جنگ خاموش

درک جهان اطلاعات و امنیت

تالیف:

آبرام ان. شولسکی و گری جی. اشمیت

پژوهشکده تحقیقات راهبردی خیزش

جنگ خاموش

درک جهان اطلاعات و امنیت

(جلد اول)

نویسندگان: آبرام ان. شولسکی و گری جی. اشمیت

مترجم: پژوهشکده تحقیقات راهبردی خیزش

مشخصات اثر:

کتاب: جنگ خاموش (درک جهان اطلاعات و امنیت)

سال انتشار: ۱۴۴۶ هجری قمری - ۲۰۲۴ میلادی

ناشر اصلی: پوتومک بوکس، واشینگتن

دیدگاه‌های مطرح‌شـــده در این کتاب لزوماً منعکس‌کننده نظرات مرکز مطالعات خیزش نیست.

پیش‌گفتار مرکز مطالعات

در روزگاری که کشورها می‌کوشند از روش‌های نظامی برای حل‌وفصل منازعات فاصله بگیرند، توجه به حوزه اطلاعات و روش‌ها و ابزارهای آن روزبه‌روز در حال افزایش است. پیامدهای ناگوار، ویرانی‌ها و آسیب‌های ناشی از جنگ‌ها که تا سال‌ها پس از پایان نبردها پابرجا می‌مانند و زخم‌های عمیقی که بر پیکر روابط میان کشورها، ملت‌ها و اقوام وارد می‌کنند، توسل به گزینه نظامی را به نوعی جنون بدل ساخته است؛ به‌ویژه زمانی که بتوان از راه‌های جایگزین بهره جست. در این میان، هیچ ابزاری کارآمدتر از فعالیت‌های اطلاعاتی و امنیتی به عنوان جایگزین یا مکمل اقدام نظامی وجود ندارد. کارکرد اطلاعاتی بارها کشورها را از ورود به جنگ‌های ویرانگر بی‌نیاز ساخته و حتی گاه بدون ریخته شدن قطره‌ای خون یا هدررفت سرمایه‌های کلان و ایجاد کینه‌های دیرینه میان نسل‌ها، پیروزی را به ارمغان آورده است.

جهان اطلاعات همواره با هاله‌ای از ابهام و پنهان‌کاری شـــدید همراه بوده اسـت؛ دو ویژگی بنیادینی که بدون آن‌ها موفقیت در این عرصـه ناممکن اسـت. فعالان این حوزه برای انجام ماموریت‌ها و حفظ امنیت خود ناگزیرند فعالیت‌ها و گاه هویت واقعی خویش را در پوشـشـی از رازداری قرار دهند. با این حال، این پنهان‌کاری به سـرعت به حوزه‌های متعددی تســری می‌یابد و توجیه‌های گوناگونی برای آن تراشـیده می‌شـود؛ توجیه‌هایی که گاه به بهانه‌ای برای فرار از مسـئولیت، سـرپوش گذاشـتن بر ناکامی‌ها و حتی بروز تخلفات اخلاقی، قانونی و مالی تبدیل می‌گردند.

کشورهای غربی به این نتیجه رسیده‌اند که شهروندانشان حق دارند از سـاختار دسـتگاه‌های اطلاعاتی، ماموریت‌های گذشـته و فعالیت‌های جاری آن‌ها آگاه شـوند. از این رو، تصـمیم به افشـای بخش عمده‌ای از اطلاعـات محرمانه گرفتنـد؛ چرا کـه آســیب‌های پنهان‌کـاری مفرط را بسیار فراتر از زیان‌های افشاگری سنجیدند. کتاب حاضر ثمره ارزشمند چنین رویکردی اســت که هدف آن، روشــنگری جامعه درباره مفهوم، عملکرد، تاریخچه و ابعاد مثبت و منفی فعالیت‌های اطلاعاتی است.

کتاب در فصــل نخســت خود به تعریف اطلاعات و شــاخه‌های آن می‌پردازد. در فصــل دوم، ابزارهـا و منـابع اطلاعـاتی اعم از منـابع انسـانی، فنی و آشکار و نحوه بهره‌برداری و دسته‌بندی بهینه داده‌های

گردآوری‌شـده تشـریح می‌شـود. فصـل سـوم به تحلیل اطلاعاتی و چگونگی تفسـیر و کاربسـت داده‌ها اختصـاص دارد. فصـل چهارم به «اقدام پنهان» می‌پردازد که فراتر از جمع‌آوری اطلاعات، شامل نفوذ و اقدام در جبهه دشـمن اسـت. فصـل پنجم موضـوع ضـد اطلاعات را بررسی می‌کند؛ همان‌گونه که یک سرویس اطلاعاتی در پی جمع‌آوری داده از دشمن یا اجرای عملیات در خاک اوست، باید مانع از دسترسی حریف به اطلاعات خودی و فعالیت او در قلمرو خویش شـود. دو فصـل پایانی کتاب نیز به بررسـی رابطه میان حاکمیت و سـاختار سیاسی با دستگاه‌های اطلاعاتی می‌پردازند.

مرکز مطالعات راهبردی خیزش با درک اهمیت و جامعیت مفاهیم این اثر و غنای آن در ارائه نمونه‌های واقعی که مفاهیم انتزاعی را ملموس می‌سـازد، اقدام به ترجمه آن از زبان عربی که توسـط مرکز خطابی از انگلیسی به عربی برگردانده شده بود، نموده است. مطالعه این کتاب برای تمامی کارکنان جامعه اطلاعاتی، پژوهشـگران، دانشگاهیان و علاقه‌مندان به این حوزه امری ضروری و اجتناب‌ناپذیر است.

افزون بر این، قلم روان و صـریح کتاب به مخاطبان غیرمتخصـص و علاقه‌مندان به مطالعه این امکان را می‌دهد تا با زوایای پنهان دانش

اطلاعاتی آشـــنا شـــوند و تصـــویری جامع از این دنیای پررمز و راز به دســـت آورند؛ شـــناختی که امروزه دولت‌ها، جوامع و افراد بیش از هر زمان دیگری به آن نیازمندند. درک درســـت از کارکرد دســـتگاه‌های اطلاعاتی، زمینه‌ساز هم‌افزایی ملی است و تنها از این طریق می‌توان بر ترس‌ها و توهماتی که مانع همکاری شـــهروندان با این نهادها می‌شود، غلبه کرد.

دیباچه نویسنده

علاقه من به کتاب «جنگ خاموش» در اصل به سرفصل‌های درسی حوزه اطلاعات بازمی‌گردد که در سال ۱۹۸۵ به عنوان استاد مهمان در مرکز مطالعات دموکراسی، نظریه و عمل «جان اولین» در دانشگاه شیکاگو تدریس می‌کردم. بازگشت به فضای آکادمیک و کلاس درس مرا واداشت تا به افکار خود در زمینه امور اطلاعاتی و امنیتی نظم ببخشم؛ موضوعی که به واسطه فعالیت حرفه‌ای‌ام در واشینگتن کاملاً با آن مانوس بودم. این کتاب نخستین بار در سال ۱۹۹۱ منتشر شد، اما اندکی پس از آن، قوانین جدیدی در حوزه اطلاعات در ایالات متحده و سایر کشورها وضع گردید و آثار ارزشمند جدیدی در این زمینه به رشته تحریر درآمد که با فروپاشی اتحاد جماهیر شوروی نیز همزمان شد. این تحولات، بازنگری و اصلاح کتاب را ضروری ساخت. در آن مقطع به دلیل بازگشتم به خدمات دولتی در وزارت دفاع، فرصت کافی برای این کار نداشتم؛ از این رو از «گری اشمیت»

جانشـــین خود در ســـمت مدیریت امور اقلیت[1] در کمیته اطلاعات مجلس ســـنای آمریکا و مدیر اجرایی پیشـــین هیئت مســـتشـــاری اطلاعات[2] خارجی ریاست‌جمهوری درخواست کردم تا بازنویسی کتاب را بر عهده گیرد که در نهایت ویرایش دوم آن در ســـال ۱۹۹۳ منتشـــر شد.

از آن زمان تاکنون، منابع علمی و پژوهش‌های اختصـــاصـــی در حوزه اطلاعات رشـد چشـمگیری داشـته اسـت. همچنین روند تدریجی اما مستمر قانون‌گذاری برای نظارت بر فعالیت‌های اطلاعاتی در سراسر جهان و انطباق این قوانین با اصول حکومت‌های مردم‌سالار و شفاف آغاز شـــده اســـت. با این حال، بزرگ‌ترین دگرگونی از زمان انتشـــار

---

[1] ؛ مدیر امور اقلیت :(Minority Staff Director) نماینده ارشـد حزب اقلیت در کمیته‌های کنگره آمریکا که مســـئولیت هماهنگی، پژوهش و پشـــتیبانی از ســـناتورهای حزب اقلیت را در آن کمیته بر عهده دارد. حزب اقلیت در مجلس سنای ایالات متحده، حزبی است که کرسی‌های کمتری را نسبت به حزب اکثریت در اختیار دارد.

[2] ؛ کمیته اطلاعات مجلس ســـنای ایالات متحده :(SSCI) کمیته‌ای نظارتی در مجلس ســـنای آمریکا که وظیفه بررســـی و نظارت بر عملکرد نهادهای اطلاعاتی کشور مانند سازمان اطلاعات مرکزی (سیا) و آژانس امنیت ملی را بر عهده دارد تا از انطباق فعالیت‌های آن‌ها با قوانین و حفاظت موثر از امنیت ملی اطمینان حاصل شود.

ویرایش‌های اول و دوم کتاب، وقوع «انقلاب اطلاعات» است که سرعت پردازش و تبادل داده‌ها را به شدت افزایش داده است. این کتاب در ویرایش سوم خود می‌کوشد به این پرسش پاسخ دهد که تغییر در دسترسی و گردش اطلاعات چگونه بر فعالیت‌های اطلاعاتی دولت‌ها که وظیفه اصلی‌شان جمع‌آوری، حفاظت و انتقال اطلاعات است، تاثیر می‌گذارد.

هرچند کتاب «جنگ خاموش» تاکنون دو بار مورد بازنگری و ویرایش قرار گرفته، اما فرضیه اصلی، ساختار و بخش عمده‌ای از محتوای بنیادین آن دست‌نخورده باقی مانده است. هدف این کتاب هرگز ارائه کارنامه‌ای از فعالیت‌های اطلاعاتی یک کشور خاص در دوره‌ای مشخص از تاریخ نبوده است؛ اگرچه بسیاری از نمونه‌های ذکرشده در کتاب از تجارب اطلاعاتی ایالات متحده و بریتانیا اقتباس شده‌اند، اما هدف کلی آن‌ها تبیین مفاهیم اساسی و چالش‌های موجود در تجربه اطلاعاتی است. بی‌تردید پایان جنگ سرد، ظهور دوران راهبردی جدید و آغاز عصر اطلاعات، شیوه‌ها و نیازمندی‌های اطلاعاتی را تا حدی تغییر داده است، اما فرضیه بنیادین کتاب همچنان پابرجاست: اطلاعات پیوندی ناگسستنی با رقابت میان دولت‌ها دارد. تا زمانی که الگوهای منازعه میان ملت‌ها برقرار باشد و به تعبیر کانت به «صلح

پایدار»[3] دست نیافته باشیم، اطلاعات نیز همانند دیپلماسی و قدرت نظامی، ابزاری حیاتی در اعمال حاکمیت و جهانداری باقی خواهد ماند. از این رو، شهروندان و پژوهشگران به یک اندازه نیازمند درک عناصر کلیدی اطلاعات، تعاملات آن و همچنین چالش‌ها و مناسبات میان این فعالیت‌های پنهان با دولت‌های دموکراتیک و جوامعی هستند که به آن‌ها خدمت می‌کنند.

این ویرایش و نسخه‌های پیشین کتاب، همواره از ارزیابی‌ها، نظرات و توصیه‌های دانشجویان، دوستان و همکاران متعددی بهره‌مند شده است. در این میان، شایسته است از الیوت کوهن، کنت دگرافنرید، هیلل فرادکین، وسام هالبرین، شیلا کر، کارنس لورد، کنت رابرتسون و دیانا رودرک صمیمانه سپاسگزاری کنم.

نگارش ویرایش نخست این کتاب به دورانی بازمی‌گردد که به عنوان پژوهشگر ارشد در «دفتر ملی اطلاعات استخباراتی» فعالیت داشتم و از حمایت‌های مالی بنیادهای «جان ام. اولین»، «لیند» و «هری بردلی» بهره‌مند بودم. ویرایش دوم اثر حاضر توسط «گری اشمیت»،

[3] ؛ صلح پایدار: اشاره به نظریه ایمانوئل کانت در رساله «به سوی صلح پایدار» که معتقد است صلح پایدار و پایدار تنها زمانی محقق می‌شود که کشورها دارای ساختار جمهوری و قانون‌مدار بوده و روابط آن‌ها بر پایه حقوق بین‌الملل تنظیم شود، نه حکومت‌های استبدادی و پادشاهی.

که او نیز از پژوهشگران ارشد این دفتر بود، بازبینی و اصلاح شده است. در اینجا لازم می‌دانم از «روی گادسن»، رئیس دفتر ملی اطلاعات استخباراتی، و «جفری برمن»، مدیر اجرایی این نهاد، به پاس تلاش‌های بی‌شائبه و دوستی صمیمانه‌شان در طول سالیان متمادی، صمیمانه سپاسگزاری کنم.

آبرام شولسکی

واشینگتن دی.سی.

یادداشتی برای خواننده

محتوای این کتاب با توجه به حملات تروریستی ۱۱ سپتامبر ۲۰۰۱ بازبینی نشده است؛ چرا که این رویداد هم‌زمان با مراحل نهایی چاپ کتاب رخ داد. بی‌تردید ارزیابی و احصای تمامی پیامدهای این حملات نیازمند زمان زیادی است، اما پرواضح است که در آینده، تمرکز اصلی بر تقویت توانمندی‌های انسانی در حوزه جمع‌آوری اطلاعات برای مقابله با انواع اهداف اطلاعاتی معطوف خواهد شد. به‌ویژه آنکه تمرکز بر پوشش‌های غیررسمی افسران اطلاعاتی افزایش خواهد یافت. همچنین می‌توان انتظار داشت که قوانین گوناگون ناظر بر نظارت‌های داخلی، شنود و دیگر فناوری‌های مراقبتی دستخوش بازنگری و اصلاح شوند. در این میان، پرسش بنیادینی که بار دیگر مطرح خواهد شد این است که آیا افراد یا گروه‌ها صرفاً به دلیل مواضع سیاسی‌شان و بدون وجود ارتباطی آشکار با یک اقدام مجرمانه مشخص، باید تحت مراقبت و نظارت قرار گیرند یا خیر.

مقدمه: نگارش درباره اسرار اطلاعاتی

طی ربع قرن گذشته، علی‌رغم اینکه پنهان‌کاری همچنان یکی از ویژگی‌های اصلی حوزه اطلاعات به شمار می‌رود، این موضوع جایگاهی ثابت در اخبار رسانه‌ها یافته و به موضوعی برای پژوهش‌های دانشگاهی گسترده و تألیف کتاب‌های متعدد تبدیل شده است. امروزه بحث‌های علنی درباره مسائل اطلاعاتی دیگر به افشاگری یا جنجال‌های رسانه‌ای محدود نمی‌شود، بلکه به بخشی طبیعی از گفتمان عمومی پیرامون فعالیت‌های دولتی بدل شده است.

اگرچه بحث‌های عمومی درباره رویدادهای جاری در دنیای اطلاعات همچنان تا حد زیادی به افشای اطلاعات طبقه‌بندی‌شده (اعم از مجاز یا غیرمجاز) وابسته است، اما ادبیات دانشگاهی در این حوزه رشد چشمگیری داشته است. با گذشت زمان و اتخاذ رویکردی بازتر از سوی برخی دولت‌های دموکراتیک، بخش عمده‌ای از اسناد تاریخی

مربوط به جنگ جهانی دوم و دوران جنگ سـرد از حالت طبقه‌بندی خارج شده است. فروپاشی کمونیسم در اتحاد جماهیر شوروی سابق و اروپای شرقی نیز دسترسی پژوهشگران را به برخی اسناد آرشیوی، به‌ویژه در آلمان شـرقی سـابق و تا حدی در روسـیه، هموار سـاخت. امروزه ادغام ابعاد اطلاعاتی در تاریخ دیپلماتیک و نظامی به امری رایج تبدیل شده است.

با این حال، افزایش بحث‌های عمومی پیرامون مسـائل اطلاعاتی همواره به درک بهتر این حوزه منجر نشـده اسـت؛ چرا که این گفتگوها اغلب با نادیده گرفتن پرسـش‌های بنیادین درباره نقش مناسـب اطلاعات و پنهان‌کاری در یک نظام دموکراتیک همراه بوده اسـت. به طور کلی، به اسـتثنای موجی از نگارش‌ها که هم‌زمان با آخرین تلاش کنگره آمریکا برای اصـلاح سـاختار اطلاعاتی در اوایل دهه نود میلادی شکل گرفت، رویکرد عمومی به مسائل اطلاعاتی (در مواردی که جنبه تاریخی نداشـته‌اند) عمدتاً محدود به جزییات پرونده‌های جاسـوسـی خاص بوده است.

این تفاوت‌ها با موج قبلی نگارش‌های اطلاعاتی به دوره میان دهه هفتاد تا اوایل دهه نود میلادی بازمی‌گردد. در آن زمان، بخش عمده‌ای از مباحث عمومی درباره اطلاعات (به‌ویژه در ایالات متحده که بازتاب آن به بسـیاری از نظام‌های دموکراتیک دیگر نیز رسـید) بر اسـاس

رویکرد روش‌شـــناختی یـا دیـدگـاهشـــان دربـاره نقش اطلاعـات در دموکراســـی و رابطه پنهان‌کاری با معیارهای حکومت دموکراتیک، به دو طیف فکری تقسیم می‌شدند.

بر اســاس دیدگاه طیف نخســت، فعالیت‌های اطلاعاتی باید از قلمرو پنهان‌کاری مطلق خارج شـــده و به علوم اجتماعی نزدیک‌تر شـــوند؛ علومی که کارکرد آن‌ها تحلیل و پیش‌بینی رویدادهای ســـیاســـی، اقتصـــادی، اجتماعی و نظامی اســـت. از این منظر، ماهیت اطلاعات لزوماً نیازمند پنهان‌کاری نیست. اگرچه ممکن است حفظ برخی اسرار برای صـــیانت از منابع اطلاعاتی حیاتی لازم باشـــد، اما مهم‌ترین واقعیت‌های سیاسی، اقتصادی، اجتماعی، فناوری و جمعیت‌شناختی که مسـیر بلندمدت یک کشـور را تعیین می‌کنند، محرمانه نیسـتند[4].

---

[4] ؛ شیرمن کنت، افسر پیشین اطلاعاتی، این مکتب فکری را در اواخر دهه ۱۹۴۰ پیش‌بینی کرد و همچنان برجسته‌ترین و مهم‌ترین نظریه‌پرداز آن به شمار می‌رود. او برای نخســـتین بار تز خود را در کتابش با عنوان «اســـتراتژی اطلاعـاتی در سیاست جهانی آمریکا» مطرح ساخت.

کتاب «اطلاعات در خدمت امنیت ملی آمریکا» اثر بروس برکوویتز و آلن گودمن نیز در همین راســتا نگاشــته شــده اســت. نویســندگان این کتاب اذعان دارند که اثرشان با همان روحیه کتاب کنت نوشته شده (و صرفاً به‌روزرسانی آن نیست). به نظر می‌رسـد آنها دسـت‌کم تا حدودی درک کنت از اطلاعات اسـتراتژیک را به اشـتراک می‌گذارند. این دو نویسـنده بیان می‌کنند که برخلاف اطلاعات عملیاتی، اطلاعات استراتژیک «پایه‌ای گسترده‌تر و اهدافی بزرگ‌تر دارد و اقتصاد، سیاست،

بنابراین، نه تنها می‌توان درباره مسائل اطلاعاتی بدون موانع جدی به بحث علنی پرداخت، بلکه گفتمان عمومی از طریق ابهام‌زدایی از این حوزه و تسهیل تبادل ایده میان نهادهای اطلاعاتی و محافل دانشگاهی، می‌تواند به حرکت اطلاعات در مسیر درست خود کمک کند؛ مسیری که در آن سازمان‌های اطلاعاتی بیشتر به اندیشکده‌ها شبیه می‌شوند و کارکردی نزدیک به علوم اجتماعی پیدا می‌کنند [5].

در مقابل، طیف دوم هدف از نگارش علنی درباره اطلاعات را افشای خطاها و کاستی‌ها و کمک به بهبود عملکرد سازمان‌های اطلاعاتی می‌دانستند[6]. از این دیدگاه، پنهان‌کاری در فعالیت‌های اطلاعاتی یا خود زمینه‌ساز انحرافات بوده یا بستر لازم را برای آن فراهم آورده است. بنابراین، بحث عمومی درباره اطلاعات، خود بخشی از راهکار

مطالعات اجتماعی و فناوری را در هم می‌آمیزد. اطلاعات استراتژیک برای ارائه تصویری کلان به مسئولان و پیش‌بینی‌های بلندمدت مورد نیاز برای برنامه‌ریزی آینده، پدید آمده است.»

[5] ؛ سناتور دیوید بورن، رئیس وقت کمیته اطلاعاتی سنا، هدف از اصلاحات پیشنهادی خود در اوایل دهه نود را ایجاد یک «اندیشکده سطح بالا» و در واقع بهترین مرکز پژوهش‌های فکری در جهان عنوان کرد؛ بنگرید به مقاله او در نشریه فارین افرز، تابستان ۱۹۹۲.

[6] ؛ یکی از نخستین و معروف‌ترین کتاب‌ها در این زمینه با این گزاره آغاز می‌شود: «امروز در ایالات متحده فرقه‌ای قدرتمند و خطرناک وجود دارد؛ فرقه اطلاعات». بنگرید به کتاب فکتور مارکتی و جان مارکس با عنوان «سیا و فرقه اطلاعات».

درمانی به شـمار می‌رفت. از نظر این گروه، هرگونه آسـیب ناشـی از افشـای اسـرار در مقایسـه با پیامدهای مخرب فعالیت سـازمان‌های اطلاعاتی خارج از نظارت عمومی، ثانویه و ناچیز تلقی می‌شـد. از این رو، افشـای اطلاعات درباره سـازمان‌های اصـلاح‌نشـده بلامانع بود؛ هرچند مشـخص نیسـت نویسـندگان این طیف درباره بحث عمومی پیرامون سـازمان‌های اطلاعاتی پس از انجام اصـلاحات چه دیدگاهی دارند، اگرچه می‌توان اسـتدلال کرد که نبود نظارت عمومی در هر صورت می‌تواند هر نهادی را به انحراف بکشاند.

در سـال‌های اخیر، بخش عمده‌ای از پژوهش‌های دانشـگاهی و نگارش‌ها به سـمت روایت‌های تاریخی از فعالیت‌های اطلاعاتی معطوف شـده اسـت[7]. در این میان، روایت پرونده‌های جاسـوسـی خاص بر مباحث معاصـر سـایه افکنده و تمرکز بیشـتر بر ادعاهای مربوط به ناکارآمدی و ضعف حرفه‌ای بوده است تا تخلفات اخلاقی و

[7] ؛ نشریه بریتانیایی «اطلاعات و امنیت ملی» در این زمینه اهمیت ویژه‌ای دارد و پژوهش‌های تاریخی ارزشـمندی درباره ابعاد اطلاعاتی تاریخ دیپلماتیک و نظامی منتشر کرده است.

سیاسی[8]. جهت‌گیری این پژوهش‌ها و آثار کمتر معطوف به اهداف سیاسی یا ایدئولوژیک بوده است (فارغ از این اصل بدیهی که داشتن یک سرویس اطلاعاتی کارآمد بهتر از یک سرویس ناکارآمد است).

کتاب «جنگ خاموش» در پی پاسخگویی به گونه‌های متفاوتی از پرسش‌هاست و می‌کوشد مفاهیم بنیادین درک جهان اطلاعات را به بحث بگذارد. هدف این اثر، توانمندسازی خواننده برای اندیشیدن درباره مسائل کلان سیاست‌گذاری اطلاعاتی به شیوه‌ای است که پیچیدگی‌ها و ظرافت‌های این موضوع را به شایستگی مد نظر قرار دهد. از این رو، رویکرد اتخاذشده در این کتاب اساساً نظری است و با بهره‌گیری از جزییات فعالیت‌های اطلاعاتی واقعی، به تبیین چارچوب‌های کلی کار اطلاعاتی می‌پردازد[9]. در این اثر هیچ تلاشی برای ارائه یک تاریخچه جامع از ابعاد مختلف اطلاعات یا وضعیت کنونی آن صورت نگرفته است.

---

[8] ؛ نمونه‌هایی از این دست را می‌توان در آثار دیوید وایز یافت؛ از جمله کتاب «جاسوسی که گریخت: داستان واقعی ادوارد لی هوارد» و کتاب «شکار خائنانی که سیا را ویران کردند».

[9] ؛ این امر علت فراوانی نمونه‌های مربوط به جنگ جهانی دوم و جنگ سرد را در کتاب توضیح می‌دهد؛ چرا که اسناد مربوط به این دوره‌ها بیش از سایر دوران‌ها منتشر شده است. هدف از این نمونه‌ها صرفاً تبیین اصول کلی است.

بنابراین، این کتاب بر اطلاعات در دسترس عموم درباره فعالیت‌های اطلاعاتی تکیه دارد[10] و تلاشی برای ارائه داده‌های منتشرنشده انجام نداده است. یکی از دلایل این امر آن است که اگرچه ما به اطلاعات طبقه‌بندی‌شده در سطوح مختلف دولت آمریکا (خارج از سازمان‌های اطلاعاتی) دسترسی داشتیم، اما متعهد به عدم افشای این اطلاعات بودیم[11].

مهم‌تر از آن، ما پنهان‌کاری را برای عملیات‌های اطلاعاتی حیاتی می‌دانیم و انتشار جزییات عملیاتی سازمان‌های اطلاعاتی آمریکا را امری صحیح تلقی نمی‌کنیم؛ چرا که بخش عمده این جزییات برای عموم جامعه فاقد اهمیت بوده و نقشی در درک مفاهیم پایه‌ای اطلاعات که هدف این کتاب است، ندارد.

اگرچه مطالعات اطلاعاتی به یک رشته دانشگاهی منظم به‌ویژه در کشورهای انگلیسی‌زبان تبدیل شده است، اما رویکرد نظری آن

---

[10] ؛ یکی از روش‌های مناسب برای به‌روز ماندن، مراجعه به پایگاه‌های اینترنتی فعال در حوزه گردآوری اطلاعات است، مانند وب‌سایت فدراسیون دانشمندان آمریکا (fas.org/irp).

[11] ؛ شایان ذکر است که این کتاب پیش از انتشار، جهت بازبینی امنیتی به سازمان اطلاعات مرکزی آمریکا (سیا) و کمیته اطلاعاتی مجلس سنا ارائه شد؛ هرچند تأیید عدم وجود اطلاعات طبقه‌بندی‌شده در کتاب، به معنای تأیید محتوای آن از سوی این نهادها نیست.

همچنان به بلوغ کافی نرسیده است. ما در این کتاب می‌کوشیم این خلاء را برطرف کنیم، هرچند آگاهیم که تکیه بر تجربه بریتانیایی-آمریکایی مانع از دستیابی کامل به یک «نظریه عمومی اطلاعات» می‌شود. علت این تمرکز آن است که بیشتر اطلاعات در دسترس عموم درباره مسائل اطلاعاتی، از سازمان‌های اطلاعاتی کشورهایی با بازترین نظام‌های سیاسی سرچشمه می‌گیرد. با این حال، در طول کتاب تا حد امکان به فعالیت‌های اطلاعاتی سایر کشورها نیز اشاره کرده و این واقعیت را مد نظر قرار داده‌ایم که سازمان‌های اطلاعاتی بسته به ماهیت نظام‌های سیاسی حاکم بر آن‌ها متفاوت عمل می‌کنند.

بنابراین، این کتاب هیچ‌گونه راز، اطلاعات درونی یا افشاگری‌های شگفت‌انگیزی ارائه نمی‌دهد، بلکه امیدوار است بستری برای درک عمیق‌تر خودِ پدیده اطلاعات و تحلیل روایت‌هایی فراهم کند که دیر یا زود به عرصه عمومی راه خواهند یافت.

بخش نخست: اطلاعات چیست؟

در باور عمومی و تصور جامعه، مفهوم اطلاعات اغلب با جاسوسی، فریبکاری، جذابیت‌های زنانه افرادی چون «ماتا هاری» [12]و ماجراجویی‌های پررمزوراز «جیمز باند» درآمیخته است. اگرچه چنین

[12] ؛ مارگارت گرترود زله، معروف به ماتا هاری، رقصنده هلندی که در جریان جنگ جهانی اول به اتهام جاسوسی برای آلمان اعدام شد.

فعالیت‌هایی جایگاه خاص خود را در دنیای اطلاعات دارند، اما مفهوم کلی اطلاعات بسیار گسترده‌تر از این کلیشه‌هاست. برای درک این گستردگی، می‌توان بررسی را با دسته‌بندی پدیده‌هایی آغاز کرد که تحت عنوان «اطلاعات» قرار می‌گیرند؛ این پدیده‌ها شامل انواع خاصی از داده‌ها، فعالیت‌ها و سازمان‌ها می‌شوند[13].

اطلاعات به داده‌های مرتبط با یک نهاد دولتی و کارکرد آن در اجرای سیاست‌ها، منافع امنیت ملی و مواجهه با تهدیدهای بالفعل یا بالقوه از سوی رقبا اشاره دارد (واژه «رقبا» در اینجا در معنای گسترده آن به کار می‌رود؛ برای نمونه، یک دولت دوست که طرف مذاکره برای امضای یک پیمان‌نامه است، در بستر مذاکرات می‌تواند رقیب محسوب شود؛ زیرا طرفین برای کسب بیشترین امتیاز ممکن تلاش می‌کنند). در ملموس‌ترین حالت، این داده‌ها به مسائل نظامی مانند توانمندی‌ها و طرح‌های عملیاتی دشمن مربوط می‌شوند؛ اطلاعاتی که دشمن همواره می‌کوشد آن‌ها را پنهان نگاه دارد. البته انواع دیگر اطلاعات نیز می‌توانند به همین اندازه حیاتی باشند؛ مانند اطلاعات

[13] ؛ کتاب «اطلاعات استراتژیک برای سیاست جهانی آمریکا» نوشته شرمن کنت این ساختار سه‌گانه را دنبال می‌کند.

مربوط به فعالیت‌های دیپلماتیک، تصمیمات و نیات یک کشور دیگر و همچنین فعالیت‌های اطلاعاتی آن.

علاوه بر این نوع داده‌ها، شناخت جنبه‌های دیگر درباره رقبای بالفعل یا بالقوه نیز سودمند است، حتی اگر رقیب حساسیتی نسبت به افشای آن‌ها نداشته باشد؛ مواردی نظیر امور سیاسی داخلی، تحولات اجتماعی و آمارهای اقتصادی و جمعیت‌شناختی. میزان انتشار واقعی این‌گونه داده‌ها به ماهیت نظام سیاسی بستگی دارد؛ در جوامع دموکراتیک این اطلاعات غالباً در دسترس عموم قرار دارند، در حالی که نظام‌های اقتدارگرا و توتالیتر می‌کوشند هرگونه اطلاعات درباره سیاست‌های داخلی، تحولات اقتصادی یا روندهای اجتماعی خود را که ممکن است مورد بهره‌برداری رقیب قرار گیرد، پنهان کنند. صرف‌نظر از اینکه آیا اطلاعات منابع آشکار را باید اطلاعات واقعی دانست یا خیر، فرآیند غربالگری و پردازشی لازم است تا این داده‌ها به شکلی کارآمد در اختیار تصمیم‌گیران حکومتی قرار گیرد؛ وظیفه‌ای که معمولاً بر عهده سازمان‌های اطلاعاتی است.

در نهایت، اطلاعات تنها شامل «داده‌های خام» جمع‌آوری‌شده از طریق جاسوسی یا دیگر ابزارها نیست، بلکه تحلیل و ارزیابی این داده‌ها را نیز در بر می‌گیرد. این محصول نهایی تحت عنوان «تولیدات

اطلاعاتی» شناخته می‌شود و ارزش بالایی برای سیاست‌گذاران دارد. میزان تلاش سازمان‌های اطلاعاتی برای ارائه یک ارزیابی جامع بر اساس تمامی داده‌های آشکار و پنهان، از سازمانی به سازمان دیگر متفاوت است.

قلمرو اطلاعات: اطلاعات شامل جمع‌آوری و تحلیل داده‌ها و همچنین اقداماتی است که برای مقابله با فعالیت‌های اطلاعاتی حریف انجام می‌شود؛ اقداماتی که یا از طریق محروم‌سازی حریف از دسترسی به اطلاعات صورت می‌گیرد یا با گمراه کردن او درباره واقعیت‌ها و اهمیت آن‌ها.

بنابراین، اطلاعات طیف وسیعی از فعالیت‌ها را پوشش می‌دهد؛ برای مثال، روش‌های متنوعی برای جمع‌آوری اطلاعات وجود دارد، از جمله: جاسوسی، تصویربرداری هوایی، شنود ارتباطات، پژوهش در اسناد آشکار، رصد رسانه‌های صوتی و تصویری و اینترنت. همچنین فنون متعددی برای تحلیل اطلاعات جمع‌آوری‌شده به کار می‌رود؛ برخی از این روش‌ها شبیه به تحلیل‌های علوم اجتماعی هستند، در حالی که برخی دیگر مانند رمزنگاری و رمزگشایی پیام‌ها، کاملاً تخصصی و متمایز از علوم اجتماعی به شمار می‌روند.

به همین ترتیب، تلاش برای محروم کردن دیگران از دسترسی به اطلاعات، فعالیت‌های گوناگونی را شامل می‌شود؛ برخی از آن‌ها

شـــبیه به اقدامات ضـــابطان قضـــایی و مجریان قانون اســـت، مانند بازجویی و محاکمه عوامل مظنون به جاسـوسـی برای بیگانگان جهت کشـــف فعالیت‌های آنان؛ و برخی دیگر تخصـــصـــی‌تر هســـتند، مانند اسـتفاده از رمزنگاری برای حفاظت از ارتباطات (اگرچه پیشـرفت‌های اخیر در فناوری اطلاعات، ابزارهای رمزنگاری را به صـــورت تجاری در دسـترس همگان قرار داده اسـت). در نهایت، روش‌های متعددی برای فریب دشمن وجود دارد، مانند عملیات‌های «عامل دوطرفه» و ارسال پیام‌های گمراه‌کننده (پیام‌هایی که ارسـال می‌شـوند تا دشـمن آن‌ها را ردیابی کرده و باور کند).

تنوع گسـترده این فعالیت‌ها ممکن اسـت آن‌ها را نامرتبط جلوه دهد، اما همگی در راســـتای کســـب اطلاعات یا حفاظت از آن هماهنگ می‌شـوند. از این رو، اطلاعات به عنوان یک فعالیت را می‌توان یکی از مؤلفه‌های منازعه میان رقبا تعریف کرد که به طور عمده با مدیریت اطلاعات ســـرکار دارد؛ مانند رقابت اقتصـــادی، مانورهای دیپلماتیک، مذاکرات یا تهدید به استفاده از نیروی نظامی.

