انقلاب سایبری و تحول در پدیدهٔ جاسوسی

تاریخ دریافت: ۱۳۹۵/۰٤/۱۰ تاریخ پذیرش: ۱۳۹۵/۰٦/۱۵

میرابراهیم صدیق*

چکیده

این مقاله، ضمن تبیین ماهیت انقلاب سایبری، به‌دنبال پاسخ به این سوال است که این انقلاب چگونه بر ماهیت و محتوای جاسوسی تأثیر گذاشته است؟ فضای سایبر با فراهم کردن امکان فرا رفتن جاسوسی از محدودیت‌های زمانی و مکانی و در نتیجه گستردگی امکان جاسوسی، باعث ورود بازیگران و ابزارهای جدید به عرصه جاسوسی شده است و از این طریق، تأثیرات انقلابی و بنیادینی در ماهیت و شکل جاسوسی برجای گذاشته است؛ به‌گونه‌ای که استفاده از واژگانی مانند جاسوسی سایبری سیاسی، جاسوسی سایبری صنعتی، جاسوسی سایبری نظامی و جاسوسی سایبری علمی نشان‌گر آغاز روند جدیدی در این عرصه است. یافته‌های این مقاله نشان می‌دهد تحت تأثیر انقلاب سایبری، انقلاب در عرصه جاسوسی واقعیتی جدی و اجتناب‌ناپذیر است.

واژگان کلیدی: انقلاب سایبری، جاسوسی سنتی، جاسوسی سایبری، بازیگران جدید.

---

* استادیار و عضو هیئت علمی دانشگاه آزاد اسلامی واحد ایلام e.seddigh@gmail.com

مقدمه

«جاسوسی سایبری»[1] یکی از اصلاحات جدید در حوزه امنیت سایبری محسوب می‌شود که نگرانی جدی در میان بازیگران مختلف جهانی ایجاد کرده است. در این راستا، بارها مشاهده شده که رهبران کشورها، کارشناسان حوزه امنیت سایبری، مدیران شرکت‌های بزرگ چندملیتی و همچنین افراد مختلف از جاسوسی سایبری به‌عنوان تهدید بزرگی علیه منافع و امنیت‌شان صحبت می‌کنند. با وجود این، از منظر معنایی و محتوایی همچنان ابهامات گسترده‌ای در ارتباط با این مفهوم وجود دارد. به‌عنوان نمونه، جاسوسی سایبری به‌طور معمول در کنار سایر مفاهیم مرتبط با امنیت سایبری همچون «جنگ سایبری»[2]، «سایبرتروریسم»[3]، «سایبرتروریسم دولتی»[4] و همچنین «جرائم سایبری»[5] به کار می‌رود. حتی در مواردی، این مفاهیم به جای هم به کار می‌روند، که این امر گویای ابهامات گسترده و پیچیدگی‌های وسیع معنایی و محتوایی در حوزه امنیت سایبری است. البته بخش مهمی از این ابهام، به جدید بودن حوزه امنیت سایبری، حداقل برای کشورهای در حال توسعه و همچنین پیچیدگی‌های ذاتی محیط سایبر برمی‌گردد. این پیچیدگی و در عین حال جدیدبودن، در حدی است که اصولاً قابل قیاس با سایر حوزه‌های امنیتی نیست. در نتیجه، تا اندازه زیادی ابهام در زمینه تعریف تهدیداتی چون جاسوسی سایبری، طبیعی به نظر می‌رسد.

با وجود این شرایط پیچیده، می‌توان با تمرکز بر ابعاد و مؤلفه‌های موجود، به تعریف نسبتاً جامعی از جاسوسی سایبری رسید و همچنین تفاوت‌ها، شباهت‌ها و قرابت‌های آن را با سایر مفاهیم نزدیک به آن مورد بحث و بررسی قرار داد. البته برای تحقق چنین امری، ابتدا باید تأثیر فضای سایبر را بر جاسوسی مورد کنکاش قرار داد. به تعبیری دیگر، تا زمانی که فهم دقیقی از ماهیت تأثیرگذاری فضای سایبر بر جاسوسی صورت نگیرد، نمی‌توان فهم مناسبی از شرایط جدید داشت. بنابراین، کلید فهم تحولات جدید در عرصه جاسوسی، فهم دقیق از شکل و ماهیت تأثیرگذاری فضای سایبر بر جاسوسی است. در این راستا، برخی برای توضیح

---

1. Cyber Spying
2. Cyber War
3. Cyber Terrorism
4. State Cyber Terrorism
5. Cyber Crime

تأثیرگذاری فضای سایبر بر جاسوسی، از واژه انقلاب در عرصه جاسوسی یاد می‌کنند (Slater, 2014: 6) که این امر نشان‌دهنده تغییرات بنیادین در این حوزه است. برخی کارشناسان بر این باورند که در نتیجه انقلاب سایبری، باید از واژه‌ها، تعاریف، راهبردها، تاکتیک‌ها و حتی آموزش‌های جدید در عرصه جاسوسی استفاده کرد. به تعبیر دیگر، به باور آن‌ها، از نظر ماهیت، ساختار، راهبرد و تاکتیک، جاسوسی سایبری تفاوت‌های بنیادینی با جاسوسی سنتی دارد. در مقابل، برخی دیگر مخالف تغییر بنیادین در اوضاع و احوال هستند و همچنان موافق تداوم تعاریف، برداشت‌ها و روش‌های گذشته هستند. به باور آن‌ها فضای سایبر نمی‌تواند تأثیرات محتوایی و ماهوی بر فضای جاسوسی داشته باشد. به هر حال، تبیین دقیق این اختلافات و فهم عمیق ماهیت و شکل تأثیرگذاری فضای سایبر بر عرصه جاسوسی و در نتیجه، تعریف جاسوسی سایبری، ابعاد، ویژگی‌ها و انواع آن، مهم‌ترین دغدغه و مسئله مقاله حاضر است. در راستای این دغدغه، سؤال سوال اصلی مقاله بدین شکل مطرح می‌شود: «انقلاب سایبری چه تأثیراتی بر ماهیت و محتوای جاسوسی گذاشته است؟»

در پاسخ به سؤال اصلی فوق، این فرضیه مطرح می‌شود: «فضای سایبر تأثیراتی انقلابی و بنیادین در ماهیت و محتوای جاسوسی داشته، به طوری که استفاده از واژه جاسوسی سایبری نشان‌گر آغازی جدید در این عرصه محسوب می‌شود».

تردیدی در این زمینه نیست که فهم تأثیرگذاری فضای سایبر در عرصه جاسوسی و به شکل کلی، فهم ابعاد و ماهیت جاسوسی سایبری، یکی از مهم‌ترین موضوعات امنیتی برای کشورهای مختلف به حساب می‌آید. در این زمینه، می‌توان به دولت آمریکا اشاره نمود که طی چند سال گذشته، تهدیدات سایبری و به خصوص جاسوسی سایبری را مهم‌ترین تهدید علیه منافع و امنیت خود معرفی کرده و برای مقابله با آن در ابعاد مختلف، سرمایه‌گذاری‌های گسترده‌ای انجام داده است. این موضوع برای جمهوری اسلامی ایران نیز که یکی از اهداف سازمان‌های امنیتی و اطلاعاتی غربی است، از ضرورت بیشتری برخوردار است. در این زمینه، می‌توان به حملات سایبری همچون «استاکس‌نت»[1] و «شعله آتش» یا «فلیم»[2] اشاره کرد، که

1. Stuxnet
2 .Flame

هدف آن‌ها، ضربه‌زدن به تأسیسات هسته‌ای ایران بوده است. کلید موفقیت امنیتی کشورها در فضای پیچیده امروزی، شناخت عمیق از تأثیرگذاری انقلاب سایبری بر جاسوسی و ایجاد تغییرات مطابق با آن است. با توجه به این شرایط، کلید داشتن امنیت، به خصوص امنیت سایبری، در مقابله با جاسوسی، افزایش آگاهی و دانش، پیش‌گام بودن و در یک کلام، آیجاد آمادگی همه‌جانبه است.

