مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

عصر فضای مجازی
سی و یکم

# درآمدی بر جنگ اقتصادی سایبری

An Introduction
to Cyber-Enabled Economic Warfare


# عصر فضای مجازی

گزارش شماره ۳۱
بهمن ۱۳۹۹

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

# درآمدی بر جنگ اقتصادی سایبری

**محتوای انتشار یافته در این اثر**
**الزاماً بیانگر دیدگاه مرکز ملی فضای مجازی نیست**


**تهیه شده در پژوهشگاه فضای مجازی**
(گروه مطالعات اقتصادی)

تهیه کننده: امیر عزیزی (دانشجوی دکتری دانشگاه تهران و عضو اندیشکده سیاستگذاری اقتصادی تهران)
ناظر علمی: دکتر مهدی نوری (دکتری اقتصاد و مدرس دانشگاه تهران)





نشانی: تهران، میدان آرژانتین، خیابان بیهقی، نبش خیابان ۱۶غربی، پلاک ۲۰
تلفن: ۰۲۱-۸۶۱۵۱۰۶۱
کد پستی: ۱۵۱۵۶۷۴۳۱۱

# فهرست

# سخن نخست

# سخن نخست

فضای مجازی با شتاب شگرف و رو به تزایدی که در حال بسط و گسترش است تمام ساحات اجتماعی، اقتصادی، سیاسی و فرهنگی زندگی بشر را درنوردیده و هر روز بخش بزرگی از زندگی واقعی را در خود فرو برده و حیات متفاوت و جدیدی به آن می‌دهد. لذا به نظر می‌رسد دو نگاه کلان به فضای مجازی وجود دارد: نگاه اول که بالاخص در ابتدای رشد و تکوین فضای مجازی مسلط شده بود، آن را همچون ابزاری کنار سایر ابزارهای بشری تصویر می‌کرد که تنها طریقیت داشت. اما نگاه دوم، در نتیجه رشد تحولات خیره‌کننده فضای مجازی و سایه گستری آن در حوزه‌ها و شئون بشر در یک دهه اخیر آن را چون سکویی می‌داند که بسیار فراتر از شأن ابزاری حیات انسان‌ها را سامان جدیدی داده و ادعای تمدن نوینی را دارد. رویکردی که از قضا از چشمان بصیر رهبر انقلاب نیز دور نمانده و انتظاری تمدنی از فضای مجازی در ایران را مطالبه داشته‌اند.

در همین راستا گزارش‌های عصرفضای مجازی تلاش می‌کند تا فهم سازمان‌ها و دستگاه‌های مرتبط با حوزه فضای مجازی را ارتقاء بخشیده و آن‌ها را برای مواجهه فعال و خردمندانه با تحولات این عرصه مهیا سازد.

سید ابوالحسن فیروزآبادی
دبیر شورای عالی و رئیس مرکز ملی فضای مجازی

# چکیده

# چکیده

جهان شاهد نوع جدیدی از جنگ است؛ جنگی که نه با استفاده از تسلیحات نظامی متداول، بلکه با بهره‌جویی از نظامات و روابط اقتصادی و مالی و با استفاده از سخت‌افزارها و نرم‌افزارهای ارتباطاتی و اطلاعاتی انجام می‌شود. امروزه، زرادخانه جنگ اقتصادی در کنار انبوهی از روش‌های قدیمی، ابزارهای نوآورانه جدید را نیز در بر می‌گیرد. ابزارهای نوآورانه جدید جنگ اقتصادی منعکس‌کننده نظامات اقتصادی و مالی مدرن فعلی است. با ابتنای هر چه بیشتر نظامات اقتصادی و مالی بر فضای سایبر، میدان جنگ اقتصادی به این فضا گسترش یافته و ابزارهای جنگ سایبری نیز به ابزارهای قدیمی‌تر جنگ اقتصادی اضافه شده است. حملات و عملیات‌های سایبری می‌توانند باعث انواع مختلفی از لطمات اقتصادی شوند که ممکن است از حیث پیامدهای منفی و هزینه‌های اقتصادی با پیامدهای منفی و هزینه‌های اقتصادی جنگ‌های نظامی قابل مقایسه باشد. اگرچه جنگ اقتصادی سنتی و جنگ سایبری هر دو

به طور گسترده مورد مطالعه قرار گرفته‌اند، اما همپوشانی بین این دو حوزه از جنگ، که از آن با عنوان جنگ اقتصادی سایبری اطلاق می‌شود، هنوز آن گونه که باید مورد توجه قرار نگرفته است. جنگ اقتصادی سایبری به عنوان راهبردی جنگ‌طلبانه مشتمل بر حملات علیه یک کشور با استفاده از فناوری‌های سایبری به قصد تضعیف قدرت سیاسی و نظامی آن کشور از طریق تضعیف اقتصاد آن تعریف می‌شود. هدف این گزارش معرفی جنگ اقتصادی سایبری در قالب ارائه مجموعه‌ای از تعاریف برای مفاهیم مرتبط با این نوع جنگ است. همچنین، در این گزارش برخی از مهم‌ترین مصادیق واقعی جنگ اقتصادی سایبری به اختصار مورد بررسی قرار خواهد گرفت. علاوه بر این، برخی از مهم‌ترین فعالیت‌های کشورهای ایالات متحده آمریکا، چین، روسیه، کره شمالی و ایران، که از مهم‌ترین بازیگران عرصه جنگ اقتصادی سایبری محسوب می‌شوند، بررسی خواهد شد.

**واژگان کلیدی:** جنگ اقتصادی، جنگ سایبری، جنگ اقتصادی سایبری، دفاع سایبری، بازدارندگی سایبری

# مقدمه

# مقدمه

اگرچه استفاده از تهاجم اقتصادی علیه دشمنان، قدمتی به اندازه ایجاد نظام‌های اقتصادی دارد، اما تاکتیک‌های جنگ اقتصادی[1] با گذشته زمان پیشرفت کرده‌اند. طی دهه‌های اخیر، با شروع عصر اطلاعات و گسترش فضای سایبر[2]، به ویژه لایه شخصیت سایبری[3] آن، روندهای جدیدی در حوزه جنگ اقتصادی در حال شکل‌گیری است. جهان شاهد نوع جدیدی از جنگ است، جنگی نه با استفاده از تسلیحات نظامی متداول، بلکه با استفاده از روابط اقتصادی و مالی و سخت‌افزارها و نرم‌افزارهای ارتباطاتی و اطلاعاتی. امروزه، زرادخانه جنگ اقتصادی در کنار انبوهی از روش‌های قدیمی، ابزارهای نوآورانه جدیدی را نیز در بر می‌گیرد. ابزارهای نوآورانه جدید منعکس‌کننده نظام‌های اقتصادی و مالی مدرن فعلی است. حملات سایبری و حملات سایبرممکن[4] می‌توانند باعث انواع مختلفی از لطمات اقتصادی شوند که ممکن است پیامدهای منفی و هزینه‌های اقتصادی آن‌ها با پیامدهای منفی و هزینه‌های اقتصادی جنگ‌های نظامی قابل

1.Economic warfare
2.Cyberspace
3.Cyber-persona
در بخش ۳،۱ منظور از شخصیت سایبری و جایگاه آن به عنوان لایه‌ای از فضای سایبر توضیح داده شده است.
4.Cyber-enabled attacks
منظور از حملات سایبرممکن حملاتی است که به لطف وجود فضای سایبر امکان‌پذیر شده‌اند.

مقایسه باشد. گسترش اقتصاد مبتنی بر فضای سایبر در حال تغییر دادن ویژگی‌های جنگ اقتصادی است و فضای سایبر در حال تبدیل شدن به یکی از اصلی‌ترین میدان‌های نبرد[1] است. اگرچه جنگ اقتصادی سنتی و جنگ سایبری[2] هر دو به طور نسبتاً گسترده مورد مطالعه قرار گرفته‌اند، اما همپوشانی بین این دو موضوع هنوز آن گونه که باید مورد توجه قرار نگرفته است. برای درک سیر تطوّر جنگ اقتصادی در چهارچوب واقعیت‌های جدید ناشی از وجود فضای سایبر به مطالعات گسترده‌ای نیاز است. با ظهور اقتصاد جهانی شبکه‌ای، ادغام و وابستگی متقابل بین بخش‌های تشکیل‌دهنده آن، دولت‌ها و بازیگران غیردولتی[3] مشغول توسعه روش‌ها و راهبردهای جدید مرتبط با جنگ اقتصادی هستند. هم دولت‌ها و هم کنشگران غیردولتی به طور فزاینده‌ای قادر به برنامه‌ریزی و انجام حملات سایبری هولناک علیه دارایی‌ها و نظامات اقتصادی حیاتی دشمنان‌شان هستند و از این طریق امنیت ملی و قابلیت‌ها و توانمندی‌های نظامی آن‌ها را هدف قرار می‌دهند. این نوع جدید از تهدیدها جنگ اقتصادی سایبرممکن[4] (به اختصار، جنگ اقتصادی سایبری) نامیده می‌شود. هدف این گزارش معرفی جنگ اقتصادی سایبری در قالب ارائه مجموعه‌ای از تعاریف برای مفاهیم مرتبط با این نوع جنگ و نیز مروری بر برخی از مهم‌ترین مصادیق واقعی جنگ اقتصادی سایبری است. جنگ اقتصادی سایبری به راهبردی جنگ‌طلبانه مشتمل بر حملات علیه یک کشور با استفاده از فناوری سایبری به قصد

1.Battlefield
2.Cyber warfare
3.Non-state actors
۴.در روابط بین‌الملل، کنشگران غیردولتی اشخاص یا گروه‌هایی از اشخاص تاثیرگذار هستند که یا کاملاً یا نسبتاً از دولت‌ها مستقل هستند. شرکت‌های چندملیتی، رسانه‌های بین‌المللی، ثروتمندان منتفذ، سازمان‌های مردم‌نهاد، جنبش‌های مردمی، جنبش‌های آزادی‌بخش و گروه‌های مذهبی ذی‌نفوذ از جمله کنشگران غیردولتی محسوب می‌شوند.

تضعیف اقتصاد آن و از این طریق تضعیف قدرت سیاسی و نظامی آن اطلاق می‌شود (راویش و فیکسلر[1]، ۲۰۱۷). در سال‌های اخیر، ایران هدف انواع مختلفی از حملات سایبری بوده که ذیل مفهوم جنگ اقتصادی سایبری قابل طبقه‌بندی است. جلوگیری از دسترسی بانک‌ها و موسسات مالی اعتباری غیربانکی ایرانی به سامانه سوئیفت[2] نمونه‌هایی از جنگ‌های اقتصادی (مالی) سایبری تحمیلی به ایران بوده است. برای اطمینان یافتن از این که امنیت و منافع ملی کشور در چنین شرایطی حفظ و تامین می‌شود، به دکترین‌ها[3]، ابزارهای تحلیلی و راهبردها و سیاست‌ها جدیدی نیاز است. در عین حال، ایران در کنار کشورهای آمریکا، چین، روسیه و کره شمالی به عنوان یکی از فعال‌ترین بازیگران در عرصه جنگ اقتصادی سایبری در نظر گرفته می‌شود (کاخ سفید، ۲۰۱۸). این موضوع باعث می‌شود که آشنایی با مقوله جنگ اقتصادی سایبری ضرورت مضاعف یابد. برای این منظور، در بخش دو گزارش حاضر، مهم‌ترین مفاهیم پیرامون جنگ اقتصادی مورد بررسی قرار می‌گیرد. سپس، در بخش سه، برخی از مهم‌ترین مفاهیم مرتبط با جنگ سایبری به اختصار معرفی می‌شود. در بخش چهار، ویژگی‌های جنگ اقتصادی سایبری و شرایطی که به موجب آن یک حمله به عنوان جنگ اقتصادی سایبری طبقه‌بندی می‌شود، بررسی می‌شود. همچنین، در این بخش، برخی از مهم‌ترین فعالیت‌های ایالات متحده آمریکا، چین، روسیه، کره شمالی و ایران در حوزه جنگ اقتصادی سایبری مورد بررسی قرار می‌گیرد. در بخش پنج، جمع‌بندی گزارش ارائه می‌شود.

1.Ravich and Fixler
2.Society for Worldwide Interbank Financial Telecommunication (SWIFT)
3.Doctrine
به اصول بنیادین که نحوه استفاده از نیروها در اقدام هماهنگ به سمت هدفی مشترک را تعیین می‌کند، دکترین اطلاق می‌شود.

# بخش اول

# بخش اول

## درآمدی بر جنگ اقتصادی

جنـگ اقتصـادی عبـارت اسـت از اسـتفاده یـا تهدیـد بـه اسـتفاده از ابزارهـا و روش‌هـای اقتصـادی علیـه یـک کشـور یـا جامعـه بـه منظـور تضعیـف اقتصـاد آن و از ایـن طریـق، کاسـتن از قـدرت سیاسـی و نظامـی آن کشـور یـا جامعـه (شـمبوف[1]، ۱۹۹۸). جنـگ اقتصـادی اسـتفاده از روش‌هـا و ابزارهـای اقتصـادی بـرای وادار کـردن کشـور یـا جامعـه حریـف[2] یـا دشـمن بـه تغییـر دادن سیاسـت‌ها یـا رفتـار خـود یـا تضعیـف توانایـی آن بـرای داشـتن روابـط عـادی بـا سـایر کشـورها یـا جوامـع را نیـز شـامل می‌شـود. جلوگیـری از صـادرات کالاهـا و خدمـات بـه کشـور یـا جوامـع هـدف[3]، خـودداری از واردات کالاهـا و خدمـات از کشـور یـا جوامـع هـدف[4]، قـرار دادن نـام اشـخاص مرتبـط بـا کشـور یـا جوامـع هـدف در فهرسـت اشـخاص ممنـوع معاملـه (فهرسـت سـیاه)[5]، خریـد عمـدی منابـع حیاتـی کمیـاب بـه منظـور ممانعـت از دسترسـی کشـورها یـا جوامـع هـدف بـه آنهـا (خریـد محروم‌کننـده)[6]، عرضـه اقـلام تقلبـی[7] بـه کشـور یـا جوامـع هـدف، خرابـکاری (نظیـر انسـداد، اختـلال، تخریـب و انهـدام) در امکانـات و

1.Shambaugh

2.Adversary اگـر عناصـر طیـف برخـورد بـه صـورت «خـودی، شـریک، رقیـب، حریـف و دشـمن» در نظـر گرفتـه شـوند، حریـف بـه عنـوان عنصری تعریـف مـی شـود کـه سـطح برخـورد بـا آن از دشـمن ضعیـف تـر، امـا از رقیـب قـوی تـر اسـت. حریـف عنصـری اسـت کـه بـه دنبـال برتـری یافتـن از طریـق شکسـت دادن طـرف مقابـل اسـت؛ امـا، دشـمن بـه دنبـال برتـری یافتـن از طریـق نابـود کـردن طـرف مقابـل اسـت

3.Embargo

4.Boycotts

5.Blacklist

6.Preclusive buying

7.Counterfeit

تجهیزات تولیدی[1]، اعمال تبعیض تعرفه‌ای[2] و/یا مالیات‌های تنبیهی[3] علیه کشور یا جوامع هدف، سلب مالکیت[4] از اشخاص حقیقی و حقوقی مرتبط با کشورها یا جوامع هدف، مسدود کردن دارایی‌های مالی کشورها یا جوامع هدف، تعلیق کمک‌های فنی و اعتباری به کشورها یا جوامع هدف، سهمیه‌بندی خرید یا فروش کالا، ممنوعیت سرمایه‌گذاری، محدودیت روی تراکنش‌های مالی و جریان سرمایه و ممانعت از عضویت کشورها یا جوامع هدف در سازمان‌های بین‌المللی تسهیل‌کننده امر تجارت از جمله مهم‌ترین روش‌هایی هستند که در جنگ اقتصادی مورد استفاده قرار می‌گیرند. وقتی جنگ اقتصادی به عنوان بخشی از تنش نظامی مورد استفاده قرار می‌گیرد، جلوگیری از صادرات و واردات به شکل حصر یا محاصره[5] عینیت پیدا می‌کند. جنگ اقتصادی مفهومی گسترده است و می‌تواند انواع متنوعی از تنش-های اقتصادی تخاصمی بین کشورها و جوامع را در بر گیرد. بسته به میدانی که جنگ اقتصادی در آن رخ می‌دهد یا ابزارهایی که برای انجام جنگ اقتصادی مورد استفاده قرار می-گیرد، می‌توان انواع مختلفی از جنگ‌های اقتصادی را تعریف و طبقه‌بندی کرد. عباراتی نظیر جنگ تجاری[6] و جنگ مالی[7] ناشی از همین طبقه‌بندی است. هدف کشورها و جوامعی که اقدام به جنگ اقتصادی می‌کنند، این است که یا از طریق جلوگیری از دسترسی کشورها و جوامع هدف به منابع فیزیکی، مالی و فناورانه، یا از طریق جلوگیری از توانایی این کشورها و جوامع برای نفع بردن از مبادلات تجاری، مالی

1.Sabotage
2.Tariff discrimination
3.Punitive taxation
4.Expropriation
5.Blockade
6.Trade warfare
7.Financial warfare

و فناورانه با سایر کشورها و جوامع، اقتصاد آن‌ها را تضعیف کنند. ممکن است، جنگ اقتصادی به عنوان جایگزین جنگ‌های نظامی مورد استفاده قرار گیرد. در این شرایط، معمولاً، جنگ اقتصادی بخشی از راهبرد گسترده‌تر زمام‌داری اقتصادی[1] کشور یا جامعه‌ای است که اقدام به استفاده از این نوع جنگ می‌کند. همچنین، ممکن است جنگ اقتصادی به عنوان مکمل سایر انواع روش‌های جنگی، نظیر جنگ نظامی و جنگ روانی، مورد استفاده قرار گیرد. در این شرایط، معمولاً، جنگ اقتصادی بخشی از جنگ ترکیبی[2] یا جنگ تمام‌عیار[3] است. زمام‌داری اقتصادی اصطلاحی است که برای اشاره به مجموعه اقدامات کشورها در استفاده از روش‌ها و ابزارهای اقتصادی برای دستیابی به اهداف خود در حوزه سیاست خارجی[4] مورد استفاده قرار می‌گیرد (بالدوین[5]، ۲۰۱۶). ارتباط زمام‌داری اقتصادی با حوزه سیاست خارجی باعث شده است که بعضاً به جای زمام‌داری اقتصادی از اصطلاح دیپلماسی اقتصادی[6] نیز استفاده شود (برای نمونه، ون برگئیجک و مونس[7]، ۲۰۰۹)، اما باید توجه داشت که در مقایسه با دیپلماسی اقتصادی، زمام‌داری اقتصادی طیف گسترده‌تری از موضوعات را در بر می‌گیرد. زمام‌داری اقتصادی یکی از ارکان اصلی سیاست خارجی و امنیت ملی ایالات متحده آمریکا و جمهوری خلق چین، به عنوان دو ابرقدرت حال حاضر در جهان، است. زمام‌داری اقتصادی به شکل‌های مختلفی اعمال می‌شود. می‌توان روش‌های اعمال زمام‌داری اقتصادی را به دو دسته کلی مجازات‌ها

1.Economic statecraft
2.Hybrid warfare
3.Total war
۴.در مفهوم رایج، اصطلاح زمام¬داری اقتصادی کشورها در نسبت با سیاست خارجی آنها موضوعیت پیدا می کند و برای اشاره به سیاست¬های اقتصادی دولت‌ها در نسبت با سیاست داخلی آنها از اصطلاحات دیگری استفاده می شود.
5.Baldwin
6.Economic diplomacy
7.van Bergijk and Moons

یـا تنبیه‌هـا[1] و مشـوق‌ها یـا حمایت‌هـا[2] تقسـیم کـرد (بالدویـن، ۲۰۱۶). زمـام‌داری اقتصـادی عـلاوه بـر اعمـال واقعـی مجـازات و ارائـه واقعـی مشـوق، می‌توانـد بـه شـکل تهدیـد بـه اعمـال مجـازات یـا تعهـد بـه ارائـه مشـوق نیـز عملیاتـی گـردد. مجازات‌هـای اقتصـادی در چهارچـوب زمـام‌داری اقتصـادی شـامل همـان روش‌هـا و ابزارهایـی می‌شـود کـه در جنـگ اقتصـادی مـورد اسـتفاده قـرار می‌گیـرد. در مقابـل، مالیات‌هـا و تعرفه‌هـای ترجیحـی، اهـدای کمک‌هـای فنـی و اعتبـاری، فراهـم کـردن امـکان دسترسـی بـه کالاهـا و خدمـات، ارائـه تضمیـن بـه سـرمایه‌گذاری خارجـی و پذیـرش عضویـت کشـورها در سـازمان‌های بین‌المللـی تسـهیل‌کننده تجـارت نمونه‌هایـی از مشـوق‌ها هسـتند کـه می‌تواننـد در چهارچـوب زمـام‌داری اقتصـادی مـورد اسـتفاده قـرار گیرنـد. لازم بـه ذکـر اسـت، یکـی از مهم‌تریـن نواقـص طبقه‌بنـدی فـوق ایـن اسـت کـه برخـی از مهم‌تریـن موضوعـات مرتبـط بـا زمـام‌داری اقتصـادی را در بـر نمی‌گیـرد. بـرای نمونـه، جاسوسـی[3] اقتصـادی یـا صنعتـی از رقبـا، حریفـان و دشـمنان کـه معمـولاً در زمـام‌داری اقتصـادی مـورد اسـتفاده قـرار می‌گیـرد و اهمیـت ویـژه‌ای در جنگ‌هـای اقتصـادی سـایبری دارد، نـه بـه عنـوان واکنش‌هـای مثبـت و نـه بـه عنـوان واکنش‌هـای منفـی پیشـنهادی بالدویـن (۲۰۱۶) قابـل طبقه‌-بنـدی اسـت. لازم بـه ذکـر اسـت، جاسوسـی اقتصـادی یـا صنعتـی عبـارت اسـت از (الـف) دسـتیابی بـه اسـرار تجـاری یـا اطلاعـات اختصاصـی یـا سـرقت، تصاحـب، جابجایـی یـا پنهـان کـردن آنهـا از طریـق فریبـکاری و نیرنـگ بـدون مجـوز مالـک

1.Negative sanctions
2.Positive sanctions
3.Espionage

این اسرار و اطلاعات؛ (ب) نسخه‌برداری، بارگذاری، بارگیری، تخریب، انتقال، تحویل، ارسال و مبادله اسرار تجاری[1] یا اطلاعات اختصاصی بدون مجوز مالک این اسرار و اطلاعات؛ یا (ج) دریافت، خرید یا تملک آگاهانه اسرار تجاری یا اطلاعات اختصاصی که ربوده شده یا بدون مجوز مالک این اسرار و اطلاعات، تصاحب شده یا تغییر یافته است (مرکز ملی ضدجاسوسی و امنیت ایالات متحده آمریکا[2]، ۲۰۱۸).

