‌ای را تجزیه و تحلیل کند، برتری استراتژیک کادر صحنه عملیاتی این جنگ را تضمین می‌کند. در نتیجه، پیروزی در این جنگ مدیون پیروزی در جنگ نرم‌افزارهای اطلاعاتی خواهد بود. جنگ نرم‌افزارها که طراحان و سیستمهای بزرگتر رایانه‌ای را به میدان مبارزه کشانیده‌است، تا آن حد پیچیده گردیده که هزینه‌های هنگفتی را بر سازمانهای به کارگیرنده سیستمهای رایانه‌ای تحمیل می‌کند (در بخش بعدی این بحث به آن اشاره خواهیم داشت). جنگ نرم‌افزارها که بیش از هر چیز حوزه فرآیندهای اطلاعاتی پایه‌ای را هدف قرار می‌دهد، در پی برنامه‌ریزی برای تخریب یا بهره‌برداریهای خاص از شبکه‌ها و اطلاعات پایه‌ای است که مجموعاً در دو مرحله خلاصه می‌شود؛[۲۷] بهره‌برداریهای ویژه[۲۸] وتخریب سیستمهای نرم‌افزاری. امروزه نفوذ در سیستمهای شبکه‌ای جهان، بیشترین عامل تخریب هر شبکه را تشکیل می‌دهد. دارندگان واژه‌های عبور در سیستمها، گاه خود مخرب‌ترین عناصر هستند. در انگلستان اغلب فعالیتهای مربوط به این حوزه پس از بررسیهای فراوان به افرادی منتهی گردیده‌است که‌به‌نحوی از کاربرهای خاص یک شبکه بوده‌اند، و یا از طریق دیگر می‌توانستند با یک کاربر خاص ارتباط برقرار کنند.

در هر حال در جنگ نرم‌افزاری، همه نیروهای این نرم‌افزارها هستند؛ و طراحی نرم‌افزارهای پیچیده متناسب با برد جنگهای ذهنی متخصصان رایانه‌ای و حافظان سیستمهای شبکه‌ای است. این جنگ به صورت فعال تازه آغاز گردیده است.

در حوزهٔ دفاع در برابر یورشهای اطلاعاتی نیز پیشرفتهای چشمگیری انجام شده‌است. تعداد حمله‌های رایانه‌ای، و نقش هکرها و متخصصان مزدور این جنگ، استفاده کنندگان از شبکه‌ها در حوزه‌های مختلف اقتصادی، سیاسی و بویژه امنیتی و دفاعی را هم به دفاع در برابر این یورشها کشانیده است. برخی از کارشناسان، استراتژیهای بهینه را در هر حوزه‌ای از جنگ اطلاعاتی (بویژه دفاع اطلاعاتی)، مبتنی بر عملیات رقیب دانسته‌اند. ولی در حوزهٔ دفاع در برابر یورشهای اطلاعاتی، شاید نتوان این دفاع را بر عملیات رقیب بنا کرد. اصولاً غافلگیریهای استراتژیک از این حوزه‌ها آغاز می‌گردند. مبتکران سیستمهای اطلاعاتی، برای پرهیز از غافلگیریهای استراتژیک در هر حوزه‌ای از اطلاعات، دانش را سرآغاز ابتکار عمل می‌دانند، و اطلاع از استراتژی رقیب

و دشمن را از این مرحله، دفاع بهینه می‌خوانند و این حوزه نیز از عملیات اطلاعاتی مستثنی نیست.

در حوزه تاکتیکها "دفاع در برابر یورشهای اطلاعاتی" نیز متنوع گردیده است. فریبهای اطلاعاتی در سیستمهای آشکار در اشکال گوناگون و با ویژگیهای متنوع آن، یکی از مهمترین تاکتیکها در حوزه دفاع در برابر یورشهای اطلاعاتی شده است. ایجاد فرآیندهای اطلاعاتی بدیل، ارائه اطلاعات باز و متغیر در سیستمها، اتکا به روشهای غیر تکراری در صحنه‌های پردازش اطلاعاتی در هر دو میدان، "یورش و اطلاعات تصمیم گیرندگان" و "یورش به شبکه‌های اطلاعاتی پایه‌ای"، امروز به کار گرفته می‌شود.

گروههای تروریستی و سازمانهای اطلاعاتی در یورشهایشان گاهی در دام ضد حمله‌های شبکه‌ای قرار گرفته، و مورد تخریب و دستیابی به سیستمهای حفاظتی اطلاعاتی در شبکه‌ها قرار می‌گیرند.[۲۹] گذشته از آن، حفاظت از اطلاعات را در "دو مرحله" تخریب و بهره‌برداری تا آن اندازه گسترش داده‌اند که امروزه هکرها و متخصصهای جنگهای شبکه‌ای نیز از بیم آسیب‌پذیری، بسیار محتاطانه عمل می‌کنند. از سوی دیگر، بهره‌برداری از روشهای آنالیز اطلاعاتی، و ارزیابی آنها موجب شده‌است که محافظان اطلاعات شبکه‌ای دست به اقدامات نوینی بزنند و اطلاعات را به گونه‌ای در شبکه قرار دهند که نتیجه ارزیابی آنها، دشمن را در یک فریب اطلاعاتی پیچیده قرار دهد. در پایان این بحث یادآور می‌شویم که گستردگی این جنگ، نوین بودن روشهای آن، و آسیب‌پذیری وسیع کشورها و سازمانهای اطلاعاتی را باید نتیجه فرآیند انقلاب اطلاعات و تحول فن‌آوری اطلاعاتیی دانست که ناچار همه را دربرگرفته‌است، و در آینده‌ای نزدیک پیامدهای خاص خود را بروز خواهد داد. از هم اکنون کارشناسان سیستمهای امنیتی و دفاعی باید شیپور این جنگ را بشنوند، و در تربیت نیروی خودی و به‌کارگرفتن‌امکانات پیش‌دستی کنند؛ چرا که هرگونه غفلتی سرچشمه شکستی سنگین‌است.

جنگ اطلاعاتی تروریستی*

یکی از پردامنه‌ترین جنگهای اطلاعاتی کنونی، جنگی است که گروهها و سازمانهای تروریستی با استفاده از جنگ‌افزارهای شبکه‌ای و اطلاعاتی مدرن انجام می‌دهند. بهره‌برداری از شبکه‌های اطلاعاتی آشکار که امروزه به بهترین وسائل ارتباطی نیز مبدل

* Terroristic Information Warfare

گردیده‌اند، نیازهای تروریستها را هم در ایجاد ارتباطات برآورده می‌سازند و هم زمینه‌های جمع آوری اطلاعاتی را برای آنها فراهم می‌سازند.[۳۰] ترسیم چگونگی رخداد این جنگ و مبارزات فکری و ذهنی جنگجویان اطلاعاتی و تک‌ها و پاتک‌های اطلاعاتی شبکه‌ای به مبحث بسیار مهمی در این حوزه تبدیل گردیده‌است که به احتمال بسیار زیاد دامنه شعله‌های آن در آینده‌ای نه چندان دور کشور ما را نیز دربرخواهد گرفت. پرداختن به چنین مقوله‌ای و ایجاد بسترهای پیشگیری و شناسایی این نوع رزم می‌تواند آینده موفقیت‌آمیز را از چنگالهای تروریستهای اطلاعاتی خارج سازد.