علاوه بر این جنبه‌های سلبی، می‌توان به جنبه‌های ایجابی اهمیت فهم و شناخت تأثیرگذاری انقلاب سایبری بر جاسوسی نیز اشاره کرد. از جمله اینکه شناخت عمیق فضای سایبر و داشتن توانایی برتر در آن، می‌تواند گامی اساسی در اقدامات تهاجمی علیه اهداف و دشمنان باشد. در این زمینه، می‌توان گفت امکانات فضای سایبر عملاً جاسوسی را از محدودیت‌های زمانی و مکانی خارج نموده و بنابراین به کشورهایی که توان‌مندی لازم را در این زمینه دارند، قدرت آفندی و تهاجمی بسیاری داده است. بر این اساس، می‌توان گفت کلید موفقیت در هرگونه استراتژی تهاجمی، داشتن شناخت عمیق از امکانات و فرصت‌های فضای سایبر و همچنین توانایی فنی و اطلاعاتی لازم برای استفاده از آن است. اسناد منتشر شده توسط ادوراد اسنودن، به خوبی نشان می‌دهد ایالات متحده آمریکا اقدامات جاسوسی خود را بر محور استراتژی تهاجمی با کمک گرفتن از امکانات فضای سایبر، قرار داده است (Cartin, 2014: 16).

موضوع سایبر، یکی از عرصه‌های نو در مطالعات امنیتی محسوب می‌شود. با وجود این، واقعیت این است که حتی در کشورهای پیشرفته نیز هنوز ماهیت و محتوای فضای سایبر و چگونگی تأثیرگذاری آن بر سایر حوزه‌ها و به‌خصوص حوزه‌های حساسی چون جاسوسی، چندان مورد کنکاش قرار نگرفته است. بنابراین، حتی در کشورهای پیشگام در عرصه سایبری، کتب و مقالات محدودی در این زمینه چاپ شده است. یکی از دلایل اصلی چنین امری، سیال و پویا بودن فضای سایبر و مشخص نبودن حدومرز آن است. در این زمینه، می‌توان به کتاب «سایبرپولیتیک در روابط بین‌الملل» اشاره کرد (Choucri, 2012) که در نوع خود، یکی از بهترین آثار منتشرشده در ارتباط با فضای سایبر و تأثیرگذاری آن در حوزه‌های مختلف محسوب می‌شود. با وجود این، در این کتاب، بیشتر در مورد تأثیرگذاری فضای سایبر و به

تعبیری، تأثیرگذاری انقلاب سایبر بر ابعاد مختلف سیاست و امنیت اشاره شده است و بحث خاصی در حوزه اطلاعاتی و جاسوسی مطرح نشده است. همچنین، می‌توان به کتاب «ضدتروریسم و امنیت سایبری: آگاهی اطلاعاتی جامع» (Newton, 2103)، به عنوان یکی دیگر از آثار منتشرشده در حوزه امنیت سایبری و انقلاب سایبری اشاره کرد. در این کتاب نیز طی چهار بخش نویسنده کم‌وبیش تمامی ابعاد مختلف امنیت سایبری و ضدتروریسم را مورد بحث و بررسی قرار داده است. «ویلسون کلی»[1] در مقاله‌ای، ضمن تلاش برای تعریف تهدیدات سایبری به عنوان یکی از تهدیدات جدید و اساسی برای ایالات متحده آمریکا، توصیه‌های راهبردی در این زمینه ارائه کرده است. نتیجه‌ای که وی از این مقاله می‌گیرد، این است که ایالات متحده آمریکا، آسیب‌پذیری بالایی در حوزه سایبر در برابر تهدیدات دارد و هر چه سریع‌تر، باید در این زمینه کار اساسی صورت گیرد (Clay, 2008). این مقاله نیز بیشتر در ارتباط با تهدیدات سایبری است و تمرکز چندانی بر موضوع تأثیرگذاری انقلاب سایبری بر جاسوسی ندارد. در نهایت، می‌توان به مقاله «کارتین»[2] اشاره نمود، که در آن، ضمن تلاش برای شناخت محیط امنیتی جدید، از ضرورت روی آوردن به استراتژی تهاجمی در برابر تهدیدات سایبری بحث شده است. در واقع، در این مقاله، ضمن تأیید انقلاب صورت گرفته در حوزه امنیت به‌واسطه انقلاب سایبری، تنها راه تأمین امنیت نسبی، روی‌آوردن به استراتژی تهاجمی عنوان شده است (Cartin, 2014).

به زبان فارسی نیز مقاله یا کتاب خاصی نیست که به شکل دقیق بر موضوع تأثیرگذاری انقلاب سایبری بر جاسوسی تمرکز کرده باشد. طی چند سال گذشته، کتب متعددی در مورد جنگ سایبری و امنیت سایبری به زبان فارسی نوشته شده است[3]؛ با این حال، این آثار بیشتر جنبه توصیفی دارند. ضمن اینکه در این کتاب‌ها، امنیت به شکل کلی دیده شده و موضوع تأثیرگذاری فضای سایبر بر جاسوسی اصولاً مورد توجه نبوده است. همچنین، می‌توان به

1.Wilson Clay

2. Josh M. Cartin

۳. رجوع شود به مجموعه کتاب‌های چهار جلدی امنیت و جنگ سایبری (۱)، امنیت و جنگ سایبری (۲) امنیت و جنگ سایبری (۳) و امنیت و جنگ سایبری (٤) که به همت مؤسسه فرهنگی مطالعات و تحقیقات بین‌المللی ابرار معاصر تهران در سال‌های ۱۳۹۱ و ۱۳۹۲ چاپ شده است.

مقاله‌ای با عنوان «تهدیدات سایبری و تأثیر آن بر امنیت ملی» اشاره کرد (رکن‌آبادی و نورعلی‌وند، ۱۳۹۱: ۱۹۶-۱۶۸)؛ که در آن، تأثیرگذاری تهدیدات سایبری بر ابعاد مختلف امنیت مورد بررسی قرار گرفته است. امتیاز مقاله حاضر در این است که صرفاً بر روی تأثیر انقلاب سایبری بر جاسوسی تمرکز کرده است.

از منظر ساختاری، مقاله حاضر مشتمل بر سه بخش اصلی است. در بخش اول، تلاش می‌شود انقلاب صورت‌گرفته در عرصه جاسوسی مورد تجزیه و تحلیل قرار گیرد. نکته مهم این است که فهم چنین انقلابی، کمک فراوانی به فهم ابعاد مختلف جاسوسی سایبری می‌کند. موضوع بخش دوم، تعریف ابعاد محتوایی جاسوسی سایبری می‌باشد. در بخش سوم نیز با توجه با مباحث قبلی، انواع و ابعاد جاسوسی سایبری مورد بحث قرار می‌گیرد و در نهایت، نتیجه‌گیری ارائه خواهد شد.