اهداف سیاست خارجی مد نظر در زمام‌داری اقتصادی می‌تواند شامل طیف متنوعی از موضوعات باشند. نکته مهم این که در چهارچوب زمام‌داری اقتصادی می‌توان از یک ابزار واحد برای دستیابی به اهداف متفاوت و بعضاً متضاد استفاده کرد. جلوگیری از جنگ با سایر کشورها یا جوامع، آماده کردن شرایط مناسب برای شروع جنگ با کشورها یا جوامع طرف تخاصم، تضعیف کشورها یا جوامع دشمن در هنگام جنگ با آنها، تشویق کشورها یا جوامع هدف برای شرکت در مذاکره، ترویج نظام سیاسی مورد نظر در کشورها یا جوامع هدف، جلوگیری از استقرار نظام سیاسی غیر همسو در کشورها یا جوامع هدف، حمایت از نظام‌های سیاسی همسو مستقر در کشورها یا جوامع هدف، تضعیف نظام سیاسی غیر همسو مستقر در کشورها یا جوامع هدف، حمایت از توسعه اقتصادی کشور یا جامعه هدف و جلوگیری از توسعه اقتصادی کشور یا جامعه هدف از جمله اهدافی هستند که زمام‌داری اقتصادی برای تحقق آن‌ها اعمال می‌گردد. بسته به عرصه‌ای که زمام‌داری اقتصادی در آن رخ می‌دهد یا ابزارهایی

1.Trade secret
2.National Counterintelligence and Security Center

کـه بـرای ایـن منظـور مـورد اسـتفاده قـرار می‌گیـرد، می‌تـوان انـواع مختلفـی از زمـام‌داری اقتصـادی را تعریـف و طبقه-بنـدی کـرد. عباراتـی نظیـر زمـام‌داری مالـی[1] ، زمـام‌داری پولـی[2] و زمـام‌داری نهـادی[3] ناشـی از همیـن طبقه‌بنـدی اسـت. شـکلی خاصـی از زمـام‌داری اقتصـادی کـه غالبـاً بـه شـکل تحریم‌هـای مالـی و مشـوق‌های مالـی مـورد اسـتفاده قـرار می‌گیـرد، بـه عنـوان زمـام‌داری مالـی طبقه‌بنـدی می‌شـود. زمـام‌داری مالـی ناظـر بـه اقدامـات یـک کشـور بـه اسـتفاده از ظرفیت‌هـای مالـی خـود بـه منظـور دسـتیابی بـه اهـداف سیاسـت خارجـی خـود اسـت (مک‌دوئـل[4] ، ۲۰۱۹). همچنیـن، بـرای اشـاره بـه بخـش خاصـی از زمـام‌داری مالـی کـه بـه موضوعـات پولـی محـدود می‌شـود، از اصطـلاح زمـام‌داری پولـی اسـتفاده می‌شـود (کوهـن[5] ، ۲۰۱۹). زمـام‌داری نهـادی نیـز ناظـر بـه مجموعـه اقدامـات یـک کشـور بـرای ایجـاد نهادهـای بین‌المللـی و اسـتفاده از ظرفیـت ایـن نهادهـا بـه منظـور دسـتیابی بـه اهـداف سیاسـت خارجـی خـود اسـت (ایکنبـری و لیـم[6] ، ۲۰۱۷). معمـولاً، جنـگ اقتصـادی بـه تنهایـی نمی‌توانـد مسـایل مربـوط بـه سیاسـت خارجـی و امنیـت خارجـی کشـورها یـا جوامـع را حـل کنـد، بـه همیـن دلیـل ایـن نـوع از جنـگ در ترکیـب بـا سـایر انـواع جنـگ مـورد اسـتفاده قـرار می‌گیـرد. در گسـترده‌ترین شـکل، جنـگ ترکیبـی بـه تمـام حوزه‌هـای ممکـن بـرای رویارویـی کشـیده می‌شـود. در ایـن حالـت، تنـش بیـن کشـورهای حریـف بـه جنـگ تمام‌عیـار تبدیـل می‌شـود. جنـگ تمام‌عیـار نوعـی از جنـگ اسـت کـه در آن تمـام

1.Financial statecraft
2.Currency statecraft
3.Institutional statecraft
4.McDowell
5.Cohn
6.Ikenberry and Lim

منابع و زیرساخت‌های غیرنظامی به مثابه اهداف مشروع نظامی در نظر گرفته می‌شوند. در این شرایط، تمام منابع کشور یا جامعه درگیر جنگ برای پیشبرد جنگ مورد استفاده قرار می‌گیرد و در مقابل نیازهای غیر جنگی، به نیازهای جنگی اولویت داده می‌شود (ویراستاران دایره المعارف بریتانیکا[1]، ۲۰۱۹). در جنگ تمام‌عیار هیچ محدودیتی در خصوص سلاح‌های مورد استفاده، قلمرو جنگ و شمول جنگجویان و اهداف مد نظر وجود ندارد.

1.Editors of Encyclopaedia Britannica

# بخش دوم

# بخش دوم

## درآمدی بر جنگ سایبری

### ۲-۱-فضای سایبر

برای تبیین ابعاد جنگ اقتصادی سایبری آشنایی با مفاهیم مرتبط با جنگ سایبری نیز ضروری است. جنگ سایبری بر بستر فضای سایبر انجام می‌شود. فضای سایبر به معنی قلمرویی جهانی درون محیط اطلاعاتی[1] متشکل از شبکه‌های دارای وابستگی متقابل متشکل از زیرساخت‌های فناوری اطلاعات و داده‌های موجود در آن است و شامل اینترنت، شبکه‌های مخابراتی، نظامات رایانه‌ای[2] و پردازشگرها و کنترل‌کننده‌های نهفته[3] می‌شود (وزارت دفاع ایالات متحده آمریکا، ۲۰۱۹). منظور از محیط اطلاعاتی، مجموعه تمام اشخاص، سازمان‌ها و سامانه‌هایی است که اقدام به جمع‌آوری، پردازش و انتشار اطلاعات می‌کنند.

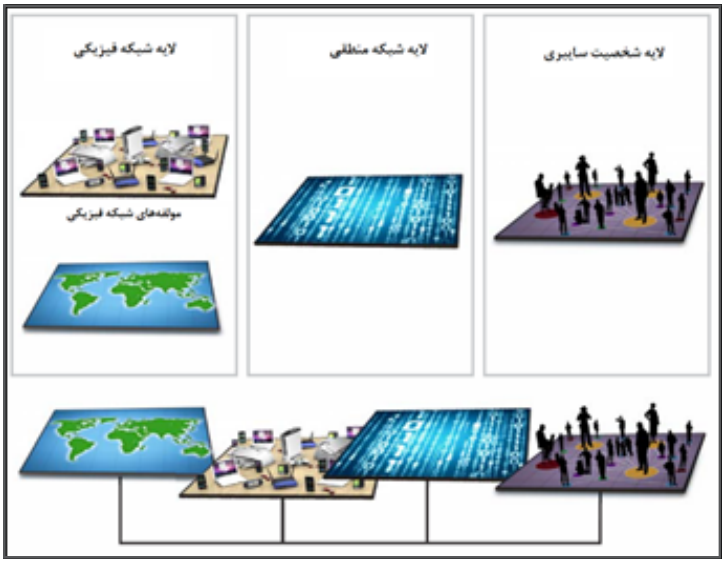
فضای سایبر از لایه‌های مختلفی تشکیل شده است. بر اساس یک طبقه‌بندی، فضای سایبر به سه لایه به هم‌مرتبط شبکه فیزیکی[4]، شبکه منطقی[5] و شخصیت سایبری[6] قابل تقسیم است

1.Information environment
2.Computer systems
3.Embedded processors and controllers
4.Physical network
5.Logical network
6.Cyber-persona

(ستاد مشترک ارتش ایالات متحده آمریکا، ۲۰۱۸). لایه شبکه فیزیکی از دستگاه‌ها و زیرساخت‌های فناوری اطلاعات در حوزه فیزیکی تشکیل می‌شود. این لایه، امکان ذخیره‌سازی، انتقال و پردازش اطلاعات در داخل فضای سایبر را فراهم می‌کند. اگرچه فضای سایبر بخشی از محیط اطلاعاتی است، اما به قلمروهای فیزیکی در هوا، زمین، دریا و فضا وابسته است. لایه شبکه منطقی شامل آن دسته از اجزای مرتبط با شبکه فیزیکی است که بر مبنای برنامه‌نویسی منطقی از شبکه فیزیکی مجزا می‌شود. اجزای مذکور مولفه‌های شبکه را به کار می‌اندازند. این به آن معنی است که روابط لزوماً به اتصالات و گره‌های فیزیکی خاص مرتبط نیست، بلکه به توانایی آنها در این که از نظر منطقی مورد توجه قرار گیرند و داده را مبادله و پردازش کنند، ارتباط دارد. لایه شخصیت سایبری جنبه‌ای از فضای سایبر است که از طریق مجزا کردن داده از لایه شبکه منطقی ایجاد می‌شود. این مجزا کردن با استفاده از قواعدی انجام می‌شود که برای بسط توصیفات مربوط به بازنمایی‌های دیجیتالی هویت یک بازیگر[1] یا موجودیت[2] در فضای سایبر در لایه شبکه منطقه اعمال می‌شود. لایه شخصیت سایبری شامل حساب‌های کاربری و روابط آن‌ها با یکدیگر است. به عبارت دیگر، لایه شخصیت سایبری مشتمل بر مردمان تحت شبکه است؛ مردمانی که عملاً بخشی از شبکه شده‌اند. در واقع، لایه شخصیت سایبری، لایه اجتماعی فضای سایبر است. نسبت بین سه لایه‌ی

1.Actor
2.Entity

مجـزا ولـی بـه هـم مرتبط فضای سـایبر در شـکل ۱ نشـان داده شـده اسـت.




شکل ۱: سه لایه‌ی مجزا ولی به هم مرتبط فضای سایبر
ماخذ: ستاد مشترک ارتش ایالات متحده آمریکا (۲۰۱۸)

بـا گسـترش رو بـه فزونـی فضـای سـایبر، ایـن فضـا در تمـام لایه‌هـا در حـال تبدیـل شـدن بـه میـدان رقابـت، تخاصـم و نبـرد بیـن رقبـا، حریفـان و دشـمنان اسـت. در ادامـه ایـن بخـش، مفهـوم جرایـم سـایبری، حملـه سـایبری، عملیـات سـایبری، جاسوسـی سـایبری، خرابـکاری سـایبری، تروریسـم سـایبری، جنـگ اطلاعاتـی سـایبری، قـدرت سـایبری، تهدیـد سـایبری، امنیـت سـایبری، دفـاع سـایبری، بازدارندگـی سـایبری و تـاب‌آوری سـایبری، کـه برخـی از مهم‌تریـن

مفاهیم مرتبط با جنگ سایبری هستند، مورد بررسی قرار می‌گیرد.

## ۲-۲-جرایم سایبری

با گسترش اقتصاد دیجیتال و افزایش وابستگی فعالیت‌های اقتصادی به فضای سایبر، تعداد، اندازه و پیچیدگی جرایم سایبری نیز در حال افزایش بوده است. برآورد می‌شود که ارزش در معرض خطر[1] در برابر جرایم سایبری طی پنج سال آینده (۲۰۱۹ تا ۲۰۲۳) بالغ بر ۵,۲ تریلیون دلار ایالات متحده آمریکا شود (بیسل و فونمون[2]، ۲۰۱۹). جرایم سایبری شامل (۱) دسترسی غیرمجاز به شبکه‌ای سایبری به منظور سرقت، تخریب یا تغییر اطلاعات، کلاه‌برداری، اخاذی یا تخریب دارایی (به شکل فیزیکی یا به صورت مجازی) یا (۲) ممانعت از دسترسی کاربران ذی‌حق به یک شبکه می‌شود (راویش و فیکسلر، ۲۰۱۷). جرایم سایبری مقوله‌ای گسترده است و می‌تواند شامل فعالیت‌هایی که به عنوان جاسوسی سایبری و تروریسم سایبری طبقه‌بندی می‌شوند، نیز گردد. وقتی جرایم سایبری برای دستیابی به اهداف راهبردی گسترده‌تر به منظور تضعیف توانمندی‌های اقتصادی یک کشور یا جامعه با هدف صدمه زدن به ظرفیت امنیت ملی یا خارجی آن مورد استفاده قرار گیرند، نوعی تاکتیک[3] در چهارچوب طرح جنگ اقتصادی سایبری محسوب می‌شوند. به این ترتیب، معیار اصلی برای طبقه‌بندی حملات سایبری به عنوان جرایم سایبری یا جنگ اقتصادی سایبری، نیت مهاجمان است.

---

1.Value at risk
2.Bissell and Phonemon
3.Tactics
تاکتیک عبارت است از استفاده از نیروها و سازمان‌دهی ترتیبی آنها در ارتباط با یکدیگر.

استفاده از یک مثال، به درک بهتر تمایز جنگ اقتصادی سایبری از جرایم سایبری کمک می‌کند. در فوریه ۲۰۱۶، هکرهای امنیتی[1] مرتبط به کره شمالی (راویش و فیکسلر، ۲۰۱۷)، مجموعه‌ای از درخواست‌های ساختگی برای انتقال ۱ میلیارد دلار از حسابی متعلق به بانک مرکزی بنگلادش به چند حساب خصوصی در سری لانکا و فیلیپین را به فدرال رزرو نیویورک[2] ارسال کردند. در این حمله، سارقان به سامانه پیامرسان الکترونیکی سوئیفت بانک مرکزی بنگلادش نفوذ کردند و پیش از آن که سامانه‌ها در نیویورک بتوانند رد انتقالی‌ها را بگیرند، توانستند ۸۱ میلیون دلار را سرقت کنند. حمله سایبری مذکور، که با عنوان سرقت سایبری از بانک مرکزی بنگلادش[3] شناخته می‌شود، نمونه‌ای از جرایم سایبری است. به نظر می‌رسد این حمله مانند حملات سایبری مشابه دیگری که با استفاده از فریبکاری و سرقت هویت انجام می‌شود، صرفاً نوعی سرقت سایبری بوده که هدف آن ربودن پول بوده است. به عبارت دیگر، مهاجمان قصد صدمه زدن به ظرفیت امنیت ملی بنگلادش از طریق تضعیف توانمندی‌های اقتصادی این کشور از مجرای صدمه زدن به ظرفیت امنیت سایبری بانک مرکزی این کشور را نداشتند. در اکتبر ۲۰۱۷، حمله‌ای مشابه به فار ایسترن اینترنشنال بنک[4] تایوان انجام شد. در این حمله، مهاجمان به تاییدیه‌های سوئیفت بانک مذکور دست یافتند. به نظر می‌رسد این حمله بخشی از حملات گسترده‌تری بود که طی آن‌ها یک بانک تجاری ویتنامی

1.Security hackers
2.Federal Reserve bank of New York
3.Bangladesh Bank cyber heist
4.Far Eastern International Bank

نیز هدف حمله قرار گرفته بود. لازم به ذکر است، حملات سایبری مذکور به کره شمالی نسبت داده می‌شود (ها و مکسول[1] ، ۲۰۱۸). لحاظ کردن حملات مذکور در کنار سایر حملات سایبری منتسب به کره شمالی باعث شکل‌گیری این فرضیه می‌شود که در پس حملات سایبری این کشور اهداف کلان و راهبردی‌تری وجود دارد. با در نظر گرفتن چنین اهدافی، حملات سایبری منتسب به کره شمالی در قالب جنگ اقتصادی سایبری قابل طبقه‌بندی است.

## ۲-۳-عملیات سایبری و حمله سایبری

عملیات سایبری[2] و حمله سایبری از مفاهیم پایه‌ای در جنگ سایبری هستند. عملیات سایبری به معنی استفاده از امکانات و توانمندی‌های سایبری در موقعیت‌هایی است که نیت اصلی در آنها دستیابی به اهدافی مشخص در فضای سایبر یا از طریق این فضا است (ستاد مشترک ارتش ایالات متحده آمریکا، ۲۰۱۸). منظور از امکانات و توانمندی‌های سایبری نیز سخت‌افزارها و نرم‌افزارهایی است که برای تاثیرگذاری در فضا مجازی یا از طریق فضای مجازی طراحی شده‌اند. عملیات سایبری از اتصالات و گره‌های موجود در حوزه‌های فیزیکی استفاده و دستورات محاسباتی منطقی را اجرا می‌کند تا ابتداً تاثیراتی را در فضای سایبر و سپس، در صورت نیاز، تاثیراتی را در حوزه‌های خارج از فضای سایبر ایجاد کند.

برخی از مهم‌ترین انواع عملیات سایبری، به شکل حمله سایبری

1.Ha and Maxwell
2.Cyberspace operation

انجام می‌شوند[1] . به اقدامات انجام شده در فضای سایبر که تاثیرات ممانعتی[2] (یعنی تضعیف، اختلال یا تخریب) قابل ملاحظه‌ای را در این فضا ایجاد می‌کنند یا دستکاری‌هایی که به انواعی از ممانعت در قلمروی غیرسایبری منتهی می‌شوند و به عنوان شکلی از هدف‌گیری دشمن در نظر گرفته می‌شوند، حمله سایبری اطلاق می‌شود (ستاد مشترک ارتش ایالات متحده آمریکا، ۲۰۱۸). لازم به ذکر است، منظور از قلمروهای غیرسایبری، قلمروهای زمینی، دریایی، هوایی و فضایی است که هنوز به عنوان یکی از لایه‌های فضای سایبر قلمداد نمی‌شوند. با گسترش فضای سایبر، به‌ویژه با توسعه اینترنت اشیا، از سهم قلمرو غیرسایبری کاسته می‌شود.

جاسوسی سایبری، ممانعت از دسترسی به خدمات[3] ، خرابکاری سایبری، تروریسم سایبری و جنگ اطلاعاتی سایبری از مهم‌ترین انواع عملیات سایبری تهاجمی محسوب می‌شوند، که در ادامه مورد بررسی قرار می‌گیرند. لازم به ذکر است، برخی دیگر از انواع عملیات سایبری به شکل دفاع سایبری انجام می‌شوند.

