مرکز بررسیهای استراتژیک

گزارش

نفوذ و ضد نفوذ:

مفاهیم، ابعاد و انواع

تهیه شده در

مرکز بررسی‌های استراتژیک ریاست جمهوری

۱۳۹۴

بسم‌الله الرّحمن الرّحیم

عنوان گزارش:
نفوذ و ضد نفوذ: مفاهیم، ابعاد و انواع

فهرست مطالب

خلاصه اجرایی ۱

منابع اطلاعاتی ۳

گردآوری منابع برای نفوذ ۷

خنثی‌سازی به وسیله نفوذ ۸

نفوذ و ماهیت سیاست جهانی ۱۱

نفوذ و چرخه اطلاعاتی ۱۲

کنترل و اشراف بر نفوذ ۱۴

ضدنفوذ ۱۴

نفوذ و اقدامات پنهانی ۱۵

انواع اقدامات پنهانی و نفوذ ۱۷

تبلیغات سیاسی ۱۸

عملیات‌های فریب و نفوذ ۱۹

اقدام سیاسی و نفوذ ۲۰

اقدامات شبه‌نظامی و نفوذ ۲۰

نفوذ الکترونیک در جنگ اطلاعاتی و ضداطلاعاتی ۲۰

فهرست منابع ۲۹

خلاصه اجرایی

رهبر معظم انقلاب اسلامی در ۴ آبان ماه سال ۱۳۹۴ طی سخنانی در جمع فرماندهان گردان‌های بسیج، مفهوم جدیدی را تحت عنوان «نفوذ» به ادبیات سیاسی و امنیتی کشور وارد کردند. معظم له ضمن تشریح چگونگی نفوذ دشمن به ساخت قدرت در کشور، فرمودند:

« نفوذ دو جور است: یک نفوذ موردی است، نفوذ فردی است؛ یک نفوذ جریانی است. نفوذ موردی خیلی نمونه دارد، معنایش این است که فرض کنید شما یک دم‌ودستگاهی دارید، یک مسئولی هستید؛ یک نفر را با چهره‌ی آرایش‌شده، بزک‌شده، با ماسک در مجموعه‌ی شما بفرستند؛ شما خیال کنید دوست است درحالی‌که او دوست نیست، تا او بتواند کار خودش را انجام بدهد؛ گاهی جاسوسی است که این کمترینش است؛ یعنی کم‌اهمّیّت‌ترینش جاسوسی است، خبرکشی و خبردهی است؛ گاهی کارش بالاتر از جاسوسی است، تصمیم شما را عوض میکند. شما یک مدیری هستید، یک مسئولی هستید، تصمیم‌گیر هستید، میتوانید یک حرکت بزرگ یا مؤثّری انجام بدهید، اگرچنانچه این حرکت را این‌جور انجام بدهید این به نفع دشمن است، او می‌آید کاری میکند که شما حرکت را این‌جور انجام بدهید؛ یعنی تصمیم‌سازی. در همه‌ی دستگاه‌ها سابقه هم دارد؛ فقط هم دستگاه‌های سیاسی نیست، دستگاه‌های روحانی و دینی و مانند اینها هم همیشه وجود داشته.»

ایشان همچنین در رابطه به احتمال جناحی شدن تعریف مفهوم نفوذ بیان داشتند:

« نفوذ که ما میگوییم، حالا بعضی‌ها واکنش نشان میدهند؛ آقا! مسئله‌ی نفوذ جناحی شد، استفاده‌ی جناحی کردند؛ من به این حرف‌ها کاری ندارم. خب، استفاده‌ی جناحی نکنند، بحث بیهوده درباره‌ی نفوذ نکنند، اسم نفوذ را بدون محتوای لازم مطرح نکنند؛ اینها را ما کاری نداریم ولی هر حرفی زده میشود، هر کار جدّی [می‌شود]، از اصل واقعیّت نفوذ غفلت نشود؛ غفلت نکنیم که دشمن درصدد نفوذ است.»

مرکز بررسی‌های استراتژیک لازم دانسته است تا در جهت ترسیم چارچوب‌های نظری در قانونمند کردن مبحث «نفوذ و ضدنفوذ» در کشور، موارد نفوذ و نشت اطلاعات، شیوه های نفوذ و اثرگذاری منفی، روش‌های مرسوم ضدنفوذ و ضداطلاعات را بر اساس تعاریف ارائه شده در متون اصلی ادبیات اطلاعات و ضد اطلاعات ارائه کند.

مهمترین حیطه‌های این مرور ادبیات در مسئله نفوذ عبارت‌اند از:

۱. نفوذ به چه منظوری صورت می گیرد؟
۲. اشکال متنوع نفوذ شامل چه مواردی است؟
۳. راهبردها و تاکتیک‌های فرایند ضدنفوذ چیست؟

اهمیت تشریح چارچوب برای مفهوم نفوذ آنگاه مشخص می‌شود که بدانیم در صورت نبود تعریف اجماعی درباره نفوذ و همچنین بسط نگاه تنگ نظرانه و یا جناحی از این موضوع در بدنه نظام اجرایی کشور، سبب خواهد شد تا رفته رفته عرصه باز سیاسی و امنیتی کشور، تنگ شده و در نهایت به استحاله مصالح و منافع عالیه نظام و کشور خواهد بیانجامد. در این رابطه، مهمترین تبعات راهبردی که از نبود تعریف جامع و حقوقی از پدیده نفوذ پدید خواهد آمد عبارت اند از:

۱. احتمال ظهور فضای تنگ نظری در نهادهای اطلاعاتی نسبت به شخصیت‌های اثرگذار ملی
۲. محدودیت جدی پیرامون نظرات و گزارش‌های راهبردی مشاوران و متخصصین اثرگذار کشور
۳. کاهش صراحت و اثرگذاری گزارش‌های راهبردی در فرایند اجرایی شدن
۴. سایه رکود بر فضای ایده پردازی و مشاوره تخصصی در نهادهای راهبردی
۵. افزایش دامنه اقتدار نهادهای اطلاعاتی و امنیتی نسبت به نهادهای سیاسی و اجرایی
۶. به حاشیه رانده شدن متخصصین متعهد در سایه سوء ظن
۷. نقض احتمالی حقوق شهروندی
۸. گسترش تفسیر مضیغ نسبت به اطلاعات آشکار و تفسیر موسع از اطلاعات غیرحساس
۹. انحراف هدف گذاری در ماموریت های ذاتی نهادهای اطلاعاتی از تمرکز بر ضداطلاعات خارجی بر رصد عوامل داخلی
۱۰. بروز فضای بی‌اخلاقی و اتهام زنی در جناح های سیاسی و نهادهای راهبردی رقیب

توصیه

پیشنهاد می‌شود به منظور جلوگیری از بروز پیامدهای منفی بسط دامنه تعریف و یا نبود تعریف روشن از پدیده نفوذ در کشور، اقدامات زیر مدنظر قرار گیرد:

۱. تهیه پیش‌نویس در باره مفهوم پردازی و اشکال متنوع نفوذ
۲. ارائه پیش نویس به شورایعالی امنیت ملی و تصویب تعاریف و تحدید حدود روشن از اشکال نفوذ
۳. توجیه مناسب نهادهای اطلاعاتی، امنیتی و انتظامی نسبت به مصوبه شورا در راستای جلوگیری از بروز تفسیر نادرست از مصوبه آتی
۴. ابلاغ مصوبه قانونی حدود نفوذ و ضدنفوذ به نهادهای اجرایی و راهبردی کشور

منابع اطلاعاتی

ادوارد والتز[1]، صاحب‌نظر و نویسنده کتب اطلاعاتی و امنیتی در کتابی تحت عنوان «مدیریت خبر در کار اطلاعاتی»[2] منابع داده‌های اطلاعاتی را با توجه به «دسترسی»[3] و «شیوه گردآوری»[4] اینگونه تقسیم بندی می‌کند.

وی بسته به میزان دسترسی به منابع، آن‌ها را به منابع «آشکار»[5] و «بسته»[6] (برای مثال، مناطق ممنوعه، ارتباطات ایمن یا فعالیت‌های پنهانی) تقسیم‌بندی می‌کند.

۱. منابع آشکار

به‌دلیل دسترسی فزاینده به رسانه‌های الکترونیک (ارتباطات مخابراتی، تصاویر ویدئویی و شبکه‌های کامپیوتری) و گسترش جهانی کشورهای باز، «اطلاعات منابع آشکار»[7] نیز به منبعی فزاینده از داده‌های جهانی تبدیل شده است. هرچند اطلاعات منابع آشکار باید مورد بررسی قرار گیرد و با عبور آن از فیلترهای مختلف، اعتبارسنجی شود، اما منبع اقتصادی خوبی از اطلاعات عمومی بوده و کمکی به دیگر منابع است (Waltz, 2003: 35).

بسیاری از سیاست‌گذاران و افسران اطلاعاتی بر این تصور هستند که اطلاعات به‌دست آمده به‌صورت پنهانی برتر از اطلاعات از منابع آشکار است. با این‌وجود، تمایز میان منابع آشکار و پنهان چندان واضح نیست. در نظارت و تحلیل مشکلاتی نظیر تروریسم، گسترش تسلیحات کشتار جمعی و فعالیت‌های ضداطلاعاتی، منابع آشکار غالباً از اهمیتی برابر یا حتی فراتر از اطلاعات طبقه‌بندی‌شده دارند. اطلاعات پنهان‌شده پشت دیوارهای طبقه‌بندی[8] و دسترسی ویژه[9] ممکن است ارزشی بیشتر از اطلاعات در دسترس مردم نداشته باشند. کم‌اهمیت دانستن «اطلاعات منابع آشکار»[10] در مقابل اطلاعات پنهانی که در صورت دست‌یابی به آن‌ها از هزینه بیشتری نیز برخوردارند، برای اداره سازمان‌های اطلاعاتی مناسب نیست. همچنین باید به این مسئله توجه داشت که بخش خصوصی برای کسب اطلاعات آشکار عاملی مهم در این زمینه محسوب می‌شود. بنابراین نهادهای اطلاعاتی باید توجه خاصی به این موضوع داشته باشند (Mercado, 2005).

جریان‌های آشکار و پنهان اطلاعات به‌هیچ وجه به‌طور کامل در موازی یکدیگر یا متمایز از هم نمی‌باشند؛ آن‌ها غالباً با یکدیگر ترکیب شده و نیز وارد قلمروی دیگری می‌شوند. برخی مواقع، گزارشات پنهانی ترکیبی از بخش‌های

1. Edward Waltz
2. Knowledge management in the intelligence enterprise
3. access
4. collection means
5. open
6. closed
7 .open source intelligence (OSINT)
8. classification
9. special access
10. open source intelligence (OSINT)

مختلف مطبوعات می‌باشد. برخی مواقع نیز روزنامه‌ها مبادرت به انتشار اطلاعات طبقه‌بندی‌شده که به بیرون نشت کرده، مبادرت می‌کنند که می‌تواند مورد استفاده نهادهای اطلاعاتی کشورهای دیگر قرار گیرد (Mercado, 2005).

منابع آشکار نه‌تنها زمان‌هایی غیرقابل تمایز از اسرار هستند، بلکه این‌گونه اطلاعات به‌لحاظ ارزش تحلیلی برتر از اطلاعات طبقه‌بندی‌شده هستند. ارزش این اطلاعات را می‌توان از جنبه‌های زیر مورد توجه قرار داد:

سرعت[11]: زمانی‌که بحرانی در برخی بخش‌های دور از کشور روی می‌دهد – جایی که امکان حضور مأموران و عوامل اطلاعاتی وجود ندارد – تحلیل‌گران و سیاست‌گذاران اطلاعاتی در وهله نخست به خبرهای رسانه‌ای و اینترنتی روی می‌آورند؛

کمیت[12]: به‌طور قطع وبلاگ‌نویسان، روزنامه‌نگاران، ناظران، گزارشگران تلویزیونی و متفکران بیشتری به‌نسبت افسران اطلاعاتی در جهان وجود دارند. هرچند دو یا چند افسر اطلاعاتی که به اطلاعات پنهانی دسترسی دارند، بهتر از سپاهی از گزارشگران عمل می‌کنند، ولی نظر بر این است که ترکیب قطعاتی از اطلاعات بی‌شمار منابع آشکار ارزشی به‌مراتب بیشتر از گزارشات محرمانه چند نفر دارد.

