تهدید سایبری ایران:

جاسوسی،

خرابکاری

و انتقام

نویسندگان:
کالین اندرسن و کریم سجادپور

گاهشمار

ژانویه ۱۹۹۲- ایران برای نخستین بار به اینترنت وصل می شود.

سال ۲۰۰۰- دسترسی به اینترنت بطور فزاینده ای مرسوم می شود و صدها هزار ایرانی مرتباً از اینترنت استفاده می کنند.

سال ۲۰۰۱- شورای عالی انقلاب فرهنگی مقرراتی در خصوص دسترسی به اینترنت صادر می کند، از جمله فیلترینگ اجباری و نظارت بر وبسایت هایی که به لحاظ سیاسی، فرهنگی و مذهبی برانداز به شمار می روند.

فوریه ۲۰۰۲- انجمن هکرهای آشیانه تشکیل و به عامل شتاب دهنده انجمن هکرهای ایران تبدیل می شود. این انجمن بعدها متهم به تسهیل سرکوب مخالفان توسط دولت ایران می شود.

آوریل ۲۰۰۳- سینا مطلبی بازداشت می شود؛ او یکی از نخستین وبلاگ نویسان در جهان بود که به دلیل نوشته هایش در فضای مجازی بازداشت شد؛ این آغاز سرکوب آزادی بیان در اینترنت است.

ژوئن ۲۰۰۵- محمود احمدی نژاد تندرو، به عنوان رئیس جمهور ایران انتخاب و دوره جدیدی از سرکوب داخلی و خصومت های بین المللی آغاز می شود.

سال ۲۰۰۷- عاملان تهدیدکننده ایرانی شروع به ایجاد ابزار و اجرای کمپین می کنند.

ژوئن ۲۰۰۹- انتخاب مجدد و جنجال برانگیز محمود احمدی نژاد منجر به بزرگترین قیام مردمی از سال ۱۹۷۹ به بعد می شود که به جنبش سبز معروف است.

دسامبر ۲۰۰۹- ارتش سایبری ایران در واکنش به جنبش سبز، وبسایت توییتر را تخریب کرد و آن را به مدت چند ساعت از کار انداخت.

سپتامبر ۲۰۱۱- یک هکر ایرانی به شرکت امنیتی هلندی DigiNotar نفوذ کرد و این امکان را برای دولت ایران فراهم آورد تا از کاربران جی میل در ایران جاسوسی کند. این موضوع یکی از بزرگترین نفوذهای امنیتی در تاریخ اینترنت به شمار می رود.

آوریل ۲۰۱۲- زیرساخت نفتی ایران با بدافزارهای مخرب Flame و Wiper هدف قرار گرفت.

ژوئن ۲۰۱۲- خبرنگار نیویورک تایمز، دیوید سنگر، جزئیات «عملیات بازی های المپیک» را منتشر می کند. این عملیات یکی از پیچیده ترین حملات سایبری در تاریخ است که ایالات متحده و اسرائیل در سال ۲۰۰۷ اجرا کردند تا بطور مخفیانه زیرساخت های هسته ای ایران را تخریب کنند.

ژوئیه ۲۰۱۲- عامل بدافزار Madi ، نخستین کمپین سایبری جاسوسی که به ایران نسبت داده شده، افشا می شود.

اوت ۲۰۱۲- داده های اطلاعاتی شرکت Saudi Aramco، بزرگترین شرکت نفتی جهان، با عامل بدافزار «شامون» از میان می رود.

سپتامبر ۲۰۱۲- نخستین حملات منع سرویس دهی، معروف به «عملیات ابابیل»، علیه بانک های ایالات متحده صورت می گیرد.

ژوئن ۲۰۱۳- حسن روحانی، روحانی عملگرا، با قول بهبود اقتصاد ایران از طریق حل بن بست هسته ای، به عنوان رئیس جمهور ایران انتخاب می شود.

نوامبر ۲۰۱۳- اعلام مذاکرات هسته ای بین ایالات متحده، چین، روسیه، انگلستان، فرانسه، و آلمان با ایران، که منجر به توافق موقت می شود.

ژوئیه ۲۰۱۵- توافق هسته ای نهایی تحت عنوان برنامه جامع اقدام مشترک (برجام) نهایی می شود.

نوامبر ۲۰۱۶ تا ژانویه ۲۰۱۷- حملات سایبری علیه عربستان سعودی در «شامون ۲» تجدید می شود.

خلاصه

حملاتی که ایران در آن شرکت داشته از پیچیده ترین، پرهزینه ترین و چشمگیرترین حملات در تاریخ اینترنت بوده است. جنگ سرد ایالات متحده و ایران که چهار دهه بطول انجامیده، بطور فزاینده ای به فضای سایبری منتقل شده و تهران یکی از اهداف عمده عملیات سایبری مخرب و منحصر به فرد تهاجمی از سوی ایالات متحده و متحدانش بوده است. همزمان، تهران در اجرای عملیات جاسوسی سایبری و حملات مختل کننده علیه مخالفان در داخل و خارج از کشور- از سازمان های جامعه مدنی گرفته تا نهادهای دولتی و تجاری در اسرائیل، عربستان سعودی و ایالات متحده تخصص یافته است.

محیط تهدیدات سایبری ایران

- عملیات تهاجمی سایبری به ابزار اصلی کشورداری در ایران تبدیل شده است که فرصت های کم خطرتری را برای تهران فراهم می آورد تا به جمع آوری اطلاعات و عملیات تلافی جویانه علیه دشمنان در داخل و خارج از کشور بپردازد.

- همانگونه که ایران به منظور نمایش قدرت منطقه ای خود از نیروهای نیابتی استفاده می کند، اغلب با استفاده از پراکسی ها، عملیات سایبری خود را پنهان می کند تا بتواند رسماً مسئولیت خود را انکار کند. اما نشانه های مشخصی وجود دارد که چنین عملیاتی از سوی ایران انجام شده و اغلب با دستگاه های امنیتی کشور، یعنی وزارت اطلاعات و سپاه پاسداران انقلاب اسلامی مرتبط است.

- به نظر می رسد توانایی های سایبری ایران بطور بومی توسعه یافته و خاستگاه آن دانشگاه های داخل کشور و جوامع هکرها باشد. این اکوسیستم منحصر بفرد است و گردانندگان متنوع هماهنگ با دولت را در برمی گیرد که از وابستگی ها و توانایی های متفاوت برخوردارند. طی یک دهه اشتغال ایرانیان در عملیات سایبری، عاملان تهدیدکننده ناگهان پدیدار شده اند، عملیات خود را با شدت و حدت تمام انجام داده اند تا زمانی که کمپین های آنان، اغلب به دلیل افشاگری پژوهشگران، از هم پاشیده است.

- اگرچه ایران عموما قدرت سایبری درجه سه دانسته می شود و از توانایی های چین، روسیه و ایالات متحده برخوردار نیست، اما این کشور از عدم آمادگی اهداف خود در داخل و خارج از ایران سوءاستفاده کرده است. همانطور که نفوذ روسیه به نهادهای حزب دمکراتیک طی انتخابات ریاست جمهوری ایالات متحده در سال ۲۰۱۶ نشان داد که جنگ اطلاعاتی را می توان از طریق تاکتیک های ساده انجام داد، ابزارهای ساده ایران هزینه های سیاسی و مالی هنگفت به دشمنانی تحمیل کرده که انتظار آن را نداشته اند.

- همان عاملان ایرانی که مسئول جاسوسی علیه بخش خصوصی هستند، نظارت بر مدافعان حقوق بشر را نیز بر عهده دارند. حملات علیه جامعه مدنی اغلب حاکی از تاکتیک ها و ابزاری است که علیه دیگر اهداف مورد استفاده قرار خواهند گرفت و خطرات موجود از سوی جنگ سایبری ایران را بهتر نشان می دهد.

- از طریق بررسی تکنیکی دقیق حملات سایبری، پژوهشگرانی که این کمپین ها را به ثبت می رسانند می توانند روزنه منحصر به فردی به جهان بینی و توانایی های نیروهای امنیتی ایران و همچنین چگونگی واکنش آن به محیط فن آوری و ژئوپلیتیکی به سرعت در حال تغییر فراهم آورند.

واکنش های ایالات متحده در آینده

- در حالی که ایران یک سیاست استراتژیک کلی در خصوص فضای سایبری ندارد، سوابق آن حاکی از منطقی در خصوص زمان و دلیل اجرای چنین حملاتی است. ایران از توانایی های خود در واکنش به حوادث داخلی و بین المللی سود می برد. همانطور که درگیری بین تهران و واشنگتن پس از توافق هسته ای سال ۲۰۱۵ فروکش کرد، چرخه حملات مختل کننده نیز کاهش پیدا کرد. با این همه، روند تصمیم گیری در ایران مشخص نیست، و توانایی های سایبری اش را ریاست جمهوری- همانگونه که در موارد هک کردن های درون دولتی مشهود است- کنترل نمی کند.

- فضای سایبری که ایالات متحده بر آن متکی است، به اندازه کافی تحت محافظت قرار ندارد. باید انتظار داشت که مناقشات آینده- چه آنلاین و چه آفلاین- موجب آغاز حملات سایبری علیه زیرساخت های ایالات متحده شود. اولویت نخست باید گسترش تلاش ها در جهت حفاظت از زیرساخت ها و مردم باشد، از جمله همکاری فزاینده با شرکای منطقه ای و سازمان های غیردولتی که از سوی ایران هدف قرار گرفته اند.

- با استفاده از تحریم های دقیقاً هدفمند می توان کشورهای خارجی یا سایر عاملان را از ارائه کمک به عملیات سایبری تهاجمی ایران باز داشت. چنین محدودیت هایی باید همچنان امکان دسترسی گسترده جامعه ایران به اینترنت و فن آوری های اطلاعاتی در اولویت قرار دهد تا به این ترتیب، توان رژیم در کنترل اطلاعات و ارتباطات کاهش یابد.

- ایالات متحده از استراتژی اعلام اسامی و بی آبرو کردن عاملان تهدیدکننده ایرانی استفاده کرده و باید همچنان به این کار ادامه دهد. وزارت دادگستری کیفرخواست هایی علیه ایرانیانی صادر کرده که متهم به شرکت در کمپین های مختل کننده بوده اند، و موفق شده حکم استرداد هکری را که در سرقت اسرار نظامی دخالت داشته از یک کشور ثالث بدست آورد. به دلیل جاپای کوچک عملیاتی این گروه ها، تحریم های هدفمند یا پیگردهای قانونی

بیشتر حالت نمادین دارند تا مختل کننده. این کیفرخواست ها ممکن است دست کم موجب ترس از مشارکت افراد با استعدادی که مایل به سفر یا مهاجرت هستند در این عملیات بشود.

- ایران همچنان منافع خود را از طریق عملیات سایبری دنبال کرده و دست به عملیات علیه مخالفان منطقه ای و جاسوسی علیه دولت های خارجی می زند. درک بهتر سوابق و دلایل استراتژیک فعالیت های سایبری ایران، برای ارزیابی موضع گسترده تر جنگ سایبری واشنگتن علیه دشمنان و همچنین واکنش های محتاطانه ایالات متحده به تهدیدات سایبری آینده از سوی ایران و دیگر کشورها بسیار حائز اهمیت است.

مقدمه

در جنگ سرد بین ایالات متحده و ایران که چهار دهه از عمر آن می گذرد، فضای سایبری به یکی از تازه ترین جبهه ها تبدیل شده است. جمهوری اسلامی ایران شاید بیش از هر حکومت دیگری در جهان، هدف حملات سایبری منحصراً مخرب ایالات متحده و متحدانش قرار گرفته است. در عین حال، گروه های وابسته به نیروهای امنیتی ایران- یعنی سپاه پاسداران انقلاب اسلامی و وزارت اطلاعات- در اجرای عملیات تهاجمی سایبری خود به طرز فزاینده ای مهارت یافته اند. اهداف چنین عملیاتی مخالفان دولت ایران در کشور و خارج از آن، شرکت ها و سازمان های غیردولتی و همچنین نهادهای اقتصادی، دفاعی و دیپلماتیک کشورهای مختلف، از جمله آلمان، اسرائیل، عربستان سعودی و ایالات متحده را در برمی گیرد.

حکومت ایران آشکارا روایت های متناقضی درباره عملیات تهاجمی سایبری خود ارائه کرده است و به این ترتیب به تبلیغ توانایی هایی اش پرداخته، اما در عین حال مسئولیت حملات نسبت داده به خود را به عهده نگرفته است. تهران که پیوسته از گروه های نیابتی استفاده کرده تا قدرت خود در منطقه را به نمایش بگذارد، اغلب دست داشتن در چنین عملیاتی را با استفاده از واسطه ها می پوشاند تا مانع از انتساب آنها به خود شود و تکذیبی موجه ارائه کند. به رغم این تکذیب ها، ایران در توانایی های بومی سایبری آشکارا هم برای اهداف تهاجمی و هم تدافعی خود سرمایه گذاری کرده و مایل است تا در صورت مناقشه از آنها استفاده کند.

قابلیت های تهاجمی سایبری تهران در مقایسه با کشورهایی چون چین، روسیه و ایالات متحده نسبتاً ساده و ابتدایی است. با وجود آنکه ایران از اوایل دهه ۲۰۰۰ شروع به هک کردن سایت ها کرد، اما تا پیش از سال ۲۰۰۷ مدرکی دال بر فعالیت های سایبری وابسته به دولت وجود ندارد. این آغاز نسبتاً دیرهنگام و کم سرمایه تا حدودی دلیل توانایی های اندک این کشور در این خصوص است. اما نفوذ مسکو به نهادهای حزب دمکرات و گردانندگان سیاسی طی انتخابات سال ۲۰۱۶ ایالات متحده نشان داد که جنگ های اطلاعاتی را می توان از طریق راهکارهای ابتدایی هم اجرا کرد. ایران نیز به همین ترتیب از نقایص یا عدم آمادگی اهداف آسیب پذیر هم در داخل کشور و هم خارج از آن، از جمله شرکت های نفتی سعودی، کشورهای خاورمیانه و بانک های ایالات متحده سوء استفاده کرده است. هر چند که این عملیات اغلب به زیان های بزرگ مالی منجر شده، اما شیوه های استفاده شده برای نابودسازی داده ها یا ایجاد اختلال در دستیابی به سایت ها نسبتاً ساده بوده است.

ایران نشان داده که کشورهایی که به لحاظ نظامی ضعیف ترند می توانند در مبارزه با دشمنان پیشرفته خود از عملیات تهاجمی سایبری استفاده کنند. عملیات تهران علیه منافع خارجی بیش از آنکه دزدی اقتصادی باشد، عمدتاً جاسوسی و خرابکاری در کمپین های ضد اهداف نرم در کشورهای رقیب بوده است. تهران به صورت مکرر از حملات مخرب و

ویران کننده استفاده کرده تا توانایی خود در تحمیل هزینه های انتقام جویانه به دشمنان را نشان دهد. به طور کلی، به نظر می رسد که این حوادث اخلال گرانه بر اساس محاسبات راهبردی و محدود به اقدامات تلافی جویانه در همان حوزه های مربوط به زمان مناقشه بوده است.

با این همه، اکثر قربانیان عملیات سایبری ایران یا ساکن ایران یا انبوه ایرانیان مهاجر هستند- کسانی که رهبران کشور آنها را به اصطلاح دشمنان داخلی قلمداد می کنند و از آنها می ترسند. بکارگیری زودهنگام و مؤثر اینترنت و شبکه های اجتماعی از سوی مخالفان و منتقدان رژیم این تصور را در تندروهای تهران پدید آورده که نیروهای خارجی درصدد توطئه برای براندازی جمهوری اسلامی از طریق فن آوری های جدید هستند. اما اهداف نظارت دیجیتالی تهران تنها محدود به مدافعان حقوق بشر و کسانی نیست که از نظر رژیم دشمن تلقی می شوند، بلکه نهادهای فرهنگی غیرسیاسی و حتی سازمان های دولتی ایران را هم در برمی گیرد. جاسوسی دیجیتالی و حملات اخلال گرانه علیه منتقدان حکومت به ایرانیان نشان داده که فعالیت های آنلاین آنها خارج از دسترس حکومت نیست.

این گزارش یک تحلیل تاریخی از فعالیت ها و قابلیت های مشاهده شده در عاملان تهدیدکننده ایرانی است که عملیات تهاجمی سایبری را به احتمال زیاد از جانب جمهوری اسلامی به اجرا درمی آورند. به منظور حفظ یک مجموعه اصلاحات یکدست، فعالیت های سایبری پوشش داده شده در این گزارش به عنوان «عملیات تهاجمی سایبری» مطرح می شود که از نظر وزارت دفاع ایالات متحده اقداماتی است که «به قصد نمایش قدرت بوسیله اعمال زور در فضای سایبری یا از طریق آن» یا از طریق متمایز کردن نتایج مورد نظر (مثل اختلال، استخراج غیرمجاز اطلاعات یا نابودسازی) صورت می گیرد. این امر دامنه این تحقیق را به اطلاعات و دیگر اقدامات تهاجمی محدود می کند و به تمامی تلاش های حکومت ایران در جهت تحت تأثیرگذاری آنلاین یا کنترل اطلاعات نمی پردازد.

هکرهایی که بطور هماهنگ در زمینه عملیات سایبری کار می کنند «عاملان تهدید کننده» نامیده شده اند، اگرچه این گروه ها می توانند فقط یک عضو داشته باشند و ترکیبشان به مرور زمان تغییر کند. اصطلاح «تحت حمایت دولت» یا «هماهنگ با دولت» که در سرتاسر این گزارش مورد استفاده قرار گرفته، رابطه میان مهاجمان و حکومت ایران را در سرتاسر عملیات منعکس می کند.

مدارک قضایی و دیگر مدارک جمع آوری شده در تحقیق پیرامون امنیت سایبری، شناختی بی سابقه در خصوص اولویت های امنیتی و اطلاعاتی رژیم ایران ارائه می کند. قصد واقعی یک مهاجم در فعالیت های نفوذی همیشه مشخص نیست. نفوذ در یک سیستم به منظور جاسوسی یا شناسایی می تواند بعدها به عنوان پایگاهی الکترونیکی برای خرابکاری مورد استفاده قرار بگیرد. در حالی که تهران طی دوران مناقشه با رقبای خود به حملاتی بسیار نمایان علیه آنان دست زده است، تاریخ ده ساله عملیات سایبری این کشور نشان می دهد که علت اصلی چنین کمپین هایی ظاهراً جاسوسی بوده است.

ایران هدف جاسوسی و اقدامات سرکوبگرانه و ویران کننده از سوی کشورهای خارجی- نه تنها ایالات متحده و اسرائیل، بلکه کانادا، فرانسه، روسیه و بریتانیا- بوده است. این حملات بعدها تهران را برانگیخت تا توانایی های سایبری تدافعی و تهاجمی بومی ایجاد کرده و همچنین بتواند تهدیدات تلافی جویانه خود را عملی سازد. این مبادلات مستقیماً با اوضاع داخلی و ژئوپولتیک ایران مرتبط است که بازتاب آن را می توان در کاهش حملات مختل کننده از زمان امضای توافق هسته ای ۲۰۱۵- معروف به برنامه جامع اقدام مشترک (برجام)- مشاهده کرد.

