بازدارندگی سایبری روسیه از منظر اروپا

سمیه قنبری [1]
حسین خانی [2]

مقاله حاضر در تلاش برای علت‌یابی به‌کارگیری ظرفیت‌های فضای مجازی از سوی مسکو برای دفاع سایبری در برابر حملات غرب به‌دنبال پاسخی مناسب برای این دو پرسش برآمده‌است که «دلیل اصلی روسیه برای توسل به سلاح سایبری علیه اهداف غربی چیست؟» و «نبرد سایبری روسیه در برابر غرب از چه ویژگی‌هایی برخوردار است و به چه شیوه‌ای دنبال می‌شود؟» این مطالعه از نوع توصیفی-تحلیلی بوده و در دسته پژوهش‌های پس‌رویدادی علی قرار می‌گیرد. در فرایند تحلیل داده‌ها نیز از روش‌شناسی استنتاجی در چارچوب مفاهیم جنگ سایبری و حمله‌های سایبری سیاسی استفاده شده‌است. یافته‌های مقاله نشان می‌دهند، دلیل اصلی مسکو از کاربرد سلاح سایبری علیه اهداف غربی، مقابله با اقدام‌های خصمانه غرب به‌ویژه در سرزمین‌های پساکمونیستی باتوجه به سهولت انکارپذیری بالا و نیز ضعف روسیه در مؤلفه‌های جنبشی است. مهم‌ترین ویژگی نبرد سایبری روسیه علیه غرب به توسعه مفهوم بازدارندگی سایبری نزد این کشور تا ایجاد موازنه در شرایط رقابت‌های نظامی و سیاسی متعارف بازمی‌گردد. بر این پایه، نبرد ترکیبی روسیه علیه غرب به طور عمده به شیوه حمله‌های منع سرویس توزیع‌شده، هک‌کردن و به‌کارگیری بدافزارها انجام می‌شود.

واژگان کلیدی: نبرد سایبری، بازدارندگی سایبری، روسیه، کشورهای پساکمونیستی و اتحادیه اروپایی.

---

[1]. نویسنده مسئول، استادیار گروه علوم سیاسی، دانشگاه پیام‌نور، تهران، ایران.
Email:s.ghanbari@pnu.ac.ir

[2]. استادیار گروه علوم سیاسی، دانشگاه پیام‌نور، تهران، ایران.
Email:khani630@yahoo.com

- این مقاله علمی _ پژوهشی می‌باشد، تاریخ دریافت۹۹/۶/۲۷ و تاریخ پذیرش۹۹/۸/۱۴

مقدمه

پیشرفت سریع فناوری‌های اطلاعات و ارتباطات (فاوا)[1] از اواسط دهه ۸۰ میلادی انقلابی در زیرساخت اطلاعات[2] شامل شبکه‌های ارتباطی و نرم‌افزارهای مربوطه پدیدآورده و تعامل میان مردم و سازمان‌ها را تسهیل کرده‌است. این بدان معنی است که دوران معاصر دسترسی سریع، نامحدود و بدون مانع به اطلاعات را تجربه‌می‌کند و به‌همین جهت نیز "عصر اطلاعات[3]" نام گرفته‌است. این امر به‌ویژه در کشورهای صنعتی توسعه‌یافته صادق‌است، جایی‌که تمام یا بخش عمده زیرساخت‌های حیاتی شامل ارتباطات، انرژی، ترابری، بانکداری، آب و خدمات به‌طور فزاینده‌ای به زیرساخت‌های فناوری وابسته‌هستند. بنابراین اگرچه انقلاب اطلاعات فرصت‌های جدیدی را فراهم آورده، بهره‌وری سازمانی را بهبود بخشیده و به پیوند جهانی بی‌مانندی منجرشده، اما در عین حال با آسیب‌پذیری‌های نامتعارف و تهدیدهای مربوط به پیامدهای اجتماعی، اقتصادی، سیاسی و امنیتی نیز همراه بوده‌است.

از سوی دیگر، هدف و کارکرد فضای مجازی دستیابی هرچه سریع‌تر و مؤثرتر به اطلاعات است. در این شرایط، جهان به‌حدی فشرده شده‌است که اطلاعات بی‌درنگ در دسترس تقریبا همگان قرارمی‌گیرد که این امر می‌تواند گسترش اطلاعات نادرست را تسهیل‌سازد. در واقع، افراد به همان سرعتی که اطلاعات را دریافت‌می‌کنند در معرض اطلاعات نادرست نیز قراردارند و می‌توانند گمراه شوند. عمده نگرانی در رابطه با اثرگذاری دیجیتالی و هدف قراردادن افراد در فضای سایبر این واقعیت است که رفتار فرد می‌تواند از این طریق تحت‌تأثیر قرارگیرد یا دستکاری‌شود. در این شرایط، بسیاری از کشورها لزوم انجام عملیات سایبری را به‌عنوان بخشی از راهبرد کلی خود مورد تصدیق قرار داده‌اند، ازجمله رهنامه نظامی روسیه که از سال‌ها پیش در تعقیب آن بوده‌است.

در جبهه مخالف، ایالات متحده طی سال‌های گذشته هدف حمله‌های سایبری متعددی قرار داشته که متوجه افکار عمومی، زیرساخت‌ها و نهادهای گوناگون در این کشور بوده‌است. واشنگتن به‌لحاظ اقتصادی و نظامی در رتبه نخست جهان قراردارد و بسیاری از رقبا و مخالفان این بازیگر با درک این واقعیت به روش‌های نامتقارن برای رقابت با ایالات متحده و

---

[1]. Information and Communication Technologies (ICTs)
[2]. Information Infrastructure (II)
[3]. Information Age

تنزیل قدرت این کشور روآورده‌اند. بیشتر دولت‌ها از درگیری با واشنگتن در جنگی متعارف پرهیزداشته و در جستجوی میادین نبرد در منقطه خاکستری[1] هستند تا قدرت ایالات متحده را از رهگذر جنگ اطلاعاتی با نشانه‌گرفتن منافعش در درون مرزهای این کشور کاهش‌دهند. تا جایی‌که راهبردپردازان اندیشکده آمریکایی رند کورپوریشن[2] در گزارش سال ۲۰۱۶ خود با عنوان «جنگ با چین» اظهار داشته بودند که «ما تصور می‌کنیم که چین با توجه به حداقل توانایی خود برای حمله به سرزمین اصلی ایالات متحده با استفاده از سلاح‌های متعارف، تنها از طریق فضای مجازی قادر به این کار خواهد بود» (Gompert et al., 2016:ix).

در این میان، ایالات متحده بیشترین حمله‌های سایبری علیه خود را از جانب مسکو تجربه کرده‌است و درعین‌حال روسیه نخستین دولتی به‌شمار می‌آید که به‌طور مستقیم به بهانه حمله‌های سایبری در درون مرزهای ایالات متحده –درجریان رقابت‌های انتخابات ریاست‌جمهوری سال ۲۰۱۶- ازسوی واشنگتن مورد تحریم قرار گرفت (Volz and Gardner, 2018). درحال‌حاضر نیز روسیه بیش از هر دولت دیگری در جهان موضوع تحریم‌های ضدسایبری واشنگتن قرار دارد (Perlroth,2020). تثبیت اتحادیه اروپایی به‌عنوان یک بازیگر امنیت سایبری طی دهه گذشته نیز از جهات بسیاری مرهون تلاش‌های این اتحادیه درجهت مقابله با حمله‌های سایبری روسیه علیه دولت‌های عضو و نیز کشورهای پساشوروی متمایل به اتحادیه اروپایی و ناتو بوده‌است (Barrinha, 2018:29). با این‌همه، عدم اجماع میان دولت‌های اروپایی درخصوص چگونگی مواجهه با حمله‌های سایبری روسیه به موضع انفعالی این اتحادیه در برابر اقدام‌های سایبری روسیه منجر شده‌است.

در مقابل، رهبران روسیه نیز به‌شدت نگران تهدید منافع کشورشان در فضای مجازی هستند. این نگرانی‌ها در درجه نخست به تلاش دولت‌های غربی برای تضعیف و بی‌ثبات کردن حکومت روسیه از طریق تأثیرگذاری بر افکار عمومی داخل این کشور معطوف‌است و در وهله بعدی به دغدغه‌های مربوط به نفوذ در زیرساخت‌های اطلاعاتی و تأسیسات روسیه بازمی‌گردد. پوتین در چندین نوبت وقوع انقلاب‌های رنگی[3] در اوایل سده بیست‌ویکم در گرجستان، اوکراین و قرقیزستان و بهار عربی[4] در اوایل دهه دوم در خاورمیانه و شمال آفریقا

---

1. Grey Zone
2. RAND Corporation
3. Color Revolutions
4. Arab Spring

را تحریکاتی به‌واسطه تدابیر سایبری دولت‌های غربی با هدف تضعیف رژیم‌های همراه با روسیه توصیف کرده‌است (Allen and Moore, 2018:59-60). علاوه بر این، کرملین از طرح‌های گسترش ناتو و اتحادیه اروپایی به‌سمت شرق و جذب کشورهای پساکمونیستی در نهادهای غربی نیز در هراس است. در این شرایط، بهره‌گیری از ظرفیت‌های فضای سایبر برای مقابله با کنش‌های خصمانه دولت‌های غربی از دیدگاه مسکو یک گزینه مؤثر محسوب می‌شود. به‌ویژه اینکه دشواری نسبت‌دادن حمله‌های سایبری به عاملان آنها از هزینه مقابله روسیه با دولت‌های غربی می‌کاهد.

هدف اصلی مقاله حاضر، شناسایی دلیل و انگیزه اصلی روسیه برای استفاده از فناوری‌های تجاری در حوزه سایبری و پایگاه‌های فضای مجازی در دسترس عموم برای برپایی نبرد سایبری[1] علیه اهداف غربی در ایالات متحده، اتحادیه اروپایی و کشورهای پساکمونیستی متمایل به بروکسل است. بر این پایه پرسش اصلی مقاله این‌گونه تدوین شده‌است که «دلیل اصلی روسیه برای توسل به سلاح سایبری علیه اهداف غربی چیست؟» پیش‌نیاز دستیابی به پاسخ پرسش اصلی، پاسخ‌گویی به این پرسش فرعی است که «جنگ سایبری روسیه علیه غرب از چه ویژگی‌هایی برخوردار است و به چه شیوه‌ای دنبال می‌شود؟» با توجه به ماهیت توصیفی و چندوجهی پرسش‌های مقاله، ارائه فرضیه برای آن‌ها ضروری نیست و پاسخ نهایی پرسش‌ها در پایان مقاله ارائه شده‌است. داده‌های توصیفی گردآوری‌شده نیز در بخش تجزیه‌وتحلیل طی چهار قسمت جداگانه ارائه و تحت مفاهیم جنگ سایبری و حمله‌های سایبری سیاسی تجزیه‌وتحلیل شده‌اند. همچنین تحلیل یافته‌ها و پاسخ نهایی پرسش‌های پژوهش در نتیجه‌گیری آمده است.

مقاله حاضر از نوع کیفی (توصیفی-تحلیلی) بوده و در دسته پژوهش‌های پس‌رویدادی (علی) قرار می‌گیرد. در فرایند تحلیل داده‌ها و پاسخ به پرسش‌های مقاله نیز از روش‌شناسی استنتاجی (منطق قیاسی) با تکیه بر قوه فهم پژوهشگر در چارچوب مفاهیم جنگ سایبری و حمله‌های سایبری سیاسی استفاده شده‌است. داده‌ها نیز به‌شیوه کتابخانه‌ای از راه مطالعه اسناد ملی روسیه، اظهارنظرها و بیانیه‌های رسمی دولت روسیه و دولت‌های مدعی قربانی حمله‌های سایبری مسکو، کتاب‌ها، مقاله‌ها، مجله‌ها، تارنماها، مطبوعات و خبرگزاری‌های معتبر گردآوری شده‌اند. بر این پایه، همزمان با ارائه مهم‌ترین داده‌های توصیفی مربوط به

[1]. Cyber Warfare, Cyber War, Cyberwarfare, Cyberwar

زیرمجموعه‌های چهارگانه بخش تجزیه‌وتحلیل داده‌ها (مفهوم بازدارندگی در رهنامه نظامی روسیه، سلاح سایبری روسیه در خارج نزدیک، نبرد سایبری روسیه در برابر اتحادیه اروپایی، و جنگ سایبری روسیه علیه ایالات متحده)، فرایند تحلیل داده‌ها و توسعه تدریجی یافته‌های پژوهش نیز انجام پذیرفته‌است.

چارچوب مفهومی،تصور این‌که کنش‌ها، دیدگاه‌ها و اندیشه‌های یک فرد و به‌ویژه یک جامعه می‌تواند با دستورکار برخی گروه‌های بیرونی ساخته‌شود در نظر همه دولت‌ها نگران‌کننده است. تشخیص هدف‌گیری بدخواهانه مردم با اطلاعات نادرست از تبلیغات صادقانه و خیرخواهانه دشوار است. در هر صورت، اگر مردم به‌طور حساب‌شده تحت تأثیر تبلیغات و اطلاعات هدفمند دولت‌هایشان قراردارند، باور اینکه دشمنان خارجی و مجرمان نیز می‌توانند همین‌کار را انجام‌دهند قابل‌درک است (Howe, 2019:2-13). به همین جهت، تهدیدها علیه زیرساخت اطلاعاتی و دستکاری افکار عمومی در فضای مجازی یا به‌عبارت بهتر "تهدیدهای سایبری"، نگرانی جدی دولت‌ها، افراد و سازمان‌ها اعم از عمومی و خصوصی و نیز ملی و بین‌المللی است.

پدیده‌های به‌هم نزدیک فضای مجازی، فضای سایبر و فضای مجازی به‌لحاظ فنی و مفهومی از یکدیگر متمایز هستند و درعین‌حال پیوند تنگاتنگی نیز میان آنها برقرار است. « فضای مجازی را می‌توان همچون زیرساخت‌های منطقی و فیزیکی فضای واقعی[1] در نظر گرفت که اجرای برنامه‌ها و دریافت محتوا را امکان‌پذیر می‌سازد. درحالی‌که فضای سایبر می‌تواند به‌مثابه تجربه‌های "دنیای مجازی[2]" مبتنی بر استفاده بشر از برنامه‌های فضای مجازی -پایه[3] و مصرف محتوایی که در سراسر فضای مجازی به‌اشتراک گذاشته شده‌است، تعریف شود» (Frischmann, 2003:217). در مقام مقایسه فضای مجازی با کتاب، کتاب شبیه فضای مجازی است که شیوه‌ای برای انتقال اطلاعات -نظیر داستان یا متن- از نویسنده به خواننده محسوب‌می‌شود، همان‌گونه که فضای مجازی داده‌ها را میان دو رایانه (یا سرور و یک رایانه) منتقل می‌کند. اکنون خواننده داستان را مطالعه می‌کند و آن‌را در ذهن خود به‌مثابه یک

[1]. Real-Space
[2]. Virtual-World
[3]. Internet-Enabled

واقعیت مجازی از طریق نقش‌آفرینی شخصیت‌ها و دیالوگ‌های داستان به‌تصویرمی‌کشد. این واقعیت مجازی معادل فضای سایبر است. در حقیقت فضای سایبر به چگونگی تصویرسازی کاربر از اطلاعات منتقل‌شده از طریق فضای مجازی اشاره دارد (CSI, 2015).