بنا به تعریف، جنگ اطلاعاتی تروریستی «نوعی جنگ است که در آن تروریستها تواناییهای سیستمهای اطلاعاتی شبکه‌ای را در تحقق اهداف تروریستی به کار می‌گیرند».

این نوع جنگ به سبب نوآوریهای اطلاعاتی* روزافزون بشدت متنوع می‌گردد و هر روز حوزه‌ها و دامنه‌های وسیع و گسترده‌ای را برای خود می‌یابد که پرداختن به مهمترین این قلمروها را، حایز اهمیت می‌دانیم.

در مرحله اول ارائه تعریفی از تروریسم اطلاعاتی در این مقوله بسیار مهم است، زیرا طبقه‌بندی گروهها یا سازمانها در این مقوله متناسب با تعریف تروریسم اطلاعاتی صورت خواهدگرفت. تروریسم اطلاعاتی «نوعی تروریسم است که در آن جنگ‌افزارهای اطلاعاتی شبکه‌ای به عنوان جنگ‌افزارهای تروریستی و تواناییهای سیستمهای اطلاع‌رسانی به عنوان قابلیتهای فزاینده میدان این عملیات تروریستی تلقی می‌گردند». تروریسم اطلاعاتی با هدف انجام فعالیتهای تروریستی در حوزه اطلاعات صورت می‌پذیرد که دو عامل جنگ‌افزار و محیط جنگ اطلاعاتی مهمترین پارامترهای موفقیت یا عدم موفقیت در آن محسوب می‌گردند.

عامل نخست، یعنی جنگ‌افزارهای تروریسم اطلاعاتی در شبکه‌ها امروزه به نرم‌افزارهای خاص این جنگ و شیوه‌های به‌کارگیری تعامل سیستمی در آن مربوط می‌شود. نرم‌افزارهای خاص در این حوزه نقش جنگ‌افزارهایی را برعهده دارند که سرعت و دقت عمل آنها دقیقاً بسان پارامترهای مثبت یک جنگ‌افزار در میدان نبرد در جهت ایجاد موفقیت در این جنگ، حایز اهمیت است. این نرم‌افزارها باید توانایی تعامل با سیستمهای مختلف اطلاعاتی در شبکه‌های اطلاع‌رسانی را از خود نشان دهند تا بتوانند با همسازگاریهای سیستمی به آسانی درون سیستمهای گوناگون اطلاعاتی

---

* Intelligence Innovations

دستگاههای مختلف آشکار و پنهان وارد شوند و دست‌کاریهای اطلاعاتی خود را انجام دهند. این نرم‌افزارها گاه پس از سالها کوشش و فعالیت یک گروه یا یک فرد تهیه می‌شوند و میدان نبرد اطلاعاتی را تحول می‌بخشند.

عامل دوم، تواناییهای سیستمهای اطلاعاتی است که به هر اندازه که وسیعتر و گسترده‌تر باشند و بتوانند نیازهای مختلف یک سیستم را برآورده سازند می‌توانند زمینه‌های مثبت‌تری را برای فعالیت نرم‌افزارهای خاص ایجاد کنند. قابلیتهای سیستمی هر شبکه اطلاعاتی به همان اندازه که قدرت مانور به‌کارگیرندگان آن را افزایش می‌دهد، زمینه ورود و دست‌کاریهای هکرهای حرفه‌ای را نیز فراهم می‌سازد. در جنگ اطلاعاتی تروریستی، سازمانها یا گروههای تروریستی با شناسایی زوایای پنهان و آشکار این قابلیتها، آنها را به نفع خود به کار می‌گیرند. به همین سبب امروزه سیستمهای اطلاعاتی که از شبکه‌های اطلاعات بهره‌برداریهای وسیع می‌کنند، می‌کوشند تا با روشهای مختلف این شبکه‌ها را ایمن سازند و قابلیتها را فقط در اختیار عاملان خود قرار دهند ولی نسبتِ موفقیت آنها تا اندازه زیادی قابل تأمل است.

شیوه‌های جنگ اطلاعاتی تروریستی

روشهای جنگ اطلاعاتی تروریستی متنوع و گوناگون است. اما مهمترین این شیوه‌ها را در دو مقوله نفوذ* و تخریب** طبقه‌بندی کرده‌اند.(۳۱) نفوذیافتن در سیستمهای اطلاعاتی رقبا یا دشمنان همواره مدنظر سیستمهای اطلاعاتی بوده‌است. اما امروزه این امر مطلوب نظر تروریستهای اطلاعاتی نیز هست. نفوذیافتن در شبکه‌های اطلاعاتی هدف به منظور دستیابی به اجزا و ارکان اطلاعات طبقه‌بندی شده، نخست از طریق همین شبکه‌های آشکار و سپس از طریق شبکه‌های بسته کامپیوتری و از طریق فضای کامپیوتری*** هدف صورت می‌پذیرد. تروریسم کامپیوتری**** پس از دستیابی به اطلاعات و حتی دانسته‌های خام اطلاعاتی، آنها را در بوته ارزیابی و تحلیل قرار می‌دهد و پس از طی فرآیند تحلیل***** به اطلاعاتی بدل می‌کند که شاید به دست آوردن آنها از طریق پنهان مستلزم هزینه‌های سنگین‌تری می‌بود. وجود انبوهه اطلاعات روی

---

* Penetrating
** Disrupting
*** Syber Space
**** Syber Terrorism
***** Analysis Processos