کیفیت[13]: در اغلب موارد، اطلاعات به‌دست آمده از منابع آشکار که آلوده به دروغ جاسوسان دوجانبه و فریب‌خورده نمی‌باشد، بسیار کارآمدتر از اطلاعات پنهانی ازسوی این افراد خواهد بود.

شفافیت[14]: تحلیل‌گران و سیاست‌گذاران در بسیاری از موارد «اطلاعات انسانی» حتی دقیق را نیز دارای مشکل می‌دانند. برای مثال، زمانی‌که یک افسر رده‌بالای اطلاعاتی گزارشی راجع به یک رهبر سیاسی را می‌خواند،مطمئن نیست که این گزارش صحیح باشد، زیرا از منبع آن آگاهی ندارد و نمی‌داند چه کسی این اطلاعات را بیان داشته است. در واقع، هرچند منابع اطلاعات آشکار برخی مواقع نامشخص هستند، اما در مورد اطلاعات سری، منابع همیشه نامشخص هستند.

سهولت در استفاده[15]: امکان تبادل اسرار طبقه‌بندی‌شده با دسترسی ویژه با سیاست‌گذاران و حتی همکاران اطلاعاتی نیز با دشواری صورت می‌گیرد. با این‌حال، تمامی مقامات می‌توانند اطلاعات آشکار را بخوانند.

هزینه[16]: یک ماهواره شناسایی که میلیاردها دلار هزینه برای ساخت، پرتاب و حفظ دارد، می‌تواند تصاویری از بام کارخانجات تولید تسلیحات یا بدنه کشتی‌ها تهیه کند. در مقابل، یک نشریه خارجی با آبونمانی ۱۰۰ دلاری در سال می‌تواند تصاویری از داخل کارخانجات یا کشتی‌ها داشته باشد (Mercado, 2005).

11. Speed
12. Quantity
13 .Quality
14. Clarity
15. Ease of use
16 .Cost

۲. منابع بسته

هر دو شیوه‌های فنی آشکار و پنهان از گردآوری اطلاعات، داده‌هایی را ارائه می‌دهند که با محدودیت دسترسی و محرمانه‌بودن تحت محافظت قرار گرفته‌اند. «اطلاعات تصویری»[۱۷] نیز ارزیابی‌هایی را از اشیاء قابل تشخیص به‌واسطه تصاویر گرفته‌شده از زمین ارائه می‌دهد. این نوع اطلاعات مکان، ترکیب و همچنین ویژگی منابع، زیرساخت‌ها، تأسیسات و خطوط ارتباطاتی را مشخص می‌سازند. «اطلاعات سیگنالی»[۱۸] هم بر سیگنال‌های الکترومغناطیس برای داده‌های الکترونیک (همچون رادارها) و ارتباطات (همچون ارتباطات مخابراتی صدا و داده‌ها) نظارت دارد. نیاز نوظهور به گردآوری اطلاعات از شبکه‌های دیجیتالی نیز استفاده از «بهره‌گیری شبکه کامپیوتری»[۱۹] را ایجاد کرده است. این شیوه شامل شناخت زیرساخت‌های شبکه‌ای، خروجی‌های ترافیک شبکه و ورودی‌های ارتباطاتی داده‌ها و نیز دسترسی به اتصالات کامپیوتری و بهره‌گیری از کامپیوترهای شبکه‌ای است. «اطلاعات ارزیابی و علامات»[۲۰] نیز شامل کسب خبر و آگاهی از طیف گسترده‌ای سنسورها می‌شود. از این نوع اطلاعات برای پی بردن به پدیده‌های قابل مشاهده از محیط و دستگاه‌های نظارتی و جاسوسی دشمن استفاده می‌شود (Waltz, 2003: 35).

17. imagery intelligence (IMINT)
18. signals intelligence(SIGINT)
19. computer network exploitation (CNE)
20 .measurments and signatures intelligence (MASINT)

جدول ۱ : دسته‌بندی‌های منابع اطلاعاتی با توجه به میزان دسترسی (آشکار یا بسته)

و شیوه گردآوری (انسانی یا فنی)

دسترسی	نوع منبع	دسته منبع اطلاعاتی	نمونه‌ها
آشکار	شیوه‌های انسانی و فنی	اطلاعات منبع آشکار (**OSINT**)	منابع خبری رادیو و تلویزیون خارجی محصولات چاپی خارجی: کتاب‌ها، مجلات، گزارشات، روزنامه‌ها گزارشات ارسالی ازسوی دیپلمات‌ها و وابسته‌ها مکالمات صورت‌گرفته با استفاده از موج کوتاه، تجهیزات مخابراتی و اینترنت منابع شبکه کامپیوتری خارجی – منابع خاکستری[۲۱] (چاپی و الکترونیک)
بسته	شیوه‌های انسانی	اطلاعات انسانی (**HUMINT**)	گزارشات مأموران در کشورهای خارجی گفت‌وگوها با پرسنل کشورهای خارجی گزارشات از بریده‌ها از کشورهای خارجی – پیام‌های منابع ثالث دوست
	شیوه‌های فنی	اطلاعات تصویری (**IMINT**)	تصاویر شناسایی (تصاویر ایستای هوایی و فضایی از زمین) – تصاویر شناسایی (تصاویر ویدئویی از زمین)
		اطلاعات سیگنالی (**SIGINT**)	نظارت سیگنالی الکترومغناطیس[۲۲] (**ELINT**) اطلاعات راداری[۲۳] (**RADINT**) نظارت ترافیک ارتباطات[۲۴] (**COMINT**) – اطلاعات سیگنالی تأسیسات خارجی[۲۵] (**FISINT**)
		بهره‌گیری شبکه کامپیوتری (**CNE**)	تحلیل و نظارت شبکه رهگیری پیام شبکه‌ای نفوذ و استفاده از کامپیوترها
		اطلاعات ارزیابی و علامات (**MASINT**)	اطلاعات به‌دست آمده به شیوه‌های فنی از تمامی منابع – استفاده از تأسیسات فیزیکی (هسته‌ای، میکروبی، شیمیایی)، انرژی رادیویی (فرکانس‌های رادیویی) مادون قرمز، امواج صوتی، صدای مکانیکی، تأسیسات مغناطیسی و ترکیب مواد

21. gray literature

آثار ارزشمندی که در منابعی غیر از منابع معمول یافت می‌شوند، همانند گزارش‌های فنی آژانس‌های دولتی و کارهای تحقیقاتی

22. electromagnetic signals monitoring (ELINT)
23. radar intelligence (RADINT)
24. communications traffic monitoring (COMINT)
25. foreign instrumentation signals intelligence (FISINT)

گردآوری منابع برای نفوذ

اطلاعات مطلوب در مورد سرویس‌های اطلاعاتی و امنیتی خارجی که در نهایت برای خنثی کردن فعالیت‌های خصمانه علیه کشور مورد استفاده قرار می‌گیرند، شامل داده‌ها راجع به تأسیسات، رهبری، پرسنل، شیوه‌های ارتباطاتی، شیوه‌های فریب و منافع آن‌ها بوده و از منابع مختلف به‌دست می‌آید (US Army Offensive Counterintelligence Operations, 1982: 2).

منابع آشکار مرتبط با سرویس‌های دوست یا دشمن ممکن است شامل اسناد رسمی دولتی (برای مثال، راهنمای تلفن، بروشورها، گزارشات سالانه، گزارش نشست‌های پارلمان و گزارشات کمیسیون‌های تحقیق)،کتاب‌ها، مقالات در مجلات و روزنامه‌ها باشد. مقالات روزنامه‌های اسرائیلی در مورد ماهواره‌های شناسایی این کشور،کتاب‌های پژوهشی راجع به «سرویس اطلاعاتی آلمان فدرال»[۲۶] و انتشارات رسمی همچون گزارش سالانه «کمیته برآورد اطلاعات امنیتی کانادا»[۲۷] راجع به «سرویس اطلاعات امنیتی کانادا»[۲۸]، مثال‌هایی از این نوع منابع هستند (Richelson, 2008: 397).

در مورد جوامع بسته[۲۹]، منابع آشکار محدود است؛ با این‌وجود، حتی در این کشورها نیز تحلیل‌گران برخی اخبار حساس را به‌نوعی از زیر زبان پرسنل رده‌بالای آن‌ها یا گزارشات ارائه‌شده از اقدامات سرویس اطلاعاتی و امنیتی خود به‌دست می‌آورند. اخبار مرتبط با سرویس‌های اطلاعاتی کشورهای دوست نیز از ترتیبات همکاری و آموزشی حاصل می‌شود. این نوع همکاری همچنین موجب کسب اخبار از فعالیت سرویس‌های اطلاعاتی دشمن می‌شود (Richelson, 2008: 397).

یک عامل نفوذی می‌تواند اخبار سودمندی را به سرویس بیگانه از قرار زیر ارائه کند:

عاملی که پستی رسمی را در سرویس اطلاعاتی دشمن دارا است. این شخص در یکی از دسته‌های «موش کور»[۳۰] (کسی که پیش از ورود به یک سرویس اطلاعاتی به استخدام درمی‌آید) یا «بریده در محل»[۳۱] (کسی که پس از کسب موقعیتی در سازمان اطلاعاتی دشمن با ارائه اخبار موافقت می‌کند) جای گرفته و ممکن است به‌دلایل ایدئولوژیکی یا مالی و یا در نتیجه اجبار یا حق السکوت[۳۲] بر اساس رفتارهای نادرست جنسی یا مالی دست به این کار بزند؛

بهره‌گیری از بریده‌ها که خبرهای مرتبط با جنبه‌های گوناگون ساختار یک سرویس اطلاعاتی یا امنیتی، عملیات‌ها و رهبری را ارائه می‌کنند؛

26 German Federal Intelligence Service (German: Bundesnachrichtendienst (BND))
27 Canadian Security Intelligence Review Committee
28 Canadian Security Intelligence Service (CSIS)
29 closed societies
30 mole
31 defector-in-place
32 blackmail

استفاده از پرسنل اطلاعاتی خودی در کشورهای هدف (Richelson, 2008: 398-400).

اسناد به‌دست آمده از سرویس‌های اطلاعاتی رژیم سابق و کنار رفته نیز می‌تواند اخبار ارزشمندی به‌همراه داشته باشد، زیرا می‌توان از این اخبار برای شناسایی جاسوسان و عوامل رژیم سابق که ممکن است در آینده برای سرویس اطلاعاتی دیگری کار کنند، استفاده کرد. نمونه چنین چیزی بهره‌گیری آمریکا از اسناد «وزارت امنیت دولتی آلمان شرقی»[۳۳] پس از اتحاد دو آلمان و دستیابی به پرونده‌های زیادی از «سرویس اطلاعاتی عراق»[۳۴] پس از سقوط صدام حسین بود (Richelson, 2008: 400).

فراتر از منابع انسانی و اسناد، گردآوری فنی هم داده‌های ارزشمندی را برای فعالیت‌های ضداطلاعاتی فراهم می‌سازد. رهگیری ارتباطات داخلی یک کشور یا سفارت‌خانه کشورهای دیگر در خاک خود می‌تواند فعالیت سرویس‌های امنیتی یا فعالیت‌های اطلاعاتی سرویس‌های اطلاعاتی خارجی را برملا کند (Richelson, 2008: 400).

به‌طور قطع، تصاویر ماهواره‌ای کارایی کمتری به‌نسبت عوامل نفوذی، منابع آشکار یا «اطلاعات ارتباطاتی»[۳۵] در ارائه اخبار مرتبط با فعالیت سرویس‌های اطلاعاتی خارجی دارند. با این‌حال می‌توانند داده‌هایی دقیق را از مکان و تشکیلات سرویس‌های اطلاعاتی و امنیتی ارائه دهند – داده‌هایی که در زمینه حمله مستقیم به چنین تأسیساتی بسیار سودمند هستند. برای مثال، حملات دقیق به «سازمان امنیت ویژه»[۳۶] عراق در سال ۲۰۰۳ با استفاده از تصاویر ماهواره‌ای و هواپیماهای شناسایی که پیش از آن برای پشتیبانی از فعالیت ناظران سازمان صورت گرفته بود، انجام گردید (Richelson, 2008: 401).