به‌رغم وجود این تمایز، ضرورتی برای انتخاب میان چشم‌اندازهای فضای مجازی یا فضای سایبری ازسوی پژوهشگران در اغلب پژوهش‌ها احساس نمی‌شود. درواقع، انتخاب‌کردن میان این دو پدیده خود بخشی از مشکل است (Frischmann, 2003:217). در مقاله حاضر نیز از آنجاکه تهدید و جنگ سایبری بر بستر ابرشبکه فضای مجازی جریان دارد و نمی‌توان فضای سایبر را در موضوع استفاده از سلاح‌های سایبری از فضای مجازی جدا کرد از این تمایز دوری جسته شده‌است.

نگرانی از تهدیدهای سایبری به‌ویژه در فناوری به‌سرعت درحال گسترش " فضای مجازی اشیاء[1]" که به اتصال دستگاه‌ها و وسایل گوناگون محیط پیرامون انسان به فضای مجازی اشاره دارد، بیشتر به‌چشم می‌خورد (برنا و همکاران، ۱۳۹۷: ۱۲۴). با پیشرفت فناوری، نوآوری‌ها در سوءاستفاده (استفاده استثماری[2]) از فضای سایبر نیز به‌صورت موازی ارتقا یافته‌است. گزارش‌های متعدد امنیتی گوگل، مایکروسافت، اپل، سامسونگ و دیگر شرکت‌های فناورانه درخصوص آسیب‌پذیری محصولات الکترونیکی و خدمات فضای مجازی نشان از تعداد همواره رو به افزایش ویروس‌ها، بدافزارها[3]، باج‌افزارها[4]، روزنه‌های نفوذ، خراب‌کاری‌ها و دیگر تهدیدها در فضای سایبر دارد (TDE, 2020:3). برای نمونه در یکی از بحث‌برانگیزترین رسوایی‌های اخیر در رابطه با سوءاستفاده از فضای مجازی برای اهداف سیاسی و بازی قدرت، شرکت سهامی خاص کمبریج آنالیتیکا[5] مستقر در انگلستان که به امر مشاوره سیاسی مشغول‌است با دستبرد به داده‌های شخصی بیش از ۸۷ میلیون کاربر فیسبوک در صدد نفوذ بر انتخابات ریاست‌جمهوری ۲۰۱۶ ایالات متحده و کارزار برگزیت[6] (خروج بریتانیا از اتحادیه اروپا) برآمده‌بود (Riley et al., 2018).

---

1. The Internet of Things
2. Exploitative-Use
3. Malware
4. Ransomware
5. Cambridge Analytica
6. Brexit

تعریف نبرد سایبری: ادبیات مربوط به بهره‌گیری دولت‌ها از فضای سایبر به‌مثابه سلاح چندان غنی نیست. علاوه بر تازگی این مبحث، عدم اجماع بر سر تعریفی جامع و مانع از جنگ سایبری و به‌تبع آن از سلاح سایبری نیز در این‌خصوص مؤثر بوده‌است. بحث‌های پرمفهومی از دیرباز میان اندیشمندان و متخصصان امنیت سایبری در ارتباط با مفهوم جنگ سایبری شکل گرفته‌است، اما تا هیچ تعریف رسمی (یا به‌طور کلی پذیرفته‌شده‌ای) در رابطه با چیستی جنگ سایبری وجود ندارد. در یکی از نخستین تلاش‌ها برای تعریف این مفهوم، جنگ سایبری به‌مثابه هدایت‌کردن و آمادگی برای انجام عملیات نظامی هماهنگ با اصول مرتبط با اطلاعات توصیف شده‌است. طبق این تعریف، پیامد جنگ سایبری ازهم‌گسیختگی -اگرنه انهدام- اطلاعات و سامانه‌های ارتباطی خواه بود (Arquilla and Ronfeldt, 1993:30).

این تعریف درک گسترده‌ای از مفهوم جنگ سایبری ارایه‌می‌دهد چراکه شامل هر نوع حمله سایبری با هدف آسیب‌رساندن به سیستم‌های ارتباطی می‌شود. این درک گسترده از جنگ سایبری مشکل‌ساز است زیرا وضعیتی را ترویج‌می‌کند که در آن بسیاری از حمله‌های سایبری را می‌توان صرف‌نظر از ماهیت اهداف سیاسی یا غیرسیاسی آنها تحت‌عنوان جنگ سایبری طبقه‌بندی‌کرد. علاوه بر این، بحث‌هایی نیز در مورد تعاریف گوناگون از مفاهیم مرتبط با امنیت سایبری به‌ویژه با توجه به موارد مربوط به انواع متعدد حمله‌های سایبری و سلاح‌های سایبری وجوددارد. بنابراین، مفهوم‌سازی جنگ سایبری چه به‌لحاظ فنی و چه از چشم‌انداز سیاسی و نظامی باید به‌گونه‌ای تعریف‌شود که با دیگر مفاهیم مرتبط با آن شامل امنیت سایبری، حمله‌های سایبری، سلاح‌های سایبری، جنگ اطلاعاتی، نفوذ سایبری و مواردی از این دست هماهنگ‌باشد.

در تقسیم‌بندی مبانی نظری استفاده از فضای سایبر به‌مثابه سلاح می‌توان دو بعد چرایی و چگونگی را از یکدیگر تفکیک‌نمود؛

دلایل استفاده از فضای مجازی به‌مثابه سلاح: در زمینه چرایی توسل دولت‌ها به سلاح سایبری در ساده‌ترین سطح می‌توان به این واقعیت فنی اشاره کرد که دامنه تهدید سایبری در جهان به‌دلیل ماهیت مقررات‌گریز فضای مجازی و سادگی و ارزانی راه‌اندازی جرایم سایبری رو به گسترش‌است. مهم‌تر اینکه تهدیدهای سایبری با چالش فنی شناسایی کاربران مسئولی مواجه‌است که می‌توانند با استفاده از شبکه‌های متعدد به‌راحتی هویت خود را پنهان‌نمایند. عوامل مذکور بر این واقعیت دلالت‌دارند که راه آسانی برای رهایی از این مشکل وجودندارد.

در توضیح دلایل سیاسی استفاده از فضای سایبر به‌مثابه سلاح علاوه بر اینکه ناگزیر پای دولت‌ها به‌میان می‌آید، سطح تحلیل نیز به حوزه بین‌المللی ارتقا می‌یابد. تهدیدهای سایبری جدی علیه اهداف دولتی از خارج مرزها تا اندازه‌ای از رهگذر همکاری‌های بین‌المللی قابل‌کنترل هستند، اما همکاری‌هایی از این دست به‌سختی حاصل‌می‌شوند. به‌ویژه در صورتی‌که ردپای حمله‌های سایبری به یک دولت بازگردد یا این‌گونه حمله‌ها اساسا ازسوی دولت برنامه‌ریزی و اجرا شده‌باشد (ترابی، ۱۳۹۸: ۱۹۱-۱۹۲). توسل دولت‌ها به سلاح سایبری می‌تواند در دو حالت کلی مقابله به‌مثل یا دفاع (پدافند) و تهاجم اولیه (آفند) صورت‌بپذیرد.

جنگ سایبری می‌تواند به‌طور بالقوه بین دولت‌هایی اتفاق بیفتد که از سابقه طولانی روابط خصمانه برخوردارهستند. احتمال بروز این رخداد زمانی‌که مناسبات رقابت‌آمیز به تنش‌های جدی یا شرایط بحرانی تبدیل‌می‌شود نیز افزایش خواهدیافت (Shad, 2018: 43-44). به‌رغم اهداف مشترک و کاربردهای نزدیک جنگ سایبری و جنگ اطلاعاتی این دو مفهوم از یکدیگر متمایزهستند. تیموتی توماس[1] (2014:101-102) تحلیلگر ارشد در دفتر مطالعات نظامی خارجی ایالات متحده[2] توضیح‌می‌دهد که جنگ اطلاعاتی شامل به‌کارگیری تدابیر روان‌شناختی برای هدایت رقیب به‌سمت کنش‌ها یا رفتارهای هم‌راستا با منافع کاربر است. جنگ سایبری نیز، اگرچه می‌تواند چنین هدفی را شامل‌شود، اما محدود به استفاده از تدابیر روان‌شناختی نیست و مهم‌تر از همه اینکه درعوض فضای واقعی و عینی در فضای مجازی جریان‌دارد.

دنیل گوئر[3] (2014: 97) تحلیل‌گر امنیت ملی و نایب‌رئیس ارشد سازمان تحقیقات سیاست عمومی مؤسسه لکسینگتون[4] واقع در ایالات ویرجینیا[5] معتقد است، یکپارچگی جنگ سایبری یا جنگ اطلاعاتی می‌تواند، تأثیر تعیین‌کننده‌ای طی درگیری داشته‌باشد، باعث سردرگمی در میان تصمیم‌گیرندگان شود، عملیات نظامی را گمراه‌سازد و روحیه جمعیت‌های هدف را تضعیف‌نماید. در این رابطه، مرکز عالی همکاری‌های دفاع سایبری سازمان پیمان آتلانتیک شمالی (ناتو)[6] مجموعه تعاریف یکپارچه‌ای را ارائه نموده‌است که پذیرش آنها می‌تواند با ارائه چشم‌اندازی منسجم، متوازن، گسترده، ثابت و روشن اجازه

---

1. Timothy Thomas
2. U.S. Foreign Military Studies Office
3. Daniel Goure
4. Lexington Institute
5. Virginia
6. NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE)

گفت‌وگوی آزاد پیرامون دامنه شمول و کاربرد آنها را فراهم‌آورد. ناتو حمله سایبری را به‌مثابه "اقدامی برای درهم‌گسیختگی، تکذیب، استحاله یا نابودی اطلاعات موجود در یک رایانه و/یا شبکه رایانه‌ای" تعریف‌می‌کند. این بدان معنی است که حمله سایبری تنها حمله به خود شیء (معمولا یک رایانه) نیست، بلکه حمله به کل شبکه متصل به آن و اطلاعاتی که از طریق آن اداره‌می‌شود را نیز شامل‌می‌شود. این نوع نگرش در تعریف ناتو از سلاح سایبری نیز منعکس شده‌است: "نرم‌افزار، ثابت‌افزار[1] یا سخت‌افزار طراحی‌شده یا به‌کاربرده‌شده برای ایجاد آسیب در قلمروی سایبری." این تعاریف شیوه‌ای را نمایان‌می‌سازند که طی آن چارچوبی برای سازواری این مفاهیم در شرایط مختلف سیاسی فراهم‌می‌آید (De Buen, 2016:12).

۱. چگونگی استفاده از فضای مجازی به‌مثابه سلاح

از توضیحات بالا این‌گونه برمی‌آید، بررسی دلایل توسل دولت‌ها به سلاح سایبری و شناخت چیستی جنگ سایبری پیوند نزدیکی با چگونگی استفاده از فضای سایبر به‌مثابه سلاح نزد دولت‌ها دارد. انواع گوناگونی از سلاح‌های سایبری وجوددارند که میزان اثربخشی و سختی تکنیکی آن‌ها متفاوت‌است. برخی سلاح‌ها مانند تهدید(های) پیشرفته و مستمر[2] پیچیده‌بوده و پیاده‌سازی آنها نیازمند سطوح بالایی از تخصص فنی و منابع عظیم است. معمولا اهداف تهدید(های) پیشرفته و مستمر عبارتند از "انتقال غیرمجاز اطلاعات حساس از یک شبکه هدف؛ فرسایش یا جلوگیری از جنبه‌های حیاتی یک مأموریت، برنامه یا سازمان؛ یا تثبیت جایگاه خود برای انجام این اهداف در آینده." یکی دیگر از ویژگی‌های مهم حمله‌های سایبری سیاسی استفاده از ربات‌ها[3] و یا شبکه‌ای از ربات‌ها[4] است که اغلب با هدف انجام حمله‌های منع سرویس توزیع‌شده[5] انجام‌می‌شوند (Ogu et al., 2019:338-342). حمله‌های منع سرویس توزیع‌شده به‌منظور درهم‌شکستن اهداف حمله اغلب از طریق ربات‌ها صورت‌می‌گیرند. یک حمله منع سرویس توزیع‌شده نوعی حمله سایبری است که در آن رایانه، تارنما یا کارگزار[6] با درخواست‌های غیرواقعی ارائه‌شده ازسوی تعداد زیادی رایانه اشباع‌شده که به کژکاری یا

---

1. Firmware
2. Advanced Persistent Threats (APT)
3. Bots
4. Botnets
5. Distributed Denial of Service (DDoS)
6. Server

بسته‌شدن آنها منجرمی‌شود. حمله‌های منع سرویس توزیع‌شده نسبتا مقدماتی هستند و به سطح پیشرفته‌ای از مهارت نیاز ندارند و به‌همین جهت نیز جزو رایج‌ترین انواع حمله‌های سایبری علیه دولت‌ها به‌شمارمی‌آیند (Ahn et al., 2020:1428-1430).

با اینکه انواع مختلفی از حمله‌های سایبری وجود دارد، اما برای اهداف تحلیلی این مقاله حمله‌ها به‌لحاظ سیاسی که ازسوی دولت‌های خارجی هدایت‌می‌شوند حائزاهمیت هستند. حمله‌های سایبری سیاسی خارجی به نمونه‌هایی اشاره‌دارد که در چارچوب یک رویداد سیاسی بزرگ (ازجمله تنش‌ها، درگیری‌ها و کارزارهای انتخاباتی) رخ‌می‌دهند و هدف نهایی آن در اصل تضعیف دولت هدف است. (Burton, 2019:123-125) از این رو، بهتر است تجزیه‌وتحلیل آنها نیز با لحاظ زمینه ژئوپلیتیک بزرگتری که در آن ظهورمی‌یابند، انجام‌پذیرد. با وجود این، اگرچه برخی شگردهای دیجیتال خاص می‌توانند به‌عنوان سلاح مورداستفاده قرارگیرند، اما آنها ضرورتا سلاح نیستند، همان‌گونه که نیات پشت‌پرده حمله ممکن‌است در اصل سیاسی نباشند. این واقعیت، تعیین اینکه آیا یک حادثه فضای مجازی خاص در حکم یک حمله سیاسی است یا خیر را دشوار می‌سازد (Lewis, 2015:41).

به‌همین منوال، نسبت‌دادن ویژگی اقدام جنگی به یک حمله سایبری خاص نیز دشواراست چراکه حمله‌های سایبری به‌طور عمده (اما نه همیشه) فاقد خشونت مرگبار مرتبط با حمله‌های متعارف هستند. بنابراین شناسایی یک حمله سایبری به‌مثابه اقدام جنگی، نیازمند تجزیه‌وتحلیل عمیق‌تر بسترهای سیاسی بروز حمله است (Stone, 2013:107). به همین جهت ایجادتمایز میان حمله‌های سایبری سیاسی و نظامی به‌مراتب دشوارتر خواهدبود. در نتیجه، برای شناسایی یک حمله سایبری خاص به‌مثابه یک حمله سایبری سیاسی/نظامی، اثبات برخی معیارها ضروری‌است. در اینجا می‌توان با استناد به ادبیات علمی این حوزه چهار نوع خشونت سایبری بین‌دولتی شامل خراب‌کاری، دستکاری، جاسوسی و براندازی را برای محدودکردن دامنه حمله‌های سایبری سیاسی برگزید (Rid, 2102:15). این معیارها در واقع چشم‌اندازهایی را به‌منظور تجزیه‌وتحلیل روش‌های استفاده از سلاح‌های سایبری در زمینه‌های سیاسی مانند تنش‌ها و درگیری‌ها فراهم‌می‌آورند (Reuter et al., 2019:16).