شبکه‌های آشکار از مزایای قابلیتی هر سیستم اطلاع‌رسانی است ولی همین مزیت خود در رهنمون ساختن تروریستها در به دست آوردن سرنخهای اصلی یک موضوع کاملاً نقش کلیدی دارد و به قول یکی از نویسندگان «برخی از مردم درپی‌یافتن کارتهای مسابقه بیس بال هستند و برخی دیگر قراردادها و پروتکلها را به دقت ارزیابی می‌کنند».[۳۲] هرچند که گاه اطلاعات ذی‌قیمتی را نیز می‌توان روی شبکه‌های اطلاعاتی براحتی به دست آورد؛ برای نمونه، در سوم سپتامبر سال ۱۹۹۸، انجمن کارخانه‌داران شیمیایی نتیجه مطالعه‌ای را افشا کرد مبنی بر اینکه یک سازمان حفظ محیط زیست، شبکه اینترنت را برای انتشار اطلاعات بسیار حساس و مفصل در مورد دهها هزار امکانات صنعتی مورد استفاده قرار داده‌است که خطر یورشهای تروریستی در ایالات متحده را به صورت چشمگیری افزایش می‌داد».[۳۳] این گزارش بخوبی نشان می‌دهد که تروریستها براحتی می‌توانند امکانات و تأسیسات صنعتی یک کشور را با مشخصات و حساسیتهای آنها به آسانی روی شبکه‌های اطلاع‌رسانی جهان بیابند و آنها را مورد هدف قرار دهند. گذشته از بهره‌برداریهای آشکار از سیستمهای اطلاع‌رسانی باز جهانی، یورشهای تروریستی به شبکه‌های بسته سازمانی نیز افزایش چشمگیری داشته‌است. سازمان سیستمهای اطلاعات دفاعی امریکا بر این باور است که در یک ارزیابی به عمل آمده در سال ۱۹۹۹، از ده‌هزار یورش صورت گرفته به کامپیوترهای شبکه (DoD) امریکا، حدود ۸۰٪ موفقیت‌آمیز بوده و تنها ۵٪ از آنها فاش گردیده‌اند[۳۴] و جالب اینکه این تنها تهاجماتی را برمی‌شمرد که به قصد نفوذ و به دست آوردن اطلاعات صورت می‌پذیرد. واقعیت آن است که در این فرآیند علت اساسی آسیب‌پذیری سیستمی*، وجود انبوهه‌های اطلاعاتی است که قبلاً به هرحال برای تروریستها دستیابی به آنها مقدور نبوده ولی اکنون با یک دسترسی آسان می‌توان بسیاری از اطلاعات پنهان را نیز به نحوی در دسترس قرار داد.

هرچند که شیوه‌های نفوذ در سیستمهای اطلاعاتی از طریق فضای کامپیوتری نیز خود متنوع است ولی باید دانست که اهداف و مقاصد تروریستها، به سبب آنکه نوع هدف آنها سیاسی است از اهداف و مقاصد دیگر گروهها و افراد متفاوت است. فعالیتهای جنایی، سرقتی و... نیز امروزه ازطریق فضای کامپیوتری صورت می‌گیرد ولی اهداف تروریستی با ترکیبی از مقاصد سیاسی و شیوه‌های ویژه سازمانی از دیگر

* Systematic Vulnerabilities

اهداف، متمایز می‌گردد.

مقوله دوم، تخریب است. تخریب یکی از اهداف تروریستها در دسترسی به شبکه‌های اطلاعاتی است. حرکت با هدف تخریب هم از مسیر شبکه‌های اطلاعاتی آشکار و هم از مسیر شبکه‌های بسته و پنهان هر دو صورت می‌پذیرد. تخریب سیستمهای اطلاعاتی با روشهای کامپیوتری خاص در فضای کامپیوتری یک سازمان می‌تواند برای مدتها یک فرآیند پیچیده را مختل سازد. این امر فقط مختص تروریستها نیست بلکه بسیاری از هکرهای حرفه‌ای نیز با ورود به تخریب سیستمهای اطلاع‌رسانی و گاه سیستمهای بسته اطلاعاتی به مقاصد و اهداف بزرگی دست می‌یابند. یک نمونه از موارد غیرتروریستی، ورود یک جوان روسی به نام ولادیمیر لوین* با استفاده از کدهای پیچیده عبور برای دسترسی به شبکه مدیریت کامپیوتری مالی سیتی کرپس نیویورک بود که در نتیجه توانست ۱۲ میلیون دلار را از طریق این دسترسی به حساب خود در یک بانک دیگر واریز کند. هرچند او در این کوشش چهل بار رمزهای عبور مختلف و پیچیده را آزمود ولی موفقیت او درنتیجه پیگیریهای FBI با دستگیریش متوقف ماند.(۳۵) آنچه مهم است اینکه لوین توانست با تستهای مکرر ورود خود را به یک سیستم بسته اطلاعاتی میسر سازد. بعدها لوین فاش ساخت که پس از دسترسی به شبکه سیتی کرپس با تخریب برخی از پلهای ارتباطی و تعریف پلهای جدید توانسته است که این مبلغ پول را به حساب خود واریز کند. در موارد استفاده تروریستی نیز تخریب سیستم می‌تواند توانایی تخلیه و گاهی ضربه به یک سیستم را کاملاً مقدور سازد. در یکی از مفصلترین گزارشهای وزارت دفاع آمریکا آمده است که: «حملات صورت گرفته به سیستمهای کامپیوتری این سازمان تخریبهای عمده و قابل توجهی به بار آورده‌است، تهاجم‌کنندگان، هم اطلاعات و هم نرم‌افزارها را به سرقت برده و یا تخریب کرده‌اند. آنها با نصب کردن فایلهای غیرمطلوب و ایجاد "راههای پنهانی"** از چنگالهای سیستمهای عادی مراقبتی می‌گریزند و این فایلها به آنها اجازه می‌دهد که در آینده به طور غیرمجاز به سیستم دسترسی داشته باشند».(۳۶) یک نمونه از این نوع حملات تروریستی به سیستمهای اطلاعاتی، مورد "آزمایشگاه رُم"*** است. این آزمایشگاه که متعلق به نیروی هوایی امریکا بود و در مرکز فرماندهی و کنترل قرار داشت طی ماههای آوریل و

---

* Vladimir Levin

** Back doors

*** ROME LABORATORY

مارس ۱۹۹۴ از سوی دو مهاجم اطلاعاتی ـ یک نفر انگلیسی و یک فرد ناشناخته ـ مورد تهاجم کامپیوتری قرار گرفت. آنها توانستند تا کنترل سیستمهای پشتیبانی "رُم" را برای چند روز مختل کنند و ارتباط جدیدی را با سایتهای اینترنتی خارجی از این آزمایشگاه برقرار سازند. تخریب سیستم گذشته و ایجاد پلهای ارتباطی جدید آنها را قادر ساخت کپی اطلاعات حساسی را از قبیل اطلاعات مربوط به (Air Tasking Order 2) کنند و به آورند.[۳۷] نیروی هوایی امریکا خسارات ناشی از این تخریب سیستمی و به دست ۵۰۰ آوردن اطلاعات حساس را بیش از ۰۰۰ بخوبی دلار برآورد کرد. نمونه‌های ارائه شده نشان می‌دهد که چگونه یک گروه تروریستی با مقاصد خاص خود می‌تواند با تخریب اطلاعاتی نرم‌افزاری و یا تخریب داده‌ها و ایجاد پلهای ارتباطی نوین به اطلاعات ارزشمند دست یابد و یا سیستم اطلاعاتی هدف را برای مدتها مختل ساخته و دچار خسارت کند.