خنثی‌سازی به وسیله نفوذ

خنثی‌سازی[۳۷] فعالیت سرویس‌های اطلاعاتی دشمن می‌تواند از طرق گوناگون صورت پذیرد. نفوذ[۳۸] به سرویس امنیتی دشمن نه‌تنها برای گردآوری اخبار، بلکه برای ضربه زدن به عملیات‌های آن نیز می‌توان مورد استفاده قرار داد. راه دیگر انتقال اخبار به کشور ثالثی است که منجر به اتخاذ اقدامی ازسوی آن علیه افسران و عوامل اطلاعاتی سرویس دشمن خواهد شد. در بسیاری از موارد، سیا چنین اخباری را به سرویس‌های امنیتی کشورهای دوست می‌دهد. شیوه دیگر در خنثی‌سازی استفاده از مأموران دوجانبه[۳۹] است (Richelson, 2008: 406).

33 .East German Ministry of State Security (German: Ministerium für Staatssicherheit (MfS) commonly known as the Stasi)
34. Iraqi Intelligence Service (Arabic: جهاز المخابرات العامة العراقية)
35 .communications intelligence (COMINT)
36 .Iraqi Special Security Organization (SSO) (Arabic: جهاز الأمن الخاص)
37. neutralization
38 .penetration
39. double agent(s)

در ایالات متحده، اف‌بی‌آی مسئولیت اصلی برای حفاظت از اطلاعات طبقه‌بندی‌شده و موارد دیگر همچون اطلاعات صنعتی را بر عهده دارد. سی.آی.ای نیز مسئول هماهنگی فعالیت‌های ضداطلاعاتی آمریکا در خارج از کشور است. هریک از تشکیلات نظامی نیز دارای واحد ضداطلاعات هستند که در داخل و خارج فعال هستند. هریک از این واحدها دارای مأموریت‌هایی تهاجمی و تدافعی می‌باشند. در بُعد تهاجمی تلاش می‌کنند عواملی را در سرویس‌های اطلاعاتی خارجی به استخدام خود درآورند تا بفهمند آیا عملیاتی علیه ایالات متحده در حال شکل‌گیری است. در عین‌حال بر فعالیت‌های مأموران شناخته‌شده یا مشکوک سرویس‌های خارجی نیز نظارت می‌کنند. همچنین برای پی بردن به اهداف و شیوه کار سرویس‌های اطلاعاتی خارجی دست به عملیات نیز می‌زنند. در بُعد دفاعی هم موارد احتمالی از جاسوسی را مورد بررسی قرار داده و تحلیل‌هایی را برای دولت و بخش‌های صنعتی در مورد تهدید سرویس‌های خارجی تهیه می‌کنند.

به‌هرحال، ضداطلاعات به‌عنوان کارکردی از آژانس‌های اطلاعاتی فراتر از کشف و نظارت بر فعالیت سرویس‌های اطلاعاتی خارجی و تحقیق در مورد احتمال جاسوسی است. تمامی آژانس‌هایی که دست به گردآوری اطلاعات ازطریق منابع انسانی یا شیوه‌های فنی می‌زنند، ، باید همواره مراقب باشند که آیا آنچه گردآوری می‌کنند حقیقی است یا خیر. این امر نیازمند ارزیابی پیوسته از منابع و نیز اطلاعات گردآوری‌شده ازسوی آنان است. تحلیل‌گران اطلاعاتی که با کلیت اطلاعات راجع به موضوعی خاص آشنا هستند، غالباً در پست‌هایی برای کشف موارد خلاف قرار می‌گیرند (Johnson, 2007: 265).

در همین حال، اقدامات دفاعی دیگری نیز برای حفاظت از اشخاص، مکان‌ها و چیزهایی به‌دور از چشمان شکارگر نفوذی‌های ناخوانده وجود دارد که هرچند تمامی آن‌ها لزوماً تشکیل‌دهنده ضداطلاعات نیستند، ولی بخشی از یک طیف حفاظتی هستند که از یادآوری به کارگران صنایع دفاعی برای عدم‌صحبت در مورد فعالیت‌هایشان تا ریشه‌کن کردن یک شبکه جاسوسی را شامل می‌شود. این‌گونه اقدامات حمایتی از کارکرد ضداطلاعات برای محافظت از اسرار کشور هستند که دربردارنده موارد زیر است (Clark, 2007: 69):

حفاظت اسناد[40]: یکی از شیوه‌ها برای محافظت از اسنادی که نمی‌خواهید کسی از آن آگاهی داشته باشد، کنترل دسترسی به آن‌ها است. شیوه‌های اساسی دولت آمریکا برای محدودکردن دسترسی به اخبار شامل طبقه‌بندی[41] اسناد می‌شود. سیستم آن نیز در سلسله‌مراتبی از سری[42]، محرمانه[43] و کاملاً محرمانه[44] قرار دارد. هریک از این دسته‌ها

40. document security
41. classification
42. confidential
43. secret
44. top secret

به‌ترتیب می‌توانند خسارات، خسارت جدی و خسارت عظیم به امنیت ملی آمریکا وارد سازند (Bush, ۲۰۰۳). فراتر از این سیستم استاندارد، مجموعه‌ای از محدودیت‌ها نیز به‌منظور آنچه «اخبار رده‌بندی‌شده حساس»[۴۵] خوانده می‌شود، طراحی شده‌اند. اخبار به‌دست آمده یا مرتبط با ماهواره‌های تصویری و سیگنالی و نیز اخبار حاصل از هواپیماها یا زیردریایی‌های شناسایی و اطلاعاتی در این طبقه جای می‌گیرند. خارج از این سیستم طبقه‌بندی رسمی، مجوعه‌ای فزاینده از کنترل‌های سازمانی در مورد اخبار «حساس ولی غیرطبقه‌بندی»[۴۶] اعمال می‌شود (Clark, ۲۰۰۷: ۷۰-۷۱).

حفاظت ارتباطات[۴۷]: اطلاعات ارزش چندانی ندارد، مگر کسانی‌که به آن نیاز دارند بتوانند آن‌را دریافت و درک کنند. در نتیجه، هر لحظه حجم بالایی از اخبار طبقه‌بندی‌شده در سیستم‌های ارتباطاتی گوناگون انتقال یافته و در مراکز نظامی و غیرنظامی سرتاسر جهان مورد استفاده قرار می‌گیرند. حفاظت از چنین جریانی علیه دسترسی غیرمجاز کارکرد «امنیت ارتباطات»[۴۸] است. ظهور شبکه‌های اجتماعی نیز این چتر حفاظتی را فراتر از حفاظت از تکه‌های کاغذ یا امواج کرده است. در این رابطه، اصطلاح «امنیت خبری»[۴۹] هر دو مقوله امنیت ارتباطات و و «امنیت کامپیوتری»[۵۰] را پوشش می‌دهد (Clark, 2007: 72).

حفاظت فیزیکی[۵۱]: خواه با اخبار طبقه‌بندی‌شده سروکار داشته باشیم یا نه، نمودهای امنیت فیزیکی را هر روزه در اطراف خود شاهد هستیم. بسیاری از موانع نظیر حصارها، درب‌ها، حفاظ‌ها، کارت‌های شناسایی، دستگیره‌های درب کارت‌خوان[۵۲] و اسکنرهای شبکیه چشم که مردم برای ورود به برخی تأسیسات با آن‌ها روبرو می‌شوند، همگی تمهیداتی در راستای امنیت فیزیکی هستند. چنین اقداماتی به‌دنبال ایجاد دیواری حول اسرار و اخبار بوده و از تلاش‌های ضداطلاعاتی پشتیبانی می‌کند (Clark, 2007: 73).

حفاظت پرسنلی[۵۳]: سازمان‌های مرتبط با امنیت ملی همواره به‌دنبال استخدام کسانی هستند که وفادار، قابل اعتماد و ثابت‌قدم باشند. متقاضیان استخدام ابتدا باید مانع دریافت تأئیدیه امنیتی[۵۴] را کسب کنند که نیازمند تحقیق و گزینشی کامل است (Clark, 2007: 75-76).

اقدام پنهانی نیز اصطلاحی کلی برای فعالیت‌هایی است که بدان‌وسیله سیاست امنیت ملی به‌طور سری و مخفیانه صورت می‌پذیرد. از مدت‌ها قبل چنین شیوه‌ای مورد استفاده بوده و به اقداماتی ارتباط پیدا می‌کند که عامل آن

45. Sensitive Compartmented Information (SCI)
46. sensitive but unclassified
47. communications security
48. communications security (COMSEC)
49. information security (INFOSEC)
50. computer security (COMPUSEC)
51. physical security
52. swipe-card lock
53. personnel security
54. security clearance

مشخص نیست. هرچند عملیات‌های پنهانی در معنای اطلاعات عمومی، اطلاعاتی محسوب نمی‌شوند، ولی در دوران مدرن تا حد زیادی ازسوی «سازمان‌های اطلاعاتی»[55] انجام پذیرفته است. این بدان دلیل است که سازمان‌های مذکور اساساً عملیات‌های خود را به‌صورت پنهانی انجام داده و از امکانات مورد نیاز برای انجام چنین فعالیت‌هایی برخوردارند (Clark, 2007: 1).

نفوذ و ماهیت سیاست جهانی

در مورد جایگاه نفوذ در نوشته‌های مرتبط با «سیاست جهانی»[56] باید به دو نکته توجه داشت. نخست آنکه، تفکر سنتی در مورد سیاست بین‌الملل بر تفاوت‌های میان دوران جنگ و دوران جنگ صلح تأکید دارد. حقوق بین‌الملل نیز نقش کانونی جاسوسی در گردآوری اطلاعات در دوران جنگ را مورد تصدیق قرار می‌دهد. به‌لحاظ تاریخی، «اعلامیه بروکسل»[57] در سال ۱۸۷۴، جاسوسی را شیوه‌ای قانونی از جنگ در نظر گرفته بود. ماهیت منحصر به‌فرد آن نیز مورد تأیید قرار گرفته است. برای مثال، جاسوسان[58] باید در هنگام جاسوسی دستگیر شده و اگر جاسوسی به کشور خود فرار کند، دیگر جاسوس به‌حساب نمی‌آمد. این از مقوله مجرم[59] نفوذی که تا زمان دستگیری همچنان نفوذی باقی می‌ماند، متفاوت است. با این‌حال، اگر جاسوسی در هنگام جاسوسی بازداشت گردد، «حقوق بین‌الملل از نفی حقوق و مزایای مشخص فردی برای آن جاسوس حمایت می‌کند، حال آنکه چنین حقوقی برای افراد مجرم یا نفوذی پذیرفته شده است». وضعیت جاسوسی در دوران صلح کمتر از دوران جنگ مشخص است. برخی صاحب‌نظران حقوق بین‌الملل جاسوسی در دوران صلح را غیرقانونی می‌دانند، زیرا نقض حاکمیت و استقلال سیاسی دولت‌ها است. در مقابل، برخی دیگر آن‌را به‌لحاظ اخلاقی، سیاسی و حقوقی، فعالیتی قابل قبول می‌دانند (Hastedt, 2010: xix).

تمایز میان جاسوسی و نفوذ در دوران جنگ و صلح، در حال از دست دادن اهمیت نظری و عملی خود است. اعلام رسمی جنگ بی‌مورد شده است. جنگ جهانی دوم آخرین جنگ اعلام‌شده‌ای بود که ایالات متحده در آن مشارکت داشت. جنگ کره، جنگ ویتنام، جنگ خلیج فارس، جنگ عراق، عملیات‌های حفظ صلح در کوزوو و لبنان، گرانادا و جنگ علیه تروریسم، همگی بدون اعلام جنگ صورت گرفتند. از بُعد عملیاتی، مرز میان صلح و جنگ در حال از بین رفتن است. در خلال جنگ سرد، ایالات متحده و اتحاد شوروی خودشان را در وضعیتی غیرجنگی می‌دیدند، ولی این وضعیت شامل رقابت نظامی، سیاسی و دیپلماتیک می‌شد. سیاست‌های خارجی بسیاری از کشورهای کوچک‌تر،

55. intelligence organizations
56. World Politics or international politics
57. Declaration of Brussels
58. Spies (s. spy)
59. criminal

به‌خصوص آن‌هایی که در جنگ‌های رقابتی نظیر جنگ میان دو هند و پاکستان گیر کرده‌اند نیز تمایزی میان جنگ و صلح را ایجاد نمی‌کند.

