آسیب‌پذیری انتخابات ایالات متحده در برابر حملات خارجی[1]

روایت گسل‌هایی در روند انتخابات در آمریکا

متن پیش رو، ترجمه‌ای است از مطلبی با همین عنوان که به قلم «لارنس نوردن (مدیر برنامه اصلاحات در انتخابات) و دانیل ل. وینر[2] (مشاور ارشد مرکز برنان برای عدالت در دانشگاه نیویورک»، در ۲۳ ژوئیه ۲۰۱۹، در تارنمای نشریه فارین افرز منتشر شده است. نویسندگان این مقاله به شکاف‌های موجود در نظام انتخاباتی ایالات‌متحده و امکان نفوذ در آن اشاره دارند و لزوم ورود کنگره به این موضوع و از بین بردن زمینه‌های اثرگذاری آن را ضروری می‌دانند.

حمله روسیه به انتخابات آمریکا در سال ۲۰۱۶ که در گزارش اخیر رابرت مولر دادستان ویژه تحقیقات مداخله روسیه در انتخابات آمریکا با عنوان وسیع و سیستماتیک تصدیق شده است، برای بسیاری شوک‌آور اما قابل پیش‌بینی بود؛ زیرا سال‌ها است، کارشناسان درباره خطر مداخله خارجی در انتخابات این کشور هشدار داده‌اند. تا سال ۲۰۱۶، تصویب رأی‌گیری رایانه‌ای، امنیت انتخابات در برابر مداخلات خارجی را تضعیف کرده و ایالات‌متحده را در معرض حمله قرار داده بود. از طرف دیگر، تغییر رسانه‌ها و شکل‌گیری ارتباطات دیجیتال نیز شکاف‌های جدیدی در امنیت و قانون ایجاد کرده است که می‌تواند برای دست‌کاری و باج‌گیری از آن استفاده شود. روسیه و —شاید- قدرت‌های دیگر مانند چین و ایران، احتمالاً سعی می‌کنند تا از این آسیب‌پذیری‌ها در سال ۲۰۲۰، بار دیگر سوءاستفاده نمایند. آخرین بار (۲۰۱۶) ایالات‌متحده گرفتار این مسئله شد. اکنون، تقریباً سه سال پس‌ازآنکه اولین تلاش‌های روسیه آشکار شد، ایالات‌متحده پیشرفت نسبتاً کمی در راستای ایمن کردن سیستم انتخاباتی خود در برابر مداخلات داشته است. گذشت روزها و انتظار انجام چنین کاری، احتمال برگزاری انتخابات دیگری همراه با دخالت‌های چشمگیر خارجی را افزایش داده است. خوشبختانه، هنوز تدابیری وجود دارد که کنگره، کمیسیون انتخابات فدرال و سایر سیاست‌گذاران، می‌توانند برای ممانعت از حمله آینده انجام دهند. تنها کمتر از شش ماه به آغاز انتخابات مقدماتی در نیوهمپشایر و آغاز رأی‌گیری در سال ۲۰۲۰ مانده است که قانون‌گذاران و دستگاه‌های اجرایی، باید با ارتقاء تجهیزات، محافظت در برابر هک و مبارزه با عملیات نفوذ خارجی، امنیت انتخابات را در اولویت قرار دهند.

1 – U.S. Elections Are Still Not Safe From Attack
2 – Lawrence Norden and Daniel I. Weiner

ایمنی تجهیزات را تضمین کنید

گزارش اخیر وزارت امنیت داخلی تأیید می‌کند که در سال ۲۰۱۶، روسیه به‌احتمال زیاد در هر ۵۰ ایالت، عملیات تحقیق و شناسایی علیه شبکه‌های انتخابات انجام داده است. آن‌ها در اطلاعات مربوط به یک پایگاه داده ثبت‌نام ایالتی، نفوذ و به اطلاعات دسترسی و با آلوده کردن رایانه‌ها در یک شرکت فناوری رأی‌گیری، دست‌کم با موفقیت در دو بخش از فلوریدا در شبکه‌های انتخاباتی نفوذ کرده‌اند. همچنین، بیشتر زیرساخت‌هایی رأی‌گیری در آمریکا، مورد حمله قرار گرفت. دولت فدرال در سال‌های پس‌ازآن، پیشرفت‌هایی را در زمینه ایمنی این سیستم‌ها انجام داده است. اکنون دفاتر انتخابات ایالتی و محلی، دسترسی بیشتری به مشاوران امنیت سایبری و ارزیابی ریسک دارند و ایالت‌ها، دولت فدرال و شرکت‌هایی که تجهیزات مورداستفاده در نظرسنجی‌ها را فراهم می‌کنند، نسبت به گذشته اطلاعات بیشتری به اشتراک می‌گذارند.

