گسترش بحران ایران به فضای سایبری

به قلم مایکا لودرمیلک (/fa/experts/mayka-lwdrmylk)

۹ ژوئیهٔ ۲۰۱۹
همچنین دست‌یافتنی به
(English (/policy-analysis/iran-crisis-moves-cyberspace /
العربیة (/ar/policy-analysis/alazmt-alayranyt-tntql-aly-alfda-alsybrany/)

درباره نویسنده

مایکا لودرمیلک (/fa/experts/mayka-lwdrmylk)

مایکا لودرمیلک مشاور امنیت سایبری مستقر در خاورمیانه و تحلیل‌گر ژئوپلتیک است. هر گونه نظر ابرازشده در این‌جا نظرهای خود نویسنده است.

تحلیل کوتاه

دست‌اندرکاران فضای سایبری ایران علایمی نشان می‌دهند که حاکی از آماده شدن برای نبردی سایبری است در نتیجه ایالات متحده آمریکا باید از حملات گذشته درس بگیرد و موضع دفاعی‌اش را تقویت کند.

تنش‌های فزاینده در خلیج فارس به‌تازگی جنبه‌ای سایبری پیدا کرده است: ایالات متحده در واکنش به ساقط کردن پهپادش به سامانه‌های کامپیوتری نظامی ایران حمله کرده است و از قرار هکرهای دولت ایران هم عملیات جاسوسی سایبری را فعال‌تر کرده و سازمان‌های آمریکایی را هدف قرار داده‌اند. تهران پیش‌تر هم در عرصه سایبری در برابر آمریکا دست به اقدامات تلافی‌جویانه زده است. این عرصه به دلیل آن که موانع ورودش پایین‌تر بوده فضای بازی متقابل را همسطح‌تر می‌کرده است و از طرف دیگر چون آمریکا سطح گسترده‌تری از فضای سایبری در اختیار داشته برای هدف قرار گرفتن در موضع ضعیف‌تری هم بوده است. حال که ایران علایمی حاکی از پی‌گیری این شگرد سابق را نشان می‌دهد دولت آمریکا و بخش خصوصی باید گام‌های مناسبی را برای تقویت دفاع سایبری بردارند.

مروری بر حملات سایبری تلافی‌جویانه ایران

هر وقت که ایران عملیاتی سایبری را در واکنش به درگیری‌ها و تنش‌های گذشته یا به تصور اینکه هدف حمله بوده انجام داده است عملیات‌اش را به شکلی تنظیم کرده که هزینه‌هایی ملموس به بار آورد و دسترسی استراتژیک‌اش را به رخ بکشد و در عین حال بتواند از اهرم «انکار قابل باور» استفاده کند و از بالا گرفتن تنش‌ها بپرهیزد. از حملات قابل توجه ایران یکی عملیات ابابیل در سال‌های ۲۰۱۲-۲۰۱۳ علیه نهادهای مالی آمریکاست و دیگری حمله موسوم به شمعون در سال ۲۰۱۲ علیه آرامکو غول نفتی سعودی و همچنین حمله سال ۲۰۱۴ علیه شرکت سندز در لاس وگاس.

عملیات ابابیل در زمانی اجرایی شد که واشنگتن تحریم‌های بیشتری علیه بانک مرکزی ایران و دیگر نهادهای ایران وضع کرده بود و ایران از حمله گسترده محروم‌سازی از سرویس (مشهور به دی-داس DDoS) برای ایجاد اختلال در پلتفرم‌های بانکداری آنلاین استفاده کرد. حملات دی-داس ابتدایی هستند اما عملیات ابابیل حمله هدفمند و مؤثری بود که موقتا کارکردهای تجاری یکی از ستون‌های اقتصادی آمریکا را مختل کرد و باعث ده‌ها میلیون دلار خسارت شد. هرچند یک گروه هکر-کنشگر (یا هکتیویست) به نام جنگ‌جویان سایبری عزالدین قسام مسؤولیت حمله را به عهده گرفت این حملات تقریبا به طور قطع با اجازه حکومت ایران انجام شده بود.

حملات آرامکو و سندزِ لاس وگاس از دستور کار مشابهی تبعیت می‌کردند. هرچند گروه‌های هکر-کنشگری با انگیزه‌های سیاسی مدعی آن‌ها شدند هر دو عملیات با ایران مرتبط بود و به تحولات خاصی ربط داشت که تهران آن‌ها را تهدید قلمداد می‌کرد. شمعون پس از شدت گرفتن تحریم‌های نفتی آمریکا و کشف عملیات سایبری علیه زیرساخت‌های هسته‌ای ایران رخ داد حمله سندز پس از آن رخ

داد که صاحب شرکت سندز یعنی شلدون ادلسون حامی مالی جمهوری‌خواهان از حمله پیش‌دستانه هسته‌ای علیه ایران حمایت کرده بود.