در نهایت، واژه اطلاعات به سـازمان‌هایی اشـاره دارد که این فعالیت‌ها را اجرا می‌کنند. یکی از مهم‌ترین ویژگی‌های این سازمان‌ها، پنهان‌کاری حاکم بر عملیات‌های آن‌هاســـت. بســـیاری از روش‌های کاری، مانند اســـتفاده از مأموران مخفی یا قوانین ســـخت‌گیرانه دســـترســـی به

اطلاعات، ناشی از همین نیاز به پنهان‌کاری است. از آنجا که ساختار سازمان‌های اطلاعاتی برای به حداکثر رساندن پنهان‌کاری طراحی شده است، ممکن است علاوه بر وظایف اطلاعاتی، مسئولیت انجام فعالیت‌های مخفیانه برای پیشبرد مستقیم اهداف سیاست خارجی دولت‌ها نیز به آن‌ها واگذار شود.

این‌گونه فعالیت‌ها «اقدام پنهان» نامیده می‌شوند و دامنه آن‌ها در ادبیات اطلاعاتی آمریکا می‌تواند از یک اقدام ساده مانند ارائه کمک‌های حساس و محرمانه به یک دولت دوست، تا اقدامات بزرگی چون برنامه‌ریزی برای سرنگونی یک حکومت متخاصم را در بر گیرد. اینکه آیا سازمان‌های جمع‌آوری و تحلیل اطلاعات باید متولی این‌گونه اقدامات باشند یا خیر، پرسشی بنیادین و چالش‌برانگیز است. حتی اگر وظیفه اقدامات پنهان به دلایل اداری به سازمان‌های اطلاعاتی واگذار شود، از منظر نظری و عملی این پرسش مطرح است که آیا باید اقدام پنهان را بخشی از تعریف اطلاعات دانست یا خیر؟

قلمرو اطلاعات

دولت‌ها تنها بازیگرانی نیستند که در محیط‌های رقابتی شدید فعالیت می‌کنند، بلکه این ویژگی در مورد بسیاری از سازمان‌های دیگر نیز

صدق می‌کند. از این رو، مفهوم اطلاعات را می‌توان به آن‌ها نیز تعمیم داد. برای نمونه، برخی پژوهشگران مفهوم اطلاعات را به شرکت‌های تجاری گسترش داده و آن را به عنوان «اطلاعات سازمان‌یافته... طراحی‌شده برای پاسخگویی به نیازهای ویژه سیاست‌گذاران یک پروژه خاص» تعریف می‌کنند[14]. همچنین تلاش برای آگاهی از برنامه‌های حزب رقیب یا یک کارزار سیاسی را می‌توان فعالیتی اطلاعاتی توصیف کرد.

این تعمیم‌های احتمالی از مفهوم اطلاعات در چارچوب این کتاب قرار نمی‌گیرد؛ چرا که تمرکز اثر حاضر بر قلمرو سنتی اطلاعات، یعنی داده‌ها و فعالیت‌های مرتبط با مسائل امنیت ملی کشورهاست.

با این حال، حتی با این محدودسازی نیز مرزهای قلمرو اطلاعات همچنان مبهم باقی می‌ماند؛ زیرا خودِ مفهوم امنیت ملی فاقد یک تعریف جامع و مانع است. معنای بنیادین امنیت ملی به حفاظت از کشور در برابر انواع تهدیدهای خارجی، به‌ویژه تهدیدهای نظامی مربوط می‌شود. هنگامی که کشوری مورد تهاجم قرار می‌گیرد یا در آستانه آن است، امنیت ملی آن به وضوح بر شکست مهاجمان یا بازدارندگی آنان و نیز مصون‌سازی کشور در برابر تهدیدهای مشابه در

[14] ؛ هربرت مایر در کتاب «جهان واقعی اطلاعات» و همچنین آثار رابرت دیوید استیل به این موضوع پرداخته‌اند.

آینده متمرکز می‌شود. اما در دوران ثبات و کاهش مخاطرات، تهدیدها، کشورها یا شرایط خارجی مخل امنیت ملی تا این حد آشکار نیستند و تشـــخیص آن‌ها نیازمند پویایی و دقت نظر ســـازمان‌های اطلاعاتی است[15].

اگر بدانیم که منافع امنیت ملی یک کشـــور و به تبع آن تهدیدهای پیش‌روی این منافع را نمی‌توان مســـتقل از شـــکل حکومت (یا نظام سیاسی) و رویکرد ایدئولوژیک آن بررسی کرد، به عمق پیچیدگی این مسئله پی می‌بریم. هرچند پیروان مکتب واقع‌گرایی سیاسی بر این باورند که منافع ملی کشـــورها توســـط عوامل عینی نظام بین‌الملل تعیین می‌شود، اما دیدگاه‌های ایدئولوژیک و فرهنگ سیاسی حاکم بر یک کشـــور به طور مســـتقیم بر نحوه نگرش دولت‌ها به این منافع اثرگذار است. برای نمونه، ویژگی‌های ایدئولوژیک یک نظام سیاسی می‌تواند تعیین‌کننده این باشد که آیا حکومت کشوری دیگر به عنوان یک تهدید نگریســـته می‌شـــود یا خیر؛ به‌ویژه در مورد حکومت‌های

---

[15] ؛ برای نمونه، تلاش‌های وزارتخانه‌های آمریکا در ســـال‌های ۱۹۹۱ و ۱۹۹۲ برای تدوین فهرست «نیازمندی‌های اطلاعاتی» نشان‌دهنده تأثیر پایان جنگ سرد بر تنوع موضوعات اطلاعاتی است که فراتر از مسائل سنتی نظامی و دیپلماتیک رفته است.

انقلابی که معمولاً تعاریف متفاوتی از تهدیدات امنیت ملی ارائه می‌دهند.

اطلاعات داخلی

مهم‌ترین حوزه‌ای که ماهیت نظام بر عملکرد اطلاعاتی تأثیر می‌گذارد، همان چیزی است که «اطلاعات داخلی» نامیده می‌شود. این حوزه برای هر دولتی که نه تنها به تهدیدات صرفاً خارجی (مانند تهاجم خارجی) بلکه به توانایی خود برای حکمرانی و حتی به موجودیت خود نیز اهمیت می‌دهد، حیاتی است. این تهدیدات از افراد یا گروه‌هایی در داخل مرزهای کشور نشأت می‌گیرد؛ مانند تهدیدات ناشی از گروه‌هایی که به دنبال سرنگونی دولت از راه‌های غیرقانونی هستند، از خشونت برای تغییر سیاست‌های دولت استفاده می‌کنند، یا افراد متعلق به نژادها، قومیت‌ها یا ادیان خاص را از ساختار سیاسی حذف می‌کنند. اما نحوه تعریف و شناسایی این تهدیدات داخلی توسط دولت، تا حد زیادی به نوع خود دولت بستگی دارد.

به عنوان مثال، نظامی که از یک سلسله خاص یا یک حزب سیاسی واحد نشأت می‌گیرد و قدرت را در انحصار خود دارد، اغلب هرگونه مخالفت سیاسی داخلی را تهدیدی امنیتی تلقی می‌کند و دستگاه اطلاعاتی بخش قابل توجهی از تلاش خود را به کشف و مهار این مخالفت اختصاص می‌دهد. در موارد شدیدتر، کشورهای دارای

حکومت توتالیتر می‌توانند همه افرادی را که به حزب حاکم تعلق ندارند، دشمنان بالفعل یا بالقوه تلقی کنند[16]. در مقابل، ایده «اپوزیسیون وفادار» که در نظام‌های پارلمانی و سایر نظام‌های دموکراتیک رایج است، به این معناست که مخالفان سیاسی داخلی تهدید امنیتی محسوب نمی‌شوند و اهداف مناسبی برای فعالیت‌های اطلاعاتی نیستند[17].

---

[16] ؛آنچه پس از فروپاشی رژیم کمونیستی در آلمان شرقی آشکار شد، به وضوح نشان می‌دهد که این امر در عمل چه معنایی دارد. با فروپاشی آن رژیم، دستگاه اطلاعاتی جمهوری دموکراتیک آلمان بیش از ۸۵ هزار نفر پرسنل تمام‌وقت، پانصد هزار عامل و خبرچین پاره‌وقت را به کار گرفته بود و پرونده شش میلیون شهروند آلمان شرقی را نگهداری می‌کرد. همان‌طور که جفرسون آدامز توضیح می‌دهد: «در کشوری با جمعیت حدود ۱۷ میلیون نفر، این به معنای یک شبکه بسیار متراکم است.» این مطلب در مقدمه «پیشگفتار نسخه انگلیسی» کتاب «فراسوی دیوارها: خاطرات یک جاسوس در آلمان شرقی و غربی» (انتشارات براسی، واشنگتن دی‌سی، ۱۹۹۲) اثر ورنر استیلر و جفرسون آدامز آمده است.

[17] ؛ شهروندان کشورهای دموکراتیک این موضوع را بدیهی می‌دانند، اما به رسمیت شناختن این امکان که فرد می‌تواند بدون تبدیل شدن به دشمن نظام یا دولت، به مخالف دولت حاکم تبدیل شود، دستاوردی ارزشمند است، حتی اگر برخی آن را حق مسلم خود بدانند. از سوی دیگر، مفهوم «اپوزیسیون وفادار» این امکان را در بر می‌گیرد که این اپوزیسیون در حقیقت یک اپوزیسیون واقعی نباشد. این موضوع از لحاظ نظری تا حدودی واضح به نظر می‌رسد، اما دشواری برای دموکراسی‌های لیبرال در تعیین عملی خط فاصل است. برای آشنایی با تلاش‌های پیشین دولت ایالات متحده در نظارت و گاهی اوقات مختل کردن آنچه

همچنین، گروه‌های داخلی که نه تنها با دولت مستقر، بلکه با اساس نظامی که دولت بر آن بنا شده است (یا خود نظام) دشمنی دارند، می‌توانند به اشکال مختلفی با نیروهای خارجی در ارتباط باشند یا از آن‌ها تأثیر بپذیرند. ممکن است فرد یا گروهی در صفوف اپوزیسیون به نمایندگی از یک قدرت خارجی متخاصم یا تحت هدایت آن عمل کند. یا گروه‌ها و افرادی وجود داشته باشند که اهداف مشابهی با یک قدرت خارجی دارند و برای دستیابی به این اهداف با آن همکاری می‌کنند. در نهایت، ممکن است گروه‌هایی باشند که از نظر ایدئولوژیک یا اعتقادی با دشمنان خارجی همسو هستند، اما ارتباط عملی با آن‌ها ندارند. نظام‌های مختلف دیدگاه‌های متفاوتی درباره اینکه آیا این الگوهای گروه‌ها تهدیدی برای امنیت ملی محسوب می‌شوند و آیا باید اطلاعاتی درباره آن‌ها جمع‌آوری شود، دارند.

اطلاعات و اجرای قانون

مسئله مرتبط با تهدیدات فراملی، که عمدتاً از یک دولت خارجی نشأت نمی‌گیرند، مورد بررسی قرار می‌گیرد. به عنوان مثال: قاچاق

گروه‌ها و سازمان‌های خرابکار می‌پنداشت، کتاب «اطلاعات داخلی: نظارت بر مخالفان در آمریکا» (آستین: انتشارات دانشگاه تگزاس، ۱۹۸۰) اثر ریچارد ای. مورگان را مطالعه کنید.

مواد مخدر، تروریسم بین‌المللی، یا انواع خاصی از جرایم سازمان‌یافته، می‌توانند تهدیدات جدی برای امنیت کشـور ایجاد کنند. اما این موارد بیشـتر در حوزه اجرای قانون قرار می‌گیرند تا عملیات اطلاعاتی؛ با این حال، سازمان‌های اطلاعاتی نیز در مبارزه با آن‌ها مشارکت دارند. دلایل این امر متعدد اسـت. اولاً: این فعالیت‌ها در کشـورهای خارجی انجام می‌شـوند که امکان مداخله نهادهای اجرای قانون سـایر کشـورها را به شـدت محدود می‌کند. ممکن اسـت نهادهای اجرای قانون در این کشـورها قادر یا مایل به همکاری نباشـند. در چنین شـرایطی، سـازمان‌های اطلاعاتی می‌توانند برای کسـب اطلاعات درباره ابعاد خارجی این فعالیت‌ها فراخوانده شـوند؛ اطلاعاتی که بدون کمک آن‌ها در دسترس نخواهد بود.

ثـانیـاً: رویکرد اجرای قـانون مسـتلزم انتظـار برای وقوع جرم یـا قریب‌الوقوع شـدن آن اسـت، سـپس نهادهای اجرای قانون تلاش می‌کنند تا آن جرم خاص را حل و مرتکبین آن را دسـتگیر کنند. اما این رویکرد در مورد تهدیدات فراملی قابل قبول نیسـت؛ زیرا یک حادثه واحـد، ماننـد بمـب‌گـذاری در یـک هواپیمـای مسـافربری، می‌توانـد خسارات زیادی به بار آورد که دولت باید از وقوع آن به عنوان یک جرم پیشگیری کند، نه اینکه پس از وقوع آن را حل و فصل نماید. همچنین، یک جرم خاص مانند یک عملیات قاچاق مواد مخدر، ممکن اسـت

بخشی از یک پروژه جنایی بزرگ و سازمان‌یافته باشد. در این صورت، دستگیری مرتکبین یک جرم واحد ممکن است تأثیر چندانی نداشته باشد؛ زیرا چنین دستگیری‌هایی ممکن است برای سران این گروه‌ها هزینه‌ای قابل قبول در مقایسه با فعالیت‌هایشان تلقی شود. در نهایت، حتی اگر نهادها راضی به انتظار برای وقوع یک جرم خاص باشند، شانس حل آن تا حد زیادی به دسترسی آن‌ها به حجم زیادی از اطلاعات درباره سازمان مجری بستگی دارد.

به همین دلایل، دولت‌ها به جای انتظار برای وقوع یک جرم مشخص، رویکرد اطلاعاتی را در قبال این نوع فعالیت‌ها در پیش می‌گیرند. در این رویکرد، نهادها اطلاعاتی را در طولانی‌مدت درباره افراد و گروه‌ها، از جمله انگیزه‌ها، منابع، ارتباطات داخلی، و نیات آن‌ها جمع‌آوری می‌کنند. معمولاً استفاده از خبرچین‌ها ضروری است، زیرا آن‌ها به گروه‌های درگیر نفوذ کرده و مانند جاسوسان عمل می‌کنند. همچنین، می‌توان ارتباطات را رهگیری کرد یا از سایر روش‌های فنی برای جمع‌آوری اطلاعات بهره برد. بنابراین، سازمان‌های اطلاعاتی معمولاً در مبارزه با گروه‌های فراملی مشارکت دارند و بسته به نظام حکومتی، مشارکت آن‌ها ممکن است به ابعاد خارجی این فعالیت‌ها محدود شود، در حالی که ابعاد داخلی در دست نهادهای اجرای قانون باقی می‌ماند.

حتی در مواجهه با گروه‌های کاملاً داخلیِ جرم سازمان‌یافته، نهادهای اجرای قانون معمولاً از تکنیک‌های اطلاعاتی استفاده می‌کنند. به عنوان مثال: در حوزه اجرای قانون داخلی، اداره تحقیقات فدرال آمریکا (اف‌بی‌آی) بین تحقیقات اطلاعاتی جنایی و تحقیقات مربوط به جرایم عادی تمایز قائل می‌شود. در میان این دو، نوع اول تحقیق به عنوان «گسترده‌تر و کمتر متمایز از معمول» توصیف می‌شود و به جای تمرکز بر خود عمل مجرمانه، بر سازمان جنایی از نظر حجم، ساختار، اقدامات انجام‌شده، اهداف مجرمانه‌ای که قصد انجام آن‌ها را دارد، و توانایی آن برای آسیب‌رسانی تمرکز می‌کند[18]. خط تمایز بین رویکرد اجرای قانون و رویکرد اطلاعاتی این است که آیا تمرکز بر مجازات یک عمل مجرمانه خاص است یا بر مبارزه با سازمانی که در فعالیت‌های مجرمانه درگیر است.

[18] ؛«دستورالعمل‌های دادستان کل در خصوص جرایم عمومی، باج‌گیری و تحقیقات امنیت داخلی و تروریسم»، بخش سوم، سال ۱۹۸۳. این اصول و دستورالعمل‌ها در کمیته قضایی مجلس نمایندگان ایالات متحده و در قالب دستورالعمل‌های امنیت داخلی فدرال، در نود و هشتمین دوره بازنگری در سال ۱۹۸۳ تجدید چاپ شده است.

اقتصاد و اطلاعات

در نهایت، پرسش‌هایی درباره نقش سازمان‌های اطلاعاتی از منظر اقتصادی مطرح می‌شود. و بار دیگر، این موضوع به ماهیت نظام حکومتی و نظام اقتصادی کشور بستگی دارد. در نظامی که دولت اقتصاد را اداره می‌کند، اطلاعات به مسائل اقتصادی از منظر روابط دولت با دولت‌های خارجی (مانند تجارت بین‌الملل) به همان شیوه‌ای که به سایر جنبه‌های روابط بین‌الملل می‌پردازد، توجه خواهد کرد. همچنین، می‌توان از اطلاعات برای بهبود وضعیت اقتصادی کشور بهره برد. به عنوان مثال، دستیابی به فناوری‌های پیشرفته غربی، وظیفه مهمی برای سازمان‌های اطلاعاتی شوروی سابق (و همچنان وظیفه‌ای مهم برای اطلاعات روسیه و چین) بوده است. این فعالیت نه تنها سطح فنی نظامی اتحاد جماهیر شوروی و چین را افزایش داد، بلکه هزینه‌های گزاف و دشواری‌های توسعه فناوری را برای هر دو کشور، چه در زمینه نظامی و چه غیرنظامی، کاهش داد[19].

---

[19] ؛در خصوص برنامه‌های دستیابی شوروی به فناوری، بنگرید به کتاب کاترین ای. اس. اسپلی با عنوان «جاسوسی صنعتی شوروی علیه فناوری نظامی ایالات متحده و پاسخ آمریکا، ۱۹۳۰-۱۹۴۵»، نشریه اطلاعات و امنیت ملی، دوره ۱۴، شماره ۲ (تابستان ۱۹۹۹)، و نیز گزارش «دستیابی نظامی شوروی به فناوری غربی: یک به‌روزرسانی» (واشنگتن دی.سی: دفتر چاپ دولتی، ۱۹۸۵). برای مطالعه شرحی مختصر از برنامه شوروی در دهه ۱۹۷۰ و واکنش ایالات متحده و

در اقتصاد بازار، ابهامات بیشتری پیرامون مسائل اقتصادی که ابعاد امنیت ملی دارند و مشارکت سازمان‌های اطلاعاتی را توجیه یا ایجاب می‌کنند، وجود دارد. در این میان، چندین حوزه مشخص وجود دارد، از جمله ارزیابی پتانسیل‌های اقتصادی یک رقیب نظامی احتمالی، یا پیگیری تحولاتی که بر جریان منابع استراتژیک حیاتی تأثیر می‌گذارند و دولت‌ها خواهان جزئیات آن‌ها هستند. استفاده از سازمان‌های اطلاعاتی و تکنیک‌های آن‌ها برای کسب این اطلاعات، تا حدی به این

متحدانش، بنگرید به مقاله گاس دبلیو. وایس با عنوان «پرونده وداع»، نشریه مطالعات اطلاعاتی، دوره ۳۹، شماره ۵ (۱۹۹۶)، قابل دسترسی در تارنمای www.odci.gov/csi/studies/96unclass/farewell.htm. به نظر می‌رسد سرویس اطلاعات خارجی روسیه همچنان به جمع‌آوری اسرار صنعتی و فنی سایر کشورها ادامه داده است. مرکز ملی ضدجاسوسی ایالات متحده (NACIC) — یک نهاد بین‌سازمانی که تحت نظارت شورای امنیت ملی فعالیت می‌کند — به نقل از منابع رسانه‌ای اعلام کرد که بوریس یلتسین، رئیس‌جمهور وقت روسیه، در ۷ فوریه ۱۹۹۶ در مسکو تایید کرد که روسیه در جاسوسی صنعتی دست دارد، هرچند داده‌های جمع‌آوری‌شده توسط نهادهای اطلاعاتی روسیه به طور موثر مورد استفاده قرار نمی‌گیرند؛ بنگرید به: گزارش اخبار و تحولات ضدجاسوسی NACIC، مارس ۱۹۹۶، قابل دسترسی در تارنمای www.nacic.gov/cind/1996/mar96.htm. در ارتباط با برنامه چین، بنگرید به «گزارش کمیته کاکس»: گزارش کمیته منتخب امنیت ملی ایالات متحده و دغدغه‌های نظامی و تجاری با جمهوری خلق چین (واشنگتن دی.سی: دفتر چاپ دولتی، ۱۹۹۹)، فصل اول، قابل دسترسی در تارنمای www.house.gov/coxreport.

بســـتگی دارد که آیا کشـــورهای دیگر تلاش می‌کنند این اطلاعات را محرمانه نگه دارند یا خیر. به طور کلی، مسائل اقتصادی که مستقیماً بر ارتش یا ملاحظات سیاست خارجی امنیت ملی تأثیر می‌گذارند، در حیطه اختیارات ســازمان‌های اطلاعاتی قرار می‌گیرند. به عنوان مثال: در زمان جنگ، می‌توان به ابزارهای اطلاعاتی برای دســتیابی به مواد استراتژیک (یا جلوگیری از دسترسی دشمن به آن‌ها) به عنوان یک هدف اصــلی امنیت ملی متوســل شــد. به همین ترتیب، در جریان مذاکرات با یک کشور خارجی درباره مسائل اقتصادی، ممکن است کشـــوری به ابزارهای اطلاعاتی خود متوســـل شـــود تا از مواضـــع طرف‌های مذاکره‌کننده آگاه شود.

تمایل یک کشور برای کسب اطلاعات اقتصادی درباره فعالیت‌های صنعتی، تجاری و مالی سایر کشورها، به این بستگی دارد که آیا دولت آن کشور دارای بوروکراسی «سیاست صنعتی» است که بتواند از این اطلاعات بهره‌برداری کند یا خیر. بنابراین، پرســش‌ها درباره بهره‌برداری از ســازمان‌های اطلاعاتی برای جمع‌آوری اطلاعات اقتصــادی، صــرفاً جایگزینی برای بحثی عمیق‌تر درباره نقش دولت در هدایت آینده اقتصادی کشور است.

پرسش گسترده‌تر این است که آیا سازمان‌های اطلاعاتی مایلند برای توسعه اقتصاد یک کشور[20] به کار گرفته شوند یا خیر. با پایان جنگ سرد، خطر رویارویی نظامی بین قدرت‌های بزرگ از میان رفت و به

[20] ؛پدیده‌ای متمایز و مستقل که ارتباط مستقیمی با نقش سنتی نهادهای اطلاعاتی در پشتیبانی از فرآیند سیاست‌گذاری ندارد، بهره‌گیری دولت‌ها از ظرفیت‌های اطلاعاتی برای کسب درآمدهای مالی است. سرویس‌های اطلاعاتی فرصت‌های متعددی برای درآمدزایی در اختیار دارند که عواید آن یا صرف تأمین مالی عملیات‌های ویژه خودشان می‌شود و یا به خزانه دولت متبوع واریز می‌گردد. توانمندی‌های عملیاتی پنهان این سرویس‌ها می‌تواند در فعالیت‌های سودآوری همچون قاچاق مواد مخدر و دیگر اشکال قاچاق سازمان‌یافته به کار گرفته شود. علاوه بر این، ظرفیت‌های جمع‌آوری پنهان اطلاعات می‌تواند دسترسی به داده‌های درونی و محرمانه را برای گمانه‌زنی‌ها و معاملات کلان مالی فراهم سازد. هرچند میزان استفاده دقیق کشورها از دستگاه‌های اطلاعاتی خود برای این منظور چندان روشن نیست، اما نمونه‌هایی از آن افکار عمومی را به خود جلب کرده است؛ از جمله موردی که توجه جامعه فرانسه را جلب کرد. بر اساس اظهارات رئیس سابق سرویس اطلاعات خارجی فرانسه، این سازمان در نوامبر ۱۹۷۱ دریافت که دولت ایالات متحده تصمیم دارد در ماه بعد استاندارد طلا را کنار بگذارد. در پی این آگاهی پیش‌دستانه، سرویس اطلاعاتی فرانسه با فروش چراغ‌خاموش دلار و خرید فرانک در بازارهای جهانی، عملاً از کاهش ارزش دلار نهایت بهره را برد. این اقدام به بانک مرکزی فرانسه امکان داد تا سودهای کلانی انباشت کند؛ مبالغی که برای تأمین مالی تمامی عملیات‌های آتی این سرویس کفایت می‌کرد (کنت دو مارنچ و دیوید ای. اندبلهان، جنگ جهانی چهارم، نیویورک: مورو، ۱۹۹۲).

نظر می‌رسید که قدرت اقتصادی در تعیین جایگاه و اعتبار جهانی کشورها اهمیت فزاینده‌ای پیدا کرده است. در نتیجه، علاقه به نقشی که اطلاعات می‌تواند در تقویت اقتصاد ایفا کند، افزایش یافت[21].

با این حال، رفاه اقتصادی یک کشور در طول زمان به دلیل عواملی مانند نرخ سرمایه‌گذاری، بهره‌وری نیروی کار، مهارت‌های مدیریتی و سطح آموزش نیروی کار، دچار نوسان می‌شود. در حالی که بسیاری از تحولات در اقتصاد جهانی می‌توانند پیامدهای مهمی برای امنیت ملی یک کشور داشته باشند، مشخص نیست که آیا دولت باید – یا حتی می‌تواند – اقدامات زیادی در قبال این تحولات انجام دهد.

---

[21] ؛ایالات متحده با توجه به اقتدار اقتصادی و فناورانه خود، تمرکز ویژه‌ای بر حفاظت از فناوری‌ها و اسرار تجاری معطوف کرده است. از سال ۱۹۹۵، رئیس‌جمهور آمریکا گزارش‌های سالانه‌ای را در خصوص جاسوسی‌های خارجی هدفمند علیه صنایع این کشور به کنگره ارائه می‌دهد. این گزارش‌ها به همراه «قانون جاسوسی اقتصادی مصوب ۱۹۹۶» در وب‌سایت مرکز ملی ضدجاسوسی (www.nacic.gov) قابل دسترسی است. منابع دیگری نیز در این زمینه وجود دارند؛ از جمله گزارش دیوان محاسبات آمریکا با عنوان «جاسوسی اقتصادی: اطلاعاتی درباره تهدیدات ناشی از متحدان ایالات متحده» (GAO / T-NSIAD-96-114) که در آدرس اینترنتی www.nsi.gov/Library/Espionage/allies.txt در دسترس است، و همچنین مقاله پیتر شوایتزر با عنوان «رشد جاسوسی اقتصادی: آمریکا هدف نخست است» منتشر شده در نشریه فارین افرز، دوره ۷۵، شماره ۱ (ژانویه - فوریه ۱۹۹۶).

همچنین، در یک جامعه دموکراتیک، سیاست اقتصادی اغلب بیش از آنکه بر اســـاس یک چشـــم‌انداز یکپارچه – چه مبتنی بر اطلاعات اطلاعاتی باشـــد و چه نباشـــد – از محیط اقتصـــادی جهانی آینده برنامه‌ریزی شـود، تابع منافع اقتصـادی داخلی اسـت. به همین دلایل، مشـــخص نیســـت که آیا دولت ایالات متحده از این نوع اطلاعات اطلاعاتی بهره‌بردار مهمی خواهد بود یا خیر. شـــاید منافع اقتصـــادی خصـوصـی بتوانند از این اطلاعات اطلاعاتی بهتر بهره‌برداری کنند، اما مشـــخص نیســـت که آیا اطلاعاتی که به صـــورت محرمانه و با هزینه دولت جمع‌آوری شـــده‌اند، می‌توانند به طور مســـاوی بین افراد یا مؤسسات توزیع شوند تا منافع خصوصی بیشتری را تأمین کنند[22].

[22] ؛محدودیت‌های خودخواســـته‌ای که ایالات متحده بر بهره‌برداری از اطلاعات اقتصادی اعمال کرده، مانع از طرح اتهامات از سوی سایر کشورها نشده است؛ موضوعی که در جنجال‌های پیرامون سیستم «اشلون» جهت جمع‌آوری داده‌ها از ارتباطات بین‌المللی به وضـوح نمایان اسـت. اصـطلاح اشـلون به یک سـامانه خودکـار برای غربـالگری حجم عظیمی از داده‌هـای رهگیری‌شـــده بـه روش‌هـای گوناگون توسـط ایالات متحده و متحدان انگلیسـی‌زبان آن اشـاره دارد. در همین راســـتا، گزارش جنجالی ارائه‌شـــده به پارلمان اروپا در فوریه ســـال ۲۰۰۰، ایالات متحده و متحدانش را متهم کرد که از اطلاعات حاصل از این سیستم برای کمک به شـــرکت‌های خود جهت کســـب مزیت‌های تجاری بهره‌برداری می‌کنند. این گزارش با عنوان «قابلیت‌های رهگیری ۲۰۰۰» توسـط دانکن کمپبل برای مدیرکل تحقیقات پارلمان اروپا (دفتر ارزیابی گزینه‌های علمی و فناوری) تهیه شـــده و در

سایر مسائل غیرسنتی

برخی از پژوهشگران اطلاعاتی، به ویژه در کنار اقتصاد، نوع دیگری از امور «غیرسنتی» را در حیطه کاری اطلاعات قرار می‌دهند؛ مانند مسائل زیست‌محیطی، که در مورد تأثیر مشکلات زیست‌محیطی بر امنیت ملی بحث و جدل داغی وجود دارد. به نظر می‌رسد انگیزه اصلی این است که فناوری‌های سیستم‌های جمع‌آوری اطلاعات که برای اهداف دیگر توسعه یافته‌اند، می‌توانند برای ردیابی تغییرات

آدرس اینترنتی www.iptvreports.mcmail.com/ic2kreport.htm#Report در دسترس است.

این اتهامات به طور کلی توسط جیمز وولسی، رئیس سابق سازمان اطلاعات مرکزی آمریکا (سیا)، در یک نشست خبری در ۷ مارس ۲۰۰۰ رد شد. وولسی مدعی شد که هدف‌گیری اطلاعاتی شرکت‌های خارجی صرفاً به سه حوزه محدود بوده است: اجرای تحریم‌ها، نظارت بر فروش مواد و تجهیزات مرتبط با تسلیحات کشتار جمعی، و افشای تلاش‌های شرکت‌های غیرآمریکایی برای پرداخت رشوه در رقابت با شرکت‌های ایالات متحده. وی همچنین خاطرنشان کرد موارد مشخصی که کمپبل به آن‌ها اشاره کرده، شامل تلاش‌های شرکت‌های غیرآمریکایی برای برنده شدن در قراردادهای صادراتی از طریق پرداخت رشوه به مقامات کشورهای خریدار بوده است. این اظهارات در جریان گزارش توجیهی مرکز مطبوعات خارجی با عنوان «جمع‌آوری اطلاعات و دموکراسی‌ها: مسئله جاسوسی اقتصادی و صنعتی» مطرح گردید و در آدرس اینترنتی www.fpc.gov/wool0300.htm قابل دسترسی است.

زیست‌محیطی در طول زمان و در مناطق وسیع مورد استفاده قرار گیرند و این کار با هزینه اضافی ناچیزی امکان‌پذیر است[23].

اطلاعات و عصر اطلاعات

از آنجا که اطلاعات با داده‌ها سروکار دارد، بدیهی است که با ظهور «عصر اطلاعات» به شدت تحت تأثیر قرار گرفته و همچنان تأثیر می‌پذیرد. مفهوم عصر اطلاعات، اگرچه به اذعان همگان مبهم است، اما از اهمیت بسیار بالایی برخوردار است. این مفهوم نحوه عملکرد بسیاری از نهادها – به ویژه سازمان‌های تجاری – را تغییر داده و به احتمال زیاد تأثیرات مهمی بر دولت نیز خواهد داشت.

---

[23] ؛ بر اساس یکی از پژوهش‌های انجام‌شده در این زمینه، ایالات متحده از مجموعه‌ای چشمگیر از سامانه‌های فنی برای پایش بخش‌های وسیعی از زمین، اقیانوس‌ها و جو با اهداف امنیت ملی برخوردار است. این سامانه‌ها در طول دهه‌های متمادی، حجم عظیمی از اطلاعات پیچیده را گردآوری کرده‌اند که یک آرشیو تاریخی بی‌نظیر را شکل می‌دهد. افزون بر این، ظرفیت سامانه‌های یادشده می‌تواند در حوزه پایش‌های زیست‌محیطی نیز به کار گرفته شود.
اسکات پیس، کوین ام. اوکانل و بث ای. لاکمن، استفاده از داده‌های اطلاعاتی برای نیازهای زیست‌محیطی: موازنه مصالح ملی، MR-799-CMS (سانتا مونیکا، کالیفرنیا: مؤسسه رند، ۱۹۹۷).

از منظر فنی، عامل محرک، پیشرفت چشمگیر تکنولوژیکی در پردازش و انتقال اطلاعات است. با این حال، تغییرات فنی تنها بخش کوچکی از تصویر است؛ آنچه اهمیت بیشتری دارد، تغییرات رفتاری و نهادی است که از تمرکز بر اطلاعات به عنوان کلید فعالیت سازمانی ناشی شده است. (در حوزه نظامی، آنچه معمولاً به عنوان «انقلاب در امور نظامی» از آن یاد می‌شود، اساساً بر بهبود عملکرد انواع جدید تسلیحات دقیق از نظر دقت اصابت با بهره‌گیری از اطلاعات، و همچنین بر ارتقای توانایی این تسلیحات در جمع‌آوری، پردازش و انتقال به موقع این اطلاعات برای اهداف عملیاتی متکی است.)

تأثیر این تغییرات به اشکال مختلفی نمایان می‌شود؛ این تغییرات روش‌های جدیدی را برای گردش و بهره‌برداری سریع‌تر از اطلاعات در داخل دولت فراهم می‌کنند و بدین ترتیب، فرآیند سیاست‌گذاری و اجرای آن را تسهیل می‌بخشند. همچنین، این تغییرات توجه کل جامعه را به اطلاعات در حال گردش، هم در بخش‌های غیر اطلاعاتی دولت و هم در خارج از آن، جلب می‌کنند. به این معنا که سازمان‌های اطلاعاتی درمی‌یابند که انواع دیگر سازمان‌ها – مثلاً شرکت‌های رسانه‌های اجتماعی – در حال تبدیل شدن به متخصصانی ماهرتر در جمع‌آوری، تحلیل و انتقال اطلاعات هستند. در نتیجه، سازمان‌های اطلاعاتی در کار خود برای تأمین اطلاعات برای سیاستمداران، رقبایی

پیدا کرده‌اند. از منظر کل دولت، سؤال اصلی این است: چگونه می‌توان اطلاعات تولید شده توسط سایر اقشار جامعه را به مؤثرترین شکل ممکن به کار گرفت؟ و چگونه می‌توان اطمینان حاصل کرد که محصول منحصر به فرد سازمان‌های اطلاعاتی با سایر اطلاعات از منابع دیگر به گونه‌ای مقایسه و ترکیب شود که نیازهای اطلاعاتی دولت را به بهترین نحو برآورده سازد؟[24]

عناصر اطلاعاتی

صرف‌نظر از گستره پوشش، اطلاعات را می‌توان بر اساس نوع فعالیت به چهار مؤلفه تقسیم کرد. این دسته‌ها معمولاً «عناصر اطلاعاتی» نامیده می‌شوند: **جمع‌آوری**، **تحلیل**، **عملیات پنهان** و **ضد اطلاعات**. از آنجا که این عناصر در ادامه این کتاب به تفصیل مورد بحث قرار خواهند گرفت، در بندهای زیر به تشریح ماهیت چهار نوع فعالیت اطلاعاتی و ترسیم روابط میان آن‌ها می‌پردازیم.

---

[24] ؛ درباره پیامدهای احتمالی عصر اطلاعات بر سازمان‌های اطلاعاتی، به کتاب بروس برکوویتز و آلن گودمن با عنوان «اطلاعات در عصر اطلاعات» مراجعه کنید.

