تهدیدهای خارجی برای انتخابات آمریکا
نیازهای امنیت اطلاعات انتخابات

ویلیام آراوانیا در یادداشتی که توسط مرکز ضد جاسوسی آمریکا منتشر شده است، ادعا می‌کند که نهادهای اطلاعاتی خارجی، بیشتر تمایل دارند تا انتخابات آمریکا را به‌عنوان فرصتی برای صدمه زدن به اعتماد به نهادها و فرآیندهای دموکراتیک ما ببینند، بذر تفرقه را در جامعه بکارند، متحدان ما را تضعیف نمایند و اهداف سیاسی، اقتصادی یا ایدئولوژیک خود را پیش ببرند. این نهادها در جریان‌های نظام دموکراتیک ما، فعال هستند تا منافع خود را محقق سازند که در این راستا، از ابزارهای جاسوسی سنتی در کنار عملیات سایبری و نفوذ استفاده می‌کنند.

تلاش‌های خارجی برای مداخله در انتخابات ما، به پنج دسته متمایز تقسیم می‌شود:

۱. عملیات سایبری که زیرساخت انتخابات را هدف قرار می‌دهند؛

۲. عملیات سایبری که احزاب و نهضت‌های سیاسی و همچنین، مقامات را هدف قرار می‌دهد؛

۳. عملیات نفوذ خاموش با هدف کمک یا صدمه زدن به ارگان‌های سیاسی، پویش‌ها یا مسئولان؛

۴. عملیات نفوذ خاموش با هدف تأثیرگذاری بر افکار عمومی و کاشت بذر تفرقه؛

۵. تلاش‌های مخفیانه برای تأثیرگذاری بر سیاست‌گذاران و عموم مردم.

این تهدید، ممکن است اشکال متنوعی به خود بگیرد، مانند ترویج اطلاعات نادرست، انجام عملیات هک و افشای اطلاعات یا احتمالاً تحریف و دست‌کاری داده‌ها به شکلی هدفمند با هدف تأثیرگذاری بر انتخابات. همچنین، تهدید فوق دربردارنده طیفی وسیع‌تر از بازیگران خارجی دولتی و غیردولتی است که ما در گذشته دیده‌ایم تا بدین ترتیب، نهادها و افراد با انگیزه ایدئولوژیک و همچنین، مجرمان سایبری خارجی را نیز شامل شود.

همچنین، پیچیده کردن چشم‌انداز انتخابات، طیفی از ابزار بوده که امروزه در دسترس است و می‌تواند، تأثیر اقدامات دشمنان را بزرگ ساخته و منشأ آن‌ها را بیشتر دچار ابهام نماید؛ گونه‌های

غیرسنتی جاسوسی که در آن‌ها از افسران اطلاعاتی حرفه‌ای برای جمع‌آوری اطلاعات یا دسترسی به زیرساخت‌های حیاتی استفاده نمی‌شود، فناوری‌های نظارتی و حسگرهای جدید، تأمین زنجیره عملیات و به‌صورت غیرمستقیم، سرمایه‌گذاری خارجی مستقیم، سرمایه‌گذاری‌های مشترک و ادغام و تملک تجارت‌ها و تأمین‌کنندگان مرتبط با انتخابات که می‌توانند دشمن را به سیستم‌ها، شبکه‌ها و اطلاعات کلیدی متصل سازند. ادامه پیشرفت فناوری یادگیری ماشین، ما را به‌طور خاص، نگران بازیگران تهدیدکننده خارجی می‌کند که «جعل عمیق» را به خدمت می‌گیرند؛ استفاده از فناوری برای ایجاد تصاویر، ویدئوها و صداهای دروغین اما قانع‌کننده تا بدین ترتیب، حرکت‌های نفوذ را افزایش داده و اعتماد عمومی به انتخابات را از بین ببرند.