کنگره در سال ۲۰۱۸، ۳۸۰ میلیون دلار برای تأمین هزینه انتخابات در اختیار ایالات قرار داد؛ اما هنوز، به‌طور گسترده زیرساخت انتخابات غیرمتمرکز (شامل بیش از ۸۰۰۰ حوزه انتخابیه محلی جداگانه)، ایالات‌متحده راه طولانی را باید طی کند تا انتخابات کشور را ایمن سازد. دستگاه‌هایی که مردم از طریق آن رأی می‌دهند و آراء را شمارش می‌کنند، ازنظر تعداد در شهرستان‌ها و حتی شهرها متفاوت است؛ از شمارش دستی آراء کاغذی گرفته تا ضبط دیجیتالی آراء در رایانه‌ها با صفحه لمسی. در صورت محافظت از دخالت خارجی، لازم است تجهیزات رأی‌دهی در بسیاری از مناطق، خیلی فوری ارتقا یابد. برای مثال، کارشناسان متفق‌القول‌اند که دستگاه‌های رأی‌گیری قدیمی و بدون کاغذ، بسیار ناایمن هستند و درعین‌حال، شهرستان‌ها در ۱۱ ایالت ازجمله ایالت‌های موردحمله مانند جورجیا و پنسیلوانیا، همچنان در حال استفاده از چنین ماشین‌هایی هستند. اگر کسی با دستگاه رأی‌دهی بدون کاغذ دست‌کاری کند، هیچ سابقه مستقل کاغذی وجود نخواهد داشت که با استفاده از آن، بتوانید نتایج نرم‌افزار را بررسی کرده و دست‌کاری آن را تصحیح نمایید. کنگره باید اقدامات لازم برای اطمینان از جایگزینی این سیستم‌ها را قبل از انتخابات ۲۰۲۰ انجام دهد؛ اما تهیه نسخه پشتیبان کاغذی تنها در صورت مرور شهرستان‌ها و ایالات، به آن‌ها کمک می‌کند. در حال حاضر، تنها ۲۲ ایالت از ۳۹ ایالت -که دارای پشتیبان کاغذی آراء هستند- برای اطمینان از صحت آراء الکترونیکی، نیاز به ممیزی پس از انتخابات دارند.

مدت‌زمان طولانی است که کنگره نیاز به چنین ممیزی در سراسر کشور دارد. به همین ترتیب، ارزیابی ریسک که در حال حاضر حوزه‌های انتخابیه از آن استفاده می‌کنند، تنها درصورتی‌که خطرات شناسایی‌شده قابل اصلاح باشند، می‌توانند مؤثر واقع شوند؛ اما حوزه‌های انتخابیه غالباً برای پرداختن به خطرات امنیتی‌شان بودجه ندارند. در بسیاری از موارد، مقامات انتخابات می‌دانند که باید تجهیزات خود را به‌روز کنند تا امنیت آن بیشتر شود، اما آن‌ها به‌راحتی نمی‌توانند این کار را انجام دهند. به‌عنوان‌مثال، تنها مقامات انتخابات محلی در ۳۱ ایالت اخیراً گزارش داده‌اند که آن‌ها نیاز به جایگزین کردن تجهیزات رأی‌گیری خود قبل از انتخابات ۲۰۲۰ دارند اما نزدیک به دوسوم آن‌ها، گفته‌اند که حتی پس از توزیع بودجه ۳۸۰ میلیون دلاری کنگره در سال گذشته، پولی برای انجام این کار ندارند. دموکرات‌های مجلس نمایندگان، اخیراً یک لایحه تخصیص اعتبار تصویب کرده‌اند که حدود ۶۰۰ میلیون دلار اعتبار دیگر برای حوزه‌های انتخاباتی ایالتی و محلی فراهم می‌کند. جمهوری‌خواهان مجلس، ۳۸۰ میلیون دلار دیگر پیشنهاد داده‌اند. هیچ‌یک از این موارد، زیرساخت‌های انتخاباتی ایالات‌متحده را کاملاً تضمین نمی‌کند، اما می‌تواند آغازی برای پیشرفت‌های آینده باشد.

سرانجام، کنگره باید بپذیرد که امنیت انتخابات، یک مسئله امنیت ملی است و دقیقاً همان‌گونه که کنگره وظیفه دارد از بندرهای کشور در برابر تجاوز خارجی محافظت کند، این وظیفه را هم دارد که وجوه لازم برای تأمین انتخابات را به ایالات ارائه دهد.