منبع عمده داده های استفاده شده در این گزارش، اسنادی است که از حملات علیه انواع سازمان های غیردولتی و دیگر اهداف هم در داخل و هم خارج از ایران جمع آوری شده است. شیوه های تحقیقات قانونی، چشم انداز وسیع تری از دامنه فعالیت های عاملان تهدیدکننده را میسر می سازد و به شناسایی شرکت کنندگان معین و ارتباطات احتمالی آنان با نهادهای حکومتی ایران کمک می کند. به عنوان مثال، حملات sinkholing (جلوگیری از ارتباط از طریق تغییر مسیر اسامی دامنه ها) هم در شناخت مجرمان و هم قربانیان چنین کمپین هایی کمک می کند. در سایر موارد، مهارت نداشتن گروه های ایرانی موجب افشای اسامی، نام های مستعار و ایمیل های اعضای گروه از طریق کدهای بدافزارها و سوابق ثبت دامنه شده است.

این تحقیق دست اول، گزارش های متعدد در این زمینه- که براساس منابع اصلی و منتشر شده از سوی شرکت های امنیت سایبری پیرامون حوادث یا عاملان تهدیدکننده مشخصاً مربوط به ایران تهیه شده- را تکمیل می کند. این مطالب شناختی دیگر از نحوه ای که ایران سایر بخش ها- از جمله شرکت های دفاعی و دولت ها- را هدف می گیرد و در دسترس مستقیم نویسندگان این تحقیق نیست، ارائه می دهد. فهرستی از این گزارش ها آنلاین منتشر خواهد شد. مصاحبه با اهداف کمپین های ایران- شامل کنشگران و محققان در ایران و خارج از آن- در روشن کردن انگیزه های تهران مفید است و آن حملات را در پسزمینه وسیع تری قرار می دهد. مصاحبه با افراد حرفه ای نیز پیشینه جریان های گسترده تر این صنعت را مشخص می کند.

هدف از این گزارش، استحکام مباحثات پیرامون سیاست گذاری در خصوص عملیات سایبری ایران از طریق افزایش دانش مردم درباره ماهیت چنین فعالیت هایی است. از آنجا که مطالب مربوط به تحقیقات امنیت سایبری معمولاً محدود به افشای عاملان تهدید کننده یا اینگونه حوادث است، شناختی از انگیزه های گسترده تر یا جریان های قابل مشاهده فراهم نمی کند. اما این گزارش با آنها متفاوت است، چرا که به الگوهای تاریخی و پیشینه وسیع تر عملیات سایبری ایران- بویژه رابطه آنها با تغییرات شرایط سیاسی می پردازد. بعلاوه، این گزارش بر تداخل کمپین های ایران علیه نهادهای دولت های خارجی و/یا نهادهای شرکتی از یک سو، و علیه سازمان های حقوق بشر و جامعه مدنی از سوی دیگر می پردازد که معمولاً در مباحثات پیرامون تعیین خط مشی در خصوص امنیت سایبری نادیده گرفته می شوند.
درک بهتر سوابق و دلایل استراتژیک عملیات تهاجمی سایبری ایران باید روشنگر استراتژی ایالات متحده نسبت به ایران و همچنین واکنش های آینده این کشور به اقدامات ایران باشد. این مسئله از اهمیت ویژه ای برخوردار است، چرا که

فضای سایبری که ایالات متحده متکی به آن است، از محافظت کافی برخوردار نیست و باید انتظار آن را داشته باشد که حملات سایبری آینده این کشور علیه ایران موجب حملات تلافی جویانه ای از سوی ایران به زیرساخت های ایالات متحده بشود. با توجه به سوابق اخیر ایران، چنین نتیجه ای را باید انتظار داشت.

فصل اول

ایران: اهداف و مجرمان

از زمانی انتشار نخستین مطالب درباره فعالیت های سایبری ایران در تابستان ۲۰۱۲ که در آن نام یک عامل بدافزار به نام Madi (مدی) افشا شده بود، شرکت های امنیت سایبری و سازمان های دولت های غربی مرتباً نفوذها، اختلال ها و دیگر فعالیت های مخرب از سوی ایران را ثبت کرده اند. اما گزارش های مربوطه فقط بیانگر حملاتی است که در پی براندازی زیرساخت های خارجی بودند، بی آنکه شرایط عملیات سایبری تهاجمی تهران و انگیزه های آن حملات را مشخص کرده باشند.

رویکرد تهران با حملات متعددی که زیرساخت های خود را هدف گرفته بود، شکل گرفته است. از هنگامی که یک گروه اپوزیسیون تأسیسات هسته ای مخفی ایران را در سال ۲۰۰۲ افشا کرد، بسیاری از عوامل خارجی هم به منظور جاسوسی و هم خرابکاری، تلاش کرده اند تا با عملیات نفوذی به تأسیسات هسته ای ایران، زیرساخت های اقتصادی، دستگاه های نظامی و نهادهای دولتی دسترسی پیدا کنند.

در واقع، برجسته ترین نمونه جنگ سایبری مدرن، یک کمپین خرابکاری مستمر- که به لحاظ پیچیدگی و تدارکات بی سابقه به شمار می رفت- از سوی ایالات متحده و اسرائیل علیه تأسیسات هسته ای ایران به اجرا درآمد. در عملیاتی با عنوان Operation Olympic Games (عملیات بازی های المپیک)، بدافزار Stuxnet (استاکس نت) مورد استفاده قرار گرفت تا در تأسیسات غنی سازی اورانیوم در نطنز خرابکاری کند که منجر به نابودسازی بیش از ۱۰۰۰ سانتریفیوژ شد و پیشرفت های هسته ای ایران را بیش از یک سال به تأخیر انداخت. این یکی از اولین عملیات معروف تهاجمی سایبری بود که به عنوان اقدامات سرکوب گرانه بین کشورها صورت می گرفت.

در حالی که هدف استاکس نت فقط تنزل برنامه اتمی ایران بود، سایر کمپین ها به دنبال خرابکاری در زیرساخت های مالی و نفتی کشور بودند. در ماه مه ۲۰۱۲ ، یک کنسرسیوم از محققان عملیات مخرب دیگری علیه ایران افشا کردند. بدافزارهای Wiper (وایپر) و Flame (فلیم)، جانشین های استاکس نت، زمانی آشکار شدند که ظاهراً طی عملیاتی یک جانبه از سوی اسرائیل، کامپیوترهای وزارت نفت ایران و شرکت ملی نفت ایران از کار افتادند و دیسک های سخت آنها آسیب دید.

عملیات سرکوبگرانه سایبری علیه ایران پس از «عملیات بازی های المپیک» هم ادامه یافت. در ژوئن ۲۰۱۲ که مذاکرات هسته ای بین ایران و قدرت های جهانی متوقف شده بود، وزیر اطلاعات ایران ادعا کرد که تأسیسات هسته ای

کشور در معرض یک «حمله عظیم سایبری» دیگر قرار گرفته است. مدتی بعد در همان سال، ایران ادعا کرد که عملیات مختل کننده دیگری بانک مرکزی، وزارت فرهنگ و سکوهای حفاری شرکت نفت فلات قاره ایران را هدف گرفته است.

افزون بر خرابکاری، مؤسسات اطلاعاتی خارجی هم به طور پیوسته زیرساخت های ایران را به قصد جاسوسی مورد هدف قرار می دادند؛ حقیقتی که ایران طی افشاگری های اطلاعاتی ادوارد اسنودن از آن آگاه شد. اسنودن که کارمند سابق سازمان امنیت ملی آمریکا (NSA) بود، سامانه ای به نام Boundless Informant را افشا کرد که در آن ایران به عنوان یکی از کشورهای شدیداً تحت نظارت عنوان شده بود: انبوهی از مدرک از اینترنت و تلفن در ایران توسط سازمان های اطلاعاتی ایالات متحده و شرکایش جمع آوری شده بود. در واقع، ایران آنچنان به دفعات بی شمار تحت نظارت قرار گرفته بود که یک بار یک عملیات جاسوسی کانادا که هدفش ایران بود به طور اتفاقی به یک عملیات اطلاعاتی که گرداننده اش فرانسه بود برخورد کرد که به همان شبکه نفوذ کرده بود.

ایران چگونه سرکوب سایبری را پذیرفت؟

مدت هاست که رهبر ایران، آیت الله علی خامنه ای، بر این باور است که واشنگتن به دنبال براندازی جمهوری اسلامی از طریق تحریک توده ها به شیوه انقلاب مخملی ۱۹۸۹ است که رژیم کمونیستی چکسلواکی را سرنگون کرد. بر اساس همین استدلال، اولین عملیات سایبری ایران با ترس از اینکه ثبات رژیم در معرض تهدیدات خارجی است و اینترنت این امر را تسهیل می کند، برانگیخته شد. تهران اغلب به ابراز مخالفت های آنلاین شهروندانش این برچسب را می زند که درگیر جنگ سایبری سازمان یافته از سوی دشمنان حکومت، یعنی ایالات متحده، شده اند تا جمهوری اسلامی را سرنگون کنند. حمایت دولت های غربی از دسترسی بدون محدودیت به اینترنت و شبکه های تلویزیونی ماهواره ای فارسی زبان، مثل بی بی سی فارسی، عناصر اصلی این استراتژی تلقی می شوند. ظهور سایت های شبکه های اجتماعی، مانند فیس بوک و توییتر و اپلیکیشن های پیام رسانی، مثل تلگرام بسیار تهدیدآمیز محسوب می شوند، چرا که انحصار طولانی مدت حکومت ایران بر رسانه ها و وسایل ارتباطی را به چالش می کشند.

بزرگترین نگرانی خامنه ای زمانی به تحقق پیوست که در ژوئن ۲۰۰۹ انتخاب مجدد و سؤال برانگیز محمود احمدی نژاد تندرو به عنوان رئیس جمهور در میان اتهامات گسترده تقلب، عظیم ترین قیام مردمی از زمان انقلاب ۱۹۷۹ را رقم زد. آن روزها همچنین زمانی محوری برای حکومت ایران بود تا به استقبال توانایی های تهاجمی سایبری برود، به دلیل آنکه بسیج مردمی، معروف به جنبش سبز، به یکی از اولین اهداف عملیات رژیم تبدیل شد. مبارزه آنلاین بین اپوزیسیون که از اینترنت استفاده می کرد تا مقاومت سیاسی را هماهنگ کند، و حکومت که تلاش می کرد آن بسیج مردمی را سرکوب کند، صحنه را برای درگیری های آینده، از جمله با قدرت های خارجی، آماده کرد.

اندکی پس از آنکه حدود دو میلیون ایرانی در ۱۵ ژوئن ۲۰۰۹ در تهران به تظاهرات پرداختند، حامیان جنبش سبز شروع به مبارزه با حکومت کردند که اطلاعات را کنترل می کرد. زمانی که مقامات، رسانه های خارجی را اخراج، در شبکه های موبایل مداخله، و مخالفان برجسته را دستگیر کردند، اینترنت تبدیل به کانال اصلی هماهنگ سازی در میان هرج و مرج تبدیل شد. در واکنش به این مسئله، کنگره ایالات متحده و دولت پرزیدنت وقت، باراک اوباما، و شرکت های تکنولوژی در آمریکا تلاش کردند تا دسترسی کاربران ایرانی به اینترنت برقرار بماند.

طی دوران جنبش سبز، هکرهای طرفدار رژیم یک استراتژی چندمنظوره- شامل نفوذ، اخلال در وب سایت ها و همچنین نظارت بر شبکه ها- را بکار گرفتند. از دسامبر ۲۰۰۹ تا ژوئن ۲۰۱۳ گروهی که خود را ارتش سایبری ایران می نامید، با فرستادن پیام های حامی دولت روی وب سایت های وابسته به اپوزیسیون سیاسی ایران، شرکت های تجاری اسرائیلی، رسانه های مستقل فارسی زبان، و پلتفرم های شبکه های اجتماعی، شروع به تخریب ظاهر آن سایت ها کرد. هنگامی که کنشگران حقوق بشر و رهبران اپوزیسیون فراخوان اعتراضات خیابانی می دادند، وب سایت های مهم در معرض طوفانی از ترافیک مخرب اینترنتی قرار می گرفتند که در دسترسی کاربران اختلال ایجاد می کرد، حملاتی که به نام DDoS (یا محروم سازی از سرویس) معروف بود. حکومت ایران با بدافزاری که وانمود می کرد حاوی اطلاعات مربوط به برنامه های تظاهرات آینده و رسوایی های عمومی است، از منتقدان خود جاسوسی می کرد. یک هکر ایرانی در شرکت امنیتی هلندی DigiNotar (دیجی نوتار) نفوذ کرد تا گواهی های جعلی رمزگذاری صادر کند که به تهران اجازه می داد از تمام کاربران جی میل در داخل کشور جاسوسی کند؛ این اقدام یکی از بزرگترین نفوذ های امنیتی در تاریخ اینترنت به شمار می رود.

در نهایت، نیروهای امنیتی با سبعیت، نظارت و سانسور، جنبش سبز را تضعیف کردند و اعتراضات خیابانی پیش از سال ۲۰۱۱ فروکش کرد. سازمان های امنیتی خود را با محیط مدرن دیجیتالی وفق داده بودند- از جمله سپاه پاسداران انقلاب اسلامی که طی بازجویی ها، زندگی خصوصی دستگیرشدگان را براساس نسخه های پرینت شده ارتباطات آنلاین و شبکه های اجتماعی آنها بررسی می کرد. یکی از فرماندهان سپاه بعدها گفت که قلع و قمع تظاهرکنندگان مستلزم دستگیری ها و سرکوب های گسترده و قطع کردن وسایل ارتباطی آنها، مثل موبایل و اینترنت بود. جنبش سبز نشان داد که از اینترنت می توان به عنوان وسیله بسیج مردمی استفاده کرد و حکومتی که مدت های مدید انحصار اطلاعات را در دست داشت با چالشی مؤثر مواجه ساخت.

تاکتیک ها، ابزار و عاملان تهدیدکننده بوجود آمده طی این چالش داخلی که رژیم با آن مواجه شد، خبر از وضعیت سایبری ایران مقابل مجموعه ای وسیع تر از تهدیدهای داخلی و خارجی می داد. یکی از ویژگی های ثابت عملیات سایبری ایران از همان ابتدا این بود که حد و مرز مشخصی بین عملیات علیه اپوزیسیون داخل کشور و دشمنان خارجی وجود نداشته است. عاملان تهدیدکننده ایرانی در کمپین علیه صنایع دفاعی آمریکا از همان زیرساخت ها و ابزاری استفاده می کنند که در کمپین هایی که هدفشان برنامه های فارسی زبان مربوط به پیشرفت زنان است. همان بدافزاری که در

حملات مخرب علیه نهادهای دولتی عربستان سعودی بکار گرفته شده، قبلاً در نظارت بر اعضای اپوزیسیون جنبش سبز استفاده شده بود.

توانایی های تهاجمی سایبری ایران

عملیات سایبری فرصت های کم خطرتری در زمینه جمع آوری اطلاعات و انتقام از آنچه دشمن داخلی و خارجی تلقی می کند، فراهم کرده است. حکومت ایران پیش از آنکه تکنولوژی ارتباطات اطلاعات به صورتی گسترده قابل دسترس شود، عملیات اطلاعاتی خارج از کشور را عمدتاً بر استخدام مأموران برای جاسوسی و ترور مخالفان سیاسی یا دیپلمات های رقیبان خود متمرکز می کرد. این عملیات معمولاً در صورت دستگیری مهاجمان به شرمساری بین المللی می انجامید و در صورت موفقیت محکوم می شد. در مقایسه با عملیات مخفیانه داخل کشور، قابلیت های تهاجمی سایبری امکان تکذیب قاطع تری را میسر می سازد و تا به امروز، احتمال آنکه پس از کشف منجر به تلافی شود بسیار کمتر بوده است.

طی دهه گذشته، عملیات تهاجمی سایبری به ابزار اصلی سیاستمداری ایران برای اهدافی چون جاسوسی، علامت دهی و سرکوب تبدیل شده است. گزارش های مربوط به عملیات تهاجمی سایبری ایران حاکی از یک الگوی ثابت در کمپین ها و عاملان تهدیدکننده مختلف است. این عملیات بر مجموعه ای از اهداف به خوبی تعریف شده متمرکز هستند و از کمپین هایی که به دست عاملان تهدیدکننده تحت حمایت دولت در دیگر کشورها صورت می گیرند، ابتدایی ترند: خبر دادن موثق تهدیدها و جلوگیری از آنها مستلزم آن است که این اقدامات تکرار شود- قابلیتی که تهران بطور کلی فاقد آن است.

بعلاوه، آن میزان از تخصص، تدارکات و سرمایه گذاری که برای اجرای عملیاتی چون «عملیات بازی های المپیک» لازم بود، همچنان بشدت خارج از حوزه توانایی عاملان تهدید کننده ایرانی است. برخلاف عملیات سایبری ایالات متحده و اسرائیل که بدست سرویس های اطلاعاتی حرفه ای و با حمایت بودجه های میلیارد دلاری اجرا می شد، توانایی های تهاجمی و دفاعی ایران هم بی نظم و برنامه اند و هم از حمایت مالی اندکی برخوردارند. بدین ترتیب، با وجود آنکه ایران اغلب برای اعمال فشار به حملات مخرب رو می آورد، به لحاظ توانایی و فرصت های تهدید مخالفان محدودیت دارد. تهران همچنین در جمع آوری اطلاعات جاسوسی انسانی به صورت مخفیانه در کشورهای خارجی، بویژه بیرون از خاورمیانه، نیز چندان مهارتی ندارد.

تهران بندرت مسئولیت عملیات تهاجمی سایبری نسبت داده به خود- از جمله آنچه در جهت پشتیبانی از جمهوری اسلامی است- را می پذیرد و سخنان ضد و نقیضی در خصوص وضعیت سایبری خود گفته است. مقامات ایران سابقه غلو کردن درباره توان نظامی کشور، از جمله عملیات سایبری را در کارنامه خود دارند. در اکتبر ۲۰۱۲ حیدر مصلحی، وزیر اطلاعات وقت، در پاسخ به یک سری اختلالات در زیرساخت های سازمان خود گفته بود که «جمهوری اسلامی چنان در فضای مجازی قدرتمند است که [حتی] رهبران قدرت های مستکبر هم موفقیت های کشور ما را می پذیرند و به آن اذعان

دارند.» با این همه، فرمانده سپاه پاسداران، محسن کاظمینی، ادعا کرده بود که گردان جنگ سایبری سپاه مسئول عملیات تهاجمی نیست. در لفاظی های رسمی نیز ظاهراً تلاش های دولت در جهت پیشبرد تبلیغات آنلاین همراه با توانایی تهاجمی سایبری و ادعای برخورداری از ده ها هزار جنگجوی سایبری است.