حوزه‌های جنگ اطلاعاتی تروریستی

گذشته از اینکه این حوزه‌های نبرد خود چهره‌های بسیار متنوعی دارند، دامنه‌های فراگیری آنها نیز بسرعت رشد یافته و متناسب با تحولات تکنولوژیک در عرصه‌های گوناگون فضا و زمین، از تنوعات بسیار بهره‌مند گردیده‌است. تروریستهای شرکت‌کننده در جنگهای اطلاعاتی از شیوه‌های گوناگون جنگهای اطلاعاتی به نحوی سود می‌جویند که سطح آسیب‌رسانی را در هر حوزه استراتژیک بالا می‌برند و میدانهای اصلی جنگهای اطلاعاتی را پیروزمندانه فتح می‌کنند.

جنگ تروریستی در فضای کامپیوتری وابستگی تامّی به گسترش این فضا و ارائه سرویس‌دهیهای شبکه‌ای در سیستمهای مدیریتی نظامی و غیرنظامی دارد. به همین سبب شاید به نحوی بتوان مهمترین حوزه‌های نبرد و درگیری جنگهای اطلاعاتی را در سه حوزه اصلی نظامیگری، اطلاعاتی و اقتصادی دسته‌بندی کرد.

جنگ اطلاعاتی در حوزه نظامی

جنگ اطلاعاتی تروریستی در حوزه‌های نظامی را باید در زمینه‌های نفوذ و تخریب در سیستمهای نظامی بررسی کرد. از آنجا که امروزه فضای مدیریت استراتژیک در حوزه نظامی را با پنج رکن فرماندهی، کنترل، ارتباطات، کامپیوتر و اطلاعات[۳۸] ترسیم

می‌کنند، این فضا به نحو بسیار مناسبی به سبب وابستگی بسیار زیادش به شبکه‌های کامپیوتری از یک‌سو، و اهمیت اطلاعات در این رکنها از سوی دیگر، آسیب‌پذیریهای جدّی خود را در برابر یورشهای تروریستهای اطلاعاتی نشان می‌دهد. موفقیت در صحنه اجرای این نوع فرماندهی به مثابه موفقیت در یک میدان نبرد تلقی خواهد شد. نظر به اینکه دارا بودن یک شبکه مناسب اطلاعاتی می‌تواند در حداقل زمان ممکن حداکثر ارتباطات را برقرار، و بالاترین حجم اطلاعات را در امور ارتباطی متبادل سازد، اهمیت این رکن در میان ارکان دیگر را می‌توان با نقش سیستمهای عصبی و ارتباطی آنها با سیستم دفاعی بدن تشبیه کرد.(۳۹)

تروریستهای فعال در جنگ اطلاعاتی که به این نوع جنگ به منزله یک جنگ اصیل و واقعی می‌نگرند، به سبب قلّت نیرو و امکانات محدود خود در پی بهره‌برداریهای حداکثر از آسیب‌پذیریهای این فضای مدیریتی و فرماندهی خواهندبود.

تروریستهای اطلاعاتی در تبادر به جنگ اطلاعاتی تروریستی، آنچه را که در یک نظام اطلاعاتی از اهمیت خاص بهره‌مند است، با دست یازیدن به نفوذ به دست می‌آورند و تا حداکثر بهره‌برداری از آن پیش می‌روند و سپس به تخریب و از بین بردن آن می‌پردازند. برخی از کارشناسان امور اطلاعاتی، شیوه‌های به‌کارگیری جنگ اطلاعاتی را برای تروریستهای اطلاعاتی در سه مقوله تعریف کرده‌اند: مقوله نخست، به‌کاربردن شیوه‌های نوین در حوزه فعالیتهای قدیمی؛ مقوله دوم به‌کاربردن شیوه‌های قدیمی در حوزه فعالیتهای جدید؛ سرانجام مقوله سوم به‌کارگیری شیوه‌های نوین در عرصه فعالیتهای و کنش و واکنشهای جدید است.(۴۰) مفهوم به‌کارگیری شیوه‌های نوین در عرصه فعالیتهای جدید و قدیم، به‌کارگیری همان روشهایی است که در برخوردهای اطلاعاتی درچارچوبهای مفهومی قدیم و جدید مطرح است. جمع‌آوری اطلاعاتی با سرقتهای اقتصادی و ایجاد ارتباطات وسیع و استفاده از این نوع ابزار برای جنگهای روانی و تبلیغاتی را امروزه در مقوله اول و به مثابه روشهای نوین در حوزه جنگهای اطلاعاتی طبقه‌بندی می‌کنند. استفاده تروریستهای اطلاعاتی از شبکه‌های اطلاعاتی در حوزه آسیب‌رسانی فیزیکی به سیستمها، در مقوله دوم یعنی به‌کاربردن روشهای قدیمی در حوزه فعالیتهای جدید طبقه‌بندی می‌شوند. اما مهمتر از همه دست یازیدن به جنگ اطلاعاتی تروریستی در حوزه نظامی به شیوه مندرج در مقوله سوم یعنی به‌کارگیری شیوه‌های نوین در عرصه فعالیتهای جدید است. بی‌شک این حوزه تناسبی وثیق با

موضوع انقلاب در امور نظامی[۴۱] دارد که خود جای بحث موسّع را می‌طلبد.

در مقوله سوم می‌توان از به‌کارگیری فنون و روشهای دیجیتالی علیه فعالیتهای اطلاعاتی یک هدف نام برد. حوزه نظامیگری، که در آن اعمال فرماندهی و کنترل نسبت خاصی با ارتباطات و اطلاعات پیدا کرده‌است، به همان اندازه که این ارتباط را می‌توان مغتنم شمرد باید آن را به عنوان یک آسیب‌پذیری جدی در مقابل روشهای تروریستی اطلاعاتی تلقی کرد. گروهها و یا افراد تروریست، که از شبکه‌ها به عنوان کانالهای ورود و خروج استفاده می‌کنند، در مرحله نفوذ به سیستمهای نظامی و آسیب‌رسانی به آنها اهداف ذیل را پیگیری و ارزیابی می‌کنند:

الف) بررسی و برآورد توان اطلاعاتی درطرح‌ریزیها وارزیابی اطلاعات استراتژیک؛

ب) بررسی وبرآورد تواناجرایی درحفظ ومراقبت‌ازتأسیسات وسیستمهای خودی؛

ج) بررسی و برآورد توان تهاجمی در اجرای ضربات مهلک بر دشمن؛

د) بررسی وبرآورد توانارتباطی درایجادشبکه‌های‌مناسب‌ارتباطی درحال جنگ وصلح.

