تحلیل روش و اهداف سیاسی مداخله سایبری عناصر منسوب به روسیه در انتخابات ریاست جمهوری۲۰۱۶ آمریکا

سعیده مرادی فر
دانشجوی دکتری روابط بین الملل دانشگاه اصفهان، اصفهان، ایران
علی امیدی[۱]
دانشیار روابط بین الملل، گروه علوم سیاسی، دانشگاه اصفهان، اصفهان، ایران
(تاریخ دریافت ۹۷/۱۰/۱۳- تاریخ تصویب ۹۸/۵/۵)

چکیده

با استناد به شواهدی که برخی منابع آمریکایی ارائه می‌کنند روسیه با تکیه بر توان سایبری و عملیاتی از پیش طراحی شده توانست بر انتخابات ریاست جمهوری ۲۰۱۶ آمریکا اثرگذار باشد و با بکارگیری تکنولوژی‌های فضای سایبری، اهداف سیاسی خود را در زمانی که به آن عصر پساحقیقت می‌گویند تعقیب نماید. از اینرو پرسش اصلی مقاله حاضر آن است که روسیه چگونه در انتخابات ۲۰۱۶ ریاست جمهوری آمریکا مداخله کرده و اساسا هدف روسیه از این مداخله چیست؟ فرضیه مقاله که به روش توصیفی – تحلیلی بررسی شده این است که از نظر کارشناسان و نهادهای اطلاعاتی آمریکا، عناصری در روسیه با بکارگیری فناوری‌های فضای مجازی نظیر رسانه‌های اجتماعی، ربات‌ها و ترول‌ها و با نشر اخبار جعلی و اطلاعات گزینشی بر روند انتخابات ریاست جمهوری آمریکا اثرگذار بوده و فرصت پیروزی هیلاری کلینتون را کاهش و شانس ترامپ را افزایش داده، که این مهم به نوبه خود موجب تضعیف اعتماد مردم به نهادهای سیاسی آمریکا و همچنین تشدید رقابت مسکو-واشنگتن شده است. هر چند روسیه رسما و مکررا چنین مداخله‌ای را از سوی منابع دولتی تکذیب کرده؛ ولی نگارندگان با توجه به شواهد ارائه شده از «جامعه اطلاعاتی آمریکا» و «مدیر اطلاعات ملی آمریکا» در ۲۰۱۶ و همچنین «گزارش رسمی رابرت مولر» در سال ۲۰۱۹ که در آن ۲۶ شخص و سه نهاد روس را متهم به مداخله سایبری کرد فرض بر مداخله عناصری از خاک روسیه (نه ضرورتا دولت روسیه) در انتخابات مزبور می‌گذارند. این مقاله، چگونگی و پیامدهای این مداخله را می‌کاود.

واژه‌های کلیدی: پسا حقیقت، رسانه‌های اجتماعی، جنگ اطلاعاتی، نفوذ سایبری.

---

[۱] نویسنده مسئول Email: aliomidi@ase.ui.ac.ir
فصلنامه مطالعات روابط بین الملل، سال دوازدهم، شماره ۴۷، پاییز ۱۳۹۸، صص. ۹ - ۳۷.

۱. مقدمه

امروزه اخبار جعلی الزاماً به معنای خبرهای دروغ و افتراآمیز نیست بلکه اغلب به معنی اخباری است که اعتقادات پیشینی اشخاص را مورد حمله قرار می‌دهد و اعتقادات دیگری را جایگزین آن می‌کند. این ویژگی جهان معاصر را عصر «پساحقیقت» می‌نامند (Rochlin, 2017). پساحقیقت[1] واژه‌ای است که در سال ۲۰۱۶ توسط واژه‌نامه آکسفورد بکار برده‌شده (Oxford Dictionaries,2017) و دو عامل در بکارگیری این واژه تأثیر بسزایی داشته‌است. یکی برگزاری رفراندم در بریتانیا برای خروج این کشور از اتحادیه اروپا (برگزیت) و دیگری انتخابات ریاست جمهوری آمریکا در سال ۲۰۱۶. در هر دو مورد اخبار و اطلاعات جعلی بشدت بر افکار عمومی اثرگذار بوده‌است. از آنجا که هر مفهومی که کشف می‌شود کارویژه خاص خود را دارد اصطلاح پساحقیقت نیز از این امر مستثنی نبوده و برای توصیف اثرگذاری اخبار جعلی بر افکار عمومی بکار می‌رود. هاتچینگز نیز به تاسی از فرهنگ آکسفورد معتقد است پساحقیقت می‌تواند برای توصیف رفتار اطلاع‌رسانی نادرست و کذب عمدی بویژه در «جنگ اطلاعاتی» بعنوان یکی از اجزای جنگ نرم مورد استفاده قرار گیرد (Hutchings, 2017: 2).

توجه به این نوع جنگ در جنگ سرد مجازی، در اعتراضات خیابانی ۱۲-۲۰۱۱ روسیه، با بسیج مردم بوسیله فضای مجازی (شبکه‌های اجتماعی) بوضوح دیده شده‌است. رهبران معترضان همچون ناولنی[2] از انواع مختلفی از شبکه‌های اجتماعی (توئیتر، فیس‌بوک) برای تحریک اهالی مسکو برای شرکت در تجمعات استفاده‌کردند (Park, 2014: 498). در واقع تصمیم پوتین در سال ۲۰۱۱ برای شروع دوره سوم ریاست جمهوری روسیه موجب بروز جنبشی اعتراضی گسترده‌ای علیه وی شد. هزاران نفر از تظاهرکنندگان خواستار استعفای وی در سراسر کشور شدند. برخی از نزدیک‌ترین متحدان وی با الحاق به اپوزیسیون موجب بروز شکاف بین نخبگان کرملین شدند. پوتین بر این باور بوده که

1. Post-truth
2. Navalny

کلینتون (وزیرامورخارجه وقت آمریکا) علایمی را برای بازیگران خاصی (مخالفین پوتین) در روسیه ارسال کرده و و برخی از اعتراضات علیه سیاست‌های پوتین در داخل شوروی به تحریک عناصر حزب دمکرات آمریکا، خصوصاً خانم کلینتون، صورت گرفت. لذا از دیدگاه پوتین این حمایت، «سناریوی از پیش طراحی شده» بود که سبب تحریک بی‌ثباتی و تضعیف روسیه می‌شد (Nation, 2012: 381). این امر موجب بروز استراتژی ضد آمریکایی بعنوان یکی از مهم‌ترین اقدامات پوتین در واکنش به ظهور جنبش اعتراضی مخالف غیرمنتظره پس از انتخابات دوما در دسامبر ۲۰۱۱ شد (Stent, 2012: 123).

اساساً با توجه به شکاف صورت گرفته بین مسکو-واشنگتن در دوره اوباما بر سر مسئله اکراین، آشتی دو کشور با ادامه حاکمیت این حزب امکان پذیر نمی‌باشد؛ خصوصاً اینکه ترامپ در اثنای رقابت‌های انتخاباتی شخصیت پوتین را می‌ستود. برای گریز از سناریویی که در آن وزیر امورخارجه (هیلاری کلینتون) به رئیس جمهور آمریکا تبدیل شود، تحلیلگران آمریکایی معتقدند تلاش مسکو این بوده که یکپارچگی آمریکا را با نفوذ در رای‌دهندگان تغییر دهد (Shuya, 2018: 10). لذا از این منظر، روسیه بدنبال اثرگذاری بر مخاطبان آمریکایی خود از طریق نشر اطلاعات غلط، دستکاری شده و استفاده از بدافزارها (Zakem et al, 2017: 17)، برای اثرگذاری بر انتخابات ریاست جمهوری ۲۰۱۶ آمریکا بود. از نظر تحلیگران آمریکایی، این اقدام روسیه در بهره‌گیری از فضای مجازی برای اثرگذاری بر تحولات سیاسی سایر کشورها نه تنها نمایانگر سرمایه‌گذاری زیاد روسیه روی اینترنت و فضای مجازی بعنوان بخشی از قدرت بوده (Peters, 2017: 2)، بلکه پاسخی برای رفتارهای مشابه غرب (Zakem et al, 2017: 17) در جنگ سرد دیجیتال بوده است. اما مسکو چنین تحلیل‌ها و ادعاهایی را مردود می‌داند و معتقد است اگر هکرهایی از خاک روسیه انتخابات آمریکا را هدف قرار دادند آنها بر اساس علایق شخصی خود این کار را انجام دادند؛ نه اینکه از سوی مسکو برای این کار اجیر شده باشند. به نظر پوتین، حتی افراد ادعایی گزارش رابرت مولر در سال ۲۰۱۹ مبنی بر مشارکت ۲۶ فرد روسی و سه سازمان در مداخله سایبری انتخابات ریاست جمهوری ۲۰۱۶ آمریکا، ممکن است توسط عناصری از

حاکمیت آمریکا استخدام شده بودند تا از بهبودی روابط دو کشور جلوگیری کنند. پوتین این مزدوران سایبری را اکراینی و تاتار یا یهودی می‌داند، نه روس (Smith, 2019)

بر این اساس، ظرف سه سال گذشته (۲۰۱۶-۲۰۱۹)، این گمانه در آمریکا قوت گرفته است که روسیه هزاران نفر را برای ایجاد و عرضه اخبار جعلی ضد کلینتون بکار گرفته‌بود که عمده‌ترین هدف آن جلوگیری از پیروزی کلینتون از یک سو و از کار انداختن و بی‌اعتبار ساختن نهادهای دموکراتیک در آمریکا از دیگر سو بود. اعتقاد بر این است که هکرهای روسی مسئولیت نشت و افشاء ایمیل‌های مقامات حزب دموکراتیک را بر عهده داشتند (Vasu et al, 2018: 8). ارتش گسترده هکرهای تحت کنترل روسیه در فضای مجازی (رسانه‌های اجتماعی) با بکارگیری مجموعه‌ای عظیم از ربات‌ها و ترول‌ها، اخبار جعلی را در داخل و خارج روسیه نشر دادند (Woolley, 2016) و با این شیوه توانستند روندهای محبوبیت‌های افراد و گفتگوهای اجتماعی را در انتخابات مهندسی کنند (Ludes & Jacobson, 2017: 3).