در هیچ جایی همچون جنگ علیه تروریسم، مرز میان جنگ و صلح این‌قدر مبهم نیست. همان‌طور که حوادث یازده سپتامبر ۲۰۰۱ نشان داد، سیاست‌گذاری موفق ضدتروریستی به اطلاعات بستگی دارد، ولی گردآوری و تحلیل اطلاعات که منتظر نمی‌ماند تا اقدام تروریستی صورت گیرد. بلکه باید پیش از آن و در دوران صلح صورت گیرد (Hastedt, 2010: xx).

دوم اینکه، جاسوسی ازسوی سیاست‌گذاران به‌عنوان شیوه‌ای از کاهش مخاطرات همراه با غافلگیری دیپلماتیک و نظامی دارای ارزش است. به‌هرحال، نفوذ به‌خودی خود در سیاست جهانی اهمیت چندانی ندارد. نفوذ زمانی اهمیت دارد که فرضیات اساسی زیربنای سیاست‌ها را بی‌اعتبار سازد. در انجام چنین کاری، نفوذ به‌عنوان عاملی در افزایش قدرت، به‌طور چشمگیری میزان قدرت در اختیار دولتی که دست به نفوذ می‌زند را افزایش می‌دهد. (Hastedt, 2010: xx)

جلوگیری از نفوذ کار آسانی نیست، زیرا علل نفوذ متعدد است. نخست آنکه، دولت‌ها سعی خواهند کرد اقداماتشان را پنهان ساخته و از این‌رو درگیر فریب می‌شوند. دوم اینکه، دولت‌ها تلاش می‌کنند تکه‌های مهم اطلاعات را از مجموعه‌ای درهم و برهم از اطلاعات بی‌معنی به‌دست آورند. در اینجا دشمن تلاش می‌کند با ارائه اطلاعات بسیار زیاد، سردرگمی ایجاد کند. (Hastedt, 2010: xx)

نفوذ شیوه‌ای مهم از تلاش برای جلوگیری از غافلگیری راهبردی کشور عامل است. زیرا فرصتی را در اختیار سیاست‌گذاران قرار می‌دهد تا به‌دقت نیات و توانایی‌های واقعی دشمن را شناسایی کند. در عین‌حال می‌تواند مانع فریب خود نیز شود. به این دلایل، بعید است که شاهد از بین رفتن همیشگی نفوذ باشیم. هرچند خطر شکست بسیار زیاد بوده و شمار موفقیت‌ها از شکست‌ها در این زمینه کمتر باشد، ولی سیاست‌گذاران بازهم آن‌را ارزشمند می‌دانند. با این‌حال، نفوذ راه حل دائمی مشکل غافلگیری نیست. (Hastedt, 2010: xx)

نفوذ و چرخه اطلاعاتی

جاسوسی به‌طور مجاز صورت نمی‌گیرد، بلکه بخشی از مجموعه گسترده‌تری از فعالیت‌ها است که برای آگاهی‌بخشی به سیاست‌گذاران در مورد جهان اطراف آن‌ها انجام می‌شود. این فعالیت‌ها به‌طور کلی اشاره به «چرخه اطلاعاتی»[۶۰] دارند. (Hastedt, 2010: xx)

60. intelligence cycle

نخستین گام در چرخه اطلاعاتی مشخص کردن وظیفه است. در اینجا سیاست‌گذاران و مقامات ارشد اطلاعاتی تعیین می‌کنند که به چه اطلاعاتی برای انجام مأموریت‌هایشان و حصول به اهداف سیاسی نیاز دارند. گام دوم در فرایند اطلاعاتی گردآوری است. دراینجاست که جاسوسان و مخبران وارد چرخه اطلاعاتی می‌شوند. این یکی از شیوه‌های کسب اطلاعات مهم در مرحله نخست است. جامعه اطلاعاتی کشور طیف گسترده‌ای از استراتژی‌های گردآوری را برای انتخاب از میان آن‌ها در اختیار خود دارد. یکی از اصلی‌ترین انتخاب‌ها به انتخاب میان «اطلاعات باز»[۶۱] و «اطلاعات پنهان»[۶۲] مربوط می‌شود. اطلاعات باز، اطلاعاتی در دسترس همگان است. نفوذی برای کسب اطلاعات پنهان مورد استفاده قرار می‌گیرد. انتخاب اساسی دیگر به انتخاب میان «نفوذی فنی»[۶۳] و «نفوذ کلاسیک انسانی»[۶۴] ارتباط پیدا می‌کند. نفوذ فنی تا حد زیادی بر ماهواره‌ها، هواپیماها و تجهیزات الکترونیک برای پی بردن به توانایی‌های دشمن و رهگیری ارتباطات انسانی آن تکیه دارد. اما نفوذ انسانی به‌دنبال دسترسی به عکس‌ها، اسناد و دیگر موارد برخوردار از ارزش اطلاعاتی به‌طور مستقیم با نفوذ به سازمان‌های کلیدی است. (Hastedt, 2010: xxi)

گام سوم در چرخه اطلاعاتی پردازش و ارزیابی اطلاعات به‌دست آمده است. اطلاعات عمومی تنها زمانی به اطلاعات تبدیل می‌شوند که مورد ارزیابی و سنجش قرار گیرند. ارزیابی اطلاعات شامل دو نوع قضاوت است. نخست،آن منبع تا چه اندازه قابل اعتماد است. دوم اینکه اطلاعات مذکور تا چه اندازه مناسب هستند. اعتماد در مورد ارزش اطلاعات تحت بررسی با گزارش همان اطلاعات از منابع متعدد افزایش می‌یابد. برای تقویت اعتماد به اطلاعاتی که سازمان‌های اطلاعاتی در حال کار با آن هستند، از روش‌های گردآوری چندگانه (عوامل نفوذی، ماهواره‌های نظامی، وابستگان نظامی و غیره) برای کسب اطلاعات مشابه استفاده می‌کنند.

مراکز ضدنفوذ در این مرحله وارد چرخه اطلاعاتی می‌شوند. عملیات‌های ضدنفوذ با جستجوی فعال برای یافتن نفوذی‌ها و حفاظت از اسرار و اطلاعات خودی، کمکی به افزایش اعتماد تحلیل‌گران و مصرف‌کنندگان اطلاعاتی دریافتی هستند. به‌طور متناقض، عملیات ضدنفوذ همچنین می‌تواند تأثیر معکوسی نیز داشته باشد. زیرا می‌تواند با ایجاد تردید در وفاداری همه و اطلاعات ارائه‌شده، تحلیل اطلاعاتی را فلج سازد. وقتی چنین فضایی از تردید ازسوی ذهنیت‌های توطئه‌نگر مراکز ضدنفوذ ایجاد گردد، مشکلاتی ایجاد می‌شود که رهایی از آن‌ها بسیار سخت می‌گردد.

مرحله چهارم در چرخه اطلاعاتی، تحلیل[۶۵] و تولید[۶۶] است. دراینجا تکه‌های مجزای اطلاعات گردآوری‌شده و ارزیابی‌شده در کنار یکدیگر قرار گرفته و به‌عنوان اسناد نهایی در اختیار سیاست‌گذاران گذارده می‌شود. مرحله نهایی

61. open-source information
62. secret information
63. technological espionage
64. Classic human espionage
65. analysis
66. production

در چرخه اطلاعاتی، مرحله بازخورد[67] است که در آن سیاست‌گذاران به اطلاعات دریافتی واکنش نشان می‌دهند. در ادامه فرایند چرخه اطلاعاتی دوباره از سر گرفته می‌شود. هرچند برای فهم بحث این فرایند را به‌آسانی از یکدیگر جدا می‌کنیم، ولی در جهان واقعی ممکن است این مراحل به‌طور منظم پشت سر هم روی ندهد و همپوشانی‌هایی با یکدیگر داشته باشند.(Hastedt, 2010: xxi)

کنترل و اشراف بر نفوذ

چالش همیشگی سیاست اطلاعاتی انجام پنهانی فعالیت‌های اطلاعاتی و کنترل آن است. نقطه شروع سنتی در تفکر راجع به کنترل فعالیت‌های پنهانی، تصویب قوانینی در این زمینه و نظارت مجلس بر این فعالیت‌ها است. با این‌وجود، واقعیت آن است که قانون‌گذاران نیز خود چندان تمایلی برای تصویب قوانین مرتبط با چگونگی انجام نفوذ، ضدنفوذ، اقدامات پنهانی و تحلیل اطلاعاتی ندارد ولی در مقابل اصرار دارد که از مسائل کلی آگاه بوده و ازسوی جامعه اطلاعاتی گزارش دریافت کند. (Hastedt, 2010: xxii)

نظارت ریاست‌جمهوری کشورها بر این مقوله نیز مشکلات خاص خود را دارد. برنامه‌های فشرده، زمان محدود و علاقه اندک همگی موجب غفلت از این حوزه می‌شود. حتی رؤسای جمهور علاقه‌مند به موضوعات اطلاعاتی نیز چندان علاقه‌ای به جزئیات عملیات‌های جاسوسی و نفوذ نداشته‌اند. به‌علاوه، از آنجایی‌که عملیات‌های نفوذ شامل فعالیت‌های فریب و خیانت می‌شود، بنابراین رئیس‌جمهور نیز نباید از تمامی جزئیات این‌گونه عملیات‌ها آگاهی داشته باشد. در این زمینه «**انکار مشروع**»[68] عبارتی ارزشمند در کارهای اطلاعاتی است که به سیاست‌گذاران اجازه می‌دهد در مورد خطای صورت‌گرفته در عملیات‌ها خود را به نادانی بزنند. با این‌حال، هرچه بیشتر رؤسای جمهور و قانون‌گذاران درگیر عملیات‌های نفوذ شوند، توسل به چنین ادعایی برای آن‌ها دشوارتر خواهد بود (Hastedt, 2010: xxiii) .

ضدنفوذ

هدف نهایی ضدنفوذ، حفاظت از اسرار بوده و اساساً نیازمند آگاهی از انگیزه نفوذی‌ها، رویه‌های عملیاتی آن‌ها و اهدافشان است. سابقه تاریخی بیانگر آن است که انگیزه نفوذی‌ها به عواملی ارتباط پیدا می‌کند که به یک کشور یا دوره خاص زمانی منحصر نمی‌شود. یکی از این انگیزه‌ها **باج‌خواهی**[69] است. چنین رویه‌ای به‌کرات ازسوی شوروی در یافتن جاسوسان جدید استفاده می‌شد. ارتباطات جنسی و روابط غیرقانونی یکی از شایع‌ترین انواع باج‌خواهی برای

67. feedback
68 .Plausible denial
69. blackmail

نفوذ بوده است. انگیزه دیگر **پول** است. در این زمینه، حتماً به مقادیر زیاد پول نیاز نبوده و غالباً تنها میزانی کم برای تحریک کسی به جاسوسی و نفوذ کافی بوده است. در حقیقت، پرداخت پول‌های زیاد به جاسوسان خود عامل خطرناکی است، زیرا توجه تشکیلات امنیتی آن کشور را حساس می‌کند. انگیزه سوم **ایدئولوژی** است. برخی از نفوذی‌ها دارای انگیزه‌های سیاسی هستند. آن‌ها بر این باورند که عملشان صحیح بوده و قضاوت خائنانه در مورد آن ندارند. در نهایت، برخی از نفوذی‌ها دارای مجموعه‌ای پیچیده از نیازهای روانی همچون جاه‌طلبی، قدرت، خشم و ماجراجویی هستند. (Hastedt, 2010: xxiii)

نفوذ و اقدامات پنهانی

تعریف

فعالیت‌های اطلاعاتی کلاسیک پشتیبانی از سیاست و برنامه‌های آن بوده و کاری به سیاست‌گذاری یا فعالیتی که مستلزم اقدام عملی باشد، نداشت. با این‌حال، حوزه‌ای در ساختار اطلاعاتی وجود دارد که ویژگی عملی داشته و ماهیتی ابزاری دارد: بهره‌گیری از «اقدام پنهانی و نفوذ»[۷۰] که جنجالی‌ترین بخش در میان تمامی کرکردهای اطلاعاتی است. اقدام پنهانی در اساس بیانگر تلاش برای تأثیرگذاری روی مسائل داخلی کشورها یا گروه‌های دیگر بوده و در همان حال سعی دارد از انتساب چنین اقداماتی به دولت مطبوع خود اجتناب گردد. هدف نیز انجام کارهایی است که در ظاهر برای منطقه هدف آشکار و بومی است، به‌گونه‌ای که دست محرک واقعی به‌هیچ‌وجه مشخص نبوده و در حقیقت می‌تواند آن‌را انکار کند(Clark, 2007: 92).