واژه «**جمع‌آوری**» به گردآوری داده‌های خام اشاره دارد؛ از طریق جاسوسی، ابزارهای فنی (عکاسی، رهگیری ارتباطات الکترونیکی و سایر روش‌های فنی)، بهره‌برداری از «منابع آشکار» (مانند نشریات، پخش رادیویی و تلویزیونی) یا هر وسیله دیگری. شکی نیست که جمع‌آوری اطلاعات جزء لاینفک فعالیت‌های اطلاعاتی است، اما در مورد اهمیت نسبی روش‌های مختلف جمع‌آوری اطلاعات اختلاف‌نظر وجود دارد. به عنوان مثال، پژوهشگران اطلاعاتی درباره اهمیت نسبی جمع‌آوری اطلاعات از «منابع آشکار» در برابر روش‌های منحصربه‌فرد سازمان‌های اطلاعاتی، و اهمیت نسبی جاسوسی انسانی در برابر جمع‌آوری اطلاعات با ابزارهای فنی بحث کرده‌اند.

کیفیت اطلاعات جمع‌آوری‌شده هر چقدر هم بالا باشد، به خودی خود گویا نیست؛ یعنی برای مفید بودن اطلاعات برای سیاست‌مداران و فرماندهان نظامی، **تحلیل** آن‌ها ضروری است. در بیشتر موارد، اطلاعات جمع‌آوری‌شده پراکنده، مبهم و مستعد تفاسیر گوناگون است. بنابراین، فرآیند تحلیل اطلاعات موجود برای رسیدن به قضاوت‌هایی درباره توانایی‌ها، نیات و اقدامات طرف مقابل، بخش اساسی کار اطلاعاتی است. اما دشوارتر از آن، فرآیند پیش‌بینی – یا به اصطلاح حرفه‌ای اطلاعاتی آمریکا، «برآورد» – توانایی‌ها، نیات و اقدامات آتی یک دولت خارجی یا سازمان سیاسی است.

عملیات پنهان از نظر مفهومی با سایر عناصر متفاوت است. در حالی که سایر عناصر به کسب و حفاظت از اطلاعات می‌پردازند، عملیات پنهان به دنبال تأثیرگذاری مستقیم بر اقدامات سیاسی است. درجات عملیات پنهان می‌تواند از اقناع و پروپاگاندا تا اقدامات شبه‌نظامی متغیر باشد؛ به گونه‌ای که آن را «عملی در میانه دیپلماسی و جنگ» توصیف می‌کنند[25].

اگرچه تکنیک‌های اعمال این تأثیر متعددند، اما همگی دارای ویژگی پنهان‌کاری هویت هستند؛ به این معنا که نقش دولت در اجرای این فعالیت کاملاً آشکار یا برای عموم شناخته‌شده نیست. از این رو، توانایی یک سازمان اطلاعاتی برای فعالیت مخفیانه اغلب به این معناست که ممکن است مسئولیت اجرای عملیات پنهان نیز به آن محول شود. اما همان‌طور که پیش‌تر گفته شد، از آنجا که این فعالیت‌ها بیشتر شامل اجرای سیاست‌ها هستند تا ارائه اطلاعات به تصمیم‌گیرندگان، گهگاه در ایالات متحده این بحث مطرح می‌شود که عملیات پنهان وظیفه همان سازمان‌های اطلاعاتی (یعنی آژانس اطلاعات مرکزی، سیا) نیست که اطلاعات را جمع‌آوری و تحلیل

---

[25] ؛ کمیته ایالات متحده برای سازماندهی دولت در سیاست خارجی (کمیته مورفی)، گزارش (واشنگتن دی‌سی، انتشارات ملی، ۱۹۷۵).

می‌کنند. از سوی دیگر، ایالات متحده و بریتانیا از طریق تجربه دریافتند که اتکا به دو سازمان برای اجرای عملیات‌های مخفی (یکی برای جاسوسی و دیگری برای عملیات پنهان) می‌تواند به رقابتی منجر شود که انرژی‌ها را هدر داده، تلاش‌ها را مضاعف کرده و وظایف را با یکدیگر تداخل دهد[26].

ضد اطلاعات در معنای عام‌تر خود، به دنبال حفاظت از جامعه (و به ویژه توانمندی‌های اطلاعاتی آن) در برابر آسیب‌هایی است که ممکن است از سوی سازمان‌های اطلاعاتی متخاصم به آن وارد شود. ضد اطلاعات در وهله اول به دنبال محروم کردن رقبا از اطلاعات خاص است. این حفاظت از طریق برنامه‌های امنیتی (اقداماتی که برای دور نگه داشتن اطلاعات از دسترس افراد فاقد مجوز دسترسی اتخاذ

---

[26] ؛ به کتاب جان رانلاف با عنوان «آژانس: ظهور و سقوط سیا» (۱۹۸۰) مراجعه کنید که به بررسی درگیری‌های اواخر دهه ۱۹۴۰ و ۱۹۵۰ میلادی میان دفتر هماهنگی سیاست‌ها (بازوی عملیات پنهان دولت آمریکا) و دفتر عملیات ویژه (بازوی جاسوسی سیا) می‌پردازد. همچنین، کتاب کریستوفر اندرو با عنوان «سرویس مخفی علیاحضرت: شکل‌گیری جامعه اطلاعاتی بریتانیا» (نیویورک: وایکینگ، ۱۹۸۶) به رقابت میان اطلاعات بریتانیا و رئیس سرویس عملیات ویژه می‌پردازد.

می‌شـود) و ضـد جاسـوسـی (اقداماتی که برای دسـتگیری یا خنثی کردن عوامل خارجی به منظور جلوگیری از دستیابی و انتقال اطلاعات محرمانه انجام می‌شـــود) محقق می‌گردد. همچنین، ضـــد اطلاعات می‌تواند به پیشـــگیری از تحلیل اطلاعات دشـــمن و نیز جلوگیری از جمع‌آوری اطلاعـات توســـط او توجه کنـد؛ این کـار از طریق عملیـات فریب انجام می‌شـــود که عمداً اطلاعات نادرســـت یا گمراه‌کننده را به دشـــمن ارائه می‌دهد تا او را به نتایج اشـــتباهی درباره توانایی‌ها، اقدامات یا نیات ما برســـاند. با این حال، حفاظت از خود در برابر ســـازمان‌های اطلاعاتی دشـــمن، فعالیت‌های دیگری را نیز می‌طلبد. شـاید لازم باشـد اقداماتی برای اطمینان از اینکه فرد قربانی اطلاعات گمراه‌کننده‌ای که عمداً توسـط طرف مقابل ارائه شـده، نیسـت، اتخاذ شود. بنابراین، ضد اطلاعات باید یکپارچگی بین دو وظیفه جمع‌آوری و تحلیل اطلاعات را حفظ کند. همچنین، ممکن اســـت فرد بخواهد از عملیات پنهان یک دولت خارجی که قصـد دارد از طریق آن بر دولت یا جامعه ما تأثیر بگذارد، آگاه شـود. در نهایت، گسـتره فعالیت‌های ضـد اطلاعاتی با تهدیدی که از سـوی دامنه فعالیت‌های اطلاعاتی دشـمن ایجاد می‌شود، تعیین می‌گردد.

فصل دوم: جاسوس‌ها، ماشین‌ها و کتابخانه‌ها (جمع‌آوری داده‌ها)

بررسی عناصر اطلاعاتی را با پرداختن به جمع‌آوری داده‌ها آغاز می‌کنیم؛ داده‌هایی که – پس از کشف ارتباط و تحلیل آن‌ها – مبنای

ارزیابی اطلاعاتی را تشـــکیل می‌دهند. روش‌های گوناگون گردآوری داده‌ها (روش‌های اطلاعاتی) را می‌توان به سه دسته تقسیم کرد:

۱- اطلاعاتی که از منابع انسانی جمع‌آوری می‌شود (که معمولاً به آن جاســـوســـی، جمع‌آوری اطلاعات انســـانی یا به اصـــطلاح حرفه‌ای آمریکایی، HUMINT گفته می‌شود).

۲- اطلاعاتی که با ابزارهای فنی جمع‌آوری می‌شـود (اطلاعات فنی یا TECHINT).

۳- جمع‌آوری داده‌ها از منابع غیرمحرمانه از طریق روابط دیپلماتیک یا منابع اطلاعاتی عمومی مانند روزنامه‌ها، وب‌سایت‌ها و سایر منابع مبتنی بر اینترنـت، رادیو و تلویزیون (جمع‌آوری اطلاعـات از منـابع آشکار یا OSINT)[27].

[27] ؛ این دسـته‌بندی شـامل رایج‌ترین روش‌های جمع‌آوری اطلاعات اسـت، اما به معنای انحصار آن نیست. برای مثال، اطلاعات می‌تواند از طریق سرقت اسناد و کدهای محرمانه از سـفارت دشـمن جمع‌آوری شـود. این نوع سـرقت را می‌توان اطلاعات انسـانی (HUMINT) تلقی کرد، اما همان‌طور که متن اشـاره می‌کند، با جاسوسی تفاوت دارد.

جمع‌آوری اطلاعات انسانی

اولین چیزی که با شنیدن واژه «اطلاعات» به ذهن می‌رسد، جمع‌آوری اطلاعات انسانی – یعنی جاسوسی – است. جاسوسی به طور کلی شامل شناسایی و جذب یک مقام خارجی است که – به واسطه موقعیت مورد اعتماد خود در دولت کشورش – می‌تواند به اطلاعات مهمی دسترسی پیدا کند و به دلایل خاصی، آن‌ها را به مقامات یک سازمان اطلاعاتی منتقل کند. در برخی موارد – به ویژه در زمان جنگ – ممکن است فردی که اطلاعات را ارائه می‌دهد، یک مقام دولتی نباشد، بلکه یک فرد عادی باشد که فرصت دیده یا شنیدن چیزی مهم را یافته است، مانند ورود و خروج کشتی‌ها از بندر. فردی که ممکن است جذب شود، می‌تواند به واسطه رابطه نزدیک (مانند دوستی یا معاملات تجاری و غیره) با شخصی که کارش به فعالیت اطلاعاتی مرتبط است (مانند یک تروریست یا دلال بین‌المللی اسلحه)، از اطلاعات مهمی آگاه باشد.

معمولاً دو نفر در این کار نقش‌های متفاوتی ایفا می‌کنند: یک افسر اطلاعاتی که در یک سازمان اطلاعاتی کار می‌کند، و یک منبع که اطلاعات را به افسر ارائه می‌دهد تا به فرماندهی سازمان اطلاعاتی ارسال شود. افسر اطلاعاتی – یا «اپراتور» – با منبع در تماس است، دستورالعمل‌ها را از فرماندهی سازمان اطلاعاتی منتقل می‌کند،

منابع ضـروری (مانند تجهیزات کپی یا ارتباطی) را فراهم می‌آورد و به طور کلی، تلاش می‌کند تا جریان اطلاعات ادامه یابد[28].

انواع افسران اطلاعاتی

افسـران اطلاعاتی باید دور از چشـم دولت کشـوری که در آن فعالیت می‌کنند، کار کنند. آن‌ها نمی‌توانند کار خود را با اعلام تمایل به خرید اسـرار در ازای پول آغاز کنند، بلکه افسـران اطلاعاتی به آنچه در زبان حرفه‌ای «پوشـش» نامیده می‌شـود، نیاز دارند؛ یعنی: دلیلی موجه برای اقامت در کشـور، پوشـش‌های آشـکار برای دریافت حمایت مالی، و بهانه‌ای برای ملاقات با کسـانی که می‌توانند به اطلاعات حسـاس دسترسی پیدا کنند و غیره.[29]

---

[28] ؛ متأسفانه، اصطلاح رایج «عامل (agent) «تا حدودی مبهم است؛ زیرا معمولاً به «منبع» اشـاره دارد، اگرچه گاهی در زبان بوروکراتیک فدرال آمریکا به «افسـر اطلاعاتی» نیز اطلاق می‌شود.

[29] ؛ برای سـاده‌سـازی، این روایت به افسـران اطلاعاتی می‌پردازد که مأموریت جاسـوسـی از کشـورهایی را بر عهده دارند که به آنجا اعزام شـده‌اند. اما وضـعیت همیشـه این‌گونه نیسـت؛ گاهی یک افسـر به کشـور «س» فرسـتاده می‌شـود تا از

در حال حاضـــر، زبان حرفه‌ای آمریکایی بین پوشـــش «رســـمی» و پوشش «غیررسمی» تمایز قائل می‌شود. پوشش رسمی به معنای پنهان کردن هویت افســـر اطلاعاتی به عنوان یک دیپلمات یا نوع دیگری از مقامات دولتی اسـت که به خارج از کشـور اعزام می‌شـوند. پوشـش غیررسـمی به هر نوع پنهان‌کاری دیگری اشـاره دارد – مانند یک تاجر، روزنامه‌نگار، یا توریســـت و غیره – که دلیلی برای حضـــور افسـر در کشـور میزبان فراهم می‌کند. پوشـش غیررسـمی می‌تواند ملیت یک افســـر را پنهان کند و او وانمود کند که از کشـــوری غیر از کشور واقعی [30]خود است. اگر کشور میزبان از جمله کشورهایی باشد که مهاجر می‌پذیرد، افسر می‌تواند تحت این پوشش وارد شود.

کشـور «ع» (مانند افسـران اطلاعاتی، نظامی یا کارکنان سـفارت) که در آنجا نیز اقامت دارند، عامل جذب کند. در این حالت، هویت این افســـران (روابط اطلاعاتی آن‌ها) ممکن است برای مقامات کشور «س» فاش شود و هدف از پوشش آن‌ها، جلوگیری از برانگیختن سوءظن کشور «ع» است. همچنین، افسران اطلاعاتی در کشور خود نیز برای جذب دیپلمات‌های خارجی مستقر در آنجا فعالیت می‌کنند.

[30] ؛ در ادبیات اطلاعاتی برخی کشـورها (مانند اتحاد جماهیر شـوروی سـابق)، به جای پوشـــش رســـمی/غیررســـمی، بین افســـران «قانونی» و «غیرقانونی» در پوشش تمایز قائل می‌شدند. این تمایز نه بر قانونی بودن حضور افسر در کشور میزبان، بلکه بر نحوه ارتباط او با ســـتاد اطلاعاتی‌اش اســـتوار بود. افســـر

استفاده از پوشش رسمی مزایای متعددی دارد که بارزترین آن‌ها امکان اعطای مصونیت دیپلماتیک به افسر اطلاعاتی است. اگر فعالیت‌های جاسوسی او کشف شود، تنها کاری که کشور میزبان می‌تواند طبق محدودیت‌های حقوق بین‌الملل انجام دهد، این است که او را «عنصر نامطلوب» اعلام کرده و از کشور اخراج کند. همچنین، وانمود کردن افسر اطلاعاتی به عنوان یک دیپلمات، او را قادر می‌سازد تا به برخی منابع دیپلماتیک دسترسی پیدا کند، به طوری که می‌تواند – بدون برانگیختن سوءظن – با مقامات کشور میزبان به عنوان بخشی از کار عادی خود، و نیز با دیپلمات‌های کشورهای دیگر مقیم در پایتخت آن کشور ملاقات کند. از آنجا که کشورهای دیگر نیز از پوشش رسمی برای افسران اطلاعاتی خود استفاده خواهند کرد، افسران اطلاعاتی فرصت خواهند داشت تا با این افسران نیز به صورت «غیررسمی» ارتباط برقرار کنند[31].

«غیرقانونی» کسی است که مستقیماً با ستاد اطلاعاتی خود ارتباط برقرار می‌کند، بدون اینکه از طریق نهادهای «قانونی» در کشور میزبان (مانند سفارت، کنسولگری، یا وابسته بازرگانی) اقدام کند.

[31] ؛ به‌طور متناقض، در برخی موارد، نظارت سرویس اطلاعاتی یک کشور بر کارکنان سفارتخانه‌های خارجی و به‌طور کلی اتباع بیگانه آن‌قدر شدید است که

تنها راه امن برای برقراری ارتباط با یک منبع در دولت آن کشور، تماس یک افسر اطلاعاتی با پوشش دیپلماتیک، به شیوه‌ای نسبتاً «آشکار» است. برای مثال، در مورد اولگ پنکوفسکی، سرهنگ اطلاعات نظامی شوروی (GRU) که در اوایل دهه ۱۹۶۰ برای اطلاعات آمریکا و بریتانیا کار می‌کرد، مشکل اصلی چگونگی تماس با او در مسکو بود. نظارت شدید ضدجاسوسی شوروی، تلاش برای ملاقات یا تماس مخفیانه با او را بسیار پرخطر می‌ساخت. یکی از راه‌حل‌ها این بود که از این واقعیت استفاده شود که پنکوفسکی در چارچوب کار عادی خود در زمینه علم و فناوری، با بسیاری از دیپلمات‌های بریتانیایی و آمریکایی ملاقات می‌کرد. یک افسر اطلاعاتی که خود را دیپلمات جا زده بود، توانست با او ارتباط برقرار کند. او از یک علامت از پیش تعیین‌شده (مانند بستن گیره کراوات با سنگ‌های قرمز) استفاده می‌کرد تا به پنکوفسکی اجازه دهد که مثلاً به دستشویی برود، و [دیپلمات/افسر اطلاعاتی] می‌توانست پنج دقیقه بعد او را دنبال کرده و پیامش را دریافت کند. نیازی به گفتگوی شخصی یا چیز دیگری نبود. [چنین ملاقات‌هایی]... امن بودند، زیرا در عرض دو یا سه دقیقه، مواد ارسالی به دست امن می‌رسید و کار تکمیل می‌شد. نیازی به سفر نبود... این روشی است که... بیشترین امنیت را فراهم می‌کند. متأسفانه، روش‌های دیگری که امنیت کمتری داشتند، مکرراً مورد استفاده قرار گرفتند و به نظر می‌رسد این امر به شناسایی پنکوفسکی به عنوان جاسوس، دستگیری و در نهایت اعدام او کمک کرد. به کتاب جرولد ال. شکتر و پیتر اس. در یابین با عنوان «جاسوسی که جهان را نجات داد» (نیویورک: اسکریبنز، ۱۹۹۲) مراجعه کنید.

همچنین، عوامل اطلاعاتی مقیم در یک سفارت تحت پوشش رسمی، تضمین می‌کنند که با برخی حوادث اضطراری به خوبی برخورد شود. اگر شهروندی از کشور میزبان با اطلاعات حساس به سفارت مراجعه کند یا پیشنهاد ارائه این اطلاعات را بدهد، در این صورت می‌توان این مسائل را توسط متخصصان کار اطلاعاتی مدیریت کرد. از این رو، وجود پوشش اطلاعاتی رسمی، تلاش‌های شهروندان کشور میزبان برای تماس با سازمان اطلاعاتی را تسهیل می‌کند. چنین مکان‌هایی به عنوان «صندوق پستی» مفید و حتی ضروری هستند، به ویژه در کشورهایی که سفر شهروندان خود به کشورهای دیگر را به شدت محدود یا ممنوع می‌کنند[32].

[32] ؛ برای اینکه این مکان‌ها به عنوان «صندوق پستی» عمل کنند، باید به‌طور کلی – حتی اگر رسماً به رسمیت شناخته نشود – این درک وجود داشته باشد که سفارت یا نهاد دیپلماتیک، کارکنانی دارد که قادر به رسیدگی به اطلاعات حساس یا محرمانه از منابع ناخواسته هستند. آلن دالس، مدیر سابق سازمان اطلاعات مرکزی (سیا)، مثالی از ماهیت نیمه‌عمومی این نوع فعالیت اطلاعاتی ارائه می‌دهد. به گفته دالس، اندکی پس از اعزام او به عنوان افسر اطلاعاتی به سوئیس در طول جنگ جهانی دوم، یک مجله برجسته سوئیسی داستانی منتشر کرد که او را فرستاده ویژه و مخفی رئیس‌جمهور روزولت توصیف می‌کرد. دالس اشاره کرد که این داستان «بداهه و بدون پشتوانه اطلاعاتی» بود و «شاید کسی تصور کند که این اعلام ناخواسته، کار مرا مختل کرد. اما دقیقاً برعکس بود؛ در

در نهایت، پوشش رسمی دارای رویه‌های اداری خاص خود است که راحتی و سهولت را فراهم می‌آورد. می‌توان به افسر پول پرداخت کرد، همچنین می‌توان برخی مسائل شخصی را از طریق کانال‌های دولتی عادی حل و فصل کرد، و می‌توان ارتباط با فرماندهی اطلاعاتی را از طریق ارتباطات امن و از طریق «ایستگاه» (گروهی از افسران اطلاعاتی با پوشش رسمی) حفظ کرد[33].

اما پوشش رسمی در عین حال معایب متعددی نیز دارد که مهم‌ترین آن‌ها تعداد نسبتاً محدود مقامات منصوب در کشور میزبان است. این امر به سازمان ضد اطلاعات کشور میزبان اجازه می‌دهد تا – با دقت کافی – افسران اطلاعاتی را که تحت پوشش دیپلماتیک فعالیت می‌کنند و آن‌هایی را که چنین نیستند، شناسایی کند. این کار – هرچند خسته‌کننده – می‌تواند از طریق نظارت بر هر مقام، پیگیری

نتیجه این داستان، گروهی از خبرچینان – البته برخی از آن‌ها افراد وسواسی بودند – به شبکه من سرازیر شدند، اما همچنین برخی افراد بسیار ارزشمند را نیز به من معرفی کردند».

[33] ؛ عملیات اطلاعاتی با اصطلاحات مختلفی نامیده می‌شود؛ برای مثال، «ایستگاه» (در ادبیات ایالات متحده) و «رزیدنتورا rezidentura» (در زبان‌های شوروی و روسیه)

تحرکات و ارتباطات او، و نصب دستگاه‌های شنود تلفنی در تلفن و آپارتمانش و غیره انجام شود. همچنین، استخدام شهروندان کشور میزبان برای کار در سفارتخانه‌ها در زمینه‌های پشتیبانی مختلف می‌تواند چنین نظارتی را تسهیل کند، به ویژه در کشورهایی که به هر کسی اجازه داده می‌شود در سفارت خارجی که با سازمان اطلاعاتی کشور میزبان[34] همکاری کرده است، کار کند. همچنین می‌توان از روش‌های ساده‌تر و کم‌هزینه‌تر برای دستیابی به همین اهداف بهره برد. به عنوان مثال، می‌توان از مطالب منتشرشده توسط یک کشور برای ردیابی ساختار شغلی کارکنان وزارت خارجه و در نتیجه شناسایی الگوهایی که به وجود ارتباط اطلاعاتی اشاره دارند، استفاده کرد.

[34] ؛مشکلات ناشی از اجازه دادن به شهروندان کشورهای میزبان برای کار در سفارتخانه‌های خارجی، قدمتی دیرینه دارد. جیمز بوکانان درباره دوران خدمتش به عنوان وزیر ایالات متحده در سن پترزبورگ روسیه، در اوایل دهه ۱۸۳۰ میلادی نوشت: «ما دائماً توسط جاسوسانی از رده‌های بالا و پایین احاطه شده‌ایم، به طوری که نمی‌توانید خدمتکاری استخدام کنید که مأمور مخفی پلیس نباشد «. Mission to Russia)، نیویورک: آرنو، ۱۹۷۵ .(برای گزارشی جدیدتر درباره مشکلات امنیتی ناشی از استفاده گسترده از شهروندان کشورهای میزبان در سفارتخانه‌ها، به کتاب رونالد کسلر با عنوان «ایستگاه مسکو: چگونه اطلاعات شوروی به سفارت آمریکا نفوذ کرد» (نیویورک: اسکریبنرز، ۱۹۸۹) مراجعه کنید

پوشش رسمی می‌تواند دسترسی آسانی را برای برخی منابع (در درجه اول دیپلمات‌ها و سایر مقامات در بوروکراسی‌های امنیت ملی کشور میزبان) فراهم کند، اما ممکن است دسترسی به دیگرانی را که در تعامل با مقامات خارجی، چه به طور کلی و چه از یک کشور خاص، تردید دارند، با مشکل مواجه کند. در هر حال، هنگامی که به افراد بالقوه جذب‌شده فوراً اطلاع داده می‌شود که با یک مقام دولتی خارجی سروکار دارند، محتاط‌تر می‌شوند. علاوه بر این، اگر روابط دیپلماتیک قطع شود – همان‌طور که در زمان بحران‌های شدید یا جنگ‌ها (زمانی که اطلاعات خوب بسیار ارزشمند است) ممکن است رخ دهد – افسران تحت پوشش رسمی مجبور به ترک کشور خواهند شد، که این امر می‌تواند عملیات شبکه‌های موجود را مختل کند.[35]

[35] ؛ برای مثال، به نظر می‌رسد اشغال سفارت آمریکا در تهران در نوامبر ۱۹۷۹ (و گروگان‌گیری کارکنان آن) به توقف کامل عملیات جمع‌آوری اطلاعات آمریکا در ایران منجر شد. هنگامی که برنامه‌ریزی برای عملیات نظامی نجات گروگان‌ها آغاز شد، هیچ «عامل آمریکایی در صحنه» وجود نداشت و به نظر می‌رسد سازمان اطلاعات مرکزی (سیا) مجبور شد یک عامل را به ایران بازگرداند تا در جمع‌آوری اطلاعات لازم برای برنامه‌ریزی عملیات نجات کمک کند. (چارلی ا. بک‌ویت و دونالد ناکس، نیروی دلتا: واحد ضدتروریسم آمریکا و مأموریت نجات گروگان‌های ایران، نیویورک: هارکورت بریس جووانوویچ، ۱۹۸۳).

معایب و مزایای پوشش غیررسمی عمدتاً بازتاب ملاحظاتی است که پیش‌تر به آن‌ها پرداختیم. از یک سو، از آنجا که آن‌ها وانمود می‌کنند که افراد دارای مشاغل متنوع و از طبقات مختلف جامعه هستند، مقامات پنهان‌شده تحت پوشش غیررسمی می‌توانند به طیف متنوع‌تر و شاید گسترده‌تری از منابع دسترسی پیدا کنند. در نتیجه، آن‌ها می‌توانند وانمود کنند که شهروندان کشوری هستند که در آن فعالیت می‌کنند یا از کشور ثالثی هستند (یا واقعاً باشند). پنهان کردن ارتباط با کشوری که برای آن کار می‌کنند، ممکن است به آن‌ها در برقراری ارتباط با منابع بالقوه و دسترسی به اطلاعات کمک کند. اگر روابط دیپلماتیک قطع شود، شاید بتوانند به کار خود ادامه دهند، و به طور کلی، کشف مقامات پنهان‌شده تحت پوشش غیررسمی برای کشور میزبان دشوارتر است.

از سوی دیگر، افسران اطلاعاتی که تحت پوشش غیررسمی کار می‌کنند، با مشکلات متعددی روبرو هستند. هزینه‌ها و دشواری‌های اداری تأمین پوشش غیررسمی بسیار بیشتر از پوشش رسمی است. یکی از روش‌ها این است که یک سازمان دولتی یا خصوصی را متقاعد کنند تا به افسر اطلاعاتی اجازه دهد وانمود کند که عضوی از تیم کاری آن‌هاست. به جای آن، افسران خودشان می‌توانند کسب‌وکاری راه‌اندازی کنند یا در فعالیت‌هایی شرکت کنند که توجیه

معقولی برای حضورشان در کشور هدف فراهم کند. عیب این کار تنها در پرهزینه بودن آن نیست، بلکه در این است که افسر اطلاعاتی باید زمان بیشتری را به فعالیت‌های مربوط به پوشش خود اختصاص دهد تا پوشش قانع‌کننده باشد، که این امر زمان و تلاشی را که افسر باید صرف مأموریت اصلی خود یعنی جمع‌آوری اطلاعات کند[36]، کاهش می‌دهد. ارتباطات اغلب دشوارتر است، زیرا افسر پنهان‌شده تحت پوشش غیررسمی نمی‌تواند بدون برانگیختن برخی سوءظن‌ها – که افسر تحت پوشش غیررسمی به شدت در تلاش برای اجتناب از آن‌هاست – از تجهیزات ارتباطی سفارت استفاده کند.

ریچارد سورگه، افسر اطلاعاتی مشهوری بود که موفقیت چشمگیری کسب کرد. او تحت پوشش غیررسمی، به عنوان یک شهروند آلمانی و خبرنگار یک روزنامه برجسته آلمانی، از سال ۱۹۳۰ تا زمان

[36] ؛ پوشش اطلاعاتی همچنین می‌تواند توسط شرکتی که خود سازمان اطلاعاتی آن را تأسیس و مالکیت کرده است، فراهم شود؛ این سازمان به عنوان «مالکیت (proprietary) «شناخته می‌شود. مالکیت می‌تواند برای اهداف عملیات پنهان و همچنین برای فراهم کردن پوشش برای افسران اطلاعاتی مفید باشد. برای مثال، یک شرکت کشتیرانی می‌تواند انتقال مخفیانه سلاح و تدارکات به شورشیان را تسهیل کند.

دستگیری‌اش در پاییز ۱۹۴۱، برای اطلاعات نظامی شوروی در چین و ژاپن جاسوسی می‌کرد. رابطه نزدیک او با اعضای سفارت آلمان در توکیو، از جمله سفیر، به او امکان دسترسی به اطلاعاتی درباره برنامه‌های جنگی آلمان و ژاپن را می‌داد. اندکی پیش از دستگیری‌اش، سورگه اطلاعات حیاتی را به مسکو ارسال کرد مبنی بر اینکه «شرق دور شوروی را می‌توان از حمله ژاپن در امان دانست». بر اساس گزارش سورگه، ژاپن تصمیم گرفته بود به اتحاد جماهیر شوروی حمله نکند و در عوض، ایالات متحده و بریتانیا را در جنوب و شرق اقیانوس آرام و مستعمرات هلند در جنوب شرق آسیا هدف قرار دهد. پس از آنکه استالین از صحت گزارش‌های سورگه اطمینان یافت، متوجه شد که می‌تواند صدها هزار سرباز را از شرق دور به مسکو منتقل کند، که این سربازان در توقف پیشروی آلمان در زمستان‌های ۱۹۴۲-۱۹۴۱ نقش داشتند. با نگاهی به گذشته، می‌بینیم که توقف ارتش آلمان در دروازه‌های مسکو، نقطه عطفی حیاتی در مسیر جنگ بود[37].

[37] ؛ در اوایل سال ۱۹۴۱، سورگه گزارش داد که آلمان قصد دارد پیمان عدم تجاوز با اتحاد جماهیر شوروی را نقض کرده و در ماه ژوئن به آن حمله کند. استالین گزارش‌های او را درباره نیت هیتلر برای نقض پیمان و تاریخ دقیق آغاز حمله آلمان نادیده گرفت. دیکتاتور شوروی ظاهراً متقاعد شده بود که این اطلاعات مشابه درباره خیانت آلمان توسط بریتانیایی‌ها ساخته شده تا بین آلمان و اتحاد

مثال دیگری از اســتفاده موفقیت‌آمیز از پوشــش غیررســمی، ارزش توانایی پنهان کردن ملیت فرد را نشـــان می‌دهد. مورد ایلی کوهن، عامل اسرائیلی، یک یهودی متولد مصر که در سال ۱۹۵۶ در سن ۳۲ ســالگی به اســرائیل مهاجرت کرد و خدمات خود را به ســازمان‌های اطلاعاتی اسرائیل پیشنهاد داد. موساد – سازمان اطلاعاتی اسرائیل – او را در ســال ۱۹۶۱ به آرژانتین فرســتاد تا پوشــشــی به عنوان یک تاجر عرب با نام مســـتعار کمال امین ثابت ایجاد کند. او به ســـرعت روابط گســـترده‌ای با جامعه مهاجران ســـوری در آرژانتین برقرار کرد، ســپس در اوایل ســال ۱۹۶۲ به دمشــق نقل مکان کرد. با اســتفاده از نامه‌های توصیه‌ای که دوستان جدید سوری‌اش در بوئنوس آیرس به

جماهیر شوروی شکاف ایجاد کرده و مسکو را به سمت اتحاد با لندن سوق دهد. به نظر می‌رسد استالین گزارش‌های سورگه درباره نیات ژاپن را تا حدی باور کرد، زیرا این گزارش‌ها از طریق رهگیری پیام‌های دیپلماتیک ژاپن توسط اتحاد جماهیر شوروی تأیید شده بودند. برای شرح زندگی و فعالیت‌های سورگه به عنوان افسر اطلاعاتی شـوروی، به کتاب گوردون دبلیو. پرانگ، با همکاری دونالد گلدشـتاین و کاترین اف. دیلون، با عنوان «هدف توکیو: داسـتان شـبکه جاسـوسـی سـورگه» (نیویورک: مک‌گراو هیل، ۱۹۸۴) مراجعه کنید.

او داده بودند، کوهن (با کمی شانس) توانست به حلقه قدرت سوریه نفوذ کند. در واقع، ارتباطات او به قدری خوب بود که مدتی به عنوان واسطه بین دولت جدید بعثی و رئیس‌جمهور سابق تبعیدی سوریه عمل کرد؛ و بعدها حتی نامزد تصدی پستی در خود دولت سوریه شد. اما پس از سه سال ارسال گزارش‌های جامع درباره امور سیاسی، نظامی و دیپلماتیک سوریه، توسط ضد اطلاعات سوریه دستگیر و در ماه مه ۱۹۶۵[38] اعدام شد.

استفاده خاص و بلندپروازانه از پوشش غیررسمی شامل افسرانی است که تحت پوشش مهاجران عادی وارد کشور میزبان می‌شوند. واضح است که وارد کردن برخی افسران به کشوری که به طور معمول تعداد زیادی مهاجر و بازدیدکننده می‌پذیرد و اهمیت زیادی به حرمت مرزهای خود نمی‌دهد، آسان‌تر از کشوری است که مهاجر نمی‌پذیرد، بازدیدکنندگان را به طور کلی تحت نظر دارد و مرزهای خود را با دقت محافظت می‌کند.

[38]؛ برای آشنایی با زندگی کوهن به عنوان عامل اسرائیلی، به کتاب ا. بلومبرگ و گوپین اوونز با عنوان «عامل بقا: اطلاعات اسرائیل از جنگ جهانی اول تا کنون» (نیویورک: پاتنام، ۱۹۸۱) مراجعه کنید.

یکی از نمونه‌های جالب که میزان زمان و تلاشـــی را که اتحاد جماهیر شـوروی به این نوع عملیات اختصـاص می‌داد، نشـان می‌دهد، مورد لیودک زیمینک اسـت، یک شـهروند چک که توسـط اطلاعات شـوروی (کمیته امنیت دولتی، معروف به کا.گ.ب، که حروف اول این جمله به زبان روســی اســت[39]) جذب شــد. با هویت رودلف هرمان (هویت واقعی رودلف هرمـان آلمـانی بود و او در طول جنـگ جهـانی دوم در اتحاد جماهیر شـــوروی درگذشـــت)، او حدود پانزده ســـال در آلمان شـرقی زندگی کرد. سـپس در اواخر سـال ۱۹۵۷، او به همراه همسـرش (که او نیز افسـر اطلاعاتی شـوروی بود) و یک نوزاد از آلمان شـرقی به آلمـان غربی رفت، جایی کـه وانمود کرد یک پنـاهنـده عـادی از آلمـان شرقی است[40].

---

[39] ؛ این روایت بر اســـاس کتاب جان بارون با عنوان «کا.گ.ب امروز: در خفا» (نیویورک: ریدرز دایجست، ۱۹۸۳) است.

[40] ؛ در میان اعضـای بلوک شـوروی، آلمان شـرقی به‌ویژه در اسـتقرار شـرکت‌های ملی نفتی (یا با استفاده از اصطلاح شوروی، «غیرقانونی‌ها») در غرب، به‌ویژه در آلمان غربی، مهارت خاصـی داشـت. یکی از اهداف اصـلی آن، تحمیل اسـتفاده از مهاجران غیرقانونی به آلمان شـــرقی بود، زیرا شـــکســـت این کشـــور در نیمه اول جنگ سـرد در کسـب به رسـمیت شـناختن دیپلماتیک گسـترده، منجر به فقدان سـفارتخانه‌ها و کنسـولگری‌ها در بسـیاری از کشـورهای غیرکمونیسـت شـده بود.