ایران از گزارش های حوادث ویرانگر استفاده می کند تا خود را قربانی تهاجم خارجی جلوه دهد، توجه را از فعالیت های خود منحرف کند و توانایی اش در خنثی کردن حملات احتمالی را به رخ بکشد. زمانی که ایالات متحده ایران را متهم به اجرای حمله ای مخرب علیه بانک های آمریکایی کرد، معاون وزارت امور خارجه ایران، حسین جابری انصاری، پاسخ داد که «دولت ایالات متحده که با حملات سایبری علیه تأسیسات هسته ای صلح آمیز ایران، جان میلیون ها انسان بی گناه را با خطر یک فاجعه محیطی مواجه می کند، در مقامی نیست که شهروندان کشورهای دیگر، از جمله ایران را بدون مدرک موجه متهم کند.» مقامات ایران پس از اینکه کشور در معرض حملات بدافزارهای «فلیم» و «وایپر» قرار گرفت، از نهادهای بین المللی درخواست کمک کردند- اقدامی که هماهنگ با فراخوان آنها در جهت کنترل بیشتر سازمان ملل بر اینترنت بود.

ایران در بیانیه های علنی خود اغلب بر توانایی های دفاعی خود تأکید کرده؛ از جمله در سال ۲۰۱۵ اعلام کرد که «مرکز فوریت های واکنش به حملات سایبری» موفق به خنثی کردن حملات سایبری ایالات متحده به زیرساخت های صنعتی کشور شده است. مقامات نظامی ایران مرتب از تولید محصولات دفاعی جدید ساخته پیمانکاران داخلی خبر می دهند که مهمترین نمونه آن، نرم افزار آنتی ویروس «پادویش» است. به رغم این ادعاها، ایران در زمینه پرورش یک صنعت امنیت سایبری کامل و جامع چندان موفق نبوده و در خصوص سرمایه گذاری در دفاع یا تنظیم سیاست های ملی برای امن کردن زیرساخت های حیاتی، از نظام های اقتصادی پیشرفته و رقبای اصلی خود در منطقه همچنان عقب است.

در حالی که حکومت ایران سال های اخیر دهها میلیون دلار به امنیت سایبری اختصاص داده، اما در مقایسه با میلیاردها دلاری که دولت ایالات متحده سالانه هزینه کرده یا صدها میلیون دلاری که بانک های آمریکایی به طور جداگانه خرج کرده اند، سرمایه گذاری های ایران رنگ می بازد. حتی اگر ایران توجه خود را معطوف بر پیشرفت توانایی های دفاعی خود می کرد، همچنان به دلیل تحریم ها، ناکارآمدی های مربوط به دیوانسالاری و کمبود مهارت تخصصی با محدودیت های قابل ملاحظه ای مواجه می شد. با توجه به کاردانی و مهارت دشمنان ایران، باید به اظهارات این کشور درباره ردیابی سریع و جلوگیری از نفوذ خارجی به شبکه های ایرانی با دیده شک نگریست و آن را نوعی ژست دفاعی دانست که احتمال تغییر آن بعید است.

ایران به رغم ادعاهای اطمینان بخش خود، به لحاظ توان سایبری غالباً یک کشور درجه سه به شمار می آید که فاقد تشکیلات پیشرفته و بومی امنیت سایبری است و مثل چین، اسرائیل، روسیه و ایالات متحده، توان اجرای عملیات ماهرانه را ندارد. هر چند که مهارت تکنیکی ایران را از اجرای عملیات سایبری موفق باز نمی دارد، اما چنین اقداماتی همچنان

حاکی از بی نظمی و کمبود تخصص است که از یک کشور فعال در این زمینه بعید به نظر می رسد و توانایی هایش را محدود می سازد. انزوای سیاسی و اقتصادی تهران نیز این کشور را از کسب تکنولوژی و تخصص از کشورها یا شرکت های خارجی محروم کرده و مدرکی دال بر همکاری قابل ملاحظه ای بین ایران و دیگر کشورها در زمینه توسعه توانایی های تهاجمی سایبری دیده نمی شود.

تفاوت بین جاسوسی و خرابکاری

روایت های رسانه ها از عملیات سایبری معمولاً بسیار کلی است و بر تمام نفوذها- چه مخرب، چه غیرمخرب- برچسب حمله می زند، در حالی که عملیات تهاجمی سایبری را می توان براساس قصد و تأثیرشان به طرز صحیح تری نامگذاری کرد و بین جاسوسی و خرابکاری تمایز قائل شد. عاملان ایرانی در نفوذهای خود هم به دنبال اخذ اطلاعات از شبکه های خارجی بوده اند (جاسوسی، جمع آوری اطلاعات) و هم برای تنبیه یا سرکوب دشمنان (خرابکاری) به فعالیت های مخرب پرداخته اند؛ در این میان یک سری فعالیت های نامشخص هم دیده می شود که شامل علامت دهی و دیگر انگیزه ها است. درک این تمایز در ارزیابی استراتژی ایران و قانونی بودن عملیات آن کشور اهمیت دارد.

در واقع، با توجه به تعداد در حال رشد کشورهایی که واجد توانایی های تهاجمی سایبری هستند، جاسوسی و جمع آوری اطلاعات از طریق عملیات سایبری به طرز فزاینده ای به عنوان یک قاعده بین المللی پذیرفته شده است. در حالی که ایالات متحده طبعاً هدف گیری کارمندان وزارت امور خارجه این کشور از سوی تهران را محکوم می کند، اما چنین حوادثی بازتاب عملیات مشابه جاسوسی ایالات متحده و دیگر سازمان های اطلاعاتی غربی علیه دیپلمات های ایرانی است.

متخصصان حقوق بین الملل معیارهایی برای تعیین آنچه «حمله مسلحانه» در فضای سایبری به شمار می آید، مشخص کرده اند که متکی به شدت، تهاجمی و مستقیم بودن، و دیگر عوامل است. چنین معیارهایی همچنین اهمیت یک مجموعه اصلاحات را دو چندان می کند، مثلاً بین جاسوسی علیه اینترانت نیروی تفنگداران دریایی ایالات متحده و حادثه مخربی چون حمله ایران به عربستان سعودی و بزرگترین شرکت نفتی جهان- آرمکو سعودی- باید تمایز قائل شد. محققان در همین خصوص ذکر کرده اند که استفاده ایران از پراکسی ها در عملیات تهاجمی سایبری، حکومت را از تعهدات قانونی یا واکنش های ناشی از آن که تا حدودی براساس پرونده حقوقی بین المللی از بحران گروگانگیری ۱۹۷۹ است، مبرا نمی سازد.

ارزیابی پیگیر مشروعیت عملیات سایبری ایران معیارهای کلی و مشخصی درباره مواردی که ایران اصول و قوانین مورد احترام بین المللی را نقض کرده و رفتار غیرقانونی در پیش گرفته، ارائه می دهد. همچنان که تهران به اجرای

عملیات تهاجمی سایبری ادامه می دهد، لازم است که سیاست گذاران قصد، دامنه و مشروعیت فعالیت های این کشور را پیش از دادن پاسخ متقابل ارزیابی کنند.

فصل دوم

اکوسیستم سایبری ایران:
عاملان تهدید کننده چه کسانی هستند؟

یکی از خصیصه های منحصر بفرد جمهوری اسلامی این است که قدرتمندترین مقامات آن، یعنی رهبر خامنه ای و سپاه پاسداران انقلاب اسلامی، غیرقابل دسترس هستند. در حالی که مقاماتی که بیش از همه در دسترس هستند- از جمله وزیر امور خارجه، محمدجواد ظریف- به مراتب از قدرت کمتری برخوردارند. فعالیت های تهاجمی سایبری ایران تقریباً بطور انحصاری تحت نظارت سپاه پاسداران است- احتمالاً بدون نظارت آندسته از مقامات کشور که «منتخب» مردم هستند- و از مجموعه پراکنده ای از پیمانکاران مستقل تشکیل شده که آمیزه ای از کارهای امنیتی، تقلب کیفری و تولید نرم افزارهای مبتذل تر را به عهده دارند. با آنکه ارتباط بین پراکسی ها و حکومت ها از حمایت انفعالی گرفته تا کنترل کامل ادامه دارد، عاملان تهدید کننده بومی ایرانی ارتباط خود با حکومت را دور نگاه می دارند، در حالی که برخی از عملیات خاص را به نحوی سازماندهی می کنند که نیازهای حکومت را تأمین کند.

عاملان تهدید کننده ایرانی پس از سرکوب موفقیت آمیز جنبش سبز در سال ۲۰۰۹ و شناسایی تهاجم «استاکس نت» در ۲۰۱۰ کمپین هایی مستمر علیه دشمنان داخلی و خارجی به راه انداختند. این عملیات بومی ظاهراً بدست گروه های کوچکی از افراد- کمتر از ده نفر در هر تیم- با سطوح مختلف تخصص در تکنولوژی اجرا می شد. این کمپین ها و منابع تولید شده بدست گروه ها هم ابتدایی و هم نسبتاً حرفه ای بودند، اما اکثر عاملان توانایی اندکی داشتند.

اگرچه مقامات ایالات متحده و برخی از شرکت های امنیت سایبری بر این گمانند که تهران از کشورهایی مثل روسیه و کره شمالی کمک های فنی دریافت کرده، پیشرفتگی و مهارت این عملیات در حد شیوه های معمول هکرهای داخل ایران است. هرچند که ایرانیان استعداد خود را در مهندسی اجتماعی نشان داده و خود را در شبکه هایی که مورد نفوذ قرار گرفته اند، جای داده اند؛ این صرفاً حاکی از تعلیم و آموزش خارجی یا انتقالات تکنولوژیکی نیست.

عاملان تهدیدکننده ایرانی چندین بار به منظور اجرای کمپین های خود از نسخه های حاضر و آماده یا سرقت شده ابزار نفوذ آزمایشی حرفه ای بهره برده اند، اما دلیل و مدرکی دال بر اینکه تهران از دولت های خارجی «اکسپلویت» (کدهای مخرب) یا بدافزار دریافت کرده باشد، وجود ندارد. ایران سخت افزار نظارت بر اینترنت را از شرکت های مخابراتی چینی کسب کرده و توافق نامه های همکاری در زمینه امنیت سایبری با روسیه برقرار کرده، اما این نوع روابط با اینکه قابلیت های تهاجمی سایبری در اختیار تهران قرار دهند، تفاوت دارد. هیچیک از حملاتی که علناً ثبت یا به صورت محرمانه رصد شده اند، نشانی از کاربرد ابزار یا منابعی ندارند که ورای ظرفیت عاملان تهدیدکننده ایرانی باشد.

در اصل، ابزار و تاکتیک های استفاده شده در عملیات سایبری در معرض خطر افشا شدن هستند. بر خلاف سلاح های مرسوم، حملات بدافزاری یا سایر فعالیت های سایبری، زمانی که آشکار، و عملکرد و زیرساخت هایشان ثبت می شوند، تأثیر خود را از دست می دهند. توصیف یک سلاح، کمکی به یافتن راهی برای یک اقدام متقابل و مؤثر نمی کند، اما توصیف یک بدافزار می تواند به شرکت های آنتی ویروس و مدیران سیستم ها کمک کند تا قابلیت محافظت از سیستم ها را بدست آورند. عاملان تهدیدکننده وابسته به حکومت احتمالاً پیچیده ترین ابزار و استراتژی های قابل دسترس را بکار نمی گیرند، مگر زمانی که هدف ایشان تحت محافظت کامل قرار دارد و ارزش برملا شدن احتمالی شیوه های مخفیانه نفوذی شان را داشته باشد. با این همه، بر خلاف دیگر کشورها، نمونه ای دیده نشده که عاملان تهدیدکننده ایرانی به حملات پیچیده تری علیه دشمنان سخت خود دست زده باشند.

عاملان تهدیدکننده ایرانی کمپین های خود را با بسته های ابزاری متداول اجرا می کنند که گاه سال ها بطول می انجامد و صدها هدف را تسخیر می کنند. با این همه، ماهیت سیال و تمرکززدایی این گروه ها، تعقیب آنها را نسبتاً دشوار می سازد. بدافزاری که آشکارا به تهران نسبت داده می شود، اغلب به محض افشا شدن، رها می شود و اعضای قابل شناسایی گروه نیز ظاهراً به مرور زمان تغییر می کنند. به نظر می رسد که بعضی از گروه ها تقسیم می شوند یا اعضایشان به مکانی دیگر فرستاده می شوند یا حتی همکاری می کنند و بدین ترتیب، شناسایی و تشخیص دسته بندی شان مشکل تر می شود. مثلاً گروهی وابسته به سپاه پاسداران به نام Rocket Kitten (راکت کیتن) که به مدت یک دوره دوساله (۲۰۱۴-۲۰۱۶) از فعالترین عاملان بود و به عنوان تهدید برتر ایران، توجه مطبوعات را جلب کرده بود، ناپدید شد و تحت الشعاع عامل Oilrig (اویلریگ) قرار گرفت.

به رغم تأثیرات قابل توجه مالی، عملیات مخرب تهران علیه اهداف خارجی به لحاظ تکنیکی ساده بوده است. نفوذ به دستگاه های تعداد اندکی از کارکنان فن آوری اطلاعات به نابودسازی داده های کامپیوترهای شرکت Saudi Armeco(آرمکو سعودی) انجامید که حاصل آن صدها میلیون دلار زیان بود. عاملان تهدیدکننده ایرانی فقط در تعداد کمی از کمپین هایشان مهارت و تخصصی که تقریباً از یک عامل ملت-کشور انتظار می رود، نشان داده اند. یکی از این نمونه ها عملیاتی بود که مستقیماً وابسته به وزارت اطلاعات بود. (عملیات Magic Kitten که بعد مورد بررسی قرار خواهد گرفت.)

موفقیت ها اغلب نتیجه شکست امنیتی و حمایت ناقص از زیرساخت های یک قربانی است که به آن می توان هدف گیری فرصت طلبانه و بردباری مهاجم را نیز اضافه کرد. تخریب ظاهر وب سایت صدای آمریکا بدست ارتش سایبری ایران یکی از اولین حملات مخرب ایران علیه ایالات متحده بود که از طریق مهندسی اجتماعی نام دامنه ارائه دهنده سرویس به آن آژانس خبری، میسر شد. دیگر شکست های امنیتی ابتدایی به ایرانیان این فرصت را داد که جاپای خود را در شبکه های شرکت Las Vegas Sands بجای بگذارند؛ این اقدام پس از آنکه مالک آن، Sheldon Adelson، از نفوذ نظامی علیه ایران حمایت کرد، صورت گرفت. شرکت امنیت سایبری آمریکایی Symantec متوجه شد که مجرمان کمپین اخیر

علیه عربستان سعودی، «مدت زمان بسیاری را وقف تدارک و آماده سازی برای عملیات» کرده بودند، اما به گفته شرکت امنیت سایبری روسی Kaspersky، آن بدافزار سفارشی که بخشی از آن از بسته افزاری منابع باز گرفته شده بود «بطور کلی از کیفیتی پایین» برخوردار بوده است.

به همین ترتیب، تهاجمی عمده به بخش مالی آمریکا، معروف به عملیات «ابابیل»، که صدها میلیون دلار ضرر به بار آورد، یکی از بزرگترین حملات DDoS (حملات گسترده منع سرویس دهی) در آن زمان شناخته شد. ولی آن حمله فقط بدست تعدادی اندک از جوانان ایرانی متخصص کامپیوتر صورت گرفت که به هزاران وب سایتی که با نرم افزارهای آسیب پذیر اداره می شدند، رخنه کردند تا با استفاده از پهنای باند زیرساخت های بانک ها را از کار بیندازند و موجب از کار افتادگی غیرقابل پیش بینی نرم افزارها بشوند. بنابراین، با وجود آنکه عاملان تهدیدکننده ایرانی از ظرفیت کمی برخوردارند، با مخفی کاری های ابتدایی و سماجت می توانند همچنان در جاسوسی و خرابکاری تأثیرگذار باشند.

مهارت کلی و تعهد مشهود در چنین کمپین هایی، طی ده سال عملیات تهاجمی سایبری ایران تغییر چشمگیری نکرده است: حملات ثبت شده علیه شرکت Las Vegas Sands در سال ۲۰۱۴ شبیه به حملات علیه عربستان سعودی طی دشمنی مجدد با آن کشور در سال های ۲۰۱۷-۲۰۱۶ است. در واقع، بسیاری از تحقیقات حاکی از آن است که گروه هایی چندین سال با استفاده از یک نوع بدافزار و با تغییرات مکرر طی مدت زمانی معین فعال بوده اند.

در حالی که مهارت محض شاید معیاری سطحی برای تهدید ایجاد شده باشد، عملیات ایرانیان چندان نشانی از اقدامات احتیاطی مرسومی ندارد که عاملان ملت-دولت های دیگر بکار می گیرند (مثل غامض جلوه دادن بدافزار)، و حتی با توانایی های قوی مهندسی اجتماعی، حملات معمولاً به علت کمبود سرمایه گذاری در منابع غیر فنی برملا می شوند (مثل فصاحت در زبان انگلیسی یا سازگار کردن شخصی پیام ها به منظور خاص). علاوه بر این، چنین محدودیت هایی در منابع نشان می دهد که چرا ایران در به دام انداختن مخالفان حکومت موفق است: عاملان تهدیدکننده ایرانی از شرایط و زبان هدف خود اطلاع کافی دارند، و این برخلاف زمانی است که آنها در پی اهدافی با زبان خارجی یا فرهنگ های دیگر هستند. نشانی از آنکه ایران در آینده ای نزدیک بتواند به یک قدرت سایبری درجه یک بدل شود، وجود ندارد مگر آنکه به سازماندهی بیشتر عملیات بپردازد و همچنین در کسب مهارت سرمایه گذاری کند.

عملیات Magic Kitten

در ژانویه ۲۰۱۵ ، مجله آلمانی اشپیگل اسناد منتشرنشده ای در خصوص عملیات جاسوسی سایبری سازمان های اطلاعاتی آمریکا افشا کرد. یکی از آن سندها نوعی تاکتیک متعلق به سازمان امنیت ملی آمریکا به نام Fourth party collection را برملا می کرد که عبارت از نفوذ به مراکز فرماندهی و کنترل زیرساخت های هکرهای مورد حمایت حکومت های خارجی به منظور نظارت بر فعالیت های آنان بود. این نمونه ای واقعی از کسب اطلاعات و سرقت قربانیان

از گروهی بود که سازمان امنیت ملی آمریکا به آن اسم رمز VOYEUR داده بود و نام دیگرش Magic Kitten (مجیک کیتن) بود.

به نظر می رسد که مجیک کیتن یکی از قدیمی ترین و دقیق ترین عاملان تهدیدکننده ای بود که در ایران ابداع شد و وجه تمایزش از دیگر گروه ها، ارتباط ظاهری اش با وزارت اطلاعات ایران بجای سپاه پاسداران بود. با این همه، فعالیت های مجیک کیتن انعکاس دهنده اقدامات دیگر گروه هاست و اهداف اصلی آن را ایرانیان داخل کشور و رقبای منطقه ای کشور تشکیل می دهند. نخستین نمونه های قابل مشاهده نرم افزار مرسوم مجیک کیتن به سال ۲۰۰۷ - یعنی مدت ها پیش از ابداع دیگر بدافزارهای شناخته شده- برمی گردد. این عامل تهدیدکننده همچنان فعال است.