به‌لحاظ سنتی، اقدامات پنهانی[۷۱] که همچنین به «فعالیت‌های ویژه»[۷۲] نیز معروف هستند، شامل هرنوع عملیاتی با هدف تأثیرگذاری روی دولت‌ها، افراد یا تحولات خارجی در راستای حمایت از اهداف سیاست خارجی دولت خود و در همان حال پنهان نگه داشتن حمایت دولتی از این عملیات می‌شود. در حالی که در گردآوری پنهانی تأکید روی محرمانه نگه‌داشتن فعالیت است، در نفوذ تأکید بر روی محرمانه نگه‌داشتن حمایت دولت است(Richelson,2008: 3).

«قانون اختیارات اطلاعاتی»[۷۳] سال ۱۹۹۱، اقدام پنهانی و نفوذ را به‌عنوان «فعالیت یا فعالیت‌هایی ازسوی دولت برای تأثیرگذاری بر شرایط سیاسی، اقتصادی یا نظامی در خارج» تعریف می‌کند، «جایی‌که قصد بر آن است تا نقش دولت ایالات متحده آشکار نباشد» (Clark, 2007: 92).

70. covert action (CA)
71. covert action(s)
72. special activities
73. Intelligence Authorization Act of 1991

این قانون در عین‌حال موارد زیر را شامل اقدام پنهانی نمی‌داند: (۱) فعالیت‌هایی که هدف از آن‌ها کسب اطلاعات، فعالیت‌های ضداطلاعاتی، فعالیت‌های سنتی برای بهبودبخشی با حفظ امنیت عملیاتی برنامه‌های دولت ایالات متحده یا فعالیت‌های اداری؛ (۲) فعالیت‌های دیپلماتیک یا نظامی سنتی یا پشتیبانی مرسوم از چنین فعالیت‌هایی؛ (۳) فعالیت‌های مرتبط با اجرای قانون ازسوی آژانس‌های مربوطه یا پشتیبانی مرسوم از چنین فعالیت‌هایی؛ و (۴) فعالیت در راستای پشتیبانی مرسوم از فعالیت‌های آشکار در خارج از کشور. این قانون همچنین تصریح می‌کند که هیچ نوع اقدام نفوذی با هدف تأثیرگذاری روی فرایندهای سیاسی، افکار عمومی، سیاست‌ها یا رسانه‌های کشور نباید صورت گیرد (Clark, 2007: 92).

هرچند عملیات‌های نفوذ در اساس اطلاعاتی محسوب نمی‌شوند، ولی در دوران مدرن تا حد زیادی ازسوی سازمان‌های اطلاعاتی صورت می‌گیرند. این بدان دلیل است که آژانس‌های اطلاعاتی سازمان‌هایی دولتی هستند که می‌توانند به‌طور مخفی و سری کار کرده و از توانایی‌های لازم برای انجام چنین فعالیت‌هایی برخوردارند (Clark, 2007: 93).

انجام این نوع اقدامات سابقه‌ای طولانی دارد، ولی اصطلاح «اقدام پنهانی» مربوط به دوران مدرن بوده و ریشه در فعالیت سازمان‌های اطلاعاتی آمریکا دارد. برخی کشورها نیز از عبارات دیگری استفاده می‌کنند که به‌هرحال در عمل ماهیت مشابهی با اقدام پنهانی دارند. برای مثال انگلیسی‌ها از «**اقدام سیاسی ویژه**»[۷۴] و روس‌ها از «**اقدامات فعال**»[۷۵] برای اشاره به این نوع فعالیت‌ها استفاده می‌کنند. اقدام پنهانی در عین‌حال واژه‌ای است که برای اشاره به فعالیت‌هایی است که بدان طریق سیاست‌ها به‌صورت مخفیانه به اجرا درمی‌آیند. این نوع اقدامات را می‌توان در طیفی از فعالیت‌های کم‌خطر و کم سروصدا برمبنای اقناع[۷۶] تا پُرخطر و پُر سروصدا که متضمن استفاده از زور است، قرار داد. با توجه به انعطاف‌پذیری زیاد آن، اقدام پنهانی غالباً به‌عنوان راهی برای فراهم آوردن گزینه‌های بیشتر پیش روی سیاست‌گذاران میان گفت‌وگو (دیپلماسی) یا مقابله (جنگ) در تلاش برای حفاظت از منافع ملی دیده می‌شود. از آن نیز به‌عنوان «**راه سوم**»[۷۷] یا «**راه خاموش**»[۷۸] نام می‌برند (Clark, 2007: 93).

در ایالات متحده، مسئولیت انجام اقدامات پنهانی بر عهده سازمان سیا است؛ نهادی که طبق قانون امنیت ملی سال ۱۹۴۷، مدیرکل آن مسئولیت انجام این‌گونه عملیات‌ها را بر عهده دارد (Johnson, 2007). به‌طور مشخص نیز می‌توان گفت که تمامی رؤسای جمهور آن از ترومن تاکنون از اقدامات نفوذی سازمان سیا برای دخالت در امور داخلی دیگر

74. special political action
75. active measures
76. persuasion
77. third option
78. quiet option

کشورها استفاده کرده‌اند. البته برخی از آن‌ها همچون جان اف کندی و رونالد ریگان بیش از دیگران چنین شیوه‌هایی را به کار گرفته‌اند. در این میان برخی همچون بیل کلینتون تمایل چندانی به استفاده از این حربه نداشتند. افرادی مانند جیمی کارتر و باراک اوباما نیز همواره نسبت به چنین تکنیک‌هایی در مدیریت امور دولتی انتقاد می‌کنند. با این‌حال، در نهایت تمامی آن‌ها دلایل و بهانه لازم برای توسل به چنین اقداماتی را پیدا می‌کردند. از سال ۱۹۴۷ تا ۱۹۷۴ اقدامات پنهانی تقریباً به‌طور انحصاری موضوعی میان رؤسای جمهور و سیا قلمداد می‌شد. پس از سال ۱۹۷۴ و تا دهه ۱۹۹۰، نظارت کنگره و مداخله آن در موضوعات اطلاعاتی به‌طور کلی - و اقدامات پنهانی به‌طور خاص – افزایش یافت (Clark, 2007: 97).

انواع اقدامات پنهانی و نفوذ

انواع مختلفی از اقدام پنهانی و نفوذ وجود دارد: **تبلیغات سیاسی**[۷۹]: **تبلیغات سیاه**[۸۰] (تبلیغاتی که وانمود می‌شود از منبعی غیر از منبع حقیقی می‌باشد)، **تبلیغات خاکستری**[۸۱] (که در آن پشتیبان اصلی شناخته نمی‌شود) و **تبلیغات سفید**[۸۲] (دستکاری اطلاعات پخش‌شده در رسانه‌ها بدون پنهان‌کردن منشاء آن‌ها)؛ اقدامات **شبه‌نظامی**[۸۳] یا سیاسی با هدف سرنگونی، تضعیف یا حمایت از یک رژیم؛ اقدامات شبه‌نظامی یا سیاسی با هدف مقابله با تلاش‌های یک رژیم برای دستیابی یا ساخت تسلیحات پیشرفته؛ **حمایت** (کمک اقتصادی، نظامی و آموزشی) از اشخاص یا سازمان‌ها (بخش‌های دولتی، احزاب سیاسی، اتحادیه‌های کارگری و مراکز انتشاراتی)؛ **عملیات‌های اقتصادی**؛ ارائه **اطلاعات گمراه‌کننده**؛ و **ترور** (Richelson, 2008: 3). با این‌حال، تمامی اشکال مذکور می‌توانند در یک عملیات به‌کار گرفته شوند. تکنیک‌های «جنگ اطلاعاتی»[۸۴] ابزاری جدید هستند - یا شاید نوع چهارم - که در سال‌های اخیر به گزینه‌های در دسترس در اقدام نفوذ و پنهانی افزوده شده‌اند. همچون حوزه گسترده اقدام پنهانی، جنگ اطلاعاتی نیز طیفی از استفاده‌ها را دارد که از حداقل تهاجم تا حداکثر تهاجم و اختلال قرار می‌گیرد (Clark, 2007: 93).

79. propaganda
80. black propaganda
81. gray propaganda
82. white propaganda
83. paramilitary (PM)
84. information warfare

تبلیغات سیاسی

بر روی طیف اقدام پنهانی، تبلیغات در انتهای حداقل تهاجم قرار می‌گیرد. **یک نبرد تبلیغاتی در ساده‌ترین شکل می‌تواند پرداخت پول به یک روزنامه‌نگار در کشور هدف برای نگارش مقالاتی در جهت حمایت از سیاست‌های مورد نظر کشور پرداخت‌کننده پول باشد.** با این‌حال، اوضاع به این صورت هم خیلی ساده نیست. حتی یک نبرد تبلیغاتی سطح پائین نیازمند تعیین هدف، هدایت فرایند برای تضمین از پیروی سیاست‌ها و آمادگی لازم است. در اکثر موارد نیز نیازمند افرادی است که قادر به درک نیازها و انجام آن‌ها هستند. **نبردهای تبلیغاتی فعالیت‌هایی خلق الساعه نیستند، بلکه به تماس‌هایی بلندمدت نیاز است.** این بخشی از زیرساخت هر عملیات اقدام پنهانی و نفوذ است که باید در طی زمان صورت گیرد (Clark, 2007: 93-94).

همان‌طور که گفتیم دو نوع تبلیغات وجود دارد: تبلیغات سیاه و تبلیغات خاکستری. در تبلیغات سیاه که همچنین به «اطلاعات گمراه‌کننده»[۸۵] معروف است، مطالب به‌نظر حقیقی می‌آیند، اما ممکن است به‌طور کامل اشتباه باشند و اینکه منشاء آن گروه یا شخصی شناخته‌شده باشد، اما در واقع ازسوی فرد یا گروه دیگری تولید شده است. در زمان جنگ سرد هر دو بلوک غرب و شرق از این شیوه به‌وفور علیه یکدیگر استفاده می‌کردند. برای مثال، اتحاد جماهیر شوروی این باور را ایجاد کرده بود که ویروس ایدز در آزمایشگاه‌های کشور آمریکا ایجاد شده‌اند (Clark, 2007: 94).

تبلغیات سیاه غالباً برای کاهش روحیه نیروهای دشمن یا ایجاد اختلال در عملیات‌ها یا فعالیت‌های عادی آنان مورد استفاده قرار می‌گیرد. برای نمونه، در خلال جنگ کره (۲۵ جون ۱۹۵۰ تا ۲۷ جولای ۱۹۵۳)، سیا دست به جعل اسناد و فرامین نظامی چین زد. سپس مأموران سیا آن‌ها را وارد شبکه فرماندهی چین کرده و موجب گمراهی سربازان چینی را فراهم ساختند (Smith, 2003: 31).

در تبلیغات خاکستری نیز سعی در آن است که عامل اصلی نفوذی خاص شناخته نشود. برای نمونه پس از شکست در تهاجم مورد حمایت سیا در خلیج خوک‌ها[۸۶] در سال ۱۹۶۱ علیه کوبا، رادیو صدای آمریکا[۸۷] هر نوع دست داشتن آمریکا در این تهاجم را رد کرد. دائره المعارف اطلاعاتی سیا نیز تبلیغات خاکستری را اطلاعاتی در رسانه‌ها می‌داند که شناسایی منبع نفوذی خاص را مشکل سازند- برخلاف تبلیغات سیاه که منبع اساساً نامشخص است- (Smith, 2003: 113).