پس از چهار سال اقامت در آلمان غربی، هرمان به کانادا مهاجرت کرد، جایی که سرانجام یک کسب‌وکار کوچک تولید تبلیغات و فیلم‌های تجاری را راه‌اندازی کرد و وظایف ثانویه مختلفی را برای کا.گ.ب انجام داد، مانند ارائه «گزارش‌های شخصی» درباره سیاستمداران و روزنامه‌نگارانی که در طول کارش با آن‌ها ملاقات کرده بود، و ارتباط خود را با یک پروفسور کانادایی که عامل کا.گ.ب بود، حفظ کرد. اما مهم‌ترین وظیفه او حفظ پوشش خود بود تا در صورت قطع روابط

این امر همچنین با این واقعیت که آلمان غربی فعالانه مهاجرت از شرق را تشویق می‌کرد، آسان‌تر شد. به گفته یک افسر اطلاعاتی سابق آلمان شرقی، در اواخر دهه ۱۹۵۰، بین دو تا سه هزار عامل وجود داشتند که مشهورترین آن‌ها گونتر گیوم بود که موفق شد تا حدی به نخبگان سیاسی آلمان غربی نفوذ کند که به منشی شخصی صدراعظم ویلی برانت تبدیل شد. او این سمت را از سال ۱۹۶۹ تا زمان دستگیری‌اش در سال ۱۹۷۴ بر عهده داشت. (کریستوفر اندرو و اولگ گوردیفسکی، کا.گ.ب: داستان از درون، نیویورک: هارپر کالینز، ۱۹۹۰؛ نسخه هارپرپرنیال، ۱۹۹۱). برای شرحی از استفاده آلمان شرقی از «غیرقانونی‌ها» از منظر عملیاتی یک افسر اطلاعاتی سابق آلمان شرقی، به کتاب ورنر استیلر با همکاری جفرسون آدامز، «آن سوی دیوار: خاطرات یک جاسوس آلمان شرقی و غربی» (واشنگتن دی‌سی: براسی [ایالات متحده]، ۱۹۹۲) مراجعه کنید.

دیپلماتیک بین اتحاد جماهیر شوروی و کانادا، بتواند کنترل شبکه‌ای از منابع کانادایی را از مقیم قانونی (رئیس ایستگاه کا.گ.ب در سفارت شوروی در اتاوا) به دست گیرد.

پس از شش سال در کانادا، هرمان دستورالعمل‌هایی برای انتقال از کانادا به ایالات متحده دریافت کرد، جایی که وظایف مشابهی را انجام داد. هنگامی که پسرش پیتر هفده ساله شد، هرمان او را برای کار برای کا.گ.ب جذب کرد. از آنجا که پیتر در چهار سالگی به آلمان آورده شده بود و در کانادا و ایالات متحده بزرگ شده بود، پیشینه او هیچ سوءظنی را برنمی‌انگیخت؛ او خود را برای کار در دولت آمریکا آماده می‌کرد، جایی که می‌توانست به عنوان یک منبع بلندمدت برای شوروی‌ها، یعنی به عنوان یک «خال» (جاسوس نفوذی)، فعالیت کند. شاید او می‌توانست این نقش را ایفا کند، اگر اف‌بی‌آی پدرش هرمان را چند سال بعد کشف نمی‌کرد و او را با تهدید به دستگیری خودش و مادرش، مجبور به همکاری با آن‌ها نمی‌کرد.

پوشش‌های رسمی و غیررسمی که یک دولت خاص در اجرای فعالیت‌های جمع‌آوری اطلاعات انسانی استفاده می‌کند، به عوامل

متعددی بستگی دارد. به طور کلی، دو عامل مهم‌ترین هستند: اطلاعات اطلاعاتی مورد نیاز و ابزارهای موجود برای دستیابی به آن‌ها. در مورد ایالات متحده و متحدانش در طول جنگ سرد، جمع‌آوری اطلاعات انسانی درباره اتحاد جماهیر شوروی عمدتاً بر تلاش برای آگاهی از نیات رهبری شوروی، توانایی‌های نظامی کشور، و تلاش‌های سازمان اطلاعاتی شوروی علیه غرب متمرکز بود. این تمرکز، همراه با نظارت سازمان‌های امنیتی شوروی بر همه خارجی‌ها، منجر به این شد که تلاش‌های ایالات متحده و سایر کشورها در جمع‌آوری اطلاعات انسانی عمدتاً بر افسران اطلاعاتی فعال تحت پوشش رسمی متکی باشد.

اما چین در سال‌های اخیر به شدت به پوشش غیررسمی برای اجرای برنامه جمع‌آوری اطلاعات خود درباره ایالات متحده متکی شده است. اگرچه برنامه‌های اطلاعاتی چین برخی از فعالیت‌های سنتی جذب نیرو و جمع‌آوری داده‌ها را با استفاده از پوشش رسمی انجام می‌دهند، اما اطلاعات انسانی چین به طور معمول از مکانیزم‌های متنوعی از پوشش غیررسمی استفاده می‌کند، از جمله شرکت‌های صوری که صرفاً به عنوان پوشش عمل می‌کنند، برنامه‌های تبادل علمی و دانشجویی، و هیئت‌های تجاری و علمی. همچنین، اطلاعات چین از عوامل «خفته» استفاده می‌کند که از چین مهاجرت کرده و

خود را به عنوان عوامل مقیم برای مدت طولانی آماده می‌کنند، پیش از آنکه فعالیت‌های اطلاعاتی را در کشـــورهایی که به آن‌ها مهاجرت کرده‌اند، انجام دهند. این اســتفاده بیش از حد از پوشــش غیررســمی ناشــی از اولویتی اســت که چین به دســتیابی به فناوری پیشــرفته آمریکایی و اطلاعات مرتبط با آن می‌دهد، ماهیت نســبتاً باز بازارهای تجاری آمریکا، سهولت نفوذ جاسوسان مقیم در ایالات متحده و وجود جامعه بزرگی از آمریکایی‌های چینی‌تبار که مهاجران جدید می‌توانند در آن ادغام شوند[41].

[41] ؛ برای یک نمای کلی از فعالیت‌های اطلاعات انســانی چین، به کتاب نیکلاس افتیمیادس با عنوان «عملیات اطلاعاتی چین» (آرلینگتون، ویرجینیا: نیوکامب، ۱۹۹۸) مراجعه کنی فصــل پنجم، درباره برنامه چین برای دســتیابی به فناوری پیشــرفته آمریکا، رجوع شــود به "گزارش کمیته کاکس": گزارش کمیته منتخب در مورد امنیت ملی و نگرانی‌های نظامی/تجاری با جمهوری خلق چین (واشــنگتن دی‌ســی: دفــتــر چــاپ دولــتــی، ۱۹۹۹)، فصــل اول در آدرس www.house.gov/coxreport در دســترس اســت. همچنین رجوع شــود بـه "جاســوســی با فناوری پیشــرفته در چین"، مروری دو قســمتی بر منابع و تکنیک‌های کســب اطلاعات علمی و فناوری دفاع ملی، یک «کتابچه راهنما»ی چینی درباره جاســوســی در غرب، در مرکز ملی ضــدجاســوســی [که از این پس NACIC نامیده می‌شود]، اخبار و تحولات ضدجاسوسی (ژوئن، سپتامبر ۲۰۰۰)،

انواع منابع اطلاعاتی

به محض اینکه افسران اطلاعاتی را به دو دسته تحت پوشش رسمی یا غیررسمی طبقه‌بندی کردیم، بین انواع مختلفی از منابع اطلاعاتی تمایز قائل می‌شویم. یکی از تفاوت‌های اساسی بین منابعی است که افسر اطلاعاتی پس از فراهم آوردن شرایط برای کار در سازمان اطلاعاتی جذب می‌کند، و کسانی که کاملاً تغییر جهت داده‌اند و داوطلبانه به سازمان اطلاعاتی یک کشور خارجی کمک کرده‌اند، و در برخی موارد، عملاً با مراجعه به سفارتخانه‌های آن کشورها، مسیر خود را تغییر داده‌اند.

منابعی که جذب می‌شوند، عموماً قابل اعتماد تلقی می‌شوند، زیرا افسر اطلاعاتی فرصت یافته است تا پیش از تلاش برای جذب آن‌ها[42]،

جلدهای ۲ و ۳، قابل دسترسی در وب‌سایت: www.nacic.gov، و وب‌سایت NACIC..

[42] ؛ با این حال، نمی‌توان این احتمال را نادیده گرفت که منبع، پس از تماس با یک افسر اطلاعاتی خارجی، دولت خود را از تلاش برای جذب نیرو مطلع کرده و از آن‌ها خواسته باشد که "برای مدت طولانی بازی کنند"

شـخصـیت و انگیزه‌هایشـان را مطالعه کند. منابعی که جذب خواهند شـد، بر اسـاس امکان دسـترسـی به اطلاعات مهم انتخاب می‌شـوند. اگرچه شـناسـایی و جذب منابع کاری دشـوار و زمان‌بر اسـت، و هیچ تضمینی وجود ندارد که منبع به تلاش برای جذب یا حتی اشاره به آن، حتی اگر با دقت انتخاب شده باشد، پاسخ مثبت دهد.

اما از سـوی دیگر، فراریان ذاتاً مشـکوک هسـتند، زیرا همیشـه این احتمال وجود دارد که این فراری در واقع فرسـتاده‌ای از سـازمان اطلاعاتی کشـور خود باشـد با هدف انتقال اطلاعات نادرسـت یا گمراه‌کننده، یا اطلاع‌رسـانی به کشـورش درباره روش‌های کار سـازمان اطلاعاتی کشـور رقیب، یا به دام انداختن افسـری از سـازمان اطلاعاتی کشور رقیب به گونه‌ای که دستگیر یا از کشور اخراج شود. با این حال، سـازمان اطلاعاتی که بیش از حد به فراریان مشـکوک اسـت، ممکن اسـت فرصـت‌های دسـتیابی به اطلاعاتی را که به راحتی می‌تواند به دسـت آورد، از دسـت بدهد. سـنت‌ها و تاریخ اطلاعاتی شـامل داستان‌هایی از فراریانی است که در ابتدا نادیده گرفته یا اخراج شدند، اما بعدها مشخص شد که منابع ارزشمندی برای اطلاعات بوده‌اند.

یکی از نمونـه‌هـای مشـهور این موارد، پرونـده فریتز کولـب، یکی از مقامات وزارت خارجه آلمان در طول جنگ جهانی دوم اسـت. کار کولـب، انتقال تماس‌های تلفنی بود که هر روز از سـفارتخانه‌های

خارجی در سراسر جهان به برلین سرازیر می‌شد. این تماس‌ها به موضوعات حساس استراتژیک، نظامی، اطلاعاتی و همچنین امور دیپلماتیک می‌پرداخت. پس از آنکه به عنوان فرستاده رسمی مأمور شد، کولب در اوت ۱۹۴۳ به سوئیس سفر کرد و حدود ۲۰۰ سند را که از پرونده‌های وزارت خارجه در برلین برداشته بود، با خود برد. او ابتدا به سفارت بریتانیا در برن مراجعه کرد، اما بریتانیایی‌ها از ترس «عوامل آلمانی از نوع طعمه[43]» یا عملیات نفوذ جاسوسان آلمانی، پیشنهاد کولب را رد کردند. سپس او به آلن دالاس، که ریاست عملیات اطلاعاتی آمریکا در سوئیس را بر عهده داشت، روی آورد. آمریکایی‌ها با احتیاط، اما کمتر از متحدان بریتانیایی خود، با کولب کار کردند. او از طریق سفرهای بعدی خود به برن، بیش از ۱۵۰۰ سند محرمانه را به آن‌ها ارائه داد. شاید کولب بزرگترین موفقیت جاسوسی ایالات متحده در جنگ بود[44].

برای طبقه‌بندی منابع، می‌توانیم بین دلایل انگیزشی برای ارائه اطلاعات نیز تمایز قائل شویم. انگیزه ممکن است ایدئولوژیک،

---

[43] ؛ طعمه (Bait): نوعی جاسوس که به گونه‌ای عمل می‌کند که جاسوسی‌اش آشکار شود، سپس سرویس اطلاعاتی دشمن برای جذب او اقدام می‌کند.

[44] ؛ برای اطلاعات بیشتر، به کتاب جوزف ای. پرسیکو، "نفوذ به رایش: نفوذ عوامل مخفی آمریکایی به آلمان نازی در طول جنگ جهانی دوم" (نیویورک: وایکینگ، ۱۹۷۹)، ۷۲-۶۲، ۳۲۸ مراجعه کنید.

ملی‌گرایانه یا مربوط به وفاداری مذهبی باشـــد که می‌تواند قوی‌تر از پیوندهای آن‌ها با کشـــورهای متبوعشـــان باشـــد. ممکن اســـت از ســـیاســـت‌ها یا ایدئولوژی‌های دولت‌های خود ناامید شـــده باشـــند؛ ممکن است حریص باشند؛ ممکن است افراد عادی نباشند و امیدوار باشند هیجان بیشتری به زندگی خود ببخشند؛ ممکن است به دنبال انتقام از آنچه که رفتار بد دولت‌هایشـــان می‌دانند، باشـــند؛ یا ممکن است تحت باج‌گیری قرار گرفته باشند. اهمیت نسبی این انگیزه‌ها به ویژگی‌های جوامع و تاکتیک‌هایی که ســـازمان‌های اطلاعاتی کشـــور رقیب دنبال می‌کنند، بســـتگی دارد. به عنوان مثال، از تاریخ اتحاد جماهیر شوروی در جمع‌آوری اطلاعات انسانی درباره ایالات متحده و بریتانیا از دهه ۱۹۳۰، مشـــخص می‌شـــود که یک تغییر کیفی از ایدئولوژی به حرص و انتقام به عنوان دلایل خیانت آمریکایی‌ها و بریتانیایی‌ها به کشورهایشان رخ داده است. در دهه ۱۹۳۰، شوروی‌ها دریافتند که جذابیت کمونیسم برای بسیاری از دانشجویان و اساتید دانشـــگاه کمبریج، که برخی از آن‌ها از خانواده‌های برجســـته بودند، فضای ایدئولوژیک را بسیار مطلوب کرده بود. از جمله دانشجویانی که در آن زمان جذب شدند، کسانی بودند که بعدها به عوامل اصلی

شـــوروی در دولت بریتانیا تبدیل شـــدند، مانند گای برگس، دونالد مک‌لین و هارولد کیم فیلبی[45].

از سـوی دیگر، مشـخص شـد که آمریکایی‌ها و بریتانیایی‌هایی که در اواخر دهه ۱۹۷۰ و ۱۹۸۰ به دلیل جاســوســی برای اتحاد جماهیر شـوروی دسـتگیر شـدند، حرص و طمع بزرگترین انگیزه آن‌ها بود[46]. در مثالی دیگر، ادوارد لی هاوارد، افســر ســابق ســیا، جزئیات عملیاتی

[45] ؛ بورجس و مک‌لین هر دو در وزارت امور خارجه فعالیت می‌کردند، در حالی که فیلبی به ســرویس اطلاعات خارجی بریتانیا (MI6) پیوســت و تا ریاســت بخش ضدجاسوسی و افسر رابط در واشنگتن با سیا و اف‌بی‌آی ارتقا یافت. برای کسب اطلاعات درباره شبکه جاسوسی شوروی که ریشه‌های آن به دانشگاه کمبریج در دهه ۱۹۳۰ بازمی‌گردد، به کتاب اندرو بویل، "مرد چهارم" (نیویورک: دیال، ۱۹۷۹) مراجعه کنید. همچنین، به مقاله رابرت ســیســیل، "کمینترن کمبریج" در کتاب "بعد گمشــده: دولت‌ها، جوامع و اطلاعات در قرن بیســتم"، به ویراســتاری کریستوفر اندرو و دیوید دیلکس (اوربانا: انتشارات دانشگاه ایلینوی، ۱۹۸۴) رجوع کنید.

[46] ؛ سازمان اطلاعات نظامی، مرکز تحقیقات امنیتی، "پرونده‌های اخیر جاسوسی، ۱۹۷۵-۱۹۹۹" (سپتامبر ۱۹۹۹)، در وب‌سایت www.dss.mil/training/pub.htm موجود است و شامل مروری کلی و خلاصه‌ای از پرونده‌های اخیر است

مربوط به فعالیت‌های آژانس در مسکو را به شوروی‌ها داد، و انگیزه او انتقام از سیا بود، زیرا او را اخراج کرده بود[47].

به طور کلی، شاید در تصور عمومی درباره استفاده از رابطه جنسی برای دستیابی به اسرار و شیوع باج‌گیری به عنوان دلیلی برای جاسوسی، اغراق شده باشد. اگرچه امکان باج‌گیری شاید افسر اطلاعاتی را قادر سازد تا منبع فعالی را به دست آورد که به دلایلی جاسوس می‌شود، اما باید از این کار دست بردارد. با این حال، برخی موارد وجود داشته‌اند که شامل اغوا و باج‌گیری از نوعی است که در رمان‌های جاسوسی رایج دیده می‌شود. به عنوان مثال، زنی آمریکایی به نام بتی پاک در طول جنگ جهانی دوم، به سبک ماتا هاری عمل می‌کرد. پاک، متولد آمریکا و همسر یک دیپلمات بریتانیایی، برای هر دو سازمان اطلاعاتی بریتانیا و آمریکا کار می‌کرد. او در روش خود بر برقراری روابط با مقامات دولتی خارجی رده‌بالا تکیه داشت. از جمله دستاوردهای بزرگ او این بود که اطلاعات دیپلماتیک ارزشمندی درباره وزارت خارجه لهستان پیش از جنگ جمع‌آوری کرد، همچنین داده‌های مهمی درباره تلاش‌های رمزنگاری لهستان برای شکستن کدهای آلمانی به دست آورد، و تمام فعالیت‌های داخلی سفارت

---

[47] ؛ دیوید وایز، "جاسوسی که دور شد: داستان درونی ادوارد لی" (نیویورک: رندوم هاوس، ۱۹۸۸).

فرانســـه (ویشـــی) در واشـــنگتن را فاش کرد، و همچنین رمزهای فرانسوی و ایتالیایی را کشف کرد[48].

اما استفاده از رابطه جنسی برای به دام انداختن یک مقام که می‌تواند به مواد یا اطلاعات حساس دسترسی پیدا کند و سپس باج‌گیری از او، رایج‌تر از استفاده از اغواگری است. یکی از نمونه‌های سنتی این مورد: پرونده موریس دیژن، سفیر فرانسه در مسکو در دهه‌های ۱۹۵۰ و ۱۹۶۰ است. پس از آنکه کا.گ.ب متوجه نقطه ضعف رایج سفیر متأهل شد، یک همکار زیبا (شهروند شوروی که مجبور به همکاری شده بود) را مأمور اغوای او کرد. به محض آغاز رابطه بین آن‌ها، هر دو با بازگشت ناگهانی شوهر زن غافلگیر شدند. شوهر خشمگین تهدید کرد که سفیر را رسوا کرده و به دادگاه خواهد کشاند. دیژن راز خود را به یک دوست روسی گفت، اما او در واقع افسر ارشد کا.گ.ب بود که عملیات را از ابتدا هماهنگ کرده بود. دوســـت پیشـــنهاد کمک برای مخفی نگه داشتن کل ماجرا را داد. نقشه کا.گ.ب این بود که از این توافق برای باج‌گیری از دیژن و مجبور کردن او به کار برای آن‌ها اســـتفاده کند، زمانی که به فرانســـه بازگردد و – همان‌طور که آرزو

---

[48] ؛ به کتاب مری لوول، "دنیای ارواح: زندگی یک جاسوس آمریکایی که مسیر جنگ جهانی دوم را تغییر داد" (نیویورک: پنتاگون، ۱۹۹۲) مراجعه کنید.

داشـــتند – به مقام بالاتری ارتقا یابد. اما این توطئه شـــوروی زمانی شکست خورد که یک فیلمنامه‌نویس روسی که از این توطئه آگاه بود، ماجرا را فاش کرد[49].

مشکلات جمع‌آوری اطلاعات انسانی

بسیاری از مشکلاتی که جمع‌آوری اطلاعات انسانی با آن روبرو است، در ماهیت خود پروژه نهفته اســـت، در حالی که مشـــکلات دیگر در ماهیت هدف اطلاعاتی قرار دارند. در مورد اول، مهم‌ترین چیز اطمینان از کیفیت اطلاعات و اعتماد به واقعی بودن منابع اطلاعاتی اســـت. منابع ممکن اســـت به انگیزه پول، اطلاعات را جعل کنند یا اطلاعات منتشـــرشـــده را بازســـازی و تحریف کنند تا به نظر برســـد که از منابع رده‌بالا و دارای موقعیت‌های برجسته صادر شده‌اند (در زبان حرفه‌ای اطلاعاتی به این منابع «آســـیاب‌های کاغذی» گفته می‌شـــود). تاریخ اطلاعاتی شـــامل نمونه‌هایی از آســـیاب‌های کاغذی باهوش اســـت که عوامـل خود را فریـب داده و مبـالغ هنگفتی پول از آن‌هـا دریـافـت کرده‌اند. برخی از آســـیاب‌های کاغذی در اواخر دهه ۱۹۴۰ و اوایل دهه

[49] ؛ برای اطلاعات درباره دیگان، به کتاب جان بارون، "کا.گ.ب.: عملیات مخفی عوامل سری شوروی" (نیویورک: ریدر دایجست، ۱۹۷۴)، ۱۴۰-۱۱۴ مراجعه کنید.

۱۹۵۰ رونق گرفتند، جایی که از دشـــواری‌هایی کـه ســـازمان‌های اطلاعاتی غربی در کار در کشـورهای کمونیسـتی اروپای شـرقی با آن روبرو بودنـد، بهره‌برداری کردنـد. آن‌هـا اغلـب مهـاجران فقیر از این کشـورها را به کار می‌گرفتند، کسـانی که به سـرعت کشـف کردند که می‌توانند با فروش «اطلاعاتی» که ادعا می‌کردند از آشـنایان هموطن خود که در مناصب عالی در دولت کمونیستی جدید قرار گرفته بودند، به دســت آورده‌اند، امرار معاش کنند. از آنجا که بیشـــتر این مهاجران تحصیل‌کرده و دارای سطح بالایی از فرهنگ سیاسی بودند، توانستند اطلاعـات عمومی موجود را تزئین و تفســـیر کننـد تـا گزارش‌هـای اطلاعاتی قانع‌کننده‌ای ارائه دهند[50].

مشـکل کنترل کیفیت از امکان جذب یک عامل برای تبدیل شـدن به عامل دوگانه ناشـــی می‌شـــود، یعنی اینکه او به طور مخفیانه برای هدف فرضـی خود کار کند و اطلاعاتی را که به اپراتورهای فرضـی خود ارائه می‌دهد، به گونه‌ای انتخاب کند که آن‌ها را فریب دهد. این جذب به عنوان عامل دوگانه می‌تواند زمانی رخ دهد که یک منبع اطلاعاتی

[50] ؛ آلن دالس، "حرفه اطلاعاتی" (۱۹۸۵)، ۲۱۶.

دستگیر شود و برای اجتناب از مجازات[51]، همکاری با دستگیرکنندگان خود را انتخاب کند. به جای آن، منبع می‌تواند از ابتدا یک عامل دوگانه باشد – یک منبع فرضی اطلاعاتی که در واقع برای کشوری کار می‌کند که به نظر می‌رسد برای آن جاسوسی می‌کند – همان‌طور که پیش‌تر در مورد فراریان اشاره شد.

یکی از جذاب‌ترین و مشهورترین داستان‌ها در تاریخ اطلاعاتی در مورد استفاده از عوامل دوگانه، به عنوان مثال: عملیات موسوم به «سیستم صلیب دوگانه» است، زمانی که بریتانیایی‌ها موفق شدند کنترل کامل تلاش‌های اطلاعاتی آلمان برای جمع‌آوری اطلاعات در بریتانیا را در طول جنگ جهانی دوم به دست گیرند. تقریباً از ابتدای جنگ، بریتانیایی‌ها بر تمام گزارش‌های اطلاعاتی که عوامل آلمانی به کشورشان ارسال می‌کردند، کنترل داشتند. از جمله دستاوردهای این عملیات: این گزارش‌ها به فریب آلمانی‌ها درباره مکان و ماهیت پیاده‌سازی نرماندی کمک کرد. حتی در اواخر نهم ژوئن ۱۹۴۴ – یعنی سه روز پیش از پیاده‌سازی – پیامی از یک منبع تحت کنترل

[51] ؛ اگر جاسوس اسیر از همکاری امتناع کند، ممکن است سرویس اطلاعاتی که او را دستگیر کرده است، با ارسال پیام‌هایی به نام او، هویتش را جعل کند. این روش می‌تواند در موقعیت‌هایی مانند جاسوسی در زمان جنگ در خاک دشمن، که انتظار نمی‌رود منبع با رابطان خود دیدارهای حضوری داشته باشد، موفقیت‌آمیز باشد.

بریتانیایی‌ها توصـــیه کرد که لشـــکر زرهی آلمان در منطقه کاله نگه داشته شود (تا از پیاده‌سازی قریب‌الوقوع یک نیروی اصلی که وجود نداشـــت، جلوگیری کند)، و بدین ترتیب به نیروی پیاده‌ســـازی واقعی کمک کرد تا جای پایی برای خود پیدا کند[52].

مشـکلات دیگری نیز از ماهیت هدف ناشـی می‌شـود. هرچه کارایی و گســـتردگی دســـتگاه امنیت داخلی در یک کشـــور بیشـــتر باشـــد، دشـواری‌هایی که برای جمع‌آوری اطلاعات انسـانی در آن کشـور ایجاد می‌کند، بیشـــتر خواهد بود. دولتی که نظارت شـــدیدی بر ســـفر و ارتباطات بین‌المللی، و بر تحرکات، ارتباطات و فعالیت‌های اقتصـادی شـــهروندان خود به طور کلی اعمال می‌کند، می‌تواند کار را برای افسـران اطلاعاتی پنهان‌شـده تحت پوشـش غیررسـمی یا غیرقانونی برای سـفر به آن کشـور، ایجاد فعالیت‌های مربوط به پوشـش خود، و کار بدون کشف شدن، دشوار کند. افسرانی که تحت پوشش رسمی کار می‌کنند، می‌توانند تحت نظارت شـــدید قرار گیرند، که این امر ملاقات با شهروندان کشور هدف را بدون دیده شدن برای آن‌ها دشوار

---

[52] ؛ اگر جاسوس اسیر از همکاری امتناع کند، ممکن است سرویس اطلاعاتی که او را دستگیر کرده است، با ارسال پیام‌هایی به نام او، هویتش را جعل کند. این روش می‌تواند در موقعیت‌هایی مانند جاسوسی در زمان جنگ در خاک دشمن، که انتظار نمی‌رود منبع با رابطان خود دیدارهای حضـــوری داشـــته باشـــد، موفقیت‌آمیز باشد.

می‌کند. نتیجه این اســـت که در زبان حرفه‌ای اطلاعاتی به آن «هدف ســـخت» یا «منطقه ممنوعه» گفته می‌شـــود، کشـــوری که در آن فعالیت‌های اطلاعاتی تنها با پوشـــش رســـمی و در نتیجه با دشـــواری فراوان امکان‌پذیر است.

اهداف دیگر نیز مشـــکلات خاص خود را دارند. به عنوان مثال: فرآیند جمع‌آوری اطلاعات درباره تروریسم با ماهیت گروه‌های تروریستی که اغلب نســـبتاً کوچک، مخفی و بســـیار منســـجم هســـتند – مانند ملاحظاتی که در مورد جمع‌آوری اطلاعات انســـانی درباره گروه‌های جرم ســـازمان‌یافته صـــدق می‌کند – برخورد می‌کند، به گونه‌ای که عضویت فرد در این گروه‌ها به شناخت طولانی‌مدت، روابط خانوادگی، یا سـوابق جنایی قبلی بسـتگی دارد. وارد کردن یک منبع اطلاعاتی به آن‌ها (طبق اصطلاح حرفه‌ای اطلاعاتی، «نفوذ به آن‌ها») بسیار دشوار می‌شـــود. به همین ترتیب، وفاداری‌ها در چنین گروهی (گذشـــته از انضـــباطی که می‌توان بر افراد اعمال کرد) متقاعد کردن یک عضـــو موجود در گروه را برای خیانت به گروهش دشوار می‌سازد.

دشـــواری‌هـا حتی اگر بتوان منبعی را بـا موفقیـت وارد یـک گروه تروریســـتی کرد، پایان نمی‌یابد. برای اینکه یک عامل در وضـــعیت خوبی باقی بماند، باید کمک‌هایی ارائه دهد که از اقدامات تروریسـتی حمایت – یا به آن‌ها کمک – کند، در حالی که بیشـــتر ســـازمان‌های

اطلاعاتی احســـاس می‌کنند مجبورند محدودیت‌هایی برای اقداماتی که افسر یا منبع می‌تواند انجام دهد تا قابل اعتماد باقی بماند، تعیین کنند. در عین حال، اســـتفاده از اطلاعاتی که منبع ارائه می‌دهد برای هشـــدار درباره طرح‌های اقدامات تروریســـتی یا جلوگیری از آن‌ها، می‌تواند وجود یک خبرچین در میان تروریســـت‌ها را فاش کند، و در نتیجه زندگی منبع را به خطر بیندازد. ســـازمان اطلاعاتی فرصـــت نخواهد یافت تا از فعالیت‌های داخلی گروه مطلع شود، مگر اینکه این عضو دستگیر شود.

حرفه

روش‌های خاصی که افسر اطلاعاتی برای به کارگیری منابع و برقراری ارتباط با آن‌ها بدون اینکه توسـط سـازمان اطلاعاتی دشـمن کشـف شود، استفاده می‌کند، به نام «حرفه» شناخته می‌شود. خطرناک‌ترین مشـکلی که یک افسـر اطلاعاتی می‌تواند با آن روبرو شـود این اسـت که طرف مقابل به احتمال زیاد او را تحت نظر خواهد داشـت – یعنی او را زیر نظر گرفته و ردیابی خواهد کرد؛ تا تحرکاتش را رصـــد کرده و کسـانی را که با آن‌ها در تماس اسـت، شـناسـایی کند. در این صـورت، وظیفه افسر این است که تشخیص دهد آیا تحت نظارت است یا خیر. اگر تحت نظارت باشـــد، باید برای مدت کافی از نظارت فرار کند تا

بتواند با منابع یا افرادی که قصد جذب آن‌ها را دارد، بدون اینکه هویتشان فاش شود، ارتباط برقرار کند[53].

یکی از تکنیک‌های فرار از نظارت که سیا به افسران خود آموزش داده بود، با ترفندی که ادوارد لی هاوارد، افسر سیا که به عنوان صندوقدار کار می‌کرد، برای فرار از نظارت اف‌بی‌آی در سال ۱۹۸۵ به کار برد، روشن می‌شود. او شب‌ها در ماشین خود بازمی‌گشت و همسرش رانندگی می‌کرد. چون معتقد بود اف‌بی‌آی او را تعقیب می‌کند، هاوارد از همسرش خواست در یک چهارراه تاریک به سرعت بپیچد. بلافاصله پس از پیچیدن، او در ماشین را از سمت خود باز کرد و به بیرون غلتید. در همان زمان، همسر هاوارد یک عروسک به جای او گذاشت، به طوری که برای هر کسی که از دور نظارت می‌کرد، به نظر می‌رسید هاوارد هنوز در ماشین است. سپس او ماشین را به خانه راند، وارد گاراژ شد و در آن را بست، که این امر تیم نظارتی را از فرار هاوارد

[53] ؛ یک جزوه آموزشی قدیمی اما همچنان مفید شوروی، درس‌هایی درباره نحوه برقراری ارتباط و کنترل منابع اطلاعاتی در ایالات متحده ارائه می‌داد. از جمله مطالبی که توسط اولگ پنکوفسکی، افسر شوروی که در اواخر دهه ۱۹۵۰ و اوایل دهه ۱۹۶۰ برای ایالات متحده و بریتانیا جاسوسی می‌کرد، ارائه شد، "سخنرانی ریخودیکو" در کتاب فرانک جینی، "پنکوفسکی" (نیویورک: دابل‌دی، ۱۹۶۵)، ۱۶۲-۱۰۲ است.

بی‌خبر گذاشت و او اکنون می‌توانست هر طور که می‌خواست، بدون اینکه کسی او را تعقیب کند، حرکت کند[54].

معمول است که یک افسر اطلاعاتی برای رسیدن به یک جلسه، ساعت‌ها در مسیرهای پرپیچ‌وخم سفر کند و از وسایل نقلیه مختلفی استفاده نماید. اگر او متوجه شود که فردی که در قطار متروی غرب‌رو کنارش نشسته بود، دوباره در قطار شرق‌رو نیز همراه اوست، منطقاً نتیجه می‌گیرد که تحت تعقیب قرار دارد[55]. تیم‌های مراقبت می‌توانند با استفاده از سیستم چرخشی، از لو رفتن خود جلوگیری کنند؛ به این ترتیب که یک فرد مشخص، افسر مورد نظر را به طور مداوم تعقیب

[54] ؛ وایز، "جاسوسی که دور شد". برای تکمیل این ترفند، همسر هاوارد پس از بازگشت به خانه با مطب پزشک هاوارد تماس گرفت. در آن ساعت، پزشک طبق انتظار در مطب نبود و دستگاه پاسخگویی او فعال بود. همسر هاوارد، با فرض اینکه تلفن شنود می‌شود، پیامی ضبط‌شده را که هاوارد قبلاً برای پزشک خود ضبط کرده بود، پخش کرد. این اقدام به اف‌بی‌آی کمک کرد تا بازگشت هاوارد به خانه با همسرش را تأیید کند. همانطور که بعداً مشخص شد، تلاش‌های نظارتی دقیق نبود.

[55] ؛ در این صورت، او نتیجه خواهد گرفت که این فرد نیز همان مسیر پرپیچ‌وخم او را دنبال می‌کند.

نکند. این بازی تعقیب و گریز و ضـدتعقیب می‌تواند بسـیار پیچیده و اغلب طولانی‌مدت شود[56].

همچنین، روش‌هایی برای برقراری ارتباط با منبع وجود دارد که هرگز نیازی به ملاقات حضـوری نیسـت. به عنوان مثال، یک افسـر می‌تواند

[56] ؛ مثالی از این تعامل بین نظارت و ضـد نظارت توسـط پیتر رایت، مقام سـابق MI5 (ضدجاسـوسـی بریتانیا)، در کتابش "جاسـوس‌گیر" توصیف شـده اسـت. به گفته رایت، تکنسـین‌های شـوروی که در سـفارت خود در لندن کار می‌کردند، قادر بودند ارتباطات تیم‌های نظارتی متحرک ("ناظران") مورد اسـتفاده MI5 را رصـد کننـد. بـا تجزیـه و تحلیـل این ارتبـاطـات و مرتبط کردن آن‌هـا بـا عملیـات خود، شـوروی‌ها می‌توانسـتند نتیجه بگیرند که آیا یک جلسـه خاص بین یک افسـر اطلاعاتی شـوروی و منبعش احتمالاً تحت نظارت اسـت یا خیر. در این صـورت، به افسـر هشـدار داده می‌شـد تا جلسـه را لغو کند. به گفته رایت، سـازمان ضدجاسـوسـی بریتانیا توانسـت این ضـعف را در سیسـتم نظارتی خود شـناسـایی کند، زمانی که از داخل سـفارت روسـیه، انتشـار امواج الکترونیکی را کشـف کرد که به طور منحصـر به فردی با عملیات رهگیری رادیویی ارتباطات شـوروی مرتبط بود. به طور خلاصه، همانطور که رایت می‌گوید، MI5 شـوروی‌ها را زیر نظر داشـت که ناظران را تماشـا می‌کردند، و ناظران نیز به نوبه خود مشـغول تماشـای شـوروی‌ها بودند. رایت، "جاسـوس‌گیر: زندگی‌نامه صـریح یک افسـر ارشـد اطلاعاتی" (نیویورک: وایکینگ، ۱۹۸۷)، ۵۷-۵۲، ۹۱-۹۳.