این در حالی است که دولت آمریکا، نهادها و دستگاه‌های امنیتی و اطلاعاتیِ آن که خود سال‌ها پیشرو و بانی حملات سایبری و خرابکاری الکترونیکی در کشورهای دوست و دشمن در اقصی نقاط جهان بوده‌اند؛ اکنون مدعی هستند که حملات در فضای مجازی با اهداف سخت (خرابکاری) و نرم (دستکاری افکار عمومی) اکثراً تحت حمایت بازیگران دولتی، عمدتاً توسط کشورهایی همچون روسیه، چین و ایران راه‌اندازی می‌شوند (Mazzetti & Sanger, 2013). با توجه به این واقعیات، پرسش اصلی این مقاله آن است که عناصر سایبری روس چگونه در انتخابات ۲۰۱۶ ریاست جمهوری آمریکا مداخله کرده و اساساً هدف از این مداخله چه بود؟ فرضیه مقاله که به روش توصیفی – تحلیلی بررسی شده آن است که عناصری از روسیه با بکارگیری فضای مجازی، نظیر رسانه‌های اجتماعی، ربات‌ها و ترول‌ها با نشر اخبار جعلی و اطلاعات گزینشی برروند انتخابات ریاست جمهوری آمریکا اثرگذار بوده و فرصت پیروزی کلینتون را کاهش و شانس ترامپ را افزایش داده، که این مهم به نوبه خود موجب تضعیف اعتماد مردم به نهادهای سیاسی آمریکا و همچنین تشدید

رقابت مسکو-واشنگتن شده است. مقاله حاضر در سه محور اصلی سازماندهی شده‌است. نگارندگان در ابتدا به تحلیل تئوریک مفهوم جنگ اطلاعاتی و نفوذ سایبری پرداخته‌اند و در ادامه به ابعاد و شواهد فنی نفوذ سایبری عناصر منسوب به روسیه در انتخابات ۲۰۱۶ آمریکا مبادرت ورزیده‌اند. در پایان نیز هدف اصلی نفوذ سایبری منسوب به مسکو از جهت سیاسی تحلیل شده است.

۲. نبرد سایبری[1] و جنگ اطلاعاتی[2]

نبرد سایبری یا اطلاعاتی محصول عصر اطلاعات است که در آن تاکید بسیاری بر روی فناوری‌های اطلاعاتی و اطلاعات به عنوان تسلیحات شده است (Mulvenon, 1999: 180). اطلاعات در این نوع نبرد در حکم قلمرو، سلاح و هدف بشمار می‌رود (Wilson, 2004:2). نبرد اطلاعاتی توسط جوامع و ارتش‌های پیشرفته توسعه می‌یابد. تسلیحات این نوع نبرد تنها می‌تواند در برابر دشمنی مورد استفاده قرار گیرد که دارای قابلیت‌های پیشرفته مشابهی باشد (Haeni, 1997: 3).

این نوع نبرد نسبتاً جدید بوده و اصطلاح نبرد اطلاعاتی دارای معانی مختلفی نیز بوده‌است (Haeni, 1997: 4). لذا می‌توان شاهد فقدان وجود تعریف رسمی برای تبیین مفهوم نبرد اطلاعاتی بود. این امر در حالی است که نبرد اطلاعاتی بطور معمول بعنوان بکارگیری و مدیریت اطلاعات برای پیگیری مزیت‌های رقابتی، از جمله تلاش‌های تدافعی و تهاجمی مفهوم‌سازی می‌شود (Theohary, 2018: 1). بنابراین این نبرد نه تنها دارای بعد نظامی بوده بلکه برای توصیف «جنگ» در اینترنت مورد استفاده قرار می‌گیرد (Haeni, 1997: 4). در ابتدا اصطلاح نبرد اطلاعاتی تنها براساس استفاده از فناوری‌های اطلاعاتی و ارتباطی برای شکست زیرساخت‌های اطلاعاتی بمنظور اخلال در آنها یا دستیابی به اطلاعات و اطلاعات مرتبط به منابع حریف، استراتژی نظامی و.... تعریف می‌شده است

1. Cyber Warfare
2. Information Warfare

(Taddeo, 2011:109). هاینی بر این باور بوده که نبرد اطلاعاتی اقدامات صورت گرفته‌ای است که برای دستیابی به برتری اطلاعاتی همراه با اثرگذاری بر اطلاعات دشمن، فرایندهای مبتنی بر اطلاعات، سیستم‌های اطلاعاتی و شبکه‌های مبتنی بر کامپیوتر می‌باشد و در عین حال دفاع از اطلاعات خود، پشتیبانی و دفاع از فرایندهای مبتنی بر اطلاعات سیستم‌های اطلاعاتی و شبکه‌های کامپیوتری خودی است (Haeni, 1997: 4). در واقع نبرد اطلاعاتی کاربرد فناوری‌های اطلاعاتی و ارتباطی در یک استراتژی نظامی تهاجمی و تدافعی است. این نبرد با تأیید دولت‌ها به راه انداخته می‌شود و هدف از آن فروپاشی یا کنترل فوری منابع دشمن است که در محیط اطلاعاتی با عوامل و اهدافی در هر دو حوزه فیزیکی و غیرفیزیکی و با سطوح مختلف خشونتی آغاز می‌شود (Taddeo, 2011: 114).

نبرد اطلاعاتی یک حمله مبتنی بر اطلاعات است که شامل هرگونه تلاش غیرمجاز در کپی کردن اطلاعات و یا تغییر در اطلاعات و دستورالعمل‌های مرتبط به آن است. نبرد اطلاعاتی فراتر از محدوده کامپیوترها و شبکه‌های کامپیوتری است. این نبرد شامل عملیات‌های هدایت شده درباره اطلاعات به هر شکل ممکن و از طریق هر رسانه‌ای است؛ که می‌توان شاهد عملیات‌هایی بوده که بر ضد محتوای اطلاعاتی، سیستم‌های پشیبانی‌کننده و نرم‌افزارهای آن، دستگاه‌های سخت افزاری مخصوص ذخیره اطلاعات و دستورالعمل‌ها و همچنین شیوه‌ها و ادراکات انسانی انجام می‌شود (Wilson, 2004: 2).

دولت‌های رقیب و دشمن و حتی افراد حقیقی تلاش می‌کنند از طریق بکارگیری ابزارهای مختلف از جمله استخدام ترول‌ها، هکرها و دستکاری در محتوای تولید شده در فضای مجازی (از جمله رسانه‌های اجتماعی) توان بازدارندگی خود را افزایش دهند. دولت‌ها طیف مختلفی از اقدامات از جمله جلوگیری از دسترسی به رسانه‌های اجتماعی، شایعه پراکنی در رسانه‌های اجتماعی و نیز تحمیل برداشت خود را برای اعمال قدرت خود در فضای مجازی بکار می‌گیرند (Jaitner, 2012: 17). در این میان، حملات سایبری به گزینه قدرتمندی در جنگ تبدیل شده‌است و رقابت در فضای مجازی همانند فضای واقعی بین دولت‌ها در جریان می‌باشد. یکی از مهم‌ترین نمودهای این امر رقابت بین دو قدرت

بزرگ، آمریکا و روسیه برای استفاده از فضای مجازی جهت اثرگذاری بر رویدادها و تحولات داخلی یکدیگر و دستیابی به نتایج دلخواه است. لذا می‌توان اینگونه بیان کرد که هک کردن سیستم‌های اطلاعاتی، نشر اخبار جعلی و ترندسازی در رسانه‌های اجتماعی، استفاده از ترول و ربات از اهمیت ویژه‌ای در رقابت برخوردارند. (Nagy, 2012: 25). موارد ذیل ازجمله بسترهای لازم مداخلاتی عناصر منسوب به روسیه در انتخابات ۲۰۱۶ بشمار می‌روند که نگارندگان به تشریح مختصری از این مباحث پرداخته‌اند:

۱. هک کردن سیستم‌های اطلاعاتی به معنای حمله برای ایجاد وقفه کامل در تناوب خاموشی سیستم‌ها، ایجاد خطای داده‌های تصادفی، سرقت اطلاعات، سرقت خدمات، نظارت بر سیستم‌های غیرقانونی (جمع‌آوری اطلاعات)، تزریق ترافیک پیام نادرست و دسترسی به اطلاعات می‌باشد (Libicki, 1995: 49-50).