تبلیغات سفید نیز اشاره به اطلاعات دستکاری شده‌ای در رسانه‌ها دارد که تلاشی برای پنهان کردن منشاء آن صورت نمی‌گیرد (Smith, 2003: 244). در واقع، این نوع تبلیغات از منبعی می‌آید که به‌درستی شناخته شده است و

85.disinformation
86. Bay of Pigs
87 .The Voice of America (VOA)

اطلاعات در پیام نیز در ظاهر درست به‌نظر می‌آید. رادیو صدای آمریکا مثال خوبی از یک واحد تبلیغات سفید است، زیرا سعی دارد تصویری مثبت را از ایالات متحده نشان دهد. هرچند صدای آمریکا ارتباطی با ارتش ندارد، ولی نیروهای مسلح معمولاً از این رادیو برای تخریب اراده نیروهای دشمن برای مقاومت استفاده می‌کند. در زمان جنگ خلیج فارس در سال ۱۹۹۱، «گروه چهارم عملیات روانی»[88] ایالات متحده مبادرت به تهیه یک برنامه رادیویی تبلیغات سفید کرد که در آن از خوشحالی اسرای عراقی حرف زده شده، تلاوت آیه‌هایی از قرآن پخش می‌شد و به مکان اهداف بمباران روز بعد اشاره می‌گردید. پس از این حملات، بسیاری از فراریان عراقی عنوان می‌کردند که برنامه‌های مذکور تأثیر زیادی در تصمیم آن‌ها برای تسلیم داشته است. تبلیغات سفید سعی دارد با متقاعد کردن مخاطب به نیات خوب ارسال‌کننده پیام‌ها، اعتماد آن‌ها را جلب کند (Lerner & Lerner, 2004**b**: 450).

عملیات‌های فریب و نفوذ

«عملیات‌های فریب»[89] با هدف مقابله با یک تصمیم‌گیرنده مشخص با استفاده از واقعیتی نادرست یا گمراه ساختن دشمن با دستکاری، تحریف یا جعل شواهد برای ایجاد برداشتی اشتباه و نادرست صورت می‌گیرد. در سال ۱۹۹۱، حضور نیروی عظیمی از تفنگداران دریایی آمریکا در ساحل کویت این باور را در صدام حسین ایجاد کرد که آمریکا قصد دارد از این جهت و نه غرب حمله **کند** (Daugherty & Bowden, 2006: 79).

قبل از اینکه بتوان عملیاتی فریب را آغاز کرد، باید برنامه‌ای دقیق و منسجم داشت، به‌طوری‌که عنصر فریب موجب تقویت این برنامه گردد. پس از آن، عملیات واقعی فریب نیازمند توجه زیاد به جزئیات در دوره‌ای بلندمدت است، وضعیتی که به‌ناچار نیازمند سرمایه‌گذاری عظیم در نیروی انسانی و منابع دیگر در کشور (یا کشورهای) هدف برای کسب بازخورد نسبت به پیامدهای عملیات است. در این تلاش‌ها، یک‌پارچگی کامل عملیات فریب در برنامه کلی و حمایت از آن توسط دیگر اجزا که مسئولیت مقابله با گردآوری اطلاعات ازسوی دشمن را برعهده دارند، از اهمیت خاصی برخوردار است (Daugherty & Bowden, 2006: 80).

مسئله مهم دیگر در عملیات فریب **اطمینان از رسیدن مطالب و اطلاعات فریب‌آمیز به سیاست‌گذاران و سرویس‌های اطلاعاتی هدف و تأیید صحت آن‌ها** است. در این صورت، می‌توان از کارایی عملیات نیز اطمینان حاصل کرد (Daugherty & Bowden, 2006: 81).

88. Fourth Psychological Operations Group
89. deception operations

اقدام سیاسی و نفوذ

فعالیت‌هایی که در چارچوب اقدام سیاسی قرار می‌گیرند، به‌لحاظ تهاجمی بودن فراتر از تبلیغات هستند، اما در اینجا نیز از زور استفاده نمی‌شود. در این رابطه شیوه‌های متعددی وجود دارد که برخی تهاجمی‌تر از دیگری هستند. برای مثال می‌توان به تأمین مالی و مشاوره در مبارزات سیاسی، حمایت از انواع مختلف گروه‌های فرهنگی و مدنی، کمک مالی به اعتصابات کارگری و دیگر انواع تظاهرات، ایجاد شرایط نابسامان اقتصادی و کمک به وقوع کودتا برای سرنگونی دولتی مستقر اشاره داشت. یاری رساندن به دولت‌ها یا گروه‌های دیگر برای افزایش تونمندی‌های اطلاعاتی خود شکل دیگری از اقدام سیاسی است. کمک اطلاعاتی شامل ارائه آموزش‌های تخصصی به پلیس محلی، شبه‌نظامیان و پرسنل اطلاعاتی؛ یا ارسال تجهیزات فنی (همچون ایجاد توانمندی اطلاعات سیگنالی برای یک سرویس خارجی) یا دیگر موارد می‌شود. بسیاری از فعالیت‌های مرتبط با اقدام سیاسی متضمن تأمین مالی و مشاوره به گروه‌ها یا اشخاص مختلف در راستای کمک به آن‌ها در انجام کاری (نظیر پیروزی در انتخابات) است که خواهان آن هستند، اما فاقد منابع لازم برای انجام آن می‌باشند. کلید اصلی در اینجا تطابق دستاورد آن‌ها با منافع طرف کمک‌کننده است. بسیاری از عملیات‌های مرتبط با اقدام سیاسی همچنین با نبردهای تبلیغاتی با هدف تقویت تأثیرات دیگر فعالیت‌ها پشتیبانی می‌شوند (Clark, 2007: 94).

اقدامات شبه‌نظامی و نفوذ

در انتهای دیگر طیف اقدام پنهانی از تبلیغات، عملیات‌های شبه‌نظامی وجود دارد – اقدامات از نوع نظامی با استفاده از پرسنل غیرنظامی. پس از جنگ جهانی دوم، اکثر مباحث در حوزه اقدامات پنهانی به فعالیت‌هایی همچون کمک به جنبش‌های مقاومت زیرزمینی، گروه‌های آزادی‌بخش چریکی و جنبش‌های بومی ضدکمونیست مربوط می‌شد. کمک اطلاعاتی در این زمینه می‌تواند به‌تدریج وارد حوزه اقدامات شبه‌نظامی شود، به‌گونه‌ای که آموزش شورشیان برای مقاومت راه را برای کمک به آن‌ها در برنامه‌ریزی و مشارکت در انجام عملیات‌ها هموار می‌سازد. در حقیقت، هرچه عملیات یک گروه شبه‌نظامی بزرگ‌تر باشد، کمتر می‌توان آن‌را اقدامی پنهانی نامید. در اکثر مواقع، فعالیت‌های گسترده شبه‌نظامیان ممکن است به‌طور رسمی مورد تأیید نباشد (Clark, 2007: 94).

نفوذ الکترونیک در جنگ اطلاعاتی و ضداطلاعاتی

استفاده از کامپیوتر شخصی، شبکه‌های ارتباطاتی و داده‌خانه‌های الکترونیک ازسوی سازمان‌های دولتی و نهادهای تجاری از هر نوع، سرگرمی تازه‌ای را برای افراد خلاق ایجاد کرده است، به‌گونه‌ای که با نشستن پشت کامپیوترهای

خود در منزل، به‌طور پنهانی وارد سیستم‌های کامپیوتری یا مراکز بزرگ داده سازمان‌های دولتی شده و فارغ از بُعد مسافت مبادرت به سرقت، تغییر و نابودی داده‌ها کرده یا اینکه به نزم‌افزارها یا سخت‌افزارهای هدف آسیب وارد می‌سازند (Daugherty & Bowden, 2006: 85-86).

وقتی چنین نفوذی ازسوی افرادی با ابتکار خود و به‌دلایلی که مدنظرشان است، صورت گیرد، اسم آن‌را «هک»[۹۰] می‌گذارند. هرچند در این رابطه تعاریف متفاوتی وجود دارد، ولی دستورالعمل شماره ۳۲۱۰.۰۱ رئیس ستاد مشترک آمریکا در تاریخ ۲ ژانویه ۱۹۹۶ آن‌را این‌گونه تعریف می‌کند: «اقدامات صورت‌گرفته برای کسب برتری اطلاعاتی با تأثیرگذاری بر اطلاعات دشمن، فرایندهای اطلاعات‌محور، سیستم‌های اطلاعاتی و شبکه‌های کامپیوترمحور و در همان حال دفاع از اطلاعات، فرایندهای اطلاعات‌محور، سیستم‌های اطلاعاتی و شبکه‌های کامپیوترمحور خودی» (Joint Operations Warfare Policy, 1996).

وزارت دفاع آمریکا با تمرکز بر حوزه نظامی، حملات اخبارمحور را شامل تلاش غیرمجاز برای کپی داده‌ها یا تغییر مستقیم داده‌ها یا دستورالعمل‌ها می‌داند. از این دید، جنگ اطلاعاتی چیزی بیش از کامپیوترها و شبکه‌های اجتماعی بوده و شامل عملیات‌هایی علیه اخبار در هر شکلی و در هر رسانه‌ای، ازجمله عملیات علیه محتوای خبری، سیستم‌ها و نرم‌افزارهای پشتیبانی‌کننده آن، سخت‌افزارهای فیزیکی مربوطه برای ذخیره آنان و نیز کارکردها و برداشت‌های انسانی می‌شود (Denning, 1999: 9-19).

دولت ژاپن قانونی را به تصویب رسانده که در آن هک یا «تروریسم سایبر»[۹۱] به‌عنوان «ورود غیرمجاز به سیستم‌های کامپیوتری ازطریق شبکه‌های ارتباطاتی... و آسیب رساندن به این سیستم‌ها به‌واسطه دسترسی غیرمجاز» تعریف شده است (Love, 1999: 205).

وقتی هک ازسوی ارتش یک کشور یا آژانس اطلاعاتی یا امنیتی دولتی خاص و در راستای اهداف امنیت ملی آن انجام شود، از اصطلاح «جنگ اطلاعاتی»[۹۲] استفاده می‌شود که علیه زیرساخت‌های دولتی، شبکه‌های برق و انرژی، نهادهای مالی و بانکی و رسانه‌ها و نیز زیرساخت‌های سازمان‌های غیرقانونی نظیر گروه‌های تروریستی و قاچاقچیان مواد مخدر به کار گرفته می‌شود (Daugherty & Bowden, 2006: 86).

جنگ اطلاعاتی همچنین برای توصیف حملات علیه دولت‌ها و نهادهای غیرنظامی ازسوی تروریست‌ها، گروه‌های جنایی و دیگر تشکیلات غیرقانونی مورد استفاده قرار می‌گیرد (برخلاف اشخاصی که برای تفریح یا سرگرمی دست به

90. hacking
91. cyberterrorism
92. information warfare

هک می‌زنند). خلاصه، آنچه هک را از جنگ اطلاعاتی متمایز می‌سازد عبارت از وابستگی (یا عدم وابستگی) شخص یا سازمان پشت این اقدام یا انگیزه آن‌ها برای انجام چنین اقدامی است (Daugherty & Bowden, 2006: 86).

وین شوارتاو[۹۳] از متخصصان مسائل امنیتی و ضدتروریسم، در کتاب «جنگ اطلاعاتی»[۹۴] سه دسته از این نوع جنگ را مورد توجه قرار می‌دهد:

جنگ اطلاعاتی فردی[۹۵]: حملات صورت‌گرفته علیه حریم خصوصی افراد در حوزه الکترونیک که شامل افشای سوابق دیجیتال و داده‌های آن‌ها می‌شود؛

جنگ اطلاعاتی شرکتی[۹۶]: رقابت یا جنگ میان شرکت‌ها در سرتاسر جهان؛ و

جنگ اطلاعاتی جهانی[۹۷]: جنگ علیه صنایع، نیروهای اقتصادی جهانی یا علیه کشورها یا دولت‌ها در سرتاسر جهان (Schwartau, 1994).