الف. مبانی نظری و مفهومی

احتمالاً «گستردگی»، کلیدی‌ترین مفهومی است که نشان‌گر و نماد انقلاب در عرصه جاسوسی در دوران انقلاب اطلاعات و ارتباطات سایبری است. به تعبیر دیگر، فضای سایبر با ایجاد زمینه و فضای گسترده برای جاسوسی در عرصه‌ها، حوزه‌ها، مکان‌ها و فضاهای جدید، عملاً جاسوسی را از محذورات مکانی و زمانی خارج نموده و بدین ترتیب، انقلابی در عرصه جاسوسی ایجاد کرده است. از جمله اینکه فضای سایبر، زمینه و شرایط ورود بازیگران زیادی را به عرصه جاسوسی فراهم کرده و محیط را برای دولت‌ها به‌عنوان بازیگر سنتی پیچیده‌تر کرده است. در ادبیات اطلاعاتی سنتی، معمولاً در تعریف جاسوسی، بر محوریت بازیگری دولت تأکید می‌شود؛ بدین معنا که تنها اقدامات صورت‌گرفته توسط دولت‌ها، جاسوسی محسوب می‌شوند (Braff, 2005:1). با وجود این، در دنیای سایبری، عملاً این نوع نگاه به جاسوسی تغییر کرده و تمامی بازیگران با منافع متفاوت، به دنبال دسترسی به اطلاعات مهم و حیاتی هستند. در این زمینه، می‌توان به شرکت‌های چندملیتی، گروه‌های تروریستی و خرابکار، گروه‌های درگیر جرایم بین‌المللی سازمان‌یافته، هکرها و حتی افراد نام برد که هر کدام به دلایل متفاوتی به دنبال کسب اطلاعات حساس هستند. بنابراین، یکی از تأثیرات فضای سایبر در عرصه

جاسوسی، ایجاد شرایط برای ورود سایر بازیگران به عرصه جاسوسی، برای کسب اطلاعات حساس و تأمین منافع، است. البته در ادبیات امنیتی همچنان اقداماتی که توسط دولت‌ها یا تحت هدایت آن‌ها برای به‌دست آوردن اطلاعات مهم صورت می‌گیرد، جاسوسی شناخته می‌شود، با این حال، انقلاب سایبری عملاً راه را برای ورود و بازیگری سایر بازیگران، در این حوزه مهیا کرده است (Braff, 2005: 2).

انقلاب ارتباطات و اطلاعات، از منظر زمانی و مکانی جهان را فشرده کرده و در نتیجه امکان جاسوسی در گستره زمان و مکان را چنان مهیا نموده، که در گذشته اصولاً قابل تصور نبود. در واقع، به زبان ساده معنای چنین تحولی این است که برای آن‌هایی که به‌دنبال جاسوسی هستند، دیگر زمان و مکان معنایش را از دست داده و جاسوسی به فرای محدودیت‌های زمانی و مکانی رسیده است. این در شرایطی است که قبل از انقلاب سایبری در عرصه جاسوسی، عملاً محدودیت زمانی و به‌خصوص مکانی، از مهم‌ترین موانع محسوب می‌شدند. امروزه تقریباً تمامی محیط‌های فردی، شخصی، اقتصادی، نظامی، سیاسی، اطلاعاتی و امنیتی به‌شکلی به دنیای سایبر متصل هستند و یا اینکه دنیای سایبر عملاً امکانات رسوخ به آن‌ها را فراهم نموده است. بر اساس آمارهای معتبر بین‌المللی در سال ۲۰۱۵، استفاده از اینترنت طی دهه گذشته حداقل چهار برابر شده است. همچنین، طی سال‌های اخیر، بیش از ۳ میلیارد نفر کاربر اینترنت در سطح جهان فعال بوده‌اند. بر اساس آخرین آمارهای بین‌المللی، در حال حاضر ٤٠ درصد از جمعیت جهان ارتباط روزانه و مداوم اینترنتی دارند. این در شرایطی است که در سال ۱۹۹۵ این میزان چیزی در حدود ۱ درصد بود. ضمن اینکه در همین مدت، میزان پهنای باند و سرعت اینترنت و در نتیجه، سرعت تبادل اطلاعات و داده‌ها به شدت افزایش یافته که این امر در مجموع عرصه‌ای جدید برای تأثیرگذاری و تأثیرپذیری و در عین حال جاسوسی و قدرت‌یابی در عرصه‌های مختلف مهیا کرده است (Internet Users, 2015 :1). در نهایت، باید به این آمار ابعاد دیگر دنیای سایبر از جمله میزان استفاده از رایانه، انواع حافظه جانبی، تلویزیون‌های دیجیتال و نظیر این‌ها را اضافه کرد.

کاربران اینترنت در جهان در سال ۲۰۱۶

سال	کاربران اینترنت	میزان نفوذ اینترنت به درصد	میزان جمعیت جهان	عدم دسترسی به اینترنت	تغیرات سالیانه به درصد	تغیرات سالیانه به نفر	تغیرات جمعیتی به درصد
۲۰۱۶	۳٤۲٤۹۷۱۲۳۷	٤٦	۷٤۳۲٦٦۳۲۷٦٥	٤۰۰۷٦۹۲۰۳۸	۷/٥	۲۳۸۹۷٥۰۸۲	۱/۱۳
۲۰۱٥	۳۱۸٥۹۹٦۱٥٥	٤۳	۷۳٤۹٤۷۲۰۹۹	٤۱٦۳٤۷٥۹٤٤	۷/۸	۲۲۹٦۱۰٥۸۹	۱/۱٥

http://www.internetlivestats.com/internet-users/iran/

با توجه به این شرایط، کشورهایی که دارای دانش و توانایی لازم هستند، در عمل می‌توانند تقریباً اکثر نقاط حساس و مهم کشورهای مختلف را در هر زمان و مکانی رصد کنند و اطلاعات لازم و حیاتی را به دست آورند (Cartin, 2014: 1). اطلاعات منتشرشده توسط سایت «ویکی‌لیکس»[1] و افرادی چون «جولیان آسانژ»[2] و «ریچارد اسنودن»[3] به خوبی این موضوع را تأیید می‌کنند. از جمله اینکه اطلاعات منتشرشده نشان می‌دهند سازمان‌های اطلاعاتی آمریکا با توجه به امکانات سایبری این کشور، عملاً بیشتر کشورها را به شکل گسترده در هر زمانی که اراده کرده‌اند، مورد رصد قرار داده‌اند (Davies, 2014: 1-14).

از دیگر جنبه‌های تأثیرگذاری انقلاب سایبری در عرصه جاسوسی، امکان‌پذیری و گستردگی دسترسی به ابعاد و حوزه‌های مختلف کشورها آن هم با کمترین هزینه و زمان است. به تعبیر دیگر، فضای سایبر این امکان را برای بازیگران مختلف از جمله دولت‌ها فراهم کرده تا با کمترین نیروی انسانی و هزینه، عملاً بیشتر ابعاد و حوزه‌های مختلف یک کشور را رصد کنند و اطلاعات لازم و حساسی را به دست آورند. این ابعاد و حوزه‌ها شامل ابعاد سیاسی، اقتصادی، صنعتی، نظامی، آموزشی، پژوهشی و در نهایت اجتماعی و فرهنگی می‌شود. به

1.WikiLeaks
2.Julian Assange
3. Edward Snowden

عنوان نمونه، فضای سایبر این امکان را فراهم نموده تا حتی حساس‌ترین اطلاعات سیاسی کشورها در دسترس دیگران قرار گیرد. در این زمینه می‌توان به اطلاعات منتشرشده سایت ویکی‌لیکس و اسنودن اشاره نمود که در آن‌ها به وضوح نشان داده شده ایالات متحده آمریکا تقریباً حساس‌ترین مراکز سیاسی و امنیتی کشورهای مختلف را رصد کرده است. از جمله، ایالات متحده آمریکا حتی مکالمات رهبران نزدیک‌ترین کشورها به خود از جمله رهبران آلمان، فرانسه و انگلیس را رصد کرده و از آخرین و حساس‌ترین اطلاعات سیاسی و امنیتی این کشورها باخبر بوده است. همین اطلاعات به خوبی نشان می‌دهد آمریکا و احتمالاً سایر کشورها، عملاً در حال رصد رهبران و مراکز حساس سیاسی سایر کشورها به خصوص کشورهای هدف هستند (Slater, 2014: 36).