۲. خدماتی که در پرتو وب ۲[۱] حاصل شده امکان تعاملات اجتماعی از طریق رسانه‌ها را افزایش داده و آنچه اصطلاحاً «رسانه‌های اجتماعی» خوانده می‌شود به معنی واقعی کلمه تحقق پیداکرد. رسانه‌های اجتماعی اشکال مختلفی دارد؛ از جمله مجلات، انجمن‌های اینترنتی، وبلاگ‌ها، وبلاگ‌های اجتماعی، میکروبلاگینگ، ویکی‌ها، پادکست‌ها، سایت‌های اشتراک‌گذاری تصاویر و ویدئو و شبکه‌های اجتماعی. رسانه‌های اجتماعی نقش مهمی در ترویج ایده‌ها و اندیشه‌ها، از جمله در زمینه سیاست‌های داخلی و خارجی ایفا می‌کنند. بازیگران سیاسی و دولت‌ها در سراسر جهان، از رسانه‌های اجتماعی برای شکل دادن به زندگی عمومی مردم بهره می‌گیرند (Baruah, 2012: 1).

۳. یکی از اقداماتی که از طریق رسانه‌های اجتماعی می‌توان آنرا اعمال کرده و بر تحولات سیاسی کشورها از جمله انتخابات اثرگذار بود، اخبار جعلی است. اخبار جعلی به این صورت تعریف می‌شود: داستان و سرتیترهایی که به صورت آگاهانه نوشته شده و در

---

[۱].اصطلاح وب ۲ در سال ۲۰۰۴ برای توصیف مجموعه‌ای از خدمات نوینی معرفی شد که تغییر تدریجی خدمات موجود در وب ۱ را توضیح می‌داد. وب ۲ برخلاف وب ۱ از جریان اطلاعات دوطرفه و محتوای تولید شده توسط کاربر حمایت می‌کند (Khan, 2017: 2).

وبسایت‌هایی که بنظر می‌رسد برای انتشار اخبار واقعی طراحی شده‌اند، منتشر می‌شود و از طریق رسانه‌های اجتماعی گسترش می‌یابد. هدف این نوع اخبار آن است که تا حد امکان تعداد قابل توجهی از مردم را وادار کنند که این گونه اخبار را در فضای مجازی لایک کرده و به اشتراک بگذارند، به این دلیل که کلیک بیشتر برای دریافت لینک به معنی دستیابی به پول بیشتر از طریق تبلیغات است. محرک اصلی که انتشار دهندگان اخبار جعلی را ترغیب می‌کند این است که تعداد زیادی از مردم فقط عناوین و سرتیترهای مقاله را می‌خوانند (Rochlin, 2017: 388). آنچه گفته شد یک تعریف موسع از اخبار جعلی است. تعریف مضیق اخبار جعلی عبارت است از اخباری که عمداً دروغ و نادرست است و می‌تواند خوانندگان را گمراه کند. در این تعریف دو ویژگی کلیدی وجود دارد: اصالت و نیت. اولاً، اخبار جعلی شامل اطلاعات غلط است که می‌تواند تا جایی که ممکن است متنوع باشد. ثانیاً، اخبار جعلی با نیت بد برای گمراه کردن مصرف‌کنندگان ایجاد شده‌است (Shu et al, 2017: 2).

۴. استفاده از ربات‌ها در کمپین‌های سیاسی به اواسط سال ۲۰۰۰ باز می‌گردد؛ زمانی که در آمریکا از ربات‌ها برای پیوند نام سیاستمداران با داستان‌های خارق‌العاده درباره آنها استفاده می‌شد. با این وجود تنها در سال‌های اخیر بود که دامنه و پیچیدگی فعالیت‌های ربات‌ها در رسانه‌های اجتماعی نظیر توئیتر افزایش یافته است تا حدی که این ربات‌ها توجه بسیاری از بازیگران سیاسی و دولتی را به خود جلب کرده‌است (Stukal et al, 2017: 311). با در نظر داشت این موضوع می‌توان اینگونه ربات را تشریح کرد؛ ربات یا عامل نرم افزاری، برنامه کامپیوتری است که پایدار، مستقل و واکنش‌پذیر است. ربات‌ها توسط برنامه کدنویسی تعریف می‌شود که بطور مداوم اجرا می‌شود و می‌تواند توسط خودش فعال شود. آن‌ها تصمیمات را بدون دخالت و درک انسانی می‌گیرند و به اجرا در می‌آورند و با بستر و زمینه‌ای که در آن کار می‌کنند، سازگار می‌شوند. ربات‌های اینترنتی، همچنین به عنوان ربات‌های شبکه شناخته می‌شوند؛ ربات‌هایی که در اینترنت راه‌اندازی می‌شوند. آن‌ها بلافاصله بعد از ایجاد و گسترش شبکه جهانی وب ظاهر شدند. انواع مختلفی از ربات‌های

اینترنتی وجود دارد که سیستم پیچیده تعاملات اجتماعی را تشکیل می‌دهند(Tsvetkova et al, 2017: 2).

۵. یکی دیگر از موضوعات پراهمیت در نبرد سایبری بکارگیری ترول‌ها است. ترول‌ها افرادی هستند که به عمد و با هدف ایجاد حداکثر اختلاف، پیام‌های تحریک‌آمیزی را به گفتگوهای جمعی از جمله گروه‌های خبری یا گفتگوهای آنلاین ارسال می‌کنند. ترول کردن شامل اقداماتی از جمله شلعه‌ور ساختن، تهمت زدن یا حملات شخصی، تجلیل از افراد در قالب شوخی و سرگرم کردن جمع یا خارج کردن برخی از افراد از بحث است که عمدتاً خارج از مرزها و با حد و حدودهای پذیرفته شده‌است (Cheng et al, 2017: 12-18).

۳. ابعاد فنی و شواهد موید دخالت عناصر منسوب به روسیه در انتخابات ریاست جمهوری آمریکا

منابع آمریکایی ادعا دارند که عناصر منسوب به روسیه با بسیج و بهره‌برداری رسانه‌های جدید و قدیم از طریق عملیات اطلاعاتی، همواره در پی دستیابی به اهداف سیاست خارجی خود بوده است. از نظر این منابع، در واقع کرملین اطلاعات را به عنوان «سلاح» در نظر گرفته و رسانه را همواره به عنوان سلاحی فریبنده/پرت‌کننده جمعی حواس و ابزار غیررسمی در گسترش ارتش و دیپلماسی خود بکار گرفته است. ریشه این استراتژی به دوران اتحادجماهیرشوروی باز می‌گردد؛ زمانیکه شوروی روش‌هایی نظیر «کنترل انعکاسی» و «اقدامات فعال» را برای گمراهی، دستکاری اطلاعات و ترساندن مخالفان خود در غرب استفاده می‌کرد. اما اثربخشی این روش‌ها در طول جنگ سرد محدود بود. با این وجود، ظهور اینترنت و رسانه‌های اجتماعی فرصت‌های نوین قابل توجهی را برای جنگ اطلاعاتی کرملین ایجاد کرده‌است. هدف مسکو در بکارگیری اطلاعات و فضای سایبر، بعنوان عناصر حیاتی امنیت ملی در تعدادی از اسناد اخیر نظیر دکترین نظامی ۲۰۱۴، دکترین امنیت اطلاعاتی ۲۰۱۵ و استراتژی امنیت ملی ۲۰۱۵ مطرح شده‌است (Cordy, 2017: 8).

بعنوان مثال در استراتژی امنیت ملی روسیه تا سال ۲۰۲۰، امنیت اطلاعات بعنوان جزء کلیدی امنیت ملی در نظر گرفته شده‌است (Zinovyeva, 2013: 39). در این اسناد روسیه به عنوان قربانی «تهاجم اطلاعاتی» غرب به تصویر کشیده‌است و بر ضرورت مقابله با تهدیدات اطلاعاتی برای حمایت حاکمیت و امنیت روسیه و توسعه ابزاری مؤثر برای نفوذ در افکار عمومی خارج از کشور تاکید دارد (Cordy, 2017: 8). کارشناسان آمریکایی مدعی‌اند که روسیه از ابزارهای سایبری، هک، ترول، ربات و رسانه‌های اجتماعی برای پیشبرد مؤثر کار خود استفاده کرده‌است. به نظر آنها، در حال حاضر هکرهای روسی با بکارگیری ابزارهای تبلیغاتی بروزرسانی شده، بواسطه رسانه‌های دولتی (نظیر راشاتودی، اسپوتنیک، ارتش حساب‌های رسانه‌ای جعلی) که بصورت خودکار عمل می‌کند، بر روند انتخابات در آمریکا، اسپانیا، انگلیس و سایر نقاط اروپا اثرگذار بوده‌است (Dorell, 2018).

از دید کارشناسان آمریکایی، انتخابات ۲۰۱۶ آمریکا را می‌توان نمونه‌ای کامل از نفوذ سایبری روسیه قلمداد کرد. از نظر آنها، روسیه مدت‌هاست که ترکیبی از تاکتیک‌های پنهان و آشکاری را برای پیشبرد اهداف خود بکار می‌برد اما حوزه و صراحت اقداماتش در انتخابات آمریکا بی‌سابقه بود (Treverton & Chen, 2017: 2). حتی برخی ناظران آمریکایی ادعا دارند که «روس‌ها دوباره در سال ۲۰۲۰ باز خواهند گشت، روس‌ها هرگز این فضا را ترک نخواهند کرد. شواهد نشان می‌دهد که مداخله آنها در زندگی سیاسی آمریکایی‌ها هر روز درحال افزایش است»(Ludes & Jacobson, 2017: 14).