جلوگیری از خطر باج‌گیری و شانتاژ

همه دخالت‌ها در انتخابات، شامل دست‌کاری مستقیم در رأی‌گیری‌ها نیست. موفق‌ترین جنبه حمله روسیه در سال ۲۰۱۶، هک کردن و انتشار ایمیل‌های شرم‌آور از سرورهای حزب دموکرات و حساب‌های شخصی بود. این تلاش، به لطف پوشش گسترده رسانه‌های آمریکا، بی‌نهایت مخاطب پیدا کرد. رابرت مولر به این نتیجه رسید که کمپین انتخاباتی ترامپ از این استراتژی آگاهی داشت، آن را تشویق کرده و با اشتیاق، از این استراتژی سود می‌برد اما به‌طور جدی در آن شرکت نکرد. روسیه سابقه طولانی در استفاده از اطلاعات آسیب‌رسان[3] برای شرمساری یا تهدید مقامات برجسته سایر کشورها دارد. عصر دیجیتال باعث شده تا چنین تاکتیک‌هایی راحت‌تر پیش بروند و ثمره آن‌ها، زودتر به بار نشینند. گرچه هک کردن ایمیل شخصی شخص دیگر و سرقت اطلاعات آن در ایالات‌متحده غیرقانونی است، اما چنین قوانینی برای دولت رقیب، به‌سختی اهمیت دارد. تنها راه محافظت مؤثر در برابر باج‌گیری‌های دیجیتال، سرمایه‌گذاری در محافظت از اهداف حساس به لحاظ سیاسی است. در دنیای ایدئال، دولت، این حمایت‌ها را تأمین می‌کند، اما حتی اگر کنگره هم نخواهد پول اضافی خرج کند، تغییرات قانونی دیگری نیز وجود دارد که به آن‌ها کمک می‌کند.

کمپین‌های انتخاباتی فعالیت‌های کوتاه‌مدت هستند و به همین دلیل، بعید است که سرمایه‌های خود را در امنیت سایبری سرمایه‌گذاری کنند؛ اما برخی از تغییرات دقیق تنظیم‌شده در قوانین مالی کمپین، به آن‌ها اجازه می‌دهد تا منابع خارجی را برای این منظور بپذیرند. در این راستا، کمیسیون انتخابات فدرال قبلاً چندین قدم برداشته است؛ در ماه مه تصمیم گرفت که یک سازمان غیرانتفاعی -که توسط مرکز بلفر در دانشکده کندی هاروارد تأسیس شده است- می‌تواند بدون ایجاد محدودیت مشارکت در تبلیغات، به تبلیغات غیرحزبی در فضای مجازی کمک کند. البته اخیراً نظر دیگری صادر کرده است که به یک شرکت انتفاعی کمک می‌کند تا به‌عنوان بخشی از مدل تجاری خود، کمک‌های نامحدود در این زمینه ارائه نماید. اگرچه این تلاش‌های جزئی مفید است، اما راه‌حل جامع‌تر، احتمالاً باید از کنگره بیاید. در مرحله اول، کنگره می‌تواند هزینه‌های افزایش امنیت سایبری را از محدودیت سقف میزان کمک مالی سازمان‌های احزاب ملی، مانند کمیته ملی دموکرات‌ها[4] و کمیته ملی جمهوری‌خواه‌ها[5]، به

3- kompromat

4- The Democratic National Committee (DNC)
5- The Republican National Committee (RNC)

کاندیداهای وابسته معاف کند. پس از سرقت ابزارهای خطرناک، ابزارهای اندکی برای کنترل تأثیرگذاری آن‌ها وجود دارد. احتمالاً اصلاحیه اول، دولت را از محدود کردن استفاده رسانه‌ها از اطلاعات سرقت شده بازمی‌دارد؛ اما دولت می‌تواند رسانه‌های خبری ایالات‌متحده را تشویق کند تا مخاطبان را نسبت به دست‌کاری در انتخابات و هشدار به بازپخش اطلاعات سرقت شده، آگاه کنند. دولت فرانسه این کارها را در برابر تلاش روسیه برای مداخله در انتخابات ریاست جمهوری ۲۰۱۷، از طریق دور ریختن اطلاعات هک شده از فعالیت‌های ریاست جمهوری امانوئل مکرون که با اسناد جعلی درهم‌آمیخته بود، به کار برد.