وقتی فضای سایبر امکان دسترسی به فضاهای حساس سیاسی در هر زمان و مکان را مهیا کرده، می‌توان گفت عملاً فضاهای کمتر حساس و در نتیجه کمتر حفاظت‌شده‌ای چون فضاهای اقتصادی و صنعتی، علمی، پژوهشی، اجتماعی و فرهنگی بیشتر در دسترس سازمان‌ها و مراکز اطلاعاتی قرار گرفته‌اند. در این زمینه، می‌توان به رقابت گسترده بین کشورهای مختلف برای دسترسی به اطلاعات غیرسیاسی و غیرامنیتی همدیگر اشاره کرد. از جمله می‌توان به تلاش گسترده دولت و مراکز علمی و صنعتی چین برای دسترسی به اطلاعات علمی، تکنولوژیکی و صنعتی آمریکا اشاره نمود که عمدتاً با امکانات فضای سایبر صورت می‌گیرد. فضای سایبر همچنین این امکان را مهیا کرده که برخی از کشورها از جمله آمریکا، ویژگی‌های فرهنگی، اجتماعی و تمایلات مردمان کشورها مختلف را رصد کرده و از آن‌ها برای سیاست‌گذاری و اقدام استفاده کنند. بر اساس اسناد سایت ویکی‌لیکس، دولت آمریکا ارتباطات بسیار نزدیکی با شرکت‌های اصلی در عرصه فضای سایبر دارد و از آن‌ها می‌خواهد اطلاعات شهروندان کشورهای مختلف را در اختیار سازمان‌های اطلاعاتی آمریکا قرار دهند. با توجه به این شرایط، باید گفت یکی از مهم‌ترین پیامدهای انقلاب سایبری در عرصه جاسوسی، تسهیل جمع‌آوری اطلاعات، آن هم به شکل گسترده در ابعاد و حوزه‌های مختلف یک کشور توسط سایرین است که این خود یکی از ویژگی‌های ماهوی تفاوت‌زا بین جاسوسی سنتی و جاسوسی سایبری در معنای عام است.

ب. جاسوسی سایبری و نسبت آن با جنگ سایبری و سایبرتروریسم

نگاهی گذرا به تعاریف متنوع از جاسوسی سایبری نشان می‌دهد اجماع روشنی در این مورد وجود ندارد. علت اصلی این امر آن است که هنوز برخی، انقلاب صورت‌گرفته در عرصه جاسوسی به واسطه انقلاب سایبری را باور ندارند. در این زمینه، حتی برخی، اصولاً جاسوسی سایبری را به عنوان حوزه جدیدی در عرصه جاسوسی قبول ندارند. به باور آن‌ها، جاسوسی در معنای عام، تلاشی برای به دست آوردن اطلاعات مهم و طبقه‌بندی شده است. بنابراین، هر گونه تلاش برای به دست آوردن چنین اطلاعاتی، نوعی جاسوسی محسوب می‌شود. بر این اساس، در جاسوسی، مهم‌ترین مسئله، محتوای عمل و نه ابزار مورد استفاده است. به تعبیر دیگر، جاسوسی سایبری همان جاسوسی سنتی با ابزار دیگر است. بنابراین، نباید آن را حوزه و موضوعی جدید فرض کرد. در مقابل، برخی بر این باورند که جاسوسی سایبری اصولاً انقلابی در عرصه جاسوسی محسوب می‌شود که نه فقط ابزار، بلکه ماهیت، حوزه و گستره عمل را نیز تغییر داده است. بر این اساس، باید این حوزه مورد تعریف خاص‌تر قرار گیرد و از آن به عنوان حوزه جدید جاسوسی در مقابل جاسوسی کلاسیک یاد شود (Sterken, 2013: 1).

در مقابل، برخی دیگر تلاش کرده‌اند جدای از این مجادلات، تعاریف مورد قبولی از جاسوسی سایبری ارائه دهند. به عنوان نمونه، برخی، جاسوسی سایبری را سرقت اطلاعات با فرمت دیجیتال از کامپیوتر و دنیای دیجیتال مترادف دانسته‌اند (cyber spying definition, 2015: 1). برخی، جاسوسی سایبری را این گونه تعریف کرده‌اند: «جاسوسی سایبری اشاره به عملی دارد که با هدف به دست آوردن اسرار (اطلاعات حساس، طبقه‌بندی شده و حیاتی) از افراد، دولت‌ها، رقبا، دشمنان و شرکت‌های بزرگ تجاری، با هدف بهره‌برداری سیاسی، اقتصادی و نظامی و با توسل به اینترنت، شبکه، نرم‌افزار و کامپیوتر صورت می‌گیرد (What does Cyberspying mean, 2015: 1-2). در تعریفی مشابه، جاسوسی سایبری، به دست آوردن اطلاعات سری بدون اجازه مالک آن معنا شده است. این مالک می‌تواند فرد، دولت، شرکت یا هر بازیگر دیگری باشد (Definition of cyber espionage, 2013: 1). برخی دیگر، جاسوسی سایبری را هر گونه تلاش برای به دست آوردن اطلاعات طبقه‌بندی‌شده با ابزارهای

دنیای دیجیتال تعریف کرده‌اند که تنها توسط دولت‌ها یا کسانی انجام می‌شود که از دولت‌ها دستور می‌گیرند (Definition of cyber espionage, 2013: 1).

همان‌گونه که از این تعاریف نسبتاً مورد اجماع مشخص است، کم‌وبیش اختلاف محوری در زمینه بازیگر اصلی در این زمینه است. سؤال محوری در این زمینه این است که بازیگر اصلی در عرصه جاسوسی سایبری چه کسی است؟ آیا باید هر گونه تلاش توسط هر بازیگری برای به دست آوردن اطلاعات در فضای سایبر و دنیای دیجیتال را جاسوسی سایبری معرفی کرد؟ یا اینکه جاسوسی سایبری اقدامی است منتسب به دولت‌ها؟ همان‌گونه که از تعاریف ارائه‌شده برمی‌آید، برای برخی، تفاوت مهمی بین دولت‌ها و سایر بازیگران در این حوزه وجود ندارد. بدین معنا، تلاش برای به دست آوردن اطلاعات حیاتی و مهم، با امکانات فضای سایبر، توسط هر بازیگری، مصداق جاسوسی سایبری محسوب می‌شود. بر این اساس، عامل جاسوسی سایبری می‌تواند دولت‌های مختلف، شرکت‌های چندملیتی و حتی گروه‌های خرابکار سایبری و هکرها باشند.

نگاه این تعاریف به جاسوسی، بیشتر تحت تأثیر کسانی می‌باشد که جاسوسی سایبری را مرحله‌ای نوین در عرصه جاسوسی ارزیابی می‌کنند که در بیشتر زمینه‌ها قابل قیاس با جاسوسی سنتی نیست. از جمله اینکه فضای سایبر چنان امکاناتی برای جاسوسی فراهم کرده که هر بازیگری در هر زمینه‌ای که بخواهد، در صورت داشتن توانایی و دانش لازم، می‌تواند دست به اقدام زند. این همان چیزی است که از آن تحت عنوان انقلاب در جاسوسی یاد می‌شود؛ انقلابی که گستره بازیگران، امکانات، محتوا و فضای جاسوسی را به کلی تغییر داده است (Benner, 2015: 1-2).