منابع آمریکایی، شیوه‌های نفوذ سایبری منسوب به روسیه را بصورت زیر ارزیابی کرده‌اند:

۳-۱. هک و نشر اطلاعات

در سال ۲۰۱۵ و ۲۰۱۶ کمیته ملی دموکراتیک، کمیته کمپین کنگره دموکراتیک و کمپین هیلاری کلینتون، همه توسط عملیات جاسوسی سایبری تحت حمایت کرملین مورد حمله قرارگرفتند (Baezner & Patrice ,2017 :4, Treverton & Chen, 2017:

4, Ferguson, 2018: 12). روسیه از گروه‌های مختلف جاسوسی برای هک رایانه‌ها و سیستم‌های ایمیل در انتخابات ۲۰۱۶ آمریکا استفاده کرد. علاوه براین، تیم‌های جاسوسی سایبری روسی توانسته‌اند به اطلاعاتی در رایانه‌ها و سایر سیستم‌ها دست یابند که برخی از اطلاعات و ایمیل‌ها از طریق دسترسی غیرمجاز کشف و بعداً منتشر شد (Van De Velde, 2017: 11).

دو گروه از هکرهای وابسته به دولت روسیه که تحت عنوان کوزی‌بر و فانسی‌بر[1] از آنها یاد می‌شود، در انتخابات آمریکا از همان روش عملیاتی استفاده کردند که قبلاً علیه سایر سازمان‌ها و دولت‌های خارجی بکار گرفته‌بودند. اسناد و اطلاعات به سرقت رفته از این شبکه‌ها در ابتدا، از طریق اشخاص و وبسایت‌های ایجاد شده توسط دولت روسیه (نظیر دی. سی.لیکس، گوسیفر ۲)[2] و سپس از طریق ویکی‌لیکس و سایر رسانه‌های جریان اصلی منتشر شد. همچنین سرویس اطلاعاتی روسیه از ژوئن ۲۰۱۵ تا اواخر ژوئن ۲۰۱۶ به شبکه کمیته ملی دموکراتیک دسترسی پیدا کرد (Treverton & Chen, 2017: 4).

کوزی‌بر با نام APT29 شناخته می‌شود و اولین گروه برای دسترسی به شبکه کمیته ملی دموکراتیک در ژوئن ۲۰۱۵ بود. نفوذ در شبکه، از طریق ایمیل‌های فیشینگ بود که معمولاً شامل لینک‌های وب یا پیوست‌های مخرب بوده که یک بدافزار مخرب را نصب می‌کردند. در مطالعه کمیته ملی دموکراتیک، کوزی‌بر از بدافزاری[3] استفاده کرده که یک نرم‌افزار مخرب بسیار قابل تنظیم و رمزگذاری شده بود. این بدافزار به هکرها اجازه می‌داد به اطلاعات شبکه‌های خارجی و کانال‌های ارتباطی درون آن نظارت کنند (Treverton & Chen, 2017: 4).

فانسی‌بر نیز با نام APT28 شناخته می‌شود. این گروه بطور موفقیت‌آمیزی شبکه کمیته ملی دموکراتیک را در آوریل ۲۰۱۶ هک کرد و پس از آن پرونده‌های مخالفت درباره

1. CozyBear & FancyBear
2. Guccifer 2.0, DCLeaks.com
3. SeaDaddy

ترامپ را سرقت کرد و به سرعت حذف کرد. فانسی‌بر علاوه بر ایمیل‌های فیشینگ همانند کوزی‌بر اقدام به سرقت اطلاعات کاربران نمود. همچنین این گروه، نرم‌افزار مخربی بکار گرفت که اجازه دستورات از راه دور، انتقال فایل‌ها، کلید زدن از راه دور و امکان دسترسی آسان به کلمه عبور را می‌داد، که این امر سبب به مخاطره افتادن رایانه‌های کاربران می‌شد. این بدافزار پیکربندی شده قابلیت اجرا روی هر دو سیستم عامل رایانه‌ها و گوشی‌های همراه را دارا بود (Treverton & Chen, 2017: 4).

این تکنیک‌ها، قابلیت دسترسی به شبکه‌های رایانه‌ای قربانیان و دستیابی به اطلاعات حساس از راه دور را به گروه‌های هکری داد (Baezner & Patrice, 2017: 4). روسیه برخی از ایمیل‌های هک شده را بصورت گزینشی منتشر کرد. مقامات اطلاعاتی روسیه، ایمیل‌ها و اسناد خصوصی بدست آمده از هک را در ژوئیه ۲۰۱۶ از طریق ویکی‌لیکس، دی. سی.لیکس، گوسیفر ۲ و سایر وبسایت‌ها منتشر کردند. انتشار اطلاعات بطور قابل توجهی روی مبارزات کنگره و بطور کلی اعتماد شهروندان در روند دموکراتیک تأثیر بسزایی داشت. عواقب انتشار ایمیل‌های کمیته ملی دموکراتیک فوری بود؛ چراکه دبی واسرمن شولتز، ریس کمیته ملی دموکراتیک مجبور به استعفا شد (Van De Velde, 2017: 11).

۳-۲. بکارگیری ربات‌ها و ترول‌ها برای اخبار جعلی

تاکتیک اصلی عناصر منسوب به روسیه، نفوذ در رسانه‌های اجتماعی و بکارگیری روایت‌های نادرست در باره کلینتون بود (Journell, 2017: 14). از اینرو عناصر مزبور گروه‌هایی از ترول‌ها را در رسانه‌های اجتماعی به عنوان بخشی از استراتژی برای نفوذ در افکار عمومی بکار گرفت (Sides et al, 2017: 71). برخی محققان استدلال کرده‌اند که گروهای فیسبوکی جعلی را پیدا کرده‌اند که تقریباً تمام اعضای این گروه‌ها از ربات‌ها تشکیل شده‌است. این گروه‌های جعلی که بطور قانع کننده‌ای عمل می‌کردند، هماهنگ بودند و در نهایت طرفداران واقعی را جذب می‌کردند. ممکن است یکی از دلایلی که بسیاری از طرفداران ترامپ را جسور کرد تا بطور آشکار حمایت خود را از وی اعلام کنند

ناشی از این ادراک مصنوعی ایجاد شده به وسیله این گروه‌های جعلی باشد. به این ترتیب برخی از این صفحه‌های اصلی جعلی یا گروهای متشکل از افراد واقعی اثرگذاری خود را انجام داده‌اند (Vasu et al, 2018: 9-10).استوکال و همکاران در پژوهش خود دریافتند که شایع‌ترین نوع ربات، رباتی است که تیتر خبرها را بدون لینک دادن به منبع اصلی خبرها توئیت و منتشر می‌کند. این موضوع نشان می‌دهد که بکارگیری ربات‌ها برای اهداف تبلیغاتی یک استراتژی مهم است؛ چراکه ممکن است از این ربات‌ها برای تبلیغ داستان‌های خبری خاص و رسانه‌های خبری در رتبه‌بندی موتورهای جستجو استفاده شود. اگرچه بسیاری از ربات‌ها اطلاعاتی را منتشر می‌کنند، اما ممکن است ربات‌های ضدرژیمی نیز وجود داشته‌باشد که اطلاعات مربوط به فعالیت‌های مخالفین یا انتقاد و رد رژیم را منتشرکنند (Stukal et al, 2017: 319).

ربات‌های رسانه‌های اجتماعی در طول انتخابات ریاست جمهوری ۲۰۱۶ آمریکا در مقیاس بسیار گسترده‌ای بحث‌ها و گفتگوهای آنلاین را دچار تحریف کردند و حدود ۱۹ میلیون حساب رباتی در حمایت از ترامپ یا کلینتون در هفته قبل از روز انتخابات در فضای توئیتر، توئیت کردند. همچنین ترول‌ها نقش قابل توجهی را در گسترش اخبار جعلی در رسانه‌های اجتماعی ایفا می‌کنند. همانگونه که گفته شد ترول‌ها، کاربران به ظاهر انسان واقعی هستند که هدف آنها نابودی ارتباطات و مجموعه‌های آنلاین، متقاعدسازی کاربران برای ورود به یک فضای احساسی و اتخاذ یک پاسخ احساسی است. شواهد نشان می‌دهد که ۱۰۰۰ نفر از این ترول‌ها توسط عناصر منسوب به روسیه اجیر شده‌بودند تا اخبار جعلی را عیله کلینتون تولید کنند، سیاهپوستان را از رأی دادن منصرف کنند و محافظه‌کاران را به طرفداری از ترامپ وا دارند. رفتارهای ترول‌ها به شدت بر خلق‌وخوی مردم و همچنین زمینه‌های بحث آنلاین تأثیر می‌گذارد. این امر زمینه‌های انتشار آسان اخبار جعلی در میان گروه‌ها و مجموعه‌های آنلاین را فراهم می‌کند. اثرات ترول‌ها احساسات منفی درونی افراد از جمله عصبانیت و ترس را مورد هدف قرار می‌دهد و منجر به شک، بی‌اعتمادی و رفتارهای غیرعقلانی می‌شود (Shu et al, 2017: 25)