مقابله با تهدیدهای پیچیده و گسترده که در این انتخابات، انتظار آن‌ها می‌رود، باید وظیفه اصلی کل دولت آمریکا باشد که مستلزم رویکردی است که کل جامعه را پوشش می‌دهد، ازجمله حمایت از بخش خصوصی و مشارکت فعال از سوی مردمی آگاه. مرکز ضد جاسوسی و امنیت ملّی،[1] همکاری تنگاتنگی با وزارت امنیت داخلی[2]، بخش اجرایی تهدیدهای انتخاباتی دفتر مدیریت اطلاعات ملّی[3]، اف بی آی[4]، اداره تحقیقات فدرال[5] و دیگر نهادهای فدرال دارد تا برنامه‌ها و اقدامات دولت‌های خارجی برای مداخله در انتخابات ایالات‌متحده را برآورد و خنثی نماید. بنده به آن‌ها که درگیر انتخابات هستند، توصیه می‌کنم تا اطلاعات تفصیلی را که حکایت از دخالت احتمالی بازیگران خارجی در انتخابات آمریکا دارند، به وزارت امنیت داخلی یا اف بی آی گزارش دهند. این کار، شامل ارائه یک توضیح مختصر از شرح ماوقع، اینکه چه سیستم‌ها یا فرآیندهایی، تحت تأثیر قرارگرفته‌اند، چه اقداماتی برای کاهش آن‌ها، صورت پذیرفته است و همچنین، میزان مؤثر بودن آن تلاش‌ها می‌شود. اقدامات خصمانه خارجی احتمالی که اهمیت خاصی دارند، در ادامه ذکر شده‌اند.

ویلیام آر اوانیا[6]

مدیر، مرکز ضد جاسوسی و امنیت ملی

نیازهای امنیت اطلاعات انتخابات

۱. ورود یا تلاش غیرمجاز برای دسترسی به مراکز رأی‌گیری و تأسیسات تجمیع و حفظ زیرساخت‌های نظام اخذ رأی و انتخابات، ازجمله آن‌ها که در اماکن خصوصی و عمومی قرار دارند.

۲. رویدادهایی از فیشینگ هدف‌دار یا تلاش برای هک کردن سیستم‌های ثبت‌نام از قبیل حمله به نهادهای به نظر نامرتبط دولتی یا محلی مانند دپارتمان وسایل نقلیه موتوری[7] یا تشکل‌های مدنی که مسئولیت ثبت‌نام رأی‌دهندگان را برعهده دارند.

۳. تلاش برای دسترسی، تحریف یا تخریب سیستم‌هایی که برای صلاحیت سنجی نامزدها، تولید و توزیع برگه‌های رأی، تدارک دیدن،

1. National Counterintelligence and Security Center
2. Department of Homeland Security
3. ODNI Election Threats Executive
4. Federal Bureau of Investigation
5. Federal Bureau of Investigation

6. William R. Evanina
7. Departments of Motor Vehicles

مدیریت کردن و آماده‌سازی تجهیزات رأی‌گیری، فرآیند درخواست برای آرای غایب و ذخیره و مدیریت فرآیندهای اجرایی انتخابات، به کار می‌رود.

۴. دسترسی یا تلاش برای نفوذ غیرمجاز به زیرساخت یا سیستم‌های فناوری اطلاعات که برای مدیریت انتخابات استفاده می‌شود، ازجمله سیستم‌هایی که نتایج انتخابات را شمارش، بررسی یا نمایش می‌دهند و سیستم‌هایی که برای تأیید یا تصدیق نتایج پس از انتخابات، به کار می‌روند.

۵. تلاش برای هک، فیشینگ هدف‌دار یا افشای ایمیل‌های شخصی یا حرفه‌ای و همچنین، حساب‌های شبکه‌های اجتماعی مقامات، کارمندان و داوطلبان فعال در انتخابات.

۶. اقدام موفق یا غیر از آن، برای نفوذ و هک احزاب سیاسی، سیستم‌های فناوری اطلاعات متعلّق به کمپین‌های تبلیغاتی یا دستگاه‌های فناوری اطلاعات شخصی مربوط به نامزدها، کارمندان یا مشاوران و پیمانکاران مرتبط.

۷. اقدام برای دسترسی، هک، تحریف یا مختل کردن زیرساخت‌هایی که آراء غایبان را دریافت یا بررسی می‌کند، مانند مراکز جدول‌بندی، پرتال‌های اینترنتی، ایمیل‌ها یا دستگاه‌های فکس. همچنین، هرگونه تلاش از سوی نهادها یا افراد خارجی برای دخالت در آرایی که از طریق سرویس پست آمریکا ارسال می‌شود.

۸. افشا شدن شبکه‌ها یا سیستم‌های سخت‌افزاری و نرم‌افزاری، توسط بازیگران سایبری همچون تاکتیک‌ها، تکنیک‌ها، فرآیندها و تأثیر بر شبکه‌ها و سیستم‌های مرتبط با انتخابات. به‌علاوه، هر نشانه‌ای که از مداخله در شبکه‌ها یا سیستم‌های دولتی حکایت می‌کند یا شاخصه‌های امنیت سایبری برای افشای اطلاعات.