با وجود این، برخی دیگر، مخالف چنین تعریف گسترده‌ای از جاسوسی سایبری یا استفاده از عباراتی همچون انقلاب سایبری در زمینه جاسوسی هستند. به باور آن‌ها، جاسوسی سایبری را باید با همان محتوا و ماهیت جاسوسی سنتی در نظر گرفت. بدین معنا، جاسوسی سایبری هر گونه تلاش در فضا و دنیای دیجیتال و سایبر برای به دست آوردن هر گونه اطلاعات طبقه‌بندی‌شده در عرصه‌های مختلف سیاسی، اقتصادی، امنیتی، نظامی، علمی، اجتماعی و فرهنگی محسوب می‌شود؛ که توسط دولت‌ها یا به نمایندگی از آن‌ها صورت می‌گیرد. بر این

اساس، نمی‌توان اقدامات افراد، گروه‌ها، هکرها و امثال آن‌ها را در فضای جدید، جاسوسی سایبری نامید. به باور این افراد، موضوع مهم در زمینه جاسوسی سایبری، نقش دولت به عنوان بازیگر اصلی است؛ بدین معنا که بود و نبود آن‌ها ممکن است ماهیت عملی کاملاً مشابه را از جاسوسی سایبری به جرم سایبری تقلیل دهد. به عنوان نمونه، تلاش برای کسب اطلاعات و دانش صنعتی شرکت‌های یک کشور، اگر با حمایت و هدایت دولت صورت گیرد، مصداق جاسوسی سایبری محسوب می‌شود. در مقابل، اگر همین عمل توسط شرکت‌های رقیب در کشورهای مختلف صورت گیرد، مصداق جرایم سایبری است. در نتیجه، موضوع مهم در جاسوسی سایبری، نقش اساسی دولت به عنوان بازیگر اصلی است (Sauver, 2008: 1-5).

در نهایت، باید به این نکته اشاره کرد که بیشتر کارشناسان و همچنین اکثر کشورهای جهان متمایل به این هستند که نقش برجسته دولت در تعریف جاسوسی سایبری را به رسمیت بشناسند. علت اصلی این امر نیز موضوع تأمین امنیت در حوزه سایبر و همچنین پاسخ‌گویی آسان‌تر دولت‌ها در مقایسه با سایر بازیگران است. به هر حال، دولت‌ها ترجیح می‌دهند صرفاً جاسوسی صورت‌گرفته توسط یکدیگر در عرصه سایبری را جاسوسی سایبری معرفی کنند و از گستردگی تعریف که منجر به پیچیدگی بیشتر می‌شود، جلوگیری کنند. البته، این بدین معنا نیست که آن‌ها تحولات عمیق صورت‌گرفته در عرصه جاسوسی را باور ندارند، بلکه این امر بیشتر بنا به ملاحظات سیاسی و امنیتی است. به هر حال، با توجه به این برداشت‌ها و معانی مختلف از جاسوسی سایبری، در ادامه تلاش می‌شود با هدف روشن‌ترشدن بحث و ابعاد ریزتر موضوع، مشابهت‌ها و تفاوت‌های جاسوسی سایبری با سایر پدیده‌های نزدیک به آن، مورد تجزیه و تحلیل قرار گیرد (What does Cyber spying mean, 2015: 1).

۱. نسبت مفهومی و محتوایی با جنگ سایبری

گاهی جاسوسی سایبری و جنگ سایبری به شکل هم‌زمان و حتی گاهی به جای همدیگر به کار می‌روند. چرایی این موضوع از ابعاد مختلف قابل بررسی است. اول اینکه در بسیاری از موارد، جاسوسی سایبری، خود مقدمه جنگ سایبری یا حتی جنگ در معنای عام آن محسوب می‌شود. در این راستا، کشورهای مختلف تلاش می‌کنند با توسل به امکانات دنیای سایبر، اطلاعات لازم

را درباره توانمندی‌های کشور مقابل، در عرصه‌های مهم، به دست آورند. ضمن اینکه جاسوسی سایبری خود گاهی با هدف شناساسی نقاط ضعف سیستم سایبری کشور هدف مورد استفاده قرار می‌گیرد تا زمینه برای ساخت بدافزارها و سلاح‌های سایبری مخرب آماده شود. بنابراین، کاملاً طبیعی به نظر می‌رسد که جاسوسی سایبری به عنوان مقدمه جنگ سایبری یا حتی جنگ در معنای عام آن در نظر گرفته شود. موضوع دوم در این زمینه، که بر پیچیدگی‌های موضوعی و محتوایی می‌افزاید، هم‌زمانی این دو در برخی موارد است. در واقع، می‌توان گفت در برخی از جنگ‌های سایبری، گاهی هر دو پدیده در کنار هم دیده شده‌اند. در مواردی نیز مشاهده می‌شود که بدافزاری یا ویروس اینترنتی به شکل هم‌زمان هم باعث تخریب در سیستم‌های کشور هدف شده و هم اینکه هم‌زمان جاسوسی می‌کند. بر این اساس، در دنیای واقعی، گاهی تفاوت چندانی بین جاسوسی سایبری و جنگ سایبری دیده نمی‌شود و این دو گاه ملازم با هم و گاهی یکی پس از دیگری مشاهده می‌شوند (Bruce, 2014: 1).

با وجود این، این بدان معنا نیست که این دو مفهوم هیچ‌گونه تفاوت ماهوی با هم ندارند. واقعیت این است که این دو مفهوم بیش از شباهت، با هم تفاوت دارند. مهم‌ترین تفاوت این دو مفهوم، به هدف و انگیزه متفاوت آن‌ها برمی‌گردد. جنگ سایبری اقدامی است که توسط دولت‌ها صورت می‌گیرد، تا از طریق نرم‌افزار، بدافزار، ویروس، تروجان یا هر ابزار اینترنتی دیگر، تخریب عینی و واقعی در امکانات و تاسیسات حیاتی دولت دشمن ایجاد کند. با توجه به این تعریف، مسئله اصلی در جنگ سایبری، ایجاد تخریب در کشور دشمن با توسل به امکانات فضای سایبر است. در مقابل، جاسوسی سایبری توسط دولت‌ها و تنها با هدف کسب اطلاعات حیاتی و طبقه‌بندی‌شده در ابعاد مختلف صورت می‌گیرد؛ هرچند این اطلاعات می‌تواند باعث ایجاد برتری در حوزه‌های مختلف و گاهی در عرصه نبرد سایبری یا نظامی شوند. با توجه به این تفاوت ماهوی و مهم، نمی‌توان این دو مفهوم را دقیقاً به جای هم به کار برد. با عنایت به این امر، به شکل خلاصه می‌توان گفت نکته کلیدی در جنگ سایبری، تخریب و ویرانی و در جاسوسی سایبری، جمع‌آوری و کسب اطلاعات حیاتی و طبقه‌بندی‌شده است. شباهت‌های این دو مفهوم بیشتر جنبه ظاهری دارد، حال آنکه تفاوت‌ها، جنبه ماهوی و محتوایی دارند (Sauver, 2008: 5).