از قرار معلوم، مجیک کیتن نشانگر کامل ترین فنون مخفیانه ای است که عاملان تهدیدکننده ساکن ایران بکار می گیرند. مجیک کیتن به طرز فرصت طلبانه ای به دهها وب سایت (از جمله وب سایت های یک بیمارستان هندی، یک معمار ایتالیایی و یک کمدین معروف کانادایی) نفوذ کرد تا با ایجاد یک شبکه کمکی، فعالیت هایش را پنهان کند. چنین توجهی به فنون مخفیانه ظاهراً جای دیگری در عملیات مجیک کیتن هم دیده می شود، مثلاً طراحی این بدافزار که ماهیت مدولار دارد.

براساس مشاهدات، مجیک کیتن از شیوه های پیچیده و ماهرانه ای استفاده نکرده، بلکه بیشتر از مهندسی اجتماعی و دیگر تاکتیک های مرسوم برای فریب کاربران بهره برده است. در مورد وحید پوراستاد روزنامه نگار، بدافزار از سوی بازجوی سابق او در وزارت اطلاعات فرستاده شده بود و تهدید ضمیمه شده به آن براساس سوابق محرمانه ای بود که تنها در دسترس عاملان دولتی قرار داشت. این هماهنگی هم بیانگر تأیید مستقل سازمان امنیت ملی آمریکا بود و هم نمونه ای از استراتژی های افراطی مجیک کیتن محسوب می شد. از قرار معلوم، دیگر نمونه های این عامل بدافزار در هیئت انجمن های پناهندگی ترکیه برای پناهجویان سوری ارائه شده بود.

آنچه سازمان امنیت ملی آمریکا ارائه داده، نمایی از اهداف مجیک کیتن تا ماه مه ۲۰۱۱ ، شامل عملیات متمرکز بر آمریکای شمالی، اروپا و خاورمیانه است. این کمپین ها تا ژوئن ۲۰۱۳ که حسن روحانی به عنوان رئیس جمهور انتخاب شد، ادامه یافت و گوگل را به انتشار مطلبی درباره حملات مربوطه در بلاگ خود برانگیخت. با فرارسیدن زمان انتخابات، لاگ های افشا شده، ثبت روزانه دهها حساب مربوط به شخصیت های فرهنگی و رسانه ای ایرانی، فارغ التحصیلان و فعالان اجتماعی (از جمله افرادی که بعد به دولت روحانی ملحق شدند) را نشان می داد. مجیک کیتن پس از انتخابات نیز به تعقیب ایرانیان ادامه داد و از مطالبی درباره حقوق زنان و ایجاد امنیت به عنوان طعمه استفاده می کرد تا نقاب از چهره آن دسته از کاربران اینترنت که از نام مستعار استفاده می کردند، بردارد.

دومین هدف مهم مجیک کیتن، مانند دیگر عملیات ایران، جاسوسی علیه کشورهای منطقه و نهادهای بین المللی سیاست گذاری خارجی است. یک شرکت امنیت سایبری آمریکایی دیگر به نام CrowdStrike تا حدی دلیل این تمرکز بر «شرکت های بین المللی عمدتاً فعال در تکنولوژی» و دیگر اهداف سیاسی است. یک لغزش از سوی سازمان امنیت ملی آمریکا در مورد نقشه مربوط به یک قربانی، عملیاتی گسترده که هدف آن تقریباً تمام کشورهای خاورمیانه را شامل می شد، تصویر می کرد. داده های Sinkhole که برگرفته از دامنه های منقضی شده ای بود که قبلاً به عنوان دامنه های کمکی و دیگر زیرساخت های پشتیبانی مورد استفاده قرار می گرفت، حاکی از آن است که مجیک کیتن یا عامل بدافزار استفاده شده همچنان افراد را در آلمان، اندونزی، عراق، لبنان، هلند، فلسطین، پاکستان، قطر، سوئد، سوئیس، تایلند و امارات متحده عربی به خطر می اندازد. افرادی که بویژه در عراق در معرض خطر قرار گرفته بودند، چنان که انتظار می رفت، ساکن کردستان عراق بودند- که این امر نشانگر یک الگوی مشترک با دیگر عاملان تهدیدکننده بود.

نموداری که سازمان امنیت ملی آمریکا تهیه کرده نشان می دهد که عامل بدافزار بکار رفته در مجیک کیتن بطور همزمان مورد استفاده حزب الله لبنان- نماینده شیعی ایران- تحت یک زیرساخت مستقل قرار گرفته بود. با آنکه حزب الله معمولاً خود مسئول حملات تهاجمی سایبری است و اطلاعات را با ایران سهیم می شود، سند و مدرکی در خصوص اشتراک مستقیم ابزار بین دو کشور وجود ندارد.

شناخت دخالت های حکومت ایران در عملیات و نسبت دادن عملیات به این کشور

تعیین خاستگاه و مجرمان عملیات تهاجمی سایبری غالباً دشوار است، چرا که این کمپین ها گاه به سرعت ناپدید می شوند. علنی شدن آنها معمولاً به تغییر تاکتیک ها و رها کردن ابزارها می انجامد که ردیابی را حتی مشکل تر می کند. سابقه عملیات سایبری که ایرانیان را هدف می گیرد و خاستگاه آن ایران است، انباشته از گروه هایی است که ناگهان سبز می شوند و به دلایلی مبهم، کمپین هایی را طی یک دوره زمانی محدود اجرا می کنند و سپس ناپدید می شوند. این آشفتگی غیرمعمول آشکارا اکوسیستم هک کردن های ایران را از بقیه- بویژه آنهایی که وابسته به عاملان حکومتی در کشورهای پیشرفته هستند- جدا می کند.

هکرهای غیر حرفه ای وابسته به گروه های ایرانی عملیات تخریب ظاهر وبسایت ها، مدت زیادی به لحاظ سیاسی درگیر بوده و اغلب به دلایل ظاهراً ناسیونالیستی به تخریب سایت های خارجی پرداخته اند. در یکی از اولین حوادث بین المللی که به ایران نسبت داده شد، گروه های هکر داخلی در اواسط سال ۲۰۰۸ با رقبای خود در کشورهای عرب همسایه به تبادل فعالیت های تخریبی تلافی جویانه پرداختند. این اقدام پس از تخریب سایت های رسمی آیت الله علی سیستانی با مطالب ضد شیعه از سوی یک هکر اماراتی صورت گرفت. چنین فعالیت های تخریبی اغلب به فعالیت های وابسته به دولت تکامل می یابند: یکی از شرکت کنندگان در کمپین ضد سنی تخریب وب سایت ها در سال ۲۰۰۸ بعدها با ارتش

سایبری ایران ارتباط یافت. گذار هکرهای میهن پرست به عاملان تهدیدکننده هماهنگ با حکومت، و ابهام موجود میان ناسیونالیسم مدنی و مشارکت حکومت، نشانگر پیشرفت ظاهری جوامع سایبری در چین و جاهای دیگر است.

تنها ظرف دو حادثه، نهادهای حکومت ایران امتیاز تخریب سایت های سیاسی اپوزیسیون را مستقیماً به خود اختصاص دادند؛ هر دو مورد به بخش های سپاه پاسداران نسبت داده شد. اولین مورد، از کار انداختن سایت های مرتبط با سازمان فعالان حقوق بشر در ایران در مارس ۲۰۱۰ بود که براساس ادعاهایی، تیم هایی را تعلیم می دادند تا مانند انقلاب مخملی، مردم را علیه رژیم بسیج کنند. آن حمله متکی به تاکتیک های پیچیده نبود، بلکه با دستگیری گرداننده وب سایت در داخل کشور صورت گرفت. دستگیری ها و نابودسازی داده ها، با ایجاد ترس در اعضا و شایعات درباره همدستی آن سازمان با حکومت، تأثیری پایدار بر آن سازمان گذاشت.

دومین کمپینی که حکومت اجرا کرد، طی تعطیلات مذهبی در دسامبر ۲۰۱۳ صورت پذیرفت که طی آن ۹ وب سایت حقوق بشر و رسانه های مستقل با یک سوره قرآن به زبان های عربی و فارسی مورد تخریب قرار گرفتند. روابط عمومی سپاه پاسداران اعلام کرد که آن عملیات بدست شعبه کرمان سپاه اجرا شده و ادعا کرد که وب سایت های تخریب شده از سوی دشمنان حکومت دایر شده و مورد حمایت فتنه گران داخلی بودند.

در اکثر موارد، ایران می توانست با استفاده از سازمان های واسطه یا نیابتی فاصله خود را از حوادث مختل کننده و تخریب ظاهر سایت ها با اهداف تبلیغاتی حفظ کند. این سازمان های واسطه خود را به عنوان ایرانیان میهن پرست یا جنبش های پان اسلامیسم معرفی می کنند که بطور مستقل در جهت دفاع از رهبر، اقتدار ملی و آرمان های مذهبی فعالیت می کنند. با اجرای عملیات تهاجمی سایبری از طریق سازمان های مخفی، تهران می تواند هر گونه حمله را بطور قابل باوری تکذیب کند و بدین ترتیب هم ادعای خود مبنی بر قربانی بودن را ثابت کند و هم به مخالفان خود ضرب شستی نشان دهد. چنین تاکتیک هایی مؤثرند: مثلاً هنوز توافق قطعی و همگانی درباره اینکه چه کسی مسئول حملات ارتش سایبری یمن بود وجود ندارد- حمله ای که منجر به سرقت اسنادی از وزارت امور خارجه عربستان سعودی شد که ویکی لیکس آنها را منتشر کرد. عده ای ایران و عده ای روسیه را مسئول آن حملات می دانند. سازمان های واسطه در پی آن هستند تا تصورات غلط خود را بسط داده و با آنان مانند عوامل فعالی رفتار می شود که تاریخ انقضایشان گذشته است، در نتیجه توانایی های ایران را در اذهان بزرگتر جلوه دهند.

با این همه، بررسی جامع عملیات سایبری مرتبط با ایران بیشتر اوقات دخالت آن کشور را در اقدامات نیابتی برملا می کند. زمانی که وزارت دادگستری ایالات متحده در مارس ۲۰۱۶ مهر کیفرخواست عملیات ابابیل را گشود، از دو نهاد شرکتی ایرانی نام برد که دست کم هفت نفر از پیمانکاران حکومت ایران را استخدام کرده بودند. کیفرخواست به سه تن از شرکت کنندگان در عملیات اشاره کرده بود که جزو «ارتش آفتاب»، یکی از گروه های واسطه ایرانی فعال در تخریب ظاهر سایت ها بودند. ارتش آفتاب تابع همان الگوی مرسوم ارتش سایبری ایران و دیگر سازمان های تخریب سایبری

هماهنگ با حکومت بود که ناگهان ظهور می کردند تا فعالیت های هدفمند سیاسی را ظرف دوران کوتاهی به اجرا بگذارند. اولین عملیات تخریبی ثبت شده آنها در فوریه ۲۰۱۰ اجرا شد که سایت های مرتبط با مهدی کروبی، رهبر اپوزیسیون که اکنون در حبس است را هدف گرفته بود. آن عملیات تخریبی کروبی را متهم به خیانت می کرد و زمان آن به نحوی تنظیم شده بود که در سازماندهی تظاهرات خیابانی ضد حکومت وقفه ایجاد کند.

با حرفه ای تر شدن عملیات امنیت سایبری ایران، برخی از گروه های تخریب گر تصمیم گرفتند بدنامی خود را تبدیل به موفقیت کنند. افشای اطلاعات شخصی عاملان تهدیدکننده نشان می داد که افراد دخیل در عملیات تهاجمی سایبری یا در نهادهای شرکتی (مثل شرکت های مشاوره تکنولوژی اطلاعات) کار می کنند یا پیمانکاران نیروهای امنیتی ایران هستند. مثلاً جنبه هایی از کمپین جاسوسی «مدی» گروهی به نام تیم امنیتی زیرزمینی Mortal Kombat نشانگر یک گروه کوچک ایرانی بود که حداقل از سال ۲۰۰۸ به دنبال فروش نرم افزار جاسوسی و دیگر ابزار هک کردن بود. تداخل مکرر سایت های تجاری دیجیتالی مشروع با سرورهایی که برای کمپین های نفوذی استفاده می شد، اثبات می کند که حد و مرز روشن و واضحی بین آن دو وجود ندارد. بدین ترتیب، یک شرکت می تواند بطور همزمان هم خدمات طراحی وب به مراکز کسب و کار ارائه دهد و هم برای دولت به هک کردن بپردازد.

تغییر یک هکر غیرحرفه ای به پیمانکار سازمان های امنیتی حکومت در ویژگی ها و الگوهای زندگی اکثر عاملان تهدیدکننده دیده می شود. نشانه های مشخصی از اینکه عاملان تهدیدکننده مجری عملیات، صرفاً ایرانیان ساکن داخل کشور- و نه ایرانیان مهاجر یا غیرایرانیان هستند- وجود دارد. در ساده ترین سطح، آنها از همان الگوهای عادی زندگی کارمندان ادارات پیروی می کنند که طی روزهای هفته (شنبه تا چهارشنبه) فعالند و طی تعطیلات کشور، بویژه تعطیلات بلند نوروز یا سال نو ایرانی، کار نمی کنند.

برملا شدن نام های مستعار و واقعی که ناشی از بی توجهی به امنیت عملیات به دلیل حفاظت از پیامدها یا کمبود مهارت بوده است، به افشای زندگی و انگیزه های عوامل ایرانی تهدید کمک کرده است. در حالی که افراد پشت این گروه ها احتمالاً ناسیونالیست یا به لحاظ ایدئولوژیک وابسته به رژیم هستند، به نظر نمی رسد که اعضای ارتش یا دستگاه های امنیتی باشند. این افراد و گروه ها از نظر علایق اجتماعی و مذهبی نیز با هم تفاوت دارند؛ بعضی از آنها در شبکه های اجتماعی خود، استفاده از مواد مخدر را ترویج می کنند و به تبادل پورنوگرافی می پردازند، اما برخی دیگر از صمیم قلب مذهبی هستند و منابع مذهبی را در کدهای بدافزار می گنجانند. عاملان تهدیدکننده ایرانی اغلب از پورنوگرافی به عنوان طعمه در کمپین های spear phishing یا «فیشینگ هدفمند» (جمع آوری اطلاعات شخصی افراد) استفاده می کنند و نوعی شوخ طبعی اهانت آمیز را به نمایش می گذارند.

معیار ارزیابی مستقل دخالت حکومت

کمپین هایی که علیه مخالفان و دیگران در ایران اجرا می شود، کامل ترین گواه دخالت حکومت است. در حالی که ردیابی عواقب جاسوسی خارج از کشور دشوار است، برای کسانی که ساکن کشور هستند، پیامدها به مراتب مستقیم تر و محسوس تر است. همچنان که بین عملیات سایبری و فعالیت های آفلاین نیروهای امنیتی الگوهایی شکل می گیرد، رابطه بین این دو واضح تر می شود. در حالی که این نمونه های همدستی فقط بین تعداد کمی از عاملان تهدیدکننده دیده می شود، الگوها روایت گسترده تری از اکوسیستم نفوذ را اثبات می کنند. عملیات تهاجمی سایبری ایرانیان به دلایل زیر وابسته به حکومت است:

- کمپین ها براساس اطلاعاتی که به نظر می رسد از سازمان های امنیتی گرفته شده اجرا شده اند. در موارد معین، کمپین ها با هماهنگی کارمندان دولت و پیش از دستگیری هدف مورد نظر اجرا شده اند.
- اهداف چنین حملاتی همساز با حساسیت های جمهوری اسلامی هستند و افراد معین به مرور زمان و بصورت مکرر از سوی چندین عامل تهدیدکننده مورد هدف قرار گرفته اند.
- کمپین های مداوم و پر هزینه علیه هزاران هدف اجرا شده اند بدون اینکه انگیزه مالی آشکاری داشته باشند یا نشانه ای مشخص از پایان استفاده از اطلاعات بدست آمده از نفوذ تعیین شده باشد.

در موارد نادر، رابطه احتمالی با حکومت حتی از سوی خود شرکت کنندگان نیز افشا شده است. یاسر بلاغی، یکی از توسعه دهندگان بدافزاری که مرتبط با گروه «راکت کیتن» بود، از طریق یک نام مستعار در کد بدافزار شناسایی شد. بلاغی در سوابق شغلی سال ۲۰۱۳ خود، پروژه های اطلاعات امنیتی و هک کردن را نام برده بود که طی قراردادی با یک «سازمان سایبری» بدون نام اجرا کرده بود. بلاغی تنها کسی نیست که پروژه های هک کردن خود را در سوابق شغلی اش ذکر کرده بود؛ نام های مستعار دیگری هم در کد نرم افزار علیه عربستان سعودی و مخالفان داخل کشور استفاده شده بود که با پروفایل لینکدین افرادی که خود را به عنوان «محقق امنیت اطلاعاتی» در یک گروه «مخفی» معرفی کرده اند، مرتبط هستند.

یکی از دشواری های معمول در تحقیقات امنیت سایبری این است که اغلب به سختی می توان یک تقلب الکترونیکی معمولی را از اختلالات با انگیزه های سیاسی و تلاش های نظارتی مورد حمایت حکومت متمایز کرد، بویژه زمانی که حملات از مهارت و پیچیدگی برخوردار نیستند. دست کم در یک مورد، ایرانیانی که بارها تلاش کرده بودند حملاتی علیه سازمان های سیاست خارجی ایالات متحده و وزارتخانه های امور خارجه متعلق به دو کشور اروپایی اجرا کنند، زیرساخت هایی مرتبط با تقلب های تجاری بانکی نیز داشتند.

در یک نمونه دیگر، همان مهارت های مهندسی اجتماعی که فردی از ارتش سایبری ایران در عملیات تخریبی استفاده کرده بود، در سرقت تجاری دامنه ها و تقلب حساب PayPal هم با موفقیت بکار گرفته شد. اخیراً وزارت دادگستری ایالات متحده در کیفرخواستی علیه یک ایرانی که به تلاش برای اخاذی از شبکه HBO از طریق سرقت

نسخه های پخش نشده اپیزودهای یک سریال تلویزیونی در تابستان ۲۰۱۷ متهم شده بود، ادعا کرد که فرد مزبور از طرف حکومت ایران سیستم های نظامی و زیرساخت های اسرائیل را هم هدف گرفته بود.

تحلیل عملیات تهاجمی سایبری ایران اغلب متکی به نظارت های سختگیرانه در داخل کشور است که خود نشانه حمایت از چنین عملیاتی است- اینکه حکومت اجازه نمی دهد آنچه که نمی خواهد اتفاق بیفتد. با این همه، نظارت های تهران چندان هم مطلق نیستند و بسیاری از عملیات، به دلیل سادگی، مخفیانه اجرا می شوند. فعالیت های سایبری که از ایران سرچشمه می گیرد، ظاهراً بدون اجازه رسمی، رضایت یا حتی آگاهی حکومت هم قابل اجراست. میلیون ها ایرانی هر روز با استفاده از ابزارهای فیلترشکن، سانسور و محدودیت های شبکه ها را دور می زنند و ارتباطات خود را کدگذاری و از نظارت مصون نگاه می دارند. این ابزارها به ایرانیان اجازه می دهد تا به فعالیت های علیه حکومت بپردازند بدوی آنکه مجازات شوند و به این ترتیب، فعالیت های سایبری خود را نیز پنهان کنند. بنابراین، خاستگاه ایرانی صرفاً نشانگر حمایت حکومتی نیست.