بااین حال، وقتی صحبت از رفتار کمپین‌های انتخاباتی می‌شود، کنگره می‌تواند و باید برخی خطوط قانونی روشن را ترسیم کند و حتماً این کار را زودتر از موعد انجام دهد. گزارش مولر نمونه‌هایی از تلاش مقامات کمپین انتخاباتی ترامپ در تشویق به انتشار اطلاعات هک شده برای شرمساری طرفداران جناح سیاسی مقابل را آشکار می‌کند. درحالی‌که برخی از این رفتارها می‌توانست قوانین موجود را نقض کند، کنگره باید این قانون را روشن کند تا شک و تردید در مورد فعالیت یا درخواست حزب و کمپین برای کمک دولت خارجی ممنوع باشد. کنگره، همچنین باید از کمپین‌ها بخواهد که همکاری رایگان از طرف دولت‌های خارجی، احزاب سیاسی و کلیه پرداخت‌ها از سوی حامیان خارجی را گزارش دهند.

بستن شکاف‌ها در قانون

دخالت روسیه در سال ۲۰۱۶، کمپین دروغ‌پردازی و پروپاگاندایی -که هدف آن کاهش مشارکت رأی‌دهندگان آمریکایی است- را آشکار کرد. این کمپین، متمرکز بر تقویت اختلافات اجتماعی بود؛ کاهش مشارکت، به‌ویژه در جوامع اقلیت و کمک به دونالد ترامپ برای شکست هیلاری کلینتون. عاملان روسی از پشتیبان پست‌هایی در رسانه‌های اجتماعی استفاده کردند تا به مخاطبان موردنظرشان، دسترسی پیدا کنند اما برای عموم گسترده‌تر قابل‌رؤیت نباشد. برخی از این پشتیبانان پست‌ها، به نامزدهای انتخاباتی یا شعارهای انتخاباتی مربوط بودند، اما بیشتر آن‌ها به مسائل سیاسی تفرقه‌انگیز پرداخته یا تئوری‌های توطئه را به‌منظور تحریک تنش‌های اجتماعی و جلوگیری از رأی دادن گسترش می‌دادند. درحالی‌که خود پست‌ها، پشتیبان پست هستند، اما به‌گونه‌ای طراحی‌شده بودند که به‌صورت رایگان به اشتراک گذاشته شوند. روسیه از تعداد زیادی حساب رسانه‌های اجتماعی شرم‌آور، صفحات فیس‌بوک و وب‌سایت‌ها برای پرداختن به موضوعات مشابه در پشتیبان پست‌ها استفاده کرد. این ارتباطات حمایت نشده نیز برای اشتراک‌گذاری گسترده، طراحی شده بود.

بسیاری از افراد با استفاده از هویت‌های فرضی آنلاین بودند که برخی از آن‌ها توسط ربات‌هایی انسان‌نما ایجاد شده بودند. سازمان‌های رسانه‌ای تحت حمایت دولت روسیه مانند راشا تودی و اسپوتنیک، به گسترش بیشتر مطالبی که در هر دو شکل اسپانسر پست‌ها و غیر اسپانسر پست‌ها ظاهر شده‌اند، کمک کرده است. روسیه همچنین، دست به کمپین‌های تبلیغاتی سنتی‌تر نیز زد؛ به گفته خبرنگاران گاردین، افرادی که با دولت روسیه ارتباط داشتند، کمک‌های قابل‌توجهی به حداقل یک سازمان غیرانتفاعی در ایالات‌متحده، یعنی انجمن ملی سلاح انجام داده‌اند که بیش از ۳۰ میلیون دلار برای تبلیغات در حمایت از دونالد ترامپ، در این کشور خرج کرده است. همه این فعالیت‌ها، با توجه به وجود شکاف در قوانین ایالات‌متحده امکان‌پذیر بود.

گروه‌های به‌اصطلاح پول سیاه مانند ان. آر. ای،[6] نیازی به افشای هویت هیچ‌یک از اهداکنندگان کمک‌های خود ندارند و این کار را برای تسهیل مجاری دریافت پول نقد خارجی

6- The National Rifle Association of America is a gun rights advocacy group based in the United States.

انجام می‌دهند. همچنین، تبلیغات کمپین‌های اینترنتی می‌تواند در یک منطقه خاکستری ازنظر نظارت قرار بگیرد؛ قوانین شفافیت و ممنوعیت تبلیغات از جانب اتباع بیگانه، فقط در مورد ارتباطات حاوی کلمات خاص اعمال می‌شود که صریحاً موافق یا مخالف نامزدها باشند. به همین ترتیب، این قوانین به‌راحتی قابل دور زدن هستند. فعال انتخاباتی که به هیچ نامزدی اشاره نمی‌کند، کاملاً کنترل نشده است و درحالی‌که نمایندگان دولت‌های دیگر-که در ایالات‌متحده فعالیت می‌کنند- ازجمله نهادهای رسانه‌ای تحت حمایت دولت روسیه مانند راشا تودی و اسپوتنیک -که نفوذ قابل‌توجهی در بازارهای ایالات‌متحده دارند- می‌توانند مطابق الزامات قانون ثبت نمایندگی‌های خارجی[7] باشند، این قانون، مستثناهای بی‌شماری را شامل می‌شود و ازنظر اجرایی ضعیف است.