وخیم‌ترین شکل بهره‌برداری از فضای مجازی ازسوی دولت‌ها شامل حمله‌ها به شبکه‌های رایانه‌ای و افکار عمومی شهروندان یک دولت دیگر در جریان تعاملات خصمانه بین‌دولتی است که با برچسب جنگ سایبری یا درگیری سایبری مشخص‌می‌شوند (مایلی و بهمنی، ۱۳۹۱: ۱۳۹).

جنگ سایبری دست‌کم به کاربر امکان می‌دهد تا به‌طور مؤثر از جنگ‌اوری جنبشی[1] (جنگ سنتی) در تعقیب اهداف هم‌زمان اهداف سیاسی و نظامی استفاده‌کند (Chivvis, 2017:317). جنگ سایبری تنها بین دولت‌ها صورت‌نمی‌گیرد و می‌تواند شامل بازیگران غیردولتی ازجمله افراد، شرکت‌ها و تروریست‌ها نیز باشد. جنگ سایبری بین‌دولتی به احتمال زیاد در زمینه هماوردی (رقابت) رخ می‌دهد. مفهوم هماوردی که به معنی درگیری طولانی‌مدت با یک دشمن سرسخت است به زمینه‌یابی و زمینه‌سازی جنگ یا درگیری سایبری در تاریخ تعاملات دیپلماتیک، نظامی و اجتماعی-فرهنگی میان دولت‌ها کمک‌می‌کند.

درک دیدگاه‌های سیاسی مؤثر بر استفاده دولت‌ها از شگردها و سیاست‌های سایبری مرتبط با اینترنت هم نیازمند تدقیق در گذشته و هم کشف پیشرفت‌های اخیر است. تقویت و توسعه ایدئولوژی‌ها و مفاهیمی که در دهه‌های ۸۰ و ۹۰ میلادی طی جنگ سرد ایجاد شده‌بودند، می‌توانند تا حدودی برای ارجاع به پیشرفت‌های فنی اخیر مورد استفاده قرارگیرند. رویدادهای بین‌المللی و داخلی می‌توانند نگرش دولت‌ها را تغییردهند و رویکرد نظامی آنها را به‌لحاظ داخلی و بین‌المللی تحت تأثیر قراردهند و آنها را به‌سمت استفاده از سلاح‌های سایبری سوق‌دهند یا دور نگاه دارند. بنابراین فهم انگیزه‌ها و دیدگاه‌های منتهی به توسل به فضای سایبری به‌مثابه سلاح از منظر دولت‌ها برای درک بهتر تهدیدهای سایبری بالقوه از جانب روسیه علیه غرب ضروری‌است.

علاوه بر درک مفهوم حمله‌های سایبری و نسبت آن با جنگ سایبری که در بالا توضیح داده‌شد، شناخت ابزارهای نبرد سایبری نیز برای نسبت‌دادن حمله‌های سایبری علیه غرب به مسکو اهمیت‌دارد. ابزارهای جنگ سایبری که معادل سلاح‌های سایبری فرض‌می‌شوند از سایر کنش‌های معمول سایبری به‌ندرت قابل تمیزهستند و قاعده خاصی برای شناسایی آنها وجودندارد (Wheeler, 2018). به همین جهت، ابزارهای جنگ سایبری نسبت مستقیمی با اهداف سیاسی، امنیتی یا نظامی به‌کارگیری آنها دارد. حمله‌های منع سرویس توزیع‌شده، نخستین و متداول‌ترین سلاح سایبری در نبردهای سیاسی به‌شمارمی‌آیند (Crowell, 2017:17). نفوذ به سیستم‌های رایانه‌ای بدون داشتن اجازه دسترسی به آنها یا به‌اصطلاح هک‌کردن، دسته دوم ابزارهای جنگ سایبری را تشکیل می‌دهند که در همه عرصه‌های سیاسی، امنیتی و نظامی کاربرددارد. هک‌کردن می‌تواند با

[1]. Kinetic Warfare

هدف سرقت اطلاعات، افشاگری، جاسوسی، خرابکاری، اخطار یا حتی اظهار وجود صورت‌بپذیرد که بسته به هر یک از این اهداف در زمره ابزارهای سایبری سیاسی، امنیتی یا نظامی دسته‌بندی‌می‌شود (Atkinson, 2018:68). عملیات نفوذ غیرمجاز به سیستم‌های رایانه‌ای همچنین ممکن‌است از طریق انتقال ویروس‌ها یا بدافزارها رخ دهد (Gonçalves, 2019).

بدافزارها یا ویروس‌ها را می‌توان به‌مثابه مخرب‌ترین نوع سلاح سایبری با گوناگونی بسیار بالا در دسته سوم سلاح‌های سایبری جای‌داد. بدافزارها در کنار عملیات هک از راه دور می‌توانند برخلاف حمله‌های منع سرویس توزیع‌شده مستقیما به مرگ افراد منجر شوند (Dewar, 2017:7). به‌عنوان مثال، اختلال از راه دور در سیستم‌های آفندی و پدافندی متصل به شبکه می‌تواند به شلیک غیرارادی آنها و کشته‌شدن افراد منجر شود (Gisel and Olejnik, 2018:18). همچنین بدافزارها می‌توانند با نفوذ در شبکه برق نیروگاه‌های هسته‌ای یا تارنماهای غنی‌سازی اورانیوم فاجعه به‌بار آوردند (Kim et al., 2018:995). هک از راه دور و یا از طریق بدافزار در سطوح سیاسی نیز ممکن‌است بدون برجاگذاشتن تلفات انسانی کاملا مؤثر واقع‌شود.

دسته چهارم و آخر ابزارهای جنگ سایبری را می‌توان به تهدیدهای پیشرفته و مستمر نسبت‌داد که از طریق آمیزه‌ای از سه سلاح پیشین اعمال‌می‌شوند. این ابزار جنگ سایبری به‌طور عمده در سطوح نظامی و با هدف از کارانداختن سیستم‌های دفاعی و تهاجمی و به‌جا گذاشتن تلفات انسانی مورد استفاده قرارمی‌گیرد. بخش حاضر مفاهیم و وضعیت‌هایی را به‌لحاظ نظری تشریح‌نمود که شناخت آنها برای ارزیابی کنش‌های سایبری روسیه در قبال دولت‌ها و اهداف غربی و اینکه آیا چنین کنش‌هایی در حوزه جنگ سایبری قرارمی‌گیرند یا خیر ضروری‌است.

۲. بازدارندگی سایبری روسیه

تا یک دهه پس از پایان جنگ سرد، اهمیت توان نظامی به‌مثابه نمایش قدرت یک کشور کماکان در طرز فکر رهبران روسیه باقی مانده‌بود. با این‌همه، ضعف اقتصادی و فروپاشی نسبی ارتش روسیه پس از تجزیه اتحاد جماهیر شوروی، رهبران کرملین را به‌سوی اثربخشی هزینه‌ها در انجام فعالیت‌های نظامی این کشور سوق‌داد. این درحالی بود که طی

دهه ۹۰ میلادی جنگ به‌تدریج به‌شکل منحصربه‌فردی از درگیری متمایل می‌شد که توان نظامی صرف و عوامل به‌لحاظ سنتی مؤثر در آن رنگ‌می‌باخت. در این شرایط، پیدایش رایانه‌های شخصی و افزایش استفاده از فضای مجازی شیوه‌های جدیدی را برای جنگ‌اوری معرفی‌کرد که همچون بسیاری از کشورها مورد توجه ارتش روسیه نیز قرارگرفت.

در طبقه‌بندی اقدام‌های نظامی روسیه، ظرفیت‌های اینترنت و جنگ سایبری بخشی از حوزه وسیع‌تر جنگ اطلاعاتی و عملیات استخباری به‌شمارمی‌آید. جنگ اطلاعاتی از مدت‌ها پیش یکی از ابعاد آموزه‌های نظامی روسیه محسوب‌می‌شد. تعدادی از رهبران نظامی روسی و متخصصان امنیت ملی بر این باور هستند که نقطه کانونی جنگ‌های جدید درحال جابه‌جایی از نیروی محرکه جنبشی[1] به‌سمت قلمروهای دیجیتال است. "زمین و دریا، دیگر صحنه‌های اصلی جنگ به‌شمار نمی‌آیند" و تمرکز جنگ‌ها به‌سمت "هوافضا و حوزه‌های اطلاعاتی ازجمله امنیت سایبری سوق یافته‌است" (Goure,2014:97). در همین راستا، ژنرال والری گراسیموف[2] (2016:24) در مقاله‌ای با عنوان "ارزش علم در دوراندیشی است[3]"، تأکیددارد که "تمرکز روش‌های کاربردی درگیری در جهت استفاده گسترده از روش‌های سیاسی، اقتصادی، اطلاعاتی، انسان‌دوستانه و سایر تدابیر غیرنظامی که با ابزارهای نظامی تکمیل‌می‌شوند، دگرگون شده‌است".

در سطح رهبری سیاسی و کلان نیز ولادیمیر پوتین در سال ۲۰۰۶ خواستار واکنش‌های نظامی " مبتنی بر برتری فکری و پاسخ‌های نامتقارن و کم‌هزینه‌تر" شده بود (Thomas, 2014:105) که به‌معنای بهره‌گیری ارتش این کشور از تدابیر جنگ سایبری است. در ادامه نیز رهنامه نظامی فدراسیون روسیه در سال ۲۰۱۰ برپایه استفاده از ظرفیت‌های آفندی و پدافندی فضای سایبر مورد تجدیدنظر قرارگرفت و در نسخه ۲۰۱۴ بر اهمیت آن افزوده‌شد (Hastings, 2019:2-3). پیش از آن نیز روسیه عملا فضای سایبری را به‌مثابه یک زیرساخت جدید برای پی‌گیری منافعش در عرصه نظامی پذیرفته‌بود و پیشروترین دولت در استفاده از روش جنگ ترکیبی برپایه استفاده هم‌زمان از ظرفیت‌های نبرد جنبشی[4] (نبرد مسلحانه سنتی) و تهاجم سایبری به‌شمارمی‌آید (Pietkiewicz, 2018: 514; Sambaluk, 2020: 90).

---

1. Kinetic
2. Valery Gerasimov
3. The Value of Science Is in the Foresight
4. Kinetic Warfare

ارتش روسیه، اگرچه امروزه به‌لحاظ دسترسی به سلاح‌های سنتی در وضعیتی بهتر از پایان جنگ سرد به‌سر می‌برد، اما جنگ فیزیکی متعارف با ایالات‌متحده یا ناتو احتمالا به شکست مسکو منجر خواهدشد. به‌همین جهت گراسیموف در سال ۲۰۱۳ "کنش‌های نامتقارن" ازجمله جنگ سایبری را مورد ستایش قرارداده و اظهار داشته‌بود که "کاربرد گسترده آنها امکان بی‌اثرسازی مزایای دشمن را ممکن‌می‌سازد" (Gerasimov, 2016:25). دولت روسیه بسیار پیش از مفهوم‌سازی ظرفیت‌های سایبری از اطلاعات به‌عنوان ابزار قدرت استفاده‌می‌کرد، اما رهبران نظامی روسیه از سال ۲۰۱۳ "چنین ملاحظاتی را در صدر اولویت‌های راهبردی خود" قراردادند (Allen and Moore, 2018:59).

لزوم برخورداری نیروهای روسی از آمادگی تدافعی و تهاجمی در نبردهای منقطه خاکستری[1] طی سال‌های گذشته همواره مورد تأکید رهبران نظامی و سیاسی این کشور بوده‌است (کلانتری و صادقی، ۱۳۹۸: ۱۲۰). ژنرال والری گراسیموف[2] رئیس ستاد مشترک نیروهای مسلح فدراسیون روسیه در سال ۲۰۱۸ پیش در خصوص ماهیت آینده درگیری‌های نظامی خطاب به اعضای آکادمی نظامی این کشور اظهار داشته‌بود که علاوه بر حوزه‌های سنتی نبرد مسلحانه دو حوزه اطلاعات و فضا نیز به‌طور پویا حضور خواهندداشت و ارتش روسیه باید از توانایی لازم در این حوزه‌ها به‌خوبی برخورداباشد (McDermott, 2018:2). همچنین در پی تأکید ولادیمیر پوتین، رئیس‌جمهوری روسیه بر ضرورت آمادگی این کشور برای مقابله کارآمدتر با تهدیدهای سایبری، ژنرال سرگئی شایگو[3] وزیر دفاع روسیه در فوریه ۲۰۱۷ از ایجاد ارتش سایبری در این کشور خبرداد (RNA, 22 Feb 2017).

دولت روسیه همچنین تمایل به دخالت غیرنظامیان در اقدام‌های بالقوه نظامی ازجمله در فضای سایبر را پنهان‌نمی‌سازد. پس از جنگ سرد، نظام سیاسی روسیه از تمامیت‌خواهی[4] به‌سمت سرمایه‌داری دولتی جرگه‌سالار[5] سوق پیداکرد. محیط سرمایه‌داری جرگه‌سالار مشوق وفاداری اعضای جرگه به حکومت روسیه با هدف حفظ بقای آنها در ساختار قدرت است (Lanskoy and Myles-Primakoff, 2018:77). در فضای مجازی نیز پیوندهای

---

1. Grey Zone
2. Valery Gerasimov
3. Sergey Shoygu
4. Totalitarianism
5. Oligarchic State Capitalism

کرملین با صاحبان کسب‌وکارهای بزرگ روسیه به‌مثابه اعضای جرگه تا اقدام‌های سایبری تعمیم یافته‌است. در کیفرخواست وزارت دادگستری ایالات متحده علیه اتباع روسیه در ارتباط با دخالت سایبری در انتخابات ۲۰۱۶ ریاست‌جمهوری ایالات متحده نیز سه شرکت روسی در کنار ۱۳ افسر اطلاعاتی متهم‌شده‌اند (Department of Justice, 2018).

روس‌ها برخلاف تصور رایج غرب از ذات تهاجمی اقدام‌های سایبری این کشور، ماهیت اقدام‌های خود در فضای سایبر را پدافندی می‌دانند. از چشم‌انداز روسیه، فناوری روش منحصربه‌فردی است که غرب برای "حمله" به این کشور استفاده می‌کند (Ajir and Vaillant, 2018:71). غرب بیش از آنکه از این روش منحصربه‌فرد برای تحمیل ضربات فلج‌کننده و ناگهانی علیه مسکو استفاده‌کند برای گسترش ایده‌ها، هنجارها، شیوه‌ها و رفتارهای غیرقابل قبول از دیدگاه مسکو بهره‌می‌برد. از این رو، سرویس‌های اطلاعاتی روسیه به‌طور فزاینده‌ای نگران آثار مخرب ناشی از کاربرد فضای مجازی به‌عنوان ابزار تبلیغاتی غرب علیه امنیت ملی این کشور هستند.