۲. نسبت مفهومی و محتوایی با سایبرتروریسم

آنچه باعث می‌شود که سایبرتروریسم از منظر محتوایی و معنایی جدا از جاسوسی و جنگ سایبری باشد، محوریت موضوع تروریسم و تروریست‌هاست. همان‌گونه که گفته شد، در جنگ سایبری یا جاسوسی سایبری، بازیگر اصلی دولت‌ها هستند. این موضوع، به قدری مهم است که اگر جنگ سایبری توسط بازیگران غیردولتی صورت گیرد، از آن تحت عنوان جرایم یا خرابکاری سایبری یاد می‌شود (Catherine and Rollins, 2015: 9). همین موضوع نیز در مورد جاسوسی سایبری صادق است. در این راستا، حتی اگر سایبرتروریست‌ها در عمل موفق شوند جاسوسی سایبری گسترده‌ای را سامان دهند و با توسل به اطلاعات کسب‌شده، تخریب‌های گسترده‌ای را ایجاد کنند، در عمل هیچ‌کدام از این موارد مشمول تعریف جنگ یا جاسوسی سایبری نمی‌شود. بر این اساس، تفاوت بنیادین سایبرتروریسم با جنگ و جاسوسی سایبری، به موضوع بازیگر اصلی آن‌ها برمی‌گردد (Catherine and Rollins, 2015: 1).

البته اشاره به این نکته ضروری است که در دنیای واقعی، تشخیص این موارد چندان آسان به نظر نمی‌رسد. دلیل این موضوع در آن است که فضای سایبر عموماً و ذاتاً فضای پیچیدگی‌ها و ابهامات دامنه‌دار است. به عنوان نمونه، در فضای سایبر، هیچ‌گاه نمی‌توان به آسانی و با دلیل و مدرک، عاملین جاسوسی، جنگ یا خرابکاری سایبری را معرفی کرد؛ تا بر اساس آن، بتوان به تعاریف ارائه شده از جنگ، جاسوسی سایبری با سایبرتروریسم استناد کرد. در این زمینه، می‌توان به جنگ‌های سایبری چند سال گذشته علیه برخی کشورها از جمله ایران اشاره کرد، که در هیچ‌کدام از آن‌ها، عاملین نه با دلیل و مدرک مستند، بلکه بیشتر با نیت‌خوانی سیاسی شناسایی شدند. همین موضوع، در مورد جنگ‌ها و خرابکاری‌های سایبری علیه سایر کشورها از جمله گرجستان، استونی، اکراین، عربستان، چین و روسیه نیز صادق است.

افزون بر این موارد، باید به «سایبرتروریسم دولتی» اشاره کرد که به شدت بر پیچیدگی‌های این سه مفهوم محوری در حوزه امنیت سایبری افزوده است. به هر حال، سایبرتروریسم دولتی، پیوندی بین بازیگری دولت و تروریست‌هاست؛ که این امر، حد فاصل محتوایی و معنایی جنگ و جاسوسی سایبری با سایبرتروریسم را از بین برده است. در واقع، همان‌گونه که

«تروریسم دولتی»[1] معانی و مفاهیم سنتی امنیت را مـورد تجـاوز قـرار داده و محیطـی پیچیـده ایجاد کرده، استفاده دولت‌ها از گروه‌های تروریستی فعال در حوزه سایبر نیز چنـین مشـکلاتی ایجاد کرده است. در واقع، به همین دلیل است که کارشناسـان حـوزه امنیـت، بـه کـرات و بـا نگرانی در مورد عواقب جدی و خطرناک توسل دولت‌ها به فضـای سـایبر، بـه عنـوان ابـزاری برای ایجاد تهدید، تخریب و جنگ، هشدار می‌دهند. نگرانی این کارشناسان، ناشی از آن اسـت که در آینده نه‌چندان دور، کنترل فضای سایبر از دست دولت‌ها خارج شود. در این زمینه، حتی برخی بر این باروند که این امر در شرایط کنونی اتفاق افتـاده و کشـوری همچـون آمریکـا کـه خود عامل و محور اصلی در ایجاد، گسترش و مدیریت جهان سایبر محسوب می‌شـود نیـز بـا تهدیداتی جدی در این عرصه مواجه است (Swicegood, 2014: 1-16).

ج. ابعاد و حوزه‌های جاسوسی سایبری

همان‌گونه که گفته شد، جاسوسی سایبری اشاره به انقلابی دارد که به واسطه انفجار اطلاعـات و ارتباطات یا آنچه از آن تحت عنـوان انقـلاب دیجیتـال یـا سـایبر یـاد مـی‌شـود، در عرصـه جاسوسی صورت گرفته است. این انقلاب، تأثیرات گسـترده، عمیـق و مـاهوی بـر جاسوسـی گذاشته، به‌شکلی که دیگر نمی‌توان آن را در قالـب و چـارچوب‌هـای سـنتی در نظـر گرفـت. به‌عنوان نمونه، در نتیجه چنین انقلابی، نیاز ضروری برای شناخت و تعریف مجدد جاسوسـی، ابعاد و حوزه‌های آن، تعریف و بازنگری راهبردها، سیاست‌ها، آموزش‌ها و حتـی جـذب‌هـا و استخدام‌ها به‌وجود آمده است. به این ترتیب، حوزه‌های مختلـف جاسوسـی نیـز تحـت تـأثیر چنین انقلابی قرار گرفتـه؛ کـه در نتیجـه آن، امـروزه از مفـاهیم ترکیبـی و جدیـدی همچـون «جاسوسی سایبری سیاسی»[2]، «جاسوسی سایبری نظامی»[3]، «جاسوسی سایبری صنعتی»[4] و حتی «جاسوسی سایبری علمی»[5] استفاده می‌شود.

---

1. State Terrorism
2. Political Cyber Spy
3. Military Cyber Spy
4. Industrial Cyber Spy
5. Scientific Cyber Spy

۱. جاسوسی سایبری سیاسی

جاسوسی سایبری سیاسی، به مجموعه اقداماتی گفته می‌شود که با توسل به امکانات و فرصت‌های فضای سایبری، با هدف کسب اطلاعات سیاسی کشورهای رقیب یا دشمن، صورت می‌گیرد (Angela Merkel's call to Obama: are you bugging my mobile phone, 2014:1). در واقع، از منظر ماهوی، تفاوت چندانی بین جاسوسی سیاسی در معنای سنتی و جاسوسی سیاسی سایبری وجود ندارد. در هر دو مورد، در نهایت هدف اصلی کسب اطلاعات حیاتی سیاسی کشورهای دیگر با هدف شناخت و در نتیجه سیاست‌گذاری و اقدام بهتر و منطقی‌تر است. منظور از اطلاعات سیاسی حساس، راهبردهای کلان سیاسی، امنیتی و نظامی است که توسط عالی‌ترین مقامات سیاسی، امنیتی و نظامی کشورها در برهه‌های زمانی کوتاه‌مدت، میان‌مدت و بلندمدت اتخاذ می‌شود. به‌رغم این شباهت، در تعریف و هدف، تفاوت‌های بنیادینی بین این دو به‌خصوص در استفاده از ابزارها و همچنین سطح و گستره وجود دارد (Angela Merkel's call to Obama: are you bugging my mobile phone, 2014: 2). بدین معنا، جاسوسی سیاسی سایبری به‌واسطه استفاده از ابزارهای جدید، عملاً سطح و گستره‌ای عجیب یافته و بسیاری از محدودیت‌ها و محذورات گذشته را کنار زده است. بر این اساس، به نظر می‌رسد اصولاً جاسوسی سیاسی به‌واسطه ورود به فضای سایبر، عملاً با انقلابی در مفهوم و به‌خصوص در حوزه و گستره و امکانات و فرصت‌ها مواجه شده است. عصاره و چکیده چنین تحولی این است که با توجه به انقلاب سایبری، دیگر کمتر فضای سیاسی امنی وجود دارد، که برای سایرین قابل دسترسی نباشد. در این زمینه، می‌توان به اطلاعات منتشرشده توسط سایت ویکی‌لیکس و همچنین افشاگری‌های اسنودن اشاره کرد. اطلاعاتی که از این دو منبع منتشر شده، نشان می‌دهد دستگاه‌های اطلاعاتی و جاسوسی آمریکا، تقریباً به شخصیت‌های سیاسی برجسته هر کشوری که خواسته‌اند و همچنین مراکز حیاتی کشورها، دسترسی داشته است. عمق نگرانی زمانی مشخص شد که رهبران کشورهای همچون آلمان، که خود از جمله کشورهای پیشرو در عرصه فضای سایبر و جاسوسی سایبری هستند نیز مورد جاسوسی سیاسی سایبری آمریکا قرار گرفته‌اند. بر اساس اطلاعات منتشرشده، تلفن همراه خانم آنگلا مرکل، صدراعظم آلمان، توسط دستگاه‌های جاسوسی آمریکا مورد