تروریستهای اطلاعاتی در جنگ خود پس از بررسی مناسب و برآوردهای گوناگون مورد نیاز که ناشی از یک عملیات نفوذ موفقیت‌آمیز است درصدد بهره‌برداری از این بررسیها برمی‌آیند و با تمسک به روشهای تخلیه اطلاعاتی تا آنجا که ممکن است حوزه‌های نفوذ خود را گسترش می‌دهند. این مرحله خود ضربه اساسی بر پیکره هر سیستم نظامی وارد می‌کند و در صورت استمرار نفوذ در این حوزه، می‌تواند به مرحله تخریب سیستمی بینجامد. تروریستها در مرحله "الف"، به آسیب‌رسانی به شبکه‌های اطلاعاتی و سیستمهای اطلاعات نظامی مبادرت می‌ورزند. وارد کردن اطلاعات نادرست، قرارگرفتن بر سرپلهای اطلاعاتی شبکه‌ای، تخلیه اطلاعات و به دست آوردن نشانیها و آدرسهای ارتباطی می‌تواند سیستمهای عملیاتی آنها را در یک فرصت مناسب در یک پوشش و غافلگیری استراتژیک قرار دهد که ضربه‌زنی بر یک سیستم و یا تأسیسات حیاتی با تلفاتی بسیار پایین در صحنه عملیات نظامی از پیامدهای مهم آن است. در مرحله "ج"، سازمان یا فرد نفوذکننده با داشتن برآوردی از توان تهاجمی و در اختیارگذاری این توان به دشمنان و یا بررسی و ارزیابی عملیات تهاجمی مناسب علیه این تسهیلات و امکانات می‌تواند در جنگ چریکی خرابکارانه یا یک عملیات تیمی موفقیت‌آمیز ضربه را برجایی وارد سازد که با کمترین تلفات، مفاصل استراتژیک هر سیستم نظامی را از یکدیگر جدا کند.

درمرحله "د"، تروریستهای اطلاعاتی درجنگ خود با شناسایی ارتباطی و طبقه‌بندی آنها ازنظر استراتژیک و ضریب آسیب‌پذیرییها به نوعی ارزیابی از توان ارتباطی در یک سیستم نظامی دست پیدا می‌کنند و می‌توانند این توان را درحین انجام عملیاتهای نظامی، رزم منطقه‌ای، مانورها و... محک بزنند. تروریستهای اطلاعاتی در مرحله نفوذ با واردشدن در این شبکه‌ها در مناطق خاصی از این شبکه‌ها کمین می‌کنند و در فرصتهای مناسب و با استفاده از زمانهای غافلگیرکننده به وسیله ایجاد ارتباطهای ساختگی، قطع ارتباطات کلیدی و مهم و تعریف چارچوبهای اطلاعاتی جدید به نحوی غافلگیرکننده ضربات اساسی خود را وارد می‌آورند. انجام مجموعه‌ای عملیات شبکه‌ای و گسترده از زمانهای بسیار پیش از انجام عملیاتهای نظامی، فرصتی را به وجود می‌آورد که از رهگذر آن تروریستهای اطلاعاتی یک جنگ شبکه‌ای* منظم را سامان و سازمان می‌دهند. ارزیابی مدوم توان ارتباطی و شناخت تواناییهای ارتباطی شبکه‌ای و ایجاد یک بستر مناسب برای آسیب‌رسانی بموقع به این شبکه و در عین حال حضور و ورود به صحنه و میدان این ارتباطات می‌تواند به گونه‌ای مؤثر، تأثیر ضربات وارده را دوچندان سازد.

جنگ اطلاعاتی تروریستی در حوزهٔ اطلاعات

اما آنچه واقعاً تروریسم اطلاعاتی** خوانده می‌شود، مجموعه‌ای از تلاشهای درون شبکه‌های اطلاعاتی جهان است که از این تسهیلات، شبکه‌های آسیب‌رسانی به سیستمهای اطلاعاتی دشمنان یا حریفان فراهم می‌آید. اما این تروریسم در حوزه اطلاعات به چه معنی است؟ با تحلیلی از وضعیت اطلاعات روی شبکه‌های جهانی اطلاعاتی و همین‌طور شبکه‌های منطقه‌ای ارکان ذیل‌الذکر برای هر شبکه اطلاعاتی قابل ذکر است:

۱)وجود اطلاعات پایه‌ای و مبنایی از هر حوزه؛

۲) وجود امکان پردازشهای آشکار اطلاعات؛ و

۳) دسترسی سهل و آسان به سیستمهای اطلاعاتی.

تروریستهای اطلاعاتی که در حوزه اطلاعات به جنگ می‌پردازند از هریک از این ویژگیها بهره‌برداری می‌کنند و یک سیستم را مورد حمله قرار می‌دهند. به طور مثال، در مرحله نخست، یعنی اطلاعات پایه‌ای و مبنایی از هر حوزه، تروریستهای اطلاعاتی می‌کوشند تا با دسترسی به این نوع از اطلاعات از توان اطلاعاتی دشمن یا حریف آگاه

---

* Netwar

** Intelligence Terrorism

شوند و بتوانند ارزیابی صحیحی از وضعیت استراتژیک دشمن به دست آوردند. قبلاً نیز گفته شد که دسترسی به این مرحله از اطلاعات پس از نفوذ به شبکه‌های اطلاعاتی دشمن قابل دسترسی است. سیستمهای حفاظتی در برابر این هجومها دست به ابتکارهای نوینی زده‌اند تا با ایجاد نرم‌افزارهای دقیق، سیستمهای شبکه‌ای خود را در برابر این نوع هجومها ایمن سازند. یک نرم‌افزار معروف در این زمینه، ساتن* است. این نرم‌افزار اصولاً برای تأمین وضعیت اطلاعات و شبکه در برابر هجومها طراحی شده‌است. اما با این همه هنوز موفقیتهای تروریستی در حوزه نبرد اطلاعاتی چشمگیر است. این تروریستها با استفاده از افراد زبده و متخصص، ممکن است سیستمهای دولتی، سازمانهای سیاسی و یا شبکه‌های اطلاعاتی را مورد هجوم قرار دهند.(۴۲) اطلاعات پایه‌ای و مبنایی در هر یک از حوزه‌ها به سیستمهای پردازش آن اطلاعات، خوراک لازم را می‌رسانند. این اطلاعات دربرگیرنده هر نوع اطلاعاتی است که هر سیستم تحلیلگر برای دستیابی به نتایج مفید خود به آنها نیازمند است.

در مرحله بعد، یعنی دستیابی به سیستم پردازش اطلاعاتی در شبکه‌های اطلاعاتی، تروریستها برآنند تا با یافتن مکانیزم پردازش اطلاعاتی دشمن در آن رخنه کنند و در مفاصل اطلاعاتی از روزنه‌های اطلاعاتی که خود ایجاد می‌کنند، اطلاعات لازم را به سرقت ببرند. این اطلاعات، که ممکن است اطلاعات پردازش شده باشد، در هر یک از مراحل اطلاعاتی می‌تواند حاوی اطلاعات مفیدی برای تروریستها باشد.

پردازشهای آشکار اطلاعاتی سیستمها و شبکه‌های اطلاعاتی به شیوه‌های گوناگون صورت می‌پذیرد که هریک می‌تواند براساس یک فرآیند اطلاعاتی خاص و یا یک چارچوب پردازشی ویژه صورت پذیرد. کشف این مکانیزمها به تروریستها امکان می‌دهد تا علاقه‌مندیها، ارتباطات، سیر منطقی و دیگر مراحل پردازش اطلاعاتی مورد استفاده هر سیستم اطلاعاتی را به دست آورند. طبیعی است که این دستیابیها می‌تواند در آینده، کار دسترسی و آسیب‌رسانی به اطلاعات و سیستمهای اطلاعاتی را برای تروریستها آسانتر کند.