ازجمله تسلیحات جنگ اطلاعاتی نیز عبارتند از:

الف) حمله قطع سرویس

«حمله قطع سرویس»[۹۸]، «تهاجم به شبکه‌ای مشخص با ایجاد سیلی از درخواست‌ها است که موجب می‌گردد ترافیک معمولی کند شده یا به‌طور کامل قطع گردد.» ویژگی این حمله تلاش برای جلوگیری از استفاده کاربران از سرویس مشخصی است. یکی از مزایای این نوع حمله آن است که می‌تواند با منابع محدودی علیه یک کامپیوتر یا شبکه‌ای پیچیده‌تر و بزرگ‌تر مورد استفاده قرار گیرد. برای مثال، مهاجم می‌توان با یک کامپیوتر قدیمی و یک مودم با سرعت پائین، کامپیوترها و شبکه‌های پیشرفته‌تر و سریع‌تر را از کار بیندازد (Schaap, 2009: 134).

«حمله قطع سرویس توزیعی»[۹۹] نیز حمله‌ای است که در آن انبوهی از کامپیوترها و سیستم‌های آلوده، به یک سیستم دیگر حمله می‌کنند. وقتی چنین حمله‌ای صورت می‌گیرد، مهاجم از هزاران کامپیوتر آلوده – معروف به زامبی‌ها[۱۰۰] یا بوت‌ها[۱۰۱] – برای حمله هم‌زمان به یک سیستم مجزا بهره می‌گیرد. جلوگیری از حملات مذکور دشوار است، زیرا ایجادسیلی‌از داده‌ها علیه‌سیستم، از کامپیوترهای مختلف و مکان‌های گوناگون صورت می‌گیرد (Schaap, 2009: 134).

93 Winn Schwartau
94 Information Warfare
95 personal information warfare
96 corporate information warfare
97 global information warfare
98 Denial-of-Service (DoS) attack
99 Distributed Denial of Service (DDoS) attack
100 zombies
101 bots

«حمله دائمی قطع سرویس»[۱۰۲] نیز آنچنان خسارت بدی به یک سیستم وارد می‌سازد که نیازمند جایگزینی یا نصب دوباره سخت‌افزار خواهد بود. برخلاف حمله «حمله توزیع قطع سرویس» که برای خرابکاری در یک سرویس یا وب‌سایت مورد استفاده قرار می‌گرفت یا پوششی برای وارد کردن «بدافزار»[۱۰۳] محسوب می‌شود، این حمله نوعی خرابکاری سخت‌افزاری است (Schaap, 2009: 135).

ب) برنامه‌های مخرب

برنامه‌های مخرب[۱۰۴] با ایجاد اختلال در عملکردهای معمولی کامپیوتر یا ایجاد راهی برای یک مهاجم جهت در اختیار گرفتن کنترل آن کامپیوتر دست به حمله می‌زند. این نوع حمله می‌تواند یک کامپیوتر را از کار انداخته یا اینکه باعث شود در زمانی مشخص و طی فرمانی خاص، سیگنال‌هایی مخرب را ارسال کند که کامپیوترهای دیگر را مختل سازد. در این رابطه غالباً برای اشاره به برنامه‌های مخرب از واژه «بدافزار» استفاده می‌کنند. بدافزار می‌تواند فایل‌ها را پاک کرده یا اینکه آن‌ها غیرقابل استفاده سازد. ویروس‌ها، کرم‌ها[۱۰۵] و اسب‌های تروا[۱۰۶] نمونه‌هایی از بدافزارها هستند (Schaap, 2009: 135).

ویروس خود را به یک برنامه یا فایل چسبانده تا بتواند از یک کامپیوتر به کامپیوتر دیگر منتقل شود. ویروس با کپی‌کردن خود، در تمامی دیسک‌ها و شبکه‌ها پخش می‌شود. ویروس علاوه بر یک کد که توانایی کپی خود را به آن می‌دهد، دارای یک «بار»[۱۰۷] نیز است. مهاجمان سایبر می‌توانند بار مذکور را طوری برنامه‌ریزی کنند که تأثیرات جانبی مخربی نظیر تخریب یا نابودی داده‌ها را به‌همراه داشته باشد. تقریباً تمامی ویروس‌ها به یک فایل اجرایی[۱۰۸] می‌چسبند؛ بدین معنی که ویروس ممکن است در یک کامپیوتر باشد، اما تا زمانی‌که کاربر آن‌را اجرا یا باز نکرده، برنامه مخرب نمی‌تواند کاری انجام دهد (Schaap, 2009: 135-136).

کرم نیز همچون یک ویروس عمل می‌کند، به‌طوری که از یک کامپیوتر به کامپیوتری دیگر منتقل می‌شود. با این‌حال، برخلاف ویروس، این توانایی را دارد که بدون کمک کسی منتقل شود و این کار را نیز با استفاده از مشخصه‌های انتقال فایل یا اطلاعات در یک سیستم انجام می‌دهد. بزرگ‌ترین خطر کرم به توانایی آن برای کپی خود در یک سیستم مربوط می‌شود. بنابراین، به‌جای یک کرم می‌تواند صدها یا هزاران کپی از خود را منتقل کند. به‌دلیل توانایی کرم در کپی خود و سرایت در سرتاسر شبکه‌ها، نتیجه نهایی در اکثر موارد آن است که کرم فضای بسیاری را

102. Permanent Denial-of-Service (PDoS)
103. malware
104. malicious programs
105. worms
106. trojan horses
107. payload
108. executable file

در حافظه سیستم یا پهنای باند شبکه را اشغال کرده و عملکرد سرورهای وب، سرورهای شبکه و کامپیوترهای شخصی را متوقف می‌سازد. مهاجمان سایبر حملات کرمی اخیر را برای ورود به یک سیستم کامپیوتری طراحی کرده و به کاربران مخرب این امکان را می‌دهند که از راه دور کامپیوتر آلوده به کرم را کنترل کنند (Schaap, 2009: 136).

اسب تروا «برنامه‌ای حاوی کدی مخرب در داخل برنامه‌ها یا داده‌هایی ظاهراً سالم است که می‌تواند کنترل کامپیوتر مورد نظر را به‌دست گرفته و خساراتی را که می‌خواهد وارد سازد.» **آن‌هایی که یک اسب تروا را دریافت می‌کنند، معمولاً فریب خورده و آن‌را باز می‌کنند، زیرا به‌نظر می‌رسد آن فایل سالم بوده یا از منبعی سالم دریافت شده است.** اسب‌های تروا می‌توانند با پاک کردن فایل‌ها و نابودی اطلاعات موجود روی سیستم، خساراتی جدی را وارد سازند. در عین‌حال می‌توانند راهی پنهانی را به کامپیوترها باز کنند که به کاربران بدخواه امکان دسترسی به آن سیستم و اطلاعات محرمانه و شخصی موجود در آن‌را بدهد. برخلاف ویروس‌ها و کرم‌ها، اسب‌های تروا نمی‌توانند با آلوده کردن دیگر فایل‌ها و یا به‌صورت خودکار خود را کپی کنند (Schaap, 2009: 136).

تهدید ترکیبی[109] نیز «حمله‌ای پیچیده با استفاده از مجموعه‌ای ویروس‌ها،کرم‌ها، اسب‌های تروا و کده‌های مخرب» است. این نوع از نقاط آسیب‌پذیر سرورها و اینترنت برای حمله استفاده کرده و به‌سرعت گسترش یافته و خسارات فراوانی را به‌بار می‌آورند (Schaap, 2009: 136-137).

«بدافزار چندشکلی»[110] نیز «نرم‌افزاری مخرب با توانایی تغییر شکل خود در هر مرتبه از کپی» است. این تکنیک برای فرار از شناسایی توسط برنامه‌های ضدجاسوس‌افزار[111] است. در این بدافزارها، تنها ظاهر کد تغییر کرده و در عملکرد آن تغییری روی نمی‌دهد (Schaap, 2009: 137).

ج) بمب منطقی

بمب منطقی کدی مخرب است که در صورت وقوع حوادثی یا در زمانی از پیش تعیین‌شده اجرا می‌شود. وقتی که اجرا شود نیز می‌تواند کامپیوتر را از کار انداخته، داده‌ها را پاک کند یا با ایجاد تراکنش‌هایی ساختگی به یک «حمله قطع سرویس» (دی‌اُاِس) مبادرت ورزد (Schaap, 2009: 137).

د) جعل آی‌پی

«جعل آی‌پی»[112] تکنیکی برای ربودن است که طی آن رباینده‌گان به‌عنوان میزبانی مورد اعتماد خود را نشان می‌دهند تا هویتشان را پنهان ساخته، وب‌سایتی را جعل کرده، مرورگرها را بربایند یا به یک شبکه دسترسی پیدا کنند. وقتی از این

109. blended threat
110. polymorphic malware
111. anti-spyware programs
112. IP spoofing

شیوه برای ربودن یک مرورگر استفاده می‌شود، کاربری که در قسمت «مکان‌یاب واحد منبع» (یوآرال)[113] آدرس سایتی را تایپ می‌کند، به صفحه‌ای جعلی می‌رود که ازسوی رباینده‌گان ایجاد شده است. اگر کاربر با «محتوای پویا»[114] در یک صفحه جعلی کار کند، رباینده می‌تواند به اطلاعات حساس یا منابع کامپیوتر یا شبکه دسترسی پیدا کند (Schaap, 2009: 137).

ه) دستکاری دیجیتالی

«دستکاری تصویر دیجیتالی»[115] عبارت از تغییر یک تصویر با استفاده از ابزارهای برنامه‌های کامپیوتری یا نرم‌افزارهای مختلف برای ایجاد تصویری ساختگی است که برداشت متفاوتی از آن حاصل شود. در این تکنیک از تصاویر موجود همچون عکس‌ها و ویدئوها استفاده می‌شود (Schaap, 2009: 137).

اهمیت این اقدام از آنجا مشخص می‌شود که بدانیم اغلب نهادهای اطلاعاتی که درصدد جناحی عمل کردن هستند، به این روش برای حذف جریان‌ها و شخصیت‌های دیگر گروه‌های رقیب روی می‌آورند. جعل تصاویر به‌اندازه خود هنر عکاسی قدمت دارد. یکی از اهداف تغییر عکس در سازمان‌های اطلاعاتی و امنیتی، گمراه کردن یا فریب است. با افزایش نرم‌افزاهای دستکاری دیجیتالی عکس و مهارت بیشتر کاربران در استفاده از این امکانات، وظیفه شناسایی تصاویر دستکاری‌شده نیز به چالشی سخت تبدیل شده و دستکاری دیجیتالی تصاویر هم‌اکنون آنچنان پیشرفت کرده که در برخی مواقع امکان تشخیص وضعیت و حالت اشخاص و اشیاء در زمانی‌که آن عکس گرفته می‌شده، امکان‌پذیر نیست. در سال ۲۰۰۶ فاش شد که رسانه‌ها در خلال جنگ میان اسرائیل و حزب‌الله لبنان مبادرت به دستکاری تصاویر می‌کردند. به‌هرحال، قابل درک است که کشوری بتواند به‌آسانی به چنین کارهایی دست زند و حتی شاید تصاویری را که ازسوی کشورهای دیگر در اینترنت قرار داده شده را تغییر دهد (Schaap, 2009: 138).

هم‌اکنون امکان دستکاری تصاویر ویدئویی نیز وجود دارد. این امکان از ماهیت تغییرپذیر پیکسل‌هایی که تصاویر ویدئویی را تشکیل می‌دهند، ناشی می‌شود. هم‌اکنون امکان قرار دادن پیکسل‌هایی در داده‌های تصویری ماهواره‌ای نیز وجود دارد؛ چیزی که مفسران آن‌را گردان‌هایی از تانک یا هواپیماهای جنگی می‌نامند (Schaap, 2009: 138).