هنگام عبور از خیابان، یک برگه یا بســته‌ای از اوراق را به منبع تحویل دهد که به آن «عبور قلم‌مو» (brush pass) گفته می‌شود. اگر این کار به درســتی انجام شــود، تیم مراقبت طرف مقابل متوجه آن نخواهد شــد. روش دیگر این اســت که افســر کیف خود را کنار صــندلی روی زمین بگذارد تا در کافه نوشــیدنی بنوشــد. منبع نیز میز کناری را انتخاب کرده و کیف خود را – که از نظر ظاهری کاملاً شبیه کیف افسر اســت – کنار خود روی زمین می‌گذارد. هنگام خروج، منبع به جای کیف خود، کیف افســر را برمی‌دارد. در این حالت نیز، تیم مراقبت متوجه این جابجایی نخواهد شــد، مگر اینکه با دقت بســیار نحوه قرار دادن و برداشتن کیف‌ها را زیر نظر داشته باشند.

این روش‌ها ضــروری هســتند؛ زیرا به دلیلی نامعلوم، مأمور اف‌بی‌آی مســئول مراقبت از خانه، در وهله اول خروج هواردز را از دســت داده بود و خودروی هواردز در واقع هرگز ردیابی نشد.

به همین ترتیب، افســر می‌تواند پیامی را در محلی که از پیش تعیین شــده اســت، مانند شــکافی در تنه درختی در یک پارک، قرار دهد. این پیام ســاعت‌ها بعد توســط منبع از «صــندوق مرده» (dead drop)

برداشته می‌شود[57]. اگر افسر پیام را بدون اینکه مراقبش متوجه شود، قرار دهد، آن‌ها به تعقیب او ادامه خواهند داد، بدون اینکه بدانند ملاقات عملاً انجام شده است. رابرت هانسن، متخصص ضدجاسوسی اف‌بی‌آی که بیش از پانزده سال برای اتحاد جماهیر شوروی و سپس فدراسیون روسیه جاسوسی می‌کرد، تمام ارتباطات خود را همواره از طریق «صندوق مرده» انجام می‌داد؛ این امر به وضوح به دلیل آشنایی او با مقررات کاری اف‌بی‌آی بود، زیرا او این روش را سریع‌ترین راه می‌دانست[58].

---

[57] ؛ برای توضیح فرآیند آماده‌سازی "صندوق مرده"، به توصیف جان بارون از شبکه جاسوسی شوروی به رهبری جان واکر در کتاب "کشف شبکه" (بوستون: هاتون میفلین، ۱۹۸۷)، ۹۶-۸۰ مراجعه کنید.

[58] ؛ شهادت اف‌بی‌آی در حمایت از حکم‌های بازداشت و تفتیش در پرونده هانسن، حاوی نقل‌قول‌های مفصلی از پیام‌های مبادله شده بین هانسن و کا.گ.ب. (و بعدها سرویس اطلاعات خارجی روسیه یا SVR) است. در این پیام‌ها، هانسن به دلایل امنیتی دیدارهای مستقیم (حتی در کشورهای خارجی) را رد کرده و تقریباً به طور کامل بر استفاده از صندوق‌های مرده اصرار داشت. (تماس اولیه از طریق پست به منزل یک افسر اطلاعاتی شوروی بود؛ و در موارد معدودی تماس‌های تلفنی نیز برقرار شد.) شهادت مکتوب، موجود در www.fas.org/irp/ops/ci hanssen_affidavit.html/، گواه ملموسی بر استفاده از صندوق‌های مرده است.

نکته دیگری که سازمان‌های اطلاعاتی باید تا حد امکان از آن اجتناب کنند، ملاقات با منبع در کشوری است که علیه آن جاسوسی می‌کنند. در عوض، ملاقات در یک کشور ثالث امن انجام می‌شود، جایی که مراقبت ممکن است کمتر شدید یا اصلاً وجود نداشته باشد. به عنوان مثال، اتحاد جماهیر شوروی همواره ترجیح می‌داد با منابع بسیار مهم خود در ایالات متحده، مانند جان واکر (که مقادیر عظیمی از اطلاعات محرمانه مربوط به ارتباطات و عملیات دریایی را به شوروی‌ها می‌رساند)، در استرالیا ملاقات کند. استرالیا کشوری بود که با وجود نظام دموکراتیک غربی‌اش، رسماً بی‌طرف محسوب می‌شد.

پرونده واکر نشان داد که شوروی‌ها چگونه یک عامل مهم را با دقت اداره می‌کردند. بیشتر ملاقات‌های او با شوروی‌ها در وین و استرالیا انجام می‌شد. در طول این جلسات، واکر و مأمور کاگ‌ب که قصد ارتباط با او را داشت، در خیابان‌ها قدم می‌زدند و از هیچ خانه امنی برای ملاقات استفاده نمی‌کردند. از آنجا که مأمور کاگ‌ب مستقیماً از مسکو می‌آمد، مأموران مقیم در وین (یعنی گروه افسران کاگ‌ب که از سفارت شوروی فعالیت می‌کردند) از این عملیات بی‌خبر بودند[59].

[59] ؛ هربرت رومرستاین و استانیسلاو لفچنکو، "کا.گ.ب. علیه دشمن اصلی: چگونه اطلاعات شوروی علیه ایالات متحده عمل می‌کند" (لکسینگتون، ماساچوست: لکسینگتون، ۱۹۸۹)، ۲۹۳. کا.گ.ب. با پنهان کردن افسران اطلاعاتی

در موارد دیگر، سازمان‌های اطلاعاتی که علیه ایالات متحده فعالیت می‌کردند، ترجیح می‌دادند با منابع خود در کانادا یا مکزیک ملاقات کنند. این انتخاب‌ها با توجه به سهولت سفر آمریکایی‌ها به این کشورها و تعداد زیاد بازدیدکنندگان، منطقی به نظر می‌رسد. به عنوان مثال، وائو تای شین، زبان‌شناس و تحلیلگر سیا که برای مدت طولانی به نفع جمهوری خلق چین جاسوسی می‌کرد، سفرهای مکرری به تورنتو [60] داشت تا از مسئول عملیاتی خود دستورالعمل دریافت کرده و فیلمی را به او تحویل دهد[61].

از دیگر روش‌هایی که افسران اطلاعاتی و منابع می‌توانند بدون ملاقات حضوری با یکدیگر ارتباط برقرار کنند، «نوشتار مخفی» (secret writing) و «میکروفیلم‌ها» (microdots) هستند. این تکنیک‌ها در مواردی مفیدند که افسر و منبع ظاهراً دلیلی بی‌خطر برای ارتباط دارند، اما گمان می‌کنند که پیام‌هایشان احتمالاً توسط طرف مقابل باز و خوانده خواهد شد. برای استفاده از نوشتار مخفی، افسر یا منبع ابتدا یک متن پوششی بی‌خطر برای پیام می‌نویسد،

شوروی مستقر در وین، خطر اینکه نظارت ایالات متحده بر افسران اطلاعاتی شوروی در آنجا عملیات واکر را به خطر بیندازد، کاهش داد.

[60] در کانادا.

[61] ؛ نیکلاس افتیمیادیس، "عملیات اطلاعاتی چین" (آرلینگتون، ویرجینیا: نیوکامب، ۱۹۹۸)، ۳۳، ۳۷-۳۶.

سپس – معمولاً با استفاده از نوع خاصی از کاغذ کاربن – پیام محرمانه را روی سطح پیام اصلی می‌نویسد. این پیام با چشم غیرمسلح قابل مشاهده نیست و تنها زمانی قابل خواندن می‌شود که با یک ماده شیمیایی خاص که فقط سازمان اطلاعاتی مربوطه می‌داند، پردازش شود. میکروفیلم‌ها نیز روش دیگری برای ارتباط هستند. در این حالت، تصاویر به اندازه میکروسکوپی کوچک شده و در جایی از پیام پنهان می‌شوند؛ شاید زیر تمبر یا مهر پاکت، یا بالای علائم نگارشی در حروف نوشته شده.

منشقین

تاکنون به منابع اطلاعاتی «درون‌جایگاه» (in-place sources) پرداختیم؛ یعنی افرادی که اطلاعات را منتقل می‌کنند و در عین حال موقعیت رسمی خود را حفظ کرده‌اند که به آن‌ها امکان دسترسی به اطلاعات را می‌دهد. بدیهی است که این بهترین وضعیت از منظر گردآوری اطلاعات است، زیرا شامل دسترسی مستمر به اطلاعات و همچنین امکان مأمور کردن منبع برای دستیابی به اسناد یا اطلاعات خاص و ضروری است. اما این روش مستلزم آن است که ارتباط بین منبع و مسئول عملیاتی او پنهان بماند و منبع در معرض خطر دستگیری قرار گیرد.

این دشواری‌ها در کشورهایی که تحت نظارت شدید هستند، افزایش می‌یابد. از این رو، گردآوری اطلاعات در چنین کشورهایی تا حد زیادی به «منشقین» (defectors) متکی است. از منظر اطلاعاتی، این افراد منابعی هستند که در جایگاه خود باقی نمی‌مانند، بلکه معمولاً به طور غیرقانونی از کشورهایشان فرار کرده و حق پناهندگی دریافت می‌کنند. در حقبه پس از جنگ جهانی دوم، غرب در گردآوری اطلاعات درباره اتحاد جماهیر شوروی تا حد زیادی به چنین افرادی متکی بود. به عنوان مثال: در دهه 1950، سازمان‌های اطلاعاتی غربی تنها توانایی محدودی برای جذب افسران اطلاعاتی شوروی داشتند، اما در سال 1954، پنج افسر در عرض چهار ماه به غرب پناهنده شدند. این انشقاق‌ها به غنی‌سازی اطلاعات درباره عملیات‌های اطلاعاتی شوروی در دهه پس از جنگ جهانی دوم منجر شد. از طریق این انشقاق‌ها، اطلاعات مهم و جدیدی درباره فعالیت‌های مخفی و عملیات‌های کاگ‌ب، تلاش‌های آن برای رمزگشایی از کدهای دولت‌های دیگر، نفوذهایش در دولت‌های غربی و توسل به ترورها به دست آمد[62].

[62] ؛در اواخر سال ۱۹۵۳، سرویس اطلاعاتی شوروی با نام MGB (وزارت امنیت دولتی) بخشی از وزارت کشور (MVD) بود. ادغام این دو بوروکراسی مهم، نتیجه تلاش لاورنتی بریا، رئیس سابق اطلاعات و ماجراجوی اصلی کرملین، برای قبضه قدرت پس از مرگ استالین در مارس ۱۹۵۳ بود. پس از دستگیری و اعدام بریا در

به همین ترتیب، انشقاق حسین کامل، داماد صدام حسین، دیکتاتور عراق، در سال 1995 اطلاعات ارزشمندی درباره برنامه مخفی عراق برای توسعه تسلیحات بیولوژیک ارائه داد که تیم بازرسان سازمان ملل (UNSCOM) در چهار سال پیش از انشقاق او نتوانسته بودند آن را کشف کنند[63].

دسامبر ۱۹۵۳، سرویس اطلاعاتی شوروی دوباره از وزارت کشور جدا شد و نام KGB (کمیته امنیت دولتی) را به خود گرفت. در طول این آشفتگی‌ها در سرویس اطلاعاتی، این انشقاق‌ها رخ داد. پنج نفر از جداشدگان (و کشورهایی که در آن‌ها جدا شدند) عبارتند از: یوری راستووروف (ژاپن)؛ پیوتر دریابین (اتریش)؛ ولادیمیر و اودوکیا پتروف (استرالیا)؛ و نیکولای خوخلوف (آلمان غربی). به گوردون بروک-شیرد، "پرندگان طوفان: جداشدگان شوروی پس از جنگ" (لندن: وایدنفلد و نیکلسون، ۱۹۸۸)، ۱۳۱-۵۷ مراجعه کنید

[63] ؛ بر اساس گزارش مؤسسه بین‌المللی تحقیقات صلح استکهلم، "برگه اطلاعات: عراق: تجربه آنسکام" (اکتبر ۱۹۹۸)، موجود در: editors.sipri.se/pubs/Factsheet/UNSCOM.pdf، بزرگترین عملیات تحقیق و توسعه و سایت تولید تسلیحات بیولوژیکی عراق تا زمان جدایی حسین کامل ناشناخته بود، اگرچه بازرسان آنسکام قبلاً از این سایت‌ها بازدید کرده بودند. به همین ترتیب، جدایی یک دانشمند برجسته درگیر در برنامه تسلیحات هسته‌ای عراق در سال ۱۹۹۴، اولین اطلاعات دقیق را درباره تاریخچه و عملکرد داخلی آن ارائه داد. جودیت میلر و جیمز رایزن، "جداشده بمب اتمی عراق را توصیف می‌کند"، نیویورک تایمز، ۱۵ اوت ۱۹۹۸.

با وجود اهمیتشـــان، منشـــقینی که به شـــما مراجعه می‌کنند، همان مشـــکلی را ایجاد می‌کنند کـه منشـــقین «درون‌جـایگـاه»[64] ایجـاد می‌کنند. شـــما نمی‌توانید با قاطعیت بگویید که آیا آن‌ها منشـــقین واقعی هسـتند یا شـهروندان وفاداری که توسـط دولت‌هایشـان برای فریب سـازمان‌های اطلاعاتی دشـمن فرسـتاده شـده‌اند. بدون شـک، این وضعیت حداقل در ابتدا نیازمند احتیاط در برخورد با آن‌هاست. به عنوان مثال، اطلاعات متناقضی که چندین منشق بلندپایه شوروی به ایالات متحده ارائه دادند – به ویژه در مورد وجود یا عدم وجود یک «خال» [65] بلندپایه در دولت آمریکا – هرگز به پاسـخی قاطع نرسـید و جامعه اطلاعاتی آمریکا را برای بیش از ربع قرن سردرگم کرد[66].

---

[64] ؛ جداشدگانی که تنها وفاداری خود را تغییر می‌دهند، بدون اعلام جدایی یا سفر به کشور دیگر.

[65] ؛ اطلاعات آمریکا برای جاسوسی که مدت‌ها قبل از تصدی یک پست یا توانایی کسب اطلاعات استخدام می‌شود، از اصطلاح "مول" (mole) استفاده می‌کند.

[66] ؛ این داســتان در کتاب دیوید مارتین، "ســرزمین آینه‌ها" (نیویورک: هارپر و رو، ۱۹۸۰) روایت شــده اســت. روایت‌های اخیر درباره این بحث در جامعه اطلاعاتی آمریکا شـامل کتاب‌های تونی منگولد، "جنگجوی سـرد: جیمز خسـوس انگلتون، شـکارچی جاسـوس ارشـد سـیا" (نیویورک: سـایمون و شـوسـتر، ۱۹۹۱)، و ادوارد جی. اپســتاین، "فریب: جنگ پنهان بین ســیا و کا.گ.ب." (نیویورک: ســایمون و شـوسـتر، ۱۹۸۹) اسـت. نویسـندگان منگولد و اپسـتاین به دیدگاه‌های متضـادی

گردآوری اطلاعات فنی

گردآوری اطلاعات فنی به مجموعه‌ای از تکنیک‌ها اشاره دارد که برای جمع‌آوری اطلاعات، بیشتر از فناوری‌های پیشرفته و کمتر از عوامل انسانی استفاده می‌کنند. در نهایت، این تکنیک‌ها تنها به نبوغ انسان و قوانین فیزیک متکی هستند. این روش‌ها عمدتاً شامل تصویربرداری از راه دور و رهگیری امواج الکترومغناطیسی مختلف می‌شوند، هرچند پدیده‌های دیگری (مانند سیگنال‌های صوتی) نیز مورد بهره‌برداری قرار می‌گیرند.

اطلاعات تصویری

همانطور که از نامش پیداست، «اطلاعات تصویری» (Imagery Intelligence) شامل استفاده از تصویربرداری برای گردآوری اطلاعات است. به طور خاص، از تصویربرداری از راه دور برای به دست آوردن تصاویر از مکان‌ها یا اشیایی استفاده می‌شود که دسترسی مستقیم

رسیده‌اند که دشواری رسیدن به یک قضاوت قطعی درباره حسن نیت برخی از جداشدگان را منعکس می‌کند.

به آن‌ها دشـوار اسـت. نظارت هوایی تقریباً همزمان با آغاز خود پرواز آغاز شد[67].

در آغـاز جنـگ جهـانی اول، در اوت 1914، نیروی هوایی سـلطنتی بریتانیا نظارت هوایی بر نیروهای آلمانی در حال پیشـروی از طریق بلژیک را انجام داد[68]. به محض پایان یافتن دوره اولیه تحرکات و رویارویی ارتش‌های آلمان با نیروهای متفقین در جبهه‌ای که از سـوئیس تا دریای شـمال امتداد داشـت، نظارت هوایی به عنوان جایگزینی برای گشت‌های شناسایی سواره‌نظام در نظر گرفته شد؛ گشت‌هایی که قادر به دسترسی به مناطق جناحین و پشت خطوط دشـمن نبودند. همانطور که ژنرال ویلیام میچل، پیشـگام اصـلاحات نیروی هوایی آمریکا در دوره بین دو جنگ، نوشـت: «یک پرواز بر فراز خطوط، تصویری بسیار واضح‌تر از موقعیت ارتش‌ها به من داد تا هر

---

[67] حتی پیش از آن، بالن‌ها به عنوان سکوهای نظارت هوایی مورد استفاده قرار گرفته بودند – توسط جمهوری اول فرانسه در سال ۱۷۹۴ و توسط ارتش اتحادیه در جنگ داخلی آمریکا. در هر دو مورد، موفقیت چشمگیری حاصل نشد و هر دو ارتش بعدها "نیروی هوایی" نوپای خود را منحل کردند. برای اطلاعات بیشتر، به ویلیام ای. بروز، "سیاه عمیق: جاسوسی فضایی و امنیت ملی" (نیویورک: رندوم هاوس، ۱۹۸۷؛ نیویورک: برکلی، ۱۹۸۸)، ۲۸-۲۶ مراجعه کنید.

[68] ؛ اندرو، "سرویس اطلاعات سلطنتی"، ۱۳۳

سفر زمینی»[69]. از همین جا بود که گام نسبتاً کوچکی برای نصب دوربین‌ها بر روی هواپیماهای شناسایی و توسعه قابلیت‌های تصویربرداری شناسایی هوایی برداشته شد.

پس از توسعه هوانوردی و عکاسی، شناسایی تصویری به منبع مهمی از اطلاعات در طول جنگ جهانی دوم تبدیل شد. هدف از آن تنها ردیابی استقرار و تحرکات نیروهای دشمن نبود، بلکه پیگیری پیشرفت‌های فنی نیز مد نظر بود؛ مانند تصویربرداری هوایی بریتانیا، علاوه بر سایر منابع اطلاعاتی مانند سیستم‌های پرتو رادیویی که آلمانی‌ها برای هدایت بمب‌افکن‌ها به منظور هدف قرار دادن انگلستان توسعه داده بودند، و همچنین سیستم‌های رادار دفاعی و موشک‌های V-1 و V-2[70].

تمام مثال‌هایی که تاکنون درباره شناسایی هوایی تصویری ذکر کردیم، مربوط به زمان جنگ است و این تصادفی نیست. در زمان جنگ، انگیزه نظامی برای انجام این نوع فعالیت بیشتر و موانع

[6969] ویلیام میچل، "خاطرات جنگ جهانی اول: از آغاز جنگ ما تا پایان آن" (نیویورک: رندوم هاوس، ۱۹۶۰).

[70] ؛ کتاب آر. وی. جونز، "بزرگترین اسرار جنگ"، یکی از بهترین بحث‌ها را درباره اطلاعات علمی بریتانیا در جنگ جهانی دوم، از زبان یکی از برجسته‌ترین فعالان آن، ارائه می‌دهد.

سیاسی پیش روی آن کمتر است. نه تنها اهمیت دانستن آنچه در کشور دشمن می‌گذرد در زمان جنگ افزایش می‌یابد، بلکه راه‌های جایگزین برای کسب اطلاعات نیز کاهش می‌یابد. نمی‌توان تنها به گزارش‌های مطبوعاتی یا گزارش‌های مسافران، دیپلمات‌ها و وابستگان سفارتخانه‌ها اکتفا کرد. به طور کلی، پوشش خبری تحت نظارت دقیق قرار می‌گیرد، مرزها بسته می‌شوند و سفر به کشور هدف حتی برای شهروندان همان کشور و کشورهای بی‌طرف محدود می‌شود. در عین حال، قانون بین‌المللی که پرواز در حریم هوایی یک کشور را ممنوع می‌کند، دیگر مانع سیاسی محسوب نمی‌شود.

با این همه، دشواری‌هایی که ایالات متحده در تلاش برای انجام فعالیت‌های گردآوری اطلاعات انسانی علیه اتحاد جماهیر شوروی در سال‌های اولیه پس از جنگ جهانی دوم با آن مواجه شد، این کشور را وادار کرد تا به استفاده از شناسایی تصویری در زمان صلح نیز بیندیشد. این علاقه زمانی تقویت شد که در سال 1950 این ترس غالب شد که حمله کره شمالی به کره جنوبی ممکن است مقدمه‌ای برای حمله شوروی به اروپای غربی باشد. به ویژه با توجه به کمبود منابع اطلاعاتی انسانی، ایالات متحده نگران بود که آمادگی‌های شوروی برای چنین حمله‌ای ممکن است کشف نشود. همچنین، اطلاعات اساسی درباره «نظم نبرد» (Order of Battle) شوروی

(یعنی حجم و ترکیب نیروهای مسلح) همواره ناقص بود و از این رو، برای دولت آمریکا دشوار بود که قضاوت‌های معقولی درباره میزان هزینه‌های نظامی خود داشته باشد.

یکی از نمونه‌های کمبود داده‌ها درباره نیروهای شوروی، «شکاف بمب‌افکن‌ها»ی فرضی در اواسط دهه 1950 بود. اطلاعات آمریکا درباره برنامه‌ها و توانایی‌های شوروی در ساخت بمب‌افکن‌های استراتژیک یا «سنگین» (هواپیمایی قادر به حمل بمب هسته‌ای در فواصل بین‌قاره‌ای) بسیار ناچیز بود. اما در جشن‌های روز نیروی هوایی شوروی در ژوئیه 1955، درست پیش از نشست چهار قدرت بزرگ (ایالات متحده، اتحاد جماهیر شوروی، فرانسه و بریتانیا) در ژنو، یک وابسته نظامی هوایی، بیست و هشت بمب‌افکن سنگین از انواع نسبتاً جدید را در حال پرواز مشاهده کرد. به نظر می‌رسید که شوروی‌ها برنامه سریعی برای ساخت بمب‌افکن‌های استراتژیک در پیش گرفته‌اند که با وجود برنامه‌های دفاعی آمریکا، شکافی به نام «شکاف بمب‌افکن‌ها» بین توانایی‌های آمریکا و شوروی در این زمینه ایجاد خواهد کرد. بدین ترتیب، وابسته نظامی با یک ترفند ساده فریب خورد: او بیست و هشت بمب‌افکن جدید ندیده بود، بلکه تعداد کمتری از بمب‌افکن‌ها را دیده بود که چندین بار از مقابل سکوی

نمایش عبور کرده بودند[71]. با این حال، اطلاعات نادرستی که این وابسته ارائه داد، به دلیلی برای افزایش هزینه‌های دفاعی آمریکا تبدیل شد.

تلاش‌های متعددی برای غلبه بر این کمبود اطلاعات درباره ارتش شوروی صورت گرفت. یکی از این پروژه‌ها، با نام رمز «موبی دیک»، شامل پرتاب بالن‌هایی در اروپای غربی بود که به دوربین‌های آویزان به سمت پایین مجهز بودند. ایده این بود که این بالن‌ها توسط بادهای غربی قوی از فراز اتحاد جماهیر شوروی عبور کرده و به ژاپن یا اقیانوس آرام برسند. در آن نقطه، دوربین‌ها در پاسخ به یک سیگنال رادیویی آزاد شده و بازیابی می‌شدند. در واقع، بسیاری از این بالن‌ها بر فراز اتحاد جماهیر شوروی سقوط کردند که به شوروی‌ها امکان داد تا فناوری دوربین‌ها را ارزیابی کنند. به دلیل حرکت تصادفی بالن‌ها بر فراز مساحت وسیعی از اتحاد جماهیر شوروی، تصاویر به دست آمده

[71] ؛ جان پرادوس، "برآوردهای شوروی: تحلیل‌های اطلاعاتی آمریکا و قدرت نظامی روسیه" (نیویورک، ۱۹۸۲)، ۵۰-۳۸.

از فیلم‌های بازیابی شـــده، تنها حداقل معلومات اطلاعاتی را در بر داشت[72].

در 21 ژوئیه 1955، در نشـــســـت «چهار قدرت بزرگ»، رئیس‌جمهور دوایت آیزنهاور طرح «آســـمان‌های باز» را برای نظارت هوایی متقابل بین ایالات متحده و اتحاد جماهیر شوروی پیشنهاد کرد. بر اساس این طرح، «هر کشـور نقشـه‌های تأسـیسـات نظامی خود را به کشـور دیگر ارائه می‌دهد» و هر کشـــور حق خواهد داشـــت تا به هر شـــکلی که مناسـب می‌داند، شـناسـایی هوایی از قلمرو کشـور دیگر انجام دهد[73]. آیزنهاور معتقد بود که این طرح هرگونه تلاش برای حمله غافلگیرانه را آشـکار خواهد کرد؛ او بر این باور بود که طرفی که قصـد حمله دارد، در صورت قرار گرفتن تحت شناسایی هوایی نامحدود، قادر به دستیابی به عنصـــر غافلگیری نخواهد بود. این شـــنـاســـایی همچنین اجرای توافقات آتی خلع ســـلاح را تســـهیل کرده و به تعیین اینکه آیا طرف مقابل به تعهدات خود عمل می‌کند یا خیر، کمک خواهد کرد.

---

[72] ؛ پرادوس، "برآوردهای شـــوروی"، ۳۰-۲۹. برای روایتی مفصـــل‌تر، به کتاب کورتیس پیبلز، "پروژه موبی دیک: بالن‌های شناسایی بر فراز روسیه" (واشنگتن دی‌سی: انتشارات اسمیتسونیان، ۱۹۹۱) مراجعه کنید.

[73] ؛ اســـتفان آمبروز، "آیزنهاور: رئیس‌جمهور، جلد دوم" (نیویورک: ســـایمون و شوستر، ۱۹۸۴)، ۲۶۴-۲۶۵.

با این حال، آیزنهاور حاضـــر نبود برنامه‌های خود برای بهبود گردآوری اطلاعات را به توافق شوروی گره بزند. او هشت ماه پیش از آن، در 24 دسـامبر 1954، مخفیانه با توسـعه یک هواپیمای شـناسـایی جدید به نـام U-2 موافقـت کرده بود کـه می‌توانســـت فراتر از دســـترس جنگنده‌های شـــوروی و موشـــک‌های زمین به هوا (ســـام) پرواز کند. همچنین، انتظار می‌رفت که تصـــویربرداری شـــناســـایی هوایی با اســـتفاده از ماهواره‌ها در آینده نزدیک به واقعیت بپیوندد [74]. به هر حال، نیکیتا خروشـچف، نخسـت‌وزیر شـوروی، پیشـنهاد «آسـمان‌های باز» را رد کرد و آن را تلاشـی برای مشـروعیت بخشـیدن به جاسـوسـی خواند. در ژوئن 1956، آیزنهاور با اولین پرواز هواپیمای U-2 بر فراز خاک شوروی موافقت کرد[75].

در طول چهار ســـال بعدی، هواپیماهای U-2 بر فراز خاک شـــوروی و مناطق اطراف آن، اطلاعات اطلاعاتی گســـترده‌ای جمع‌آوری کردند که برای اولین بار پوشش روتینی از تأسیسات و پایگاه‌های مهم شوروی را برای ایالات متحده فراهم آورد. شـــوروی‌ها اعتراضـــات دیپلماتیک غیرعلنی علیه این پروازها مطرح کردند، اما در ابتدا نتوانســـتند کاری

---

[74] ؛ پیش از این، در سال ۱۹۴۶، از مؤسسه راند، یک اتاق فکر که با نیروی هوایی ارتش آن زمان قرارداد داشت، خواسته شد تا امکان‌سنجی و مزایای ماهواره‌های زمینی را بررسی کند.

[75] ؛ آمبروز، "آیزنهاور"، جلد دوم.

در قبال آن‌ها انجام دهند. با این حال، تنها مسئله زمان بود تا شوروی‌ها بتوانند ابزارهایی برای حمله به U-2 توسعه دهند و در مه 1960، موفق به سرنگونی یکی از این هواپیماها و اسارت خلبان آن، گری پاورز، شدند.

حتی پیش از حادثه U-2، ایالات متحده کار بر روی پروژه‌های تصویربرداری شناسایی ماهواره‌ای را آغاز کرده بود[76]. با وجود اینکه این قابلیت در مرحله توسعه خود برای بحث‌های صریح باز بود [77]، اما وجود آن در سال‌های اولیه به شدت محرمانه طبقه‌بندی شد[78]. این

---

[76] ؛ برای اطلاع از تصمیم ایالات متحده برای ساخت ماهواره شناسایی و شکست‌ها و موفقیت‌های اولیه این برنامه، به موارد زیر مراجعه کنید:

مک‌دوگال، "آسمان‌ها و زمین"، ۱۳۱-۹۷، ۱۹۰، ۲۲۴؛ و دوین ای. دی، جان ام. لاگسدون، و برایان لاتل، "چشمی در آسمان: داستان ماهواره‌های جاسوسی کرونا" (واشنگتن دی‌سی: اسمیتسونیان، ۱۹۹۸).

[77] ؛ به شهادت سرلشکر بی. ال. شرایور، "تحقیق در برنامه‌های ماهواره‌ای و موشکی"، جلسات استماع در برابر کمیته فرعی تحقیق در آمادگی وابسته به کمیته خدمات مسلح، سنای ایالات متحده، کنگره ۸۵، جلسه دوم، ۲۲-۶ ژانویه ۱۹۵۸، بخش دوم مراجعه کنید.

[78] ؛ شوروی‌ها احتمالاً از وجود چنین قابلیت‌های نظارتی آگاه بودند، اما مناسب نمی‌دیدند که توجه عمومی را به این حقایق جلب کنند. در آن زمان، و در راستای رد طرح "آسمان‌های باز" توسط اتحاد جماهیر شوروی، این کشور موضعی اتخاذ کرده بود که شناسایی هوایی نوعی جاسوسی و مغایر با قوانین بین‌المللی

سیاست تا سال 1978 پابرجا بود، زمانی که رئیس‌جمهور جیمی کارتر – برای اطمینان دادن به مردم آمریکا درباره امکان راستی‌آزمایی معاهده دوم محدودیت تسلیحات استراتژیک (SALT II) – اعلام کرد که ایالات متحده قابلیت‌هایی دارد که وجودشان تا آن زمان محرمانه باقی مانده بود. با پایان جنگ سرد، از وجود «دفتر ملی شناسایی» (NRO) رفع طبقه‌بندی محرمانه شد. این سازمان، آژانسی است که مسئول «تحقیق و توسعه، و رهگیری داده‌های مبادله شده از طریق هوا و فضا» است و برای برآورده کردن نیازهای اطلاعاتی دولت آمریکا طراحی شده است[79].

است. در نتیجه این موضوع، دولت آمریکا نگران بود که بحث علنی درباره شناسایی هوایی، مسکو را به ایجاد مشکل در این زمینه تشویق کند. بنابراین، با وجود انجام بحث عمومی درباره شناسایی هوایی در اواخر دولت آیزنهاور، دولت کندی، با این دیدگاه که دلیلی برای تحریک خروشچف با تأکید علنی بر حق ایالات متحده برای انجام چنین شناسایی وجود ندارد، "گام‌هایی... برای تبدیل برنامه نوپای شناسایی فضایی از خاکستری متوسط به سیاه تیره" برداشت. (بروز، "سیاه عمیق"، ۱۰۷). با این حال، همانطور که والتر مک‌دوگال اشاره می‌کند، "تا سال ۱۹۶۳ شوروی‌ها شروع به پرتاب ماهواره‌های جاسوسی خود کردند که در واقع نظارت از فضا را مشروعیت بخشید"، کتاب: "آسمان‌ها و زمین"، ۳۴۸.

[79] ؛ اریک اسمیت: "واحد جاسوسی فضایی با زندگی جدید در روشنایی روز روبرو می‌شود"، نیویورک تایمز، ۳ نوامبر ۱۹۹۰.

کلید شناسایی تصویری از فضا، کیفیت و توان تجهیزات نوری مورد استفاده برای جمع‌آوری و تمرکز نور بازتاب‌شده از اجسام روی زمین است. انتخاب ارتفاع مدار ماهواره نیازمند مصالحه بین کیفیت تصویر (هرچه مدار به زمین نزدیک‌تر باشد، کیفیت تصویر در صورت مساعد بودن سایر شرایط بهتر است) و مدت زمانی است که ماهواره می‌تواند در ارتفاع باقی بماند (اگر ماهواره از لایه‌های بالایی جو عبور کند، کشش جوی – نیروی هوایی یا اصطکاکی که در خلاف جهت حرکت نسبی یک جسم عمل می‌کند – باعث کند شدن و سقوط آن به زمین می‌شود). عوامل دیگری نیز مدار را تعیین می‌کنند، از جمله الزامات برای افزایش توانایی تصویربرداری از بخش‌های خاصی از سطح زمین و موقعیت‌یابی ماهواره با در نظر گرفتن خورشید، به طوری که تصاویر تحت شرایط نوری ایده‌آل گرفته شوند. یک دشواری خاص در تصویربرداری از فضا این است که نور باید از کل جو عبور کند که تمایل به پراکندگی و در نتیجه تار کردن تصویر دارد. از سوی دیگر، دوربین‌هایی که از فضا به زمین تصویربرداری می‌کنند – برخلاف دوربین‌های نصب شده بر روی هواپیماها – در معرض لرزش موتور هواپیما یا اغتشاشات جوی قرار نمی‌گیرند[80].

[80] از قضا، تأثیرات اعوجاجات در جو زمین ممکن است برای تصویربرداری فضایی، در مقایسه با تصویربرداری هوایی، مشکل کمتری باشد. در اوایل توسعه

در ابتدا، تمام ماهواره‌های مورد استفاده در تصویربرداری هوایی از دوربین‌های با کیفیت بالا استفاده می‌کردند که فیلم را پس از دریافت فرمان از زمین، در یک کپسول رها می‌کردند. سپس فیلم پیش از رسیدن به زمین بازیابی شده، ظاهر و تحلیل می‌شد. برای اهداف خاص – مانند نظارت بر تغییرات بلندمدت یا شناسایی و مکان‌یابی تأسیسات نظامی ثابت – تأخیر بین گرفتن عکس، ظاهر کردن و تحلیل آن مشکلی ایجاد نمی‌کند. اما دشواری در سیستم بازیابی فیلم، مربوط به اهداف متحرک یا رویدادهایی است که به سرعت اتفاق می‌افتند. به عنوان مثال، تأخیر چند روزه ممکن است تفاوت بین موفقیت یا شکست یک حمله غافلگیرانه باشد.