ضرر مالی ناشی از عملیات، پیامدهای سیاسی کمپین یا تعداد اهداف نیز لزوماً به طور مستقیم با امکان دخالت حکومت مرتبط نیست. عملیات ویرانگر علیه شرکت «آرمکو سعودی» میلیون ها دلار خسارت به بار آورد، اما از آنجا که بدافزار استفاده شده در آن ابتدایی بود و حمله مستلزم منابع مالی قابل ملاحظه ای نبود، یک فرد بدون هیچ گونه حمایتی توانست آن را اجرا کند. از همین رو، نمی توان با این معیارهای ساده مربوط به ضرر و زیان، اطلاعات کافی درباره میزان دخالت حکومت در فعالیت های سایبری داخل ایران بدست آورد.

نهادهای حکومتی و عاملان تهدیدکننده

همزمانی و هماهنگی عملیات سایبری با دستگیری های ناشی از انگیزه های سیاسی، نشانه بارز دخالت مستقیم حکومت است. حداقل از ژوئیه ۲۰۱۴ یک الگو در این زمینه شکل گرفته است: افرادی که در بازداشت سپاه پاسداران هستند وادار می شوند حساب های آنلاین و دستگاه های خود را در اختیار آنان بگذارند که بلافاصله برای اجرای حملات «فیشینگ هدفمند» از سوی عاملان تهدیدکننده شناخته شده استفاده می شود.

نمونه واضح این هماهنگی را می توان در مورد سیامک نمازی مشاهده کرد، شهروند ۴۶ ساله ایرانی-آمریکایی ساکن دبی که مشاور در زمینه انرژی است و قبلاً محقق در مرکز مطالعاتی بین المللی وودرو ویلسن در واشنگتن دی سی بود. او در اکتبر ۲۰۱۵ ، ماه ها پس از توقیف گذرنامه اش هنگام سفر به کشور، از سوی نیروهای امنیتی ایران دستگیر شد. چند ساعت پس از دستگیری، در حساب های گوگل و فیس بوک نمازی مکالمه ای با جمع گسترده مخاطبان او که در سیاست خارجی و رسانه ها فعال بودند، شروع شد. متجاوزی که تظاهر می کرد نمازی است، مقاله ای به زبان انگلیسی ضعیف درباره توافق هسته ای اخیر به مخاطبان او فرستاد و درخواست ویرایش آن را

کرد. این پیام همراه با یک ایمیل بود که افراد را به یک سایت تقلبی گوگل هدایت می کرد و در آنجا کاربران باید وارد حساب های خود می شدند تا بتوانند آن مقاله را ببینند؛ این تلاشی در جهت سرقت نام و پسورد حساب های کاربری و مرتبط با «راکت کیتن» بود. تعداد زیادی از افراد در این کمپین در معرض خطر قرار گرفتند، از جمله محققان، کارمندان وزارت امور خارجه ایالات متحده، و یک روزنامه نگار برجسته که حساب جی میل او- شامل ارتباطاتش با وزیران سابق امور خارجه آمریکا، رؤسای سازمان سیا، و دیگر وزیران امور خارجه- به مدت تقریباً دو روز بدست هکرهای ایرانی افتاد. این الگو در موارد متعددی در مورد دیگر ایرانیان، دو ملیتی ها و شهروندان خارجی زندانی در ایران تکرار شده است.

تعدادی از عملیات سایبری نیز زمان تدارک برای دستگیری ثبت شده اند. یکی از نمونه های شاخص انتخاب هدف پیش از دستگیری، مربوط به بابک زنجانی، تاجر ایرانی-دانمارکی است که به دلیل فرار از تحریم های ایران، شخصاً از سوی ایالات متحده و اتحادیه اروپا مورد تحریم قرار گرفته بود. پس از اینکه ماه ها ادعاهای بسیاری درباره نقش زنجانی در اختلاس درآمد نفت مطرح شد- روندی که به تحقیق و بررسی مجلس هم کشیده شد- او سرانجام اواخر دسامبر ۲۰۱۳ دستگیر و متهم به «فساد فی الارض» شد. در پی یک روند قضایی غیر شفاف، زنجانی در مارس ۲۰۱۶ به مرگ محکوم شد- حکمی که به گفته وزارت دادگستری، در صورت همکاری زنجانی در بازپس گرفتن سرمایه های خارجی ایران، تخفیف خواهد یافت.

درست چند هفته پیش از دستگیری زنجانی، با تلاشی مستمر حساب های شخصی و زیرساخت های کسب و کار او هدف قرار گرفت. عاملان تهدیدکننده ایرانی به دنبال دستیابی به سرویس iCloud زنجانی بودند و موفق شدند کارمندان وابسته به شرکت سرمایه گذاری او به نام Sorinet را لو دهند. این فعالیت ها نشانگر آن بود که قبل از دستگیری زنجانی، گروه Flying Kitten به اطلاعات محرمانه شرکت های تابعه Sorinet و پرسنل آن دست یافته بود؛ اما مشخص نیست که از مدارک بدست آمده طی آن مدت، در تحقیق و بررسی یا پیگرد قانونی زنجانی استفاده شده باشد. قضیه زنجانی بازتاب جریانی گسترده تر است که در موارد دیگر هم مشاهده شده است: عوامل تهدیدکننده ایرانی در تعقیب های آنلاین خود، غالباً به دنبال آن دسته از افراد هستند که جمهوری اسلامی بطور معمول آنها را آفلاین مورد آزار و اذیت قرار داده است.

اتحاد میان فعالیت های سایبری ایران و سازمان های اطلاعاتی این کشور بدین گونه حمایت می شود که داده های کسب شده طی چنین عملیاتی بندرت افشا می شود. نفوذ به اینترانت نیروی تفنگداران نیروی دریایی آمریکا، حادثه شرکت Las Vegas Sands، و نفوذ به کامپیوترهای کارمندان وزارت امور خارجه آمریکا همگی به انتقال غیرمجاز میزان قابل توجهی از اطلاعات بسیار محرمانه انجامیده است. هیچ نشانه ای از انگیزه های پنهانی- مثل تقلب، اخاذی، تحقیر یا افشا کردن به مطبوعات تندرو وجود ندارد. عملیات ها مستلزم ساختارهای پرهزینه، از جمله سرورهای اختصاصی، ده ها نام دامنه و همچنین وقت کارکنان بوده است. این فعالیت ها باید تا حدی برای اعضای

شرکت کننده ایجاد درآمد هم کرده باشد، هر چند که ارزش اصلی آنها در جاسوسی بوده است. این جریان گسترده و فراگیر بیانگر روابط احتمالی بین عاملان تهدیدکننده معین و سازمان های اطلاعاتی است، روابطی تجاری که زمانی آشکار شد که ایالات متحده ایرانیان را به هک کردن متهم کرد.

فصل سوم

اهداف خارجی ایران

از آنجا که ایران قادر نیست با حریفان آماده تر از خود مبارزه ای نتیجه بخش یا بازدارنده داشته باشد، دست به حملات ویرانگر و فرصت طلبانه ای می زند تا توان خود را در تلافی کردن به اثبات برساند. این کشور بویژه در خاورمیانه می تواند آن دسته از منابع زیرساختی و اقتصادی حریفان خود که از حمایت کافی برخوردار نیستند را در صورت جنگ، بطور ضمنی تهدید به عملیات سایبری کند. در واقع، اهداف و قربانیان عملیات سایبری ایران در منطقه اغلب شامل صنایعی مثل بانک ها و فرودگاه ها هستند، که ظاهراً برای این کشور هیچ کاربردی بجز ایجاد پایگاه هایی در کشورهای رقیب ندارد.

نتایج موردنظر عملیات مختل کننده متفاوتند: از ارعاب گرفته تا نابودسازی اهداف خارجی، و از شرمنده کردن گرفته تا زیان حیاتی به مخالفان داخلی. هدف گرفتن یا نفوذ به سیستم ها به تنهایی کافی است تا تهران تمایل و توانایی خود به ضربه زدن به مخالفان را نشان دهد. تهدیدهای گاه به گاه ایران به بستن تنگه هرمز طی زمان های بحرانی- تنگه ای که حدود ۶۰ درصد از موجودی نفتی جهان روزهای مقرر از آن می گذرد- تأیید این مسئله است. اما با توجه به غیرشفاف بودن حکومت ایران، پیام ها و انتظارات مورد نظر این کشور می تواند به راحتی به غلط تفسیر شده و احتمال خطر مناقشه ای غیرعمد را افزایش دهد.

با این همه، چنین حملات مخربی در مقایسه با کمپین های جاسوسی ایران علیه نهادهای دولتی و اقتصادی کشورهای خارجی نادر هستند. این کمپین ها به نحوی فزاینده هم پایه و اساس انتقام جویی های طی مناقشه شده اند، هم نوعی ساز و کار برای کنترل تهدیدات در حال ظهور هستند. مثلاً چند روز پس از کشته شدن بیش از ۴۵۰ زائر ایرانی در اثر ازدحام در مراسم حج سپتامبر ۲۰۱۵ ، اسامی دامنه ای که هویت حکومت عربستان و وزارت حج را جعل می کرد از سوی عوامل تهدیدکننده ایرانی که شناخته شده بودند، ثبت شد. زمانی که روابط و ارتباطات بین دو کشور، بویژه به دلیل سرنوشت یک دیپلمات گمشده، سریعاً رو به زوال گذاشت، جاسوسی سایبری به ابزار کسب اطلاعات برای تهران تبدیل شد.

گذشته از عربستان سعودی، دانمارک، آلمان، اسرائیل و ایالات متحده نیز در میان کشورهایی هستند که آشکارا تلاش های جاسوسی گروه های ایرانی را علیه دولت، ارتش یا نهادهای علمی خود افشا کرده اند. تهران همچنین کشورهای همسایه در سرتاسر خاورمیانه را هدف قرار می دهد. به رغم گوناگونی عاملان تهدیدکننده ای که از جانب حکومت ایران عمل می کنند، الگوهای رفتاری آنها- از جمله اهدافشان- طی زمان معمولاً ثابت مانده است.

ایالات متحده و اروپا

در سپتامبر ۲۰۱۲ ، گروهی که خود را «جنگجویان سایبری عزالدین قسام» می نامیدند، یک کمپین حملات DDoS را علیه بخش مالی ایالات متحده آغاز کردند. پیش از این کمپین، مجرمان از آسیب پذیری در نرم افزار هزاران وب سایت سوء استفاده کرده بودند تا یک پلتفرم حمله تحت کنترل خود ایجاد کنند. با این ارتش سرورها در شرکت های میزبان، مهاجمان توانستند اهداف خود را در معرض توفانی از ترافیک سنگین و مخرب اینترنتی قرار دهند. در اولین مرحله از عملیات «ابابیل»، این گروه زیرساخت های بانکی ایالات متحده را هدف قرار داد. سیستم ها و بانک های اطلاعاتی قربانیان که برای چنین حجمی از ترافیک آمادگی نداشتند (اداره تحقیقات فدرال آمریکا اعلام کرد که بیشترین میزان ترافیک نزدیک به ۱۴۰ گیگابایت در هر ثانیه بوده که سه برابر ظرفیت بانک ها در آن زمان محسوب می شد)، به دلیل افزایش چشمگیر تقاضا از کار افتادند.

مراحل بعدی کمپین چندان نتیجه بخش نبود، چرا که بخش مالی بطور پیوسته سیستم دفاعی اش را بهتر می کرد. تا چهارمین تلاش برای حمله در ژوئیه ۲۰۱۳ ، تأثیر قابل مشاهده ای بدست نیامد. اما به گفته اف بی آی، عملیات «ابابیل» موجب شد صدها هزار نفر از مشتریان بانک ها مدتی طولانی نتوانند به حساب های خود دسترسی داشته باشند که به دهها میلیون دلار خسارت انجامید. علاوه بر این، گزارشی از سازمان امنیت ملی آمریکا انگیزه عملیات «ابابیل» را اینگونه توضیح می دهد: «[سیگنال های اطلاعاتی] نشان می دهد که این حملات در تلافی فعالیت های غرب علیه بخش اتمی ایران صورت گرفته و مقامات بلندپایه حکومت ایران نیز از این حملات آگاهی داشته اند.»

عملیات «ابابیل» مخرب ترین حمله ایران به ایالات متحده محسوب می شود. در حالی که آژانس بین المللی انرژی اتمی (IAEA) ادعا کرد که ایران دستگاه های بازرسان آن سازمان را طی بازدیدشان در سال ۲۰۱۱ به صورت الکترونیکی نظارت و دستکاری کرده بود، اطلاعاتی درباره جاسوسی سایبری ایران تا پیش از سال ۲۰۱۲ وجود نداشت. آن تابستان اولین نشانه های علنی مبنی بر اینکه عوامل تهدیدکننده ایرانی، کمپین هایی به منظور جاسوسی از رقبای خود به راه انداخته اند، دیده شد. گزارش شد که کمپین بدافزار «مدی» در طول یک سال تا ۸۰۰ قربانی را به مخاطره انداخته است. کشورها و نهادهایی که مورد هدف قرار گرفته بودند از آینده عملیات سایبری ایران به شرکت های نفتی، اندیشکده های ایالات متحده، سازمان های دولتی، شرکت های مهندسی، نهادهای مالی و جوامع دانشگاهی این کشور خبر می دادند.

چندین کشور غربی در کیفرخواست ها و گزارشات امنیتی، مدارکی پیرامون عملیات سایبری ایران تهیه کرده اند. افزون بر عملیات «ابابیل»، ادعا شده که ایران از اوت ۲۰۱۳ به مدت چندین ماه به اینترانت غیرمحرمانه نیروی تفنگداران آمریکا- سیستمی که قبلاً اطلاعات و ارتباطات غیرمحرمانه را ذخیره می کرد- دسترسی داشته است. در نسخه ۲۰۱۶ یک ارزیابی امنیتی سالیانه وزارت کشور، دولت آلمان از ایران به عنوان منبع جدید جاسوسی سایبری علیه آن کشور نام برده است. این افشاگری هماهنگ با گزارش هایی است که براساس آن، مجلس آلمان تحت تأثیر یک عملیات بدافزاری قرار گرفته که خوانندگان روزنامه اسرائیلی جروسلم پست را هدف قرار داده بود.

با این همه، بطور کلی مواردی که نفوذ ایران به زیرساخت های دولتی آمریکا و اروپا- بویژه شبکه های محرمانه بسیار امن- موفق بوده، نادر است. سازمان های دولتی معمولاً تحت حفاظت شدیدی قرار دارند، به نحوی که عاملان تهدیدکننده ایرانی توانایی نفوذ به آنها را ندارند. در نتیجه، ایران به دنبال اهداف ساده تری رفته و تلاش کرده ایمیل های شخصی و حساب های شبکه های اجتماعی کارمندان دولت ایالات متحده را مورد حملات «فیشینگ هدفمند» قرار دهد. با اینکه کمتر احتمال دارد حساب های شخصی دارای اطلاعات محرمانه دولتی باشند، اما احتمال امن بودن آنها هم کمتر است، و اغلب حاوی اطلاعات مفیدی مثل مطالب شخصی بوده و نشانه هایی از ارتباطات حرفه ای در آنها دیده می شود.

مثلاً طی مذاکرات هسته ای، ایران تلاش کرد به ایمیل های شخصی اعضای تیم آمریکایی را نفوذ کند. به همین صورت، پس از انتخابات ۲۰۱۶ ریاست جمهوری ایالات متحده، عوامل تهدیدکننده ایرانی بر کارمندان سابق اوباما، اعضای جمهوریخواه کنگره، حامیان کمپین دانلد ترامپ، سازمان های رسانه های محافظه کار و نامزدهای مناصب سیاسی متمرکز شدند تا درباره دولت جدید آمریکا اطلاعات کسب کنند. اخیراً این حملات «فیشینگ هدفمند»، منتقدان ایران در کنگره ایالات متحده را در زمانی که تحریم های جدید در حال بررسی است، هدف گرفته است.

تهران به دنبال آن است که کارکنان و سازمان های دولت های خارجی در ایالات متحده یا اروپا را که متمرکز بر ایران هستند، یعنی در زمینه سیاست های ایران یا در رسانه های فارسی زبان، مثل تلویزیون صدای آمریکا یا رادیو فردا فعال هستند، مورد هدف قرار دهد. عاملان تهدیدکننده ایرانی از حساب های لو رفته شهروندان ایرانی-آمریکایی برجسته، تاجران بین المللی و دیگر دوملیتی های دستگیر شده توسط سپاه پاسداران استفاده کرده اند تا هویت آنها را جعل کنند و حساب های ایمیل کارکنان وزارت امور خارجه ایالات متحده که در زمینه سیاست ایران فعال هستند را مورد هدف قرار دهند.

بر خلاف انتشار ایمیل های شخصی از سوی ویکی لیکس طی انتخابات ۲۰۱۶ ایالات متحده که از ایمیل های به سرقت رفته به عنوان اهرم فشاری برای جنگ اطلاعاتی استفاده شد، نفوذ به ایمیل های کارمندان وزارت امور خارجه به خرابکاری قابل مشاهده یا افشای مطالب شرم آوری منجر نشد. با آنکه تلاش های بسیاری در جهت هدف قرار دادن جمع گسترده ای از سیاستمداران آمریکایی و کارمندان دولت آن کشور صورت گرفته، اما تمام آنها عمدتاً فرصت طلبانه بوده و به عملیاتی پیچیده تر گسترش نیافته است.

پس از توافق اتمی سال ۲۰۱۵ ، فعالیت های مخفیانه و حملات تلافی جویانه بین واشنگتن و تهران کاهش یافته است. زمانی که تهران بیشتر بر مخالفان سیاسی داخل کشور و دشمنان منطقه ای، مثل اسرائیل و عربستان سعودی، متمرکز شد، گزارش های مربوط به عملیات سایبری مخرب علیه ایالات متحده و زیرساخت های ایران تقلیل یافت. درست همانطور که «عملیات بازی های المپیک» به واشنگتن این امکان را داد تا ایران را بدون دخالت نظامی

مستقیم تحت فشار قرار دهد، تهران نیز اکنون از عملیات تهاجمی سایبری استفاده می کند تا قدرت منطقه ای خود را به نمایش بگذارد.