این حملات تقریبا همزمان رخ داد ولی حملات به شرکت‌های سعودی و آمریکایی از حیث مخرب بودن تفاوت‌های زیادی داشتند. شمعون در زمره خسارت‌بارترین حملات سایبری بود که تا به حال گزارش شده و بیش از ۳۰ هزار کامپیوتر را تخریب کرد و بخش‌های وسیعی از زیرساخت فناوری اطلاعات آرامکو را پاک کرد که باعث به زانو در آوردن عملیات تجاری شرکت شد. این حملات را چه بسا فردی نفوذی تسهیل کرده بود که اطلاعات شبکه و بالا بردن سطح دسترسی را (برای حمله‌کنندگان) فراهم کرده بود وجود یک نفوذی احتمالا روشنگر این نکته هم هست که چرا یک شرکت سعودی به تلافی اقدامات آمریکا هدف قرار گرفت.

در مقایسه با آن عملیات ابابیل اثرش به‌مراتب کمتر بود و موقتا بعضی از بانک‌های آمریکایی را آفلاین کرد و دسترسی مشتریان را با اختلال روبه‌رو ساخت. مطمئنا حملات دی-داس در مقیاس گسترده‌ای انجام شده بود –و به آستانه ۷۰ گیگابایت در ثانیه می‌رسید که با معیارهای سال ۲۰۱۲ خیلی شاخص بود– اما در مقایسه با شمعون کمرنگ جلوه می‌کند موضوعی که بالقوه نشان می‌دهد تصمیم ایران حساب‌شده بود تا ضمن وارد کردن خساراتی قابل توجه به ایالات متحده از صدمات سنگینی که منجر به خطر تلافی شود پرهیز کند.

ارزیابی گزینه‌های سایبری ایران

عملیات سایبری آینده ایران علیه ایالات متحده احتمالا به شکل حملاتی هدفمند و تنظیم‌شده علیه شرکت‌های تجاری یا ستون‌های مهم اقتصادی خواهد بود با این هدف که صدمه بزند خسارات مالی وارد کند و جریان زندگی یا عملیات تجاری آمریکایی‌ها را مختل سازد. دانش روبه‌رشد ایران در زمینه حملات بدافزار (ویروس‌های پاک‌کننده اطلاعات دیسک) –در کنار اطلاعات تجسسی که از عملیات مستمر جاسوسی سایبری حاصل کرده– می‌تواند نهادهای آمریکایی بسیار بیشتری را در معرض خطر قرار دهد و توانایی واشنگتن را برای شناسایی اهداف احتمالی به چالش بگیرد.

بحران جاری تا همین‌جا هم شاهد عملیات سایبری از هر دو سو بوده است. ماه گذشته پس از این‌که رژیم ایران یک پهپاد آر.کیو4 (RQ-4) را ساقط کرد ایالات متحده آمریکا حملاتی سایبری علیه سامانه‌های تسلیحاتی ایران به راه انداخت. پخته‌تر شدن توانمندی‌های ایران و عملیات پایدار جاسوسی‌اش حاکی از خطر قابل توجهی است که نهادهای آمریکایی در معرض آن قرار دارند. همزمان شرکت‌های امنیت سایبری نیز ناظر آمادگی دست‌اندرکاران سایبری ایران برای نبرد در میدان سایبری بوده‌اند و این می‌تواند نشانه‌ای باشد از اتفاقاتی که در راه است.

در سال‌های ۲۰۱۲-۲۰۱۴ توانمندی‌های سایبری ایران چندان پیشرفته نبود و در نتیجه حملات‌اش به طور معمول اتفاقاتی منفرد بود تا حملاتی مستمر. اما امروزه تهران این حملات را خیلی بیشتر مانند چین روسیه و آمریکا هدایت می‌کند یعنی عملیات‌های کاوش و جاسوسی درازمدتی را انجام می‌دهد که اطلاعات تجسسی و دسترسی در اختیارش می‌گذارد (مثلا دسترسی به اطلاعات و اسناد شخصی و نقشه‌های شبکه و آسیب‌پذیری‌ها). طی دو سال گذشته شرکت‌های امنیتی و دولت آمریکا عملیات‌های سایبری ایران را که هدف‌اش جاسوسی از نهادهای دولتی آمریکا زیرساخت‌های حساس سازمان‌های هوانوردی نظامی/تجاری تولیدات کارخانجات شیوه مهندسی و دیگر بخش‌ها بوده شناسایی کرده‌اند. هکرهای ایران همچنین بنا به گزارش‌ها سامانه نام دامنه‌های اینترنت را هدف قرار داده‌اند و از سرویس‌دهندگان اینترنتی و شرکت‌های مخابراتی داده‌هایی را به دست آورده‌اند که می‌تواند حملات آینده را تسهیل کند.