برای تسریع این فرآیند، می‌توان فیلم را با مجموعه‌ای از نیمه‌رساناهای حساس به نور که به عنوان «مدارهای جفت‌کننده بار» (Charge-Coupled Devices یا CCD) شناخته می‌شوند، جایگزین

تصویربرداری فضایی، ورنر فون براون، کارشناس مشهور موشک، مشاهده کرد که "گرفتن عکس از فضای بیرونی، جو را از بیرون شفاف‌تر از پایین نشان می‌دهد" برای روشن شدن این نکته، او مثال زیر را مطرح کرد: "یک تکه کاغذ مومی بردارید. آن را نزدیک صورت خود قرار دهید و فقط اشکال مبهمی خواهید دید. آن را روی یک تکه روزنامه قرار دهید، آنگاه شفاف به نظر خواهد رسید" سخنرانی در دومین نشست سالانه انجمن ارتش آمریکا، ۲۶ اکتبر ۱۹۵۶، نقل شده از کتاب: "آسمان‌ها و زمین"، ۲۲۴.

کرد. هنگامی که نور به یکی از این نیمه‌رساناها می‌تابد، یک بار الکترونی متناسب با شدت نور تولید می‌شود. با اندازه‌گیری مقدار این بارها در هر حسگر از مدارهای جفت‌کننده بار و مشاهده دقیق مکان هر عنصر روی شبکه، پردازشگر می‌تواند از این اطلاعات یک تصویر روی فیلم یا رایانه بسازد. از آنجا که تأخیر کمی در ارسال الکترونیکی این داده‌ها از فضا به ایستگاه زمینی وجود دارد، تصویر را می‌توان عملاً در زمان واقعی – یعنی با تأخیر ناچیز – روی زمین بازتولید کرد[81].

با وجود این پیشرفت‌ها، قابلیت‌های شناسایی از طریق تصویربرداری هوایی همچنان به نور خورشید وابسته است و به عدم وجود پوشش ابری بستگی دارد. برای غلبه بر این محدودیت‌ها، از الگوهای دیگری از تصویربرداری با استفاده از امواج راداری یا اشعه مادون قرمز (که از گرما یا اجسام داغ ساطع می‌شود) استفاده می‌شود. به عنوان مثال: به جای اتکا به اشعه خورشید که به طور طبیعی از یک جسم روی زمین منعکس می‌شود تا تصویری ظاهر شود، یک سیستم شناسایی راداری امواج رادیویی را به سمت منطقه هدف در زیر خود

[81] ؛ این توضیح درباره دستگاه‌های جفت‌شونده با بار (Charge-Coupled Devices) از کتاب هارولد هوف، "شناسایی ماهواره‌ای" (۱۹۹۱)، ۴۸-۴۶ اقتباس شده است.

می‌فرستد و امواج منعکس شده از اجسام متعدد را دریافت می‌کند و – طی یک فرآیند پیچیده – این داده‌ها را به تصویر تبدیل می‌کند[82]. این کار با روشن کردن اهداف به طور مستقل از خورشید و با استفاده از طول موج‌هایی که می‌توانند از ابرها، مه یا بارش‌ها عبور کنند، انجام می‌شود. سیستم‌های شناسایی راداری می‌توانند به صورت 24 ساعته و در هر شرایط آب و هوایی تصویربرداری کنند.

به همین ترتیب، می‌توان از بخش دیگری از طیف الکترومغناطیسی، یعنی اشعه مادون قرمز، برای کشف اجسامی که گرم‌تر یا سردتر از محیط اطراف خود هستند، بهره برد. تصویربرداری مادون قرمز در

---

[82] ؛ از آنجایی که از سیگنال‌هایی با طول موج بلند (در مقایسه با نور) استفاده می‌شود، رادار تصویری بسیار مبهم، به معنای واقعی کلمه یک نقطه نور روی صفحه، نشان می‌دهد. بهترین راه برای جبران نارسایی در ثبت طول موج بزرگ، افزایش اندازه آنتن است. به همین دلیل، فناوری‌ای به نام رادار با دیافراگم ترکیبی (SAR) توسعه یافت که در آن یک آنتن کوچک که در یک خط مستقیم حرکت می‌کند، تأثیر یک آنتن بسیار بزرگتر را ایجاد می‌کند. به لطف پردازنده‌های قدرتمند داخلی، سیستم‌های رادار SAR هزاران تصویر با وضوح پایین را جمع‌آوری کرده و آن‌ها را برای تشکیل تصویری منسجم‌تر ترکیب می‌کنند. برای جزئیات بیشتر درباره نحوه عملکرد سیستم‌های SAR، به کتاب چارلز ایلاچی، "تصاویر راداری زمین از فضا"، مجله دانشمندان آمریکایی (دسامبر ۱۹۸۲)، ۶۱-۵۴ مراجعه کنید.

طول روز به فرد امکان می‌دهد تا برگ‌های واقعی درختان (که دارای امضای حرارتی خاصی هستند) را از بیشتر شبکه‌های استتار (که امضای حرارتی متفاوتی دارند) تشخیص دهد. در شب، اجسامی که در طول روز گرم شده‌اند، با نرخ‌های متفاوتی سرد می‌شوند. یک سیستم مادون قرمز تحلیلی ممکن است بتواند انواع مختلفی از اجسام و اهداف را کشف کند. به عنوان مثال: هنگام تاریکی هوا، اجسام فلزی – مانند تانک‌ها – کندتر از زمین اطراف و پوشش گیاهی سرد می‌شوند. سیستم تصویربرداری مادون قرمز می‌تواند این تفاوت را ثبت کند و بدین ترتیب، فرد قادر به تعیین موقعیت این تانک‌ها هنگام غروب آفتاب خواهد بود[83].

[83] ؛ وزارت دفاع ایالات متحده، "گزارش نهایی کنگره درباره جنگ خلیج فارس" (واشنگتن دی‌سی: انتشارات دولتی، ۱۹۹۲)، ۱۳۸، تاکتیک "ضربه زدن به تانک‌ها" را مورد بحث قرار می‌دهد که در طول جنگ خلیج فارس برای بهره‌برداری از این پدیده توسعه یافت. ماهواره همچنین می‌تواند از یک حسگر چندطیفی استفاده کند که هدف را با استفاده از فرکانس‌های متعدد، در داخل و خارج از طیف نور مرئی، تصویربرداری می‌کند. تصویر چندطیفی می‌تواند اطلاعاتی درباره هدف آشکار کند که با دید انسانی قابل تشخیص نیست. به عنوان مثال، در طول جنگ خلیج فارس، از تصاویر چندطیفی برای شناسایی مناطق کم‌عمق نزدیک سواحل، اطلاعات لازم برای برنامه‌ریزی عملیات آبی-خاکی، استفاده شد. علاوه بر این، از آنجایی که بیشتر تصاویر اکنون به صورت دیجیتالی فرمت می‌شوند،

با وجود اینکه این قابلیت‌های شناسایی تصویری چشمگیر و مفید هستند، اما یک نقص دارند و آن کیفیت تصویر حاصله است. به طور کلی، وضوح (دقت: کوچکترین جسم قابل مشاهده) تصاویر گرفته شده با نور مرئی بهتر از تصاویری است که از طریق امواج راداری یا سایر بخش‌های طیف الکترومغناطیسی گرفته می‌شوند. برای برخی اهداف، مانند حرکت جمعی نیروها، تصویربرداری با وضوح پایین از یک منطقه وسیع ممکن است کافی باشد. با این حال، برای سایر الزامات، مانند اطمینان از ویژگی‌های فنی یک سلاح خاص، دقت بیشتری لازم است. یکی از عوامل کلیدی در استفاده مؤثر از این انواع مختلف سیستم‌های تصویربرداری، دانستن سطح دقت مورد نیاز برای پاسخ به سؤالات دولت‌ها درباره رقبای احتمالی یا دشمنانشان در میدان نبرد است.

داده‌ها را می‌توان به راحتی پردازش کرد تا تفاوت‌های کوچک برجسته شوند، که منجر به کنتراست بیشتر و در نتیجه وضوح مؤثرتر می‌شود. تفاوت‌های ظریف در عوارض زمین که در یک تصویر سنتی قابل تشخیص نیستند، می‌توانند از طریق تکنیک‌های پیشرفته پردازش تصویر کامپیوتری آشکار شوند.

زمانی که شناسایی از طریق تصویربرداری هوایی تنها در انحصار سازمان‌های اطلاعاتی آمریکا و شوروی بود، به سر آمده است. اکنون کشورهای دیگری نیز ماهواره‌های خود را برای انجام شناسایی تصویری با اهداف اطلاعاتی پرتاب کرده‌اند. با افزایش آگاهی از اهمیت این فناوری، کشورهای بیشتری توانسته‌اند وارد این حوزه شوند، زیرا این کار نیازمند اراده و آمادگی برای پرداخت هزینه‌های لازم است. کشورهایی که ماهواره‌های خود را پرتاب کرده‌اند یا به طور جدی برای پرتاب آن‌ها فعالیت می‌کنند، عبارتند از: چین، فرانسه و ژاپن[84].

از تحولات مرتبط با این موضوع، پیشرفت‌هایی است که در قابلیت‌های شناسایی از طریق تصویربرداری هوایی برای اهداف تجاری رخ داده است. در سال 1986، یک آژانس دولتی فرانسوی ماهواره‌ای برای شناسایی تصویری هوایی (ماهواره SPOT [Satellite Pour l'Observation de la Terre] یا ماهواره رصد زمین) پرتاب کرد که تصاویری با وضوح تا ده متر و به صورت سیاه و سفید برای فروش به عموم مردم ارائه می‌داد. در سال 1999، شرکت

---

[84] ؛ بر اساس "راهنمای فضایی جهانی" فدراسیون دانشمندان آمریکایی (www.fas.org/spp/guide/china/index.html)، چین از سال ۱۹۷۵ و فرانسه از سال ۱۹۹۵ به شناسایی نوری از فضا می‌پردازند. برنامه‌های ژاپن نیز شامل پرتاب چهار ماهواره (دو رادار نوری و دو رادار با دیافراگم مصنوعی) از سال ۲۰۰۲ است.

آمریکایی آیکونوس (IKONOS) تصاویری با وضوح یک متر را به بازار عرضه کرد؛ برنامه‌های این شرکت دستیابی به تصاویر با وضوح بالاتر (وضوح نیم متر) را هدف قرار داده است.

از سال 2004، این شرکت از دولت آمریکا مجوز انجام این کار را دریافت کرد[85]. همچنین، شرکت‌ها یا مؤسسات دولتی در روسیه، آفریقای جنوبی، کانادا، هند، استرالیا، اسرائیل، چین و برزیل، خدمات شناسایی برای اهداف تجاری ارائه می‌دهند یا قصد ارائه آن را دارند[86].

---

[85] ؛ ورنون لوب: "ایالات متحده قوانین فروش تصاویر ماهواره‌ای را تسهیل می‌کند"، واشنگتن پست، ۱۶ دسامبر ۲۰۰۰.

[86] ؛ این فهرست از یک مطالعه موردی تهیه شده برای دانشکده حکمرانی جان اف. کندی دانشگاه هاروارد، توسط راشل ای. بیلینگزلی، متیو آر. دومسالا، و برایان سی. پین، "دفتر شناسایی ملی: راهبردی برای مقابله با بازاریابی تصاویر فضایی"، ۶ آوریل ۱۹۹۹، موجود در: www.fas.org/eye/ADA366610.htm، گرفته شده است. دسترسی گسترده به تصاویر تجاری مزایا و مشکلاتی را به همراه دارد. از یک سو، دولت ممکن است بخشی از نیازهای خود به تصاویر را از طریق خرید محصولات فروشندگان تأمین کند، که به سازمان‌های اطلاعاتی‌اش اجازه می‌دهد بر نیازهای تخصصی که بعید است بخش تجاری آن‌ها را برآورده کند، تمرکز کنند. از سوی دیگر، گسترش ماهواره‌های شناسایی نوری تجاری، پنهان کردن استقرار نیروها و عملیات نظامی حساس را برای دولت دشوار می‌سازد. (ایالات متحده تلاش کرده است با این مشکل از طریق "کنترل

اطلاعات ارتباطی

اطلاعات ارتباطی یکی از قدیمی‌ترین انواع اطلاعات سیگنالی است که همزمان با استفاده از رادیو برای ارتباطات نظامی و دیپلماتیک آغاز شد[87]. در پایان جنگ جهانی دوم، اطلاعات ارتباطی (همراه با رمزگشایی، یعنی شکستن کدها و رمزهایی که پیام‌های بسیار

دکمه‌های دوربین" – یعنی اختیار، در زمان بحران، برای جلوگیری از تصویربرداری اپراتورها از مناطق خاص – در مورد سیستم‌های دارای مجوز مقابله کند؛ این امر در مورد سیستم‌های ماهواره‌ای خارجی کمکی نمی‌کند.) برای یک مرور کلی مختصر درباره این موضوع، به گزارش کمیته ملی بازنگری دفتر شناسایی ملی (نوامبر ۲۰۰۰)، در www.fas.org/irp/nro/commission مراجعه کنید.

[87] ؛ با توجه به امکان رهگیری پیام‌های بی‌سیم به طور خاص، پیام‌های مهم احتمالاً به صورت رمزگذاری شده ارسال می‌شوند، به این معنی که اطلاعات ارتباطی و تحلیلگران رمز از یک سو، و فرآیند شکستن کدها و رمزها از سوی دیگر، ارتباط نزدیکی با هم دارند، اگرچه احتمالاً تحلیل رمز به عنوان یک تکنیک تحلیل اطلاعات (و نه یک تکنیک جمع‌آوری اطلاعات) در نظر گرفته می‌شود؛ به همین دلیل، بحث در مورد آن به فصل بعدی موکول شده است

حساس از طریق آن‌ها منتقل می‌شوند)[88] بر اساس اطلاعات موجود، مهم‌ترین منبع اطلاعاتی برای قدرت‌های بزرگ در زمان صلح و جنگ بود.

---

[88] با توجه به امکان رهگیری پیام‌های بی‌سیم به طور خاص، پیام‌های مهم احتمالاً به صورت رمزگذاری شده ارسال می‌شوند، به این معنی که اطلاعات ارتباطی و تحلیلگران رمز از یک سو، و فرآیند شکستن کدها و رمزها از سوی دیگر، ارتباط نزدیکی با هم دارند، اگرچه احتمالاً تحلیل رمز به عنوان یک تکنیک تحلیل اطلاعات (و نه یک تکنیک جمع‌آوری اطلاعات) در نظر گرفته می‌شود؛ به همین دلیل، بحث در مورد آن به فصل بعدی موکول شده است.
۲ .با توجه به نگرانی‌های مداوم در مورد پنهان‌کاری، بعید است که تا مدتی دیگر شرح جامعی از مزایای اطلاعات ارتباطی در طول جنگ سرد نوشته شود. با این حال، مورخان آژانس امنیت ملی(NSA) ، آژانس اطلاعات سیگنال‌های ایالات متحده، ادعا می‌کنند که موفقیت آمریکا در شکستن سیستم‌های رمزگذاری شوروی در سال‌های پس از جنگ جهانی دوم "با موفقیت‌های جنگ جهانی دوم رقابت کرد "و از دست دادن این قابلیت در سال ۱۹۴۸ شاید بزرگترین خسارت اطلاعاتی در تاریخ ایالات متحده بوده است. این خسارت در نهایت به جاسوسی ویلیام وایزبند، زبان‌شناس روسی در آژانس امنیت نیروهای مسلح) که سلف NSAبود (نسبت داده شد. کتاب دیوید ای. هچ و رابرت لوئیس بنسون، *جنگ کره: پیشینه اطلاعاتی * (www.nsa.gov/korea/papers/sigint_background_korean_war.htm)، در [آدرس وب‌سایت موجود نیست] موجود است. اما بدون دسترسی به بایگانی‌های اطلاعاتی شوروی، تعیین میزان خسارت وارده توسط جاسوس آمریکایی جان واکر، که از سال ۱۹۶۸ تا ۱۹۸۵ مواد رمزنگاری را در اختیار اتحاد جماهیر شوروی قرار داد، غیرممکن است. بر اساس بدترین سناریوها، می‌توان

یکی از اولین کاربردهای مستند اطلاعات ارتباطی، تلاش نیروی دریایی بریتانیا در طول جنگ جهانی اول برای کسب هشدار زودهنگام درباره هرگونه تلاش نیروی دریایی آلمان برای ورود به دریای شمال بود. بریتانیایی‌ها در آغاز جنگ، کابل‌های تلگراف زیردریایی آلمان را که این کشور را به قاره آمریکا، آفریقا و اسپانیا متصل می‌کرد، قطع کردند. این اقدام آلمانی‌ها را مجبور کرد تا تلگرام‌های دیپلماتیک خود را به این مناطق از طریق رادیو ارسال کنند که در معرض رهگیری توسط ایستگاه‌های شنود بریتانیا قرار گرفت[89].

استدلال کرد که موادی که واکر و همکارانش در اختیار کا گ ب شوروی قرار دادند، به آنها «مزیت مشابهی با آنچه متفقین از طریق آگاهی از کد اولترا بر آلمان نازی داشتند، می‌داد. به طور خلاصه، اگر جنگی بین دو ابرقدرت در می‌گرفت، واکر می‌توانست کفه ترازو را به نفع آمریکایی‌ها بر شوروی سنگین‌تر کند.» (آنجلو کودیولا، «تحویل اطلاعات: اطلاعات در عصر مدرن» (نیویورک فری پرس، ۱۹۹۲)، صفحات ۱۷۸-۱۷۶).

[89] ؛ برای بحث کامل در مورد اطلاعات ارتباطی در طول جنگ جهانی اول، به کتاب *اتاق ۴۰: اطلاعات نیروی دریایی بریتانیا از ۱۹۱۴ تا ۱۹۱۸* نوشته پاتریک بیزلی (نیویورک: انتشارات هارکورت، جووانوویچ، ۱۹۸۲) مراجعه کنید

با وجود موفقیت‌های اولیه، این جنگ جهانی دوم بود که اطلاعات ارتباطی را برای بریتانیا و آمریکا به اوج خود رساند. با استفاده از پروژه‌های «اولترا» و «مجیک»، ارتباطات آلمان رهگیری و رمزگشایی شدند و حجم زیادی از اطلاعات دقیق و به موقع به فرماندهان سیاسی و نظامی بریتانیا و آمریکا رسید. با این حال، اندازه‌گیری دقیق میزان تأثیر آن بر روند جنگ، یک وظیفه تاریخی عظیم باقی می‌ماند. واضح است که نقش اطلاعات ارتباطی در شکست نیروهای محور بی‌بدیل بود[90].

یکی از بارزترین مواردی که اطلاعات ارتباطی به طور قاطع در آن نقش داشت، پیروزی نیروی دریایی آمریکا بر نیروی دریایی ژاپن در نبرد میدوی بود. ژاپن امیدوار بود با بهره‌برداری از موفقیت چشمگیر خود در پرل هاربر در دسامبر ۱۹۴۱، جزیره استراتژیک میدوی[91] را تصرف

---

[90] ؛ مطالب زیادی در مورد رمزنگاری آمریکایی و بریتانیایی در طول جنگ جهانی دوم نوشته شده است؛ برای این نکته، به کتاب *خیانت شرافتمندانه: تاریخچه اطلاعات، جاسوسی و اقدامات پنهانی آمریکا از انقلاب آمریکا تا سازمان سیا* نوشته تول مراجعه کنید.)نیویورک: ماهنامه آتلانتیک، ۱۹۹۱، صفحات ۳۹۷-۳۸۴(.

[91] ؛ ژاپنی‌ها هدف خود را AF می‌نامیدند و افسران اطلاعاتی معتقد بودند که AF مخفف Midway است. با این حال، اطلاعات در واشنگتن فکر می‌کرد که ممکن است به منطقه دیگری مانند جزیره جانستون، اوهایو یا حتی ساحل غربی ایالات متحده اشاره داشته باشد. برای تأیید اینکه Midway واقعاً هدف حمله ژاپنی‌ها

کند و سپس باقیمانده نیروهای دریایی آمریکا در اقیانوس آرام را نابود سازد. اگر طرح ژاپن موفق می‌شد، دروازه‌های هاوایی برای تهاجم باز می‌شد و ایالات متحده مجبور می‌شد بر اساس خواسته‌های توکیو به صلح تن دهد. ژاپنی‌ها به دنبال یک پیروزی سریع در اقیانوس آرام بودند، زیرا نبرد طولانی با ایالات متحده – کشوری قدرتمندتر و پرجمعیت‌تر از ژاپن – در نهایت به نابودی آن‌ها منجر می‌شد. بدون اطلاع ژاپنی‌ها، متخصصان رمزگشایی نیروی دریایی آمریکا در هاوایی، ارتباطات رمزگذاری‌شده نیروی دریایی ژاپن را رهگیری و رمزگشایی کردند. در نتیجه، نیروهای آمریکایی از پیش از طرح ژاپن برای حمله به میدوی مطلع شدند. آن‌ها از این اطلاعات درباره ناوگان دریایی ژاپن در شمال جزیره در چهارم ژوئن ۱۹۴۲ بهره بردند و چهار

بوده است، ایستگاه اطلاعات نظامی در هاوایی به فرمانده آمریکایی در Midway دستور داد تا یک سیگنال رادیویی به هاوایی ارسال کند و به آنها اطلاع دهد که آب آشامیدنی در حال اتمام است. همانطور که انتظار می‌رفت، ژاپنی‌ها این پیام را رهگیری کردند. دو روز بعد، یک پیام ژاپنی (که توسط ایالات متحده رهگیری شد) به توکیو مخابره شد که بیان می‌کرد آب آشامیدنی در AF در حال اتمام است. بنابراین، آنها ناخواسته تأیید کردند که AF در واقع Midway است). نگاه کنید به : Leighton, Roger Benoit, and John Costello, *I Was There: Pearl Harbor and Midway: Unmasking the Secrets*, New York: Warsaw Press, 1985, pp. 421-422.)

ناو هواپیمابر دشـــمن منهدم شـــد. این امر توانایی ژاپن برای انجام عملیـات گســـترده در اقیـانوس آرام را از بین برد. نبرد میـدوی یـک شـــکســـت قاطع برای ژاپنی‌ها و نقطه عطفی در روند جنگ بود؛ این نبرد هرگونه امید ژاپن به پیروزی ســـریع در جنگ را، اگر اصـــلاً امکان پیروزی وجود داشت، پایان داد[92].

طبیعی اســـت که تصـــور کنیم حســـاس‌ترین پیام‌های رادیویی هر کشـــوری برای حفظ محرمانگی رمزگذاری می‌شـــوند، اما در واقعیت، همه ســـیگنال‌های حســـاس رمزگذاری نمی‌شـــوند. به دلیل هزینه و دشـــواری رمزگذاری پیام‌ها، برخی از آن‌ها رمزگذاری نمی‌شـــوند؛ به عنوان مثال، ارتباطات صـــوتی تاکتیکی، مانند ارتباط بین هواپیماها و ایسـتگاه‌های کنترل زمینی، معمولاً بدون رمزگذاری پخش می‌شـوند.

---

[92] ؛ برای داسـتان نبرد و موفقیت اطلاعاتی پشـت آن، به کتاب لیتون، «و من هم آنجا بودم» مراجعه کنید. ۳. به گزارش کمیته اطلاعات سـنا مراجعه کنید: «مقابله با چالش‌های اطلاعاتی: مروری بر برنامه‌های ضدتروریسم.« رنامه‌های اطلاعاتی و امنیتی ایـالات متحـده (واشـــنگتن دی.ســـی.: دفتر مطبوعـاتی دولـت، ۱۹۸۶)، صفحات ۳۳-۳۴۸۰-۸۱. برای سال‌های متمادی، اتحاد جماهیر شوروی و همچنین روسـیه تا سـال ۲۰۰۲، تأسـیسـات شـنود ارتباطات را در لوردس و کوبا نگهداری می‌کردند. این تأسیسات توسط بیش از ۱۵۰۰ روس اداره می‌شد که آمریکایی‌ها و داده‌های آنها را شنود می‌کردند

در موارد دیگر، مکاتبات جاری رمزگذاری نمی‌شوند، زیرا تصور می‌شود – چه این تصور درست باشد چه غلط – که دشمن تمایلی به رهگیری یا پردازش آن‌ها ندارد، یا در صورت حجم زیاد اطلاعات، قادر به انجام آن نیست. به عنوان مثال، پیام‌های ترافیک تجاری رمزگذاری نمی‌شوند، اگرچه برخی از آن‌ها می‌توانند حاوی اطلاعات بالقوه دشمن باشند. در نهایت، نباید اهمیت اینرسی (بی‌عملی) را دست کم گرفت؛ به عنوان مثال، ایالات متحده واکنش دیرهنگامی نسبت به کشف رهگیری پیام‌های تلفنی از راه دور که از طریق برج‌های مایکروویو توسط مراکز دیپلماتیک کشورهای مختلف در داخل کشور انجام می‌شد، نشان داد.

تکنیک‌هایی که به عنوان «تحلیل ترافیک ارتباطی» شناخته می‌شوند، می‌توانند اطلاعات مفیدی را از نوسانات در حجم ارتباطات رادیویی و سایر ویژگی‌های ظاهری آن‌ها استخراج کنند، حتی زمانی که درک محتوای پیام‌ها غیرممکن باشد. به عنوان مثال، اگر مقر فرماندهی ارتش و پست‌های فرماندهی تابعه آن تعداد غیرمعمولی از پیام‌ها را مبادله کنند، تحلیلگر می‌تواند نتیجه بگیرد که یک عملیات مهم در

شـرف وقوع اسـت[93]. به همین ترتیب، با اسـتفاده از جهت‌یابی برای تعیین منشأ جغرافیایی سـیگنال رادیویی، می‌توان موقعیت کشـتی، هواپیما یا مقر فرماندهی صادرکننده این سیگنال را مشخص کرد.

به عنوان مثال، در جنگ جهانی دوم، زیردریایی‌های آلمانی فعال در آب‌های آزاد از رادیو برای ارتباط با یکدیگر و با فرماندهی عالی نیروی دریایی در خشـکی اسـتفاده می‌کردند. نیروی دریایی آلمان که از تاکتیک‌های «گروه گرگ‌ها» علیه کاروان‌های متفقین استفاده می‌کرد، برای هماهنگی حملات به تبادل حجم زیادی از سـیگنال‌ها بین زیردریایی‌های نوع U و فرماندهانشـان نیاز داشـت. اما این امر

---

[93] ؛ پیتر رایت، افسر سابقMI5 ، در خاطرات خود نوشت که اطلاعات شوروی از «تحلیل سیگنال» برای کاهش اثربخشی تلاش‌های نظارتی بریتانیا علیه عملیات اطلاعاتی شوروی در داخل و اطراف لندن استفاده می‌کرد. همانطور که قبلاً اشاره شد، شوروی‌ها ارتباطات رادیویی تیم‌های نظارتی بریتانیا را از داخل سفارت خود در لندن رصد می‌کردند و رمزگذاری داده‌های شنود شده تفاوت چندانی ایجاد نمی‌کرد. اگر تفاوتی ایجاد می‌کرد، این امر باعث می‌شد که آنها در مواجهه با ترافیک رادیویی معمولی و رمزگذاری نشده شهر، بیشتر برجسته شوند. با تجزیه و تحلیل آن سیگنال‌های رادیویی، و به ویژه حجم فعالیت‌های رادیویی، شوروی‌ها توانستند زمان انجام عملیات نظارتی ضداطلاعات بریتانیا (MIS) را تعیین کنند و اینکه آیا یکی از نیروهای خودشان در نتیجه این عملیات به خطر افتاده است یا خیر. طبق ارزیابی رایت، روس‌ها بیشتر اطلاعات خود را از طریق جابجایی نشان‌ها جمع‌آوری می‌کردند، نه از منابع دیگر.از محتوای پیام‌ها: کتاب: شکارچی جاسوس، صفحات ۵۳-۵۲

زیردریایی‌ها را در معرض «کشف جهت» توسط ایستگاه‌های رهگیری سیگنال رادیویی آمریکا و بریتانیا و کشتی‌های اسکورت کاروان‌ها قرار داد. عملیات جهت‌یابی متفقین به اندازه رمزگشـــایی ارتباطات نیروی دریایی آلمان ارزشـمند نبود، اما ابزار اطلاعاتی مهمی در نبرد اقیانوس اطلس به شـمار می‌رفت. اسـتفاده از آن همراه با رمزگشـایی، اجتناب کاروان‌های متفقین از گروه‌های گرگ آلمانی را ممکن ســـاخت و به مرور زمان به تلاش‌های آمریکا و بریتانیا برای شـــکار زیردریایی‌های U کمک کرد[94].

بیشـتر اطلاعات ارتباطی شـامل رهگیری پیام‌های رادیویی اسـت، اما پیام‌هایی که از طریق ســـیم‌ها ارســـال می‌شـــوند نیز قابل رهگیری هستند. این امر مستلزم دسترسی فیزیکی به سیم‌ها است و بنابراین کاربرد کمتری نســـبت به ســـیگنال‌های رادیویی دارد، اگرچه در موارد خـاص ممکن اســـت ضـــروری بـاشـــد. بـه عنوان مثـال، می‌توان

[94] ؛ به کتاب دیوید کان، «به دست گرفتن ماشین انیگما: مسابقه برای شکستن کدهای آلمانی، ۱۹۴۳-۱۹۳۹» (بوستون: هاوتون، میفلین، ۱۹۹۱)، صفحات -۱۴۴ ۱۴۵، ۲۱۶-۲۱۵ و ۲۵۱-۲۴۴؛ و کتاب پاتریک بیزلی، «اطلاعات بسیار ویژه: داستان اطلاعات نیروی دریایی، ۱۹۴۵-۱۹۳۹» (گاردن سیتی: دابلدی) مراجعه کنید.۱۹۵ سال (۱۹۷۸) صفحات ۵۶-۵۵، ۹۸-۹۷ و ۱۱۶

دستگاه‌های شنود تلفنی را بر روی خطوط تلفن سفارت یا کنسولگری دشمن در داخل کشور نصب کرد، و گاهی اوقات می‌توان مخفیانه به تلفن یا سیم‌های تلفن مورد استفاده دشمن حتی در خارج از کشور دسترسی پیدا کرد. به عنوان مثال، در شهرهای وین و برلین – که در اوایل و اواسط دهه ۱۹۵۰ تقسیم شده بودند – سازمان‌های اطلاعاتی بریتانیا و آمریکا توانستند دستگاه‌های شنود تلفنی را بر روی خطوط تلفن مورد استفاده مقامات نظامی شوروی نصب کنند. در برلین، این شامل حفر یک تونل مخفی از نقطه‌ای در بخش آمریکایی شهر به بخش دیگر و رهگیری سیم‌هایی بود که از بخش شوروی عبور می‌کردند[95].

[95] ؛ برای جزئیات این عملیات، به دیوید مورفی، سرگئی کوندراشف و جورج بیلی، *میدان نبرد در برلین: سازمان سیا در مقابل کا گ ب در جنگ سرد* (نیوهیون دارکون، انتشارات دانشگاه ییل، ۱۹۹۷)، فصل ۱۱، «گورج بلک، یک جاسوس شوروی در سرویس اطلاعات مخفی بریتانیا(SIS) ، شوروی‌ها را در مورد تونل مطلع کرد»، مراجعه کنید و این کتاب گزارشی از یک جلسه برنامه‌ریزی سیا SIS- را بازنشر می‌دهد و در آن بحث می‌کند که آیا شوروی‌ها از دانش قبلی خود در مورد دستگاه شنود برای فریب ایالات متحده و بریتانیا استفاده کرده‌اند یا خیر، صفحات ۴۲۸-۴۲۵.

یک تکنیک مرتبط دیگر، نصب دستگاه‌های شنود تلفنی بر روی کابل‌های تلفن زیردریایی است که توسط دشمن استفاده می‌شود. به عنوان مثال، غواصانی که در دهه ۱۹۷۰ از زیردریایی‌های آمریکایی فعالیت می‌کردند، توانستند دستگاه‌های شنود تلفنی را بر روی یک کابل تلفن شوروی که از کف دریای اوخوتسک می‌گذشت و پایگاه دریایی شوروی در پتروپاولوفسک در شبه‌جزیره کامچاتکا را به ولادی‌وستوک و مسکو متصل می‌کرد، نصب کنند. غواصان دستگاهی برای ضبط مکالمات قرار دادند که این ضبط‌ها در بازدیدهای دوره‌ای از محل جمع‌آوری می‌شدند[96].

از طریق ابزارهای مخفی نیز می‌توان به تجهیزات مورد استفاده برای ارسال و دریافت ارتباطات رمزگذاری‌شده دسترسی پیدا کرد. به عنوان مثال، یک افسر اطلاعاتی سابق بریتانیایی، موفقیت سازمان اطلاعاتی خود را در نفوذ به ارتباطات دیپلماتیک مصر، به نصب یک دستگاه شنود الکترونیکی در نزدیکی دستگاه رمزگذاری موجود در سفارت مصر در لندن نسبت می‌دهد. افسران اطلاعاتی بریتانیا خود

---

[96] ؛ این عملیات که با نام رمز «آیوی بلز» شناخته می‌شد، به تفصیل در کتاب شری استینتاگ و والراس توفر دارو با عنوان «فریب مرد نابینا: داستان ناگفته جاسوسی نیروی دریایی ایالات متحده» (نیویورک: پابلیک افیرز، ۱۹۹۸) شرح داده شده است.۱۵۸-۱۸۳ و جاهای مختلف کتاب.

را به عنوان کارکنان تعمیر و نگهداری تلفن جا زدند و توانستند دستگاهی را در نزدیکی خط تلفن نصب کنند. از طریق این دستگاه، آن‌ها توانستند صداهای متمایزی را که دستگاه هنگام تنظیمات اولیه توسط مصری‌ها تولید می‌کرد، ضبط کنند. با این اطلاعات، آن‌ها توانستند با تقلید این تنظیمات بر روی نمونه‌ای از این دستگاه که به طور گسترده در دسترس بود، رمزها را بشکنند و در مدت کوتاهی ارتباطات رمزگذاری‌شده مصر را رمزگشایی کنند. به همین ترتیب، عملیاتی برای نصب میکروفون‌های مینیاتوری در ماشین‌های تحریر هنگام ارسال آن‌ها به سفارت یک کشور انجام شد[97].

[97] ؛ کتاب «شکارچی جاسوس» نوشته رایت، صفحات ۸۶-۸۱. اخیراً، اطلاعات شوروی به دلیل اقدامات... توانست امنیت ضعیف آمریکایی‌ها در دسترسی به ماشین‌های تحریر برقی که به سفارت ایالات متحده در مسکو ارسال می‌شدند، یک نگرانی امنیتی قابل توجه بود. (وزارت امور خارجه ایالات متحده ماشین‌های تحریر را از طریق حمل و نقل تجاری بدون همراه به اتحاد جماهیر شوروی ارسال کرد.) با کاشت دستگاه‌های شنود پیشرفته در ماشین‌های تحریر، شوروی‌ها توانستند مطالب (طبقه‌بندی شده یا غیرطبقه‌بندی شده) در حال تایپ را «بخوانند». به کمیته منتخب سنای ایالات متحده در امور اطلاعاتی، «مقابله با چالش جاسوسی»، صفحات ۳۵-۳۴ مراجعه کنید. برای روایتی غیررسمی از این بخش، به کتاب «ایستگاه مسکو» نوشته کسلر، صفحات ۹۲ تا ۹۷ مراجعه کنید.