این نگرانی به مرزهای روسیه محدودنمی‌شود و تلاش دولت‌های اروپایی و آمریکای شمالی برای تهییج افکار عمومی جوامع پساشوروی علیه مسکو با هدف جذب آنها به‌سوی نهادهای غربی نیز بخش مهمی از دغدغه‌های سایبری کرملین را به‌خود اختصاص‌می‌دهد. گرایش دولت‌ها و رسانه‌های غربی به انتشار اطلاعات مغرضانه در فضای سایبر علیه سیاست‌های حکومت روسیه نیز بر درک رهبران روسیه از فضای اطلاعات جهانی به‌مثابه یک تهدید جدی علیه حاکمیت این کشور دامن زده‌است. با این توصیف، دور از انتظار نیست که روسیه اقدام‌های خود در فضای سایبر علیه دولت‌های غربی را بازدارنده معرفی‌نماید.

۳. بازدارندگی سایبری در فضای پساشوروی

دیوید رونفلدت[1] و جان آرکیلا[2] در سال ۱۹۹۳ پیش‌بینی کرده‌بودند که جنگ سایبری در نهایت به بخش مهمی از اقدام نظامی دولت‌ها تبدیل خواهد

[1]. David Ronfeldt

- اندیشمند علوم سیاسی

[2]. Ohn Arquilla

- رئیس بخش تحلیل دفاعی در دانشکده تحصیلات‌تکمیلی نیروی دریایی ایالات متحده

شد (Arquilla and Ronfeldt, 1993). این پیش‌بینی که در آن زمان با برخی تردیدها همراه‌بود (Arquilla, 2013:80) با نخستین کاربرد آشکار بازدارندگی سایبری روسیه در سال ۲۰۰۷ در برابر تمایل دولت استونی به غرب و بروز بحران در مناسبات مسکو-تالین[1] به‌اثبات رسید. این بحران با تصمیم حکومت استونی برای انتقال یک یادبود به‌جامانده از دوران شوروی آغازشد که اعتراض‌ها و شورش‌هایی را در میان اقوام روس ساکن استونی به‌دنبال داشت (Chapman, 2019:4-6). این شورش‌ها با پشتیبانی مسکو و یک‌سری حمله‌های سایبری علیه مؤسسات مهم استونیایی همراه‌بود که به دولت روسیه منتسب می‌شد (دهقانی، ۱۳۹۶: ۱۳۸).

استونی: حمله‌های سایبری علیه استونی در دو موج اصلی رخداد. موج نخست که در ۲۸ آوریل ۲۰۰۷ آغازشد به‌نسبت ساده‌بود و به‌طور عمده توسط نفوذگران مستقل انجام‌می‌شد و اهدافی مانند اخلال در جلسات سخنگوی دولت استونی و وزارت دفاع این کشور را دربرمی‌گرفت. این حمله‌ها با موج دیگری از حمله‌های پیچیده‌تر در هشتم ماه می همان سال دنبال‌شد. این موج به‌طور قابل‌توجهی حمله به برخی رایانه‌ها با کارکرد حیاتی در بانک‌ها، معاملات بورس و شرکت‌های توزیع انرژی را شامل‌می‌شد (Heickerö, 2013:131-132). پیچیدگی‌ها و نیازمندی‌های فنی و ضرورت‌های سازمان‌دهی و تأمین مالی انجام چنین حمله‌هایی نشان از وجود یک دولت در پشت پرده این حمله‌ها داشت. با توجه به انگیزه‌ها و نیز سامانه‌های مورد هدف، انگشت اتهام بیش از همه متوجه روسیه بود، اما روسیه انتساب این حمله‌ها به خود را ردکرد (Herzog, 2011:50).

استونی از زمان فروپاشی اتحاد جماهیر شوروی و کسب استقلال در سال ۱۹۹۱ روابط پیچیده‌ای را با روسیه تجربه کرده‌است، به‌ویژه از سال ۲۰۰۴ که این کشور به ناتو و اتحادیه اروپایی پیوست. این رابطه وخیم بین‌دولتی در ترکیب با ایجاد تنش میان روس‌های مقیم استونی و استونیایی‌های بومی از زمان استقلال پیچیده‌تر نیز شده است (Clarke and Knake, 2010:13-16). از این رو، جابه‌جایی بنای تجلیل از نیروهای شوروی نزد روس‌های استونی به‌گونه‌ای تفسیرشد که آنها را بیگانه از عموم مردم استونی به‌تصویر می‌کشید و خشم آنها را برانگیخت. مسکو نیز با توجه به پیشینه مناسبات

[1]. Tllinn

ناخوش‌آیند با تالین از این فرصت برای افزایش شعارها و اظهارات ملی‌گرایانه علیه استونی و دیگر دولت‌های واقع در خارج نزدیک که خواهان فاصله‌گرفتن از روسیه بودند، استفاده‌کرد.

مورد گرجستان: مناسبات روسیه با گرجستان پس از فروپاشی اتحاد جماهیر شوروی نیز تقریبا به اندازه روابط با استونی پیچیده بوده‌است. وجود جمعیت قابل‌توجه روس در دو ایالت خودمختار آبخازیا[1] و اوستیای جنوبی[2] باعث شده‌است تا مسکو در پشتیبانی از آنها و منافع ملی روسیه مانع روی کارآمدن رژیم‌های طرفدار غرب در این کشور شود. در این میان، منطقه تسخینوالی گرجستان[3] -پایتخت جمهوری اوستیای جنوبی- از زمان فروپاشی اتحاد جماهیر شوروی موضوع مناقشه میان مسکو و تفلیس بوده، تا جایی‌که کرملین کسب شهروندی روسیه را به افراد ساکن در این منطقه پیشنهاد داده‌است (Littlefield, 2009:1462; Agenda, 15 Nov 2017). این منطقه همچنین یک مزیت ژئوپلیتیک به‌لحاظ راهبردی شامل کنترل مسیرهای انتقال نفت و گاز دریای خزر به اروپا را برای دولت حاکم بر آن فراهم‌می‌آورد.

در تلاشی منجر به افزایش تنش در این منطقه، رهبران سیاسی گرجستان از میانه دهه ۹۰ میلادی پیوستن به ناتو را به‌عنوان یک اولویت مهم سیاست خارجی این کشور اعلام کردند که خشم دولت روسیه را برانگیخت (Rahman,2009:139). با شروع عملیات نیروهای نظامی گرجستان در ماه اوت ۲۰۰۸ برای پایان‌دادن به فعالیت‌های جدایی‌طلبانه در منطقه پرتنش تسخینوالی، ارتش روسیه در پشتیبانی از جدایی‌طلبان به یک حمله متقابل دست‌زد. در همان بدو تهاجم، روسیه با انجام یک سری حمله‌های سایبری و تلاش‌های شناسایی موفق به محاصره بسیاری از اهداف دولتی و نظامی حساس گرجستان شد. این حمله‌ها به‌طور عمده شامل توزیع بدافزارها، منع سرویس و تغییر ظاهر وبسایت‌ها همراه با ایجاد مشکلات در ارتباطات می‌شد (Andress and Winterfeld, 2014:12). دلایل و شواهد بسیاری درباره مکان، چگونگی و چیستی حمله‌های سایبری علیه گرجستان و ارتباط آن با گروه‌های روسی ازسوی پژوهشگران منتشر شده و باور عمومی بر آن است که دولت روسیه یا عامل حمله‌های سایبری در گرجستان بوده و یا دست‌کم از آنها پشتیبانی همه‌جانبه کرده‌است (Miniats, 2019:45).

---

[1]. Abkhazia
[2]. South Ossetian
[3]. Tskhinvali Region of Georgia

مورد گرجستان نشان‌می‌دهد، ارتش روسیه جهت مبارزه با آنچه که تلاش‌های دولت‌های غربی برای تهدید روسیه از طریق کشورهای همسایه تلقی‌می‌شود به جنگ سایبری روی آورده‌است. گرجستان در سال‌های متعاقب جنگ اوت ۲۰۰۸، اگرچه به ناتو نپیوست، اما به روابط مطلوب با دولت‌های غربی ادامه‌داد و در سال ۲۰۰۹ پیمان مشارکت راهبردی با ایالات متحده و در سال ۲۰۱۴ توافق‌نامه‌های مشارکت[1] شامل موافقت‌نامه منطقه آزاد تجاری جامع و عمیق[2] با اتحادیه اروپایی را به‌امضا رساند که به‌معنای محرومیت روسیه از فضای ژئوپلیتیک این کشور بود (Hastings, 2019:11). در برابر، مسکو حمله‌های سایبری خود علیه گرجستان را تداوم‌بخشید. گزارش سال ۲۰۱۴ شرکت امنیت سایبری فایرای[3] نشان‌می‌داد که وزارت دفاع و وزارت امور داخلی گرجستان هدف حمله‌های سایبری متعددی قرار دشته‌اند و هکرها با جاسازی بدافزارهای پنهان در اسناد جعلی و طعمه قراردادن آنها به جزئیات امنیتی و نظامی حساسی دست‌یافته‌اند. یافته‌های شرکت فایرای نشان‌می‌داد که دولت روسیه به احتمال فراوان در طراحی و انجام حمله‌های سایبری علیه نهادهای دولتی گرجستان دست داشته‌است (FireEye, 2014:28).

اوکراین: در سال ۲۰۱۴ نیز روسیه پس از بهبود شگردهای حمله‌های سایبری متعاقب رویارویی سال ۲۰۰۸ با گرجستان، رویکرد جنگ ترکیبی سایبری و جنبشی را علیه اوکراین تکرارکرد (Allen and Moore, 2018:63). انقلاب نارنجی[4] اوکراین (۲۰۰۴) با پیروزی ویکتور یانکویچ از هواداران روسیه در سال ۲۰۱۰ به سمت ریاست‌جمهوری دچار دگردیسی شد، اما طرفداران اروپا در پارلمان این کشور همچنان برای نزدیکی به اتحادیه اروپایی تلاش می‌کردند. یانکویچ در نوامبر ۲۰۱۳ فرایند امضای نهایی موافقت‌نامه مشارکت اتحادیه اروپایی-اوکراین[5] که پیش از آغاز دوران ریاست‌جمهوری وی آغاز شده‌بود را به‌تعلیق درآورد. امضای این موافقت‌نامه می‌توانست نشانه‌ای محکم از جدایی اوکراین از مدار روسیه و گذار این کشور به ساختارهای غربی تعبیرشود و به‌همین جهت مسکو نیز در برابر آن به‌شدت موضع‌گرفت (Diuk, 2014:10). طرفداران اروپا با برپایی جنبش یورومیدان[6] علیه این اقدام

---

1. Association Accords (AA)
2. Deep and Comprehensive Free Trade Area (DCFTA)
3. FireEye
4. Orange Revolution
5. Ukraine–European Union Association Agreement
6. Euromaidan

یانکویچ اعتراض‌کردند که با شکل‌گیری جنبش ضدمیدان[1] طرفداران روسیه در مناطق شرق و جنوب شرق اوکراین مواجه‌شد (عبدالی و نیاکویی، ۱۳۹۸: ۷۱۵).

اعتراض‌های ضدمیدان هواداران روسیه به‌سرعت به قلمروی سایبری کشیده‌شد. این حمله‌ها البته در مقایسه با موارد پیش‌گفته چندان پیشرفته‌نبود و اغلب وب‌سایت‌های متعلق به معترضین جنبش یورومیدان و مخالفان رابطه حکومت یانوکویچ و روسیه هدف حمله‌های منع سرویس توزیع‌شده و تغییر ظاهر قرارگرفتند. این حمله‌ها ازسوی دولت‌های غربی و برخی کنش‌گران امنیت سایبری به گروه‌های هکر طرفدار کرملین نسبت داده‌شد. یک گروه هکری با نام سایبربرکات[2] که گمان‌می‌رود ازسوی دولت روسیه پشتیبانی‌می‌شود با چندین حمله منع سرویس توزیع‌شده و دیگر حمله‌های سایبری طی سال ۲۰۱۴ در اوکراین در پیوند بوده است (Baezner, 2018:12). در هر حال، وضعیت ناپایدار اوکراین و مواجهه این کشور با حمله‌های سایبری سطح‌پایینی از این دست، فرصت لازم برای روسیه جهت الحاق کریمه به خاک خود و اعلام استقلال جمهوری‌های خودخوانده دونتسک[3] و لوهانسک[4] در شرق اوکراین را فراهم‌آورد. هنگامی‌که نیروهای زمینی روسیه در ماه فوریه وارد کریمه شدند، سرویس مخفی اوکراین قربانی حمله سایبری منتسب به بازیگران غیردولتی و دولتی روسیه شد که هماهنگ با نیروهای نظامی روسیه عمل‌می‌کردند (Allen and Moore, 2018:64).

انجام حمله‌های سایبری سال ۲۰۱۴ علیه اوکراین ازسوی بازیگران غیردولتی، تمایل دولت روسیه به استفاده از جمعیت غیرنظامی در تلاش برای پیاده‌سازی اهداف نظام-سیاسی را نشان‌می‌دهد. به‌دلیل ماهیت ناشناس اینترنت، جنگ ترکیبی به‌خودی‌خود انکار موجه[5] بیشتری را برای دولت روسیه فراهم‌می‌آورد که به این کشور اجازه‌می‌دهد با کاهش نیاز به نیروهای جنبشی در هزینه‌های نظامی خود صرفه‌جویی‌کند. استفاده از گروه‌های نیابتی برای راه‌اندازی یک حمله سایبری یک سپر اضافی برای کرملین ایجادمی‌کند. گروه‌های نیابتی همچنین به مسکو اجازه‌می‌دهند که ارتش این کشور را در بسیاری از موارد بدون هزینه اضافی با استعدادها و قابلیت‌های غیرنظامی تکمیل‌کند.

---

1. Anti-Maidan
2. Cyberberkut
3. Donetsk People's Republic (DPR)
4. Luhansk People's Republic (LPR)
5. Plausible Deniability

گروه‌های نیابتی غیردولتی که توسط روسیه به‌خدمت گرفته‌می‌شوند، یک‌شکل و یکپارچه نیستند و ممکن است اعضای سازمان‌های جوانان مورد حمایت دولت باشند یا از رهبران کسب‌وکارهای نزدیک به کرملین محسوب‌شوند. اگرچه قطعا روشن نیست که آیا مسکو پشت حمله‌های سایبری علیه دولت‌های طرفدار غرب در خارج نزدیک بوده یا خیر، بسیاری از کارشناسان به این نتیجه رسیده‌اند که این‌گونه حمله‌ها یا ازسوی کرملین هدایت شده یا دست‌کم ازسوی دولت روسیه پشتیبانی شده‌اند. تحلیل سیاست دفاعی فدراسیون روسیه و نگاه رهبران سیاسی و نظامی این کشور به مفهوم امنیت ملی نیز نشان می‌دهد که امکان انتساب این حمله‌ها به دولت روسیه دست‌کم به‌لحاظ نظری دور از انتظار نیست.