۹. نمونه‌های هرگونه اختلال در مراکز اخذ رأی یا مکان‌های آموزش افراد مسئول در صندوق‌های رأی، ازجمله مکان‌های رأی‌گیری اولیه که باعث تغییر در میزان حضور رأی‌دهندگان می‌شود. اختلالات می‌تواند شامل پست‌ها در شبکه‌های اجتماعی، پیام‌های متنی یا پیام‌های ضبط شده باشد که به شکلی نادرست و غلط تغییر یافتن یا بسته شدن مکان‌های اخذ رأی را گزارش می‌کنند، همچنین، وقایع فیزیکی در مکان‌های رأی‌گیری ازجمله انتشار اطلاعات غلط در آنجا باشد. سایر اختلالات عبارت است از

سرقت برنامه‌های تلویزیونی یا تحریف برونداد آنلاین داده‌های رأی‌گیری.

۱۰. تلاش‌های دشمن خارجی برای انتشار اطلاعات نادرست ازجمله در شبکه‌های اجتماعی، وب‌سایت‌ها یا سایر منابع اینترنتی با هدف تحریف یا بستن وب‌سایت‌های دولتی و انتشار محتوای «جعل عمیق» برای دامن زدن به آشوب اجتماعی، تأثیرگذاری بر افکار، تصمیم‌ها یا اقدامات رأی‌دهندگان و تحریف میزان مشارکت در انتخابات.

۱۱. ورود غیرمجاز به مناطق شمارش یا بازخوانی آراء و همچنین، سیستم‌ها یا شبکه‌های الکترونیکی که توسط دولت‌ها و مسئولان محلی برای شمارش برگه‌های رأی غایبان، نظامیان و روز انتخابات استفاده می‌شود.

۱۲. اقدامات در راستای تأثیرگذاری بر زیرساخت‌های حیاتی که باعث محدودیت دسترسی به مکان‌های اخذ رأی می‌شود، مانند قطع برق، آب، اینترنت، تلفن و حمل‌ونقل (کنترل‌های ترافیکی).

۱۳. رفتارهای مشکوک اعضای خارجی تیم‌های نظارتی انتخابات، مانند آن‌ها که با مأموریت نظارتی سازمان امنیت و همکاری اروپا[1] برای انتخابات سال ۲۰۲۰ آمریکا مرتبط هستند؛ ازجمله بررسی مسائلی که ناظر بر مسئولان برگزاری انتخابات بوده که خارج از دامنه مأموریت و وظیفه ناظر است.

۱۴. هر نشانه‌ای مبنی بر اینکه دشمنان، به‌خصوص روسیه و چین، مشغول جمع‌آوری یا تحلیل برنامه‌های ایالت‌های آمریکا با هدف به خدمت گرفتن فناوری بلاک چین در انتخابات این کشور هستند.

۱۵. تلاش‌های مستقیم یا غیرمستقیم، موفق یا غیر از آن، توسط نهادها و افراد شناخته‌شده و مشکوک، به‌منظور لابی‌گری یا صرف هزینه برای انتخاب نامزدها و احزاب سیاسی یا سازمان‌های اقدام سیاسی در تلاش برای شکل‌دهی به نتیجه انتخابات که بالقوّه، نقض قوانین مالی برنامه‌های انتخاباتی آمریکا محسوب می‌شود.

۱۶. اقدامات مستقیم یا غیرمستقیم توسط نهادها و افراد خارجی شناخته شده یا مظنون و آن‌ها که با خارجی‌ها مرتبط هستند، به‌منظور بی‌اعتبار کردن یا ایجاد تردید نسبت به شهرت یا صلاحیت یک نامزد و حزب سیاسی با استفاده از داده‌های افشا شده (واقعی، تحریف‌شده یا ساختگی).

۱۷. فعالیت‌ها و ارسال پیام‌های مستقیم یا غیرمستقیم توسط سازمان‌های نیابتی خارجی مستقر در آمریکا، با هدف بسیج رأی‌دهندگان و در برگرفتن تجارت و شرکت‌های آمریکایی در سطح محلی، دولتی و ملی، برای حمایت از یک حزب یا نامزد سیاسی خاص.

۱۸. تلاش‌های خارجی شناخته شده یا مشکوک برای ترویج، حمایت پنهانی یا مجزا از نهضت‌های ایدئولوژیک فرعی یا گروه‌های ضد دستگاه حاکمه آمریکا به‌منظور کاشتن بذر نارضایتی اجتماعی.

منبع: مرکز ضد جاسوسی و امنیت ملی

نویسنده: ویلیام آر اوانیا

مترجم: هادی قربانیار

[1]. Organization for Security Cooperation in Europe