تروریستها در مرحله سوم یعنی دسترسی سهل به سیستمهای اطلاعاتی، درپی به دست آوردن امکان دسترسی به مجموعه یک سیستم اطلاعاتی جهت آسیب‌رسانی به آن هستند. تروریستها در این مرحله هم درپی آسیب‌رسانی فیزیکی و هم آسیب‌رسانی

---

* Security Analysis Tools for Auditing Network (SATAN)

ارتباطهای منطقی به شبکه‌اند.[۴۳] در آسیب‌رسانی فیزیکی به سیستم اطلاعاتی، تروریستها از همه امکانات خویش در این زمینه بهره‌برداری می‌کنند و می‌کوشند حتی با واردکردن نرم‌افزارهای خاص به سیستم اطلاعاتی دشمن، مشکلات سخت‌افزاری نیز ایجاد کنند. پاک‌کردن اطلاعات، مغشوش کردن اطلاعات موجود روی شبکه و سیستم تصمیم‌گیری آن می‌تواند برخی از این ضربات باشد. حتی این آسیب‌رسانی دامنه‌های وسیعتری را نیز فرا می‌گیرد تا مرحله قطع خطوط تلفنی، بمباران شبکه تلفنی، ترور پرسنل کلیدی فنی در خدمات شهری با استفاده از تکنولوژی سلاحهای جهت‌بخش انرژی* یا باپالسهای الکترومغناطیس** ژنراتورها برای تخریب مدارهای بدون محافظ گسترش یابد.[۴۴]

در مرحله آسیب‌رسانی به ارتباطات منطقی هر سیستم نیز تروریستهای اطلاعاتی می‌کوشند تا با ایجاد اختلالهای خاصی در مدارهای ارتباطی اطلاعاتی، ویژگیهایی را که یک داده را به داده دیگر متصل می‌کند، از میان ببرند و ربط منطقی ارتباطات اطلاعاتی را درهم بریزند. توضیح این فرآیند مستلزم اطلاعات فنی در سیستمهای طرح‌ریزی نرم‌افزارهاست که می‌تواند پیچیدگیهای خاصی را در برداشته باشد. اما خلاصه اینکه به شیوه‌های مختلف می‌توان نوع ارتباطات منطقی میان چندفقره را به چندین هزار فقره دیگر متصل کرد و شبکه اطلاعاتی را در یک سردرگمی خاص قرار داد. به طور مثال اگر داشته باشیم:

(۱) $p \Rightarrow q \ . \ q \Rightarrow I$

این فرآیند با

(۲) $p \Rightarrow q_1 \ , \ q_1 \Rightarrow I_1$

می‌تواند به شکلهای زیر نوعی ارتباط منطقی نیز داشته باشد. واردکردن اطلاعاتی از قبیل $q_1 ... q_n$ که نوعی ارتباط منطقی با p برقرار می‌کنند می‌تواند نتایجی را از $I_n ... I_1$ در پاسخ، نتیجه دهد. یافتن ارتباط منطقی گزاره (۱) ممکن است در بیان درگزاره (۱) و (۲) کار مشکلی نباشد اما اگر این شمار از اطلاعات داده‌ها را بتوان تا (n)گسترش داد، یافتن رتباط منطقی گزاره (۱) ممکن است با زمانبری فراوان و یا حتی با اغتشاش در طلاعات صورت پذیرد که پالایش و تحلیل آن اطلاعات و دستیابی به یک ارتباط منطقی مطلوب را بسیار مشکل می‌نماید.

جنگ اطلاعاتی تروریستی در حوزه اقتصادی

استفاده روزافزون از شبکه‌های اطلاعاتی جهانی به منظور ایجاد ارتباطات و تبادلات

---

* Directed Energy Weapons (DEW) ** Electro Magnetic Pulse (EMP)

اقتصادی و یافتن بازارهای سودآور تجاری و... آنچنان متداول و مرسوم گشته است که دیگر نمی‌توان بدون بهره‌جستن از این گونه تکنولوژیها در زمینه‌های اقتصادی موفق بود. هرچند این تکنولوژی با ویژگیهای خاص خویش تسهیلات و امکانات فراوانی را در اختیار به‌کارگیرندگان آنها قرار می‌دهد ولی وجود امتیازات اینچنینی نمی‌تواند به تنهایی در عداد محاسن آن قرار گیرد و از دیگر ویژگیهای آن به طور کلی چشم پوشاند. گروهها، سازمانها و افراد تروریست که بی‌شک نیازمند اساسی‌ترین پیش‌نیاز فعالیتهای خود یعنی پشتیبانیهای مالی هستند در این رویاروی اطلاعاتی چندین هدف عمده را دنبال می‌کنند که اهم آنها عبارت‌اند از:

۱) تأمین نیازمندیهای مالی؛

۲) تخریب سیستمهای مالی دشمن یا حریف؛

۳) بهره‌برداریهای اطلاعاتی سری.

در مرحله اول، یعنی تأمین نیازمندیهای مالی، تروریستهای اطلاعاتی درپی آن هستند که با سودجستن از تخصصهای ویژه و امکانات و ویژگیهای خاص شبکه‌های اطلاعاتی مالی بتوانند با تغییر پلهای ارتباطی و شکستن رمزهای ورود به سیستمهای ذخیره‌سازی عادی، با انتقال اطلاعات گوناگون و یا به دست آوردن کدهای سرّی و رمزهای ورود به شبکه‌ها به صورت پنهان، اموال و یا حسابهای نقدی بانکهای بزرگ، سازمانهای جهانی و یا شخصیتهای برجسته اقتصادی دنیا را به دیگر حسابهای ساختگی منتقل کنند. از ویژگیهای اصلی این گونه تهاجمات آن است که ریسک و خطرپذیری این حملات بسیار کمتر از خطراتی است که درحمله‌های فیزیکی به مراکز مالی و بانکها صورت می‌گیرد. همین ویژگی موجب شده‌است که از خصوصیت گمنامی* در شبکه بتوان حداکثر بهره‌برداری را به عمل آورد. هرچند این مفهوم در فضای کامپیوتری جای بحث و تأمل بسیار دارد ولی در همین مرحله ذکر این نکته کافی است که گمنامی در شبکه، که امروز مهمترین ویژگی همه استفاده‌کنندگان امکانات اطلاعاتی است، از مفاهیمی است که در فرآیند جنگ اطلاعاتی تروریستی کاربرد پوششی فرد را بسیار گسترده‌تر می‌سازد. در تحقیقی که در زمینه کلاهبرداریها و سرقتهای کامپیوتری ازسوی گروه مشاوره PA در سال ۱۹۹۶ صورت گرفت، نشان داده شد که در هر سال ۲۰ میلیارد لیر فقط در سیستم تجاری اقتصادی انگلستان مفقود می‌شود که بیش از سه و نیم درصد گردش مالی این