تصویب قانون افشاگری که از سال ۲۰۱۰ در هر دو مجلس، مطرح شده است، مشکل پول‌های نامشخص و سیاه را به‌کلی کم می‌کند و سازمان‌های غیرانتفاعی مانند نارا را ملزم می‌کند تا اهداکنندگان خود را هنگام کمک به هزینه‌های تبلیغات آشکار سازد. بر اساس لایحه دیگری با نام قانون فریبکاری و قانون جلوگیری از ارعاب رأی‌دهندگان، انتشار اطلاعات دروغ به‌صورت آنلاین و به‌منظور جلوگیری از شرکت رأی‌دهندگان واجد شرایط یا ثبت‌نام در رأی‌گیری را جرم محسوب می‌کند؛ مانند کاری که روس‌ها در سال ۲۰۱۹ با اقلیت‌ها کردند. کنگره باید این لایحه را تصویب کند. سرانجام، کنگره باید با این سؤال که چه راهکارهای بیشتری را می‌تواند برای کشف فعالیت‌های آنلاین فریبنده خارجی ازجمله استفاده از ربات‌ها و دیپ فیک‌ها (محتوای جعلی و ویدئویی جعلی بسیار واقع‌گرایانه) را بدون نقض آزادی‌های مدنی اتخاذ کند، پاسخ دهد.

تأمین امنیت انتخابات آتی، نه‌تنها نیازمند تصویب قوانین جدید بلکه اجرای قوانینی است که در حال حاضر وجود دارد. کمیسیون انتخابات فدرال، غالباً به دلیل بن‌بست‌های مکرر میان شش عضو خود، این کار را انجام نمی‌دهد. کنگره باید تعداد اعضای کمیسیون‌ها را از شش به پنج نفر، کاهش دهد و به کارکنان حرفه‌ای کمیسیون این امکان را بدهد که به‌طور مستقل، در مورد نقض قانون تحقیق کنند. به همین ترتیب، کنگره می‌تواند با تأسیس یک واحد اجرایی اف. ای. آر. ای در وزارت دادگستری، به اجرای قوانین اف. ای. آر. ای بپردازد و با قدرت اجرایی دادن به قانون در فعالیت‌های مدنی و مجرمانه، می‌تواند سنگینی بار دولت را برای ثابت کردن و چاره‌جویی برای تخلفات کاهش دهد. کنگره باید از ثبت‌نام‌شدگان در اف. ای. آر. ای - ازجمله نهادهای رسانه‌ای مانند راشا تودی و اسپوتنیک - بخواهد تا وضعیت خود را به‌عنوان نمایندگان خارجی در ارتباطات عمومی، ازجمله برنامه‌های تلویزیونی، رادیویی و کمپین‌های تبلیغاتی افشا کنند.

کریستوفر ری، مدیر اف بی ای در اوایل سال جاری (۲۰۱۹) گفت که دشمنان ما قصد هماهنگی و بازی هماهنگ و سطح بالا دارند. پس ایالات‌متحده نیز باید همین کار را انجام دهد. البته بده بستان‌ها دشوار خواهد بود؛ مقابله با دخالت‌های خارجی، مانند مبارزه با تروریسم، سیاست‌گذاران را ملزم می‌کند تا با این سؤال اساسی در مورد چگونگی دفاع از ایالات‌متحده، بدون به خطر انداختن ارزش‌های اصلی آن پاسخ دهند. حفاظت از حاکمیت آمریکا باید با اصول اساسی مانند جریان آزاد اطلاعات و عدم تمرکز قدرت متعادل شود. حل این معادله، همیشه آسان نیست اما باید انجام شود.

منبع

این مقاله در آدرس ذیل قابل دسترسی است:
https://www.foreignaffairs.com/articles/russia-fsu/2019-07-23/us-elections-are-still-not-safe-attack

7- DescriptionThe Foreign Agents Registration Act is a United States law passed in 1938 requiring that agents representing the interests of foreign powers in a "political or quasi-political capacity" disclose their relationship with the foreign government and information about related activities and finances