### ۲-۳-۱- جاسوسی سایبری

جاسوسی سایبری عبارت است از: جمع‌آوری و/یا انتقال اطلاعات مرتبط با امنیت ملی؛ جمع‌آوری و تحویل اطلاعات مربوط به امنیت ملی برای کمک به دولت‌های خارجی؛ و افشا یا مبادله اطلاعات طبقه‌بندی شده با استفاده از عملیات سایبری یا افشا یا مبادله

۱.عملیات هایی که به منظور دفاع سایبری انجام می شود نیز عملیات سایبری محسوب می‌شوند.

2.Denial effects

3.Denial-of-service (DoS) attack

اطلاعات طبقه‌بندی شده که از طریق عملیات سایبری تسهیل شده است (راویش و فیکسلر، ۲۰۱۷). شکل خاصی از جاسوسی سایبری، که با عنوان جنگ اطلاعاتی اقتصادی[1] نیز شناخته می‌شود (لیبیکی[2]، ۱۹۹۵) و هدف از آن استفاده از اطلاعات تجاری برای دستیابی به برتری یا سلطه اقتصادی است، کاملاً در چهارچوب جنگ اقتصادی سایبری قابل تعریف است. وقتی جاسوسی سایبری در خدمت دستیابی به اهداف راهبردی گسترده‌تری که با هدف تضعیف پایداری اقتصادی یک کشور به منظور صدمه زدن به ظرفیت امنیت ملی آن انجام شد، نوعی تاکتیک در چهارچوب طرح جنگ اقتصادی سایبری محسوب می‌شود. ممکن است هم دولت‌ها و هم شرکت‌های تجاری هدف جاسوسی سایبری قرار گیرند. در چهارچوب زمام‌داری اقتصادی، که بین امنیت ملی و منافع تجاری شرکت‌ها همسویی وجود دارد، جاسوسی از شرکت‌های تجاری مرتبط با کشور هدف به تهدیدی علیه امنیت ملی آن کشور تبدیل می‌شود. ممکن است هدف از حمله سایبری علیه شرکت‌های تجاری، صرفاً دستیابی به سهم بیشتر از بازار باشد؛ اما، همچنین، ممکن است هدف از چنین حملاتی تضعیف بنیان‌های اقتصادی کشور هدف و تضعیف قابلیت‌ها و امکانات ناظر به امنیت ملی آن کشور باشد. در واقع، جاسوسی سایبری از شرکت‌های یک کشور نه تنها بر عملکرد اقتصادی آن کشور، بلکه بر توانایی آن کشور بر دفاع از خود و اعمال قدرت در خارج از قلمرو خود تاثیر می‌گذارد. یکی از مهم‌ترین مصادیق

1.Economic information warfare
2.Libicki

جاسوسی سایبری مربوط به سرقت دارایی فکری است. کشورها برای تضعیف رقابت‌پذیری کشور هدف یا ارتقای رقابت‌پذیری خود نسبت به سرقت دارایی فکری[1] از آن‌ها اقدام می‌کنند.

### ۲-۳-۲- ممانعت از دسترسی به خدمات

ممانعت از دسترسی به خدمات نوعی حمله سایبری است که در آن مهاجم تلاش می‌کند به طور موقت یا دائم مانع دسترسی کاربران مجاز به نظامات اطلاعاتی، ابزارها و سایر منابع شبکه شود (آژانس امنیت سایبری و امنیت زیرساخت آمریکا ، ۲۰۱۹). در اینجا منظور از خدمات، خدماتی نظیر رایانامه، تارنما و حساب‌های برخط (نظیر حساب‌های بانکی) است. معمولاً ممانعت از دسترسی به خدمات از طریق ایجاد ترافیک بر رایانه میزبان یا شبکه انجام می‌شود تا به این ترتیب، هدف حمله نتواند به درخواست کاربران پاسخ دهد و بنابراین، از دسترسی کاربران مجاز به خدمات جلوگیری شود. معمولاً، در عملیات‌های سایبری از حملات توزیع‌شده ممانعت از دسترسی به خدمات[2] استفاده می‌شود. وقتی برای حمله به منظور ممانعت از دسترسی به خدمات از چندین دستگاه استفاده می‌شود، حمله توزیع‌شده نامیده می‌شود. وقتی حمله ممانعت از دسترسی به خدمات در خدمت دستیابی به اهداف راهبردی گسترده‌تری که با هدف تضعیف پایداری اقتصادی یک کشور به منظور صدمه زدن به ظرفیت امنیت ملی آن انجام شد، نوعی تاکتیک

1.Intellectual property
حق تکثیر، ثبت اختراع، نشان تجاری، طراحی صنعتی، نشان جغرافیایی و اسرار تجاری انواع دارایی فکری محسوب می‌شوند.
2.Distributed denial-of-service (DDos) attack

در چهارچوب طرح جنگ اقتصادی سایبری محسوب می‌شود.

### ۲-۳-۳- خرابکاری سایبری و تروریسم سایبری

در چهارچوب جنگ سایبری، خرابکاری سایبری و تروریسم سایبری دو مفهوم مرتبط هستند. خرابکاری سایبری عبارت است از اقدامی عمدی و بدخواهانه با بهره‌جویی از ظرفیت فضای سایبر که فرآیندها یا کارکردهای معمول شبکه را مختل می‌کند، یا این که تجهیزات یا اطلاعات را نابود یا به آنها صدمه وارد می‌کند (راویش و فیکسلر، ۲۰۱۷). استفاده از بدافزار برای اخلال در فرآیندهای فیزیکی، نظیر تولید برق یا کارکرد معمول سانتری‌فیوژهای هسته-ای یا برای نابودی داده‌های روی نظامات رایانه‌ای یا غیرعملیاتی کردن نظامات رایانه‌ای از مصادیق خرابکاری سایبری محسوب می‌شوند. وقتی خرابکاری سایبری به منظور دستیابی به هدف راهبردی گسترده‌تر تضعیف پایداری اقتصادی یک کشور مورد استفاده قرار گیرد تا از این طریق ظرفیت امنیت ملی آن صدمه ببیند، نوعی تاکتیک در چهارچوب طرح جنگ اقتصادی سایبری محسوب می‌شود.

ایجاد و استفاده از ویروس رایانه‌ای پیچیده‌ای که امروز با نام استاکس‌نت[1] شناخته می‌شود، نمونه‌ای از خرابکاری سایبری است که باعث تخریب فیزیکی شد (راویش و فیکسلر، ۲۰۱۷). این ویروس از سال ۲۰۰۸ به سامانه‌های کنترلی یکی از مراکز اتمی ایران در حوالی شهر نطنز نفوذ و برای مدت ۲ سال به صورت پنهانی فعالیت کرد

1.Stuxnet virus

(زتتر[1] ، ۲۰۱۴). ویروس مذکور، سرعت گردش سانتریفیوژهای اتمی را تغییر داد و باعث کژکاری و در نهایت نابودی آن‌ها شد. اگرچه به طور رسمی تایید نشد، اما اعتقاد بر این است ایالات متحده آمریکا و رژیم صهیونیستی، در همکاری با کشورهای دیگر، این ویروس را ایجاد کرده‌اند. اگرچه به نظر می رسد هدف حمله استاکس‌نت تاثیرگذاری مستقیم بر اقتصاد ایران نبوده و هدف از ایجاد آن تضعیف توانمندی‌های هسته‌ای و نظامی ایران بوده است، اما می‌توان این حمله را به مثابه نوعی خرابکاری صنعتی با هدف صدمه زدن به زیرساخت‌های صنعتی ایران و جلوگیری از توسعه توانمندی‌ها و ظرفیت‌های صنعتی و اقتصادی در کشور نیز در نظر گرفت. بر این اساس، ایجاد و استفاده از ویروس استاکس‌نت را نیز می‌توان به عنوان نمونه‌ای از جنگ اقتصادی سایبری طبقه‌بندی کرد.

حملات سایبری به وزارت نفت ایران و شرکت‌های تابعه آن در اوایل سال ۲۰۱۲ نیز نوعی خرابکاری سایبری بود (کمالی دهقان[2]، ۲۰۱۲). هدف این حملات اعمال فشار اقتصادی بر ایران به منظور تضعیف ظرفیت‌های سیاسی و امنیت ملی کشور بود. به همین دلیل، می‌توان این حمله سایبری را نوعی جنگ اقتصادی سایبری در نظر گرفت. طی این حملات مهاجمان تلاش کردند با استفاده از ویروس رایانه‌ای وایپر[3] حافظه‌های سخت و داده‌های ذخیره شده روی آن‌ها را تخریب کنند. تعریف ارائه شده برای خرابکاری سایبری نوع آسیب ناشی از یک حمله و روش انجام آن را توصیف می‌کند، نه انگیزه‌ای که

1.Zetter
2.Kamali Dehghan
3.Wiper

در پس آن وجود داشته است. برخی از خرابکاری‌های سایبری که با هدف تاثیرگذاری بر تصمیمات دولت‌ها از طریق اعمال تهدید و فشار اجرایی می‌شود را می‌توان به مثابه تروریسم سایبری طبقه‌بندی کرد. به طور کلی، تروریسم عبارت است از استفاده غیرقانونی از خشونت یا تهدید به خشونت به منظور القای ترس و وادار کردن دولت‌ها یا جوامع برای دستیابی به اهدافی که معمولاً سیاسی هستند (ستاد مشترک ارتش ایالات متحده آمریکا، ۲۰۱۸). به طور خاص، تروریسم سایبری عبارت است از استفاده مجرمانه از فناوری اطلاعات برای ایجاد اختلال یا صدمه شدید به منظور تاثیرگذاری بر رفتار یک دولت یا بازیگر غیردولتی از طریق تهدید کردن یا اعمال کردن فشار یا مقابله به مثل کردن در پاسخ به رفتار آن دولت یا بازیگر غیردولتی است (راویش و فیکسلر، ۲۰۱۷). همانند خرابکاری سایبری، وقتی تروریسم سایبری برای دستیابی به هدف راهبردی گسترده‌تر، یعنی تضعیف پایداری اقتصادی یک کشور به منظور تضعیف ظرفیت امنیت ملی آن کشور مورد استفاده قرار گیرد، نوعی تاکتیک در چهارچوب طرح جنگ اقتصادی سایبری محسوب می‌شود. کشورها و گروه‌های تروریستی برای استخدام، تامین منابع مالی، تبلیغات و اجرای حملات از قابلیت‌ها و امکانات سایبری استفاده می‌کنند. غالباً، تروریسم سایبری به عنوان حمله یا تهدید به حمله علیه رایانه‌ها، شبکه‌ها و اطلاعات ذخیره شده در آن‌ها برای فشار بر دولت‌ها یا شهروندان آن‌ها به منظور دستیابی به اهداف

سیاسی یا اجتماعی تعریف می‌شود. اما به نظر می‌رسد تمرکز بر ابزارها و روش‌های مورد استفاده مهاجمان (یعنی، ابزارها و روش‌های سایبری) به جای قلمرویی که مورد حمله قرار گرفته است (یعنی، قلمرو سایبری) برای مباحث مرتبط با امنیت ملی مفیدتر باشد.

حمله سایبری به شرکت سونی پیکچرز اینترتیمنت[1] در اواخر سال ۲۰۱۴، که به کره شمالی نسبت داده می‌شود، می‌تواند به عنوان نمونه‌ای از تروریسم سایبری با پیامدهای اقتصادی در نظر گرفته شود (ها و مکسول، ۲۰۱۸). در این حمله هکرها به شبکه شرکت مذکور نفوذ و حجم بالایی از داده‌های متعلق به آن را سرقت و بخشی از داده‌های این شرکت را نابود کردند. همچنین، مهاجمان تهدید کردند اگر شرکت سونی فیلم کمدی موسوم به «مصاحبه[2]»، که داستان آن در مورد طرح ترور رهبر کره شمالی بود، را منتشر کند، آنها نیز به سالن‌های سینمایی که این فیلم را نمایش می‌دهند، حملات تروریستی به شکل یازده سپتامبر را انجام خواهند داد. به این ترتیب، هم کارکنان شرکت مذکور و هم تماشاکننده بالقوه فیلم با تهدید روبرو شدند. به نظر می‌رسد تهدید مذکور موفقیت‌آمیز بود، چرا که باعث شد شرکت از پخش فیلم در سالن‌های نمایش بزرگ خودداری کند.

### ۲-۳-۴- جنگ اطلاعاتی سایبری

جنگ اطلاعاتی سایبری[3] عبارت است از تاثیرگذاری بر تصمیمات و اقدامات یک کشور خارجی از طریق تاثیرگذاری بر نظرها، عواطف

1.Sony Pictures Entertainment
2. The Interview
3.Cyber-enabled information warfare

و نگرش‌های شهروندان آن کشور با استفاده از ابزارها و روش‌های سایبری (راویش و فیکسلر، ۲۰۱۷). بر مبنای این تعریف، جنگ اطلاعاتی سایبری تا حد زیادی همان جنگ روانی[1] یا عملیات‌های تاثیرگذاری[2] است، که در فضای سایبر انجام می‌شود. در این چهارچوب، رسانه‌های اجتماعی به میدان نبرد جدید در خصوص شکل‌دهی به افکار عمومی و تاثیرگذاری روانی بر دولت‌ها و عموم آحاد جامعه تبدیل شده‌اند. با گسترش فضای سایبر انواع جدیدی از عملیات تاثیرگذاری موضوعیت یافته است. افشای اطلاعات روی اینترنت[3] و به ویژه، شبکه‌های اجتماعی و تغییر ظاهر[4] تمام یا برخی از صفحات تارنما یا حساب کاربری در رسانه‌های اجتماعی بدون کسب اجازه از مسئولان آن‌ها از مصادیق جدید عملیات تاثیرگذاری محسوب می‌شوند. لازم به ذکر است، افشای اطلاعات روی اینترنت ناظر به جستجو و انتشار اطلاعات خصوصی در مورد اشخاص حقیقی و حقوقی است که غالباً با نیات بدخواهانه انجام می‌شود (نیومن[5]، ۲۰۱۷). با گسترش قلمرو فضای سایبر جنگ اطلاعاتی اقتصادی بیش از پیش در قالب جنگ اطلاعاتی سایبری انجام می‌شود. بر این اساس، جنگ اطلاعاتی اقتصادی سایبری عبارت است از تاثیرگذاری بر تصمیمات و اقدامات اقتصادی فعالان اقتصادی یک کشور، اعم از شریک، رقیب، حریف یا دشمن طرف مهاجم از طریق تاثیرگذاری بر نظرها، عواطف و نگرش‌های اقتصادی آنها با استفاده از ابزارها و روش‌های سایبری. معمولاً، هدف از انجام چنین جنگ‌هایی

1.Psychological warfare
2.Influence operations
3.Doxing
4.Defacement
5.Newman

دستیابی به برتری و سلطه اقتصادی طرف خودی است. وقتی جنگ اطلاعاتی سایبری به منظور دستیابی به اهداف راهبری گسترده‌تر تضعیف یک کشور به منظور تضعیف توانمندی امنیت ملی آن مورد استفاده قرار می‌گیرد، به نوعی تاکتیک در چهارچوب اجرای طرح جنگی گسترده‌تر، مثلاً جنگ اقتصادی، تبدیل می‌شود. اقدام منتسب به روسیه در نشر اخبار جعلی به منظور تاثیرگذاری بر شهروندان کشورهایی نظیر آلمان و ایالات متحده آمریکا و رفتار آن‌ها در انتخابات‌های سیاسی از مصادیق جنگ اطلاعاتی سایبری محسوب می‌شود. برای نمونه، در سال ۲۰۱۶ دختری روس برای مدت ۳۰ ساعت در آلمان مفقود شد. وقتی وی به نزد خانواده‌اش بازگشت، ادعا کرد که گروهی از مهاجران خاورمیانه‌ای او را ربوده و مورد آزار و اذیت قرار داده‌اند. به رغم این که بررسی دولت آلمان نشان داد داستان مذکور به آن شکل که دخترک آن را روایت کرده، صحت نداشته است، اما این ادعا به طور گسترده میان جامعه روس‌تباران آلمان، که مخالف تمایل دولت آلمان به پذیرش آوارگان و پناهجویان خاورمیانه‌ای هستند، دست به دست شد. به نظر می رسد هدف از این کارزار تضعیف دولت مستقر در آلمان با استفاده از دستکاری افکار عمومی از طریق رسانه‌های اجتماعی بوده است (تیلور[1]، ۲۰۱۶). در مورد مداخله روسیه در انتخابات ریاست جمهوری سال ۲۰۱۶ نیز شواهدی وجود دارد. در اکتبر ۲۰۱۶، جامعه اطلاعاتی ایالات متحده آمریکا[2] و وزارتخانه امنیت میهن[3] این کشور به طور

1.Taylor

2.United States Intelligence Community (IC)

جامعه اطلاعاتی ایالات متحده آمریکا شامل ۱۷ نهاد اطلاعاتی این کشور است که به صورت جداگانه اما به طور مشترک، برای پشتیبانی از سیاست خارجی و امنیت ملی این کشور فعالیت می‌کنند.

3.Department of Homeland Security

مشترک و علنی روسیه را به حملات سایبری علیه احزاب سیاسی و به منظور تاثیرگذاری بر رقابت‌های مربوط به انتخاب ریاست جمهوری متهم کردند (وزارتخانه امنیت میهن ایالات متحده آمریکا، ۲۰۱۶). عنوان شده که هدف روسیه از این اقدامات تضعیف اعتماد به دموکراسی در ایالات متحده و کمک به شانس انتخاب ترامپ از طریق تضعیف موقعیت رقیب او یعنی کلینتون با استفاده از عملیات تاثیرگذاری بوده است (دفتر مدیر اطلاعات ملی[1] ، ۲۰۱۷).

### ۲-۴-قدرت سایبری

اجرای عملیات سایبری مستلزم داشتن قدرت و توانمندی سایبری است. توانمندی‌های سایبری برای اعمال نفوذ و تاثیرگذاری بر روابط بین‌الملل به عنوان یکی از مولفه‌های قدرت ملی در نظر گرفته می‌شود. قدرت سایبری عبارت است از توانمندی یک بازیگر سایبری برای ممانعت از دسترسی طرف مقابل به فضای سایبر، اختلال در فعالیت سایبری طرف مقابل یا تخریب فضای سایبری طرف مقابل (کراندال و تایر[2]، ۲۰۱۸). قدرت سایبری از دو مولفه اصلی تشکیل می‌شود: توانمندی بهره‌جویی از فضای سایبر[3] و توانمندی عملیات سایبری. بهره‌جویی از فضای سایبر ناظر به اقداماتی است که به منظور جمع‌آوری اطلاعات و مهیا کردن شرایط برای عملیات‌های سایبری انجام می‌شود (وزارت دفاع ایالات متحده آمریکا، ۲۰۱۹).

1.Office of the Director of National Intelligence
2.Crandall and Thayer
3.Cyberspace exploitation

### ۲-۵-تهدید سایبری

تهدید سایبری خطری محتمل است که برای تضعیف امنیت و ایجاد آسیب سایبری، از طریق صدمه زدن به داده‌ها، ربودن داده‌ها یا اختلال در زندگی سایبری، از آسیب‌پذیری‌ها در نظامات سایبری بهره‌جویی می‌کند (تیلور[1]، ۲۰۱۸). در هنگام عملیات سایبری، دولت یا بازیگر غیردولتی با استفاده از قدرت سایبری خود و به منظور تضعیف امنیت و ایجاد آسیب سایبری طرف مقابل اقدام به بهره‌جویی از آسیب‌پذیری‌های طرف مقابل می‌کند. در واقع، اقدام احتمالی دولت‌ها یا بازیگران غیردولتی به بهره‌جویی از آسیب‌پذیری‌های سایبری طرف مقابل که در قالب عملیات سایبری انجام خواهد شد، به مثابه تهدید سایبری در نظر گرفته می‌شود. مثلاً، اقدام احتمالی یک کشور به جاسوسی سایبری از کشور دیگر، تهدید سایبری کشور اول علیه کشور دوم است.