پس از حدس و گمان‌ها در مورد دخالت عناصر منسوب به روسیه در انتخابات آمریکا، توئیتر فهرستی از ۲۷۵۲ حساب کاربری را منتشر کرد که تلاش‌های تبلیغاتی روسیه برای اثرگذاری در انتخابات آمریکا را تأیید می‌کرد. توئیتر مشخص نکرد که این حساب‌های کاربری به چه صورتی شناسایی شدند اما استدلال می‌کند که آنها وابسته به آژانس تحقیقاتی اینترنتی روسیه[1] هستند. این آژانس یک نهاد شناخته شده‌است که به عنوان مزرعه ترول از حساب‌های جعلی رسانه‌های اجتماعی برای ایجاد اختلاف و درگیری استفاده می‌کند. توئیتر یادآور می‌شود که حساب‌های این آژانس از هر دو استراتژی ربات‌های خودکار و غیرخودکار استفاده می‌کرد و برخی از حساب‌ها «تلاش می‌کردند در آمریکا تظاهرات را با هدف ایجاد بی‌ثباتی سیاسی سازماندهی کنند. توییتر برآورد کرده که ۹٪ از توئیت‌های‌حساب‌های این آژانس مربوط‌به انتخابات بوده‌است»(Stewart et al,2018:1)

بداوی و همکارانش نیز براساس فهرستی که توئیتر منتشر کرد به این نتیجه دست یافتند که ترول‌های روسی در کل حدود ۲۳۵۴ توئیت منتشر شده از سوی کاربران مجزا را حدود ۶۴۵۷ بار بازتوئیت کردند. ترول‌ها یکدیگر را فقط ۵۱ بار بازتوئیت کردند. کاربران توئیتر می‌توانند موقعیت‌های مکانی، گزارش‌ها و پست‌هایی که در فضای توئیتری و پروفایل خود منتشر می‌کنند را انتخاب نمایند. بیشتر موقعیت‌های مکانی گزارش شده از سوی حساب‌های‌کاربری مربوط به ترول‌های روسیه در داخل خاک‌آمریکا(برخی‌از این حساب‌های کاربری موقعیت مکانی روسیه را برای پروفایل و پست‌های خود انتخاب کرده بودند) و بیشتر این توئیت‌ها عمدتاً از سوی کاربرانی بودند که که در ایالت‌های تنسی و تگزاس قرار داشتند. به ترتیب با ۴۹/۲۷۷ و ۲۶/۴۸۹ توئیت. ترول‌های روسی در حدود ۸۳/۷۱۹ بار بازتوئیت داشتند. با این وجود بیشتر این توئیت‌ها فقط از طرف سه حساب کاربری TEN_GOP با ۴۹/۲۸۶ توئیت، Pamela_Moore13 با ۱۶/۵۳۲ توئیت و The Founding Son با ۸/۷۵۵ توئیت بود که در کل ۸۹٪ از توئیت‌های ترول‌های روسی را

[1]. RU-IRA

بازتوئیت کردند. ترول‌های روسی در حدود ۴۰/۲۲۴ توئیت حساب‌های کاربری مجزا را بازتوئیت کردند (Badawy et al, 2018).

زانتو ۲۷۰۰ توئیت پست شده از سوی ۱۰۰۰ کاربر توئیتری را بررسی کرد که ادعا می‌شود با آژانس‌های جستجوی اینترنتی روسیه ارتباط داشته‌اند و این احتمال می‌رود که ترول‌های حمایت شده از سوی دولت هستند. بطور کلی یافته‌های وی نشان داد که حساب‌های کاربری ترول‌های روسیه موفق شدند برای مدت زمان طولانی فعال باقی بمانند و از طریق پیام‌های خود توانستند به تعداد بسیار قابل توجهی از کاربران توئیتر دسترسی پیدا کنند. با این وجود ترول‌ها نفوذ بسیار کمی در ایجاد خبرهای ویروسی در توئیتر و دیگر سیستم عامل‌های اجتماعی بطور یکسان داشتند. در واقع، ترول‌های روسی در «هل دادن» این آدرس‌های اینترنتی در توئیتر و دیگر شبکه‌های اجتماعی بسیار مؤثر بودند. موضوعات اصلی مورد بحث ترول‌های روسی، رویدادهای جهانی خاص، سازمان‌ها و موضوعات سیاسی مرتبط به ترامپ و کلینتون بود. ترول‌ها در طول زمان هویت‌های مختلفی را اتخاذ می‌کردند. به عنوان مثال، آن‌ها مشخصات خود را با حذف توئیت قبلی خود و تغییر نام پروفایل/اطلاعات آنها «بازنشانی» و بروز می‌کردند. موقعیت گزارش‌ها و پست‌های این ترول‌ها عمدتاً در چند کشور مانند آمریکا، آلمان و روسیه تمرکز یافته‌بود. شاید به این دلیل که تلاش می‌کردند به عنوان مردم و افراد بومی ظاهر شوند و بطور موثری بر دیدگاه‌های کاربران این کشورها تأثیر گذاشته و آنها را دستکاری کنند. در حالیکه کابران تصادفی توئیتر عمدتاً از سیستم عامل موبایل استفاده می‌کردند (Zannettou, 2019).

۳-۳. نفوذ در سیستم ثبت‌نام رای‌دهندگان

مداخله عناصر منسوب به روسیه در انتخابات آمریکا به مراتب فراتر از انتشار اطلاعات نادرست و اخبارجعلی بوده‌است. این عناصر در پی تلاش برای شکستن و نفوذ در

سیستم‌های اصلی دستگاه‌های رأی‌گیری آمریکا نیز بوده‌است (Van De Velde, 2017: 12). آن‌ها بیش از ۲۰ سیستم ثبت‌نام رای‌دهندگان را مورد هدف قرار داده‌است. این کشور توانسته‌بود در چهار سیستم از بیست سیستم نفوذ کند. پایگاه‌های ثبت‌نام رای‌دهندگان در آریزونا و ایلینوز برای بازیگران روسی قابل دسترسی بودند. بیش از ۲۰۰/۰۰۰ مدرک ثبت‌نام رای‌دهندگان در این نفوذ افشا شده‌است(Shackelford, 2016: 643). حتی در چندین شهر، گزارش‌های پراکنده‌ای وجود داشت مبنی براینکه اطلاعات رای‌دهندگان در پایگاه ثبت‌نام رای‌دهندگان حذف یا تغییر یافته‌بودند (Norden & Vandewalker, 2017: 4). البته هنوز هیچ نشانه‌ای وجود ندارد که اطلاعات موجود در این مدارک تغییر یافته‌باشد. در مجموع هکرهای روسی به پایگاه‌های مذکور ۳۹ ایالت حمله کردند. با این حال این نگرانی همواره وجود دارد که این حملات اعتماد عمومی به روند انتخابات (در آمریکا) را تضعیف کرده‌باشد (Shackelford, 2016: 643).

۴. هدف روسیه از مداخله

دومین پرسش مهم در این مقاله این است که اساساً هدف عناصر منسوب به روسیه از مداخله سایبری در انتخابات آمریکا چه بود. شاید کمترین جنبه درک سیاست خارجی کلینتون رویکرد وی نسبت به روسیه باشد. منتقدان اغلب از سال ۲۰۰۹ به عنوان سندی یاد می‌کنند که سیاست خارجی کلینتون (زمانیکه وی وزیر خارجه آمریکا بود) با روسیه ملایم بوده است. اما در واقع رفتار تجربی کلینتون بعنوان وزیرامورخارجه بیانگر دیدگاه تند وی نسبت به روسیه بوده‌است. سال ۲۰۱۱ وی رژیم روسیه را متهم به تقلب در انتخابات پارلمانی روسیه کرد و یک سال بعد پوتین را برای بازپس‌گیری انتخابات ریاست جمهوری ۲۰۱۲ سرزنش کرد (Shapiro, 2016: 7). بر همین مبنا پوتین بوضوح بیان کرده که

کلینتون پشتیبان اعتراضات گسترده علیه وی در دسامبر ۲۰۱۱ بوده‌است[۱]. وی در سخنرانی خود اظهار داشته؛ «آن‌ها ناعادلانه و غیرمنصفانه عمل کردند» و کلینتون «علامتی» به تظاهرکنندگان با حمایت وزارت امورخارجه آمریکا برای تضعیف قدرت وی (Crowley & Ioffe, 2016) در جهت «تغییر رژیم» مسکو نشان داده بودند (Rutland, 2017: 45).

کلینتون در زمان تصویب قانون ماگنیتسکی[۲] در سال ۲۰۱۲ وزیر امورخارجه آمریکا بود. در این لایه، تحریم‌هایی علیه نهادهای روسی که در مرگ سرگئی ماگنیتسکی نقش داشتند اعمال شد. ماگنیتسکی وکیل خصوصی بود که درباره فساد در سیستم روسیه برای تاجر آمریکایی (بنام بیل بردهر) تحقیق می‌کرد. با وجود اینکه کلینتون در سال ۲۰۱۳ وزارت امورخارجه را ترک کرد اما همچنان از پوتین انتقاد می‌کرد (Bevan, 2018). در پاسخ به قانون ماگنتیسکی، روسیه قانونی با اعمال تحریم‌های متقابل علیه گروهی از مقامات و اعضای کنگره آمریکا را به تصویب رسانید. همچنین فرزندخواندگی کودکان روسی توسط اتباع آمریکایی را ممنوع اعلام کرد (Menkiszak, 2017: 39).