۴. تقابل سایبری روسیه و اتحادیه اروپایی

اتحادیه اروپایی به‌سرعت درحال ظهور به‌مثابه یک بازیگر اصلی در قلمرو امنیت سایبری است. این نهاد منطقه‌ای طی چند سال گذشته پیشرفت شگرفی در وضع قوانین، ارتباطات و اسناد راهبردی تجربه نموده‌است که به‌طور مستقیم با حوزه امینت سایبری سروکار دارد. بیشتر این فعالیت‌ها در واکنش به فعالیت‌های روسیه در فضای مجازی انجام شده‌اند. در سال ۲۰۰۸، امنیت سایبری برای نخستین‌بار در میان چالش‌های جهانی و تهدیدهای اصلی علیه اتحادیه اروپایی قرارگرفت و در گزارش اجرای راهبرد امنیتی اروپایی[1] بر آن تأکید شد (Barrinha, 2018:29). انگیزه این اقدام، اگرچه به‌طور مستقیم تصدیق‌نشد، اما برای همگان کاملا شفاف‌بود؛ حمله‌های سایبری علیه استونی و گرجستان. این حمله‌ها که به هکرهای روسی نسبت داده شده‌بود در مجموع از پیچیدگی خاصی برخوردار نبودند، اما پیام آنها روشن بود، جنگ اطلاعاتی یک احتمال واقعی است و روسیه دلیلی برای نگرانی در این زمینه به‌شمارمی‌آید.

اتحادیه اروپایی در ادامه اقدام‌های بیشتری را برای ارتقا ظرفیت‌های سیابری دولت‌های عضو و افزایش بازدارندگی در برابر حمله‌های سایبری علیه این اتحادیه انجام‌داد. تا اینکه نخستین راهبرد امنیت سایبری اتحادیه اروپایی پنج سال پس از طرح این مباحث تدوین‌یافت. سسیلیا مالمستروم[2] کمیسر امور داخلی[1]، کاترین اشتون[2] نماینده عالی اتحادیه اروپا در

[1]. Report on the Implementation of the European Security Strategy
[2]. Cecilia Malmström

سیاست خارجی و امور امنیتی[۳] و نیلی کروز[۴] کمیسر دستورکار دیجیتال اروپایی[۵] در ژانویه ۲۰۱۳ پیش‌نویس یک سند راهبردی نسبتا فراگیر را ارائه‌کردند که به‌واسطه سه رکن اصلی کنش به امنیت سایبری نزدیک‌می‌شد؛ امنیت اطلاعات و شبکه، اجرای قانون و دفاع. هر یک از این ارکان نیز دارای مجموعه‌ای از اولویت‌های سیاستگذاری و نهادها مانند آژانس اروپایی امنیت شبکه و اطلاعات (انیسا)[۶] و مرکز اروپایی جرایم سایبری پلیس اروپا[۷] هستند (EC, 2013:3-10). علاوه بر راهبرد امنیت سایبری، اتحادیه اروپایی در سال ۲۰۱۶ دستورالعملی را درخصوص حمله‌ها علیه سامانه‌های اطلاعاتی به‌تصویب رساند و پیشنهادی را برای اعمال یک دستورالعمل در مورد امنیت شبکه و سامانه‌های اطلاعاتی موسوم به دستورالعمل نیس[۸] ارایه‌داد که از ۶ می ۲۰۱۸ به‌اجرا درآمده‌است و می‌توان آن‌را به‌عنوان نخستین نمونه واقعی از قوانین اتحادیه اروپا در زمینه امنیت سایبری به‌شمارآورد (ENISA, 2018).

رهبران اروپایی همچنین همکاری‌های سایبری با ژاپن، کره‌جنوبی و هند را تداوم‌داده‌اند و درحال گنجاندن موضوعات سایبری در مناسبات همسایگی و گسترش اتحادیه اروپا به شرق اروپا هستند. برای نمونه، کمیسیون اروپا در ابتدای سال ۲۰۱۸ شش ابتکار اصلی را برای کشورهای بالکان غربی به‌تصویب‌رساند که شامل توسعه ظرفیت‌های سایبری و تقویت همکاری به‌منظور رسیدگی به مسائل مربوط به امنیت فضای مجازی و جرایم سایبری می‌شود (EC, 2018:17). پیش از آن نیز اتحادیه اروپایی در ژوئن ۲۰۱۵ برنامه اقدام راجع به ارتباطات راهبردی[۹] را برای مقابله با آنچه که کارزارهای گمراه‌سازی[۱۰] روسیه عنوان شده‌است، به‌تصویب‌رساند. یک کارگروه ویژه تحت عنوان استارت‌کام شرق[۱۱] نیز ذیل سرویس اقدام خارجی اتحادیه اروپایی[۱۲] برای ارائه گزارش و تحلیل روایت‌های گمراه‌کننده[۱]

---

1. The Commissioner for Home Affairs
2. Catherine Ashton
3. High Representative of the Union for Foreign Affairs and Security Policy
4. Neelie Kroes
5. European Commissioner for Digital Agenda
6. European Network and Information Security Agency (ENISA)
7. Europol's European Cyber Crime Centre (EC3)
8. Network and Information Security (NIS) Directive
9. Action Plan on Strategic Communication
10. Disinformation Campaigns
11. East StratCom
12. European External Action Service (EEAS)

و کار با شرکای شرقی بر حسب توسعه تولیدات ارتباطی و کارزارهای متمرکز بر تشریح بهتر خط‌مشی‌های اتحادیه اروپایی و پشتیبانی از تقویت محیط رسانه‌ای در منطقه مشارکت شرقی[۲] دایرشد (Benková, 2018: 1; EEAS, 2018). همه این اقدام‌ها در واقع با هدف تشکیل یک جبهه سایبری علیه روسیه صورت پذیرفته‌اند.

امنیت سایبری نزد اعضای اتحادیه اروپایی طی سال‌های اخیر به‌دنبال حمله‌های سایبری منتسب به روسیه در استونی، گرجستان و اوکراین به‌گونه‌ای افزایش یافته‌است که راهبرد جهانی اتحادیه اروپایی[۳] در سال ۲۰۱۶ مسایل سایبری را در کانون سیاست خارجی اتحادیه اروپا قرارداد که نشان از تثبیت تدریجی فضای سایبری به‌مثابه اولویت راهبردی و امنیتی اتحادیه اروپایی دارد. این سند، اتحادیه اروپایی را به‌مثابه یک بازیگر سایبری پیشرو[۴] معرفی‌می‌کند که قصددارد به‌گونه‌ای برجسته از ارزش‌ها و دارایی‌های حساس خود در دنیای دیجیتال پاسداری‌نماید (EEAS, 2016:42). تهدیدهای ترکیبی از دیگر جنبه‌های مرتبط با فضای سایبر است که در این راهبرد مورد توجه بروکسل قرار گرفته‌است. خطوط اصلی اقدام برای دولت‌های عضو اتحادیه اروپایی در این زمینه از آوریل ۲۰۱۶ طی یک چارچوب مشترک پیش می‌روند که پاسخی روشن به فعالیت‌های سایبری روسیه در اوکراین بود.

راهبرد جهانی اتحادیه اروپایی مراجع چندگانه‌ای را برای رسیدگی به موضوعات سایبری به‌وجودآورده و ۵ اقدام کلیدی در رابطه با امنیت سایبری معین کرده‌است: الف) تقویت همکاری بین دولت‌های عضو و اتحادیه اروپایی از نظر تیم‌های واکنش اضطراری؛ ب) گسترش پیوندهای بیشتر با بخش خصوصی به‌منظور یافتن راه‌حل‌هایی برای محافظت از زیرساخت‌های حیاتی در برابر ابعاد سایبری تهدیدهای ترکیبی؛ ج) بهبود امنیت و تاب‌آوری[۵] شبکه‌های برق؛ د) بهبود تبادل اطلاعات در بخش مالی؛ و هـ) هماهنگ‌سازی واکنش‌ها در بخش ترابری از لحاظ پاسخ به حمله‌های سایبری (Barrinha, 2018:32). این سند همچنین به افزایش همکاری با کشورهای ثالث در ایجاد تاب‌آوری سایبری و ظرفیت سایبری از طریق ابزاراهای مشارکت در صلح و ثبات اشاره‌می‌کند و به جزئیات ایجاد یک مرکز

---

1. Disinformation Narratives
2. Eastern Partnership Region
3. EU Global Strategy
4. Forward-Looking Cyber Player
5. Resilience

ائتلافی ترکیبی[1] مستقر در فنلاند می‌پردازد (Demertzis and Wolff, 2019:2). موضوع جنگ ترکیبی همچنین در کانون بیانیه اتحادیه اروپایی-ناتو قرارداشت که در حاشیه اجلاس سران ناتو در جولای ۲۰۱۶ ارائه‌شد. این بیانیه برخی حوزه‌های همکاری شامل ایجاد تاب‌آوری در فضای سایبری و توسعه قابلیت‌های مشترک در این زمینه را تعیین‌می‌کند. در سال ۲۰۱۸ نیز مرکز عملیات فضای سایبر[2] ناتو با همکاری اتحادیه اروپایی به بهره‌برداری رسید (NATO, 2020). سومین گزارش پیشرفت پیاده‌سازی راهبرد جهانی اتحادیه اروپایی در سال ۲۰۱۹ نیز با ذکر نام روسیه بر آمادگی مقابله این اتحادیه با حمله‌های سایبری و آمادگی برای جنگ ترکیبی تأکید کرده‌بود (EEAS, 2019: 19,37-42).

اگرچه تأثیر غیرمستقیم اقدام‌های روسیه در فعالیت‌های سایبری اتحادیه اروپایی به‌روشنی مشهوداست، اما واکنش مستقیم اتحادیه اروپایی به اقدام‌های سایبری مسکو علیه منافع اعضای این اتحادیه به‌همان اندازه آشکار نبوده‌است. برای اثبات این ادعا می‌توان به بیانیه آوریل ۲۰۱۸ شورای اروپایی در مورد فعالیت‌های سایبری بدخواهانه ارجاع‌داد. شورای اروپایی در این بیانیه استفاده بدخواهانه از فناوری‌های اطلاعات و ارتباطات شامل باج‌افزارهای واناکرای[3] و نوت‌پتیا[4] که منشأ زیان‌های اقتصادی و خسارت‌های فراوان در اتحادیه اروپا و فراتر از آن بودند را محکوم‌کرد. این بیانیه بیش از یک سال پس از انجام نخستین حمله باج‌افزاری واناکرای صادرشد، حمله‌ای دارای منشأ مشترک با حمله باج‌افزاری نوت‌پتیا که متهم ردیف اول آنها روسیه بود (Ivan, 2019:6). دولت‌های عضو در خصوص نسبت‌دادن این حمله‌ها به مسکو اختلاف‌نظر فراوانی داشته و دارند. با وجود اتهام فردی برخی اعضا ازجمله بریتانیا، دانمارک، لیتوانی و استونی مبنی بر دست‌داشتن روسیه در انجام حمله‌های باج‌افزاری واناکرای و نوت‌پتیا که ازسوی لتونی، سوئد و فنلاند نیز پشتیبانی می‌شد، سایر اعضای اتحادیه اروپایی شواهد و دلایل موجود را برای ایراد این اتهام به روسیه کافی‌نمی‌دانستند (Stilgherrian, 2018).

این قضیه بازتاب‌دهنده دو مشکل مشترک در رویکرد اتحادیه اروپایی به امنیت سایبری است. نخست اینکه دولت‌های عضو به اندازه کافی به‌یکدیگر و یا اتحادیه اروپایی برای به

---

1. Hybrid Fusion Cell
2. Cyberspace Operations Centre
3. WannaCry
4. NotPetya

اشتراک‌گذاشتن اطلاعات حساسی که می‌تواند به کشف منشأ حمله‌های سایبری منجر شود، اعتمادندارند. دوم اینکه توازنی ظریف میان پذیرش موضع تهاجمی علیه مسکو و فشارهای اقتصادی و ژئوپلیتیک در هنگام مواجهه با روسیه وجوددارد که این ملاحظه به‌ویژه در رابطه با اعضای کوچک‌تر اتحادیه اروپایی که تاکنون در معرض مستقیم حمله‌های سایری روسیه قرار نداشته‌اند بیشتر به‌چشم می‌خورد. برای برخی از دولت‌های عضو، روسیه یک شریک اقتصادی مهم و بزرگ‌ترین همسایه منطقه‌ای است. این موازنه ظریف به‌گونه‌ای عمل‌می‌کند که اغلب به ادعای وجود ناسازگاری و تردید راهبردی در اتحادیه اروپایی نسبت به چگونگی مواجهه با روسیه ازجمله در عرصه سایبری منجرمی‌شود.

از چشم‌انداز اتحادیه اروپایی در هنگام طرح موضوع فضای مجازی، روسیه هم‌زمان باید به‌مثابه یک قطب جرایم سایبری، یک همسایه و یک قدرت درحال ظهور مورد ملاحظه قرارگیرد. این حوزه‌ها لزوما دو به دو ناسازگار یستند، اما قطعا دربردارنده مجموعه‌ای از رویکردهای متفاوت به‌لحاظ چگونگی تعامل با روسیه هستند. چنانچه بحث فضای سایبری در اتحادیه اروپایی پیرامون جرایم سایبری در جریان‌باشد، روسیه به‌طور عمده به‌مثابه قطبی در عرصه فعالیت‌های جنایی علیه منافع دولت‌های عضو این اتحادیه در قلمروی سایبری درنظر گرفته‌می‌شود.

شرکت روسی گروه-آی‌بی[1] -از شرکت‌های پیشرو در حوزه امنیت سایبری- در سال ۲۰۱۴ ارزش بازار جرایم سایبری در این کشور را در حدود ۲,۳ میلیارد دلار برآورد کرده بود (Maurer, 2018). با این حال، ایجاد تمایز میان جرایم سایبری دولت-محور یا مورد حمایت دولت با جرایمی که در حقیقت برای سود شخصی صورت‌می‌پذیرند، حائز اهمیت است. سابقه روسیه در حوزه جرایم سایبری در هر دوی این سطوح بسیار نگران‌کننده است. با این‌همه، درحالی‌که مجموعه فعالیت‌ها در سطح نخست پیوند نزدیکی با اهداف راهبردی گسترده‌تر دارد در سطح دوم این‌گونه نیست. بنابراین، به همان شکلی که ایالات‌متحده با چین برای همکاری در زمینه جرایم سایبری در سال ۲۰۱۵ به توافق دست‌یافت -که در آن زمان به‌مثابه یک پیروزی برای دیپلماسی سایبری به‌نظر می‌رسید- ترتیبات مشابهی نیز احتمالا می‌تواند بین اتحادیه اروپایی و مسکو ایجادشود، کما اینکه سوابقی نیز برای آن وجوددارد. روسیه تاکنون با اتحادیه اروپایی در خصوص مسائل مربوط به فعالیت سازمان‌های

[1]. Group-IB

تروریستی در فضای مجازی و حتی با پلیس اروپایی در حوزه جرایم سایبری همکاری داشته است (Barrinha, 2018:36). با این‌همه این همکاری‌ها تا به امروز بسیار محدود باقی مانده‌است.