عربستان سعودی

به نظر نمی رسد که هیچ کشور دیگری به اندازه عربستان سعودی در معرض تعداد بسیاری از عملیات تهاجمی سایبری از سوی عاملان تهدیدکننده ایرانی با حمایت حکومت قرار گرفته باشد. هر دو کشور به لحاظ قومی (عرب در مقابل ایرانی)، فرقه ای (سنی در مقابل شیعه) و بیش از همه به لحاظ ژئوپلتیک با یکدیگر رقابت داشته و در جنگ های نیابتی خونین در عراق، سوریه و یمن و همچنین نبردهای سخت سیاسی در بحرین و لبنان دو جناح مخالف یکدیگر به شمار می آیند. رابطه میان تهران و ریاض از انقلاب اسلامی ۱۹۷۹ اغلب تنش آلود بوده و پیوندهای رسمی دیپلماتیک بین دو کشور به دلیل اختلاف نظرهای سیاسی بطور متناوب معلق شده است. اخیراً عربستان سعودی در ژانویه ۲۰۱۶ سفارت خود در تهران را تعطیل کرد؛ این امر در پی حمله اراذل و اوباش با حمایت حکومت ایران به آن مکان صورت گرفت.

از ابتدای عملیات سایبری ایران، نهادهای سیاسی و اقتصادی سعودی از سوی تهران و به منظور جاسوسی و تخریب مورد نفوذ قرار گرفته اند. در گزارش های گوناگون پیرامون بدافزارها و کمپین های سرقت نام و پسورد حساب های کاربری بدست ایرانیان، از جمله تلاش برای دستیابی به پسوردها یا اطلاعات مربوط به بازیابی حساب ها، عربستان سعودی یکی از معمول ترین منابع قربانیان و اهداف بوده است. این الگو نشانگر اختلاف نظرهای عمیق ایدئولوژیک و ژئوپولیتیک (قصد) بین دو کشور و همچنین ضعف های مستمر عربستان سعودی در زمینه فضای سایبری (فرصت) است.

حمله ۱۵ اوت ۲۰۱۲ ایران به شرکت «آرمکو سعودی» طی تعطیلات عید مسلمانان (و حمله ای مشابه علیه شرکت RasGas قطر دو هفته بعد از آن)، نمونه بارز نحوه استفاده ایران از عملیات تهاجمی سایبری به منظور انتقامجویی از دشمنان خارجی است. زمانی که عاملان خارجی با اقدامات مخفی خود زیرساخت های اتمی و نفتی ایران را هدف گرفتند، گروه های ناشناخته ای که وانمود می کردند «هکتیویست» (هکر و کنشگر) مستقل با انگیزه های مبتنی بر میهن پرستی و ارزش های اسلامی هستند، شروع به سازماندهی حملات مخرب علیه زیرساخت های اقتصادی در عربستان سعودی و ایالات متحده کردند.

اقدامات تلافی جویانه را با استفاده از واسطه ها اجرا می کردند تا آن اقدامات به آنان نسبت داده نشود و یا بتوانند به نحوی قابل باور آنها را تکذیب کنند. در اثر حمله «شامون»، که براساس بدافزار مورد استفاده نامگذاری شده بود، به دهها هزار کامپیوتر شرکت «آرمکو سعودی» نفوذ شد و ده تا صدها میلیون دلار خسارت به بار آورد. گروهی که

خود را Cutting Sword of Justice (شمشیر برنده عدالت) می نامید، مسئولیت آن حمله را به عهده گرفت که طی آن تصویری از پرچم به آتش کشیده شده آمریکا جایگزین داده های قبلی دیسک های سخت کامپیوترهای آرمکو شد و به سرافکندگی آن شرکت انجامید. به رغم عملیات سایبری نهادهای خارجی علیه ایران، حملات تلافی جویانه این کشور بیشترین توجه را می طلبید.

اولین بررسی های آن حادثه نشان می داد که «شامون» احتمالاً از بدافزار «وایپر» الهام گرفته که در آوریل ۲۰۱۲ ایران را هدف گرفته بود، چرا که هر دو از یک شیوه خرابکاری، یعنی نابودسازی داده های ذخیره شده، استفاده کرده بودند. انگیزه بالقوه تهران برای اقدام تلافی جویانه، عملیات سایبری علیه زیرساخت های تولید نفت خود بود. پیام «شامون» واضح به نظر می رسید: ایران شاید همیشه قادر نباشد در برابر توانایی های پیشرفته تر سایبری از خود دفاع کند، اما می تواند با مقابله به مثل هزینه های کلانی به متحدان ایالات متحده تحمیل کند.

چرخه تلافی جویانه حملات مخفیانه ویرانگر و انتقام جویی های نمادینی که در «شامون» و «ابابیل» دیده می شود، نشانگر تاکتیک های امنیتی ایران در خصومت های آفلاین این کشور است. مثلاً بین سال های ۲۰۱۰ و ۲۰۱۲ ، چندین دانشمند هسته ای ایرانی در شرایطی مرموز ترور شدند که این اقدامات به ایالات متحده یا اسرائیل نسبت داده شد. تهران ظاهراً در اقدامی تلافی جویانه تلاش کرد مقامات اسرائیلی را در مکان هایی که انتظارش نمی رفت، مثل گرجستان، هند و تایلند ترور کند که موفق نشد. این چرخه که مضمون مکرر فعالیت های مخفیانه ایران است، نمایانگر آن است که این کشور از حملات می آموزد و به همان شکل تلافی می کند؛ این امر معیارهای احتمالی برای درک علامت دهی ها و انگیزه های ایران در اجرای عملیات مخرب سایبری فراهم می کند.

در مقایسه با دیگر دشمنان ایران (یعنی ایالات متحده و اسرائیل)، نهادهای دولتی و اقتصادی سعودی هنوز باید سیستم ها و پروتکل های کافی برای افزایش امنیت سایبری ملی به اجرا بگذارند. عاملان ایرانی مجموعه ای گسترده از نهادهای اقتصادی، نظامی و سیاسی در عربستان سعودی، از جمله شرکت «آرمکو سعودی» و شرکای خارجی آن، بنیاد ملک فیصل، وزارتخانه های بازرگانی و امور خارجه، بورس اوراق بهادار سعودی و حتی مدافعان عرب حقوق بشر را هدف گرفته اند. پژوهشگران موارد بسیاری ثبت کرده اند که به شرکت ها و سازمان های سعودی نفوذ شده است؛ یکی از این نمونه ها به استخراج میزان وسیعی از داده های آرشیوی اختصاصی و چندین ساله یک شرکت توسعه صنعتی انجامید.

دفاع سایبری ضعیف عربستان سعودی نه تنها این کشور را در برابر تهدیدات ایران آسیب پذیر کرده، بلکه ریاض را به هدفی آسان برای اقدامات تلافی جویانه تهران علیه عملیات مخرب سایبری که کشورهای ثالث به اجرا می گذارند، تبدیل کرده است. اگر ایران طی زمان مناقشه نتواند ضرر و زیان قابل ملاحظه ای به ایالات متحده بزند، به آسیب رساندن به نهادهای اقتصادی متحدان آمریکا بسنده می کند.

کمپین فشارهای سرکوبگرانه نیز همچنان ادامه دارد: وزارت دفاع سعودی و سایر شبکه ها، حملات DDoS را همان زمانی متحمل شدند که حمله به سفارت کشور خود را هنگامی که بدافزار به روز شده «شامون» که در حادثه آرمکو استفاده شده بود (پژوهشگران نام آن را «شامون ۲» گذاشتند) مجدداً از نوامبر ۲۰۱۶ تا ژانویه ۲۰۱۷ پدیدار شد، بانک های اطلاعاتی و فایل هایی که هم متعلق به دولت و هم بخش خصوصی بودند، از جمله سازمان هواپیمایی کشوری، وزارت کار، بانک مرکزی سعودی و شرکت های استخراج منابع طبیعی را از میان برد. «شامون ۲» حاوی اشاراتی به یمن بود و دیسک های سخت قربانیان را با تصویری از یک کودک پناهجوی سوری به نام «آلان کردی» جایگزین و تخریب کرد که نشان می داد حملات در تلافی سیاست های عربستان سعودی در قبال سوریه و یمن بوده اجرا شده اند.

اسرائیل

یکی از ستون های ثابت سیاست خارجی ایران، ضدیت با موجودیت اسرائیل و حمایت از گروه های جنگ طلب ضد اسرائیلی، مثل حزب الله، حماس و جهاد اسلامی فلسطین بوده است. با این همه، تهران در عملیات سایبری علیه نهادهای اسرائیلی که با هدف تخریب و جاسوسی اجرا شده، موفقیت چندانی نداشته است. اسنادی که در عملیات «مدی» به عنوان طعمه استفاده شده بود، معمولاً به زبان عبری نوشته شده یا به سیاست های امنیتی اسرائیل اشاره داشت؛ پژوهشگران در آن کمپین نفوذ به پنجاه و چهار نهاد در اسرائیل را ثبت کرده اند. طی مناقشه میان اسرائیل و غزه در تابستان ۲۰۱۴ ، معروف به Operation Protective Edge (عملیات لبه محافظ)، مقامات ادعا کردند که زیرساخت های نیروهای دفاع اسرائیل هدف حملات DDoS از سوی مجموعه وسیعی از جنگ طلبان، از جمله تهران قرار گرفته است. این حملات DDoS هماهنگ با توانایی های شناخته شده عاملان تهدیدکننده ایرانی، شامل تاکتیک های استفاده شده علیه ایالات متحده و مخالفان بود.

به رغم سابقه حملات DDoS و تخریب وب سایت های اسرائیلی، توانایی تهران در وارد کردن خسارات عمده به اسرائیل از طریق عملیات سایبری تا بحال محدود بوده و شاید در حال کاهش هم باشد. با توجه به مهارت های دفاع سایبری اسرائیل، تهران مجبور بوده عمدتاً بر اهداف ساده، در پی فرصت های محدود جاسوسی و تخریب احتمالی منابع غیرنظامی در صورت مناقشه متمرکز بماند.

ایران با هدف گرفتن اسرائیلی ها، مثل شهروندان آمریکایی، تأکید بر افرادی دارد که پیرامون ایران و سیاست های منطقه فعالیت می کنند. تهران در تلاش های «فیشینگ هدفمند» علیه نهادهای دانشگاهی، مقامات امنیت ملی، دیپلمات ها، اعضای پارلمان اسرائیل (کنست) و شرکت های هوافضای اسرائیلی دست داشته است. به همین ترتیب، عاملان ایرانی معمولاً دامنه های مخربی ایجاد کرده اند که از دامنه های متعلق به کمیته روابط عمومی آمریکا-اسرائیل

(AIPAC) تقلید کرده و کارمندان سازمان های یهودی لیبرال و محافظه کار در ایالات متحده و دیگر کشورها را هدف گرفته است.

با آنکه ایران موفقیت هایی در زمینه نفوذ به نهادهای غیرنظامی کوچکتر داشته است، اما تلاش مشهودی برای استفاده سرکوبگرانه از این رخنه کردن ها نداشته است. مسلح نکردن بلافاصله این نفوذها نشانگر آن است که چگونه محاسبات استراتژیک نتایج را شکل می دهند. نابودسازی اطلاعات بانکی یا داده های پزشکی به دلیل چالش های موهوم با جمهوری اسلامی، شاید ارزش اقدام تلافی جویانه از سوی اسرائیل را ندارد (عربستان سعودی فاقد چنین تهدیدی است). شاید تنها نفوذ به چنین نهادهایی کافی باشد که تمایل ایران به اینکه از طریق عملیات تهاجمی سایبری، اسرائیل را در معرض یک تهدید تلافی جویانه و قابل باور قرار دهد برآورده کند. بدون تردید، توانایی های سایبری مناسبات قدرت بین ایران و اسرائیل را تغییر نداده است، و احتمالاً تفاوت در ظرفیت های تکنیکی، وضعیت ایران نسبت به دشمن خود را شکل می دهد.

متحدان و دشمنان منطقه ای

در حالی که عملیات مخرب سایبری تهران در منطقه عمدتاً عربستان سعودی را هدف قرار داده، اما دیده شده که تعداد بسیاری از عاملان تهدیدکننده ایرانی تقریباً تمام کشورهای خاورمیانه، شمال آفریقا و کشورهای هم مرز ایران را هدف قرار داده اند. به عنوان مثال، «مجیک کیتن» در خاورمیانه و جنوب آسیا با موفقیت به کامپیوتر قربانیان خود نفوذ کرد. این الگو در عملیات «مدی» و حملات بعدی تا زمان حاضر تکرار شده است.

جاسوسی سایبری، آگاهی تهران نسبت به همسایگان خود را که به لحاظ سیاسی اغلب بی ثبات هستند، بیشتر کرده است. عاملان تهدیدکننده ایرانی بارها علاقه خود به زیرساخت های کشورهای همسایه، از جمله رادیوی ملی افغانستان، وزارت آموزش و پرورش و شبکه دولتی نشان داده اند. شاخص های دیگر همچنین حاکی از تمایل به سازمان های امنیتی و دفاعی پاکستان و افغانستان است. پروفایل های ساختگی در شبکه های اجتماعی و کمپین های «فیشینگ هدفمند» هم معمولاً عراقی ها، بویژه مهندسان شبکه های ارتباطات مخابرات و نخبگان سیاسی، را هدف گرفته است. علاوه بر این، گروه های ایرانی علاقه ای وافر و فعال به نهادهای سیاسی کردستان عراق نشان داده اند.

گذشته از این، تعداد زیادی از عاملان تهدیدکننده ایرانی در حملات «فیشینگ هدفمند» علیه ده ها نفر مرتبط با سازمان های حقوق بشر، جنبش های سیاسی و رسانه های مستقل در یمن، کشوری که ایران در آن یک جنگ نیابتی با عربستان سعودی دارد، شرکت داشته است. شرکت امنیت سایبری ClearSky در اسرائیل پی برد که ۱۱ درصد اهداف یک کمپین سرقت نام و پسورد حساب های کاربری (راکت کیتن) در سال ۲۰۱۵ با یمن مرتبط بوده اند. این

عملیات بطور مشخص از موضع ایران در مناقشه یمن حمایت می کرد که اخیراً منتقدان برجسته حوثی ها، گروه مسلمانان شیعه مورد حمایت ایران طی جنگ داخلی آن کشور، را هدف گرفته بود.

گفته می شود که عاملان ایرانی همچنین مخالفان سوری رژیم بشار اسد -از جمله آنان که در تبعید هستند- را در موارد محدود مورد هدف قرار داده اند. همچنین براساس گمانه زنی ها، ایران از عملیات تهاجمی سایبری متحدان سنتی خود، سوریه و حزب الله حمایت کرده است، بویژه پس از اینکه مخالفان سوری از سال ۲۰۱۲ هدف کمپین های مستمر بدافزارها قرار گرفتند. اما نه شواهد و مدارک چندانی در زمینه همکاری تکنیکی وجود دارد، نه اینکه سوریه و حزب الله به چه دلیل باید برای کسب توانایی متکی به ایران باشند.

در حالی که نشانه های موثقی از اینکه تهران به سوریه ابزار جنگی الکترونیکی سنتی داده است وجود دارد، رژیم اسد ظاهراً نیازی به کمک گسترده در زمینه توسعه توانایی های تهاجمی سایبری نداشته است. مجموعه ای پیچیده و بومی از هکرها که بستگان اسد سازماندهی کرده بودند، از ابتدای جنگ داخلی توانسته بودند مخالفان رژیم را به نحوی مؤثر هدف بگیرند. گروه های کوچکی از هکرها در سوریه معمولاً از یک نرم افزار جاسوسی استفاده کرده اند که بین گروه های هکر عرب علیه مخالفان اسد متداول بود. برعکس، با وجود آنکه اطلاعات چندانی در خصوص توانایی های تهاجمی سایبری حزب الله وجود ندارد، در گزارشی مربوط به سال ۲۰۱۵ درباره بدافزار و عملیات آنها آمده است که این گروه لبنانی ظاهراً از حامی ایرانی خود فراتر رفته است.

نبود مدارک خارجی درباره همکاری این دو کشور مانع از دیگر تلاش های هماهنگ یا به اشتراک گذاری اطلاعات بین آنها نمی شود، اما عملیات سایبری ابتدایی از جنگ های الکترونیکی- مانند پارازیت انداختن روی سیگنال، جمع آوری رادار و محل سیگنال- یا دیگر دامنه های نظامی که مستلزم پایگاه دفاعی صنعتی هستند ساده ترند. در هیچیک از قابلیت ها یا حوادث شناخته شده، دانش تخصصی که مستلزم حمایت خارجی باشد دخالت نداشت، و همه پروفایل های مستقلی در خصوص چگونگی اجرای عملیات خود داشتند. ایرانیان از همان ابزار جاسوسی مفید گروه های سوری استفاده نکرده بودند؛ این امر نشانگر آن است که گروه های طرفدار اسد بیشتر مدیون هکرهای محلی هستند تا دیگر کشورها. علاوه بر این، عدم همکاری ایران با متحدان یا قدرت های خارجی دوست، نشانگر عوامل دیگری است که بر تصمیمات مبنی بر اشتراک گذاری منابع تأثیر می گذارد. متحدان هم از یکدیگر جاسوسی می کنند: شاید ایران همچنین بخواهد بسته ابزاری خود را برای خود نگاه دارد تا بتواند در موقعیت های مورد اختلاف نظر، مثل ثبات و وفاداری، رژیم اسد را تحت نظر داشته باشد.

اهداف تجاری

بر خلاف چین، ایران استفاده محدودی از جاسوسی تجاری می کند، چرا که فاقد بخش تولید صنایع است که در آن مالکیت معنوی به سرقت رفته می توانست مورد استفاده قرار گیرد. فعالیت های جاسوسی صنعتی ایران بیشتر در خدمت ترقی صنایع و مهارت های تکنولوژیکی نظامی است تا بخش تولیدات داخلی. در ضمن، این کشور تلاشی هم نکرده تا تأثیرات تحریم های اقتصادی را با جرائم مالی گسترده منحرف کند، همانگونه که ظاهراً کره شمالی این کار را کرده است. طبق گزارشات علنی و کمپین هایی که مستقیماً رصد شده اند، نهادهای تجاری که عاملان تهدیدکننده ایرانی هدف گرفته اند چهار دسته اند:

- هوا-فضا و هواپیمایی کشوری
- پایگاه صنایع نظامی و بخش امنیتی
- منابع طبیعی و صنایع استخراجی
- شرکت های مخابرات

شواهد و مدارک دال بر علاقه ایران به سرقت رازهای دفاعی از چندین گزارش امنیت سایبری، حوادث مشاهده شده و کیفرخواست های ایالات متحده بدست آمده است. یک ایرانی به نام نیما گلستانه که از ترکیه به ایالات متحده تحویل داده شد، اعتراف کرد که در سال ۲۰۱۲ در هک کردن شرکت دفاعی Arrow Tech Associates واقع در ورمنت دست داشته است؛ او در عملیات کسب نسخه های شبیه سازی سیستم سلاحی آنها به منظور فروش نرم افزار به حکومت ایران و نهادهای نظامی شرکت کرده بود. این قضیه مقدمه ای بر تلاش های بعدی بود.