### ۲-۶-جنگ سایبری

جنگ سایبری عبارت است است از اقدامات یک کشور یا یک بازیگر غیردولتی برای حمله و آسیب رساندن به رایانه‌ها یا شبکه‌های اطلاعاتی کشور دیگر با استفاده از روش‌هایی نظیر استفاده از ویروس‌های رایانه‌ای یا حملات با هدف ممانعت از دسترسی به خدمات (رند کورپوریشن[2]، ۲۰۱۹). بر اساس تعریفی دیگر، جنگ سایبری تنشی است که به طور کلی یا جزیی، با استفاده از ابزارهای

1.Taylor
2.Rand Corporation

سایبری انجام می‌شود (راویش و فیکسلر، ۲۰۱۷). هدف اقداماتی که در چهارچوب جنگ سایبری انجام می‌شود تضعیف قابلیت‌ها و امکانات نظامی حریف یا دشمن یا جلوگیری از توانایی آن برای استفاده موثر از سامانه‌های سایبری و تسلیحات خود است. همان طور که پیش‌تر اشاره شد، امکان بروز جنگ سایبری در تمام لایه‌های فضای سایبر وجود دارد.

غالباً، تعاریف ارائه شده برای مفهوم جنگ سایبری چنان گسترده هستند که همه موضوعات از تروریسم سایبری تا جنگ اقتصادی سایبری را در بر می‌گیرند. تفاوت جنگ سایبری از جنگ اقتصادی سایبری این است که جنگ سایبری مستقیماً روی تضعیف ظرفیت‌های نظامی طرف مقابل متمرکز می‌شود، اما هدف از جنگ اقتصادی سایبری ایجاد لطمه اقتصادی به منزله روشی برای تضعیف غیرمستقیم ظرفیت‌های امنیت ملی طرف مقابل است.

بازیگران فعال در حوزه جنگ سایبری، یا راساً اقدام به تشکیل واحدهای جنگ سایبری به منظور اجرای مستقیم عملیات‌های سایبری می‌کنند یا از طریق برون‌سپاری عملیات‌های سایبری به اشخاص و گروه‌های ثالث نسبت به اجرای غیرمستقیم چنین عملیات‌هایی اقدام می‌نمایند. در حوزه امنیت اطلاعات، تهدیدهای ناشی از این واحدها یا گروه‌ها به عنوان تهدید پیشرفته و دائم[1] شناخته می‌شوند. واحدهای جنگ سایبری گروه‌های دولتی یا تحت حمایت مادی و معنوی دولتی یا تحت حمایت مادی و

1.Advanced Persistent Threat (APT)

معنی کنشگران غیردولتی هستند که تلاش می‌کنند به شبکه‌های سایبری هدف دسترسی‌های غیرمجاز داشته باشند و برای دوره زمانی طولانی قابل ملاحظه‌ای ناشناخته باقی بمانند (مالونی[1]، ۲۰۱۸). واحدهای ۶۱۳۹۸[2] و ۶۱۴۸۶[3] ارتش آزادیبخش خلق و الدرود گروپ[4] در چین، لازاروس گروپ[5] در کره شمالی، فنسی بر[6] و کوزی بر[7] و اکوئیشن گروپ[8] در آمریکا نمونه‌ای از گروه‌هایی هستند که به مثابه تهدید پیشرفته و دائم طبقه‌بندی می‌شوند. برخی از کشورها نظیر ایالات متحده آمریکا و جمهوری خلق چین پا را فراتر از این گذاشته و ساختارهای سازمانی گسترده‌تر و منسجم‌تری برای تمشیت امور مرتبط با رزم سایبری ایجاد کرده‌اند. برای نمونه، ایالات متحده اقدام به ایجاد ستاد فرماندهی سایبری[9] کرده است. همچنین، در چین، فرماندهی و مدیریت اجرای عملیات‌های سایبری بر عهده نیروی پشتیبانی راهبرد[10]ی ارتش آزادی‌بخش خلق است که در سال ۲۰۱۵ ایجاد شده است.

دولت‌ها به منابع، نیروهای انسانی و زمانی دسترسی دارند که غالباً برای بازیگران غیردولتی فراهم نیست. به همین دلیل، تهدیدهای سایبری آن‌ها معمولاً، خطرناک‌ترین تهدیدها در حوزه جنگ سایبری محسوب می‌شوند. با وجود این، با توجه به ویژگی‌های فضای سایبر و توانمندی‌های بازیگران غیردولتی، آنها نیز می‌توانند تهدیدهای سایبری قابل ملاحظه‌ای را ایجاد کنند. در برخی موارد حتی ممکن است تهدیدهای سایبری این بازیگران خطرناک‌تر از تهدیدهای

1.Maloney
2.Unit 61398
3.Unit 61486
4.Eldrwood Group
5.Lazarus Group
6.Fancy Bear
7.Cozy Bear
8.Equation Group
9.United States Cyber Command (USCYBERCOM)
10.Strategic Support Force

سایبری دولتی باشد. برای نمونه، اطلاعاتی که دو شرکت‌های بزرگ فناوری نظیر گوگل و فیس‌بوک در خصوص علایق، ترجیحات، باورهای سیاسی و روابط شخصی کاربران خود دارند بیش از نهادهای اطلاعاتی دولتی است (تپر و هارن[1]، ۲۰۱۹). گوگل حدود ۹۰ درصد سهم بازار جستجو در غیر از چین را به خود اختصاص داده است. فیس‌بوک نیز با حدود دو میلیارد کاربر، ۸۰ درصد سهم شبکه‌های اجتماعی را در اختیار دارد. چنین موقعیتی به آن‌ها امکان می‌دهد تا انواع مختلفی از عملیات‌های سایبری را اجرا کنند که حتی ممکن است بسیاری از دولت‌ها قادر به انجام آن نباشند.

## ۲-۷-امنیت سایبری، دفاع سایبری، بازدارندگی سایبری، تاب‌آوری سایبری

در چهارچوب جنگ سایبری و در مواجهه با حملات سایبری موضوعاتی نظیر امنیت سایبری[2]، دفاع سایبری[3]، تاب‌آوری سایبری[4] و بازدارندگی سایبری[5] موضوعیت پیدا می‌کنند. امنیت سایبری ناظر به اقداماتی است که برای جلوگیری از دسترسی غیرمجاز و صدمه زدن به و بهره‌جویی از رایانه‌ها، سامانه‌های ارتباطات الکترونیکی و سایر فناوری‌های اطلاعاتی، نظیر فناوری اطلاعات پلت‌فرمی، و اطلاعات موجود در آنها در فضای سایبر تحت حفاظت انجام می‌شود تا در دسترس بودن[6]، بی‌نقص بودن[7]، قابلیت سنجش اصالت[8]، قابلیت محرمانگی[9] و قابلیت عدم انکار انجام عمل[10] آن

1.Tepper and Hearn
2.Cyber security
3.Cyber defense
4.Cyber resilience
5.Cyber deterrence
6.Availability
7.Integrity
8.Authentication
9.Confidentiality
10.Nonrepudiation

فضای سایبر را تضمین کند (ستاد مشترک ارتش ایالات متحده آمریکا، ۲۰۱۸). در دسترس بودن قابل استفاده بودن فضای سایبر ایجاب می‌کند که افراد مجاز در زمان لازم بتوانند به آن دسترسی داشته باشند. بی‌نقص بودن فضای سایبر به معنی آن است که از تغییر غیرمجاز فضای سایبر جلوگیری شود و در صورت دستکاری غیرمجاز در این فضا، تغییر شناسایی شود. قابلیت سنجش اصالت مربوط به اصیل بودن اطلاعات ارسالی/دریافتی و اصیل بودن فرستنده و گیرنده است. محرمانگی یعنی جلوگیری از افشای اطلاعات برای افراد غیرمجاز. قابلیت عدم انکار انجام عمل نیز به این معنی است که عمل کننده روی اطلاعات نباید قادر به انکار عمل خود باشد. دفاع سایبری عبارت است از اقداماتی که به منظور خنثی کردن تهدیدهای مشخصی علیه فضای سایبری تحت حفاظت انجام می‌شود (ستاد مشترک ارتش ایالات متحده آمریکا، ۲۰۱۸). اقدامات مرتبط با دفاع سایبری عبارتند از شناسایی، توصیف، مقابله با تهدید و کاهش سطح تهدید، با استفاده از بدافزارها[1] یا با فعالیت‌های غیرمجاز کاربران و برگرداندن سیستم به وضعیت ایمن. راهبردهای دفاع سایبری به سه دسته کلی واکنشی[2]، فعال[3] و پیش‌کنش‌گرایانه[4] (یا پیش‌دستانه[5]) قابل تقسیم است. راهبردهای واکنشی بعد از وقوع حمله سایبری عملیاتی می‌شوند؛ راهبردهای فعال به محض وقوع حمله سایبری اجرا می‌گردند؛ و راهبردهای پیش‌کنش‌گرایانه قبل از وقوع حمله سایبری اجرایی می‌گردند.

1.Malware
2.Reactive
3.Active
4.Proactive
5.Preemptive

گاه تامین امنیت ملی از طریق ایجاد بازدارندگی پیگیری می‌شود. به طور کلی، به جلوگیری از اقدام از طریق ایجاد تهدیدی باورپذیر در خصوص اقدام متقابل غیرقابل پذیرش و/یا باور به این که هزینه اقدام از فواید احتمالی آن بیشتر است، بازدارندگی اطلاق می‌شود (ستاد مشترک ارتش آمریکا، ۲۰۱۸). در واقع، بازدارندگی از طریق متقاعد کردن کشور رقیب، حریف یا دشمن به این که اقدامات آن موفقیت‌آمیز نخواهد بود و این که متحمل صدمات قابل ملاحظه‌ای خواهد شد، عملیاتی می‌شود. به طور خاص، بازدارندگی سایبری عبارت است از دستکاری تحلیل هزینه – فایده کشور رقیب، حریف یا دشمن در خصوص یک فعالیت سایبری مشخص (راویش و فیکسلر، ۲۰۱۷). ممکن است، یک کشور بتواند از طریق کاستن از فواید انتظاری و/یا افزودن بر هزینه‌های انتظاری ناشی از یک فعالیت سایبری مشخص، رقیب، حریف یا دشمن خود را به اجتناب از اتخاذ اقدامات خصمانه خاص ترغیب کند. لازم به ذکر است، کاهش فواید انتظاری و/یا افزایش هزینه‌های انتظاری ناشی از یک فعالیت سایبری صرفاً با استفاده از روش‌های سایبری انجام نمی‌شود و این امکان وجود دارد که با استفاده از روش‌های غیرسایبری یا ترکیبی از روش‌های سایبری و غیرسایبری انجام شود. حتی در صورت استفاده از روش‌های سایبری، ضرورتی وجود ندارد که اقدام متقابل نسبت به یک حمله سایبری حتماً به صورت ضدحمله‌ای سایبری از همان جنس و در همان مقیاس (از نظر اندازه حمله و گستره پوشش آن)

باشد. بنابراین، ویژگی‌های ذاتی فضای سایبر امکان ایجاد بازدارندگی سایبری بر مبنای دکترین اقدام نامتقارن را فراهم می‌کند.

بر اساس سند راهبرد سایبری وزارت دفاع ایالات متحده آمریکا[1] (۲۰۱۵) بازدارندگی سایبری بر مبنای ترکیبی از «سیاست‌های اعلامی، شواهد و ظرفیت‌های هشداردهنده قابل ملاحظه، آرایش دفاعی، رویه‌های واکنشی موثر و تاب‌آوری کلی شبکه‌ها و سامانه‌ها» ایجاد می‌شود. اما، چالش‌های مهمی در خصوص ایجاد بازدارندگی سایبری وجود دارد. یکی از مهم‌ترین چالش‌ها، ناشناسی مهاجمان سایبری و دشواری‌های مربوط به انتساب تهدیدهای سایبری به مهاجمان احتمالی است. اتخاذ واکنش دفاعی مناسب مستلزم نسبت دادن تهدیدها به منشاء آنها است. اما، مرتبط کردن یک هویت سایبری یا اقدام سایبری به اشخاص، گروه‌ها یا دولت‌ها مشخص با اطمینان کافی و با قابلیت تایید کردن به گونه‌ای که آن‌ها را پاسخگو نماید، بسیار دشوار است. غالباً این کار به تحلیل‌های فراوان و همکاری‌های گسترده با نهادهای اطلاعاتی نیاز دارد. قابلیت پنهان کردن حامیان حمله و/یا خود تهدید در پس تاثیرات خصمانه در فضای سایبری تعیین چگونگی، زمان و مکان پاسخگویی را دشوار می‌کند. بر خلاف بازدارندگی اتمی در دوران جنگ سرد، اگرچه امروزه دفاع در مقابل حملات سایبری و کاستن از پیامدهای منفی آن‌ها ممکن است، اما بازدارندگی مستلزم تمرکز بر شکل‌دهی به رفتار بازیگران هدف و اقدامات بازدارنده (خواه به صورت انفرادی و خواه به عنوان بخشی از

1.The Department of Defense Cyber Strategy

یک کارزار کلان‌تر) ورای سطح آستانه‌ای مشخص، نه جلوگیری از تمام انواع حملات سایبری است (راویش و فیکسلر، ۲۰۱۷). بدیهی است که جلوگیری از تمام انواع حملات سایبری عملاً غیرممکن است.

تلاش‌های ایالات متحده آمریکا و متحدانش برای شکل‌دهی به رفتار بازیگران معمولاً در قالب زمام‌داری نهادی و از طریق ایجاد نهادها و کنوانسیون‌های بین‌دولی و بین‌المللی به منظور تعریف و ترویج استانداردها و رویه‌های مورد قبول و سپس، تعریف حقوق بین‌الملل بر مبنای چنین استانداردها و رویه‌هایی انجام می‌شود. برای نمونه، بر اساس سند راهبرد ملی سایبری[1] (کاخ سفید، ۲۰۱۸)، ایالات متحده آمریکا ایجاد ابتکار بازدارندگی سایبری[2] را در دستور کار قرار داده است. بر مبنای این استدلال که تاثیرگذاری فشارهای تحمیلی بر بازیگران هدف در قالب ائتلافی از دولت‌های همسو بیشتر می‌شود، آمریکا قصد دارد ابتکار بین‌المللی بازدارندگی سایبری برای ایجاد چنین ائتلافی را آغاز کند. چنین ائتلافی واکنش‌های کشورهای عضو به وقایع سایبری مهم غیرقابل قبول برای آن‌ها را هماهنگ و از چنین واکنش‌هایی پشتیبانی می‌کند.

با توجه به این که تامین امنیت سایبری کامل، حتی از طریق دفاع سایبری و بازدارندگی سایبری، تقریباً غیرممکن است، تاب‌آوری سایبری اهمیت ویژه پیدا می‌کند. تاب‌آوری سایبری ناظر به توانایی یک سامانه سایبری در ارائه مستمر نتایج مورد نظر به رغم رویدادهای سایبری نامطوب است (بجورک[3] و دیگران، ۲۰۱۵). به بیان

1.National Cyber Strategy
2.Cyber Deterrence Initiative
3.Bjorck

ساده، سامانه‌های سایبری باید بتوانند حتی در صورت وجود حملات سایبری مخرب به فعالیت ادامه دهند. بر این اساس، ایجاد شبکه ملی اطلاعات در کشور به عنوان گامی در جهت ارتقای تاب‌آوری سایبری قابل ارزیابی است. لازم به ذکر است، شبکه ملی اطلاعات، به عنوان زیرساخت ارتباطی فضای مجازی ایران، شبکه‌ای مبتنی بر قرارداد اینترنت به همراه سوئیچ‌ها و مسیریاب‌ها و مراکز داده‌ای است به صورتی که درخواست‌های دسترسی داخلی برای اخذ اطلاعاتی که در مراکز داده داخلی نگهداری می‌شوند به هیچ وجه از طریق خارج کشور مسیریابی نشود و امکان ایجاد شبکه‌های اینترانت و خصوصی و امن داخلی در آن فراهم شود (شورای عالی فضای مجازی، ۱۳۹۲). به طور کلی، به دلایل مختلفی نظیر رو به گسترش بودن فضای سایبر و پویایی‌های امنیتی در نظامات سایبری، هنوز هنجارهای حکمرانی و رژیم‌های امنیتی و دفاعی در حوزه فضای سایبر به شکل قابل قبولی شکل نگرفته‌اند (انگلوف[1]، ۲۰۱۷). در این شرایط، مسئولیت‌ها و اختیارات دولت‌ها و بخش‌های غیردولتی در خصوص تامین امنیت سایبری مشخص نیست. به طور خاص، جنگ اقتصادی سایبری ممکن است به میدان‌های نبردی گسترش یابد که در آن‌ها، شرکت‌ها و جوامع متشکل از شهروندان عادی (غیرنظامی) به دلیل بهره‌مندی از توانمندی‌های مختلف جایگاه مهمی در ساختار قدرت دارند. علاوه بر این، معمولاً در جنگ-های اقتصادی سایبری شرکت‌های تجاری و شهروندان عادی در کنار دولت و حتی بعضاً،

1.Engloff

جلوتر از دولت‌ها در خط مقدم جنگ قرار دارند. در چنین شرایطی، شرکت‌های تجاری و شهروندان عادی ناگزیر هستند نقش جدی‌تر را در تامین امنیت سایبری، دفاع سایبری، بازدارندگی سایبری و تاب‌آوری سایبری خویش و جوامع مرتبط با خویش، نظیر تامین‌کنندگان و مشتریان، ایفا کنند. در این شرایط، حتی ممکن است لازم باشد بازیگران غیردولتی راساً اقدام به پدافند عامل[1] کنند. بر مبنای مدل مزدوری سایبری[2]، سیاست‌گذاران برای تامین امنیت سایبری در چهارچوب راهبردهای مرتبط از مشارکت جدی شرکت‌های تجاری و شهروندان عادی، به مثابه مزدوران سایبری، استفاده می‌کنند (زاراته، ۲۰۱۵). در این مدل، بخشی از وظایف و اختیارات دولت‌ها به مزدوران سایبری واگذار می‌شود و آن‌ها به مثابه شبه دولت[3] فعالیت می‌کنند.

1.Active defense
2.Cyber privateering
3.Semi-state

# بخش سوم

# بخش سوم

## جنگ اقتصادی سایبری

جنگ اقتصادی سایبری به راهبردی خصمانه اطلاق می‌شود که مستلزم حمله یا حملات سایبری علیه یک کشور به منظور تضعیف قدرت سیاسی و نظامی آن کشور از طریق تضعیف اقتصاد آن است (راویش و فیکسلر، ۲۰۱۷). در واقع، در جنگ اقتصادی سایبری، تلاش می‌شود از طریق تضعیف اقتصاد یک کشور، قدرت سیاسی و نظامی آن کشور تضعیف گردد. تعریف ارائه شده برای اصطلاح جنگ اقتصادی سایبری روی هدف این نوع از جنگ تمرکز دارد و از این طریق، پیشرفت‌های فناورانه‌ای را لحاظ می‌کند که توانایی بازیگران دولتی و غیر دولتی برای درگیر شدن در راهبردهای جدید جنگ اقتصادی را گسترش می‌دهد. برای تعیین این که آیا حمله سایبری خاصی بخشی از یک جنگ اقتصادی سایبری هست یا خیر، درک هدف راهبردی مهاجم ضروری است. اگرچه ممکن است یک حمله سایبری به عنوان جرم سایبری یا جاسوسی سایبری طبقه‌بندی شود، اما برای اتخاذ راهبردهای تقابلی مناسب

ضروری است بستر گسترده‌تر و راهبرد کلان‌تر مهاجم درک شود. اگر یک حمله یا مجموعه‌ای از حملات چهار شرط زیر را داشته باشند، می‌توان آن حمله یا حملات را به عنوان جنگ اقتصادی سایبری در نظر گرفت (راویش و فیکسلر، ۲۰۱۷):

۱- از طریق فضای سایبر امکان‌پذیر شده باشد.

۲- باید باعث لطمه اقتصادی شود یا هدف از انجام آن وارد کردن لطمه اقتصادی باشد.

۳- لطمه اقتصادی باید به اندازه‌ای بزرگ باشد که قابلیت‌ها و توانمندی‌های امنیت ملی کشور هدف حمله را به شکل بالقوه‌ای تضعیف کند.

۴- انگیزه حمله یا حملات باید تضعیف قابلیت‌ها و توانمندی‌های امنیت ملی باشد.

بسته به عرصه‌ای که جنگ اقتصادی سایبری در آن رخ می‌دهد یا ابزارهایی که برای این منظور مورد استفاده قرار می‌گیرد، می‌توان انواع مختلفی از جنگ‌های اقتصادی سایبری را تعریف و طبقه‌بندی کرد. برای نمونه، جنگ مالی سایبری نوعی از جنگ‌های اقتصادی سایبری است، که بر بستر سامانه‌های مالی سایبری انجام می‌شود. هدف جنگ مالی سایبری[1] تضعیف یا تخریب زیرساخت‌ها، داده‌ها، فعالیت نظام مالی و اعتماد به این نظام و نهادهای ذی‌ربط آن به عنوان روشی برای تضعیف قدرت سیاسی و نظامی رقیبان، حریفان و دشمنان است (زاراته[2]، ۲۰۱۵).