---

[۱]. در ۵ دسامبر ۲۰۱۱ چند هزار نفر از معترضان در اعتراض به انتخابات جعلی دوما که دولت در روز قبل برگزار کرده بود جمع شدند. در ۲۴ دسامبر تعداد معترضان به بیش از ۱۰۰ هزار نفر رسید. همزمان و در ماه‌های بعد، تظاهرات مشابهی در سراسر روسیه نیزآغاز شد (Rosenberg, 2017: 14). معترضان خواهان برگزاری انتخابات مجدد دوما بودند و همچنین عقیده داشتند که انتخابات ریاست جمهوری سال ۲۰۱۲ باید بگونه‌ای برنامه‌ریزی شود که آزاد و عادلانه باشد. برای متقاعدسازی افکار عمومی، پوتین که در آن زمان نخست‌وزیر و کاندیدای ریاست جمهوری بود پیشنهاد نصب دوربین‌هایی برای راستی آزمایی انتخابات در صندوق‌هایی رأی را کرد؛ که اینگونه ناظران انتخاباتی می‌توانستند فرایند رأی‌گیری را رصد کنند. بااین‌وجود پس از رأی‌گیری پوتین توانست با جلب ۶۳٪ از آراء مشارکت‌کنندگان در انتخابات به پیروزی برسد. پیروزی پوتین در انتخابات همراه با دور جدیدی از اعتراضات بود و معترضان نسبت به نحوه رأی‌گیری و نتیجه انتخابات اعتراض داشتند. این اعتراضات ادامه اعتراضات نسبت به انتخابات دوما در سال ۲۰۱۱ بود و بسیاری از رهبران معترضین که در آن انتخابات فعالیت می‌کردند رهبری اعتراضات سال ۲۰۱۱ را نیز برعهده داشتند (Nichol, 2012: 8).

[2]. Magnitsky

کلینتون از کمک روسیه به رژیم اسد بسیار خشمگین بود. وی در سخنرانی ژوئن ۲۰۱۲ خود اعلام کرد که روس‌ها هلیکوپترهای جنگنده به سوریه فرستاده‌اند. اما روسیه ادعا کرد که آنها در جنگ داخلی مورد استفاده قرار نگرفتند. از سوی دیگر کلینتون در آن زمان، الحاق کریمه به روسیه را با تهاجم آدولف هیتلر به چکسلواکی و لهستان در دهه ۱۹۳۰ مقایسه کرد (Shapiro, 2016: 7). با توجه به این موضع‌گیری‌ها، پوتین معتقد بود که همکاری با آمریکا دور از انتظار خواهدبود اگر کلینتون وارد کاخ سفید گردد (Rutland, 2017: 45). وی بصورت عمومی درباره رقابت انتخاباتی آمریکا بدون اینکه مستقیماً جانب ترامپ را بگیرد شروع به اظهار نظر کرد. احتمالاً به این دلیل که مقامات کرملین فکر می‌کردند که هرگونه ستایش و حمایت از ترامپ می‌تواند نتیجه عکس در افکار عمومی آمریکا بهمراه داشته باشد. با این وجود پوتین به صورت عمومی اعلام می‌کرد که سیاست‌های دولتی ترامپ سنخیت و سازگاری بیشتری با ترجیحات روسیه دارد (Hastedt, 2017: 119-120).

بعداً مشخص شد که به استثنای بعضی موارد، پوتین زیاد هم بی راهه نرفته‌است. چراکه ترامپ همواره روی بهبود روابط دولت خود با روسیه تاکید داشته است. ترامپ اظهار داشت مردم کریمه تحت حکومت روسیه شادتر از تحت حکومت اوکراین هستند. همچنین وی بدنبال شناسایی کریمه به عنوان بخشی از قلمرو روسیه «خواهد بود» (Meijer, 2017: 5).

نباید این امر را فراموش کرد که در دوران کلینتون و اوباما، سیاست آمریکا و متحدانش مبتنی بر تحریم روسیه بدلیل به اصطلاح دخالت در اواکراین بوده است. با توجه به این امر پوتین همواره اظهار داشته که تحریم‌های غرب تا حد زیادی بر روسیه تأثیر داشته است. پیش از تحریم‌های اقتصادی، روسیه بطور میانگین رشد ۷٪ داشته اما پس از تحریم‌ها، تولید ناخالص داخلی روسیه کاهش یافت. در سال اول تحریم‌ها، ارز روسیه بی‌ثبات شد و به کمترین قیمت تاریخی ۸۰ روبل به یک دلار رسید. یک سال بعد در ژانویه ۲۰۱۶ روبل به قیمت پایین‌تری سقوط کرد. این نوسان در پول ملی، بطور عمده به قیمت‌های پایین

تاریخی نفت مرتبط می‌شد. از ماه اوت ۲۰۱۴، بدلیل کاهش قیمت نفت، حساب‌های بانکی روسیه نیز کاهش یافت. دستمزدها ساکن ماند، سطح فقر و نرخ تورم بطور فزاینده‌ای درحال افزایش بود. در نتیجه تحریم‌ها، روس‌ها فقیرتر شدند و بخاطر تصمیم پوتین برای دخالت در اوکراین بیشتر رنج می‌بردند. این امر منجر به دو موضوع مهم شد؛ فرصتی برای پوتین بمنظور ضربه زدن به آمریکا و مهم‌تر از آن موقعیتی که در آن پوتین نیاز به اصلاح یک تهدید برای قدرت خود داشت (Shuya, 2018: 9). همه این موارد درحالی بوده که برخی تحلیلگران عقیده دارند که ترامپ در رقابت‌های انتخاباتی ۲۰۱۶ با ارسال علائمی مبنی بر آمادگی آمریکا برای اتمام تحریم‌های روسیه، سیاست خارجی آمریکا را در ارتباط با روسیه دگرگون ساخته و از مداخله آن در انتخابات مذکور استقبال کرده است (Sachs, 2019).

قطبی کردن جامعه آمریکا از دیگر اهداف هکرهای منسوب به روسیه بوده است. البته این سیاست نه در میان دو حزب دمکرات و جمهوری خواه بلکه اساساً بدنه اجتماعی جامعه آمریکا را هدف قرار داده است. در طول انتخابات ۲۰۱۶، حساب‌های فیس‌بوکی مرتبط با روسیه، محتواهایی درباره موضوعات اجتماعی تفرقه‌انداز منتشر می‌کرد که جهت‌گیری آنها تحریک و قطبی‌سازی (تضاد) جامعه درباره مسائل مهمی نظیر نژاد، مهاجرت، مذهب و جنسیت بود (Polyakova & Boyer, 2018: 10). در نتیجه این امر نظام لیبرال دمکراسی آمریکا زیر سؤال برده می‌شود و اعتماد عمومی نسبت به انتخابات آمریکا از بین می‌رود و در نهایت بستر اجتماعی لازم را برای یک نزاع اجتماعی دائمی فراهم می‌شود (Sides et al, 2017: 71).

بنظر می‌رسد یکی دیگر از اهداف بلند مدت هکرهای روسی، برجستگی ضعف سیستم انتخاباتی و حزبی آمریکا و تضعیف مشروعیت آمریکا به عنوان نمونه کاملی از دموکراسی است. برخی تحلیلگران بر این باورند که سیستم سیاسی آمریکا تهدیدی برای پوتین است چراکه استانداردهای بالای سیستم دمکراسی آمریکا می‌تواند نمونه‌ای عالی برای تقلید یا شبیه‌سازی توسط دیگران محسوب می‌شود (Hastedt, 2017: 119). هکرهای روسی با

دستکاری این سیستم قصد داشته آنرا ناقص جلوه دهد و از این طریق نشان دهد قدرت نرم آمریکا و ادعای این کشور برای رهبری سیاسی جهان در حال تضعیف است (Ziegler, 2017: 13). برخی ناظران بر این باورند که کرملین به «چیزی کمتر از معکوس کردن فرآیندهای تاریخی مهم که از سال ۱۹۸۹ آغاز شد» و نابودی اتحاد آتلانتیک و جایگزینی آن با یک «نظم جهانی پسا- غربی»، قانع نیست (Peters, 2017: 1).