اگر ایران حملات سایبری مختل‌کننده‌اش را شدت دهد می‌تواند شبکه برق آمریکا (که پیش‌تر هم به آن نفوذ کرده بود) شبکه‌های آب (که به آن هم رخنه کرده بود) سامانه‌های مخابراتی (که از آن‌ها داده‌هایی را استخراج کرده) یا حتی مدیریت شهرها را هدف قرار دهد. سال گذشته وزارت دادگستری دو نفر ایرانی را به خاطر حمله باج‌افزاری علیه شهر آتلانتا متهم کرد. هرچند آن دو ارتباطی با دولت ایران نداشتند حملات مخرب یا انحرافی باج‌افزاری کاملا در حیطه توانمندی‌های تهران قرار دارد. متحدان آمریکا در منطقه خلیج نیز ممکن است به نحو مشابهی هدفی آسان برای هکرهای ایرانی باشند به‌ویژه عربستان سعودی که حداقل از سال ۲۰۱۳ مرتب هدف حمله یا نفوذ بوده است.

از آن‌جا که آمریکا از روش‌های سایبری برای پاسخ به یک حمله ایران که با خسارت مادی همراه بوده (سقوط پهپاد) استفاده کرده است رهبران ایران شاید دلیل چندانی برای خویشتنداری استراتژیک در فضای سایبری نبینند. در واقع اگر پاسخ آمریکا خویشتندارانه باشد می‌تواند باعث جری‌تر شدن تهران شود تا دست به اقدامات تهاجمی‌تری در این عرصه بزند چرا که فکر می‌کند واشنگتن برای اقدام در سایر عرصه‌های نظامی اکراه دارد. ابراز تردید مکرر رئیس‌جمهور ترامپ و نفی اینکه حملات سایبری علیه آمریکا از خارج صورت گرفته هم می‌تواند باعث تشویق بیشتر ایرانی‌ها به اقدام شود چنان‌که این اظهارات او که: ساقط کردن پهپاد شاید به‌اشتباه صورت گرفته باشد.

کاهش ریسک سایبری امریکا

شرکت‌های بخش خصوصی مالک و مجری بیشتر شبکه‌های حساس زیرساختی در آمریکا هستند که باعث می‌شود این شبکه‌ها خارج از حوزه اختیارات مستقیم شبکه فعالیت‌های دفاعی دولت قرار گیرد. در عین حال سیاست‌گذاران می‌توانند گام‌های متعددی برای تقویت مواضع دفاع سایبری آمریکا بردارند و بالقوه حملات ایران را از طریق نمایش قدرت در فضای مجازی تضعیف کنند.

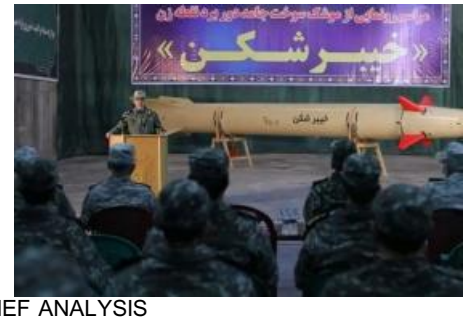
یکی از این گام‌ها آن است که اطلاعات بیشتری را در مورد اهداف بالقوه در بخش خصوصی با آنها به اشتراک بگذارند تا به آن‌ها کمک کند زیرساخت‌ها و ذخایر حساس را تقویت کنند. در حال حاضر سازمان‌های اطلاعات تجسسی با عزم راسخ اطلاعات تهدید سایبری را طبقه‌بندی محرمانه می‌کنند و استدلال آن‌ها این است که این روش برای حفاظت از منابع روش‌ها و ابزارها حیاتی است. اما چنین سیاست‌هایی مانع از این می‌شوند که نهادهای آسیب‌پذیر بتوانند اطلاعات حیاتی مورد نیازشان را برای ممانعت یا کاستن از اثر حملات سایبری به دست آورند. دولت اوباما گام‌های نخست (**https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari**) را برای حل این مشکل در سال ۲۰۱۵ برداشت ولی کارهای بیشتری لازم است تا یا اطلاعات مرتبط از طبقه‌بندی محرمانه خارج شود یا گزارش‌های توجیهی درباره آن بخش از اطلاعات محرمانه ارایه شود که به تهدید شرکت‌های دست‌اندرکار زیرساخت‌های حساس خارج از بخش دفاعی مربوط است. نهادهای خصوصی با دسترسی داشتن به اطلاعات محرمانه مناسب می‌توانند از خود در برابر حملات دفاع کنند –چنان‌که در طول عملیات ابابیل دیدیم وقتی که بانک‌ها مواضع دفاعی‌شان را به طور متناسب تغییر دادند تلاش هکرهای ایرانی به‌تدریج رنگ باخت.