1.Cyber financial warfare
2.Zarate

همانند جنگ سایبری، ممکن است جنگ اقتصادی سایبری در لایه‌های مختلف فضای سایبر اتفاق بیفتد. همچنین، ممکن است این نوع از جنگ در تلفیق با سایر انواع جنگ، نظیر جنگ تجاری، جنگ صنعتی و جنگ فناوری، مورد استفاده قرار گیرد. برای نمونه، وقتی ایالات متحده تلاش کرد دسترسی شرکت چینی هوآوی[1] به قطعات سخت‌افزاری آمریکایی را قطع کند، جمهوری خلق چین برای اطمینان یافتن از این که مورد باج‌خواهی آمریکا قرار نمی‌گیرد و برای کسب بازدارندگی سایبری، توسعه صنعت نیمه‌رسانای خود را شتاب بخشید. علاوه بر این، چین بانک اچ‌اس‌بی‌سی[2]، را به خاطر فراهم کردن اطلاعاتی که علیه شرکت هوآوی مورد استفاده قرار گرفته بود، به عنوان «شرکت غیرقابل اعتماد» تعیین کرد. به طور مشابه، تلاش‌های چین برای بین‌المللی کردن یوان و ایجاد نظامات مالی جهانی مبتنی بر آن، نظیر نظام‌های پرداخت یوان‌پایه، در سال‌های اخیر شدت گرفته است (نیومان[3]، ۲۰۱۹). با تضعیف نظام مالی جهانی کنونی، که محوریت آن با آمریکا است، توانایی این کشور در اعمال جنگ مالی به شدت تضعیف خواهد شد. در چنین شرایطی، جنگ اقتصادی سایبری در چهارچوب مفهوم گسترده‌تر زمام‌داری اقتصادی اعمال می‌گردد. در ادامه این بخش، برخی از مصادیق جنگ اقتصادی سایبری که توسط کشورهای ایالات متحده آمریکا، چین، روسیه، کره شمالی و ایران انجام شده، معرفی می‌گردد[4]. لازم به ذکر است، نقش

1.Huawei
2.HSBC
3.Newman
۴.بر اساس شواهد موجود تا کنون کشورهای اسپانیا، اندونزی، استرالیا، اتیوپی، اوگاندا، امارات متحده عربی، ایالات متحده آمریکا، ایران، بریتانیا، پاکستان، پاناما، تایوان، چین، رژیم اشغالگر قدس، روسیه، عربستان سعودی، فرانسه، قزاقستان، کانادا، کره جنوبی، کره شمالی، لبنان، مکزیک، نیوزیلند، هلند، هند، هنگ کنگ، ویتنام بانی عملیات‌های سایبری بوده‌اند (شورای روابط خارجی، ۲۰۲۰). از این میان، ایالات متحده آمریکا، چین، روسیه، کره شمالی و ایران فعال‌ترین کشورها در حوزه جنگ اقتصادی سایبری هستند.

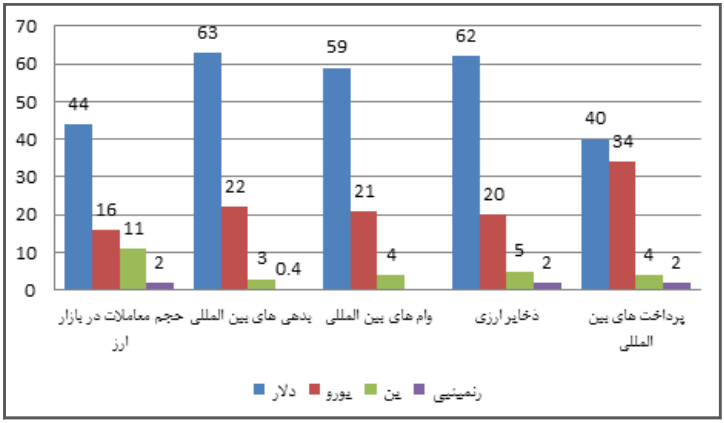
کشورهای مذکور در برخی از حملات به طور رسمی تایید نشده است و رسانه‌ها، شرکت‌های امنیت سایبری و کارشناسان اقدام به انتساب این عملیات‌های سایبری به کشورهای مذکور کرده‌اند.

### ۳-۱-ایالات متحده آمریکا

در سال‌های اخیر، زمام‌داری اقتصادی، به ویژه در قالب اقدامات اقتصادی قهرآمیز به ابزار اصلی ایالات متحده در حوزه سیاست خارجی و امنیت ملی تبدیل شده است. وجود عواملی نظیر سلطه جهانی دلار آمریکا، تاثیر قابل ملاحظه نهادهای مالی آمریکایی در نظام مالی جهانی، اندازه بزرگ و جذابیت بازار آمریکا، نقش برجسته شرکت‌های آمریکایی در زنجیره‌های تامین جهانی، نقش قابل ملاحظه شرکت‌ها و صندوق‌های سرمایه‌گذاری آمریکایی در سرمایه‌گذاری‌های جهانی و وجود رژیم قانون لازم برای اعمال تحریم‌های اقتصادی و مالی به این کشور امکان می‌دهد تا برای دستیابی به اهداف خود در حوزه سیاست خارجی و امنیت ملی از جنگ اقتصادی و زمام‌داری اقتصادی استفاده کند (هارل و روزنبرگ[1] ، ۲۰۱۹). برای نمونه، در حال حاضر، دلار آمریکا پول مسلط بر تجارت بین‌الملل، تامین مالی بین‌الملل و ذخایر بانک‌های مرکزی است. این همان وضعیتی است که از آن تعبیر به هژمونی (سلطه) جهانی دلار[2] می‌شود. اختلاف قابله ملاحظه دلار آمریکا با سایر پول‌های جهان‌روا و سلطه آن بر نظام مالی بین‌الملل در پنج حوزه معاملات بازار ارز، بدهی‌های

1.Harrell and Rosenberg
2.Dollar hegemony

بین‌المللی، وام‌های بین-المللی، ذخایر ارزی و پرداخت‌های بین‌المللی در سال ۲۰۱۶ در نمودار ذیل نشان داده شده است.




سلطه دلار آمریکا بر نظام مالی بین‌الملل در سال ۲۰۱۶

ماخذ: ایشنگرین و شیا [1] (۲۰۱۹)

از سوی دیگر، ایالات متحده خود مبدع اینترنت بوده و همین موضوع باعث شده است که این کشور در حوزه جنگ سایبری از مزیت بازیگر اول بودن [2] بهره‌مند باشد. ایالات متحده در خصوص بهره‌جویی از فضای مجازی و استفاده از قدرت سایبری برای تامین منافع ملی سابقه طولانی دارد (کراندال و تایر، ۲۰۱۹). اجرای عملیات سایبری بازی‌های المپیک [3] نمونه‌ای شناخته‌شده از استفاده ایالات متحده و متحدانش، به‌ویژه رژیم اشغال‌گر قدس از عملیات سایبری علیه یک کشور، یعنی ایران، است. عملیات بازی‌های المپیک یکی از اولین عملیات‌های سایبری است که در آن از سلاح سایبری آفندی [4] استفاده شده است

1.Eichengreen and Xia
2.First mover advantage
3.Operation Olympic Games
4.Offensive cyber weapon

(سنگر[1] ، ۲۰۱۲). در این عملیات، بدافزارهایی نظیر استاکس‌نت و فلیم[2] مورد استفاده قرار گرفته‌اند. لازم به ذکر است، بدافزار فلیم رایانه‌هایی را که در منطقه خاورمیانه، به ویژه ایران، از سیستم عامل مایکروسافت ویندوز استفاده می‌کردند، هدف جاسوسی سایبری قرار می‌داد (اردبرینک[3] ، ۲۰۱۲). وزارت نفت و شرکت ملی نفت ایران از جمله نهادهایی بودند که مورد حمله این بدافزار قرار گرفته بودند. ایالات متحده آمریکا در استفاده از جنگ اقتصادی سایبری نیز پیشگام بوده و در سال‌های گذشته، این نوع از جنگ از ارکان محوری زمامداری اقتصادی این کشور بوده است. تحریم نهادهای مالی ایرانی در دسترسی به سوئیفت، یکی از شناخته‌شده‌ترین مصادیق جنگ اقتصادی سایبری است که توسط ایالات متحده آمریکا اعمال شده است (راویش و فیکسلر، ۲۰۱۷). سوئیفت نوعی پیام‌رسان مالی بین‌المللی را فراهم کرده است که به نهادهای مالی سراسر جهان امکان می‌دهد اطلاعات مربوط به تراکنش‌های مالی را در محیطی ایمن، استاندارد و قابل اتکا ارسال و دریافت کنند و به همین دلیل، این شبکه به مثابه ستون فقرات نظام مالی جهانی عمل می‌کند. در حال حاضر، سوئیفت بیش از ۱۱ هزار نهاد مالی را به هم متصل کرده است (تارنمای سوئیفت، ۲۰۱۹). در اوایل سال ۲۰۱۲، وقتی کنگره ایالات متحده آمریکا تلاش کرد دسترسی بانک‌ها و موسسات مالی اعتباری غیربانکی ایرانی به سوئیفت را قطع کند، رژیم تحریم‌های اقتصادی – مالی این کشور

1.Sanger
2.Flame
3.Erdbrink

علیه ایران از مولفه‌ای بهره گرفت که به لطف وجود فضای سایبر ممکن شده بود (دوبویتز و فیکسلر[1]، ۲۰۱۵). هدف از این اقدام جلوگیری از فعالیت‌های نامطلوب ایران از نظر آمریکا و نیز وارد کردن صدمات قابل ملاحظه به اقتصاد ایران بود تا از طریق اعمال این فشار، ایران مجبور به تغییر رفتار خود در حوزه سیاست خارجی مطابق نظر آمریکا شود و/یا توانایی ایران برای تامین مالی تقویت توان نظام و تامین امنیت ملی خود کاهش یابد. جنگ اقتصادی سایبری ایالات متحده آمریکا علیه ایران در قالب تحریم بانک‌ها و موسسات مالی اعتباری غیربانکی ایرانی از دسترسی به سوئیفت مبتنی بر شکلی جدیدی از جنگ مالی، یعنی جنگ مالی سایبری، بود. این نوع از جنگ مالی به یکی از ارکان دکترین امنیت ملی ایالات متحده تبدیل شده است (زاراته، ۲۰۱۳). بعد از حملات یازده سپتامبر سال ۲۰۰۱، ایالات متحده آمریکا تلاشی گسترده در حوزه به اصطلاح «مقابله با تامین مالی تروریسم» را آغاز کرده که ماهیت جنگ مالی را تغییر داده است. این تلاش سه محور اصلی داشته است: بسط رژیم بین‌المللی ضد پول‌شویی، تامین مالی تروریسم و تامین مالی فعالیت-های مربوط به اشاعه سلاح‌های کشتار جمعی، توسعه ابزارها و رویه‌های تجسس مالی[2]، توسعه راهبردهای مبتنی بر فهم جدید از جایگاه دلار آمریکا در نظام مالی بین‌الملل و نقش بخش خصوصی در ارتباط با تهدیدات و موضوعات مربوط به امنیت ملی. اکنون ایالات متحده آمریکا و متحدانش نظامی بین‌المللی برای

1.Dubowitz and Fixler
2.Financial intelligence

استفاده از اطلاعات، قدرت و هدایت[1] مالی به منظور ایزوله کردن بازیگران غیرمطلوب از نظام مالی و تجاری بین‌المللی را ایجاد کرده‌اند. در این رویکرد، به جای استفاده از چهارچوب‌های قدیمی تحریم اقتصادی، بر رفتار نهادهای مالی تمرکز می‌شود. با توجه به این که محاسبات مبتنی بر هزینه – فایده نهادهای مالی به رفتار آنها شکل می‌دهد، وقتی احتمال شناسایی تراکنش‌های غیرقانونی و مواجه شدن با جرایم مقرراتی و هزینه‌های ناشی از دست رفتن حسن شهرت افزایش یابد، نهادهای مالی مجبور به تغییر رفتار خود می‌شوند. به این ترتیب، وقتی شخص حقیقی یا حقوقی توسط خزانه‌داری آمریکا در فهرست سیاه قرار می‌گیرد، دیگر نمی‌تواند با استفاده از نظام مالی آمریکا تراکنش مالی انجام دهد. افزون بر این، بانک‌های بین‌المللی، که از طریق نهادهای مالی آمریکایی اقدام به تسویه تراکنش‌های دلاری می‌کنند، با نهادهای نظارتی این کشور مواجه شده‌اند و ناگزیر به رعایت قوانین و مقررات ایالات متحده هستند. به همین دلیل، نهادهای مالی غیرآمریکایی، به‌ویژه نهادهای مالی اروپایی، نقش مهمی در اعمال تحریم‌های ثانویه[2] ایفا می‌کنند. فراتر از این، کشورهایی که بر مبنای اصولی نظیر تسهیم اطلاعات[3] و ممیزی دقیق[4]، مقررات و رویه-های ضد پول‌شویی، مقابله با تامین مالی تروریسم و اشاعه سلاح‌های کشتار جمعی ترویجی ایالات متحده آمریکا و متحدانش را اجرا می‌کنند، به اجرایی شدن ایده مذکور کمک می-کنند.

1.Suasion

2.Secondary sanctions

تحریم های اولیه (primary sanctions) شهروندان و شرکت های کشور تحریم کننده را از انجام فعالیت های اقتصادی مشخص با شهروندان و شرکت های کشور تحت تحریم منع می کند. تحریم های ثانویه با تهدید اشخاص ثالث به قطع دسترسی به کشور تحریم کننده یا قطع واقعی دسترسی، آنها را انجام فعالیت های اقتصادی مشخص با شهروندان و شرکت های کشور تحت تحریم منع می کند.

3.Information sharing

4.Due diligence

صرف نظر از موارد فوق، وزارت خزانه‌داری ایالات متحده، آژانس اطلاعات مرکزی[1] و سایر نهادهای دولتی ایالات متحده در صورت ضرورت، در چهارچوب برنامه ردگیری تامین مالی تروریسم[2] و با استفاده از عملیات‌های جاسوسی به پایگاه‌های داده مالی، نظیر پایگاه داده سوئیفت، نیز نفوذ و با کسب اطلاعات مورد نیاز اقدام به شناسایی اشخاص و روابط مالی مشکوک می‌کنند (لیختبلو و ریسن[3]، ۲۰۰۶). به این ترتیب، در جنگ مالی جدید، برای قطع دسترسی بازیگران نامطلوب به منابع مالی مورد نیاز از دسترسی آن‌ها به نظامات مالی بین-الملل جلوگیری می‌شود. برای تاثیرگذاری بر انگیزه‌ها و منافع فعالان بازار، رهبران کشورها و جوامع، بانک‌ها و نهادهای مالی جهت همراهی آن‌ها با برنامه‌های تحریمی نیز از اطلاعات و فشارهای مالی استفاده می‌شود. اتاق جنگ مالی آمریکا در وزارت خزانه‌داری این کشور قرار دارد. در واقع، خزانه‌داری ایالات متحده نقش محوری آمریکا در نظام مالی جهانی را قدرت مالی[4] تبدیل و از ابزارهای مبتنی بر این قدرت در جنگ مالی استفاده کردند (زاراته، ۲۰۱۳). در دو دهه اخیر، وزارت خزانه-داری آمریکا در خط مقدم توسعه ابزارهای مالی جدید برای تضعیف اقتصاد کشورها و جوامع رقیب، حریف و دشمن بوده است (راویش و فیکسلر، ۲۰۱۷). تشکیل اداره تروریسم و تجسس مالی[5] در وزارت خزانه‌داری در سال ۲۰۰۴ و بازتعریف نقش وزارت خزانه‌داری در عرصه جنگ مالی گامی مهم در این راستا بوده است. وظیفه این

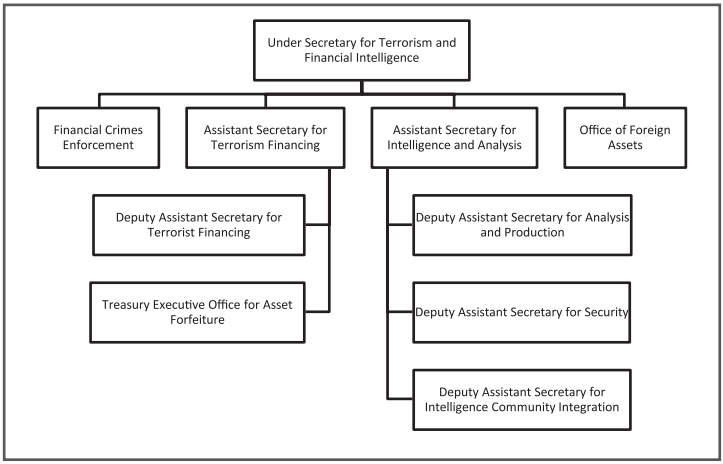
1.Central Intelligence Agency (CIA)
2.Terrorist Finance Tracking Program
3.Lichtblau and Risen
4.Financial power
5.Office of Terrorism and Financial Intelligence (TFI)

نهـاد، کـه توسـط معـاون وزیـر خزانـه‌داری ایـن کشـور اداره می‌شـود، تدویـن و اجـرای سیاسـت‌ها و مقـررات و انجـام فعالیت‌هـای اطلاعاتـی بـه منظـور قطـع خطـوط پشـتیبانی مالـی از تروریسـت‌های بین‌المللـی، اشـاعه‌دهندگان سـلاح‌های کشـتار جمعـی، قاچاقچیـان مـواد مخـدر، افـراد درگیـر در پول‌شـویی و سـایر تهدیدهـا علیـه امنیـت ملـی آمریـکا اسـت (تارنمـای وزارت خزانـه‌داری ایـالات متحـده آمریـکا، ۲۰۱۹). اداره تروریسـم و تجسـس مالـی وزارت خزانـه‌داری ایـالات متحـده از ادارات و دفاتـر مختلفـی تشـکیل شـده اسـت. اداره تامیـن مالـی تروریسـت‌ها و جرایـم مالـی[1] بخـش پیشـران و سیاسـت‌گذار اداره تروریسـم و تجسـس مالـی خزانـه‌داری آمریـکا اسـت. اداره اجرایـی خزانـه‌داری بـرای ضبـط دارایی‌هـا[2] مسـئول اداره صنـدوق ضبـط دارایی‌هـای خزانـه‌داری[3] آمریـکا اسـت. ایـن صنـدوق حسـاب دارایی‌هـای ضبـط شـده غیرمالیاتـی را اداره می‌کنـد. اداره تامیـن مالـی تروریسـت‌ها و جرایـم مالـی و اداره اجرایـی وزارت خزانـه‌داری بـرای ضبـط دارایی‌هـا ذیـل اداره تامیـن مالـی تروریسـم[4] فعالیـت می‌کننـد. همچنیـن، اداره تجسـس و تحلیـل[5] مسـئول کارکردهـای اطلاعاتـی اداره تروریسـم و تجسـس مالـی و هماهنـگ کـردن وزارت خزانـه‌داری بـا جامعـه اطلاعاتـی ایـالات متحـده آمریـکا اسـت و هـم از وزارت خزانـه‌داری و هـم از جامعـه اطلاعاتـی ایـن کشـور پشـتیبانی می‌کنـد. اداره تجسـس و تحلیـل خـود از سـه دفتـر تحلیـل و تولیـد[6]،

1.Office of Terrorist Financing and Financial Crimes (TFFC)
2.Treasury Executive Office for Asset Forfeiture (TEOAF)
3.Treasury Forfeiture Fund (TFF)
4.Office of Terrorism Financing
5.Office of Intelligence and Analysis (OIA)
6.Analysis and Production