اتحادیه اروپا و بسیاری از دولت‌های عضو آن درحال اتخاذ موضع مهار محدود در رابطه با فعالیت‌های سایبری روسیه هستند. مهار محدود نیازمند دریافت تفسیری عینی از فضای سایبری است که ترکیبی از تدابیر تعاملی بازدارنده و گزینشی علیه روسیه را در خود جای داده‌باشد. در مجموع، واکنش اعضای اتحادیه اروپایی در برابر فعالیت‌های سایبری روسیه بسته به اینکه به‌مثابه کشوری همسایه، قدرتی درحال ظهور یا قطب جرایم سایبری فرض‌شود، متفاوت خواهدبود. دلیل اصلی بی‌پاسخ ماندن اغلب حمله‌های سایبری منتسب به روسیه علیه اتحادیه اروپایی نیز به همین ناسازگاری در برداشت‌های اعضا از روسیه بازمی‌گردد. با این‌همه در هر سه فرض فوق فرصت‌هایی هم برای همکاری و هم برای تعارض نهفته است که طرفین باید برای هر دوی آنها آماده‌باشند.

۵. دفاع سایبری روسیه در برابر ایالات متحده

جامعه دفاعی غرب بر این باور است که روسیه در یک دهه گذشته از حمله‌های سایبری علیه دولت‌های پساشوروی به‌عنوان ابزاری برای دستیابی به اهداف سیاست خارجی و پیشبرد برنامه‌هایش در برابر جهان غرب استفاده کرده‌است. در عین حال، مسکو به‌تازگی به‌طور مستقیم منافع ایالات متحده را در حوزه سایبری هدف قرار داده‌است که طرح اتهام علیه اتباع و شرکت‌های روسی مبنی بر دخالت در انتخابات ریاست‌جمهوری سال ۲۰۱۶ مهم‌ترین و جدی‌ترین مورد به‌شمار می‌آید. ازسوی دیگر، عملیات جاسوسی ایالات متحده علیه بسیاری از دولت‌های خارجی اعم از هم‌پیمانان و دشمنان این کشور به‌لطف افشاسازی‌های نظارتی ادوارد اسنودن[1] و تلاش جولین آسانژ[2] برای انتشار صدها هزار سند محرمانه دولت ایالات متحده از طریق وبگاه ویکی‌لیکس[3] امروزه دیگر بر هیچ‌کس پوشیده‌نیست.

---

[1]. Edward Snowden
[2]. Julian Assange
[3]. WikiLeaks

با این‌همه، اگرچه هر دو قدرت ایالات‌متحده و فدراسیون روسیه از فضای مجازی برای مدیریت اطلاعات علیه یکدیگر از طریق جمع‌آوری اطلاعات حساس استفاده‌می‌کنند، اما روسیه در این عرصه پیشتاز است. درحالی‌که ایالات‌متحده به‌طور عمده درگیر دستکاری اطلاعات از طریق ابزارهای مخفی است، روسیه عملیات سایبری را تا "جنگ اطلاعاتی" امتدادمی‌دهد. جنگ اطلاعاتی روسیه علیه ایالات متحده دربردارنده سه هدف است: جمع‌آوری اطلاعات حساس از طریق عملیات سایبری، تبلیغات سیاسی برای دستکاری افکار عمومی و بهره‌برداری از اطلاعات برای تضعیف مقامات دولتی. از آنجاکه فعالیت سایبری با هدف جنگ اطلاعاتی در حیطه عمل سیاسی قرار می‌گیرد این فعالیت‌ها بخشی از حمله‌های سایبری سیاسی را تشکیل‌می‌دهند که به‌طور معمول با رویدادهای سیاسی عمده در پیوند هستند و دلیل مشخصی برای انجام آنها وجوددارد.

اطلاعات حساسی که از طریق جاسوسی استخراج می‌شوند به‌طور معمول توسط دولت‌ها به‌عنوان ورودی سیاستگذاری و فرایند دیپلماسی استفاده می‌شوند، اما روسیه به‌طور عمده از آنها به‌مثابه ابزاری برای تبلیغات استفاده‌می‌کند. در این زمینه، ژنرال فیلیپ بریدلاو[1] -فرمانده عالی پیشین نیروهای ائتلاف ناتو در اروپا- بیان می‌دارد که روسیه شگفت‌انگیزترین حمله رعدآسای جنگ اطلاعاتی که تاریخ جنگ‌های اطلاعاتی به‌خود دیده را برپا کرده‌است (Pomerantsev, 2014).

ایالات‌متحده و روسیه از سال ۱۹۹۸ دیپلماسی در حوزه امنیت سایبری را شروع کرده‌اند، اما پیامدهای آن قابل توجه نبوده‌است. ایالات متحده، فدراسیون روسیه و جمهوری خلق چین به‌همراه برخی دیگر از دولت‌ها در ژوئن ۲۰۱۳ موافقت‌نامه‌ای را به‌منظور ایجاد هنجارهای امنیت سایبری و هماهنگی و برقراری پیوند میان تشکیلات امنیتی ذی‌نفع در جهت رویارویی با تهدیدهای سایبری علیه زیرساخت‌های حیاتی به امضا رساندند (Libicki, 2019:42). با این حال، موافقت‌نامه مذکور به‌دلیل رویدادهایی که پس از آن اتفاق‌افتاد، تحقق‌نیافت. اندک زمانی پس از امضای این موافقت‌نامه، ادوارد اسنودن -پیمان‌کار سابق آژانس امنیت ملی ایالات متحده[2]- نظارت سایبری دولت ایالات متحده علیه شهروندان و مقامات رسمی کشورهای مختلف را با انتشار اسنادی که در اختیار داشت، افشا نمود. متعاقب طرح اتهام ایالات متحده علیه

[1]. Philip Breedlove
[2]. US National Security Agency

اسنودن و فرار وی به روسیه، مسکو درخواست واشنگتن برای استرداد وی را نپذیرفت و اعطای پناهندگی موقت به وی را تضمین‌نمود (Soesanto, 2019:19).

تنش‌های سایبری ایالات‌متحده-روسیه به‌دنبال عملیات نفوذ گسترده علیه مقامات حزب دموکرات در کارزار انتخاباتی ریاست‌جمهوری سال ۲۰۱۶ که به نفوذگرهای فضای مجازی تحت حمایت روسیه نسبت داده‌شد، به وخامت گرایید. در این عملیات، اطلاعات بسیار محرمانه‌ای از طریق نفوذ سایبری به شبکه‌های رایانه‌ای کنگره ملی دموکرات[۱] و حساب‌های رایانامه‌ای کارمندان این حزب در اختیار نفوذگرها قرار گرفته‌بود. این اطلاعات توسط فرد یا گروه نفوذگری با نام مستعار گوچیفر ۲,۰[۲] و وبگاه افشاگر ویکی‌لیکس در ماه‌های ژوئن، جولای و اکتبر ۲۰۱۶ به‌صورت برخط منتشرشدند. اطلاعات فاش‌شده شامل مکاتبات داخلی کنگره ملی دموکرات، تحقیق تقابلی علیه دونالد ترامپ[۳] و پیام‌های رایانامه‌ای جان پودستا[۴] -رئیس کارزار تبلیغاتی هیلاری کلینتون[۵] می‌شد. محتوای رایانامه‌های پودستا که توسط ویکی‌لیکس تحت عنوان "شگفتی اکتبر[۶]" منتشرشد، حاوی اطلاعات بحث‌برانگیزی درباره دیدگاه‌ها و فعالیت‌های کارزار تبلیغاتی هیلاری کلینتون بود (Abrams, 2019).

مقامات وزارت دادگستری ایالات متحد در اکتبر ۲۰۱۶ به‌طور رسمی دولت روسیه را به دخالت در نفوذ به شبکه‌های رایانه‌ای کنگره ملی دموکرات در تلاش برای تأثیرگذاری بر انتخابات ریاست‌جمهوری این کشور متهم‌کردند. در ژانویه ۲۰۱۷ نیز جامعه اطلاعاتی ایالات متحده[۷] (متشکل از سازمان اطلاعات مرکزی (سیا)[۸]، آژانس امنیت ملی[۹] و اداره تحقیقات فدرال[۱۰]) در گزارشی اعلام داشت که "کارزار نفوذ" [۱۱] علیه انتخابات ریاست‌جمهوری ایالات متحده به دستور ولادیمیر پوتین و با هدف افزایش فرصت‌های ترامپ برای کسب این منصب

---

1. Democratic National Congress (DNC)
2. Guccifer 2.0
3. Donald Trump
4. John Podesta
5. Hillary Clinton
6. October Surprise
7. US Intelligence Community (IC)
8. Central Intelligence Agency (CIA)
9. National Security Agency (NSA)
10. Federal Bureau of Investigation (FBI)
11. Influence Campaign

صورت پذیرفته‌است (Shad, 2018:48-49). اینکه آیا میان کارزار انتخاباتی ترامپ و نفوذگران روسی تبانی صورت گرفته‌بود یا اقدام این نفوذگران بدون اطلاع اطرافیان ترامپ بود، کماکان به‌لحاظ عمومی نامشخص باقی مانده‌است. در هر صورت، هدف این عملیات نفوذ که با پشتیبانی مسکو صورت گرفته‌بود به گفته مقامات اطلاعاتی ایالات‌متحده بی‌اعتبار کردن هیلاری کلینتون و کمک به پیروزی دونالد ترامپ در انتخابات ریاست‌جمهوری بود. به‌همین دلیل می‌توان احتمال داد نفوذگران روسی به برخی از شبکه‌های رایانه‌ای جمهوری‌خواهان نیز رسوخ کرده‌بودند، اما اطلاعات آن با توجه به هدفی که دنبال می‌کردند، هرگز منتشرنشد. ازسوی دیگر، اطلاعات مربوط به دموکرات‌ها و به‌ویژه هیلاری کلینتون درست در زمانی منتشر شد که می‌توانست بیش‌ترین آثار زیان‌بار را برجای بگذارد.

واکنش واشنگتن به دخالت روسیه در انتخابات ریاست‌جمهوری در مجموع محتاطانه و به نسبت تأکیدی که در قوانین ایالات متحده برای پیگرد و مجازات این‌گونه جرایم شده‌است، تساهل‌آمیز بود. بر اساس گزارش واشنگتن‌پست[1]، سازمان سیا "دخالت مستقیم پوتین در کارزاری سایبری برای ایجاد اختلال و بی‌اعتبارسازی رقابت انتخاباتی ریاست‌جمهوری" را در ابتدای آگوست ۲۰۱۶ نزد باراک اوباما[2] افشا ساخته‌بود. با این‌همه، دولت اوباما تا ماه دسامبر حاضر به تصدیق نفوذ سایبری دولت روسیه در انتخابات ریاست‌جمهوری این کشور نشد (Washington Post, 2017). واکنش اولیه دولت ایالات متحده به دخالت روسیه شامل سه مرحله بود: بررسی بیشتر در خصوص نقش و نیت مسکو، رسیدگی به آسیب‌پذیری‌ها سامانه انتخاباتی ایالات متحده، و پشتیبانی گنکره‌های هر دو حزب از بیانیه علیه روسیه.

علاوه بر این، دولت اوباما به برخی از گزینه‌ها برای واکنش در برابر روسیه ازجمله یورش سایبری به زیرساخت‌های روسیه، انتشار مطالب جمع‌آوری‌شده ازسوی سیا برای شرمسار کردن پوتین و اعمال تحریم‌های اقتصادی فلج‌کننده اشاره‌کرد. با این‌همه با در نظر گرفتن چالش‌ها و مخاطرات هر یک از این اقدام‌ها، دولت اوباما در نهایت با صدور بیانیه‌ای به ارائه پاسخی معتدل بسنده‌کرد؛ اخراج سی‌وپنج دیپلمات روس، تعطیلی دو مرکز متعلق به روس‌ها در نیویورک و مریلند و اعمال تحریم‌های اقتصادی هدفمند علیه ۶ مقام و ۵ نهاد و شرکت

[1]. Washington Post
[2]. Barack Obama

روسی. اوباما همچنین در این بیانیه تهدید کرده‌بود که این اقدام‌ها "تمام پاسخ ما به روسیه" نیست. وی همچنین اظهار داشت، "همه آمریکایی‌ها باید نسبت به اقدام‌های روسیه هوشیارباشند" (Gambino and Siddiqui, 2016).

کاوش اطلاعاتی در خصوص مداخله انتخاباتی روسیه همچنین شامل تحقیقی هم‌پوشان درباره هم‌دستی احتمالی همکاران ترامپ با مسکو در ارتباط با نفوذ سایبری به رقابت‌های انتخاباتی نیز می‌شد. نکته جالب این‌که ابعاد فرعی قضیه دخالت سایبری روسیه در انتخابات ریاست‌جمهوری ایالات متحده توجه به‌مراتب بیشتری را به نسبت اصل قضیه در محافل سیاسی و اطلاعاتی این کشور به‌ویژه پس از تنظیم کیفرخواست علیه پل منافورت[1] -رئیس پیشین کارزار انتخاباتی ترامپ- به‌خود معطوف داشته‌است (Smith, 2019). این واقعیت نشان می‌دهد که دخالت سایبری روسیه در انتخابات ایالات متحده نه‌تنها از نظر تأثیر بر انتخابات، بلکه به‌لحاظ آثار گسترده‌تری که می‌تواند بر مفاهیم امنیتی، سیاسی و اجتماعی جامعه آمریکا داشته‌باشد، حائز اهمیت است.

نفوذ سایبری روسیه در انتخابات ۲۰۱۶ ایالات متحده اولین و آخرین تلاش مسکو برای تأثیرگذاری بر بزرگ‌ترین رقیب خود به‌شمارنمی‌آید و به‌نظر می‌رسد در غیاب هرگونه موافقت‌نامه سایبری میان واشنگتن و مسکو، روابط سایبری بین دو کشور همچنان مبهم و نامطمئن باقی خواهدماند. در این میان، آگاهی از برخی مسائل برای درک عمیق‌تر تنش‌های سایبری ایالات متحده و روسیه مهم است. نخست درحالی‌که روسیه به‌دنبال تضمین امنیت سایبری از طریق یک پیمان بین‌المللی است، ایالات متحده خواهان دستیابی به این هدف از طریق تفاهم غیررسمی بین نهادهای مجری قانون است. این دوگانگی از رویکردهای متفاوت دو کشور در قبال اصلاح پیمان مقررات ارتباطات دوربرد بین‌المللی[2] در سال ۲۰۱۲ نیز مشهود است. روسیه معاهده اصلاح‌شده را امضا کرده‌است، اما ایالات متحده و اعضای اتحادیه اروپایی با اعلام اینکه معاهده جدید با افزایش کنترل دولت بر فضای مجازی دسترسی آزاد به اطلاعات را محدود می‌سازد، از پذیرش آن خودداری کرده‌اند.

دوم اینکه ایالات متحده و روسیه دست‌کم پیرامون سه بعد مهم امنیت سایبری یعنی جرایم سایبری، جاسوسی و تفکیک میان اهداف نظامی و غیرنظامی با یکدیگر اختلاف‌نظر

---

1. Paul Manafort
2. International Telecommunication Regulations (ITRs)

دارند. واشنگتن به‌طور عمده علاقه‌مند به کنترل جرایم سایبری است، اما روسیه همراه با چین بر یک توافق جامع امنیت سایبری شامل همه ابعاد تأکیددارد. سوم اینکه ایالات‌متحده و روسیه اگرچه برای مدتی طولانی در زمینه امنیت سایبری درحال مذاکره بوده‌اند، اما در ایجاد هنجارهای سایبری قابل تراضی شکست خورده‌اند. روس‌ها سلاح‌های سایبری را در زمره سلاح‌های کشتار جمعی[1] دسته‌بندی می‌کنند و بنابراین اساسا خواهان غیرقانونی اعلام‌کردن استفاده از آنها به‌مثابه ابزارهای جنگی هستند. در برابر، ایالات متحده استفاده از سلاح‌های سایبری به‌عنوان ابزار قانونی جنگ را در صورت رعایت قواعد موجود و هنجارهای درگیری‌های مسلحانه بین‌دولتی مجازمی‌شمارد.