* Anonymous

کشور است.[۴۵] اتکای بیش از اندازه سیستمهای اقتصادی غربی بر سیستمهای اطلاعاتی و شبکه‌ها موجب گردیده‌است تا سازمانهای تروریستی این امکان را به عنوان سرچشمه سودآوری تلقی کنند.[۴۶]

در مرحله سوم، یعنی مرحله تخریب سیستمهای اطلاعاتی دشمن یا حریف، تروریستها تلاش دارند که با تخریب این گونه سیستمها، نوعی سردرگمی را به وجود آورند و یا احیاناً بتوانند از طریق این تخریبها، پشتیبانیهای مالی یک مجموعه را مختل سازد و یا از بین ببرند. این وضعیت تا آن اندازه برای تروریستهای اطلاعاتی مهم است که برخی آن را هدف اصلی یا نهایی تروریستها می‌خوانند و می‌نویسند که «هرچند مسائل مالی یک پیش شرط اساسی برای یک سازمان تروریستی است ولی هدف غایی و نهایی این سازمانها در فعالیتهای کامپیوتری تخریب و یا انهدام شالوده‌های اطلاعاتی است.»[۴۷]

باید گفت که مهمترین هدف در تخریب سیستمهای مالی هر مجموعه یا سازمان نظامی، سیاسی یا اطلاعاتی و اقتصادی، آسیب‌رسانی به توان آن سیستم در حداقل زمان است. این آسیب‌رسانی گاه می‌تواند یک مجموعه را با چالشی درازمدت روبه‌رو کند. از سوی دیگر ویژگی مهم دیگر این گونه تخریبها این است که در تبادلات اقتصادی بین شرکتها، تراستهاو کارتلهای بزرگ جهانی نوعی عدم اطمینان را به وجود می‌آورند که موجب می‌شود مشتریان یا سازمانهای بیمه دیگر براحتی نتوانند با مجموعه مذکور کار کنند. از دیگر ویژگیهای ذکر شده برای تخریب سیستمهای اطلاعاتی دشمن در حوزه اقتصادی، اختلال در سیستم ارزیابی و پردازشهای اطلاعاتی است. این اختلال موجب می‌شود که یک مجموعه نتواند در ارزیابیهای خود روی وضعیت موجود بازار، رقبا، نوسانات ارزها و دیگر عوامل مؤثر بر موفقیت‌آمیز بودن پیش‌بینیهای اقتصادی، که مهمترین زمینه پیروزی در صحنه نبردهای اقتصادی جهانی است، بررسی خود را بدرستی انجام دهد. این تخریبهای شالوده‌ای اطلاعاتی می‌تواند دربرگیرنده خدمات اساسی و همچنین اطلاعات مورد نیاز لحظه‌ای مانند نقل و انتقالات پول، سیگنالهای حمل و نقل، سیستمهای سویچینگ تلفن، و... باشد و برنامه‌های تخریب این گونه سیستمهای اطلاعاتی گاه آن قدر سنگین می‌شود که برخی از شرکتها ترجیح می‌دهند که سرویسهای مورد نیاز خود را از طریق یک شرکت مطمئن دیگر تأمین کنند.

حقیقت آن است که ریزه‌کاریهای جنگ اطلاعاتی تروریستی در زمینه تخریب

سیستمهای اطلاعاتی آن قدر وسیع و گسترده شده است که خود مجالی مجزا را برای بحث می‌طلبد.

مرحله سوم از این جنگ اطلاعاتی، مرحله بهره‌برداریهای اطلاعاتی سری است. از مهلک‌ترین ضربات بر پیکره هر سیستم اقتصادی آن است که بتوان به گونه‌ای غافلگیرکننده ضربه‌ای اساسی را بر آن در صحنه بازار رقابتی اقتصادی وارد آورد. اطلاعات سری یک نوآوری صنعتی، یک اختراع جدید، یک نرم‌افزار، یک سیستم الکترونیک چندمنظوره و از این دست موضوعات که می‌توانند سازمانی را به اوج سرمایه‌داری بکشاند گاه آن قدر حیاتی است که افراد متعددی جان خود را در مسیر به دست آوردن یا حفظ آنها از دست می‌دهند.

جنجالی‌ترین صحنه نبرد اطلاعاتی همین صحنه است. جاسوسیهای اقتصادی که قبلاً ازطریق جمع‌آوریهای اطلاعاتی انسانی* صورت می‌گرفت و گاه روابط کشورها را تیره می‌ساخت و گاهی نیز با قتل چند نفری بی‌سر و صدا پایان می‌یافت به صحنه فضای کامپیوتری کشانیده شده است. با اینکه بسیار بعید به نظر می‌رسد یک شرکت یا یک سازمان اقتصادی، اطلاعات سری خود را در زمینه یک اختراع بازارگیر یا یک طرح ارزشمند روی شبکه‌های باز اطلاعاتی قرار دهد ولی ضرورت استفاده از سیستمهای اطلاعاتی، آنها را مجبور می‌سازد تا این اطلاعات را درون یک شبکه بسته اطلاعاتی داخل سیستم نگه‌دارند و یا مورد بررسی و پردازش قرار دهند؛ همین اقدام کافی است. نیاز به هکرهای حرفه‌ای از همین مرحله آغاز می‌شود؛ افراد متخصصی که می‌توانند به محض ایجاد یک ارتباط بین یک سیستم اطلاعاتی کامپیوتری با یک سیستم خارج از آن، به نحوی با ردیابی اطلاعات و شکستن کدها و رمزها وارد یک سیستم داخلی شوند و اطلاعات آن را تخلیه شوند. با پایان یافتن جنگ سرد، که بسیاری از سازمانهای اطلاعاتی بلوک شرق از یکدیگر گسیختند و از داخل فرو پاشیدند، افراد متخصص و بیکاری در دسترس قرار گرفتند که حرفه و تخصص اصلی آنها ورود به سیستمها، تخلیه اطلاعات، و تخریب سیستمهای دشمن است. از این افراد قبلاً نیز سخن رانده شد ولی در اینجا باید متذکر شد که سازمانهای تروریستی با استخدام این افراد متناسب با پیچیدگی عملیات اطلاعاتی می‌توانند از بیرون یک شبکه وارد آن شوند و اطلاعات ذی‌قیمت مربوط به مسائل اقتصادی را، که قبلاً باید از طریق جمع‌آوریهای فیزیکی پنهان

---

* Human Intelligence Collection (HUMINT)

به دست می‌آوردند، امروز از طریق کامپیوترها و فضای کامپیوتری و با استفاده از گمنامی اطلاعاتی و تخصص هکرها به دست آورند. و در یا حداقل زمان بزرگترین ضربات را بر سیستم اطلاعات مالی یک نظام یا حاکمیت وارد آورند که جبران آن مستلزم هزینه سنگین است.