امنیت[1]، هماهنگی با جامعه اطلاعاتی[2] شده است. لازم به ذکر است، در جهان است که دارای نهاد اطلاعاتی درون سازمانی خود است. اداره کنترل دارایی‌های خارجی[3] نیز تحریم‌های اقتصادی و تجاری را اجرایی می‌کند. شبکه اعمال قانون علیه جرایم مالی[4]، که مسئول اجرای قانون رازداری بانکی[5] و سایر کارکردهای در حوزه مقررات‌گذاری است، از دیگر دفاتر خزانه‌داری است که از اقدامات تجسسی ناظر به اعمال قوانین ذی‌ربط پشتیبانی می‌کند و همکاری بین دستگاهی و جهانی علیه جرایم مالی داخلی و بین‌المللی را تقویت می‌کند. همچنین، شبکه اعمال قانون علیه جرایم مالی تحلیل‌های راهبردی در خصوص روندها و الگوهای جهانی را در اختیار سیاست‌گذاران آمریکایی قرار می‌دهد. لازم به ذکر است، شبکه اعمال قانون علیه جرایم مالی در همکاری نزدیک با بخش بررسی جرایم سازمان خدمات درآمد داخلی[6] نسبت به اعمال قوانین ضد تامین مالی تروریست‌ها و پول-شویی اقدام می‌کند. ساختار سازمانی اداره تروریسم و تجسس مالی وزارت خزانه‌داری ایالات متحده به شرح شکل ۲ است:

1.Security
2.Intelligence Community Integration
3.Office of Foreign Assets Control (OFAC)
4.Financial Crimes Enforcement Network (FinCEN)
5.Bank Secrecy ACT (BSA)
6.Internal Revenue Service Criminal Investigative Division (IRS-CI)




شکل ۲: ساختار سازمانی اداره تروریسم و تجسس مالی وزارت خزانه‌داری ایالات متحده

ماخذ: تارنمای وزارت خزانه‌داری ایالات متحده آمریکا (در تاریخ ۲۰۱۹)

## ۳-۲-چین

از سال‌های آغازین دهه‌ی ۱۹۷۰، جمهوری خلق چین به منظور تقویت رقابت‌پذیری اقتصادی و موقعیت راهبردی خود تلاش‌های گسترده و مداومی را برای ربودن دارایی‌های فکری از کشورهای مختلف انجام داده است. در گذر زمان، این تلاش‌ها به طور فزاینده از طریق فناوری‌های سایبری و در چهارچوب جاسوسی اقتصادی سایبری انجام شده است (کوپر[1]، ۲۰۱۸). برآورد می‌شود که ۵۰ تا ۸۰ درصد از کل موارد سرقت دارایی فکری فرامرزی در جهان و بیش از ۹۰ درصد از جاسوسی اقتصادی سایبری از ایالات متحده آمریکا توسط چین انجام می‌شود. سرقت دارایی فکری بخش بزرگی از راهبرد

1.Cooper

جنگ اقتصادی سایبری چین علیه آمریکا و متحدان این کشور، را تشکیل می‌دهد (روایش و فیکسلر، ۲۰۱۷). علاوه بر آمریکا، شرکا و متحدان این کشور، نظیر کره جنوبی، ژاپن، کانادا، بریتانیا و آلمان نیز هدف جاسوسی اقتصادی سایبری چین قرار گرفته‌اند. در کنار سرقت دارایی فکری، جاسوسی از زیرساخت-های حیاتی نیز بخشی دیگری از راهبرد جنگ اقتصادی سایبری و زمام‌داری اقتصادی چین را تشکیل می‌دهد. همچنین، چین برای تغییر رفتار دولت‌های خارجی از فشار اقتصادی سایبری[1] استفاده می‌کند (کوپر، ۲۰۱۸). در تازه‌ترین نمونه، چین برای فشار وارد کردن بر دولت کره جنوبی برای متوقف کردن استقرار سامانه دفاع موشکی تاد[2] ایالات متحده در این کشور از تحریم‌های اقتصادی و عملیات سایبری استفاده کرد. در سال ۲۰۱۷، هکرهایی که از اینترنت چین استفاده می‌کردند شرکت کره‌ای لوته گروپ[3] را، که به دولت کره جنوبی اجازه داده بود از اراضی این شرکت برای استقرار سامانه تاد استفاده کند، هدف حمله سایبری قرار دادند. این حمله سایبری برای چندین روز تارنمای فروش شرکت مذکور را آفلاین کرد. علاوه بر این، برخی از سایت‌های تجارت الکترونیکی چینی همکاری خود با شرکت مذکور را متوقف کردند. پس از آن، دولت چین تقریباً تمام ۱۱۵ فروشگاه فیزیکی شرکت لوته در چین را به بهانه-هایی نظیر ریسک حریق بست. رسانه‌های چینی نیز فراخوان تحریم کالاهای ساخت کره جنوبی و ممنوعیت سفر به این کشور را اعلام کردند. وزارت گردشگری چین نیز از شرکت-های گردشگری چین

1.Cyber-enabled economic coercion
2.THAAD: Terminal High Altitude Area Defense
3.Lotte Group

خواست فروش تورهای گردشگری به کره جنوبی را متوقف کنند. جاسوسی سایبری اقتصادی نقش مهمی در اجرای زمام‌داری اقتصادی چین که هدف آن برتری و سلطه اقتصادی این کشور در عرصه جهانی است. تمرکز بر دستیابی به فناوری‌ها و اطلاعات مورد نیاز در چهارچوب راهبردی نسبتاً منسجم از ویژگی مهم عملیات‌های جاسوسی جمهوری خلق چین بوده است. از منظر تجاری، فناوری‌ها و اطلاعات به دست آمده از این طریق نقش بسزایی در کاهش هزینه‌های تحقیق و توسعه شرکت‌های چینی و تقویت مزیت رقابتی آن‌ها در بازارها داشته‌اند. از منظر نظامی، فناوری‌ها و اطلاعات اینچنینی نقش مهمی در نوسازی ارتش آزادی‌بخش خلق چین و تقویت قدرت نظامی این کشور داشته‌اند. یکی از مهم‌ترین ویژگی‌های عملیات سایبری چین آن است که این کشور درگیر جنگ اقتصادی سایبری آشکار با ایالات متحده آمریکا و متحدانش نشده است. یکی دیگر از ویژگی‌های مهم عملیات‌های جاسوسی سایبری چین استفاده از عوامل انسانی برای نفوذ به نهادها و شرکت‌های ذی‌ربط به عنوان جاسوس بوده است. ویژگی مهم دیگر عملیات‌های جاسوسی سایبری منتصب به جمهوری خلق چین این است که طیف متنوعی از فعالیت‌های تجاری را در بر می‌گیرد. با توجه به این که نحوه استفاده چین از جاسوسی اقتصادی سایبری حاوی اطلاعات مفیدی است، در جدول ۱، نمونه‌هایی از عملیات‌های سایبری این کشور علیه شرکت‌ها و نهادهای دولتی آمریکایی و

برخی از کشورهای هم‌پیمان این کشور به اختصار ارائه شده است.

| سال | نهاد یا شرکت هدف | حوزه فعالیت | توضیحات |
|---|---|---|---|
| ۲۰۰۶ | فورد[1] | اتومبیل | یک تبعه چین شاغل در شرکت فورد در تلاش برای یافتن شغلی در یک شرکت اتومبیل‌سازی چین ۴ هزار سند الکترونیکی شرکت فورد را با استفاده از حافظه سخت جانبی به شرکت چینی مذکور داد. برآورد می‌شود در نتیجه این اقدام شرکت فورد ۵۰ میلیون دلار زیان کرد. |
| ۲۰۰۷ | کینتیک[2] | روباتیک | وجود نوعی آسیب‌پذیری سایبری در شرکت کینتیک به هکرها امکان دسترسی به اطلاعات مربوط به روبات‌ها، ماهواره‌ها، هلیکوپترهای جنگی و پهپادهای این شرکت را داد. بعدها، ارتش آزادی بخش خلق چین از روبات خنثی‌ساز بمبی رونمایی کرد که احتمالا بر اساس فناوری ربوده شده از شرکت کینتیک ساخته شده بود. |
| ۲۰۰۸ | آلکوا[3] | فلزات | حفره‌ای امنیتی در شرکت آلکوا هکرها را قادر ساخت به رایانامه‌هایی حاوی مباحث داخلی شرکت پیرامون قرارداد احتمالی با یک شرکت دولتی چینی دست یابند و از آن برای تحمیل شرایط خود به شرکت آلکوا استفاده کنند. |
| ۲۰۰۹ | کوکا کولا | نوشیدنی | حفره‌ای امنیتی در شرکت کوکا کولا امکان دسترسی هکرها به شبکه آن در زمانی را فراهم کرد که این شرکت در تلاش برای تملک شرکت چاینا هیویوان جویس گروپ[4] بود. |
| ۲۰۰۹ | واسپار[5] | مواد شیمیایی | یک تبعه چین، شاغل در شرکت واسپار، فایل الکترونیکی اسرار تجاری این شرکت در خصوص فرمول رنگ ۱۶۰ محصول به ارزش ۲۰ میلیون دلار را به شرکت چینی نیپون پینت[6] داد. |
| ۲۰۰۹ | دوپونت[7] | مواد شیمیایی | یک شیمیدان محقق شاغل در شرکت دوپونت، اسرار تجاری مربوط به لامپ‌های دیودی نورگسیل ارگانیک[8] شرکت مذکور را به منظور تجاری‌سازی محصول به دانشگاه پکن داد. زیان شرکت در نتیجه این اقدام ۴۰۰ میلیون دلار برآورد شده است. |
| ۲۰۱۰ | گوگل | فناوری | عملیات اورورو[9] ۳۴ شرکت در حوزه‌های فناوری، مالی و دفاعی، از جمله گوگل را هدف قرار داد. گوگل ادعا کرد که در چهارچوب حمله فوق کدهای منبع[10] این شرکت دزدیده شده است. |
| ۲۰۱۰ | نهادهای دولتی و شرکت‌های مختلف نظیر وزارتخانه-های دفاع و بازرگانی و شرکت‌های | ارتباطات | برای ۱۸ دقیقه مسیر اینترنت ایالات متحده آمریکا تغییر کرد و از طریق چین عبور کرد. این عملیات به گروه‌های چینی اجازه داد تا ۱۵ درصد از ترافیک جهانی را رصد کنند. |

1.Ford
2.QinetiQ
3.Alcoa
4.China Huiyuan Juice Group
5.Valspar
6.Nippon Paint
7.DuPont
8.Organic light-emitting diode (OLED)
9.Operation Aurora
10.Source codes

| سال | نهاد یا شرکت هدف | حوزه فعالیت | توضیحات |
|---|---|---|---|
| | وزارتخانه‌های دفاع و بازرگانی و شرکت‌های مایکروسافت و دل[۱] | | |
| ۲۰۱۰ | شرکت‌های مختلف نظیر بوئینگ | هوانوردی | ۲۵۰ هزار صفحه سند در خصوص اسرار تجاری شرکت‌های مختلف آمریکایی فعال در صنعت هواپیمایی در منزل یک تبعه چینی کشف و وی به جرم جاسوسی اقتصادی به ۱۵ سال حبس محکوم شد. او صد داشت این اسناد را در اختیار شرکت‌های چینی فعال در صنعت هواپیمایی منتقل کند. |
| ۲۰۱۰ | یو اس استیل[۲] | فلزات | رایانه‌های شرکت آمریکایی یو اس استیل، در سال ۲۰۱۰، مقارن با زمانی که این شرکت در حال پیگیری دعاوی حقوقی علیه شرکت‌های چینی فعال در صنعت فولاد بود، هک شد. شرکت آمریکایی مدعی بود که هکرهای تحت حمایت تولیدکنندگان چینی روش‌های ابداعی این شرکت برای تولید فولاد سبک را سرقت کرده‌اند. |
| ۲۰۱۰ | وستینگهوس[۳] | هسته‌ای | هکرها نقشه‌های مربوط به نیروگاه‌های برق ساخت شرکت وستینگهوس و همچنین رایانامه‌های مرتبط با داد و ستد این شرکت با یک شرکت دولتی چینی را ربودند. |
| ۲۰۱۱ | آراس‌ای[۴] | دفاعی | سه گروه چینی به شرکت آراس‌ای حمله کردند. بعدها، این حمله به نفوذهایی منتهی شد که به امنیت ۲۰ درصد از شرکت‌های موجود در فهرست فورچون ۱۰۰[۵] لطمه زد. برآورد می‌شود که در مجموع ۷۲۰ شرکت از جمله شرکت‌های دفاعی نظیر لاکهید مارتین[۶] از این حملات و نفوذهای سایبری آسیب دیده باشند. |

[۱] Dell

[۲] U.S. Steel

[۳] Westinghouse

[۴] RSA

[۵] Fortune ۱۰۰

[۶] Lockheed Martin

| سال | نهاد یا شرکت هدف | حوزه فعالیت | توضیحات |
|---|---|---|---|
| ۲۰۱۱ | شرکت‌های مختلف | انرژی | مهاجمان طی عملیات موسوم به نایت دراگون[۱] داده‌هایی را از شرکت‌های فعال در حوزه نفت، انرژی و پتروشیمی سرقت و به چین منتقل کردند. |
| ۲۰۱۱ | کارگیل[۲] | کشاورزی | یکی از افرادی که سابقه کار در شرکت کارگیل و دآو کمیکال[۳] اسرار تجاری آفت‌کش‌های ارگانیک را به دانشگاهی در چین منتقل کرد. برآورد می‌شود زیان مالی این جاسوسی سایبری بیش از ۷ میلیون دلار بوده باشد. |
| ۲۰۱۱ | موتورولا[۴] | الکترونیک | یکی از مهندسان نرم‌افزار شرکت موتورولا اسرار تجاری، مشتمل بر ۱۰۰۰ سند، را از طریق ارتباطات موبایلی به ارتش چین منتقل کرد. ارزش داده‌های مذکور ۶۰۰ میلیون دلار برآورد می‌شود. |
| ۲۰۱۱ | امریکن سوپرکونداک تور کورپوریشن[۵] | الکترونیک | شرکت چینی سینوول[۶] با هدف نمونه‌برداری از فناوری و محصولات شرکت امریکن سوپرکونداکتور نسبت به سرقت اسرار تجاری مربوط به کد منبع شرکت مذکور اقدام کرد. سرقت دارایی فکری بر امریکن سوپرکونداکتور تاثیر مخرب داشت و عملاً باعث نابودی آن شد. |
| ۲۰۱۲ | سولارورلد[۷] | انرژی | در یک حمله سایبری اطلاعات شرکت سولارورلد پیرامون جریان نقد، آمار تولید، اطلاعات خط تولید، مخارج و دعاوی تجاری دزدیده شد. مقارن با این اتفاق، شرکت‌های چینی محصولات مرتبط با انرژی خورشیدی را با قیمت بسیار پایین و در حجم گسترده وارد بازار ایالات متحده کردند. |
| ۲۰۱۲ | الگنی تکنولوژیکز[۸] | ارتباطات | طی حمله‌ای سایبری به شرکت الگنی تکنولوژیکز تایید شبکه تمام کارکنان آن به سرقت رفت. این نفوذ مقارن با اختلافات تجاری این شرکت با یکی از شرکت‌های دولتی چین بود. |

۱ Night Dragon
۲ Cargill
۳ Dow Chemical
۴ Motorola
۵ American Superconductor Corporation
۶ Sinovel
۷ SolarWorld
۸ Allegheny Technologies

| سال | نهاد یا شرکت هدف | حوزه فعالیت | توضیحات |
|---|---|---|---|
| ۲۰۱۲ | ناسا[۱] | هوافضا | مهاجمان سایبری توانستند به کنترل کل شبکه ناسا دست یابند. احتمالا، این حمله باعث پیشرفت چین در فناوری‌های فضایی شده است. |
| ۲۰۱۲ | تلونت[۲] | انرژی | مهاجمان طی حمله‌ای سایبری به شرکت تلونت کانادا احتمالاً توانسته‌اند به شبکه بسیاری از خطوط نفت و گاز و شبکه‌های برق در آمریکای شمالی نفوذ کنند. |
| ۲۰۱۲ | نهادها و شرکت‌های مختلف | حوزه‌های مختلف | در عملیات موش سیاه[۳] ۲۱ نهاد دولتی، ۱۳ پیمانکار صنایع دفاعی، ۱۳ شرکت فعال در حوزه فناوری، ۶ گروه صنعتی و انبوهی از سازمان‌های غیرانتفاعی هدف حمله سایبری قرار گرفتند. اغلب اهداف در ایالات متحده بودند، اما اهدافی در کانادا، تایوان، ژاپن، کره جنوبی و بریتانیا نیز مورد حمله قرار گرفتند. |
| ۲۰۱۲ | جنرال موتورز[۴] | خودرو | دو نفر تلاش کردند اسرار تجاری مرتبط با فناوری وسایل نقلیه هیبریدی شرکت جنرال موتورز را سرقت کنند و در اختیار شرکت خودروساز چین رقیب آن قرار دهند. ارزش این فناوری ۴۰ میلیون دلار برآورد می‌شود. |
| ۲۰۱۲ | ستاد فرماندهی ترابری ایالات متحده آمریکا | پایگاه صنایع دفاعی | هکرهای چینی به ستاد فرماندهی ترابری ایالات متحده آمریکا دسترسی یافتند و از طریق پیمانکاران صنایع دفاعی حداقل ۲۰ مورد نفوذ به لوجستیک و سامانه‌های تامین ارتش ایالات متحده را انجام دادند. |
| ۲۰۱۳ | نیویورک تایمز[۵] و وال | رسانه | هکرهایی که مقرر آنها در چین بوده است، احتمالا در واکنش به گزارش‌هایی که در مورد مسایل مالی خانواده ون ژیابائو[۷] (نخست وزیر سابق چین) منتشر شد، سامانه‌های رایانه‌ای نیویورک تایمز و وال استریت ژورنال را مورد هدف حمله سایبری قرار دادند. |

۱ National Aeronautics and Space Administration (NASA)

۲ Telvent

۳ Shady RAT

۴ General Motors

۵ New York Times

۷ Wn Jiabao

| سال | نهاد یا شرکت هدف | حوزه فعالیت | توضیحات |
|---|---|---|---|
| | استریت ژورنال[۱] | | |
| ۲۰۱۳ | نهادها و شرکت‌های مختلف | فضایی | هکرهای چینی تلاش کردند با ۱۲۳ همه به طراحی‌ها و فناوری‌های مرتبط با پهپادها شرکت‌های آمریکایی دست یابند. |
| ۲۰۱۴ | کامیونیتی هلس سیستمز[۳] | بهداشت و درمان | در سال ۲۰۱۴، هکرهای چینی به شبکه‌های شرکت کامیونیتی هلس سیستمز حمله کردند و اطلاعات شخصی ۴,۵ میلیون نفر، نظیر شماره تامین اجتماعی آنها را ربودند. |
| ۲۰۱۴ | زیمنس[۴] | تولید صنعتی | یک تبعه چینی در سال ۲۰۱۴ به شبکه‌های شرکت زیمنس دسترس پیدا کرد و در سال ۲۰۱۵ بیش از ۴۰۰ گیگا بایت داده در مورد اسرار تجاری این شرکت را ربود. |
| ۲۰۱۴ | انتم[۵] | مراقبت درمانی | سوابق درمان حدود ۸۰ میلیون نفر، که در اختیار شرکت بیمه سلامت انتم بود، منتشر شد. دسترسی به این اطلاعات با استفاده از نوعی بدافزار انجام شده بود. |
| ۲۰۱۵ | تریمبل[۶] | نرم‌افزار | بین دسامبر ۲۰۱۵ و مارس ۲۰۱۶، چند تبعه چینی ۲۷۵ مگابایت داده متعلق به شکل تریمبل را ربودند. قرار بود این داده‌ها برای توسعه سامانه‌های ناوبری جهانی مورد استفاده قرار گیرند. |
| ۲۰۱۵ | یونایتد ایرلاینز[۷] | هوانوردی | هکرهای چینی برای جمع‌آوری اطلاعات به شبکه‌های شرکت یونایتد ایرلاینز نفوذ کردند. |
| ۲۰۱۶ | شرکت‌های مختلف | نیمه رساناها | سه گروه مستقر در چین برای جمع‌آوری اطلاعات به شبکه چهار شرکت فعال در حوزه ساخت نیمه‌رسانا نفوذ کردند. |