در نهایت اینکه اگرچه تنش‌های سایبری اخیر میان ایالات متحده-روسیه بر عملیات نفوذ روسیه در انتخابات ۲۰۱۶ متمرکز است، اما موضوع سایبری بلندمدت‌تر و عمیق‌تر میان دو کشور به حمله‌های سایبری مرگبار یا جنبشی مربوط‌می‌شود. چنین حمله‌هایی می‌توانند در صورت بروز یک درگیری مسلحانه تمام‌عیار روی دهند و فراگیرشدن فضای مجازی اشیاء محیطی مساعد برای به‌واقعیت پیوستن آنها فراهم آورده‌است. در مجموع، با توجه به فقدان قواعد به‌لحاظ بین‌المللی به‌رسمیت شناخته‌شده در مورد روابط سایبری بین‌دولتی و نیز عدم تحقق هرگونه موافقت‌نامه امنیت سایبری دوجانبه میان ایالات متحده و روسیه تا به امروز، مناسبت سایبری میان دو کشور در ادامه پیچیده‌تر و دشوارتر نیز خواهدشد. علاوه بر این، تنش‌های فضای واقعی میان واشنگتن و مسکو ازجمله خروج ایالات متحده و سپس روسیه از پیمان منع موشک‌های هسته‌ای میان‌برد[2] نیز بر شدت نابسامانی روابط دو کشور در فضای مجازی می‌افزاید.

نتیجه‌گیری

با توجه به ماهیت غیرمتعارف و تازگی موضوعات سایبری در روابط بین‌الملل، هنجارها و قواعد به‌لحاظ بین‌المللی پذیرفته‌شده حاکم بر فضای مجازی هنوز مشخص نشده‌اند. علاوه بر این، دولت‌ها به احتمال فراوان بیش‌ازپیش به‌سمت دخالت سایبری جذب‌می‌شوند زیرا به‌سختی می‌توان شواهد واقعی محکم و مستدلی را علیه دخالت سایبری اقامه نمود. حتی در

---

1. Weapons of Mass Destruction (WMD)
2. Intermediate-Range Nuclear Forces Treaty (INF)

صورت نگرانی دولت‌ها از ارائه شواهد واقعی تصادفی علیه آنها، استفاده از گروه‌های نفوذگر خصوصی می‌تواند زمینه انکار موجه را برایشان فراهم‌آورد. استدلال پایه‌ای مقاله حاضر این بود که تهدید سایبری، اگرچه در ظاهر یک مسأله فنی به‌شمارمی‌آید، اما به‌عنوان یک چالش سیاسی بزرگ در روابط بین‌الملل معاصر ظهور پیدا کرده‌است. بر همین اساس این مقاله با تأکید بر تهدید سایبری به‌مثابه امری سیاسی در روابط بین‌دولتی بر مطالعه تنش‌های سایبری روسیه با غرب متمرکز بود.

نبرد سایبری می‌تواند به‌طور بالقوه بین دولت‌هایی رخ‌دهد که سابقه‌ای طولانی از روابط خصمانه دارند. احتمال وقوع این رویداد نیز زمانی افزایش‌می‌یابد که روابط رقابت‌آمیز بین‌دولتی به تنش‌های جدی و یا شرایط شبه بحرانی سوق‌یابد. با این‌همه، دولت‌ها به‌طور عمده از ورود به یک جنگ سایبری آشکار اجتناب‌می‌کنند. عامل بازدارندگی سایبری به‌طور قطع در پرهیز دولت‌ها از درگیرشدن در یک جنگ سایبری تمام‌عیار مؤثراست، اما حمله‌های سایبری غیرمرگبار اکنون به‌طور فزاینده‌ای درحال انجام است که تأثیر بی‌ثبات‌کننده معنی‌داری در روابط بین‌دولتی برجای می‌گذارند. سه عامل را می‌توان برای افزایش حمله‌های سایبری در مناسبات میان دولت‌ها برشمرد؛ فقدان هنجارها و قواعد بین‌المللی حاکم بر روابط بین‌دولتی در فضای مجازی، گسترش فضای مجازی اشیاء و انکار موجه که نسبت‌دادن حمله‌های سایبری به عاملان واقعی آنها را مشکل‌می‌سازد.

علاوه بر این، زمانی که بحث مناسبات سایبری روسیه-غرب به‌میان می‌آید، عامل فقدان هرگونه توافق‌نامه دوجانبه یا چندجانبه میان روسیه با دولت‌های غربی در رابطه با تنظیم روابط متقابل در فضای مجازی را نیز باید به عوامل پیش‌گفته اضافه‌نمود. جامعه امنیتی غرب بر این باور است که روسیه به‌طور فزاینده‌ای در عملیات‌های سایبری علیه ایالات متحده و دولت‌های اروپایی به‌ویژه از زمان بحران ۲۰۱۴ اوکراین دست داشته‌است. تنش‌های سایبری میان روسیه و اتحادیه اروپایی چنان برجسته‌است که می‌توان تثبیت این اتحادیه به‌عنوان یک بازیگر سایبری جهانی مهم طی یک دهه گذشته را به تلاش بی‌وقفه اعضای این اتحادیه برای مقابله با تهدیدهای سایبری مسکو نسبت‌داد.

دولت‌های عضو اتحادیه اروپایی، جنگ سایبری روسیه علیه خود و نهادهای اروپایی را به‌مثابه بخشی از سیاست گسترده‌تر مسکو مبنی بر بی‌ثبات‌سازی و تفرقه در اروپا درک می‌کنند. اعضای اتحادیه اروپایی به‌خوبی از مخالفت روسیه با گسترش و تقویت این اتحادیه

آگاه و بر دلایل آن نیز واقف هستند. آنها به‌طور عمده نگران تبدیل فضای سایبری به عرصه جدید هماوردی با مسکو هستند. رهبران روسیه فضای مجازی را فرصتی برای جبران کاستی‌های قدرت این کشور در فضای واقعی قلمدادمی‌کنند و به‌همین جهت نیز به‌صورت برنامه‌ریزی‌شده به جنگ اطلاعاتی در فضای سایبری روی‌آورده‌اند. در برابر، اتحادیه اروپا تمایل‌دارد فضای مجازی را از عملیات اطلاعاتی جداکند و نشانه‌های واضحی نیز مبنی بر انجام تفکیک بیشتر میان این دو بعد در هر دو سطح منطقه‌ای و ملی به‌چشم می‌خورد که مهم‌ترین آنها تأسیس استارت‌کام شرق به‌منظور پیگیری عملیات اطلاعاتی خارج از سازوکارهای مرتبط با آزادی فضای مجازی است.

تنش‌های سایبری ایالات متحده-روسیه نیز در پی عملیات گسترده نفوذگرهای سایبری منتسب به دولت روسیه علیه شبکه‌های رایانه‌ای حزب دموکرات ایالات متحده طی کارزار انتخابات ریاست‌جمهوری ۲۰۱۶ این کشور به وخامت گرایید. ریشه این تنش‌ها با تنش‌های روسیه-اروپا در فضای مجازی یکسان به‌نظر می‌رسند و به‌طور عمده بازتاب موضوعات عمیق‌تر در روابط میان روسیه-غرب در فضای واقعی است.

درخصوص ویژگی‌های جنگ سایبری روسیه علیه غرب (بخش نخست پرسش فرعی مقاله) با استناد به یافته‌های مقاله می‌توان اظهارداشت جنگ سایبری روسیه علیه غرب دارای مشخصه‌هایی است که برخی از آنها در تمام جنگ‌های سایبری مشترک است: دستیابی به اهداف سیاسی و راهبردی بدون توسل به جنگ مسلحانه؛ عدم شفافیت مرز میان اهداف نظامی و غیرنظامی؛ توسل به حمله‌های سایبری ازجمله منع سرویس؛ تغییر ظاهر تارنما؛ ترویج بدافزارها و غیره. در عین حال، جنگ سایبری روسیه علیه غرب از ویژگی‌های منحصربه‌فردی نیز برخوردار است که مهم‌ترین آن به توسعه مفهوم بازدارندگی سایبری نزد این کشور تا ایجاد موازنه در شرایط رقابت‌های نظامی و سیاسی متعارف بازمی‌گردد. از دیگر ویژگی‌های انحصاری جنگ سایبری مسکو دربرابر غرب می‌توان به مواردی همچون پیوند حمله‌های سایبری روسیه-محور علیه منافع غرب با تنش‌های موجود در مناسبات روسیه-غرب در فضای واقعی؛ توسل مسکو به نیروهای نیابتی و گروه‌های نفوذگر خصوصی به‌منظور انکار موجه؛ حمله سایبری به دولت‌های پساشوروی علاقه‌مند به نزدیکی با غرب و پیوستن به نهادهای غربی و اروپایی؛ عدم‌پذیرش مسئولیت هیچ‌یک از حمله‌های منتسب به

مسکو ازسوی مقامات رسمی این کشور؛ عدم برجای‌گذاشتن تلفات انسانی مستقیم و پیوند مستقیم با رویدادهای سیاسی مهم و دارای پیامدهای حائز اهمیت برای مسکو اشاره‌کرد.

در رابطه با بخش دوم پرسش فرعی مقاله نیز می‌توان عنوان‌داشت، روسیه تقریبا از شیوه‌ها و ابزارهای گوناگونی در جریان نبرد سایبری با غرب استفاده‌می‌کند. مسکو از سه ابزار نخست جنگ سایبری شامل حمله‌های منع سرویس توزیع‌شده، هک‌کردن و به‌کارگیری بدافزارها به‌وفور علیه غرب و اهداف غربی استفاده کرده‌است، اما نسبت‌دادن استفاده از سلاح چهارم (یعنی انجام تهدیدهای پیشرفته و مستمر که از طریق آمیزه‌ای از سه سلاح پیشین اعمال‌می‌شوند) به این کشور هم به‌جهت نیاز به دانش و فناوری پیشرفته برای کاربرد آن -که شاید هنوز در اختیار مسکو نباشد- و هم به‌دلیل مشکل ردیابی افراد و دولت‌های به‌کارگیرنده آن دشوار خواهدبود.

از همه مهم‌تر اینکه انگیزه اصلی مسکو از توسل به جنگ سایبری در برابر غرب (پرسش اصلی مقاله) را جبران ضعف قدرت این کشور در فضای واقعی به‌ویژه به‌لحاظ اقتصادی و نظامی تشکیل می‌دهد. روسیه همچنین با اتخاذ رویکرد جنگ ترکیبی سایبری و جنبشی به‌دنبال حفظ دولت‌های پساشوروی در خارج نزدیک حول محور خود و جلوگیری از نزدیکی آنها به غرب است. به‌همین دلیل است، کشورهای واقع در شرق اروپا به عرصه جنگ سایبری روسیه علیه غرب کشده شده‌اند.

با این تفاسیر، دلیل اصلی استفاده روسیه از سلاح سایبری علیه اهداف غربی را می‌توان به تلاش این کشور برای تقویت بازدارندگی درمقابل اقدام‌های خصمانه غرب علیه مسکو به‌ویژه در خارج نزدیک روسیه -ازجمله تلاش برای وابسته‌ساختن هرچه بیشتر دولت‌های پساکمونیستی به نهادهای غربی همچون ناتو و اتحادیه اروپایی- نسبت‌داد. کرملین نه‌تنها نگران نفوذ سایبری دولت‌ها و نهادهای غربی به درون مرزهای این کشور با هدف تأثیرگذاری بر اذهان شهروندان این کشور است، بلکه از دورشدن کشورهای پساشوروی از مدار روسیه و پیوستن به نهادهای غربی در اثر کنش‌های متعارف و سایبری غرب نیز به‌شدت واهمه‌دارد. از این رو، در شرایط موازنه نامتوازن روسیه-غرب در مؤلفه‌های جنبشی به‌ویژه توانایی‌های نظامی و اقتصادی، کرملین برای متعادل‌ساختن این موازنه به ظرفیت‌های سایبری روی آورده‌است. بنابراین، بازدارندگی سایبری نزد روسیه به نبرد سایبری محدود نمی‌شود و از آن برای ایجاد موازنه در نبردهای نظامی و سیاسی متعارف نیز بهره‌می‌برد. دشواری نسبت‌دادن حمله‌های سایبری نیز با ایجاد امکان انکار موجه نیز توسل مسکو به سلاح سایبری را تسهیل‌می‌سازد.

منابع و مآخذ

– برنا، کیوان؛ فتحی، فرهاد و مومنی، عصمت (۱۳۹۷) «کشف دانش و کاربرد آن در اینترنت اشیاء»، فصلنامه *مطالعات دانش‌شناسی*، ۵(۱۷)، ۱۲۳-۱۵۶.

– ترابی، قاسم (۱۳۹۸)، «ضرورت‌ها و الزامات تدوین راهبرد سایبری کارآمد»، *فصلنامه مطالعات راهبردی*، ۲۲(۸۵)، ۱۸۵-۱۹۳.

– دهقانی، علی اصغر (۱۳۹۶)، «بازدارندگی سایبری در امنیت نوین جهانی: تهدید سایبری روسیه و چین علیه زیرساخت‌های حیاتی آمریکا»، *فصلنامه رهیافت‌های سیاسی و بین‌المللی*، ۸(۴)، ۱۲۱-۱۴۷.

– عبدالی، زانیار و نیاکویی، امیر (۱۳۹۸)، «تناقض بین دو اصل حق تعیین سرنوشت و حق حاکمیت ملی در حقوق بین الملل (مطالعه موردی: بحران اوکراین و جدایی کریمه از آن کشور)»، فصلنامه *سیاست*، ۴۹(۳)، ۷۰۱-۷۲۴.

– کلانتری، فتحا... و صادقی، امیر (۱۳۹۸)، «"منطقه منازعه خاکستری" مفهوم نوپدید در مدیریت دفاعی آینده»، فصلنامه *مطالعات مدیریت راهبردی دفاع ملی*، ۳(۱۰)، ۱۰۳-۱۲۸.

– مایلی، محمدرضا و بهمنی، محمدسعید (۱۳۹۱)، «جنگ سرد نوین و رقابت بین قدرت‌های جهانی در فضای سایبری»، فصلنامه *مطالعات روابط بین‌الملل*، ۵(۲۰)، ۱۳۳-۱۶۷.

–Abrams, A. (2019), "Here's What We Know So Far about Russia's 2016 Meddling", *Time*, 18 April, Available at: https://time.com/5565991/russia-influence-2016-election, Accessed on: 19 April 2020.

–*Agenda* (15 Nov 2017), "Russia Offers Easier Citizenship Procedures to People of Occupied Tskhinvali, Georgia", Available at: http://agenda.ge/en/news/2017/2506, Accessed on: 6 April 2020.