حذف اشخاص یا اشیاء از تصاویر زنده ویدئویی یا قرار دادن اشخاص یا اشیائی دیگر در صحنه‌هایی زنده، تنها شروع ماجرا است. **کسانی‌که مبادرت به چنین کارهایی می‌کنند می‌توانند کاری کنند که سخنگویان**

113. uniform resource locator (URL)
114. dynamic content
محتوای پویا: محتوای وب‌سایت یا وبلاگ که به‌کرات تغییر کرده و می‌تواند شامل انیمیشن‌ها، ویدئوها و فایل‌های صوتی نیز باشد. در اینجا بازدیدکننده می‌تواند از امکانات گوناگون آن صفحه استفاده کرده و به‌نوعی با آن وب‌سایت تعامل داشته باشد.
115. digital image manipulation

در این تصاویر کارهایی بکنند یا حرف‌هایی بزنند که به‌هیچ وجه آن‌را انجام نداده و نگفته‌اند. علاوه بر این، تکنولوژی مدرن می‌توانند فیلم یک‌ساعته سابق را به یک شصتم ثانیه فشرده کنند که همین امر اجازه دستکاری تصاویر در زمان ضبط یا پخش آن‌ها را می‌دهد (Schaap, 2009: 138-139).

این نوع تکنیک‌ها دنیایی از فرصت‌ها را برای دستکاری تصاویر فراهم می‌سازد. برای مثال، می‌توان تصویر ویدئویی رهبر کشوری را در پخش زنده شبکه خبری سی‌ان‌ان قرار داد و اینکه صحبت‌هایی کند که دولت عامل می‌خواهد. همچنین **کشورها می‌توانند تصاویری کاملاً جعلی را بسازند که دشمنانشان را به‌صورتی نشان دهد که در راستای اهداف آنان گام برمی‌دارند.** در این رابطه، جیمز کوری،[116] استاد علوم سیاسی در «دانشگاه دفاع ملی»[117] آمریکا، عضو سابق کمیته اطلاعاتی سنا و مشاور حقوقی رئیس ستاد ارتش این کشور اعتقاد دارد که ارتش و سازمان‌های اطلاعاتی از چنین امکاناتی برخوردار بوده و هستند. برنامه‌ریزان پنتاگون بحث در مورد به‌کارگیری جلوه‌های ویژه گرافیکی پس از تهاجم عراق به کویت در سال ۱۹۹۰ را شروع کردند. در این رابطه، قصد داشتند تصاویری ویدئویی را بسازند که در آن صدام حسین در حال گریه است یا اینکه رابطه‌ای غیراخلاقی دارد و سپس آن‌را در عراق و جهان توزیع کنند (Schaap, 2009: 139).

امکانات تغییر صدا اجازه شبیه‌سازی صدا و ایجاد یک کپی دقیق از صدای فردی خاص را می‌دهد. با این کار آن فرد چیزی را که می‌خواهیم خواهد گفت. جورج پاپکان[118] از «آزمایشگاه ملی لوس آلاموس»[119] این تکنولوژی را توسعه داد. واشنگتن پست جزئیات توانایی پاپکان در تغییر هم‌زمان صدا و ایجاد صدایی جعلی را منتشر ساخته است (Schaap, 2009: 139).

یک نمونه از تهدیدات سایبرتروریست‌ها برای دولت‌ها را در ژاپن و توسط گروه تروریستی موسوم به آئوم شینریکیو[120] شاهد بودیم که به‌خاطر انتشار گاز سمی سارین در متروی توکیو در سال ۱۹۹۵ معروف گردید. در سال ۲۰۰۰، بازپرسان ژاپنی با پی بردن به این موضوع که وزارت دفاع این کشور و تقریباً شماری زیاد دیگری از سازمان‌های دولتی و حدود یک‌صد شرکت تجاری مهم در از بیش از یک‌صد نرم‌افزار تولیدشده توسط آئوم شینریکیو که از بازار خریداری‌شده بود، استفاده می‌کنند، شوکه شدند. به‌گزارش آن‌ها، خسارات واردشده به‌واسطه استفاده از این نرم‌افزارها می‌توانست بسیار ویرانگر باشد: این گروه می‌توانست با «عبور از سامانه‌های امنیتی به‌واسطه دور زدن فایروال‌ها (دیواره‌های آتش)، دسترسی به اخبار با سیستم‌های حساس، فراهم آوردن حمله ازسوی اشخاص خارجی، قرار دادن

116. James Currie
117. National Defense University
118. George Papcun
119. Los Alamos National Laboratory
120. Aum Shinrikyo

ویروس‌هایی که بعدها منتشر می‌شدند یا قرار دادن کدهای مخرب، سیستم‌های کامپیوتری و سیستم‌های کلیدی داده‌ها را از کار بیندازد» (Love, 1999: 198)

توسل دولت‌ها به جنگ اطلاعاتی در راستای اهداف امنیت خود کاملاً قابل پیش‌بینی بود؛ چرا که قریب به اتفاق تمامی کشورهای جهان، سازمان‌های تجاری و حتی سازمان‌های جنایی (برای مثال، کمپانی‌هایی که توسط کارتل‌های مواد مخدر و گروه‌های تروریستی ایجاد شده‌اند یا حساب‌های بانکی که برای پولشویی مورد استفاده قرار می‌گیرند) به سیستم‌های کامپیوتری وابسته شده‌اند. دشوار کردن دفاع دشمن در مقابل حملات اطلاعاتی خودی و تسهیل اقدام تهاجمی مبارزان جنگ اطلاعاتی در جبهه خودی، ماهیت اساسی «شبکه گسترده جهانی» است که به‌گفته ریچارد لاو، متخصص سایبرتروریسم؛ »)این شبکه) که برای افزایش کارآمدی و نه امنیت توسعه یافت... اجازه دسترسی آسان را فراهم می‌آورد، ولی در همان حال کنترل خطاکاران در دست زدن به اقدامات غیرقانونی را دشوار می‌سازد» (Love, 1999: 201). همین موضوع را می‌توان در مورد دیگر شبکه‌های کامپیوتری سازمان‌های مختلف گفت. در ایالات متحده، «۸۵ درصد از زیرساخت‌های حیاتی در مالکیت بخش خصوصی است که همین امر اجرای راه‌حل‌های دولتی برای امنیت و حفاظت از شهروندان را بدون همکاری بخش خصوصی غیرممکن می‌سازد (Love, 1999: 202). در بریتانیا، یکی از وزاری خارجه سابق اذعان کرده بود که «هک می‌تواند سریع‌تر از حمله نظامی بریتانیا را فلج سازد»، زیرا زیرساخت‌های نظامی این کشور با استفاده از کامپیوترها مدیریت و کنترل می‌شوند (Love, 1999: 202).

جنگ اطلاعاتی به‌عنوان یکی از ابزارهای اقدام پنهانی، توانمندی خاصی است که سال‌ها وجود داشته، ولی تا پیش از حملات یازده سپتامبر ۲۰۰۱ به‌ندرت ازسوی رؤسای جمهور آمریکا مورد استفاده قرار می‌گرفته است. هرچند سیا و نیروهای نظامی ایالات متحده از توانایی‌ها و شیوه‌های مشابه زیادی برای اجرای جنگ اطلاعاتی به‌عنوان اقدامی پنهانی برخوردارند، اما اهداف آن‌ها به‌کلی متفاوت از یکدیگر است. اگر یک سرویس نظامی آمریکا در زمان صلح به‌طور پنهانی و از راه دور وارد سیستم کامپیوتری نیروی نظامی کشوری متخاصم - برای مثال، یک شبکه دفاع هوایی یا یک شبکه فرماندهی و کنترل - جهت تغییر یا آسیب رساندن به داده‌ها، سخت‌افزارها یا نرم‌افزارها گردد، این اقدام شکلی فنی یا الکترونیکی از «آماده‌سازی میدان نبرد»[121] و با قصد اجازه به ارتش خود برای از کار انداختن کامپیوترها و داده‌های آن قبل از حمله خواهد بود. اگرچه این اقدام شبیه اقدام پنهانی خواهد بود، اما برخلاف اقدام پنهانی، در این مورد به هیچ دستوری از رئیس‌جمهور نیاز نیست، زیرا آماده‌سازی میدان نبرد اساساً در حوزه اختیارات قانونی ارتش تعریف شده است. در مقابل، اگر ارتش ازسوی رئیس‌جمهور موظف به استفاده از تونمندی‌های خود برای ورود پنهانی و از راه دور به داده‌خانه یک بانک در کشوری خارجی یا تغییر داده‌ها در یک یک حساب بانکی مربوط به یک

121. preparation of battlefield

قاچاقچی تسلیحات گردد، آنگاه صدور چنین دستوری ضروری خواهد بود. اگر سیا بخواهد وارد عملیات جنگ اطلاعاتی به‌عنوان اقدامی پنهانی در دوران صلح گردد، قضیه تفاوت می‌کند. همچون هر نوع اقدام پنهانی، در اینجا نیز نیاز به فرمان رئیس‌جمهوری و گزارش مناسب به کنگره می‌باشد (Daugherty & Bowden, 2006: 88). لذا مشخص است که قوانین به گونه‌ای تنظیم شده است که حیطه اختیارات عملیات‌های نفوذ و پنهانی نهادهای نظامی و امنیتی به روشنی تحدید حدود شده و مقامات ارشد سیاسی کشور، همچنان امکان نظارت و کنترل بر عملکرد پنهانی نهادهای امنیتی بر اهداف داخلی و خارجی احتمالی را دارند.

فهرست منابع

- Bush, G. W. (2003, March 25). Executive Order 13292: Classified National Security Information.(amending Executive Order 12958, as amended), § 1.2(a)(1)-(3): http://www.fas.org/sgp/bush/eoamend.html
- Clark, J. R. (2007). Intelligence and national security: a reference handbook. Westport, CT: Greenwood Publishing Group.
- Daugherty, W. J. & Bowden, M. (2006). Executive Secrets: Covert Action and the Presidency. Lexington, Kentucky: University Press of Kentucky.
- Denning, D. E. R. (1999). Information warfare and security. Boston: Addison-Wesley.
- Hastedt, G. P. (2010). Spies, Wiretaps, and Secret Operations: An Encyclopedia of American Espionage, Volume 1. Santa Barbara, California: ABC-CLIO
- Johnson, L. K. (2008). Book Reviews. Intelligence and National Security, 23(2): 276-288.
- Johnson, L. K. (2009). Sketches for a Theory of Strategic Intelligence. In Gill, P., Marrin, S. & Phythian, M. Intelligence Theory: Key Questions and Debates. pp. 33-54.
- Joint Operations Warfare Policy. (1996, January 2). Joint Chiefs of Staff Instruction, CJCSI S-3210.01A.
- Lerner, K. L. & Lerner, B. W. (2004a). Encyclopedia of espionage, intelligence, and security, Volume 1. Farmington Hills, Michigan: Thomson/Gale.
- Lerner, K. L. & Lerner, B. W. (2004b). Encyclopedia of espionage, intelligence, and security, Volume 2. Farmington Hills, Michigan: Thomson/Gale.
- Lerner, K. L. & Lerner, B. W. (2004c). Encyclopedia of espionage, intelligence, and security, Volume 3. Farmington Hills, Michigan: Thomson/Gale.
- Love, R. A. (1999). The Cyber threat Continuum. In Love. M. C. Beyond Sovereignty: Issues for a Global Agenda. New York: Worth Publishers.
- Mercado, S. C. (2005). Reexamining the Distinction between Open Information and Secrets. CIA Studies in Intelligence Unclassified Edition 49(2).
- Richelson, J. (2008). The US intelligence community. Boulder, Colorado: Westview Press
- Richelson, J. T. (1990). America's Secret Eyes in Space: The U.S. Keyhole Spy Satellite
- Schaap, A. (2009). Cyber warfare operations: development and use under international law. Air Force Law Review 64. 121-174.
- Schwartau, W. (1994). Information Warfare, Chaos on the electronic superhighway. New York New: Thunder's mounth press.
- Smith, W. T. (2003). Encyclopedia of the Central Intelligence Agency. United States. New York: Checkmark Books.
- US Army Offensive Counterintelligence Operations. (1982, June 15). US Army Form AR-381-47, US Army: http://armypubs.army.mil/epubs/pdf/r381_47.pdf
- Waltz, E. (2003). Knowledge management in the intelligence enterprise. London: Artech House.