[۱] Wall Street Journal

[۳] Community Health Systems

[۴] Siemens

[۵] Anthem

[۶] Trimble

[۷] United Airlines

| سال | نهاد یا شرکت هدف | حوزه فعالیت | توضیحات |
|---|---|---|---|
| ۲۰۱۶ | شرکت‌های مختلف | فناوری اطلاعات | گروه ای‌پی‌تی ۱۰ برای جمع‌آوری اطلاعات، در عملیات کلود هوپر[1]، به چند شرکت ارائه‌دهنده خدمات فناوری اطلاعات حمله کردند. |
| ۲۰۱۷ | مدروبوتیکز کورپوریشن[2] | روبات | یک شهروند دو تابعیتی کانادایی و چینی به دفاتر شرکت مدروبوتیکز کورپوریشن دسترسی فیزیکی پیدا کرد و تلاش نمود با استفاده از رایانه‌ها و سایر تجهیزات شبکه اطلاعاتی را برباید. این فرد قبلاً تلاش کرده بود که به صورت دیجیتالی با تعدادی از کارکنان در شرکت ارتباط برقرار کند. |
| ۲۰۱۷ | نهادها و شرکت‌های مختلف | سیاست‌گذاری عمومی | جاسوسان چینی حداقل ۶ حمله با هدف جاسوسی سایبری به منظور دستیابی به اسناد مرتبط با راهبرد نظامی ایالات متحده آمریکا را انجام دادند. |
| ۲۰۱۸ | پیمانکار نامشخص | صنایع دفاعی | هکرهای منتسب به دولت چین داده‌های حساس مربوط به پروژه موشکلی موسوم به سی دراگون[3] و همچنین داده‌ها و اطلاعات مربوط به سیگنال‌ها و حسگرهای مرتبط با سامانه‌های رمزنگاری را از شرکتی که روی جنگ زیردریایی کار می‌کرد، دزدیدند. |

جدول ۱: مصادیق عملیات‌های سایبری چین

ماخذ: کوپر (۲۰۱۸)

## ۳-۳-روسیه

روسیه دارای برنامه سایبری آفندی[1] به شدت پیشرفته است. بر خلاف چین، روسیه تمایل بیشتری به استفاده از جنگ سایبری علیه کشورهایی که به نوعی متحد آمریکا محسوب می‌شوند، نشان داده است. حملات سایبری روسیه علیه استونی در بهار ۲۰۰۷ از اولین مصادیق جنگ اقتصادی سایبری محسوب می‌شود (زیلبرمن[2]، ۲۰۱۸). این حملات که در ابتدا به شکل ممنوعیت از دسترسی به خدمات بود، تارنماهای دولتی را از کار انداخت و توانایی دولت در ارتباط با شهروندان را مختل کرد. مراکز خبری نیز مورد حمله قرار گرفتند. در

1.Offensive
2.Zilberman

نهایت، بزرگ‌ترین بانک استونی، موسوم به هانسابانک[1] به طور موقت تمام فعالیت‌های خود را متوقف کرد. این حمله تقریباً کل نظام مالی استونی را تا مرز سقوط کشاند. به نظر می‌رسد قصد روسیه از این اقدامات تضعیف دولت استونی و تاثیرگذاری بر تصمیمات این کشور، مثلاً در زمینه تغییر مکان یادبود جنگ جهانی دوم، بوده است. از کار افتادن حسگرها و دوربین‌های کنترلی خط لوله انتقال نفت باکو – تفلیس – جیحان[2] در سال ۲۰۰۸ که باعث آسیب فیزیکی و از دست رفتن بیش از یک میلیارد دلار درآمد شد، نیز به روسیه نسبت داده می‌شود (روبرستون و ریلی[3]، ۲۰۱۴). این حمله، که در سطح تاکتیکی از مصادیق خرابکاری سایبری محسوب می‌شود، در سطح راهبردی نمونه‌ای از عملیات‌های جنگ اقتصادی سایبری است. از گذشته، روسیه مخالف ایجاد خط لوله باکو – تفلیس – جیحان و سایر تلاش‌ها برای انتقال نفت و گاز دریای خزر به بازار از طریق کنار گذاشتن این کشور بوده است. نکته مهم این که، ۳ روز پس از خرابکاری سایبری مذکور، جنگ روسیه – گرجستان آغاز شد. با در نظر گرفتن این جنگ، به نظر می‌رسد، خرابکاری در خط لوله باکو – تفلیس – جیحان بخشی از جنگ ترکیبی گسترده‌تر روسیه علیه گرجستان بوده است. در سال ۲۰۱۵، هکرهای مرتبط با روسیه شبکه برق اوکراین را از کار انداختند (زیلبرمن، ۲۰۱۸). این مساله باعث خاموشی‌های گسترده موقت در اوکراین شد. حمله مذکور باعث نابودی حجم انبوهی از اطلاعات مهم وزارت خزانه‌داری اوکراین نیز شد. به این ترتیب،

1.Hansabank
2.Baku-Tbilisi-Ceyhan pipeline
3.Roberston and Riley

مهاجمان توانستند از طریق وارد کردن تاثیرات اقتصادی منفی بر این کشور، امنیت ملی آن را تضعیف کنند. در سطح تاکتیکی، می‌توان این حمله سایبری را هم به عنوان نوعی خرابکاری سایبری و هم به مثابه نوعی تروریسم سایبری محسوب کرد. همچنین، در سطح راهبردی، این حمله از مصادیق جنگ اقتصادی سایبری است. حمله سایبری نوت‌پتیا[1]، که با زیان برآوردی بیش از ۱۰ میلیارد دلاری از مخرب‌ترین حملات سایبری تا کنون محسوب می‌شود، نیز به عنوان حمله‌ای سایبری علیه اوکراین شروع شد (گرینبرگ[2]، ۲۰۱۸). در این حملات که طی سال‌های ۲۰۱۶ و ۲۰۱۷ انجام شد، نوعی باج‌افزار[3] رمزنگاری از نقایص سیستم عامل ویندوز استفاده می‌کرد و از طریق رمزنگاری فایل‌های سیستمی حافظه سخت رایانه‌ها مانع اجرای سیستم عامل می‌شد و در نهایت، کاربر را مجبور می‌کرد برای دسترسی به رایانه خود مبلغی را به صورت بیت‌کوین پرداخت نماید. اگرچه حدود ۸۰ درصد از حملات مذکور در اوکراین انجام شده بود، این حملات به کشورهای فرانسه، آلمان، ایتالیا، لهستان، بریتانیا، ایالات متحده آمریکا و استرالیا نیز گسترش یافت. کارشناسان بر این باورند که روسیه از اوکراین به عنوان محیط آزمایشگاهی برای توسعه و تکمیل قابلیت‌های تهاجمی سایبری استفاده کرده است.

### ۳-۴-کره شمالی

کره شمالی که برای سال‌ها با تحریم‌های شدید ایالات متحده

1.NotPetya
2.Greenberg
3.Ransomware

آمریکا و متحدانش روبرو بوده است، برای دسترسی به منابع مالی مورد نیاز خود از عملیات‌های سایبری استفاده می‌کنند. استفاده از باج‌افزارها، حک سایت‌های خرید و فروش رمزینه‌پول‌ها[1] و حک سیستم‌های پرداخت بین‌بانکی از مهم‌ترین روش‌های مورد استفاده کره شمالی در جنگ سایبری با زمینه-های اقتصادی بوده‌اند. کره جنوبی یکی از کشورهای هدف اصلی حملات سایبری کره شمالی بوده است. کارشناسان برآورد می‌کنند که هکرهای کره شمالی هر روز به طور متوسط ۱٫۵ میلیون نفوذ سایبری[2] به رایانه‌های کره جنوبی انجام می‌دهند (ها و ماکسول، ۲۰۱۸). اگرچه عملیات‌های سایبری کره شمالی هنوز مصداق جنگ اقتصادی سایبری، بر اساس تعریف ارائه شده توسط راویش و فیکسلر نیستند، اما حاکی از توانمندی‌های سایبری این کشور است که ممکن است در آینده به مصادیق کامل جنگ اقتصاد سایبری منتهی شوند. نخستین قابلیت‌های سایبری کره شمالی در حوزه جنگ سایبری در جولای ۲۰۰۹ ظهور پیدا کرد. در آن زمان هکرهای وابسته به کره شمالی طی مجموعه‌ای از حملات سایبری به ۲۷ وب سایت کره جنوبی و آمریکا که معلق به نهادهای دولتی، بانک‌ها و شرکت‌های بزرگ بودند، حمله کردند (شرستوبیتوف[3] و دیگران، ۲۰۱۲). هدف این حملات که به صورت ممانعت از دسترسی به خدمات انجام شد، کاهش سرعت و اختلال در دسترسی به خدمات وبی در ایالات متحده و کره جنوبی بود.

1.Cryptocurrency exchange
2.Cyber Intrusion
3.Sherstobitoff

در سال ۲۰۱۱، حمله سایبری موسوم به تن دیز آو رین[1] برای مدت ده روز کارکرد شعب، دستگاه‌های خودکار و خدمات بانکی برخط بانک نونگهیوپ کره جنوبی را مختل کرد (هارلان و ناکاشیما[2]، ۲۰۱۱). البته حمله به بانک مذکور، بخشی از حمله گسترده‌تر به دولت، ارتش و شرکت‌های صنعتی کره جنوبی بود. در سال ۲۰۱۳ نیز هکرهای تحت حمایت دولت کره شمالی حمله سایبری موسوم به دارک‌سئول[3] را انجام دادند (راویش و فیکسلر، ۲۰۱۷). این حمله علیه سه بانک و سه شرکت رسانه‌ای بزرگ کره جنوبی انجام شد. هکرها از بدافزاری پیچیده استفاده کردند که به هزاران رایانه صدمه وارد و تعدادی از سرورهای بسیار مهم را مختل کرد. حمله مذکور نه تنها هزینه‌ای بالغ بر ۸۰۰ میلیون دلار را به بار آورد، بلکه از طریق مختل کردن فعالیت‌های سه بانک هدف، برای مدت ده روز باعث ایجاد تاخیر و سردرگمی در نظام مالی کره جنوبی شد. در نوامبر ۲۰۱۴ نیز هکرهای منتسب به کره شمالی، به سامانه‌های رایانه‌ای شرکت سونی پیکچرز اینترتینمنت حمله کردند. بین حمله سایبری مذکور و حمله دارک‌سئول مشابهت‌های ساختاری و تکنیکی فراوانی وجود داشته است (اداره تحقیقات فدرال[4]، ۲۰۱۴). اگرچه حمله سایبری مذکور به شرکت سونی پیکچرز به عنوان نمونه‌ای از تروریسم سایبری طبقه‌بندی می‌شود، اما نشان می‌دهد کره شمالی در حال دستیابی به توانمندی‌های است که ممکن است برای ضربه زدن به منافع اقتصادی شرکت‌های فعال در کشورهای متخاصم و دشمن نیز

1.Ten Days of Rain
2.Harlan and Nakashima
3.DarkSeoul
4.Federal Bureau of Investigation (FBI)

مورد استفاده قرار گیرد. برای نمونه، در نوامبر ۲۰۱۷، وزارت امنیت میهنی ایالات متحده آمریکا و اداره تحقیقات فدرال این کشور هشدار فنی زودهنگام مشترکی را صادر کردند مبنی بر این که فعالان سایبری مرتبط با کره شمالی صنایع هوا و فضا، ارتباطات و مالی این کشور را هدف گرفته‌اند (تیم آمادگی وضعیت اضطرار رایانه‌ای ایالات متحده آمریکا [1]، ۲۰۱۷). مشخص شد برخی از بدافزارهایی که در حمله به شرکت سونی پیکچرز مورد استفاده قرار گرفته بود، به رایانه‌هایی که مورد حمله قرار گرفته بودند دسترسی‌هایی از جنس در پشتی [2] داشتند. به این ترتیب، هکرها می‌توانستند در حمله به زیرساخت‌های اساسی در آمریکا از چنین قابلیت‌هایی استفاده کنند. در سال ۲۰۱۵، نیز حمله‌ای به شرکت کوریا هیدروپاور اند نوکلیر پاور [3] کره جنوبی انجام شد، که ویژگی‌های آن شبه عملیات‌های سایبری منتسب به کره شمالی، به ویژه شرکت سونی پیکچرز، بود (استاهلر و هاگارد [4]، ۲۰۱۵). مهاجمان اطلاعات شخصی حدود ۱۱ هزار نفر از کارکنان شرکت را منتشر کردند. همچنین، آنها اطلاعیه‌ای را در توئیتر منتشر کردند که طی آن ادعا کردند اطلاعات مربوط به راکتورهای هسته‌ای کره جنوبی را ربوده‌اند و سپس، اسناد سرقتی را به صورت برخط منتشر کردند. در نهایت، هکرها تهدید کردند که اگر شرکت ۳ راکتور از ۲۳ راکتور را خاموش نکند، به تاسیسات شرکت صدمه فیزیکی می‌زنند. حمله سایبری به بانک مرکزی بنگلادش منتسب به کره شمالی که

1.U.S. Computer Emergency Readiness Team
2.Backdoor access
3.Korea Hydro and Nuclear Power
4.Stahler and Haggard

قبلاً به آن اشاره شد، اگرچه به عنوان جنگ اقتصادی سایبری قابل طبقه‌بندی نیست، گویای توانایی‌های کره شمالی در استفاده از این نوع جنگ است. گسترش بازار رمزینه‌پول‌ها نیز فرصت‌های جدید برای فعالیت‌های سایبری اقتصادی کره شمالی فراهم کرده است. هک سایت‌های خرید و فروش رمزینه پول‌ها نمونه‌ای از فعالیت‌های مذکور بوده است. برای نمونه، بین آوریل و جولای ۲۰۱۷، مجموعه‌ای از حملات سایبری به سه شرکت خرید و فروش رمزینه پول انجام شد، که به هکرهای تحت امر کره شمالی نسبت داده می‌شوند (مک‌نامارا[1]، ۲۰۱۷). بین فوریه و می ۲۰۱۷ نیز هکرها با استفاده از باج‌افزار واناکرای[2] به بیش از ۲۳۰ هزار رایانه در بیش از ۱۵۰ کشورها جهان حمله کردند. این باج‌افزار نسبت به رمزنگاری ۱۷۶ فایل از انواع مختلف در هر رایانه اقدام می‌کرد و برای رمزگشایی فایل‌های رمزگشایی شده ۳۰۰ دلار به صورت بیت کوین طلب می‌کرد (شرکت سیمنتک[3]، ۲۰۱۷).

### ۳-۵-ایران

توانمندی‌های سایبری ایران به اندازه‌ای قابل ملاحظه بوده است که برخی از کارشناسان از آن به عنوان قدرت سایبری (کراندال و تایر، ۲۰۱۸) و بعضا به عنوان یکی از اعضای باشگاه ابرقدرت‌های سایبری[4] یاد می‌کنند (جونز[5]، ۲۰۱۶). نکته مهم در مورد ایران این است که توانمندی‌های سایبری آن به شکل قابل ملاحظه‌ای موثرتر از

1.MacNamara
2.WannaCry
3.Symantec
4.Cyber superpower
5.Jones

توانمندی‌های جنگ متعارف[1] آن است (لوئیس[2]، ۲۰۱۹). این مساله در تلاش ایران بر توسعه توانمندی‌های مرتبط با جنگ نامتقارن ریشه دارد. در اواسط سال ۲۰۱۲، حمله سایبری گسترده‌ای علیه شرکت نفت عربستان سعودی (آرامکو)[3] انجام شد که باعث نابودی حدود ۳۵ هزار رایانه (سه چهارم از رایانه‌های) این شرکت شد. در نتیجه حمله مذکور، این شرکت مجبور شد برای دریافت و ارسال پیام‌ها و مدیریت قراردادها و تدارکات به سامانه‌های آنالوگی بازگردد (پرلروت[4]، ۲۰۱۲). اگرچه مقامات رسمی ایران در این خصوص اظهار نظر نکردند، اما به نظر می‌رسد، حمله مزبور در پاسخ به اقدامات عربستان سعود در پشتیبانی از تحریم‌های اقتصادی تحمیلی بر ایران به بهانه برنامه هسته‌ای ایران و همچنین، حملات سایبری به سامانه‌های تولید وزارت نفت ایران و شرکت-های تابعه آن در اوایل سال ۲۰۱۲ انجام شد. این حمله سایبری گسترده نه تنها به یکی از تولیدکنندگان عمده نفت در جهان آسیب وارد کرد و باعث افزایش قیمت نفت شد، بلکه به اقتصاد عربستان سعودی نیز صدمه زد. طی سال‌های ۲۰۱۱ و ۲۰۱۳، حملات سایبری متعددی به حداقل ۴۶ بانک و نهاد خدمات مالی بزرگ آمریکایی، از جمله جی‌پی مورگان چیس[5]، بنک آف امریکا[6]، سی‌تی‌گروپ[7]، ولز فارگو[8]، یو.اس. بنکورپ[9]، فیدلیتی[10]، کپیتال وان[11]، بی‌بی‌اندتی[12]، امریکن اکسپرس[13] و بورس اوراق بهادار نیویورک در قالب ممانعت از دسترسی به خدمات انجام شد (وولز و فینکله[14]، ۲۰۱۶). این حملات مانع دسترسی صدها هزار نفر

1.Conventional warfare
2.Lewis
3.Saudi Arabian Oil Company (Aramco)
4.Perlroth
5.JP Morgan Chase
6.Bank of America
7.Citigroup
8.Wells Fargo
9.U.S. Bancorp
10.Fidelity
11.Capital One
12.BB&T
13.American Express
14.Volz and Finkle

از اشخاص و تعداد زیادی از شرکت‌ها به حساب‌های برخط خود شد و اصلاح این وضعیت ده‌ها میلیون دلار هزینه ایجاد کرد. وزارت دادگستری ایالات متحده آمریکا حملات مذکور و نیز حمله سایبری به سامانه کنترلی سد بومن[1] در حوالی نیویورک را به هکرهای ایرانی نسبت داد (وزارت دادگستری ایالات متحده آمریکا، ۲۰۱۶). اگرچه هدف انجام این حملات که به عنوان عملیات ابابیل[2] شناخته می‌شود، هنوز مشخص نشده، اما بر حسب شواهد می‌توان این حملات را در سطح تاکتیکی نوعی خرابکاری سایبری و در سطح راهبردی نوعی جنگ اقتصادی سایبری در نظر گرفت (فیکسلر و کیلوفو[3]، ۲۰۱۸). در فوریه ۲۰۱۴، حملات گسترده‌ای علیه شرکت آمریکایی لاس وگاس سندز[4] انجام شد که به ایران نسبت داده می‌شود (الگین و ریلی[5]، ۲۰۱۴). طی این حمله سه چهارم رایانه‌های شرکت از کار افتادند، رایانامه شرکت از حالت برخط خارج شد، همچنین تلفن‌ها و سایر پلت‌فرم‌های عملیاتی که با استفاده از آن‌ها شرکت ۱۴ میلیاردی اداره می‌شد، ضربه سنگین خورد. در نتیجه این حمله ۴۰ میلیارد صدمه مالی به شرکت مذکور وارد شد و بازگشت شبکه‌های شرکت یک هفته طول کشید.

1.Bowman
2.Ababil Operation
3.Fixler and Cilluffo
4.Las Vegas Sands Corporation
5.Elgin and Riley

# جمع بندی

# جمع‌بندی

در این گزارش، به اختصار برخی از مهم‌ترین مباحث مرتبط با جنگ اقتصادی سایبری مورد بررسی قرار گرفت. جنگ اقتصادی سایبری عرصه‌ای پویا و رو به گسترش است و بررسی جامع تمام مباحث مرتبط با آن خارج از حیطه گزارش حاضر است. پیشنهاد می‌شود در گزارش‌های آتی ابعاد تکنیکی، تاکتیکی و راهبردی عملیات‌های سایبری مهم در این حوزه مورد بررسی عمیق‌تر قرار گیرد. فعالیت‌های کشورهای مورد بررسی در حوزه جنگ اقتصادی سایبری بر مبنای دکترین‌های مختلفی سازمان‌دهی شده است. این دکترین‌ها ناظر به نقاط قوت و ضعف کشور مهاجم و کشور هدف حمله و نیز اهداف کشور مهاجم است. شناخت دکترین‌های جنگ اقتصادی سایبری کشورهای مختلف و راهبردهایی که بر مبنای این دکترین‌ها طراحی و اجرا می‌شود، هم از منظر تقویت توانمندی‌های دفاعی کشور در مواجهه با تهدیدها و جنگ‌های اقتصادی سایبری فعلی تحمیلی بر کشور و نیز تهدیدها و جنگ‌های

اقتصادی احتمالی در آینده ضروری است. بررسی کارکرد این دکترین‌ها در نحوه سازماندهی جنگ اقتصادی سایبری و تاثیر آن‌ها در موفقیت یا عدم موفقت این جنگ‌ها نیز از نظر آفندی و پدافندی حاوی آموزه‌های ارزشمندی برای سیاست‌گذاری‌ها و اقدامات مرتبط در ایران است. بر این اساس، پیشنهاد می‌شود بررسی اقدامات کشورها در حوزه جنگ اقتصادی سایبری با تاکید بر دکترین‌های مورد استفاده آنها به منظور شناسایی آموزه‌های مرتبط برای سیاست‌گذاری و اقدام در ایران در دستور کار قرار گیرد.