–Ahn, M. K., Kim, Y. H. and Lee, J.-R. (2020), "Hierarchical Multi-Stage Cyber Attack Scenario Modeling Based on G&E Model for Cyber Risk Simulation Analysis", *Applied Sciences*, 10(4): 1426-1442.

–Ajir, M. and Vaillant, B. (2018), "Russian Information Warfare: Implications for Deterrence Theory", *Strategic Studies Quarterly*, 12(3): 70-89.

–Allen, T. S. and Moore, A. J. (2018), "Victory without Casualties: Russia's Information Operations", *Parameters* 48(1): 59-71.

–Andress, J. and Winterfeld, S. (2014), *Cyber Warfare: Techniques, Tactics, and Tools for Security Practitioners*, Waltham: Syngress.

–Arquilla, J. (2013), "Twenty Years of Cyberwar", *Journal of Military Ethics* 12(1): 80-87.

–Arquilla, J. and Ronfeldt, D. (1993), "Cyberwar is Coming!", In J. Arquilla and D. Ronfeldt (Eds.), *In Athena's Camp: Preparing for Conflict in the Information Age* (pp. 23–60), Santa Monica: RAND, Available at:

https://www.rand.org/content/dam/rand/pubs/reprints/2007/RAND_RP223.pdf, Accessed on: 10 April 2020.
- Atkinson, C. (2018), "Hybrid Warfare and Societal Resilience: Implications for Democratic Governance", *Information & Security: An International Journal*, 39(1), 63-76.
- Baezner, M. (2018), *Cyber and Information Warfare in the Ukrainian Conflict*, Zurich: Center for Security Studies (CSS).
- Barrinha, A. (2018), "Virtual Neighbors: Russia and the EU in Cyberspace", *Insight Turkey* 20(3): 29-42.
- Barrinha, A. (2018), "Virtual Neighbors: Russia and the EU in Cyberspace", *Insight Turkey*, 20(3): 29-41, DOI: 10.25253/99.2018203.02.
- Benková, L. (2018), "The Rise of Russian Disinformation in Europe", *AIES Fokus*, Available at: https://www.aies.at/download/2018/AIES-Fokus_2018-03.pdf, Accessed on: 8 April 2020.
- Burton, J. (2019), "Cyber-Attacks and Freedom of Expression: Coercion, Intimidation and Virtual Occupation", *Baltic Journal of European Studies*, 9(3), 116–133.
- Chapman, B. (2019), "Recent U.S. and International Assessment of Baltic Security Developments", *Security and Defence Quarterly*, 26(4): 3–33.
- Chivvis, C. S. (2017), "Hybrid War: Russian Contemporary Political Warfare", *Bulletin of the Atomic Scientists* 73(5): 316-321.
- Clarke, R. and Knake, R. (2010), *Cyber War: The Next Threat to National Security and What to Do About It*, New York: HarperCollins.
- Crowell, R. M. (2017), "Some Principles of Cyber Warfare; Using Corbett to Understand War in the Early Twenty–First Century", *Corbett Paper*, No. 19, Available at: https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense, Accessed on: 13 December 2019.
- CSI (2015), "The Difference Between Cyberspace & The Internet", *Cyber Security Intelligence*, 22 May, Available at: https://www.cybersecurityintelligence.com/blog/the-difference-between-cyberspace-and-the-internet-2412.html, Accessed on: 26 October 2020.
- de Buen, A. T. (2016), *The Role of Cyberspace in Interstate Tensions and Conflicts*, Master Thesis, Leiden University, Leiden, Netherlands, Available at: https://openaccess.leidenuniv.nl/bitstream/handle/1887/42682/MAISThesis%20FINAL%20s1752189.pdf?sequence=1, Accessed on: 5 April 2020.
- Demertzis, M. and Wolff, G. (2019), "Hybrid and cybersecurity threats and the European Union's financial system", *Policy Contribution*, No. 10. September, Available at: https://www.bruegel.org/wp-content/uploads/2019/09/PC-10_2019.pdf, Accessed on: 5 April 2020.

−Department of Justice (2018), "Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to interfere in the United States Political System", *U.S. Department of Justice*, 16 February, Available at: https://www.justice.gov/opa/pr/grand-jury-indicts-thirteen-russian-individuals-and-three-russian-companies-scheme-interfere, Accessed on: 13 April 2020.
−Dewar, R. S. (2017), "Cyberweapons: Capability, Intent and Context in Cyberdefense", *Center for Security Studies (CSS)*, November, Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2017-06.PDF, Accessed on: 13 April 2020.
−Diuk, N. (2014), "EUROMAIDAN: Ukraine's Self-Organizing Revolution", *World Affairs* 176(6): 9-16.
−EC (2013), "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", *European Commission*, 7 February, Available at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf, Accessed on: 4 April 2020.
−EC (2018), "A Credible Enlargement Perspective for and Enhanced EU Engagement with the Western Balkans", *European Commission*, 6 February, Available at: https://ec.europa.eu/commission/sites/beta-political/files/communication-credible-enlargement-perspective-western-balkans_en.pdf, Accessed on: 4 April 2020.
−EEAS (2016), "A Global Strategy for the European Union's Foreign and Security Policy", *European External Action Service*, June, Available at: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf, Accessed on: 8 April 2020.
−EEAS (2018), "Questions and Answers about the East StratCom Task Force", *European External Action Service*, 5 December, Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/2116/-questions-and-answers-about-the-east-stratcom-task-force_en, Accessed on: 8 April 2020.
−EEAS (2019), "The European Union's Global Strategy Three Years on, Looking Forward", *European External Action Service*, Available at: https://www.bruegel.org/wp-content/uploads/2019/09/PC-10_2019.pdf, Accessed on: 5 April 2020.
−ENISA (2018), "NIS Directive", *European Network and Information Security Agency*, Available at: https://www.enisa.europa.eu/topics/nis-directive Accessed on: 3 April 2020.
−*FireEye* (2014), "APT28: A Window into Russia's Cyber Espionage Operations?", Available at: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf, Accessed on: 3 April 2020.
−Frischmann, B. M. (2003), "The Prospect of Reconciling Internet and Cyberspace", *Loyola University Chicago Law Journal*, 35(1): 205-234.

−Gambino, L. and Siddiqui, S. (2016), "Obama Expels 35 Russian Diplomats in Retaliation for US Election Hacking", *The Guardian*, 30 December, Available at: https://www.theguardian.com/us-news/2016/dec/29/barack-obama-sanctions-russia-election-hack, Accessed on: 8 April 2020.
−Gerasimov, V. (2016), "The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations", *Military Review* 96(1): 23-29.
−Gisel, L. and Olejnik, L. (2018), "The Potential Human Cost of Cyber Operations", *ICRC Expert Meeting*, 14–16 November, Geneva, Available at: https://www.icrc.org/en/download/file/97346/the-potential-human-cost-of-cyber-operations.pdf, Accessed on: 13 October 2020.
−Gompert, D. C., Cevallos, A. S. and Garafola, C. L. (2016), *War with China: Thinking Through the Unthinkable*, Santa Monica: RAND Corporation, Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1140/RAND_RR1140.pdf, Accessed on: 24 October 2020.
−Gonçalves, C. P. (2019), "Cyberspace and Artificial Intelligence: The New Face of Cyber-Enhanced Hybrid Threats", *Intech Open*, Available at: https://www.intechopen.com/online-first/cyberspace-and-artificial-intelligence-the-new-face-of-cyber-enhanced-hybrid-threats, Accessed on: 10 December 2019.
−Goure, D. (2014), "Moscow's Visions of Future War: So Many Conflict Scenarios So Little Time, Money and Forces, *Journal of Slavic Military Studies* 27(1): 63-100.
−Hastings, R. M. (2019), *Ear Factor: the Effect of Russian Political and World Views on Cyber Actions and Policy*, Master Thesis, Faculty of Utica College, Utica, New York, United States.
−Heickerö, R. (2013), *The Dark Sides of the Internet: on Cyber Threats and Information Warfare*, Frankfurt: Peter Lang.
−Herzog, S. (2011), "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses", *Journal of Strategic Security* 4(2): 49-60.
−Howe, R. (2019), *Russia's Cyber Influence Attack on the United States*, Master Thesis, Faculty of Utica College, Utica, New York, United States.
−Ivan, P. (2019), "Responding to Cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox", *European Policy Centre*, 18 March, Available at: http://aei.pitt.edu/97071/1/pub_9081_responding_cyberattacks.pdf, Accessed on: 7 April 2020.
−Kim, S., Heo, G., Zio, E., Shin, J. and Song, J. (2020), "Cyber Attack Taxonomy for Digital Environment in Nuclear Power Plants", *Nuclear Engineering and Technology*, 52(5): 995–1001, DOI: 10.1016/j.net.2019.11.001.

−Lanskoy, M. and Myles-Primakoff, D. (2018), "The Rise of Kleptocracy: Power and Plunder in Putin's Russia", *Journal of Democracy* 29(1): 76-85.
−Lewis, J. (2015), "Compelling Opponents to Our Will", In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* 39-48, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.
−Libicki, M. C. (2019), "Norms and Normalization", in C. J. Connolly (Ed.), *The Cyber Defense Review* (pp. 41-52), New York: Army Cyber Institute.
−Littlefield, S. (2009), "Citizenship, Identity and Foreign Policy: The Contradictions and Consequences of Russia's Passport Distribution in the Separatist Regions of Georgia", *Europe-Asia Studies* 61(8): 1461-1482.
−Maurer, T. (2015), "Cyber Proxies and the Crisis in Ukraine", In K. Geers (Ed.), *Cyber War in Perspective: Russian Aggression against Ukraine* (pp. 79-86), Tallinn: NATO Cooperative Cyber Defense Centre of Excellence.
−Maurer, T. (2018), "Why the Russian Government Turns a Blind Eye to Cybercriminals", *Slate*, 2 February, Available at: https://slate.com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals.html, Accessed on: 1 April 2020.
−McDermott, R. (2018), "Gerasimov Outlines Russian General Staff's Perspectives on Future Warfare", *Eurasia Daily Monitor* 15(50): 1-2.
−Miniats, M. A. (2019), "War of Nerves: Russia's Use of Cyber Warfare in Estonia, Georgia and Ukraine", *Bard College Bard Digital Commons*, No. 116, Spring, Available at: https://digitalcommons.bard.edu/cgi/viewcontent.cgi?article=1191&context=senproj_s2019, Accessed on: 1 April 2020.
−NATO (2020), "Cyber Defence", *The North Atlantic Treaty Organization*, 17 March, Available at: https://www.bruegel.org/wp-content/uploads/2019/09/PC-10_2019.pdf, Accessed on: 27 March 2020.
−Ogu, E. C., Ojesanmi, O. A., Awodele, O. and Kuyoro, S. (2019), "A Botnets Circumspection: The Current Threat Landscape, and What We Know So Far", *Information*, 10(11): 337-364.
−Perlroth, N. (2020), "U.S. Issues Sanctions on Russian Center Involved in Potentially Deadly Cyberattacks", *The New York Times*, 23 October, Available at: https://www.nytimes.com/2020/10/23/us/politics/russia-cyberattack-saudi-plant-sanctions.html, Accessed on: 24 October 2020.
−Pietkiewicz, M. (2018), "The Military Doctrine of the Russian Federation", *Polish Political Science Yearbook* 47(3): 505–520.
−Pomerantsev, P. (2014), "Russia and the Menace of Unreality: How Vladimir Putin Is Revolutionizing Information Warfare", *Business Insider*, 10 September, Available at: https://www.theatlantic.com/international/archive/2014/09/russia-putin-revolutionizing-information-warfare/379880, Accessed on: 29 March 2020.

−Rahman, M. S. (2009), "Georgia and Russia: What Caused the August War?", Identity, *Culture & Politics: An Afro-Asian Dialogue* 10(1): 132-146.
−Reuter C., Aldehoff L., Riebe T. and Kaufhold M. A. (2019, "IT in Peace, Conflict, and Security Research", In C. Reuter (Ed.), *Information Technology for Peace and Security* (pp. 11-37), Wiesbaden: Springer Vieweg.
−Rid, T. (2102). "Cyber War Will Not Take Place", *The Journal of Strategic Studies* 35(1): 5-32.
−Riley, M., Frier, S. and Baker, S. (2018), "How the Facebook-Cambridge Analytica Saga Unfolded", *Bloomberg*, 11 April, Available at: https://www.bloomberg.com/news/articles/2018-03-21/understanding-the-facebook-cambridge-analytica-story-quicktake, Accessed on: 2 April 2020.
−RNA (22 Feb 2017), "Russia's Defense Chief to Mobilize New Cyber Army", *Russian News Agency*, Available at:
https://www.bloomberg.com/news/articles/2018-03-21/understanding-the-facebook-cambridge-analytica-story-quicktake, Accessed on: 12 April 2020.
−Sambaluk, N. M. (2020), *Myths and Realities of Cyber Warfare: Conflict in the Digital Realm*, Santa Barbara: ABC-CLIO.
−Shad, M. R. (2018), "Cyber Threat in Interstate Relations: Case of US-Russia Cyber Tensions", *Policy Perspectives* 15(2): 41-55.
−Smith, D. (2019), "Paul Manafort, Trump's Ex-Campaign Chair, sentenced to 47 Months", *The Guardian*, 8 March, Available at:
https://www.theguardian.com/us-news/2019/mar/07/paul-manafort-sentencing-trump-campaign-chief, Accessed on: 8 April 2020.
−Soesanto, S. (2019), *Trend Analysis the Evolution of US Defense Strategy in Cyberspace (1988 – 2019)*, Zürich: Center for Security Studies (CSS).
−Stilgherrian (2018), "Blaming Russia for NotPetya Was Coordinated Diplomatic Action," *ZD Net*, 12 April, Available at:
https://www.zdnet.com/article/blaming-russia-for-notpetya-was-coordinated-diplomatic-action, Accessed on: 5 April 2020.
−Stone, J. (2013), "Cyber War Will Take Place!", *Journal of Strategic Studies* 36(1): 101-08.
−TDE (2020), "CyberSecurity Report 2019 H2", *Telefonica Digital Espana, S.L.*, Available at:
https://www.elevenpaths.com/wp-content/uploads/2020/01/cybersecurity-report-19h2-EN.pdf, Accessed on: 1 May 2020.
−Thomas, T. (2014), "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?", *Journal of Slavic Military Studies* 27(1): 101-130.
−Volz, D. and Gardner, T. (2018), "In a First, U.S. Blames Russia for Cyber Attacks on Energy Grid", *Reuters*, 15 March, Available at:

https://www.reuters.com/article/us-usa-russia-sanctions-energygrid-idUSKCN1GR2G3, Accessed on: 24 October 2020.
- *Washington Post* (23 June 2017), "Obama's Secret Struggle to Punish Russia for Putin's Election Assault", Available at: https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.9b66faf523b4, Accessed on: 27 March 2020.
- Wheeler, T. (2018), "In Cyberwar, There Are No Rules; Why the World Desperately Needs Digital Geneva Conventions", *Foreign Policy*, 12(Fall), Available at: https://foreignpolicy.com/2018/09/12/in-cyberwar-there-are-no-rules-cybersecurity-war-defense, Accessed on: 10 December 2019.