اوایل سال ۲۰۱۴ به موازات هدف گرفتن برنامه های توسعه زنان ایران و دیگران، عامل تهدیدکننده Flying Kitten، وب سایت یک کنفرانس سیستم هوا-فضا را جعل کرد تا آن بدافزار را بین پیمانکاران دفاعی پخش کند، تاکتیکی که هنوز هم علیه صنایع دفاعی استفاده می شود. یک عامل تهدیدکننده ایرانی دیگر از سال ۲۰۱۵ تا ۲۰۱۶ مرتب به ایجاد وب سایت های ساختگی برای شرکت دفاعی آمریکایی Oshkosh می پرداخت تا نام و پسورد حساب های کاربری شبکه داخلی محرمانه آن شرکت را بدست آورد؛ این عامل همچنین به هدف قرار دادن شرکت های هواپیمایی، از جمله تولیدکنندگان موتور هواپیما و شرکت های ماهواره ای ادامه داد. گزارش های مربوط به تلاش های عاملان تهدیدکننده ایرانی در جهت جاسوسی نظامی به شدت یک شکل هستند و مجموعه ای گسترده از صنایع، بویژه تکنولوژی های هوا-فضا را در برمی گیرند.

اما به نظر می رسد که این عملیات موفقیت چندانی نداشته اند. از آنجا که شرکت هایی مثل Oshkosh هم در صنعت دفاعی و هم در زمینه مسائل مرتبط با جاسوسی صنایع توسط چین هم فعالند، امنیت اطلاعاتی را اولویت قرار داده اند، به نحوی که سازمان های غیردولتی این کار را انجام نداده اند. بنابراین، با وجود آنکه معمولاً نشانه هایی از مورد هدف

قرار گرفتن کارمندان شرکت و حتی نفوذ به کامپیوترهای آنها دیده می شود، به ندرت گزارشی از سرقت مطالب سری و فوق العاده حساس توسط ایران به چشم می خورد.

هدف قرار دادن شرکت های دفاعی همچنین بیش از آنکه صرفاً به منظور سرقت تکنولوژی های نظامی باشد، ناشی از سیاست های منطقه ای است. چندین شرکت صنایع دفاعی مثل Oshkosh که مورد هدف عاملان تهدیدکننده ایرانی قرار گرفته اند، به میزان قابل توجهی به عربستان سعودی و دیگر کشورهای خلیج کمک های امنیتی و نظامی می کنند. بسیاری از شرکت های آمریکایی، از جمله Oshkosh که از سوی وزارت امور خارجه ایران در مارس ۲۰۱۷ در اقدامی تلافی جویانه به دلیل نقض حقوق بشر و ارتباط با ارتش اسرائیل مورد تحریم قرار گرفتند هم هدف عملیات سایبری ایران بوده اند.

مانند دیگر حوزه ها، تعیین قصد و نیت ایران صرفاً از طریق کسانی که هدف قرار می دهد یا هویت آنان را جعل می کند، دشوار است. در موارد معین، به نظر می رسد که عوامل تهدیدکننده ایرانی مشاوران فن آوری اطلاعات که ساکن خاورمیانه بوده اند را به دلیل دولت ها یا کسب و کارهایی که مشتری آنها بوده اند، به مخاطره انداخته اند. این عملیات اغلب کارمندان شرکت های واقع در خاورمیانه را هدف می گیرند که احتمالاً علت آن کسب اطلاعات در خصوص توانایی های نظامی رقیبان یا دستیابی به دیگر اهداف (مثل حملات زنجیره ای) است. یک کمپین اخیر دیگر که با ظاهر و شمایل شرکت Boeing و Northrop Grumman اجرا شد، بر بخش های نظامی و هواپیمایی تجاری عربستان سعودی متمرکز بود.

به همین ترتیب، ایران با هدف قرار دادن شرکت های مخابرات، بانک ها و شرکت های هواپیمایی کشوری می تواند پایگاهی در زیرساخت های حیاتی برای خود مهیا سازد، آنچه که احتمالاً به زیان های اقتصادی قابل ملاحظه یا حتی به مخاطره انداختن زندگی افراد منجر خواهد شد. اما به نظر می رسد که تهران تا کنون از چنین اهدافی برای عملیات شناسایی استفاده کرده که بازتاب فعالیت های سایبری دیگر کشورهاست. با این همه، طبق دلایل موجه و نگران کننده، قصد تهران از هدف گرفتن زیرساخت های حیاتی این است که دارایی های اجتماعی و اقتصادی در کشورهای دشمن را- در صورت نیاز به تشدید یا تلافی طی دوران مناقشه- در معرض خطر قرار دهد.

فصل چهارم

اهداف داخلی ایران

سابقه عملیات سایبری تهاجمی ایران ثابت کرده است که همان عاملان تهدیدکننده ای که مسئول جاسوسی علیه بخش خصوصی هستند در نظارت بر مدافعان حقوق بشر مشارکت دارند و با توجه به محدودیت منابع مدافعان، این گروه موفقیت چشمگیری داشته اند. از دریچه این حملات، رابطه بین فعالیت های سایبری آغاز شده از ایران و حکومت این کشور و همچنین انگیزه های چنین عملیاتی مشخص تر می شود. این انجمن ها از تاکتیک ها و ابزاری خبر می دهند که علیه دیگر اهداف مورد استفاده قرار خواهند گرفت، و افزایش اطلاعات در این زمینه به استراتژی های آموزشی و تعدیلی مفیدتر منجر خواهد شد.

در حالی که اینترنت امکانات جدیدی برای نهادهای امنیتی تهران فراهم آورده تا بر ارتباطات شهروندان خود نظارت و از آن جلوگیری کند، فن آوری های اطلاعاتی همزمان میزان دسترسی حکومت را نیز محدود می کند. ایران یکی از نخستین کشورهای خاورمیانه بود که به اینترنت متصل شد، و در نتیجه بیش از نیمی از جمعیت آن از مارس ۲۰۱۷ به بعد، اینترنت را اغلب مورد استفاده قرار داده اند. کاربران ایرانی اینترنت به سرعت از شبکه های اجتماعی و اپلیکیشن های ویژه چت به عنوان محل های تبادل نظر که در آن آزادی های اجتماعی بیشتری وجود دارد، استقبال کردند.

از آنجا که شهروندان ایرانی ارتباطات خود را به پلتفرم های اینترنتی میزبان واقع در خارج از ایران منتقل کرده و با استفاده از رمز گذاری، ارتباطات خود را در برابر شنود محافظت کرده اند، از ابزار سنتی تری که نیروی انتظامی ایران و نهادهای امنیتی برای نظارت استفاده می کنند، گریخته اند. در حالی که ارائه دهندگان محلی خدمات اینترنتی و شبکه های اجتماعی ممکن است مجبور به از میان بردن محتوا و افشای اطلاعات صاحب حساب بشوند، پلتفرم های میزبان خارج از کشور در دسترس حکومت ایران قرار ندارند.

هرچند که دولت ایران کوشیده تا شرکت های خارجی را مجبور به پذیرش درخواست های مربوط به اطلاعات کاربران بکند، اما در این کار موفق نبوده است. جایگزین های داخلی برای خدمات خارجی، که از سوی طرح اینترنت ملی حکومت پشتیبانی می شود، در جذب چشمگیر کاربران ناکام بوده است (حتی مسئولان ایرانی نیز تمایل به استفاده از ابزار ارتباطات و اپلیکیشن های شبکه اجتماعی ایجاد شده در ایالات متحده دارند). افزون بر این، میلیون ها نفر از ایرانیان در تبعید- که بسیاری از آنان کشور را به دلیل فشارهای حکومت ترک کرده اند- در کشورهایی زندگی می کنند که توافق همکاری های امنیتی با تهران ندارند و مجبور نیستند از طریق پلتفرم های ناامن ایرانی ارتباط برقرار کنند. در نتیجه، برخلاف دو دهه نخست پس از انقلاب ایران، ارتباطات ایرانیان و فعالیت های شخصی آنها بطور فزاینده ای خارج از دسترس حکومت قرار گرفته است. این پویایی ماهیت نظارت های حکومتی را از پایه و اساس تغییر داده است.

دولت ایران تلاش کرده است تا به چالش هایی که اینترنت در برابر انحصار حکومت بر اطلاعات و ارتباطات ایجاد کرده، واکنش نشان دهد. از میان نخستین واکنش ها می توان به فیلترینگ اجباری محتوا اشاره کرد که شامل مسدود کردن دسترسی به تمام سایت هایی است که پورنوگرافیک، ضد مذهب یا به لحاظ سیاسی برانداز محسوب می شوند. با این همه، با افزایش ابزارهای دور زدن، فیلترینگ تأثیر خود را از دست داد. متعاقباً عملیات سایبری تهاجمی اساسی، از قبیل مختل کردن سایت های مخالفان طی جنبش سبز، به رژیم این توان را داد تا بخشی از کنترل خود بر گردش اطلاعات را بازیابد و توهم سلطه جمهوری اسلامی بر اینترنت را به نمایش بگذارد.

عملیاتی سایبری ایران بسیار انعطاف پذیرند، زیرا ابزار و پلتفرم های اینترنتی که مورد استفاده عموم قرار می گیرند در حال تغییر هستند. به عنوان مثال، پس از اینکه ایرانیان به دلیل امکان چت عمومی بدون فیلتر و ادعای امن بودن تلگرام، به این پیام رسان رو آوردند، عاملان تهدیدکننده ایرانی نیز توجه خود را معطوف به آن کردند. همزمان با عملیات سرقت نام و پسورد حساب های کاربران تلگرام، به نظر می رسد که یکی از این عاملان تهدید کننده تا آنجا پیش رفته که نقشه ای از حساب های تلگرام که مرتبط با شماره های تلفن ایرانیان بوده ترسیم کرده است. این عملیات جمع آوری اطلاعات ارتباطی عمیق تر با هدف قرار دادن کاربران اپلیکیشن های چت داشت و همچنین هماهنگ با بازداشت های مکرر مدیران گروهای تلگرامی منتقد بود. این روند آموزشی در جاهای دیگر، از جمله تلفن های موبایل و کامپیوتر های اپل نیز تکرار شد.

عملیات های سایبری تهاجمی هماهنگ با دولت که توسط گروه های مختلف عاملان تهدیدکننده در دوره های زمانی مختلف صورت پذیرفته، عمدتاً بر اهداف مشابه تمرکز داشته اند:

۱-مقامات دولتی
۲-سیاستمداران اصلاح طلب
۳-شخصیت های رسانه ای
۴-اقلیت های دینی
۵-شخصیت های فرهنگی
۶-گروه های اپوزیسیون، سازمان های تروریستی، و جنبش های جدایی طلب قومی

مسئولان دولتی

تعداد زیادی از عاملان تهدید کننده ایرانی کوشیده اند تا اعضای دولت حسن روحانی، دولت رئیس جمهور سابق، محمود احمدی نژاد و نهادهای اداری حکومت را مورد حمله نفوذی قرار بدهند. این عملیات ها نه تنها مسئولان دولتی، بلکه بستگان آنها را نیز هدف گرفته اند، از جمله کمپین مستمری علیه خانواده گسترده و درجه اول روحانی (بویژه برادر و

مشاور وی، حسین فریدون) اجرا شده است. «مجیک کیتن»، نخستین عامل تهدیدکننده شناخته شده، از آغاز در عملیات نفوذی شبکه تلویزیونی حکومت، صدا و سیمای جمهوری اسلامی، و مرکز تحقیقات استراتژیک -اندیشکده ای که شعبه تحقیقاتی مجمع تشخیص مصلحت نظام است و در آن زمان روحانی رئیس آن بود- شرکت داشت.

کمپین هایی که هدفشان حکومت ایران است همچنان در جریانند. هدف قرار دادن اعضای دولت -افرادی که پیش از این از سوی رژیم مورد تحقیق و بررسی قرار گرفته اند- نشانگر اهمیت نظارت سایبری به عنوان ابزاری در دست یک حکومت امنیتی تندرو است که می تواند در جهت کنترل کردن رقبای احتمالی به منظور کسب قدرت و همچنین جمع آوری اطلاعات حساس در خصوص زندگی مردم، احتمالاً برای باج گیری یا تحقیر آنان، بکار رود.

وزارت امور خارجه ایران برجسته ترین و مشهودترین نمونه از جاسوسی درون دولتی را به دست می دهد. از آغاز دولت روحانی، دیپلمات های ایرانی اغلب آماج «فیشینگ هدفمند» از سوی عاملان تهدیدکننده وابسته به سپاه قرار گرفته اند. این فعالیت ها همسو با اتهامات نشریات تندرو مبنی بر اینکه در توافق هسته ای به منافع ایران خیانت شده است، صورت پذیرفته اند. تلاش های صورت گرفته برای هک کردن همچنین نمایانگر سابقه بازداشت ها و فشارهایی است که علیه اعضای کادر دیپلماتیک رخ داده است. از جمله می توان به بازداشت عبدالرسول دری اصفهانی- یکی از اعضای تیم مذاکره کننده هسته ای در زمان برجام- به جرم جاسوسی اشاره کرد. در حالی که دیپلماسی مستلزم تعامل با مقامات دولت ها و کارشناسان خارجی است، چنین تماس هایی را می توان سریعاً به عنوان جاسوسی برای قدرت های خارجی تصویر کرد.

در حالی که وزیر امور خارجه، محمد جواد ظریف و دیگر شخصیت ها هدف تهدید و تخریب در شبکه های اجتماعی قرار گرفته اند، قصد و نیت کمپین های عاملان تهدیدکننده بومی که در این گزارش ترسیم شده اند، با هک-کنشگری یا یک تخریب ساده تفاوت دارد. هدف در اینجا جمع آوری اطلاعات شخصی از حساب های کاربری شخصی در پلتفرم های بین المللی و همچنین نظارت بر شبکه های حرفه ای و سیاسی خصوصی مسئولان دولت است. این تاکتیک ها شامل تلاش های نوعی برای سرقت نام و پسورد حساب های ایمیل شخصی است که در جاهای دیگر نیز دیده می شود. با این همه، تلاش ویژه ای صورت گرفته تا مسئولان دولت و اعضای خانواده های آنها را از طریق فریب کاری های پیچیده و با استفاده از منابع محرمانه به مخاطره بیندازند. سپس، این حساب ها مخاطبان دیپلماتیک و همتایان آنان را نشانه گرفته است. طبق گزارش ها، از اوایل سال ۲۰۱۳ و همین اواخر در فوریه ۲۰۱۷، عوامل تهدیدکننده وابسته به سپاه پاسداران ظریف و دیگر دیپلمات های ارشد را هدف قرار داده و خود را به جای آنان جا زده اند.

اعضای اصلی تیم دیپلماتیک تنها هدف جاسوسی درون دولتی نیستند: حساب های ایمیل شخصی چند تن از مسئولان کابینه دولت روحانی نیز نفوذ شده است. عملیات سایبری عاملان تهدیدکننده ایرانی فراتر از اعضای اصلی دولت رفته و اعضای حکومت مذهبی شیعی که از ایدئولوژی حکومت و امور سیاسی حفاظت می کنند را هم هدف قرار داده است. کمپین ها

موجب به مخاطره افتادن چندین فرد در قم -مرکز امور مذهبی ایران- شامل میزبان هایی در مرکز خدمات حوزه های علمیه اسلامی و دفتر تبلیغات اسلامی شده است.

سیاستمداران اصلاح طلب

حساب های اصلاح طلبان ایرانی از اهداف عمده عاملان تهدیدکننده ایرانی به شمار می روند. اگرچه اصلاح طلبان وفاداری خود را به انقلاب و جمهوری اسلامی ابراز می کنند، اما طرفدار مداخله کمتر حکومت در جامعه، سیاست خارجی مسالمت آمیز و همچنین ارجحیت دادن منافع ملی بر ایدئولوژی انقلابی می باشند. در نتیجه، اصلاح طلبان بطور فزاینده ای از سیاست ایران پاکسازی شده اند، و برجسته ترین رهبر آنان، محمد خاتمی- رئیس جمهور سابق ایران از سال ۱۹۹۷ تا ۲۰۰۵- ممنوع التصویر و ممنوع الخروج شده است.

پس از جنبش سبز، افراد وابسته به کاندیداهای اصلاح طلب انتخابات ریاست جمهوری سال ۲۰۰۹، مهدی کروبی و میرحسین موسوی، به صورتی تهاجمی هدف رژیم قرار گرفتند که می کوشید تا فعالیت های آنها -حتی کسانی که تحت فشار اذیت و آزار گریخته بودند- سرکوب کنند. رژیم ایران که نمی خواست جنبش سبز تکرار شود، کنترل اطلاعات را در آستانه انتخابات سال ۲۰۱۳ که در آن حسن روحانی به ریاست جمهوری رسید شدیدتر کرد. دسترسی به ابزار متداول ضدسانسور قطع و سرعت اینترنت تا پس از اعلام نتایج انتخابات کاهش داده شد. در این دوره، چندین عامل ایرانی بطور هماهنگ حساب های مخالفان سیاسی ایرانی را هدف قرار دادند. خارج از فضای اینترنت، خانواده های کارکنان رسانه های فارسی زبان بین المللی مورد آزار قرار گرفتند و گزارشگران داخل ایران نیز در معرض سانسور یا بازداشت قرار گرفتند.

یکی از نخستین موارد معروف هک کردن با انگیزه سیاسی در ایران زمانی بود که بلاگ محمد علی ابطحی، معاون وزیر ارشاد و فرهنگ اسلامی در دوره خاتمی، پس از نوشتن مطلبی درباره بازداشت وبلاگ نویسان در سال ۲۰۰۵ تخریب شد. پس از آن، عاملان تهدیدکننده ایرانی متفاوتی که در سرقت نام و پسورد حساب های کاربری و عملیات مهندسی اجتماعی نقش داشته اند، بطور مکرر به ابطحی حمله کرده و هویت او را جعل کرده اند. تجربه ابطحی نشان می دهد که اصلاح طلبان یکی از اولویت های چنین گروهی است. شخصیت های دولتی در جنبش اصلاح طلبان از بخش های متفاوت جامعه و سیاست مورد هدف قرار گرفته اند. این موضوع نه تنها شامل کنشگران سرکوب شده مرتبط با خاتمی، کروبی، موسوی، بلکه مسئولان سابق دولت، پژوهشگران دینی، سیاستمداران و اساتید را نیز در بر می گیرد.

عملیات سایبری علیه اصلاح طلبان، گسترده، موفق و مکرر بوده است. یکی از عاملان تهدیدکننده توانست ماه ها به کامپیوتر یک روحانی اصلاح طلب و معاون یک دانشگاه معروف دسترسی پیدا کند و فعالیت های سیاسی و مصاحبه های او با رسانه ها را رصد کند. به همین ترتیب، در دسامبر ۲۰۱۵ حساب فیس بوک غلامرضا رجایی، کنشگر سیاسی

نزدیک به رئیس جمهور سابق ایران، اکبر هاشمی رفسنجانی، مورد استفاده قرار گرفته بود تا با «فیشینگ هدفمند» به حساب های شخصی روزنامه نگاران و دیگران حمله کند. یک سال قبل از آن، همان عامل تهدیدکننده («راکت کیتن») با موفقیت تعدادی از نمایندگان سابق مجلس و دیگر اصلاح طلبان در تبعید را مورد حملات نفوذی قرار داد که بعدها به دستگیری آنها انجامید.