ایران، یکی از کشورهایی بوده که با شدیدترین مصادیق جنگ اقتصادی سایبری مواجه شده است. در نتیجه، تامین امنیت سایبری برای کشور از طریق دستیابی به مولفه‌های قدرت سایبری به منظور عملیاتی کردن دفاع سایبری در مقابل جنگ اقتصادی سایبری یا ایجاد بازدارندگی در مقابل تهدید اقتصادی سایبری در کنار ایجاد تاب‌آوری اقتصادی سایبری مساله‌ای بسیار مهم است. این مساله مستلزم شناسایی آسیب‌پذیری‌های کشور از منظر جنگ اقتصادی سایبری است. غالباً، تهدیدهای مرتبط با جنگ اقتصادی سایبری تحمیلی به کشور نیز ناظر به همین آسیب‌پذیری‌ها بوده‌اند یا خواهند بود. با شناسایی آسیب‌پذیری‌ها و تهدیدهای مذکور اولویت‌های کشور در حوزه امنیت سایبری، دفاع سایبری، بازدارندگی سایبری و بازدارندگی سایبری تعیین می‌شود. بر این اساس، پیشنهاد می‌شود تهدیدهای پیش روی کشور در حوزه جنگ اقتصادی سایبری به طور مستمر

مورد رصد و پایش قرار گیرد.

همان طور که پیش‌تر اشاره شد، به طور کلی، یکی از چالش‌های مهم در زمینه تامین امنیت سایبری، به ویژه از منظر جنگ اقتصادی سایبری، نامشخص بودن وظایف و اختیارات دولت و اشخاص غیردولتی در این خصوص است. بر این اساس، پیشنهاد می‌شود تعیین وظایف و اختیارات دولت و اشخاص غیردولتی در تامین امنیت سایبری در مواجهه با جنگ اقتصادی سایبری، به طور خاص و جنگ سایبری، به طور عام در دستور سیاستگذاران قرار گیرد. ضروری است در تامین امنیت سایبری از مشارکت تمام ذینفعان فضای سایبر، به ویژه حیطه مرتبط با فعالیت‌های اقتصادی، استفاده شود.

همچنین، ضروری است کشور در حوزه جنگ اقتصادی سایبری به توانمندی‌های آفندی مناسب نیز دست یابد. موفقیت در جنگ اقتصادی سایبری ایجاب می‌کند که ارتقای آن دسته از توانمندی‌های آفندی در حوزه جنگ اقتصادی سایبری در دستور کار قرار گیرد که به بهترین شکل می‌توانند از آسیب‌پذیری‌های کشورهای متخاصم بهره‌جویی نمایند. بر این اساس، پیشنهاد می‌شود ضمن تعریف کشورهای متخاصم در حوزه جنگ اقتصادی سایبری، شناسایی مستمر آسیب‌پذیری‌های آن‌ها در دستور کار قرار گیرد. علاوه بر این، ضروری است راهبرد مشخص برای تقویت توانمندی‌های سایبری کشور، به ویژه در حوزه جنگ اقتصادی سایبری، در دستور کار سیاستگذاران قرار گیرد. ایالات متحده آمریکا که آغازگر

جنگ اقتصادی سایبری علیه ایران و برخی از کشورهای دیگر بوده و نیز، نسبت به اعمال تهدید به استفاده از این نوع جنگ علیه کشورهای مختلف اقدام کرده است، با واکنش متقابل برخی از کشورهای تحت حمله یا تهدید روبرو شده است. جنگ‌های اقتصادی سایبری قابلیت این را دارند که صدمات اقتصادی قابل ملاحظه‌ای را به آمریکا و متحدانش وارد و از این طریق، امنیت ملی آن‌ها را با مخاطره روبرو کنند. به این ترتیب، آسیب‌پذیری‌های اقتصادی سایبری آمریکا و متحدانش به نقطه ضعف اقتصادی و امنیتی آن‌ها تبدیل می‌شود. برای نمونه، اگرچه پلتفرم‌های مالی سایبری، نظیر پلتفرم‌های تسویه مرکزی[1] می‌توانند به مثابه تنگه[2] مالی برای اعمال فشار بر رقیبان، حریفان و دشمنان مورد بهره‌جویی قرار گیرند، اما تمرکز روابط مالی متقابل روی آن‌ها باعث آسیب‌پذیری این پلتفرم‌ها و کشورهایی که از آنها بهره‌برداری می‌کنند، نیز می‌شود. مثلاً، در حال حاضر، سوئیفت بیش از ۱۱ هزار نهاد مالی در بیش از ۲۰۰ کشور و قلمرو سرزمینی را به هم متصل کرده است. هر گونه اختلال در این شبکه می‌تواند پیامدهای اقتصادی و سیاسی منفی فاجعه‌باری را به بار آورد. چنین آسیب‌پذیریی به پلتفرم‌های مالی سایبری محدود نمی‌شود و تقریباً تمام کسب‌وکارهای پلتفرمی سایبری از آسیب‌پذیری مشابهی رنج می‌برند. در عصری که پلتفرم‌ها تقریباً تمام ابعاد زندگی مردم آمریکا را در بر گرفته‌اند، آسیب‌پذیری پلتفرم‌ها، باعث آسیب‌پذیری کل اقتصاد آمریکا و از آن طریق،

1.Central clearing platforms
2.Choke point
در راهبرد نظامی، تنگه یا خفتگاه عارضه ای طبیعی، نظیر دره یا تنگه دریایی، یا انسانی نظیر پل است که نیروی نظامی مجبور به عبور از آن است. عبور از این موقعیت، که معمولاً جبهه به مراتب باریک تری دارد به شکل قابل ملاحظه ای توان رزمی نیروی نظامی را کاهش می دهد.

امنیت ملی آن کشور می‌شود. به دلیل وجود چنین آسیب‌پذیری‌هایی است که در تازه‌ترین سند راهبرد امنیت ملی ایالات متحده آمریکا[1] جنگ اقتصادی سایبری مورد توجه قرار گرفته است (کاخ سفید، ۲۰۱۷). فراتر از این، اهمیت امنیت فضای سایبر در تامین امنیت ملی ایالات متحده باعث شده که دولت این کشور بر مبنای راهبرد امنیت ملی خود، در سال ۲۰۱۸ اقدام به ارائه راهبرد سایبری ملی[2] نیز نماید. در این سند، ضرورت ایجاد ابتکار بین‌المللی بازدارندگی سایبری توسط ایالات متحده آمریکا و متحدانش مورد تاکید قرار گرفته است.

1.National Security Strategy of United States of America

۲.راهبرد امنیت ملی سندی است که به طور ادواری توسط قوه مجریه دولت ایالات متحده آمریکا برای ارائه به کنگره آمریکا تهیه می شود. این سند حاوی چالش های عمده امنیت ملی ایالات متحده آمریکا و برنامه دولت این کشور برای مقابله با آنها است.

National Cyber Strategy

# منابع

[1]Baldwin, D. A. (2016, January 21). Economic statecraft. Retrieved November 2019 ,11, from Encyclopædia Britannica: https://www.britannica.com/topic/economic-statecraft

[2]Bissell, K., & Ponemon, L. (2019). The Cost of Cybercrime: Ninth Annual Cost of Cybercrime Study. Accenture.

[3]Bjorck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience - Fundamentals for a Definition. In Advances in Intelligent Systems and Computing (pp. 316-311). Springer.

[4]Cohn, B. J. (2019). Currency statecraft monetary rivalry and geopolitical ambition. Chicago London: The University of Chicago Press.

[5]Cooper, Z. (2018). Understanding the Chinese Communist Party›s Approach to Cyber_Enabled Economic Warfare. Washington, D.C.: Foundation for Defense of Democracies.

[6]Council on Foreign Relations. (n.d.). Cyber Operations Tracker. Retrieved February 2020 ,6, from Council on Foreign Relations: https://www.cfr.org/interactive/cyber-operations

[7]Crandall, M., & Thayer, B. (2018, November 25). The Balance of Cyberpower. Retrieved January 2020 ,9, from National Interest: https://nationalinterest.org/feature/balance-cyberpower36637-

[8]Cybersecurity and Infrastructure Security Agency. (2019, November 20). Understanding Denial-of-Service Attacks. Retrieved February 6,

2020, from Cybersecurity and Infrastructure Security Agency: https://www.us-cert.gov/ncas/tips/ST015-04

[9]Department of Defense. (2019). Dictionary of Military and Associated Terms. Department of Defense.

[10]Department Of Homeland Security. (2016, October 7). Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. Retrieved January 2020 ,7, from Department Of Homeland Security: https://www.dhs.gov/news/07/10/2016/joint-statement-department-homeland-security-and-office-director-national

[11]Director of National Intelligence. (2017, January 6). Background to 'Assessing Russian Activities and Intentions in Recent US Elections': The Analytic Process and Cyber Incident Attribution. Washington, DC: Director of National Intelligence.

[12]Dubowitz, M., & Fixler, A. (2015). Cyber-Enabled 'Swift' Warfare: Power, Blowback, and Hardening American Defenses. Wachington D.C.: Hudson Institute.

[13]Editors of Encyclopaedia Britannica. (2019, November 21). Total War. Retrieved December 2019 ,8, from Encyclopaedia Britannica: https://www.britannica.com/topic/total-war

[14]Eichengreen, B., & Xia, G. (2018). China and the SDR: Financial

Liberalization through the Back Door. Waterloo: Centre for International Governance Innovation.

[15]Elgin, B., & Riley, M. (2014, December 13). Now at the Sands Casino: An Iranian Hacker in Every Server. Retrieved January 2020 ,12, from Bloomberg: https://www.bloomberg.com/news/articles/11-12-2014/iranian-hackers-hit-sheldon-adelsons-sands-casino-in-las-vegas

[16]Engloff, F. (2017). Cybersecurity and the Age of Privateering. Washington, D.C.: Carnegie Endowment for International Peace.

[17]Erdbrink, T. (2012, April 23). Facing Cyberattack, Iranian Officials Disconnect Some Oil Terminals From Internet. Retrieved February 2020 ,6, from The New York Times: https://www.nytimes.com/24/04/2012/world/middleeast/iranian-oil-sites-go-offline-amid-cyberattack.html

[18]Federal Bureau of Investigation. (2014, December 19). Update on Sony Investigation. Retrieved January 2020 ,14, from Federal Bureau of Investigation: https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

[19]Fixler, A., & Cilluffo, F. (2018). Evolving Menace: Iran›s Use of Cyber-Enabled Economic Warfare. Washington, DC: Foundation for Defense of Democracies.

[20]Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the

Most Devastating Cyberattack in History. Retrieved January 2020 ,10, from Wired: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[21]Ha, M., & Maxwell, D. (2018). Kim Jong Un›s ‹All-Purpose Sword›: North Korean Cyber-Enabled Economic Warfare. Washington, DC: Foundation for Defense of Democracies .

[22]Harlan, C., & Nakashima, E. (2011, August 29). Suspected North Korean cyber attack on a bank raises fears for S. Korea, allies. Retrieved January 2020 ,13, from The Washington Post: https://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raisesfears-

[23]Harrell, P., & Rosenber, E. (2019). Economic Dominance, Financial Technology, and the Future of U.S. Economic Coercion. Washington D.C.: Center for a New American Security.

[24]Ikenberry, J., & Lim, D. J. (2017). China's emerging institutional statecraft: The Asian Infrastructure Investment Bank and the Prospects for Counter-hegemony. Washington D.C.: Brookings Institute.

[25]Joint Chiefs of Staff. (2018). Cyberspace Operations. Joint Chiefs of Staff.

[26]Jones, S. (2016, April 26). Iran opens new front: cyber warfare. Retrieved January 2020 ,9, from Financial Times: https://www.ft.com/

content/15e1acf0-0a11-47e-6b0f61-1f222853ff3

[27]Kamali Dehghan, S. (2012, April 23). Iranian oil ministry hit by cyber-attack. Retrieved Janauary 2020 ,7, from The Guardian: https://www.theguardian.com/world/2012/apr/23/iranian-oil-ministry-cyber-attack

[28]Libicki, M. (1995). What is Information Warfare? Washington, DC: Center for Advanced Concepts and Technology, National Defense University.

[29]Lichtblau, E., & Risen, J. (2006, June 23). Bank Data Is Sifted by U.S. in Secret to Block Terror. Retrieved January 2020 ,11, from The New York Times: https://www.nytimes.com/23/06/2006/washington/23intel.html?hp&ex=1151121600&en=18f9ed2cf37511d5&ei=5094&partner=homepage

[30 Maloney, S. (2018, January 9). WHAT IS AN ADVANCED PERSISTENT THREAT (APT)? Retrieved December 2019 ,18, from Cybereason: https://www.cybereason.com/blog/advanced-persistent-threat-apt

[31]McDowell, D. (2017). Brother, Can You Spare a Billion? The United States, the IMF, and the International Lender of Last Resort. New York: Oxford University Press.

[32]McNamara, L. (2017, September 11). Why is North Korea

So Interested in Bitcoin? Retrieved January 2020 ,14, from FireEye: https://www.fireeye.com/blog/threatresearch/09/2017/north-korea-interested-in-bitcoin.html

[33]National Counterintelligence and Security Center. (2018). Foreign Economic Espionage in Cyberspace. Washington, DC: National Counterintelligence and Security Center.

[34]Newman, A. (2019, September 1). US and China are weaponising global trade networks: Businesses and supply chains have become pawns in a strategic 'quiet war'. Retrieved December 2019 ,9, from Financial Times: https://www.ft.com/content/a8ab8cd-2c99c11-e-9af-46b09e8bfe60c0

[35]Newman, L. H. (2017, September 12). What to Do if You're Being Doxed. Retrieved February 2020 ,6, from Wired: https://www.wired.com/story/what-do-to-if-you-are-being-doxed/

[36]Office of Terrorism and Financial Intelligence. (2018, May 23). Office of Terrorism and Financial Intelligence. Retrieved December ,9 2019, from U.S. Department of the Treasury: https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx

[37]Perlroth, N. (2012, October 23). In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. Retrieved January 2020 ,9, from New York Times:

https://www.nytimes.com/24/10/2012/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html?_r=0

[38]RAND CORPORATION. (n.d.). https://www.rand.org/topics/cyber-warfare.html. Retrieved December 2019 ,8, from RAND CORPORATION: https://www.rand.org/topics/cyber-warfare.html

[39]Ravich, S. F., & Fixler, A. (2017). Framework and Terminology for Understanding Cyber-Enabled Economic Warfare. Washington D.C.: Foundation of Defense of Democracies.

[40]Robertson, J., & Riley, M. (2014, December 10). Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar. Retrieved January 2020 ,4, from Bloomber: https://www.bloomberg.com/news/articles/10-12-2014/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar

[41]Sanger, D. E. (2012, June 1). Obama Order Sped Up Wave of Cyberattacks Against Iran. Retrieved January 2020 ,12, from The New York Times: https://www.nytimes.com/01/06/2012/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0

[42]Shambaugh, G. (1998, July 20). Economic warfare. Retrieved November 2019 ,5, from Encyclopædia Britannica: https://www.britannica.com/topic/economic-warfare

[43]Shambaugh, G. (1998, July 20). Economic warfare. Retrieved

December 2019 ,8, from Encyclopedia Britannica: https://www.britannica.com/topic/economic-warfare

[44]Sherstobitoff, R., Liba, I., & Walter, J. (2012, November 28). Dissecting Operation Troy: Cyberespionage in ROK. Retrieved January 2020 ,13, from McAfee: https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2013/dissecting-operation-troy.pdf

[45]Stahler, K., & Haggard, S. (2015). More Cyber: The Korea Hydro and Nuclear Power Company (KHNP) Hacks. Washington, DC: Paterson Institute for International Economics.

[46]Symantec. (2017, May 23). What you need to know about the WannaCry Ransomware. Retrieved January 2020 ,14, from Symantec: https://www.symantec.com/blogs/threatintelligence/wannary-ransomware-attack/

[47]Taylor, A. (2016, February 1). An alleged rape sparked tensions between Russia and Germany. Now police say it was fabricated. Retrieved January 2020 ,07, from Washington Post: https://www.washingtonpost.com/news/worldviews/wp/29/01/2016/an-alleged-rape-sparked-tensions-between-russia-and-germany-now-police-say-it-was-fabricated/

[48]Taylor, H. (2018, September 21). What Are Cyber Threats: How They Affect You and What to Do About Them. Retrieved January 10,

2020, from Prey Nation: https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/

[49]Tepper, J., & Hearn, D. (2019). The Myth of Capitalism: Monopolies and the Death of Competition. Hoboken: John Wiley & Sons, Inc.

[50]The White House. (2017). National Security Strategy of the United States of America. Washington D.C.: The White House.

[51]The White House. (2018). National Cyber Strategy. Washington D.C.: The White House.

[52]U. S. Department of Defense. (2015). Cyber Strategy. Washington, DC: U.S. Department of Defense.

[53]U.S. Computer Emergency Readiness Team. (2017, November 22). Alert (TA318-17A): Hidden Cobra – North Korean Remote Administration Tool: FALLCHILL. Retrieved January 2020 ,14, from Cyber Security and Infrastructure Security Agency: https://www.us-cert.gov/ncas/alerts/TA318-17A

[54]U.S. Department of Justice, S. (2016, March 24). Manhattan U.S. Attorney Announces Charges Against Seven Iranians For Conducting Coordinated Campaign Of Cyber Attacks Against U.S. Financial Sector On Behalf Of Islamic Revolutionary Guard Corps-Sponsored Entities. Retrieved January 2020 ,9, from U.S. Department of Justice: https://www.justice.gov/usao-sdny/pr/manhattan-us-attorney-announces-

charges-against-seven-iranians-conducting-coordinated

[55]van Bergeijk, P. A., & Sewyn, M. (2009). Economic Diplomacy and Economic Security. In C. G. Costa (Ed.), NEW FRONTIERS FOR ECONOMIC DIPLOMACY (pp. 54-37). Instituto Superior de Ciéncias Sociais e Politicas.

[56]Volz, D., & Finkle, J. (2016, March 24). U.S. indicts Iranians for hacking dozens of banks, New York dam. Retrieved January 2020 ,9, from Reuters: https://www.reuters.com/article/us-usa-iran-cyber-idUSKCN0WQ1JF

[57]Zarate, J. C. (2013). Treasury›s War: The Unleashing of a New Era of Financial Warfare. New York: Public Affairs.

[58]Zarate, J. C. (2015). The Cyber Financial Wars on the Horizon: The Convergence of Financial and Cyber Warfare and the Need for a 21st Century National Security Response. Washington D.C.: Foundation for Defense of Democracies.

[59]Zilberman, B. (2018). Kaspersky and Beyond: Understanding Russia›s Approach to Cyber-Enabled Economic Warfare. Washington, DC: Foundation for Defense of Democracies.

[۶۰]شورای عالی فضای مجازی. (۱۳۹۳, بهمن ۲۳). مصوبات جلسه پانزدهم شورای عالی فضای مجازی در خصوص تعریف و الزامات حاکم بر تحقق شبکه ملی اطلاعات و بودجه سال ۱۳۹۳ مرکز ملی فضای مجازی. بازیابی در بهمن ۱۷, ۱۳۹۸، از روزنامه رسمی جمهوری اسلامی ایران: http://www.rrk.ir/Laws/ShowLaw.aspx?Code=۱۶۴۰

مرکز ملی فضای مجازی
پژوهشگاه فضای مجازی

csri.majazi.ir

حـوزه فضـای مجـازی بـه انـدازه انقـلاب اسـلامی اهمیـت دارد. ایـن فضـا مثـل یـک رودخانـه پـر از آب و خروشـان اسـت کـه مـی آیـد و دائمـاً هـم بـر آب آن افـزوده و خروشـان تـر مـی شـود. اگـر مـا بـر ایـن رودخانـه تدبیـر کنیـم و برنامـه داشـته باشـیم، زه‌کشـی کنیـم و هدایـت کنیـم ایـن رودخانـه را تـا بـه سـد بریـزد، می‌شـود فرصـت. اگـر رهایـش کنیـم و برنامـه‌ای بـرای آن نداشـته باشـیم می‌شـود یـک تهدید.

csri.majazi.ir