پیشـــرفت‌های فنی در ارتباطات، مشـــکلات جدیدی را برای اطلاعات ارتباطی به همراه داشـــته اســـت. در حالی که رهگیری فرســـتنده‌های سیگنال رادیویی سنتی به توانایی قرار دادن آنتن گیرنده با حساسیت کافی در مکان صحیح بستگی دارد و نصب دستگاه‌های شنود تلفنی بر روی خطوط تلفن اسـتاندارد به دسـترسـی فیزیکی وابسـته اسـت، رهگیری روش‌های ارتباطی جدید مشکلات دشوارتری را ایجاد می‌کند. به عنوان مثال، کابل‌های فیبر نوری که به دلیل ارائه پهنای باند بسـیار بیشـتر (و در نتیجه، توانایی ارسـال اطلاعات بیشـتر در هر واحد زمان) به صـورت تجاری مورد اسـتفاده قرار گرفته‌اند، نصـب دسـتگاه شـنود تلفنی بر روی آن‌ها دشـــوارتر از ســـیم‌های تلفنی اســـت که جایگزین آن‌ها شـده‌اند[98]. همین امر در مورد تلفن‌های همراه نیز صـدق می‌کند؛ اگرچه آن‌ها سـیگنال‌ها را از طریق امواج رادیویی ارسـال می‌کنند، اما به دلیل الگوریتم‌های پیچیده‌ای که تلفن‌های شخصی هنگام جابجایی

[98] ؛ برای کســـب اطلاعات در مورد دشـــواری‌های شـــنود مخفیانه کابل‌های فیبر نوری، به ویژه آن‌هایی که در زیر اقیانوس قرار دارند، به مقاله نیل کینگ با عنوان «با پیشرفت فناوری، دستگاه‌های جاسوسی آماده حفظ روش‌های استراق سمع خود هستند» در وال استریت ژورنال مراجعه کنید. ژورنال، ۲۳ مه ۲۰۰۱

تماس‌گیرنده از یک مکان به مکان دیگر بر اســـاس آن‌ها کار می‌کنند، مشکلات پیچیده‌ای را ایجاد می‌کنند[99].

اطلاعات تله‌متری

اطلاعات تله‌متری و سایر اشکال اطلاعات سیگنالی، جدیدتر از اشکال نوین اطلاعات ارتباطی هستند و بازتابی از گسترش روزافزون استفاده نظامی از پدیده‌های الکترومغناطیسی محسوب می‌شوند. اطلاعات تله‌متری از نظر مفهوم مشابه اطلاعات ارتباطی است، با این تفاوت که ارتباطات شنودشده بین یک وسیله آزمایشی (مانند موشک) و یک ایستگاه زمینی برقرار می‌شود و شامل کلمات نیست، بلکه شامل قرائت‌هایی از حسگرهای مختلف و سایر تجهیزات موجود در وسیله نقلیه است (این ارتباطات به عنوان «تله‌متری» شناخته می‌شوند). مقادیر متغیرهایی مانند شتاب حرکت وسیله نقلیه، دما

---

[99] ؛ برای مثال: در سال ۲۰۰۰، کمیته منتخب سنای ایالات متحده در امور اطلاعاتی اظهار داشت: «این کمیته عمیقاً از ناتوانی فزاینده آژانس امنیت ملی در مواجهه با چالش‌های فناوری و ارائه اطلاعات SIGINT (اطلاعات سیگنالی) به رهبران آمریکا نگران است.» (گزارش کمیته منتخب سنا در مورد تخصیص بودجه اطلاعاتی برای سال مالی ۲۰۰۱ در مورد فعالیت‌های اطلاعاتی دولت ایالات متحده و سیستم بازنشستگی و از کارافتادگی اطلاعاتی)سنترال، مه ۲۰۰۰.

در نقاط مختلف آن، نرخ جریان سوخت و غیره، هنگامی که به طور کامل نمایش داده می‌شوند، تصویری از آنچه در وسیله آزمایشی می‌گذرد به مهندسان می‌دهند. این امر به مهندسان کمک می‌کند تا هرگونه مشکلی را که ممکن است در طول آزمایش رخ دهد، کشف کرده و عملکرد وسیله نقلیه را بهبود بخشند.

در عین حال، واضح است که این اطلاعات مکانیسمی برای کارگران روزه‌دار است. با این حال، ایده استفاده از این داده‌ها در سیستم‌های تجزیه و تحلیل داده‌های اندازه‌گیری از راه دور بسیار دشوار است. علاوه بر بخش مربوط به تجزیه و تحلیل تایر، فصل دوم به آن به عنوان نوعی تحقیق اطلاعاتی و جایگاهی در مالکیت استانداردهای اصالت در کشوری که آزمایش در آن انجام می‌شود، می‌پردازد تا دیگران را از پرسش در مورد اجزای اندازه‌گیری از راه دور، عربی به کیفیت‌های زمینی، محروم کند. از این طریق، می‌توان داده‌های آزمایش را از راه دور ثبت و آن را در وسیله نقلیه وارداتی ذخیره کرد.و استخراج این اطلاعات مالی بعداً روش خوبی برای مدیریت داده‌ها از علائم است، به طوری که ممکن است مصری در معرض خطر باشد، زیرا ممکن است خطایی در دفتر مدیر خودرو رخ دهد.داده‌ها یا ارسال می‌شوند یا افراد زیادی از محل آن عبور می‌کنند.

اطلاعات الکترونیکی

اطلاعات الکترونیکی شـــامل نظارت و تجزیه و تحلیل ســـیگنال‌های الکترومغناطیســی ســاطع شــده توســط تجهیزات نظامی خارجی، به استثنای سیگنال‌های ارتباطی، می‌شود. در ابتدایی‌ترین سطح خود، اطلاعات الکترونیکی یک دولت را قادر می‌ســـازد تا عناصـــر کلیدی نیروهای مســـلح دولت دیگر (مانند رادارهای دفاع هوایی، مراکز فرماندهی و کنترل و غیره) را ردیابی کند. این امر معمولاً به عنوان "دستور نبرد الکترونیکی "شناخته می‌شود. استفاده از سیستم EORSAT(ماهواره شناسایی الکترونیکی بر فراز اقیانوس) توسط اتحاد جماهیر شـوروی سـابق و روسـیه امروزی نمونه‌ای از این نوع نظارت اســت. این روش جمع‌آوری داده‌های مبتنی بر فضــا ســال‌ها برای مکان‌یابی و ردیابی کشـــتی‌های جنگی ایالات متحده با رهگیری سیگنال‌های الکترونیکی معمول ساطع شده توسط کشتی‌ها هنگام حرکت در دریاهای آزاد استفاده می‌شد[100].

---

[100] ؛ کتاب *شمشیر و سپر: دستگاه اطلاعات و امنیت شوروی* نوشته جفری ریچلسون (کمبریج، ماساچوست: پالاور، ۱۹۸۶)، صفحات ۱۰۵-۱۰۳. همچنین به کتاب *نگهبانان: ماهواره‌های شناسایی استراتژیک* نوشته کورتیس یبلز (نوواتو، کالیفرنیا: پرزیدیو، ۱۹۸۷)، صـــفحات ۲۸۹-۲۷۹ مراجعه کنید. ماهواره‌های الکترونیکی، که مدار و تعداد ماهواره‌های مورد نیاز آنها از پیش تعیین شده است، مانند ماهواره‌های شناسایی تصویربرداری، به وظایف خاص جمع‌آوری اطلاعات

با وجود این، کار اطلاعات الکترونیکی فراتر از تشخیص وجود فرستنده‌های سیگنال الکترونیکی است. به عنوان مثال، با رهگیری سیگنال‌های رادار، می‌توان ویژگی‌های عملیاتی مختلف رادار، مانند پهنای پرتو (میزان مساحتی که رادار می‌تواند به طور همزمان اسکن کند) و حداکثر برد عملیاتی را تعیین کرد. به عنوان مثال، برد یک رادار که پالس‌های گسسته ساطع می‌کند را می‌توان از نرخ تکرار پالس (تعداد پالس‌های گسسته یا "بسته‌های "امواج رادیویی ساطع شده

الکترونیکی نیاز دارند سیستم‌های نظامی یک کشور دیگر، ماهواره‌های متعددی را که در ارتفاع پایین پرواز می‌کنند، ردیابی می‌کنند. برای کمک به تیم اطلاعات الکترونیکی در تعیین دقیق ویژگی‌های الکترونیکی سیستم نظامی، احتمالاً ماهواره در مدار بیضوی قرار می‌گیرد. در چنین مداری، با نزدیک شدن ماهواره به اوج (نقطه‌ای که در آن بیشترین فاصله را از زمین دارد)، به نظر می‌رسد که نسبتاً به آرامی بر فراز منطقه هدف پرواز می‌کند و به آن زمان بیشتری برای دریافت و ثبت سیگنال‌های مورد نیاز می‌دهد. همچنین می‌توان ماهواره‌ای را در مدار زمین‌ثابت قرار داد. یک ماهواره زمین‌ثابت در بالای خط استوا به دور زمین می‌چرخد و هر روز یک دایره کامل را طی می‌کند. از زمین، به نظر می‌رسد که بی‌حرکت بالای یک نقطه خاص روی خط استوا "آویزان "است. این امر به گیرنده‌های ماهواره اجازه می‌دهد تا به طور مداوم یک کشور را رصد کنند. عیب این روش، فاصله قابل توجه از فرستنده‌ها خواهد بود. سودمندی هر سیستم زمین‌ثابت به قدرت سیگنال دریافتی و حساسیت گیرنده‌های موجود در ماهواره بستگی دارد.

در ثانیه) تعیین کرد[101]. بنابراین، در طول جنگ جهانی دوم، اطلاعات علمی بریتانیا توانست بر اساس این واقعیت که این رادار با نرخ تکرار پالس 500 پالس در ثانیه کار می‌کرد، استنباط کند که حداکثر برد رادار دفاع هوایی فریا آلمان 300 کیلومتر است (1.(حادثه جدیدتری که ارزش اطلاعات الکترونیکی را نشان داد، در جریان حمله اسرائیل به لبنان در سال ۱۹۸۲ رخ داد. هنگامی که نیروهای اسرائیلی برای ریشه کن کردن نیروهای سازمان آزادیبخش فلسطین (PLO)که در آنجا فعالیت می‌کردند، به لبنان حمله کردند، فرماندهی عالی اسرائیل نگران احتمال حمله نیروهایش از جناحین توسط سربازان و تانک‌های سوری بود که به شدت در دره بقاع در غرب لبنان مستقر شده بودند. این نیروها توسط باتری‌های موشک‌های SAMمحافظت می‌شدند. اسرائیلی‌ها با استفاده از پهپادهای کندپرواز، توانستند پدافندهای سوریه را که فعال شده بودند، فریب دهند.آنها می‌توانستند پرونده را از منظر معنایش تحلیل کنند.

---

[101] ؛ محاسبه به شرح زیر است: موج رادیویی ساطع شده توسط رادار با سرعت نور - یعنی سیصد کیلومتر در ثانیه - حرکت می‌کند و بنابراین بین هر پالس مسافتی بین ۵۰۰/۳۰۰۰۰۰ تا ۶۰۰ کیلومتر را طی خواهد کرد. اگر موج به هدف برسد و قبل از انتشار پالس بعدی به رادار بازگردد، هدف نمی‌تواند بیش از سیصد کیلومتر از رادار فاصله داشته باشد. کتاب "پیشگوی جنگ "نوشته جونز

رادارهای کنترل آتش با دریافت سیگنال‌های ساطع شده از پهپادها فعال می‌شدند و بدین ترتیب این رادارها را در معرض دید هواپیما قرار می‌دادند. سپس امواج سوریه توسط گروه دوم پهپادها جمع‌آوری می‌شد. بر اساس این اطلاعات، اسرائیلی‌ها توانستند ویژگی‌های عملیاتی و مکان‌های رادارهای SAM را تعیین کنند. متعاقباً، نیروی هوایی اسرائیل توانست ظرف چند ساعت تمام باتری‌های موشک‌های ضدهوایی سوریه را منهدم کند و کنترل کامل بر حریم هوایی لبنان را برقرار کند و هرگونه امکان حمله نیروهای سوری که اکنون در معرض دید قرار گرفته بودند به نبرد در کنار سازمان آزادی‌بخش فلسطین را از بین ببرند[102].

اطلاعات اندازه‌گیری و نشانه‌گذاری (MASINT)

قابلیت‌های اطلاعات فنی تنها به قوانین فیزیک و نبوغ انسانی بستگی دارد. علاوه بر اطلاعات تصویری و اطلاعات سیگنالی، تکنیک‌های دیگری نیز برای جمع‌آوری اطلاعات استفاده شده‌اند که این تکنیک‌ها تحت عنوان اطلاعات اندازه‌گیری و نشانه‌گذاری

[102] ؛ داستان این فصل از کتاب «جاسوسان الکترونیکی» چاپ ۱۹۹۱، صفحات ۱۰۶-۱۰۷

(MASINT) گردآوری شده‌اند، اگرچه ویژگی‌های مشترک زیادی ندارند (جز اینکه نه اطلاعات تصویری هستند و نه اطلاعات سیگنالی)[103].

به عنوان مثال، حسگرهای ویژه‌ای برای کشف انفجارهای هسته‌ای و تعیین ویژگی‌های آن‌ها توسعه یافته‌اند. این شامل لرزه‌سنج‌هایی است که امواج شوک ناشی از آزمایش‌های هسته‌ای زیرزمینی را اندازه‌گیری می‌کنند؛ دستگاه‌هایی برای تشخیص فعالیت رادیواکتیو ناشی از شکافت مواد هسته‌ای در زیر زمین و بالای زمین؛ و حسگرهایی برای تشخیص فلاش ناشی از آزمایش‌های هسته‌ای

[103] ؛ طبق تعریف رسمی ایالات متحده، حسگرهای اطلاعاتی اندازه‌گیری و ردیابی «شامل موارد زیر می‌شوند، اما محدود به آنها نیستند:ادار، لیزر، مادون قرمز، آکوستیک، تابش هسته‌ای، سیستم‌های تشخیص تابش، اندازه‌گیری‌های طیف‌سنجی، سیستم‌های لرزه‌نگاری و سیستم‌های نمونه‌برداری گاز، مایع و جامد، داده‌های اطلاعاتی تولید می‌کنند که پس از جمع‌آوری، پردازش و تجزیه و تحلیل، امضاها (ویژگی‌های متمایز) منابع هدف ثابت و پویا را شناسایی، ردیابی، شناسایی یا توصیف می‌کنند. اطلاعات اندازه‌گیری و ضربه در سال ۱۹۸۶ رسماً به عنوان یک رشته اطلاعاتی (INT) طبقه‌بندی شد و در سال ۱۹۹۳ وزیر دفاع، دفتر مرکزی اندازه‌گیری و ضربه اطلاعات (CMO) را در آژانس اطلاعات دفاعی برای نظارت بر فعالیت‌های ملی و دفاعی تأسیس کرد. به فصل ۷، "اطلاعات اندازه‌گیری و ضربه "مراجعه کنید.ایالات متحده) org/irp/congress/1996_rpt/ic21/index.html.مرجع «در لینک(«

بالای زمین[104]. همچنین سونار نیز وجود دارد که از پدیده طبیعی دیگری، یعنی امواج صوتی، برای کشف زیردریایی‌ها در زیر سطح اقیانوس استفاده می‌کند؛ صرف نظر از موقعیت آن‌ها، سایر ویژگی‌های زیردریایی را می‌توان از تحلیل صداهایی که تولید می‌کند یا از آن منعکس می‌شود، کشف کرد[105].

بسترهای جمع‌آوری اطلاعات

[104] ؛ برای توصیف خوش‌بینانه‌ای از فناوری مورد استفاده در پایش لرزه‌ای آزمایش‌های هسته‌ای زیرزمینی، به این منابع مراجعه کنید: کنگره ایالات متحده، دفتر ارزیابی فناوری، تأیید لرزه‌ای معاهدات آزمایش هسته‌ای، OTAISC-361 (واشنگتن دی.سی.: دفتر مطبوعاتی دولت ایالات متحده، مه ۱۹۸۸). در مورد تشخیص از راه دور آزمایش‌های هسته‌ای روی زمین، به Peebles ، The* Guardians*، صفحات ۳۴۲-۳۳۱ مراجعه کنید.

[105] ؛ برای روایتی علمی-تخیلی از جمع‌آوری اطلاعات با استفاده از سونار، به کتاب *شکار اکتبر سرخ* نوشته تام کلنسی (آناپولیس: موسسه نیروی دریایی، ۱۹۸۴) مراجعه کنید. کشف روایت‌های غیرداستانی دشوار است، اما به مقاله جوئل ویت، «تحولات در جنگ ضد زیردریایی»، در مجله Scientific American ، فوریه ۱۹۸۱ مراجعه کنید. در مورد امکان شناسایی زیردریایی‌ها با روش‌های جدید، به مقاله تام استفانیک، «شناسایی غیرصوتی زیردریایی‌ها»، Scientific American، مارس ۱۹۸۸ مراجعه کنید.

در بحث‌های عمومی و تا حدودی در تحقیقات ما، تمرکز بر جمع‌آوری اطلاعات از طریق سیستم‌های نصب‌شده بر روی ماهواره‌ها قرار گرفته است. یکی از مزایای آشکار ماهواره‌ها، توانایی آن‌ها در پرواز بر فراز هر نقطه از جهان بدون رعایت مرزهای بین‌المللی است[106]. به همین دلیل، این بسترها اهمیت ویژه‌ای پیدا می‌کنند.

ماهواره‌ها در جمع‌آوری اطلاعات استخباراتی از کشورهایی که به دلیل انزوا و تدابیر امنیتی سخت‌گیرانه، دسترسی به آن‌ها از طرق

---

[106] ؛ به طور دقیق، هیچ توافق جهانی وجود ندارد که حقوق بین‌الملل، شناسایی ماهواره‌ای را مجاز بداند. به عنوان مثال، معاهده فضای بیرونی ۱۹۶۷ مستقیماً به موضوع اکتشافات فضایی نمی‌پردازد. معاهدات کنترل تسلیحات به «ابزارهای فنی ملی تأیید» اشاره دارند، اما این اصطلاحات را تعریف نمی‌کنند. به عنوان مثال، ماده نهم معاهده کاهش تسلیحات استراتژیک ۱۹۹۱ بین ایالات متحده و اتحاد جماهیر شوروی سابق، صرفاً «استفاده از ابزارهای فنی ملی تأیید به شیوه‌ای سازگار با اصول عموماً شناخته شده حقوق بین‌الملل» را بیان می‌کند. موضع ایالات متحده این بود که حاکمیت یک ملت به فضای بیرونی (یعنی فراتر از جو زمین) گسترش نمی‌یابد و بنابراین یک دولت همان آزادی را دارد که در دریاهای آزاد برای انجام فعالیت‌های شناسایی از فضای بیرونی دارد. در آغاز عصر فضا، دیدگاه اتحاد جماهیر شوروی این بود که شناسایی از فضا هرگز قانونی نبوده است، همانطور که شناسایی هوایی، که شامل پروازهای غیرمجاز بر فراز قلمرو یک کشور دیگر می‌شود، هرگز قانونی نبوده است. با این حال، از نظر عملی، استفاده عملی از فضا برای شناسایی توسط تعدادی از کشورها، از جمله اتحاد جماهیر شوروی سابق، مسئله قانونی بودن آن را تحت حقوق بین‌الملل به یک مسئله پیچیده تبدیل کرده است.حقوق بین الملل مورد بحث است.

دیگر ممکن نیســـت، اهمیت ویژه‌ای دارند. با این حال، اســـتفاده از ماهواره‌ها معایبی نیز به همراه دارد:

- هزینه بالا: ماهواره‌ها معمولاً گران‌تر از ســایر پلتفرم‌های شــناســایی هستند[107]

[107] :. تمامی کشورها هزینه واقعی سامانه‌های شناسایی فضایی را محرمانه نگه می‌دارند. با این حال، برآوردهای غیررســمی نشــان می‌دهد که ســاخت و پرتاب ماهواره‌ها بســیار گران اســت. به همین دلیل، رویکرد رایج، خرید تعداد کمی ماهواره با قابلیت‌های بالا و طراحی آن‌ها برای عمر طولانی در فضــا (شــاید هفت سال یا بیشتر) بوده است. این رویکرد، اگرچه در ظاهر مقرون‌به‌صرفه است، اما یک نقطه ضــعف عمده دارد: در صــورت بروز اتفاقی غیرمنتظره برای یک یا چند ماهواره، یا وقوع رویدادی در بخشـــی از جهان که به راحتی توســـط مدارهای سامانه‌های شناسایی فعلی پوشش داده نمی‌شود، ممکن است کشور مربوطه "کور" شـــود. اســـتراتژی جایگزین، که انعطاف‌پذیری و قابلیت بیشـــتری ارائه می‌دهد، ساخت ماهواره‌های بیشــتر اما ارزان‌تر با عمر فضــایی کوتاه‌تر اســت. در ســال ۱۹۹۶، مطالعه‌ای توســط کارگروه کمیته دائمی اطلاعات مجلس نمایندگان آمریکا نشــان داد که "انقلاب‌های مســتمر در توان پردازشــی، امکان اســتفاده از فضـــاپیماهای ســـبک‌تر، ارزان‌تر و در عین حال مولدتر در جمع‌آوری اطلاعات اســـتخباراتی را فراهم می‌کند. برای برخی کاربردها، 'ماهواره‌های کوچک' به صــورت 'خوشـــه‌ای' مســـتقر شـــده‌اند. این رویکرد می‌تواند با تجمیع و عملکرد توزیع‌شده، امکان تغییر مسیر سریع مجموعه‌ای ارزان‌قیمت یا جایگزینی انتخابی قطعات را فراهم آورد." (IC21: جامعه اطلاعاتی در قرن بیســت و یکم، واشــنگتن

- محدودیت در نزدیکی به هدف: ماهواره‌ها نمی‌توانند بیش از حد به اهداف خود نزدیک شوند (ماهواره‌های مدار پایین عموماً در ارتفاعات بیش از صد مایل باقی می‌مانند، در حالی که ماهواره‌های زمین‌ثابت باید در ارتفاع ۲۲۴۰۰ مایلی قرار گیرند).

- کارایی پایین در برخی مواقع: حتی اگر مدارهای آن‌ها برای افزایش اطلاعات جمع‌آوری‌شده محاسبه شده باشد، در بیشتر مواقع نسبتاً بی‌فایده هستند (به عنوان مثال، ماهواره‌ای که برای تصویربرداری از روسیه و خاورمیانه طراحی شده است، به دلیل قوانین فیزیکی مدارها، باید زمان زیادی را نیز به طور غیرمولد در نیمکره جنوبی بگذراند).

- مدارهای قابل پیش‌بینی: مدارهای آن‌ها قابل پیش‌بینی است، بنابراین دشمنان می‌توانند نیروها و تأسیسات حساس خود را هنگام قرار گرفتن در معرض نظارت ماهواره‌های شناسایی، هشدار دهند. تغییرات جزئی اما غیرمنتظره در مدار ماهواره‌ها را می‌توان با پرتاب

دی‌سی: دفتر چاپ دولتی، ۱۹۹۶). از آنجا که ماهواره‌های ارزان‌تر عموماً قابلیت‌های کمتری دارند، بخش عمده‌ای از هزینه به دلیل هزینه‌های پرتاب است. انتخاب استراتژی به اولویت‌های تعیین‌شده توسط دولت و پیشرفت‌های فنی سازندگان ماهواره بستگی دارد. (برای بحثی مختصر در این باره و مسائل مرتبط، به کتاب کوفیلا، "حرفه اطلاعات" مراجعه کنید).

موشـــک‌های کوچک حامل ماهواره‌ها انجام داد؛ تعداد و اندازه چنین مانورهایی به ظرفیت مخزن سوخت ماهواره بستگی دارد [108]

بنابراین، شـناسـایی فضـایی مزایای متعدد و اسـاسـی دارد، اما انواع دیگر پلتفرم‌های شـناسـایی همچنان توانایی ایفای نقش‌های مهمی را در جمع‌آوری اطلاعات فنی دارند. به عنوان مثال، هواپیماها می‌توانند در امتداد سواحل کشورهای متخاصم پرواز کرده و مأموریت‌های خود را انجام دهند؛ آن‌ها قادرند ارتباطاتی را که از فضـــا قابل رهگیری نیســـتند، رهگیری کنند و از مناطق نزدیک به مرزها عکس بگیرند، در حالی که خود از حریم هوایی آن کشورها دور می‌مانند. همچنین، آن‌ها می‌توانند ســـیگنال‌های رادارهای پدافند هوایی را رهگیری کنند که برخی از آن‌ها ممکن اســت برای شـــناســـایی مســیر دقیق هواپیماها فعال شـــوند. هواپیماهای بدون ســـرنشـــین (UAVs) نیز می‌توانند در مناطقی به کار گرفته شـــوند که پدافند هوایی دشـــمن خطر بالایی را برای خلبانان یا خدمه هواپیماهای ســـرنشـــین‌دار ایجاد می‌کند. هواپیماها مزایای متعددی دارند (در مقایســـه با معایب ماهواره‌های ذکر شـــده): آن‌ها ارزان‌تر از ماهواره‌ها هســـتند، می‌توانند بیشـــتر به

[108] ؛(برای اطلاعات بیشـــتر، به کتاب ویکتور ســـوووروف، "درون ارتش شـــوروی"، نیویورک: مک‌میلان، ۱۹۸۲ مراجعه کنید).

اهداف خود نزدیک شوند، قادرند بر فراز مناطق مورد نظر برای نظارت پرواز کنند، و مهم‌تر از همه، مسیر پرواز آن‌ها قابل پیش‌بینی نیست.

در جنگ خلیج فارس بین سال‌های ۱۹۹۱-۱۹۹۰، هواپیماهای شناسایی آواکس (AWACS - سیستم هشدار و کنترل هوابرد) و جی‌ستارز (J-STARS - سیستم مشترک نظارت راداری و حمله) که در پشت خطوط نیروهای آمریکایی پرواز می‌کردند، به فرماندهان آمریکایی اجازه دادند تا تقریباً در زمان واقعی، حرکت هوایی و نیروهای زمینی عراق را ردیابی و هدف قرار دهند. به طور خاص، هواپیمای جی‌ستارز اطلاعات مهمی درباره استقرار نیروهای زمینی عراق درست پیش از آغاز حمله نیروهای ائتلاف ارائه داد که به ائتلاف اطمینان بخشید مانور غافلگیرکننده آن‌ها در جناح راست تقریباً بدون مقاومت پیش خواهد رفت. در طول نبرد خفجی در ۲۹ ژانویه ۱۹۹۱، هواپیمای جی‌ستارز یک ستون نظامی عراقی را که به سمت شمال شهر کویت در حرکت بود، شناسایی کرد. این اطلاعات بلافاصله به فرماندهان ائتلاف منتقل شد و آن‌ها دستور حملات هوایی علیه نیروهای عراقی در حال پیشروی را صادر کردند. ظرف چند ساعت،

پنجاه و هشت دستگاه از شصت و یک دستگاه خودروی موجود در آن ستون منهدم شد [109]

عملیات ناتو در کوزوو در سال ۱۹۹۹ (عملیات نیروی متحد) شاهد استفاده بی‌سابقه‌ای از هواپیماهای بدون سرنشین برای اهداف شناسایی بود که "نیاز به اعزام هواپیماهای سرنشین‌دار به حریم هوایی دشمن را کاهش داد." مقامات ارشد آمریکایی بر انعطاف‌پذیری هواپیماهای بدون سرنشین با این اظهارات تأکید کردند: "ما تعداد زیادی هواپیمای بدون سرنشین را از دست دادیم، اما توانایی آن‌ها در مانور در مناطق دشمن، اطلاعات شناسایی را فراهم کرد که بدون به خطر انداختن خدمه هواپیماهایمان، نمی‌توانستیم به دست آوریم. همچنین، از دست دادن هواپیماهای بدون سرنشین یک ریسک حساب‌شده است؛ آن‌ها بر اساس توازن بین احتمال از دست دادن و سودمندی استفاده از آن‌ها طراحی شده‌اند." [110]

---

[109] ؛(وزارت دفاع آمریکا، گزارش جنگ خلیج فارس).

[110] ؛(نقل قول از بیانیه مشترک وزیر دفاع آمریکا، ویلیام کوهن، و ژنرال هنری شلتون، رئیس ستاد مشترک ارتش، در برابر کمیته نیروهای مسلح سنای آمریکا در ۱۴ اکتبر ۱۹۹۹، موجود در: www.fas.org/man/dod/101-ops/docs99/b10141999_bt478-99.htm).

پلتفرم‌های دیگری به جز هواپیماها نیز می‌توانند برای جمع‌آوری اطلاعات استخباراتی مفید باشند. ون‌ها و کامیون‌ها می‌توانند به طور مخفیانه ارتباطات و سیگنال‌ها را در نزدیکی مکان‌های نظامی، دیپلماتیک یا علمی رصد کنند. کشتی‌ها می‌توانند سیگنال‌های رادیویی را از فراسوی سواحل دشمن رهگیری کنند. رادارها، چه دریایی و چه زمینی، اگر به اندازه کافی نزدیک به محل پرتاب موشک‌های آزمایشی یا محل ورود کلاهک‌ها به جو قرار گیرند، می‌توانند مسیر موشک‌های آزمایش‌شده را ردیابی کرده و برخی از ویژگی‌های آن‌ها را مشخص کنند. همچنین، ایستگاه‌های راداری زمینی می‌توانند سیگنال‌های رادیویی متنوعی را رهگیری کنند، از جمله سیگنال‌هایی که ممکن است به طور ناخواسته از سطح ماه بازتاب یابند[111]. در نهایت، کوچک‌سازی دستگاه‌های استراق سمع و سایر حسگرها به سازمان‌های اطلاعاتی اجازه می‌دهد تا زمانی که

[111] ؛برای فهرستی از کارهایی که می‌توان تحت پوشش یک کامیون معمولی انجام داد، به کتاب دزموند، پاول، اطلاعات سیگنال شوروی مراجعه کنید: سامانه‌ها و عملیات‌های وسایل نقلیه اطلاعاتی و امنیت ملی (ژانویه ۱۹۸۹)، صفحات ۲۷-۵. در یک جنبه غیرمعمول‌تر، برای شرح پروژه Moonbounce ایالات متحده، که سیگنال‌های رادار شوروی منعکس شده از یک ماهواره را جمع‌آوری می‌کرد، به کتاب *تاریخچه جنگ الکترونیک آمریکا: سال‌های رنسانس*، نوشته آلفرد پرایس، ۱۹۶۴-۱۹۴۶) الکساندریا، ویرجینیا: انتشارات Crows Old of Association، ۱۹۸۹(، صفحات ۱۶۱-۸۹ مراجعه کنید.

یک عامل انسانی بتواند به اندازه کافی به هدف نزدیک شود و حسگر را مخفیانه نصب کند، اطلاعات استخباراتی جمع‌آوری کنند[112]. به طور خلاصه، پلتفرم‌های جمع‌آوری اطلاعات استخباراتی می‌توانند از عادی تا عجیب متغیر باشند. برای یک جامعه اطلاعاتی مدرن و پیشرفته از نظر فنی، تصمیم‌گیری در مورد پلتفرم‌های مورد استفاده نتیجه دو ارزیابی است: اولاً، کدام پلتفرم‌ها می‌توانند اطلاعات استخباراتی مورد نظر را به بهترین شکل جمع‌آوری کنند؟ و ثانیاً، هزینه تخمینی و خطرات ناشی از استفاده از پلتفرم‌های خاص چیست؟

مقایسه اطلاعات انسانی و فنی

[112] ؛کوچک‌سازی همچنین به وزارت دفاع ایالات متحده اجازه می‌دهد تا پهپادهای شناسایی به اندازه کف دست و ربات‌های اکتشافی کودک‌مانند را برای استفاده در میدان نبرد توسعه دهد. این هواپیماهای جاسوسی کوچک، که "وسایل نقلیه هوایی ریز (MAV) "نامیده می‌شوند، و ربات‌ها به واحدهای رزمی کوچک این توانایی را می‌دهند که محیط‌های اطراف خود را کاوش کنند. (مایکل ای. دورنهن، "پهپادها می‌توانند به ابزار نظامی جدید تبدیل شوند"، ۱۹۹۸، صفحات ۴۸-۴۲؛ کوین کال، "ربات("ربات‌های شناسایی اسکاتس ممکن است در سال ۲۰۰۰ برای نیروی دریایی ایالات متحده اطلاعات جمع‌آوری کنند.

سال‌هاست که در ایالات متحده بحثی مستمر درباره اهمیت نسبی اطلاعات انسانی (HUMINT) و اطلاعات فنی (TECHINT) در جریان است. از یک سو، برخی معتقدند که اطلاعات فنی شکل اصلی اطلاعات است و با پیشرفت فناوری، اهمیت نسبی آن افزایش خواهد یافت. از سوی دیگر، عده‌ای بر این باورند که اطلاعات فنی بیش از حد بر حساب جاسوسی سنتی اهمیت یافته و لازم است تعادلی دوباره بین این دو برقرار شود. شاید بزرگترین سهم در این بحث داغ، دفاع پرشور دریاسالار استنسفیلد ترنر، مدیر سیا در دوران ریاست‌جمهوری کارتر، از اولویت اطلاعات فنی باشد: "اکنون ما سامانه‌های فنی داریم که از ماهواره‌هایی که در فضا کل کره زمین را دور می‌زنند، تا هواپیماهای بدون سرنشینی که آزادانه در آسمان پرواز می‌کنند، و حسگرهایی به قدری کوچک که می‌توانیم آن‌ها را در هر نقطه‌ای از جهان، حتی بیش از یک حسگر، نصب کنیم. ما می‌توانیم از فواصل بسیار دور تصاویر دقیقی بگیریم، منابع حرارت را با دستگاه‌های فروسرخ کشف کنیم، فلزات را با ردیاب‌های مغناطیسی به دقت شناسایی کنیم، حرکت، هرچند ساده، را از اجسام ساکن با استفاده از رادار داپلر تشخیص دهیم، از رادار برای کشف اجسام پنهان یا پوشیده در تاریکی استفاده کنیم، به انواع سیگنال‌ها از صدای انسان تا امواج راداری گوش دهیم، تشعشعات هسته‌ای را با دستگاه گایگر کشف

کنیم، و انفجارهای زیرزمینی را از فواصل دور با لرزه‌نگارها حس کنیم. بیشتر فعالیت‌هایی که می‌خواهیم نظارت کنیم، الگوهای متعددی از سیگنال‌ها را منتشر می‌کنند؛ تانک‌ها در نبرد را می‌توان از حرارت موتورهایشان، یا از جاذبه مغناطیسی زره‌هایشان، یا از تصاویرشان کشف کرد. ایستگاه‌های تسلیحات هسته‌ای تشعشعاتی منتشر می‌کنند، شکل فیزیکی خاصی دارند، و نوع خاصی از تدارکات را دریافت می‌کنند. به هر حال، به زودی قادر خواهیم بود بیشتر فعالیت‌ها را در سطح زمین، شب یا روز، در هوای خوب یا بد، ردیابی کنیم."[113]

---

[113] ؛استنسفیلد ترنر، «رازداری و دموکراسی: سازمان سیا در حال گذار» (بوستون: هاوتون میفلین، ۱۹۸۵؛ نیویورک: هاربر و رو، ۱۹۸۶؛ بوستون: هاوتون، ۱۹۸۵). پس از جنگ سرد، ترنر استدلال کرد که «واشنگتن می‌تواند به راحتی سیستمی ایجاد کند که هرگونه فعالیت قابل توجهی را در سطح زمین، شب یا روز، زیر ابرها یا پوشش جنگلی، با فرکانسی که فرار عمدی را دشوار می‌کند، شناسایی کند. [هزینه ۵ میلیارد دلار برای به دست آوردن و ۱ میلیارد دلار در سال برای عملیاتی کردن [4] یک معامله خواهد بود.]» به گفته مدیر سابق اطلاعات مرکزی، نقشی برای جمع‌آوری اطلاعات انسانی در دوران پس از جنگ سرد وجود دارد، اما به طور کلی، «نظم جهانی جدید سیستم‌های تکنولوژیکی تولید خواهد کرد که شمشیر، پیشگام گسترده جمع‌آوری اطلاعات، و جمع‌آوری اطلاعات انسانی شمشیری خواهد بود که به طور عاقلانه برای الزامات بسیار خاص به کار گرفته می‌شود.» ترنر، اطلاعات برای نظم جهانی، صفحات ۱۵۹-۱۵۱ (جدید: امور خارجه، ۷۰، شماره ۴، پاییز ۱۹۹۱)

مهارت فنی فوق‌العاده‌ای که این نوع دستگاه‌های فنی به نمایش می‌گذارند، واقعاً چشمگیر است. با این حال، شیفتگی به فناوری می‌تواند به راحتی منجر به اغراق در توانایی‌های اطلاعات فنی و کم‌اهمیت جلوه دادن اطلاعات انسانی شود. به ویژه در ایالات متحده، این دیدگاه در اواسط تا اواخر دهه هفتاد رایج بود، تا اینکه اطلاعات انسانی در آن زمان دوباره ارزش خود را بازیافت. نقل قول بالا قدرت اطلاعات انسانی را توصیف می‌کند. اطلاعات فنی برای ایالات متحده در جمع‌آوری بخش اصلی اطلاعات مربوط به اتحاد جماهیر شوروی ضروری بود. باید توجه داشت که در بسیاری از کشورهای دیگر، بخش بزرگی از این اطلاعات در دسترس عموم قرار دارد؛ به عنوان مثال، اطلاعات مربوط به حجم و استقرار کلی نیروهای مسلح و توسعه سامانه‌های تسلیحاتی جدید در اسناد رسمی (به ویژه اسناد بودجه و پارلمان) موجود است. اما جمع‌آوری چنین اطلاعاتی درباره اتحاد جماهیر شوروی، به دلیل پنهان‌کاری شدید رژیم در مورد مسائل نظامی به طور خاص و مسائل امنیت ملی به طور کلی، نیازمند ابزارهای اطلاعاتی فنی دقیق بود. بیشتر تلاش‌های جمع‌آوری

اطلاعات که طی سال‌ها توسعه یافت، به منظور مقابله با همین پنهان‌کاری اختصاص داده شده بود.