نتیجه‌گیری

از آنچه که مورد بحث قرارگرفت روشن می‌شود که جنگ اطلاعاتی در حوزه‌های گوناگون جنگ اطلاعاتی استراتژیک، جنگ اطلاعات دفاعی و جنگ اطلاعاتی تروریستی در اشکال و انحای گوناگون خود می‌رود تا صحنه وسیع و فراگیری را در میدانهای رقابتی و مبارزاتی میان کشورها، واحدهای سیاسی و گروهها و سازمانها و حتی افراد به دست آورد. شناخت تکنولوژی اطلاعات، مزایا و معایب آن، دسترسی به سیستمهای پیچیده‌تر ایمنی‌ساز سیستمها و ردیابی با انواع جنگهای اطلاعاتی که ممکن است منافع ملی یک ملت یا یک نظام را با خطر روبه‌رو سازد از مهمترین مسائلی است که می‌تواند چالشهای آینده رویاروی یک نظام را جهتی نو و تازه بخشد. مسلح شدن به سلاح تکنولوژی اطلاعات و پذیراشدن انقلابهای هر روزه در این سیستم و اتکای بیش از حد یک نظام یا سازمان که لاجرم در طول زمان شکل می‌گیرد. آسیب‌پذیریهای جدّی نظامها را مضاعف می‌سازد و موجب می‌گردد که درهر برهه از زمان و بویژه در بحرانها بتوان این نقاط استراتژیک را مورد هجوم قرار داد. سؤال اساسی این است که در این شرایط و با این ویژگیها چه باید کرد؟ آیا از تکنولوژی اطلاعات و دامنه‌های وسیع آن باید حذر کرد؟ اصولاً چنین چیزی در هیچ‌یک از حوزه‌های تمدنی امروز ممکن است؟ و اگر ممکن نیست کشورهایی که به تبع کشورهای صاحب تکنولوژی وارد صحنه بهره‌برداری از این نوع سیستمها می‌شوند چگونه می‌توانند خود را در برابر آسیب‌پذیریهای جدی و جدید آن مصون نگاه دارند؟ در حوزه‌های دفاعی و امنیتی که امنیت ملی یک کشور در آن حوزه‌ها رقم می‌خورد شکل و شرایط بروز این تهدیدات و شیوه استفاده از این فرصتها چگونه است؟ این پرسشها دهها پرسش اساسی و استراتژیک دیگر هم پاسخ می‌طلبند و هم صحنه کارزار را بسیار پیچیده‌تر از گذشته در برابرمان ترسیم می‌کند.

یادداشتها

۱- برای بررسی تأثیرات تکنولوژی اطلاعاتی بنگرید :

- David Alberts, ***The Unintended cansequences of International Technologies*** (U.S.A.: NDU Press, 1996).

2- John Arguilla. ***Cyberwar is Coming*** (Santa Monica : RAND, 1993), p.4.

3- ***Ibid.***, p.30.

4- Gary Wheatley, ***Information Warfare and Deterrence*** (U.S.A. : NDU Press, 1996), p.30.

5- Lorenzo Valeri. "The Information Warriors", ***Defence Systems International*** (Aut. 1997), p.105.

6- Andrew Rathmell, "Cyber - Terrorism", ***RUSI Journal***, Oct. 1997, pp.40-45.

7- Jeffrey Cooper, ***Understanding IW***.(U.S. : SCIP pub., 1996), p.13.

8- ***Ibid***.

9- ***Op.Cit.***, p.4.

10- Martin Libicki. "What is Information Warfare?". ***ACIS Papers***, No.3, August 1995, pp.18-45.

11- Steven Metz, ***Information Revolution and Postmodern Warfare***, (U.S.A. : American Defence College, 2000), p.63.

12- Rager Molander. ***Strategic Information Warfare*** (Santa Monica : RAND, 1999), p.2.

13- Zalmy Khalilzad . ***Information Warfare***, (Santa Monica : Rand, 1999), p.30.

14- ***Op.Cit.***, p 7.

15- ***Ibid***.

16- Molander, ***Op.Cit.*** p.24.

17- ***Op.Cit.***, ch.7, p.41.

18- Steven Metz, ***Armed Conflict in 21st Century*** (Carlisle : International Strategic Studies Institutes, 2000), p.20.

19- Andrew Rathmell, "Cyber - Terrorism", ***Op.Cit.***, pp.44.

20- "Hackers Penterate DoD Computer Systems", Report of Testimony, 1991.

۲۱- برای مطالعه بیشتر در این مورد بنگرید:

- "Ensuring Joint Force Superiority in the Information Age". ***Defense Issues***, Vol.11, (No.82), pp.57-92.

22- Lorenzo Voleri, ***Op.Cit.***, p.3.

23- ***Ibid***.

24- Andrew Rothmell, ***IW Threat from Sub-State groups***, Paper Presented at the Institute for National Strategic Studies, Jun. 17 1997.

25- GAO GENERAL Accounting office. Report to Congress, 1997, p.11.

26- GAO, ***Computer attacks at Department of Defference***. 1997, chapter1.

27- Andrew Rathmell. "The IW Threat from Sub-States groups". ***Op.Cit.***, p.2.

28- Cramer. ***Economic Espionage : An information perspective***, (1996). P.3.

29- David Ronfeldt, John Arquilla. ***Netcuor KS, Netcuar, and Information - Age Terrorism*** (Santa Monica : RAND, 1999), p.14.

30- Andrew Rathmell. "The IW Threat from Sub-States groups". ***Op.Cit.***, p.1.

31- Andrew Rathmell, "The IW Threat from Sub-States groups". ***Op.Cit.***, p.5.

32- ***Jane's Intelligence Review***. December 1999.

33- George Copley. "Strategic Intelligence for Everyone". ***Defence and Foreign Affairs Strategic Policy***. October 1999, p.11.

34- ***Op.Cit.***, p.9.

35- Defence and Foreign Affairs Strategic Policy, 1999, p.10.

36- Dorothy Elizabeth Denning. ***Information Warfare and Security*** (U.S.: Longman, 1998), p.27.

37- GAO : Information Security. ***Op.Cit.,*** p.22.

38- C4I = Command - Control - Communication - Computer - Intelligence

39- Andrew, W. Marshall.***The Changing role of information*** (Santa Monica : RAND, 1999), p.3.

40- Andrew Rathmall, "Cyber - Terrorism". ***Op.Cit.***, pp.44.

41- Revolution in Military Affairs

42- Andrew Rethmell, "The IW Treat From Sub-State Groups". ***Op.Cit.***, p.4.

43- Cyber Terrorism. ***Op.Cit.***, p.5.

44- ***Ibid.***

45- "The IW Threat Form Sub-state Groups". ***Op.Cit.,*** p.5.

46- ***Ibid.***

47- ***Ibid.***, p.6.