جاسوسی قرار گرفته است. می‌توان جاسوسی سایبری سیاسی از رهبران سایر کشورها از جمله فرانسه و انگلستان را نیز به این مورد اضافه کرد. بـه هـر حـال، زمـانی کـه امکـان جاسوسـی سایبری از رهبران قوی‌ترین کشورهای اروپـایی وجـود دارد، عمـلاً ایـن نگرانـی بـرای سـایر کشورها کاملاً جدی و نگران‌کننده است. ضمن اینکه این رویدادها، نشان‌دهنده این هستند کـه جاسوسی سیاسی سایبری از نظر حوزه و گستره، قابل قیاس بـا جاسوسـی سیاسـی در معنـای سـنتی نیسـت (Angela Merkel's call to Obama: are you bugging my mobile phone, 2014).

۲. جاسوسی سایبری در حوزه نظامی

یکی از پیامدهای جدی انقلاب صورت‌گرفته در فضای سـایبر، ایجـاد امکـان بـرای بـه‌دسـت آوردن اطلاعات حساس نظامی است. بر این اساس، برخلاف گذشـته و جاسوسـی نظـامی در معنای سنتی، که محدودیت و محذورات حرف اول را مـی‌زنـد، در چـارچوب جدیـد، عمـلاً انقلابی صورت گرفته؛ که تحت تأثیر آن، فضای کمتری برای پنهان‌کردن اطلاعات و مکان‌های حساس نظامی وجود دارد. جاسوسی نظامی سایبری، به مجموعه اقداماتی گفته می‌شود، که بـا توسل به فرصت‌ها و امکانات انقلاب سایبری، با هدف کسب هرگونه اطلاعات حساس مـورد نیاز نظامی از کشورها یا سایر بازیگران فعال از جملـه گـروه‌هـای جنایـت‌کـار بـین‌المللـی یـا تروریست‌ها، صورت می‌گیرد. بنابراین، از حیث هدف، تفاوتی بین جاسوسی نظامی در معنـای سنتی و جاسوسی سـایبری نظـامی وجـود نـدارد. در هـر دو مـورد، در نهایـت هـدف کسـب اطلاعات نظامی است. با این حال، آنچه جاسوسی نظامی سایبری را متفاوت می‌کند، توسل بـه امکانات و فرصت‌هایی است، که انقلاب سایبری مهیا کرده است.

لازم به ذکر است که برای کشورهای مختلف به‌خصوص آنهایی که رقیب یا دشمن هستند، کسب اطلاعات نظامی، ضروری محسوب می‌شود. در واقع، اطلاعات کامل از تـوان، آمـادگی، مراکز، راهبردها، تاکتیک‌ها، فرمانـدهان، خریـدهای تسـلیحاتی و مسـائلی از ایـن قبیـل، کلیـد موفقیت در فضای صلح و جنگ محسوب می‌شود. به همین دلیل، کشورهای مختلـف همـواره بخشی از توان اطلاعاتی و امنیتی خود را صرف به‌دست آوردن اطلاعات مهم نظامی از سایرین

و به‌خصوص کشورهای دشمن می‌کنند. در این زمینه، می‌توان به رقابت‌های گسترده جاسوسی آمریکا و اتحاد جماهیر شوروی در دوران جنگ سرد اشاره کرد. به هر حال، در چنین فضای از اهمیت و ضرورت، فضای سایبر عملاً شرایط را به گونه‌ای رقم زده، که کشورهای توانمند در این عرصه، کم‌وبیش با کمترین هزینه انسانی و مادی و همچنین کمترین خطر می‌توانند به اطلاعات مورد نظر دست یابند. بی‌تردید برخلاف گذشته، که در جاسوسی، محدودیت‌های زمانی و مکانی و به‌خصوص محدودیت‌های انسانی حرف اول را می‌زد، در دنیای امروز، در صورت داشتن دانش و تبحر لازم، عملاً محدودیت‌ها می‌توانند تبدیل به فرصت شود (Vincent, 2014).

۳. جاسوسی سایبری اقتصادی و صنعتی

جاسوسی صنعتی اشاره به مجموعه اقداماتی دارد، که توسط کشورها و گاهاً شرکت‌های مختلف، با هدف کسب دانش، تجربه، اطلاعات و به تعبیری چم‌وخم فعالیت‌های پیشرو در اقتصاد و صنعت، صورت می‌گیرد. در این زمینه، می‌توان به رقابت‌های صنعتی و اقتصادی و در نتیجه، جاسوسی‌های صنعتی گسترده در دهه‌های اخیر بین کشورهای مختلف از جمله آمریکا و اتحادجماهیر شوروی، چین و شوروی و اخیراً چین علیه آمریکا اشاره کرد. بر اساس اطلاعات منتشر شده توسط دولت آمریکا، دولت و شرکت‌های چینی بزرگترین سطح و میزان جاسوسی صنعتی را در جهان علیه کشورهای اروپایی و آمریکا سامان داده‌اند (Williams, 2014: 1).

اصولاً جاسوسی صنعتی در گذشته به گستردگی وجود داشته و یکی از حوزه‌های برجسته جاسوسی و رقابت بین کشورهای مختلف بوده است. با این حال، فضای سایبر همچون سایر حوزه‌ها، عملاً انقلابی در این عرصه ایجاد کرده، به‌شکلی که برای تبیین این تحول جدید، از مفهوم جاسوسی سایبری صنعتی استفاده می‌شود. در واقع، همچون سایر حوزه‌ها و ابعاد، ایجاد فرصت و امکان گسترده برای جاسوسی، یکی از تأثیرات انقلاب‌گونه فضای سایبر برای جاسوسی در این عرصه محسوب می‌شود. بر این اساس، برخلاف گذشته که شرکت‌ها و مراکز مهم صنعتی و اقتصادی در زمینه حفظ اطلاعات و دانش حساس خود، دست بالا را داشتند، امروزه این مهاجمان هستند که به‌واسطه دسترسی به فضای سایبر، دست بالا را دارند. در این

زمینه، می‌توان به اطلاعات منتشرشده توسط دولت و مراکز مختلف آمریکایی اشاره کرد؛ که نشان‌دهنده سطح وسیعی از موفقیت در عرصه جاسوسی سایبری برای مهاجمان، به‌خصوص دولت و شرکت‌های چینی، است. نگاهی به دستاوردهای اقتصادی چین که به باور بسیاری حداقل بخشی از آن‌ها ناشی از کپی‌برداری از دانش شرکت‌های غربی است، خود گویای این مطلب است (ONCIX Reports to Congress, 2011: 5).