اما از زمان فروپاشی اتحاد جماهیر شوروی و پیمان ورشو، تعداد اهداف دشوار به طور چشمگیری کاهش یافته است. با این حال، اتکا به جمع‌آوری اطلاعات استخباراتی از طریق ابزارهای فنی همچنان بسیار رایج است. قطعاً هنوز جوامع بسته‌ای وجود دارند که برخی از آن‌ها – مانند کره شمالی – از اهمیت اطلاعاتی بالایی برخوردارند، و در چنین مواردی، اتکا به اطلاعات فنی اغلب ادامه می‌یابد. مورد مهم‌تر، جمهوری خلق چین است که همچنان کشوری است که جاسوسی در آن دشوار است، اما در زمینه سفر و ارتباطات بازتر از اتحاد جماهیر شوروی سابق است. در مورد بسیاری از انواع اطلاعاتی که کشورها آن‌ها را محرمانه نگه می‌دارند – مانند نیات و برنامه‌های سیاسی و نظامی – اطلاعات انسانی همواره مورد نیاز بوده و خواهد بود. حامیان اطلاعات انسانی تأکید می‌کنند که با وجود پیشرفت مداوم فناوری، جاسوسی سنتی برای آگاهی از نیات، فعالیت‌های سیاسی و مفاهیم استراتژیک رهبری دشمن، اساسی باقی می‌ماند. به عنوان مثال، اطلاعات فنی به وضوح تجمع نیروهای عراقی در مرز کویت را در ژوئیه ۱۹۹۰ آشکار کرد، اما این اطلاعات نیات صدام

حسین را فاش نکرد: آیا قصد او حمله به کویت بود، یا می‌خواست با ارعاب، امتیازات و امتیازات مالی به دست آورد؟ در مقابل، یک عامل در موقعیتی حساس در ستاد کل ارتش لهستان توانست گزارشی درباره تصمیم محرمانه دولت لهستان در اواخر سال ۱۹۸۱ برای اعمال حکومت نظامی به منظور سرکوب جنبش مستقل کارگری همبستگی تهیه کند[114]. به طور خلاصه: درک نیات دشمن، استراتژی و برداشت‌های او از موقعیت‌هایی که در آن قرار می‌گیرد، اغلب مهم‌ترین اطلاعات استخباراتی است که می‌توان به دست آورد. رهگیری ارتباطات سطح بالای بین رهبری سیاسی و نظامی دشمن نیز می‌تواند اطلاعات استخباراتی از این نوع ارائه دهد، که مشابه حالتی است که شما یک عامل انسانی با دسترسی عالی به رهبران دشمن داشته باشید. اما دستیابی به این اطلاعات از طریق اطلاعات ارتباطی دشوارتر از آن چیزی است که بیانیه ترنر (فرضیه مرز یا فرضیه ترنر درباره مرزهای آمریکا) نشان می‌دهد. این استدلال که

---

[114] ؛سرهنگ ارتش لهستان، ریشارد جی. کوکلینسکی، در طول دهه فعالیتش برای اطلاعات ایالات متحده، هزاران صفحه اسناد طبقه‌بندی‌شده، از جمله نقشه‌های جنگی شوروی برای جنگ در اروپا را ارائه داد. برای شرح فعالیت‌های جاسوسی سرهنگ کوکلینسکی، به بنجامین وایزر، «افسر لهستانی که دریچه‌ای به نقشه‌های جنگی شوروی در آمریکا بود»، واشنگتن پست، ۲۷ سپتامبر ۱۹۹۲، و مجله واشنگتن پست مراجعه کنید.در ۱۳ دسامبر ۱۹۹۲.

توسط مورخ فردریک جکسون ترنر در سال ۱۸۹۳ ارائه شد، بیان می‌کند که دموکراسی آمریکا به دلیل مرزهای آمریکا شکل گرفته است. او بر فرآیند – خط مرزی متحرک – و تأثیر آن بر پیشگامانی که این فرآیند را طی می‌کنند، تأکید کرد. همچنین بر نتایج، به ویژه اینکه دموکراسی آمریکا نتیجه اولیه در کنار برابری، بی‌توجهی به فرهنگ و خشونت بود، تأکید داشت. "دموکراسی آمریکا از رویای عدم وجود هیچ نظری متولد شد و نه در سوزان کنستانت به ویرجینیا، و نه در می فلاور به پلیموث، اجرا نشد. بلکه از جنگل آمریکا بیرون آمد و هر بار که با مرز جدیدی تماس پیدا می‌کرد، قدرت جدیدی به دست می‌آورد."

اولاً: انتظار می‌رود دشمن بیشتر ارتباطات حساس خود را رمزگذاری کند. در این زمینه، باید توجه داشت که جمع‌آوری اطلاعات استخباراتی می‌تواند مفید و حتی حیاتی باشد، زیرا از طریق آن می‌توان به سوابق رمزها و سایر اطلاعاتی دست یافت که رمزگشایی پیام‌ها را تسهیل می‌کند. به عنوان مثال: در اوایل دهه ۱۹۳۰، اطلاعات فرانسه از یک عامل در آلمان، اطلاعات مهمی درباره دستگاه رمزگذاری آلمانی به نام "انیگما" به دست آورد، از جمله دستورالعمل‌های استفاده از آن، برخی جزئیات درباره ساختار آن، و برخی کلیدهایی که تنظیمات

عملیاتی روزانه دستگاه را مشخص می‌کردند. این اطلاعات توسط فرانسوی‌ها به سازمان اطلاعات لهستان منتقل شد که به پیشرفت بزرگی در تحلیل رمزها دست یافت و این پیشرفت اساس موفقیت نهایی بریتانیا در طول جنگ جهانی دوم بود[115].

ثانیاً: می‌توان بر بیشتر قابلیت‌های اطلاعات ارتباطی با توقف پخش پیام‌ها غلبه کرد، به این معنی که پیام‌ها از طریق سیم‌ها منتقل شوند. رهگیری پیام‌های خطوط زمینی نیازمند دسترسی به سیم‌ها است که اغلب دشوار است. همچنین – همانطور که قبلاً اشاره شد – سیم‌ها با فیبرهای نوری جایگزین می‌شوند که از نور منسجم (پرتوهای لیزر) برای انتقال پیام‌ها استفاده می‌کنند و کمتر در معرض نصب مدارهای شنود قرار می‌گیرند. علاوه بر این، بیشتر انواع جمع‌آوری اطلاعات فنی، از جمله اطلاعات ارتباطی، از احتمال "شرمساری از ثروتمندان" رنج می‌برند، به دلیل گسترش جهانی سامانه‌های جمع‌آوری اطلاعات

---

[115] ؛جوزف گارلینسکی، *جنگ انیگما*، نیویورک: شوگر پانر (۱۹۷۹)، صفحه ۱۶. این مورخ، هانس تئو اشمیت، مأمور آلمانی، را به عنوان «تأثیرگذارترین جاسوس جنگ جهانی دوم» توصیف کرد. *کان در باب کدها: اسرار علم جدید رمزنگاری* (نیویورک: مک‌میلان، ۱۹۸۳)، صفحات ۸۸-۷۶.

فنی. باید راهی وجود داشته باشد تا مسئولان جمع‌آوری اطلاعات فنی بدانند کدام اهداف را باید رصد کنند و کدام اهداف را نادیده بگیرند[116]. در حالی که ممکن است درست باشد که "به زودی می‌توانیم تقریباً هر نقطه‌ای از سطح زمین را اسکن کنیم"، اما هیچ کس نمی‌تواند همه آن‌ها را همزمان اسکن کند. حتی اگر کسی بتواند این کار را انجام دهد، هیچ کس قادر به پردازش و تحلیل تمام داده‌هایی که حسگرها می‌توانند جمع‌آوری کنند، نیست. بنابراین، وجود قابلیت‌های فنی مانند آنچه ترنر توصیف کرد، به این معنی نیست که هیچ چیز مهمی نمی‌تواند از نظارت دستگاه‌های اطلاعاتی مجهز به آخرین فناوری‌ها در امان بماند. همانطور که از بازرسی‌های پس از جنگ خلیج فارس مشخص شد، جمع‌آوری اطلاعات فنی

[116] ؛طلاعات انسانی نیز ممکن است در این امر نقش داشته باشد. به عنوان مثال، طبق گزارش‌های خبری، سرهنگ کوکلینسکی اطلاعاتی در مورد «اهداف شوروی که از طریق ماهواره قابل مشاهده بودند؛ آیا آنها واقعاً یک فریب بودند؟ و کدام یک واقعی بودند؟» ارائه داد. علاوه بر این، گزارش‌های کوکلینسکی به اطلاعات ایالات متحده این امکان را داد تا برنامه نظامی شوروی را برای ساخت شبکه‌ای از پناهگاه‌های فرماندهی و کنترل پنهان که شوروی و متحدانش قصد داشتند در صورت جنگ در اروپا از آنها استفاده کنند، ردیابی کنند. وایزر،این افسر لهستانی دریچه‌ای برای ایالات متحده به سوی نقشه‌های جنگی شوروی بود

آمریکا برای ردیابی تلاش‌های عراق برای ساخت سلاح هسته‌ای[117] کافی نبود.

مسئله این نیست که آیا جمع‌آوری اطلاعات استخباراتی فنی ارزشمند است یا خیر؛ قطعاً ارزشمند است. اما مسئله این است که زمین مکانی وسیع، متنوع و در برخی نقاط شلوغ است. بنابراین، موفقیت تا حد زیادی به امکان قرار دادن حسگرها در مکان مناسب بستگی دارد. جمع‌آوری اطلاعات انسانی می‌تواند اولین نشانه اساسی را ارائه دهد که چیز مهمی در جایی در حال وقوع است یا اتفاق خواهد افتاد، و این امر هدف‌گیری سامانه‌های فنی در آن منطقه را ممکن می‌سازد. بدون این نوع شواهد، سامانه‌ها کارایی کمتری خواهند داشت و ممکن است تحولات مهم را برای مدت طولانی یا به طور کامل از دست بدهند. منبع اطلاعات انسانی می‌تواند سرنخ‌های ضروری را برای تفسیر داده‌های خامی که از طریق سامانه‌های جمع‌آوری اطلاعات استخباراتی فنی جمع‌آوری

---

[117] ؛به مقالات جفری اسمیت مراجعه کنید: «تلاش‌های مخفیانه عراق: درس‌هایی برای جهان»، واشنگتن پست، ۱۱ آگوست ۱۹۹۱؛ جفری اسمیت، «قدرت‌های هسته‌ای عراق که ایالات متحده آنها را دست کم گرفت»، واشنگتن پست، ۱۳ نوامبر ۱۹۹۱؛ «رویای صدام برای سلاح‌های هسته‌ای: کابوسی که دوام آورد»، واشنگتن پست، ۱۳ نوامبر ۱۹۹۱.

شده‌اند، ارائه دهد. به عنوان مثال، در صورت وجود یک تصویر خوب از یک ساختمان، تحلیلگر اطلاعاتی ممکن است نتواند عملکرد آن را تشخیص دهد. با این حال، یک منبع انسانی که آن را به خوبی می‌شناسد، شاید بتواند وجود جزئیات خاصی را تفسیر کند، حتی اگر به وضوح قابل مشاهده نباشند، که نشان می‌دهد ساختمان برای هدف خاصی مرتبط با یک برنامه نظامی معین طراحی شده است. بدون منبع انسانی، شاید این جزئیات مورد توجه قرار نگیرد و اهمیت آن درک نشود، اما به محض شناسایی این "اثر انگشت"، می‌توان تصاویر ساختمان‌های مشابه را برای یافتن همان جزئیات بررسی کرد.

اما در تعدادی از موارد، شناسایی یا ردیابی اهداف احتمالی دشوار است، اگر بتوان آن‌ها را شناسایی کرد. این امر گاهی به این دلیل است که اهداف کوچک‌تر، متحرک‌تر شده‌اند یا در زیر زمین پنهان شده‌اند. در موارد دیگر، به این دلیل است که فعالیت‌های اطلاعاتی مهم (مانند تحقیقات تسلیحات شیمیایی و بیولوژیکی) به راحتی از وظایف مشروع در این نوع کارها (مانند تولید دارو و حشره‌کش) قابل تشخیص نیستند. همچنین، گاهی اوقات می‌توان تمام شواهد اصلی را از بین برد. پس از جنگ خلیج فارس، سازمان ملل متحد تیمی را به عراق فرستاد تا تأسیسات هسته‌ای این کشور را جستجو و برچیند. این تیم کشف کرد که عراق با دقت بسیاری از ساختمان‌ها را در

برنامه خود به گونه‌ای ساخته بود تا از شناسایی توسط ماهواره‌ها و سایر سامانه‌های جمع‌آوری اطلاعات فنی جلوگیری کند. برخی از آن‌ها برای جلوگیری از انتشار تشعشعات ساخته شده بودند، در حالی که برخی دیگر به گونه‌ای طراحی شده بودند که تا حد امکان جلب توجه نکنند و با تقلید از ظاهر تأسیسات صنعتی مشروع، خود را پنهان سازند. به نظر می‌رسد این تأسیسات تنها پس از ارائه اطلاعاتی توسط یک مهندس عراقی که پس از جنگ فرار کرده بود، به عنوان بخشی از تلاش صدام حسین برای دستیابی به بمب هسته‌ای شناسایی شدند.

در مورد برخی الگوهای اطلاعاتی، مشکل هدف‌گیری صحیح سامانه‌های جمع‌آوری اطلاعات فنی ممکن است عملاً غیرقابل حل باشد. به عنوان مثال: به احتمال زیاد، اطلاعات انسانی برای جمع‌آوری اطلاعات حساس درباره اهداف ثابت یا شبکه‌های ارتباطی که در معرض ابزارهای جمع‌آوری اطلاعات فنی قرار دارند، ضروری است – یعنی هرچه تعداد مکان‌های شناخته‌شده‌ای که یک گروه می‌تواند به آن‌ها رفت و آمد کند کمتر باشد، هدف‌گیری آن مکان‌ها با حسگرهای فنی دشوارتر می‌شود. جمع‌آوری اطلاعات استخباراتی علیه این گروه‌ها اغلب به توانایی نفوذ به گروه یا جذب افراد آن به عنوان خبرچین بستگی دارد. اگر چنین گروه‌هایی به اهداف اطلاعاتی مهمی

تبدیل شوند، جمع‌آوری اطلاعات انسانی اهمیت بیشتری پیدا می‌کند. در این صورت، اطلاعات انسانی و فنی می‌توانند نقش‌های مکمل ایفا کنند و هر یک به تنهایی می‌توانند انواع متمایزی از اطلاعات را ارائه دهند. البته، فروپاشی "پرده آهنین" دلیل اصلی توسعه یک سیستم پیچیده جمع‌آوری اطلاعات فنی توسط ایالات متحده را از بین برد، اما ادامه تعهد به زرادخانه‌های سایر کشورها، به ویژه جوامع بسته و برنامه‌های فعال توسعه سلاح‌های کشتار جمعی، و همچنین افزایش تقاضا از سوی ارتش آمریکا برای جمع‌آوری اطلاعات فنی به منظور پشتیبانی از عملیات خود، نشان می‌دهد که تغییر عمده‌ای در کار جمع‌آوری اطلاعات فنی رخ نخواهد داد. از سوی دیگر، الزامات اطلاعاتی درباره کشورهای جدید، بازیگران سیاسی جدید، و نگرانی‌های جدید در حال گسترش است، و شاید اطلاعات انسانی بهترین راه برای مقابله با آن‌ها باشد، در حالی که ترکیب صحیح اطلاعات انسانی و فنی – همانند گذشته – مورد بحث خواهد بود، شکی نیست که یک قدرت بزرگ مانند ایالات متحده به استفاده از هر دو نوع ادامه خواهد داد. اطلاعات انسانی و فنی جایگاه برجسته‌ای در بحث‌های مربوط به اطلاعات استراتژیک – یعنی اطلاعاتی که برای تصمیم‌گیرندگان در سطح کشور هدایت می‌شود – به دست آورده‌اند. همچنین توجه به این نکته مهم است که پیشرفت‌ها در ارتباطات

تلفنی و قابلیت‌های رایانه‌ای، امکان رساندن اطلاعات از طریق سامانه‌های اطلاعات فنی – از جمله اطلاعاتی که برای اهداف در سطح ملی آماده شده‌اند – را به فرماندهان در میدان نبرد در زمان واقعی و با سرعت کافی برای بهره‌برداری تاکتیکی فراهم کرده است. این پیشرفت هنوز در مراحل اولیه خود است، اما نویدبخش بوده و شاید به یک کاربرد مهم برای سامانه‌های اطلاعات فنی تبدیل شود[118].

[118] ؛برای بحث در مورد نقش اطلاعات در «انقلاب در امور نظامی»، به کتاب جیمز فیتزسیموند، «اطلاعات و انقلاب در امور نظامی»، در «اطلاعات آمریکا در یک دوراهی: دستور کار اصلاحات»، جادسون، ارنست آر. می، و گری اشمیت، واشنگتن دی سی: براسیز [ایالات متحده]، (۱۹۹۵)، صفحات ۲۸۷-۲۶۵ مراجعه کنید. فیتزسیموند از جمله وظایفی که باید برای استفاده کامل از فناوری برای اهداف تاکتیکی انجام شود، موارد زیر را ذکر می‌کند: «پوشش جهانی - شناسایی یک منطقه وسیع، همه‌جانبه، روز و شب از اهداف ثابت و متحرک در ساحل، دریا، هوا و فضا؛ هدف‌گیری مداوم در زمان واقعی یا تقریباً زمان واقعی، از جمله ارزیابی تلفات نبرد، و پیوند همزمان اطلاعات هدف‌گیری با کلاهک‌ها، از جمله آنهایی که در هوا هستند«.

جمع‌آوری اطلاعات از منابع باز

موضـوع جمع‌آوری اطلاعات اسـتخباراتی بدون اشـاره به جمع‌آوری اطلاعات از منابع باز – یعنی: روزنامه‌ها، کتاب‌ها، پخش رادیویی و تلویزیونی، اینترنت، و هر منبع عمومی اطلاعات – کامل نخواهد بود. اهمیت منابع باز در فرآیند جمع‌آوری اطلاعات استخباراتی یک مسئله بحث‌برانگیز اسـت و در نهایت به سـؤالات اسـاسـی درباره ماهیت اطلاعات گره می‌خورد. یکی از دیدگاه‌ها، که توسط شرمن کنت تجسم یافته، بیان می‌کند که بخش عمده‌ای از "اطلاعات مثبت خارجی سـطح بالا باید از طریق نظارت و تحقیق باز، گسـترده و جدی انجام شود.[119]" از سوی دیگر، دیدگاه سنتی این است که از آنجا که منابع باز ممکن است زمینه و پیش‌زمینه‌ای مهم برای حقایق اساسی ارائه دهند، اطلاعاتی مانند نیات مشخص دشمن باید عمدتاً – اگر نگوییم تنها – از منابع غیرعلنی از طریق جاسوسی یا اطلاعات فنی به دست آید. فصـل هفتم به طور کامل به این موضـوع می‌پردازد، اما در این مرحله، تمرکز بر کاربردهای متنوع منابع باز خواهد بود. به عنوان مثال:

---

[119] ؛شرمن کنت، اطلاعات استراتژیک برای سیاست جهانی آمریکا (پرینستون، نیوجرسی: انتشارات دانشگاه پرینستون، چاپ ۱۹۴۹، ۱۹۶۶)، صفحات ۴-۳. کنت، از اعضای باسابقه دفتر خدمات استراتژیک(OSS) ، سازمان اطلاعاتی ایالات متحده در دوران جنگ جهانی دوم، یک نظریه عجیب آمریکایی در مورد اطلاعات پس از جنگ ارائه دادجهان دوم به طور مستقیم

وظیفه معمول افسران اطلاعات نظامی، تهیه خلاصه‌ای جامع از اطلاعات مربوط به کشورهایی بود که ممکن است در آینده عملیات نظامی علیه آن‌ها انجام شود. چنین خلاصه‌ای معمولاً شامل تمام اطلاعاتی است که نظامیان ممکن است از آن بهره‌مند شوند، و اطلاعاتی مربوط به جغرافیای کشور، شبکه‌های ارتباطی و حمل و نقل آن، تأسیسات نظامی و اقتصادی اصلی، و غیره. جزئیات کافی باید گنجانده شود تا به برنامه‌ریز اجازه دهد طیف وسیعی از تصمیمات، از جمله تعیین سرعتی که نیروها و تدارکات باید از نقطه الف به نقطه ب حرکت کنند. به استثنای بیشتر کشورهای بسیار محرمانه (مانند اتحاد جماهیر شوروی سابق که در سال ۱۹۸۸ اعتراف کرد برخی نقشه‌ها را به عنوان یک اقدام امنیتی جعل کرده است)[120]، بسیاری از این اطلاعات در منابع باز موجود خواهد بود: نقشه‌های جاده‌ها و راه‌آهن و زمان‌بندی‌ها، مقالات روزنامه‌ها و مجلات، گزارش‌های دولتی و آماری، و حتی راهنماهای سفر قدیمی. اما جمع‌آوری و فهرست‌بندی آن‌ها مسئله دیگری است، زیرا شامل حجم زیادی از اطلاعات می‌شود. اطلاعات مورد نیاز برای هر کشور مرتبط، به طور کامل در دسترس نیست. اگر نیروهای آمریکایی در سال ۱۹۸۳

[120] ؛۱ .کتاب «اجازه انتشار» نوشته زکین، ایزوتا، ۳ سپتامبر ۱۹۸۸.

به گرانادا حمله کردند – همانطور که در فصل بعدی بحث خواهیم کرد – بدون اینکه نقشه‌ها و سایر اطلاعات مربوط به جزیره را داشته باشند، این به دلیل دشواری در جمع‌آوری اطلاعات نبود، بلکه به دلیل عدم تخصیص منابع کافی به چیزی بود که برای بسیاری یک جزیره کوچک و دورافتاده به نظر می‌رسید. به طور مشابه، تعداد زیادی از منابع آماری در سراسر جهان داده‌های اقتصادی را منتشر می‌کنند، اما تعیین آنچه باید جمع‌آوری شود، نیازمند درکی از الزامات اطلاعاتی است. داده‌های اقتصادی ممکن است برای پشتیبانی از فرآیند تدوین سیاست در مورد تجارت بین‌المللی یا اعمال تحریم‌ها، و برای مقابله با تأثیرات نارسایی توافق‌نامه‌های کارتل‌های بین‌المللی – انجمنی از تولیدکنندگان یا عرضه‌کنندگان با هدف حفظ قیمت‌ها در سطح بالا و محدود کردن رقابت – (مانند سازمان کشورهای صادرکننده نفت) مورد نیاز باشد. به همین ترتیب، انواع دیگر داده‌های اقتصادی، مانند آن‌هایی که از نظارت بر جریان‌های نقدی به دست می‌آیند، می‌توانند بر تجارت بین‌المللی مواد مخدر پرتو افکنند. در نهایت: اطلاعات اقتصادی ممکن است برای پشتیبانی از تحلیل‌های سیاسی و نظامی مورد نیاز باشد. به عنوان مثال، در طول جنگ جهانی دوم، اقتصاددانان دفتر خدمات استراتژیک (OSS) – که برای ستاد نیروی هوایی در اروپا کار می‌کردند – مجموعه‌ای بزرگی از داده‌های

غیرمحرمانه را برای کمک به برنامه‌ریزی یک کمپین بمباران استفاده کردند؛ هدف، تخریب بخش‌هایی از زیرساخت‌های صنعتی آلمان – مانند تأسیسات نفتی و تولید بلبرینگ – بود، زیرا اعتقاد بر این بود که این‌ها برای تداوم تلاش جنگی نازی‌ها حیاتی هستند[121]. بعدها، پیش‌بینی‌ها درباره رفتار اتحاد جماهیر شوروی در اواخر دهه ۱۹۸۰، بیشتر حول این سؤال بود که چگونه موقعیت اقتصادی آن می‌تواند تحت تأثیر سیاست‌های سایر مناطق قرار گیرد، و هر یک از این الزامات اطلاعاتی، انواع مختلفی از داده‌های اقتصادی را می‌طلبید. همچنین، این انواع مختلف مواد منبع باز، سرنخ‌های ضروری برای تفسیر داده‌های خامی هستند که از طریق سامانه‌های جمع‌آوری اطلاعات باز جمع‌آوری شده‌اند. در واقع، تفسیر و تحلیل‌هایی که شخصیت‌های سیاسی برجسته دریافت می‌کنند، متون قوانین و قانون اساسی، سرشماری‌های جمعیتی و سایر داده‌های دموگرافیک،

---

[121] ؛بمباران استراتژیک نتایج متفاوتی داشت. اقتصاددانان OSS به خاطر طراحی یک سیستم انتخاب هدف نسبتاً پیچیده و مفید شایسته تقدیر هستند، اما آنها فاقد داده‌های کافی در مورد اقتصاد آلمان در زمان جنگ بودند تا بتوانند از تحلیل استراتژیک خود به طور کامل استفاده کنند. در این موارد، به کتاب «پیروزی در جنگ بعدی: نوآوری و ارتش مدرن» نوشته استفن پیتر روزن مراجعه کنید.)ایتاکا، نیویورک: انتشارات دانشگاه کرنل (۱۹۹۱) صفحات ۱۷۰-۱۴۸.

برای هر تحلیل آکادمیک از شرایط سیاسی یا اجتماعی در یک کشور خارجی مورد نیاز خواهد بود؛ و در واقع، محصول نهایی ممکن است مشابه باشد. بر اساس منابع موجود، یک سازمان اطلاعاتی می‌تواند داده‌های خاصی را در مقادیری جمع‌آوری کند که می‌تواند محققان دانشگاهی را خسته کند. به عنوان مثال: یکی از روش‌های مهم برای درک سیاست‌ها و فرآیندهای تصمیم‌گیری سیاسی در سیستم‌های بسته؛ ردیابی مشاغل تعداد زیادی از افراد بانفوذ است که از میان آن‌ها مدیران ارشد اجرایی انتخاب می‌شوند. به محض اینکه روابط کارمند حمایت‌شده با حامی بانفوذ نسبی ذینفعان سطح بالا مشخص شود، اجرای این کار نیازمند جمع‌آوری یک پایگاه داده بزرگ و گسترده از سوابق زندگی است، و مستلزم خواندن تمام روزنامه‌ها و اخبار رادیویی، ثبت هر خبری که به ارتقا یا برکناری از یک پست، یا انتقال یک مسئول یا ارتباط بین مسئولان اشاره دارد، و ثبت پایگاه داده در رایانه که منجر به ساخت پایگاه داده‌ای می‌شود که محققان می‌توانند از آن بهره‌مند شوند، و انجام این وظیفه برای یک محقق یا مؤسسه دانشگاهی به تنهایی دشوار است[122].

[122] ؛ممکن است این سوال پیش بیاید که چرا یک سازمان اطلاعاتی در وهله اول چنین عملیاتی را انجام می‌دهد، با توجه به اینکه این پروژه کاملاً به منابع و روش‌های متن‌باز متکی است که - در دنیای آکادمیک توسعه یافته‌اند - برای کشوری که پرسنل آن را مطالعه کرده‌اند، آشنا هستند. واضح است که لزوماً

گزارش‌های دیپلماتیک و گزارش‌های وابسته نظامی

روش دیگری برای جمع‌آوری اطلاعات – که می‌توان آن را ترکیبی از اطلاعات انسانی و منابع باز دانست؛ زیرا عوامل انسانی آن را به روش‌های آشکار و صریح به دست می‌آورند – گزارش‌های دیپلماتیک و پرونده وابسته نظامی مربوط به رویدادها در کشورهایی است که آن‌ها را اعزام کرده‌اند. در واقع، مرز بین دیپلمات و افسر اطلاعاتی همیشه واضح نیست، و همانطور که یکی از مورخان دیپلماسی می‌گوید: "سفیران گاهی اوقات آماده‌اند تا از خط باریک بین روش‌های مشروع جمع‌آوری اطلاعات و جاسوسی و سایر

اینطور نیست، اما اینکه آیا قرار دادن آن در یک مرکز تحقیقاتی غیرمحرمانه ایده خوبی است یا خیر، به تعادل چندین عامل بستگی دارد. از یک سو، ممکن است تأمین نیروی انسانی در چنین مرکز باز آسان‌تر باشد و خروجی آن بتواند به راحتی با جامعه دانشگاهی به اشتراک گذاشته شود. از سوی دیگر، برای ادغام این منابع متن‌باز با اطلاعات طبقه‌بندی‌شده یا استفاده از این اطلاعات برای پشتیبانی از فعالیت‌های اطلاعاتی مخفی، به رویه‌های ویژه‌ای نیاز خواهد بود و این رویه‌ها احتمالاً دست و پا گیر خواهند بود. به عنوان مثال، اگر برای پشتیبانی از استخدام یک مقام رسمی برای اهداف جاسوسی به اطلاعات نیاز باشد، درخواست باید برای پنهان کردن دلیل، پنهان شود

فعالیت‌های بدنام عبور کنند."[123] اما حتی امروز که این دو وظیفه از هم جدا هستند، گزارش‌های دیپلماتیک درباره وضعیت سیاسی در کشور میزبان می‌تواند داده‌های مهمی برای هر تحلیل سیاسی باشد. دیپلماتی که می‌تواند به شخصیت‌های سیاسی اصلی در یک کشور دسترسی داشته باشد یا پیچیدگی‌های تاریخ کشور و پوشش سیاسی آن را ارزیابی کند، قادر است به بینشی عمیق درباره وضعیت سیاسی داخلی دست یابد که در رسانه‌ها پیدا نخواهد شد.

به همین ترتیب، وابستگان نظامی می‌توانند متناسب با میزان دسترسی خود به افسران کشور میزبان، شناخت عمیقی از ساختار نظامی آن کشور به دست آورند. آن‌ها برای نمونه می‌توانند از

---

[123] إکتاب *دفتر سفیر در قرون وسطی* نوشته دونالد وای. کوهلر (پرینستون: انتشارات دانشگاه پرینستون، ۱۹۶۷)، صفحه ۹۰. یک نمونه کلاسیک از گزارش‌های دیپلماتیک از این نوع، *تلگرام طولانی* نوشته جورج کنان در سال ۱۹۴۶ است که زمانی نوشته شده که کنان کاردار ایالات متحده در مسکو بود. تلگرام کنان در مورد اتحاد جماهیر شوروی، پایه فکری سیاست "مهار "اتحاد جماهیر شوروی در بیشتر دوران جنگ سرد توسط ایالات متحده را بنا نهاد. برای متن تلگرام کنان،
رجوع کنید به کنت ام. جنسن، ویراستار، ریشه‌های جنگ سرد: «تلگرام‌های طولانی» نوویکوف، کنان و رابرتز در سال ۱۹۴۶)واشنگتن دی.سی. موسسه صلح ایالات متحده، .((1991)

ویژگی‌های شخصیتی و میزان شایستگی فرماندهان نظامی، طرز تفکر فردی، دیدگاه‌های آنان درباره دکترین نظامی و همچنین نوع رابطه آن‌ها با رهبران غیرنظامی (سیاستمداران) آگاه شوند. علاوه بر این، ممکن است از وابستگان نظامی برای نظارت بر رزمایش‌ها یا حضور در مراسم رونمایی و انتقال سلاح‌های جدید دعوت شود. آن‌ها همچنین اجازه دارند به نقاط مختلف کشور میزبان سفر کنند و از این طریق، فرودگاه‌ها، بنادر و سایر تاسیسات مهم نظامی و غیرنظامی را زیر نظر بگیرند[124].

سایر منابع پنهان اطلاعات انسانی

[124] ؛ آنچه متن توصیف می‌کند، یک فعالیت معمول برای یک وابسته نظامی است، اساساً یک فعالیت عمومی، اگرچه او ممکن است برای مشاهده چیزهایی که کشور میزبان ترجیح می‌دهد مخفی نگه دارد، تلاش کند به مناطق محدود سفر کند یا به آنها نزدیک شود. علاوه بر این، می‌توان از آن استفاده کرد سمت وابسته نظامی (مانند هر پست دیپلماتیک) پوششی برای یک افسر اطلاعاتی است

دیپلمات‌ها و وابستگان نظامی تنها اتباع خارجی نیستند که با سفر به کشـــورهای دیگر، دیده‌ها و شـــنیده‌های خود را گزارش می‌کنند. به عنوان مثال، «پیمان موشک‌های هسته‌ای میان‌برد (INF) «مصوب ۱۹۸۷ میان ایالات متحده و اتحاد جماهیر شوروی، و همچنین «پیمان کاهش تسلیحات استراتژیک (START) «که اخیراً منعقد شده است، به طرفین این حق را می‌دهد که برای شناسایی تاسیسات نظامی کشور مقابل و اطمینان از پایبندی به مفاد توافق، بازرسانی را اعزام کنند. این بازرســـان در مقایســـه با وابســـتگان دیپلماتیک یا دیگر مسافران، دسترسی بسیار بیشتری به این تاسیسات دارند و بدیهی است که گزارش‌های آن‌ها حاوی اطلاعات ارزشمندی درباره نیروهای نظامی کشور میزبان خواهد بود.به همین ترتیب، بازرگانان، دانشمندان و دیگر مســـافران نیز اطلاعاتی درباره کشـــورهای مورد بازدید خود کسب می‌کنند که اگرچه رسماً طبقه‌بندی‌شده و سری نیستند، اما در رسانه‌های عمومی هم یافت نمی‌شوند. انتقال این دست اطلاعات به دولت‌های متبوع این افراد ـ در کشورهایی که شهروندان برای سفر به خارج نیازی به مجوز ویژه ندارند به تمایل خودِ مســـافران برای گزارش‌دهی بستگی دارد. با این حال، رشد چشمگیر تجارت بین‌الملل، سفرها و پژوهش‌های علمی در سال‌های اخیر، فرصت‌های بی‌نظیری

را برای گسـترش روزافزون این نوع جمع‌آوری پنهان اطلاعات انسـانی فراهم کرده است.


پژوهشکده تحقیقات راهبردی خیزش
Research Institute Strategic studies