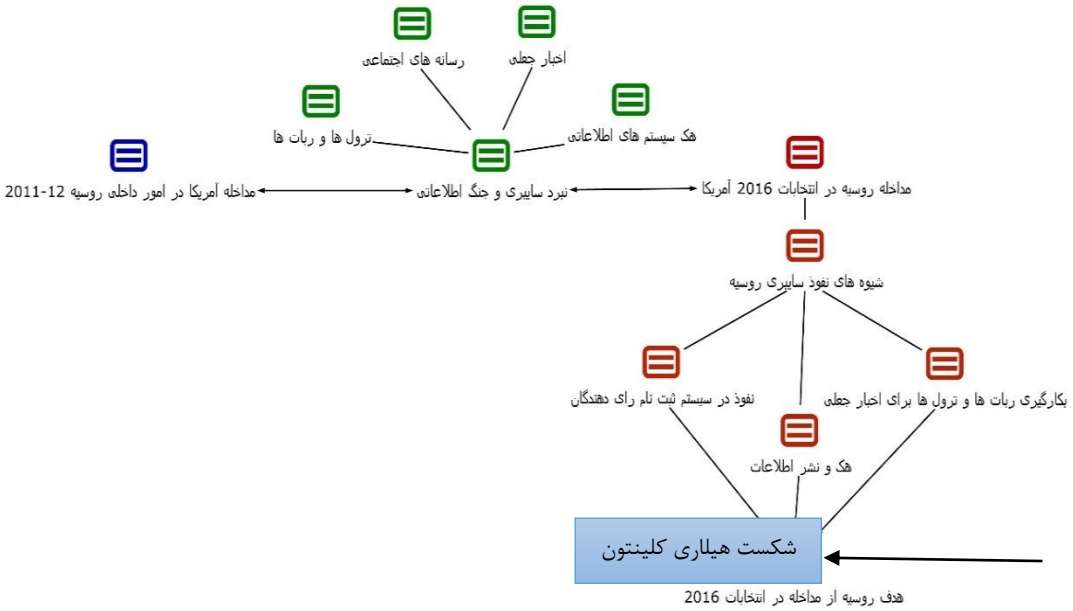
کاشت بذر اختلاف در غرب یکی دیگر از اهداف اصلی عناصر منسوب به روسیه برای مداخله در انتخابات آمریکا است؛ این چیزی است که ترزا می، نخست‌وزیر وقت انگلیس و باراک اوباما، رئیس‌جمهور سابق آمریکا صراحتاً به آن اشاره کرده‌اند (Peters, 2017: 1). یکی از جلوه‌های این اختلاف ایجاد شکاف درون ناتو بود. از دید روسیه قدرت‌گیری ترامپ در آمریکا می‌توانست موجب تضعیف ناتو گردد (Ziegler, 2017: 14). زیرا در طول مبارزات انتخاباتی، ترامپ بارها تمایل خود را برای کاهش دخالت آمریکا در ناتو اعلام کرده بود. شیرف[1]، ژنرال سابق بریتانیا، اذعان داشته که اتخاذ چنین سیاستی از سوی ترامپ سبب بی‌ثباتی در نظم جهانی خواهد شد و اروپا نیز شاهد افزایش ملی‌گرایی خواهد بود. وقتی ناتو از شرق اروپا خارج شود، روسیه فرصت تشدید مواضح تحریک‌آمیز خود را با آوردن سربازان به مرزهای بالتیک و موشک‌های دارای کلاهک هسته‌ای نزدیک به سرزمین‌های اروپایی، بدست می‌آورد (Baenzer & Patrice, 2017: 16).

حدس روسیه بعد از پیروزی ترامپ درست از آب درآمد. ترامپ بطور مداوم تاکید داشته که تعهد آمریکا به ماده ۵ ناتو (دفاع جمعی) بر این خواهد بود که اعضا اروپایی «سواری رایگان» را متوقف کنند و سهم مالی بیشتر برای اتحادیه بعهده گیرند. ترامپ می‌گوید: «آمریکا میلیاردها دلار برای ناتو صرف می‌کند»، «ما بیش از حد پرداخت می‌کنیم»، «شما کشورهایی در ناتو دارید که سواری رایگان بدست می‌آورند و این بسیار غیرمنصفانه است»(Meijer, 2017: 5-6).

[1]. Shirreff

جنگ تجاری پس از ۲۰۱۷ بین اروپا و آمریکا می‌تواند یکی دیگر از پیامدهای روی کارآمدن ترامپ در آمریکا باشد. خواسته یا ناخواسته روند امور در این زمینه نیز بنفع پوتین تمام می‌شود. ترامپ تاکید کرده بود که «آمریکایی شدن و نه جهانی شدن، اعتبار ما خواهد بود». این امر نمایانگر حمایت ترامپ از یک نوع سیستم حمایت از تولیدات داخلی بوده است. وی در طول انتخابات متعهد به بازنگری در سیاست تجاری آمریکا و در صورت لزوم خروج از طیف گسترده‌ای از توافقنامه‌هایی نظیر تجارت آزاد آمریکای شمالی، پیمان تجاری اقیانوس آرام و حتی سازمان تجارت جهانی شد. ترامپ بدنبال ایجاد شکل افراطی سیستم حمایت از تولیدات داخلی و حتی شروع جنگ تجاری با شرکای تجاری اصلی آمریکا از جمله اتحادیه اروپا بوده است (Arnault, 2017: 2). اما نباید این امر را از یاد برد که اتحادیه اروپا بزرگ‌ترین سرمایه‌گذار آمریکا با ۶۰٪ سرمایه‌گذاری در سال ۲۰۱۶ است. از طرفی نیز آمریکا بزرگ‌ترین سرمایه‌گذار اروپا است اما تنها ۴۰٪ سرمایه‌گذاری خارجی در سال ۲۰۱۶ را به خود اختصاص داده است. از سال ۲۰۰۶ سرمایه‌گذاری اتحادیه اروپا در آمریکا از سرمایه‌گذاری آمریکا در اتحادیه اروپا فراتر رفته است (Colibasanu, 2018). ترامپ شرکای تجاری خود را تهدید به تحمیل تعرفه‌های فراتر از ۴۵٪ کرده است مگر اینکه آنها با شرایط تجاری آمریکا موافقت کنند (Arnault, 2017: 2). تحمیل این تعرفه‌ها و موانع واردات نه تنها مانع تجارت بلکه سرمایه‌گذاری نیز شده و سبب ایجاد یک جنگ تجاری شده است (Colibasanu, 2018). نمودار زیر نمایانگر نبرد سایبری عناصر منسوب به روسیه در انتخابات ۲۰۱۶ آمریکا است:

نبرد سایبری عناصر منسوب به روسیه در انتخابات ۲۰۱۶؛ (منبع نگارندگان)



نتیجه‌گیری

اگر دخالت عناصر منسوب به روسیه در انتخابات ریاست جمهوری ۲۰۱۶ آمریکا را واقعی بنگاریم این امر به خوبی نشان داد که چگونه بکارگیری ابزارها و تاکتیک‌های قدرت‌های بزرگ در عصر پساحقیقت متحول شده است و رقابت تسلیحاتی و سخت‌افزارانه روسیه و آمریکا در دوران جنگ سرد تبدیل به رقابت در حصول تکنولوژی‌های پیشرفته و نرم‌افزارانه برای دستابی به نتایج دلخواه در دوره پسا- جنگ سرد شده است.

بنظر می‌رسد تجربه انتخابات ۲۰۱۶ آمریکا نشان داد که نیروهای سایبری با پی بردن به اهمیت قدرت سایبری و سرمایه‌گذاری بر روی آن بویژه در عرصه فضای مجازی، خود را برای ورود به جنگ‌های آینده آماده کرده‌اند. دخالت در انتخابات ریاست جمهوری آمریکا صرفنظر از نتایج و پیامدهای بعدی آن، یکی از تجربیات موفق نیروهای نبرد سایبری قلمداد می‌شود. عناصر منسوب به روسیه در آن صحنه نبرد با استفاده از ابزارهای سایبری

بر تحولات سیاسی آمریکا نفوذ کردند و باعث شدند دست کم بین بد و بدتر برای روسیه، نامزد بد به کاخ سفید راه یابد. هکرهای روسی در این مسیر توانایی و قدرت مجازی خود را به نمایش گذاشتند اما این نمایش قدرت نه در جهت جذب دیگران به ارزش‌های روسی بلکه در جهت ایجاد تردید در دیگران نسبت به گرایش به ارزش‌های آمریکایی بود؛ چراکه هدف این هکرها جهت‌دهی به افکار عمومی مخاطبان با نشر اطلاعات لازم برای ممانعت از پیروزی کلینتون و ضربه به ارزش‌های آمریکا نیز بود. البته این فقط بخشی از اهداف آنها بود.

آنگونه که بعضی از تحلیلگران باور دارند عناصر روسی با دخالت در انتخابات آمریکا مجموعه‌ای از اهداف را دنبال می‌کردند که مهم‌ترین آنها عبارت بودند از؛ شکست هیلاری کلینتون، تضعیف روابط فراآتلانتیکی از جمله ناتو، کاهش تقاضای بین‌المللی از آمریکا، لطمه زدن به اعتبار آمریکا در خارج، احیاء دوباره قدرت روسیه، حفظ رژیم پوتین از تهدید قدرت مردم، بی‌اعتباری هیلاری کلینتون و ضربه به پتانسیل‌های انتخاباتی وی.

در هر حال، آنچه عناصر منسوب به روسیه در انتخابات آمریکا انجام دادند هنوز هم پس لرزه‌های آن دامن‌گیر جامعه آمریکا است و این نشان می‌دهد که نفوذ سایبری در جهان امروز، تا چه حد اهمیت یافته است. بدون تردید وقایع این چنینی کشورهایی نظیر ایران را با توجه به همه‌گیر شدن استفاده مردم از رسانه‌های اجتماعی به سمتی سوق می‌دهد که بتدریج جنگ‌های سایبری (به عنوان جایگزین جنگ‌های مسلحانه و فیزیکی) می‌توانند بر روند تحولات آینده سیاسی ایران بسیار اثرگذار باشد.