علاوه بر این وقتی عوامل دست‌اندرکار نسبت به توانمندی‌های آمریکا کور باشند بازدارندگی سایبری دشوار است. معنای این سخن این نیست که آمریکا باید تمام جعبه‌ابزار سایبری‌اش را افشا کند. اما سازمان‌های اطلاعات تجسسی می‌توانند گام‌های معینی بردارند تا به ایران نشان دهند دسترسی‌شان به فضای سایبری ایران چقدر است و شواهدی ارایه دهند که ایران بداند کدام ذخایر آن‌ها در شبکه می‌تواند در معرض خطر حمله قرار گیرد. به همین ترتیب آمریکا می‌تواند مستقیما سراغ هکرهای ایرانی در شبکه‌های خودشان برود و نشان بدهد که فعالیت‌های آن‌ها را در لحظه انجام آن رصد می‌کند. این تاکتیک سابقه دارد چنان‌که فرماندهی سایبری آمریکا عملیات مشابهی را علیه عاملان روسی نشردهنده اطلاعات جعلی در سال گذشته انجام داد. چنین کارهایی لازم نیست عمومی و پُرسروصدا انجام شود در واقع نمایش قدرت بی‌سروصدا می‌تواند مؤثرتر باشد و هم توانمندی‌های آمریکا را به رخ بکشد و هم علاقه واقعی واشنگتن را به کاهش تنش نشان بدهد. هرچند این عرض اندام‌ها به‌خودی‌خود راه‌حل‌هایی درازمدت نیستند ولی می‌توانند ایران را وادارند تا در حملات سایبری ارزیابی مجددی از سود و زیان حمله انجام دهد.

نکته آخر این‌که سیاست‌گذاران باید وقتی خط قرمزها را در مورد تلافی کردن حملات سایبری ترسیم می‌کنند دقت به خرج دهند. ایالات متحده نمی‌خواهد طوری رفتار کند که ایران تصور کند چنین حملاتی بی‌هزینه است. اما اعلام خط قرمز مشخص می‌تواند گزینه‌های واکنش آمریکا را محدود کند و یا در صورتی که نتواند پس از هر تحریک سایبری ایران آن را به دقت شناسایی یا کاملا حساب‌کشی کند به اعتبار آمریکا صدمه بزند.

**مریکا لودرمیلک مشاور امنیت سایبری مستقر در خاورمیانه و تحلیل‌گر ژئوپلتیک است. هر گونه نظر ابرازشده در این‌جا نظرهای خود نویسنده است.* ❖

RECOMMENDED



BRIEF ANALYSIS

Iran Takes Next Steps on Rocket Technology

فوریهٔ ۲۰۲۲ ۱۱

◆

Farzin Nadimi

(/policy-analysis/iran-takes-next-steps-rocket-technology)

BRIEF ANALYSIS

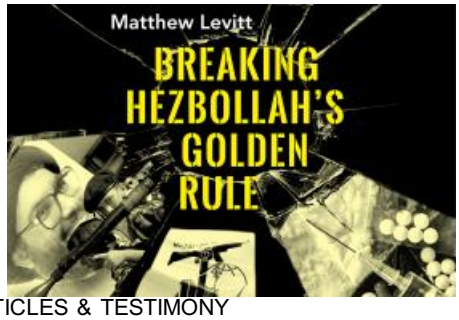
Saudi Arabia Adjusts Its History, Diminishing the Role of Wahhabism

فوریهٔ ۲۰۲۲ ۱۱

◆

Simon Henderson

(/policy-analysis/saudi-arabia-adjusts-its-history-diminishing-role-wahhabism)



ARTICLES & TESTIMONY

Podcast: Breaking Hezbollah's Golden Rule

فوریهٔ ۲۰۲۲ ۹

◆

Matthew Levitt

(/policy-analysis/podcast-breaking-hezbollahs-golden-rule)

TOPICS

انرژی و اقتصاد **(/fa/policy-analysis/anrzhy-w-aqtsad)**

خلیج و سیاست حوزه انرژی **(/fa/policy-analysis/khlyj-w-syast-hwzh-anrzhy)**

نظامی و امنیتی **(/fa/policy-analysis/nzamy-w-amnyty)** تروریسم **(/fa/policy-analysis/trwrysm)**

REGIONS & COUNTRIES

ایران **(/fa/policy-analysis/ayran)** کشورهای حاشیهخلیج فارس **(/fa/policy-analysis/kshwrhay-hashyhkhlyj-fars)**