تحول دیگری که در جاسوسی صنعتی سایبری در مقایسه با جاسوسی صنعتی سنتی می‌توان مشاهده کرد، تعدد بازیگران در کنار بازیگران دولتی است. در واقع، در جاسوسی صنعتی سنتی، معمولاً نقش دولت‌ها برجسته است. بر این اساس، در جاسوسی صنعتی یا دولت‌ها به‌شکل مستقیم از طریق سیستم‌های اطلاعاتی و جاسوسی خود، برای به‌دست آوردن اطلاعات و دانش صنعتی و اقتصادی دست به اقدام می‌زنند یا اینکه عملاً از اقدام شرکت‌ها و مراکز صنعتی فعال در این حوزه حمایت می‌کنند. محدودیت‌ها و محذورات گسترده‌ای در عرصه جاسوسی صنعتی در معنای سنتی وجود داشت که باعث می‌شد تنها دولت‌ها توانایی، تجربه و دانش لازم برای ورود به آن را داشته باشند.

با وجود این، در عرصه جاسوسی سایبری صنعتی، عملاً فضا برای ورود سایر بازیگران مهیاست. به‌عنوان نمونه، بر اساس اطلاعات موجود، بسیاری از شرکت‌های چینی به‌جای «سرمایه‌گذاری برای تحقیق و توسعه»، عملاً بخشی را برای جاسوسی صنعتی از غرب ایجاد کرده‌اند، که عمدتاً با توسل به فضای سایبری صورت می‌گیرد. در این زمینه، حتی شرکت‌های مافیایی تشکیل شده، که دست به جاسوسی سایبری می‌زنند و اطلاعات سرقت‌شده را به شرکت‌های مختلف می‌فروشند (ONCIX Reports to Congress, 2011:4-5).

نتیجه‌گیری

انقلاب سایبری عملاً حجاب را در عرصه‌های مختلف سیاسی، اقتصادی، صنعتی، علمی، پژوهشی، اجتماعی و فرهنگی برداشته و شرایط را چنان مهیا نموده، که امروزه کشورهای مختلف آسان‌تر از گذشته می‌توانند به اطلاعات همدیگر دست یابند. بنابراین، اولین نتیجه انقلاب سایبری در حوزه جاسوسی، گستردگی امکان جاسوسی در حوزه‌ها و عرصه‌های

مختلف است. ضمن اینکه انقلاب سایبری، در کنار دولت‌ها، فضا را برای سایر بازیگران ذینفع در اقتصاد و صنعت، همچون شرکت‌های بزرگ چند میلیتی و همچنین تروریست‌ها و گروه‌های فعال در جرایم بین‌الملل و هکرها مهیا کرده تا به اطلاعات مهم و دلخواه دست یابند. بنابراین، نتیجه دیگر انقلاب سایبری، ایجاد امکان جاسوسی برای بازیگرانی به غیر از دولت‌هاست.

یکی دیگر از نتایج انقلاب سایبری، فرارفتن جاسوسی از بُعد زمان و مکان است. بدین معنا، انقلاب سایبری چنان شرایط را تغییر داده، که عملاً امکان جاسوسی از هر مکان و در هر زمانی کم‌وبیش مهیا شده است. این در شرایطی است که در جاسوسی سنتی، محدودیت‌های زمانی و مکانی همیشه مشکل اساسی و جدی بودند. بدین ترتیب، انقلاب سایبری، گستره جاسوسی را در ابعاد مختلف شدت بخشیده و ابعاد، حوزه‌ها و بازیگران جدیدی را به آن اضافه کرده است. بر این اساس، می‌توان گفت همچون عرصه نظامی، که از «انقلاب در عرصه نظامی» صحبت می‌شود، می‌توان از انقلاب در عرصه اطلاعاتی نیز سخن گفت.

منابع

خلیلی‌پور رکن‌آبادی، علی و نورعلی‌وند، یاسر (۱۳۹۱) «تهدیدات سایبری و تأثیر آن بـر امنیـت ملـی»، **فصـلنامه مطالعات راهبردی**، سال پانزدهم، شماره دوم.

Angela Merkel's call to Obama: are you bugging my mobile phone? (2014) at:http://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german

Benner, Katie (2015) **Benner on Tech: Cyber Spying Road Rules**, at: http://www.bloombergview.com/articles/2015-02-20/benner-on-tech-cyber-spying-road-rules

Braff, T. Andrew (2005) **Defining Spyware: Necessary or Dangerous**,1-10 at:https://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/365/vol2_no1_art1.pdf?sequence=1

Choucri, Nazli (2012),**Cyberpolitics in International Relations,** The MIT Press Cambridge, Massachusetts London, England

Cyber spying definition (2015), at: http://lexicon.ft.com/Term?term=cyber-espionage

Cyberspying, Definition - What does Cyber spying mean (2015), at:http://www.techopedia.com/definition/27101/cyberspying (1393.11.10)

Davies, Simon (2014) **A Crisis of Accountability A global analysis of the impact of the Snowden revelations**, at: http://www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf

Definition of cyber espionage (2013) at: http://resources.infosecinstitute.com/cyber-exploitation/

Favre Slater, William (2014) **The Edward Snowden NSA Data Breach of 2013: How it happened, and its consequences and implications for the U.S. and the IT Industry**, at: http://www.billslater.com/snowden/The_Edward_Snowden_2013_Data_Breach_by_W_F_Slater_for_Forensecure_2014_v02.1_.pdf

Internet Users (2015) at: http://www.internetlivestats.com/internet-users/

Josh M. Cartin (2014) Don't Forget the Humans: Toward a 21st Century Offensive Cyber Strategy, at: http://globalsecuritystudies.com/Cartin%20Cyber%20AG.pdf

Newton, Lee (2013) **Counterterrorism and Cyber security, Total Information Awareness**, Springer New York Heidelberg Dordrecht London

ONCIX Reports to Congress: Foreign Economic and Industrial Espionage (2011) at: http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

Schneier, Bruce (2014) When Does Cyber Spying Become a Cyber Attack?, at: http://www.defenseone.com/technology/2014/03/when-does-cyber-spying-become-cyber-attack/80206/

St Sauver, Joe (2008) **Cyber War, Cyber Terrorism and Cyber Espionage**, at: http://pages.uoregon.edu/joe/cyberwar/cyberwar.pdf

Sterken, Robert (2013) **The Digital Revolution in International Relations: Chinese Accused of Widespread Cyber-Espionage**, at: http://community.cengage.com/GECResource2/info/b/intl_relations/archive/2013/05/07/the-digital-revolution-in-international-relations-chinese-accused-of-widespread-cyber-espionage

Swicegood, J. David (2014) **State-Sponsored Intrusion and Cyber-Terrorism**, at:http://www.giac.org/paper/gsec/3916/state-sponsored-intrusionandcyber-terrorism/106263

Theohary, Catherine and Rollins, John (2015) Cyber warfare and Cyber terrorism: In Brief, at: http://fas.org/sgp/crs/natsec/R43955.pdf

Vincent, Michael (2014), **United States charges Chinese military officials over cyber spying, corporate espionage**, at: http://www.abc.net.au/news/2014-05-19/us-charges-chinese-military-with-cyber-spying/5463492

What does Cyber spying mean (2015), at:
http://www.techopedia.com/definition/27101/cyberspying

Williams, Pete (2014) **US charges China with cyber-spying on American firms**, at: http://www.cnbc.com/id/101684269#.

Wilson, Clay (2008), **Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress**, at: http://fas.org/sgp/crs/terror/RL32114.pdf