منابع:

- Busby, Joshua W. (2007). "Climate Change and National Security, an Agenda for Action", CFR NO.32, November, **Council on Foreign Relations**.
- Arnault, B. (2017). "The Trump presidency: What consequences will this have on Europe? Fondation Robert Schuman Policy Paper". **Europe an Issues**, 417. pp.1-11.
- Badawy, A., Ferrara, E., & Lerman, K. (2018). "Analyzing the digital traces of political manipulation: the 2016 Russian interference Twitter campaign". **In 2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining** (ASONAM). IEEE.
- Baezner, M. & Robin, P. (2017). "Cyber-conflict between the United States of America and Russia". **ETH Zurich**, 2.
- Baruah, T. D. (2012). "Effectiveness of Social Media as a tool of communication and its potential for technology enabled connections: A micro-level study". **International Journal of Scientific and Research Publications**, 2(5), pp.1-10.
- Bevan, M. (2018). "Why does Vladimir Putin hate Hillary Clinton?". (May 22), Available at: https://www.abc.net.au/news/2018-05-22/vladimir-putin-and-hillary-clinton-hatred-explained/9783076
- Cheng, J., Bernstein, M., Danescu-Niculescu-Mizil, C. & Leskovec, J. (2017). "Anyone can become a troll: Causes of trolling behavior in online discussions". In CSCW: proceedings of the Conference on Computer-Supported Cooperative Work. **Conference on Computer-Supported Cooperative Work**. NIH Public Access.
- Colibasanu, A. (2018). "Why the US Can't Afford a Trade War With the EU". Available at: https://geopoliticalfutures.com/us-cant-afford-trade-war-eu/
- Cordy, J. (2017). "Social Media Revolution: Political and Security Implications". **NATO Parliamentary Assembly**. Available at: https://www.nato-pa.int/download-file?filename=sites/default/files/2017-11/2017%20

- Crowley, M. & Ioffe, J. (2016). "Why Putin hates Hillary". (July 25), Available at: https://www.politico.com/story/2016/07/clinton-putin-226153
- Dorell, O. (2018). "Another Cold War? Tensions between U.S. and Russia may be higher now". (March 29), Available at: https://www.usatoday.com/story/news/world/2018/03/29/united-states-russia-cold-war-putin-trump/467806002/
- Ferguson, N. (2018). **The Square and the Tower: Networks and Power, from the Freemasons to Facebook**. New York: Penguin Press.
- Haeni, R. E. (1997). "Information Warfare - an introduction". **The George Washington University Cyberspace Policy Institute**, pp1-16.
- Hastedt, P. G. (2017). **Readings in American Foreign Policy: Problems and Responses**. **Rowman & Littlefield Publishers**. Maryland
- Hutchings, S. (2017). "Fake news and 'post truth': some preliminary notes". **Russian Journal of Communication**, DOI: 10.1080/19409419.2017.1323178.
- Jaitner, M. (2012). "Exercising Power in Social Media: A Study of Hard and Soft Power in the Context of Russian Elections 2011-2012". M.A Disertation, National defence college, New Delhi, India.
- Journell, W. (2017). "Fake News, Alternative Facts, and Trump: Teaching Social Studies in a Post-Truth Era". **Social Studies Journal**, 37, pp.8-21.
- Khan, G. F. (2017). **Social Media for Government**. Springer Nature Singapore Pte Ltd.
- Libicki, M. C. (1995). **What is information warfare?**. Natinal defense UNIV Washington DC inst for national strategic studies.
- Ludes, J.M. & Jacobson, M.R. (2017). "Shatter the House of Mirrors: A Conference Report on Russian Influence Operations". The Pell Center for International Relations and Public Policy at Salve Regina University.
- Mazzetti, M. & Sanger, D. E.(2013). "Security Leader Says U.S. Would Retaliate Against Cyberattacks". (March 12), Available at:

https://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html?pagewanted=all

- Meijer, H. (2017). "Strategic Implications of Donald Trump's Election". **IRSEM**. Research Paper, 33, pp.1-13.
- Menkiszak, M. (2017). "Russia's best enemy, Russian policy towards the United States in Putin's era". **Point of View**, 62, pp.5-55.
- Mulvenon, J. (1999). "The PLA and information warfare". The People's Liberation Army in the Information Age, 297, pp.175-186.
- Nagy, V. (2012). "The geostrategic struggle in cyberspace between the United States, China, and Russia". **AARMS: Academic & Applied Research in Military Science,** 11(1),pp.13-26.
- Nation, R. C. (2012). "Reset or rerun? Sources of discord in Russian–American relations". **Communist and Post-Communist Studies**, 45(3-4), 379-387.
- Nichol, J. (2012). "Russia's March 2012 Presidential Election: Outcome and Implications". **Congressional Research Service**, Library of Congress. pp.1-12.
- Norden, L. and Vandewalker, L. (2017). "Securing Elections from Foreign Interference, Brennan Center for Justice". Available at: https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference.pdf
- Oxford Dictionaries (2017). "Post-truth, Oxforddictionaries". Available at: https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016
- Peters, M.A. (2017). "The information wars, fake news and the end of globalization". **Educational Philosophy and Theory**, pp.1-4. DOI: 10.1080/00131857.2017.1417200.
- Polyakova, A. & Sencer p. B. (2018). "The Future of Political Warfare: Russia, The West, and The Coming Age of Global Digital Competition". **EUROPE**.
- Rochlin, N. (2017). "Fake news: belief in post-truth". **Library Hi Tech**, 35(3), pp.386-392.

- Rosenberg, D. (2017). **The "Colorless" Protests in Russia: Mixed Messages and an Uncertain Future**. Springe. Cham
- Rutland, P. (2017). "Trump, Putin, and the Future of US-Russian Relations". **Slavic Review**, 76(1), pp.41-56.
- Sachs, J. (2019). "Congress should initiate impeachment proceedings against Trump". Available at: https://edition.cnn.com/2019/04/20/opinions/mueller-report-trump-congress-initiate-impeachment-sachs/index.html
- Sather, J. (2017). "An Invisible Curtain Falls between Russia and the West". Stratfor, **(**May 26), Available at: https://worldview.stratfor.com/article/invisible-curtain-falls-between-russia-and-west
- Shackelford, S. J., Schneier, B., Sulmeyer, M., Boustead, A., Buchanan, B., Deckard, A. N. C., ... & Smith, J. M. (2016). "Making Democracy Harder to Hack". **University of Michigan Journal of Law Reform**, 50(3), pp.629-668.
- Shapiro, J. (2016). "The Everyday and The Existential: How Clinton and Trump Challenge Transatlantic Relations". **European Council on Foreign Relations**, pp.1-9.
- Shu, K., Sliva, A., Wang, S., Tang, J., & Liu, H. (2017). "Fake news detection on social media: A data mining perspective". **ACM SIGKDD Explorations Newsletter**, 19(1), pp.22-36.
- Shuya, M. (2018). "Russian Cyber Aggression and the New Cold War". **Journal of Strategic Security**, 11(1), pp.1-18. DOI: https://doi.org/10.5038/1944-0472.11.1.1646
- Sides, W. G. J., Tesler, M., Vavreck, L., Snyder, J., Puddington, A., Roylance, T., ... & Lynch, G. (2017). "The 2016 US Election". **Journal of Democracy**, 28(2).
- Park, S. H. (2014). "Contentious Politics in Contemporary Russia: Protest Movement of 2011-2013". **6th East Asian Conference on Slavic Eurasian Studies**, Seoul, (June 27-28).
- Smith, A. (March 10, 2018). "Alexan Putin on U.S. election interference: 'I couldn't care less", **NBC News**.
- Stent, A. (2012). "US–Russia Relations in the Second Obama Administration". **Survival**, 54(6), pp.123–138.

- Stewart, L. G., Arif, A., & Starbird, K. (2018). "Examining trolls and polarization with a retweet network". In Proc. **ACM WSDM**, Workshop on Misinformation and Misbehavior Mining on the Web (to appear).
- Stukal, D., Sanovich, S., Bonneau, R., & Tucker, J. A. (2017). "Detecting Bots on Russian Political Twitter". **Big data**, 5(4), pp.310-324.
- Taddeo, M. (2012). "Information warfare: A philosophical perspective". **Philosophy & Technology**, 25(1), pp.105-120.
- Theohary, C. A. (2018). "Information Warfare: Issues for Congress". **Congressional Research Service**.
- Treverton, G. F. & Chen, A. R. (2017). "Hybrid Threats: Russian Interference in the 2016 US Election". *SMA*, Inc.
- Tsvetkova, M., García-Gavilanes, R., Floridi, L., & Yasseri, T. (2017). "Even good bots fight: The case of Wikipedia". **PLoS ONE**, 12. (2), pp.1-13.
- Van De Velde, J. (2017). "The Law of Cyber Interference in Elections". **SSRN**. Available at: https://ssrn.com/abstract=3043828
- Vasu, Norman, Benjamin Ang, Terri-Anne-Teo, Shashi Jayakumar, Muhammad Faizal, and Juhi A. (2018). "Fake News: National Security in the Post-Truth Era". **RSIS**, pp.1-25.
- Wilson, C. (2004). "Information Warfare and Cyberwar: Capabilities and Related Policy Issues". **CRS Report for Congress**. pp.1-21
- Woolley, S. C. (2016). "Automating power: Social bot interference in global politics". **First Monday**, 21(4).
- Zakem, V., Saunders, P., Hashimova, U., & Frier, P. K. (2017). "Mapping Russian Media Network: Media's Role in Russian Foreign Policy and Decision-Making". **CNA Analysis and Solutions Arlington United States**.
- Zannettou, S., Caulfield, T., De Cristofaro, E., Sirivianos, M., Stringhini, G., & Blackburn, J. (2019). "Disinformation warfare: Understanding state-sponsored trolls on Twitter and their influence on the web". **In Companion Proceedings of the 2019 World Wide Web Conference** (pp. 218-226). ACM.

- Ziegler, C.E. (2017). "International dimensions of electoral processes: Russia, the USA, and the 2016 elections". **International Politics**, pp.1-18.
- Zinovyeva, E. (2013). "US digital diplomacy: Impact on international security and opportunities for Russia". **Security Index: A Russian Journal on International Security,** 19(2), pp.33-43.