کنشگران جوانی که طی مقدمات انتخابات فوریه ۲۰۱۶ مجلس، مسئول تدارکات برای اصلاح طلبان بودند، بویژه افراد مرتبط با کاندیداهای زن، هدف بدافزارها و عملیات سرقت نام و پسورد حساب های کاربری قرار گرفتند. این هدف گرفتن ها اغلب همسو با فشارهای آقلاین سپاه پاسداران و وزارت اطلاعات صورت می گیرد: زمانی که به دفتر کار یک اصلاح طلب نزدیک به روحانی در ماه مه ۲۰۱۷ حمله شد، او بطور مکرر هدف حملات «فیشینگ هدفمند» نیز قرار گرفت. به رغم ترقی تعداد بیشتری از اصلاح طلبان به جایگاه قدرت، آنان همچنان هدف اصلی حملات سایبری حکومت هستند.

شخصیت های رسانه ای

تمرکز عملیات های سایبری ایرانیان مرتباً بر خبرنگارانی است که با رسانه های اصلاح طلب و شبکه های ماهواره ای بین المللی کار می کنند که خارج از کنترل سختگیرانه حکومت هستند. چندین عامل تهدیدکننده ایرانی از طریق اطلاع رسانی های جعلی، عملیات متعدد سرقت نام و پسورد حساب های کاربری علیه خبرنگاران خارجی مستقر در ایران و همچنین روزنامه نگاران ایرانی شاغل در نشریات برجسته ای چون روزنامه شرق و ایلنا اجرا کردند. به همین ترتیب، گزارشگران آزاد داخل ایران نیز مرتب از طریق شخصیت های ساختگی که برای آنان بدافزارهایی با ظاهر خبر می فرستند، مورد نفوذ قرار می گیرند. هدف این کمپین ها اغلب نشریاتی است که بعدها تعطیل می شوند و یا روزنامه نگارانی که بوسیله نیروهای امنیتی ایران بازداشت می شوند. چنین حوادثی بیشتر اوقات همزمان با انتخابات رخ می دهد، یعنی زمانی که حکومت با شدت بیشتر خبرنگاران را تحت پیگرد قانونی قرار می دهد.

آنچه که بر سر جیسون رضائیان -خبرنگار سابق روزنامه واشنگتن پست در ایران- آمد، نشانگر تمرکز عاملان تهدیدکننده همسو با دولت بر مطبوعات خارجی فعال در ایران است. رضائیان پیش از بازداشت در ۲۲ ژوئیه ۲۰۱۴ و تحمل ۱۸ ماه زندان از سوی سپاه پاسداران، هدف تلاش های نفوذی و هماهنگ یک عامل تهدیدکننده به نام Flying Kitten قرار گرفته بود. این عامل تهدیدکننده کوشیده بود با حساب های ساختگی امنیتی، از طریق سرقت نام و پسورد چندین بار به حساب های هات میل و جی میل رضائیان نفوذ کند. این ایمیل ها در مورد اسپمی که از آن حساب فرستاده شده بود و دیگر خطرات هک شدن هشدار می داد. این ایمیل ها به لحاظ تکنیکی پیچیده نبودند، چرا که انگلیسی ضعیفی در آنها استفاده شده و رویکردشان نیز ناشیانه بود. با این همه، نحوه عملیات- اینکه از میان مجموعه کوچکی از اهداف، حساب های رضائیان چند ماه پیش از بازداشت او انتخاب شده بود- منحصر بفرد بود.

اقلیت های دینی

اقلیت های دینی ایران اهداف مشخص نیروهای امنیتی ایران هستند، بویژه پیروان دین بهایی که به شدت مورد اذیت و آزار قرار گرفته و مدت های مدید متهم به اشاعه توطئه علیه حکومت اسلامی بوده اند. مراکز رهبری بهائیان که عمدتاً در ایالات متحده و حیفا در اسرائیل قرار دارند، با استفاده گسترده از اینترنت از فرصت های سازمانی و ارتباطی جدیدی برخوردار شدند که بدون اینترنت از آن محروم بودند. با این همه، همان فن آوری ها توانایی های جدیدی برای حکومت ایران فراهم آورد تا به جمع آوری اطلاعات و انتشار تبلیغات علیه بهائیان بپردازد.

در آوریل ۲۰۱۴، از داخل ایران به حساب جی میل یکی از مدیران سابق امور خارجی سازمان بهائیان ایالات متحده، دسترسی پیدا کردند. این مدیر سابقه دفاع در سطح بین المللی از طرف مجمع بهائیان، از جمله شهادت در برابر کنگره ایالات متحده پیرامون موقعیت اقلیت های دینی در ایران، را داشت. همین موضوع او را به یکی از اهداف طبیعی ایران تبدیل کرد. پروفایل های جعلی لینکدین و شبکه های اجتماعی که پیش از این علیه صنایع دفاعی ایالات متحده بکار گرفته شده بود- از جمله پروفایلی که ادعا می کرد جان بولتون، سفیر سابق ایالات متحده در سازمان ملل است- برای هدف قرار دادن این مدیر بهایی مورد استفاده قرار گرفت. این امر از طریق تلاش برای سرقت نام و پسورد، تحت لوای گزارشی در خصوص آزار و شکنجه مذهبی صورت پذیرفت.

اعضای برجسته این مذهب، از جمله بستگان مهاجر رهبران بهایی که در ایران زندانی هستند، همچنان بطور مستمر در معرض عملیات سایبری قرار دارند. بتازگی در فوریه ۲۰۱۷، گروه های واسطه همزمان با مناسبت هایی چون سالگرد انقلاب اسلامی، وبسایت های بهائیان را با تبلیغات به نفع رژیم تخریب کردند. هدف قرار دادن مستمر بهائیان و تخریب وبسایت های آنان تأکیدی است بر نگرانی رژیم ایران در مورد سازمان هایی که برانداز تلقی می کند. این امر همچنین نشان می دهد که رژیم از حملات مخرب برای مستحکم کردن برنامه های ایدئولوژیک خود استفاده می کند.

اهداف مذهبی عملیات سایبری ایران تنها به گروه هایی مثل بهائیان که به نحوی خصمانه نادیده گرفته شده اند، محدود نمی شود، بلکه جوامع مذاهب رسمی، مثل مسیحیان، یهودیان، زرتشتیان، و مسلمانان سنی را نیز در برمی گیرد. به عنوان مثال، رهبر یکی از جوامع اصلی یهودیان در تهران، هنگام سازماندهی رویدادها و مدیریت یک نشریه مذهبی محلی، از طریق بدافزار در معرض خطر و زیر نظر گرفته شده بود. دیگر کمپین های فیشینگ هدفمند، بطور مرتب نوگرویدگان به مسیحیت تبشیری، خداناباوران، و فرقه های مذهبی عصر جدید را هدف قرار داده اند. در سطحی گسترده تر، کمپین بدافزاری در هیئت اطلاعات در خصوص آزار و شکنجه نوگرویدگان مسیحی، به سازمان های حقوق بشری فرستاده شد، و همچنین پروفایل های جعلی در هیئت اقلیت های دینی درآمده اند تا به شبکه های فارسی زبان مسیحیت تبشیری نفوذ کنند.

چهره های فرهنگی

کمپین های فیشینگ هدفمند شکل گرفته در ایران، چهره های فرهنگی این کشور- ازجمله هنرمندان، موزیسین ها، کمدین ها، کاریکاتوریست ها و طنزپردازان- را چه در داخل و چه خارج از کشور هدف قرار داده اند. این کمپین ها عبارتند از هدف قرار دادن و نفوذ به حساب های ایمیل و شبکه های اجتماعی شاهین نجفی، موزیسین ساکن آلمان، چندین ستاره موسیقی پاپ که ایران را پس از انقلاب اسلامی ترک کردند، یک خواننده ایرانی-اسرائیلی، و یک زن موزیسین سبک metal که متولد ایران و ساکن ایالات متحده و افراد دیگر است. علاوه بر این، در دستگاه ها و حساب های هنرمندان زیرزمینی ساکن ایران که از شهرت کمتری برخوردارند و همچنین پروفایل های جعلی شبکه های اجتماعی مرتبط با گروه های موسیقی death metal rock و hip hop نیز نفوذ هایی صورت گرفته است. هدف قرار دادن موزیسین های مشهور سبک پاپ و همکاران آنان در ایران و خارج از کشور مرتب تکرار می شود و این صرفاً متمرکز بر منتقدان حکومت نیست.

نیروهای امنیتی ایران علناً به عملیات شناسایی افرادی که آنلاین «رفتارهای غیراخلاقی» دارند، اذعان کرده اند. در ژانویه ۲۰۱۶، چند مانکن معروف در شبکه های اجتماعی، به دلیل فعالیت های آنلاین خود بازداشت و مجبور شدند تا حساب های خود را حذف کنند- عملیاتی که سپاه پاسداران آن را «عملیات عنکبوت» نامید. همزمان، دستگیری کارمندان شبکه تلویزیونی AAA Music که خارج از کشور قرار دارد، منجر به آن شد که حساب های شبکه های اجتماعی آنها با پیامی در خصوص غیرقانونی بودن این شبکه- که ظاهرا از سوی وزارت اطلاعات بود- تخریب شود. در مصاحبه ها و بیانیه های عمومی کسانی که طی «عملیات عنکبوت» بطور جمعی دستگیر شدند، این افراد معمولاً آشکارا عمل می کردند و تخریب ها زمانی صورت پذیرفت که آنها پسوردهای خود را داده بودند.

«عملیات عنکبوت» نخستین عملیات از این دست نبود: فعالیت های Flying Kitten حاکی از آن است که آنها پیشتر نیز در پی نظارت بر صنعت مد ایران بوده اند. اوایل سال ۲۰۱۴، این عامل تهدیدکننده موجب نفوذ به کامپیوتر یکی از مانکن های شبکه های اجتماعی شد که به علت آنکه با نپوشیدن حجاب اجباری یک سبک زندگی مد روز را تصویر می کرد، معروف بود. پس از آن حمله نفوذی، او از اینترنت کناره گرفت، از ورود به وبسایت های مدلینگ خودداری کرد و حساب فیس بوک خود را حذف کرد. تصویر او نیز به منظور اجرای عملیات بعدی علیه دیگر گروه ها استفاده شد. ماهیت غیرشفاف کمپین هایی چون «عملیات عنکبوت» به ابهام در مورد چگونگی ردیابی افرادی چون مانکن های اینترنتی توسط مقامات ایرانی می افزاید. با این همه، حوادثی مانند نفوذ از طریق Flying Kitten، نفوذ به شبکه های حامی دگرباشان جنسی (همجنس گرایان زن، همجنس گرایان مرد، دوجنس گرایان، تراجنسیتی ها) و انجمن های شبکه های اجتماعی کارگران جنسی از سوی دیگران، حاکی از ارتباط میان این تلاش هاست.

گروه های اپوزیسیون، سازمان های تروریستی و جنبش های جدایی طلب بومی

به رغم اینکه ایران مخالفت مدنی را تهدید علیه امنیت ملی تلقی می کند، این کشور با تهدیدهای واقعی تروریستی و جنایات سازمان یافته از سوی عوامل غیردولتی مواجه است. به عنوان نمونه، می توان به حملات حکومت خودخوانده داعش علیه مجلس ایران و مقبره رهبر سابق ایران، آیت الله روح الله خمینی، در ژوئن ۲۰۱۷ اشاره کرد. اگرچه در مستندات پژوهشگران بین المللی پیرامون عملیات سایبری ایران معمولاً فرض بر این است که تمام اهداف داخلی کمپین های نفوذی، مخالفان سیاسی هستند، بخش کوچکی از این کمپین ها بر حوزه هایی متمرکز است که هک کردن توسط مجریان قانون- بویژه هنگام جمع آوری شواهد و اطلاعات در خصوص فعالیت های تروریستی خشونت آمیز و جرائم مالی- در سطح بین المللی عادی شده است.

به عنوان نمونه، عاملان تهدیدکننده ایرانی فعالانه کوشیده اند تا عملیات دیجیتالی جنبش های جهادی سنی را از طریق سرقت نام و پسورد، بدافزار و دیگر عملیات مورد نفوذ قرار بدهند. عاملان ایرانی برای نفوذ به سازمان های اسلام گرا از اسناد و پیام هایی به زبان های فارسی و عربی به عنوان طعمه حداکثر استفاده را کرده اند، و خود را به جای سازمان های رسانه ای از قبیل الجزیره و العربیه جا زده اند. عامل Flying Kitten کوشید تا با قرار دادن نظراتی روی صفحه فیس بوک العربیه که در ظاهر جهادگرایی را تبلیغ می کرد، بدافزاری را منتشر کند. اینگونه تلاش های اطلاعاتی، گروه های جهادی در خاورمیانه و شمال آفریقا، پاکستان و افغانستان- از جمله داعش و القاعده- را هدف قرار داده و در عین حال بر گروهای عراقی و فارسی زبان هم تمرکز داشته اند.

عملیات سایبری امنیتی به نحوی گسترش یافته که آن دسته از سازمان های سیاسی که قبلاً درگیر جنگ علیه جمهوری اسلامی بودند را به حاشیه برانند. عاملان تهدیدکننده ایرانی موفق شده اند موجب به مخاطره افتادن افراد مرتبط با گروه های پوششی برای سازمان اپوزیسیون مجاهدین خلق، از جمله انجمن ایرانی-آمریکایی های تگزاس و شبکه تلویزیونی سیمای آزادی بشوند. این عملیات نفوذی امکان دسترسی به گروه های بحث و تبادل نظر خصوصی در فیس بوک و همچنین برنامه ریزی های درون سازمانی برای تظاهرات مجاهدین خلق، کانال های تلگرام و تلویزیون مجاهدین را میسر ساخت. با توجه به افشاگری های مجاهدین خلق در خصوص برنامه هسته ای ایران- که این سازمان ادعا می کند از طریق شبکه همدستان آنها در داخل کشور انجام شده بود- این فعالیت ها نیز یک برنامه ضد جاسوسی به شمار می آیند.

عاملان تهدیدکننده ایرانی همچنین تمرکز عمده ای بر اقلیت های بومی محروم از حقوق خود دارند که خواهان استقلال بیشتر می باشند. یکی از اهداف مکرر آنان، گروه های بلوچی- جمعیت مسلمان سنی مستقر در ایران و پاکستان- بوده اند. رسانه های خبری و حساب های شبکه های اجتماعی متعلق به سازمان های ستیزه جو مثل جندالله، بطور مکرر از سوی تهران هدف قرار گرفته اند. به عنوان نمونه می توان به رخنه به چندین وبسایت وابسته به جندالله از اوایل ژوئیه ۲۰۱۰ اشاره کرد که هدفش انتقال بدافزارها به کاربران بود. این حمله Watering hole به گونه ای طراحی شده بود که جدایی طلبان خشونت طلب مورد نظر سازمان های امنیتی ایران را تحت نظارت قرار دهد. در موارد دیگر، جندالله با بدافزاری

مورد هدف قرار گرفت که روی دامنه ای که ظاهراً مرتبط با ارتش آزاد سوریه بود قرار داشت. این بدافزار از طریق ایمیل هایی فرستاده می شد که ادعا می کرد حاوی اسنادی در خصوص حملات به سپاه پاسداران است.

ایران همچنین منابع چشمگیری به عملیات سایبری علیه سازمان های کرد در داخل و خارج از کشور اختصاص داده است. از آوریل ۲۰۱۵، نمونه هایی از بدافزارها حزب حیات آزاد کردستان (پژاک) که شاخه ایرانی حزب مارکسیستی-لنینیستی کارگران کردستان (پ.ک.ک) است را هدف قرار داده اند. به نظر می رسد همان عامل تهدیدکننده بطور موفقیت آمیزی موجب نفوذ به شبکه تلویزیونی ماهواره ای «نوروز تی وی» شد که وابسته به پ.ک. ک است. «نوروز تی وی» همچنین با بدافزار Flying Kitten در سال ۲۰۱۴ مورد حمله قرار گرفت که نشان می دهد نه تنها در دستورات عاملان تهدیدکننده، بلکه در اهداف دقیق شان نیز تداخل به وجود آمده است. علاوه بر این، دیگر گروه ها نیز از پروفایل های جعلی لینکدین استفاده کرده اند تا با نمایندگان دولت اقلیم کردستان در عراق ارتباط برقرار کنند. طبق اسامی کامپیوترها و دیگر شاخصه ها، می توان اینگونه برآورد کرد که بسیاری از کسانی که با بدافزار ایرانی لو مورد نفوذ قرار گرفتند در استان کردستان ایران قرار داشتند، در حالی که دیگران در کردستان عراق یا از جمعیت کرد ساکن اروپا بودند.

جامعه مدنی

اینترنت ارتباط و سازمان دهی بین ایرانیان و سازمان های خارجی مهاجران را تسهیل کرده، اما موجب افزایش فرصت های دولت ایران برای نظارت و سرکوب علیه عملیات های خارج از کشور نیز شده است.

اگرچه بسیاری از سازمان های جامعه مدنی در معرض تلاش های مستمر ایران در جهت نفوذ و اختلال قرار گرفته اند، اما تعداد اندکی از آنان به اندازه بنیاد اوراسیا متحمل حملات مداوم و تهاجمی شدند. این سازمان غیردولتی در واشنگتن دی سی مستقر است و برنامه هایی در زمینه توسعه در کشورهای شوروی سابق، خاورمیانه و چین اجرا می کند. بنیاد اورسیا در اکتبر ۲۰۰۹ به عنوان بخشی از برنامه های توسعه اجتماعی متمرکز بر ایران، «مدرسه کارآفرینی خورشید» را به راه انداخت که از طریق دروس آموزشی از راه دور و همچنین ایجاد فرصت های حرفه ای، از کارآفرینی زنان پشتیبانی می کرد.

برنامه ها و سابقه سازمانی بنیاد اوراسیا پیوندی نزدیک با هراس خامنه ای از انقلاب مخملی دارد. این بنیاد بعدها چند برنامه آنلاین دیگر به زبان فارسی به راه انداخت که موضوعات مختلفی -از کارآفرینی اجتماعی گرفته تا قوانین خانواده- را پوشش می داد. نخستین تلاش برای نفوذ اندکی پس از انتشار مقاله ای در روزنامه تندرو کیهان در فوریه ۲۰۱۴ صورت گرفت. این مقاله بنیاد اوراسیا را متهم می کرد که از طریق ایجاد شبکه های زنان و معلمان، مشغول مهندسی اجتماعی است تا رژیم را تحت فشارهای اقتصادی، سیاسی و اجتماعی از سوی توده های مردم قرار دهد. براساس این مقاله، بنیاد اوراسیا تمام این فعالیت ها را به دستور آژانس توسعه بین المللی ایالات متحده و وزارت امور خارجه ایالات

متحده انجام می داد. ده روز پس از انتشار این مقاله، Flying Kitten کمپین فیشینگ هدفمند علیه این بنیاد را آغاز کرد. سپس به مدت دو سال، بنیاد اوراسیا مرتباً هدف بدافزارها، سرقت نام و پسورد حساب های کاربری و مهندسی اجتماعی از سوی عاملان تهدیدکننده متفاوت با استراتژی های گوناگون قرار گرفت.

کمپین علیه بنیاد اوراسیا، نشانگر سابقه طولانی و همچنان در جریان عملیات سایبری ایران علیه سازمان های غیردولتی مستقر در ایالات متحده است. اندیشکده های آمریکایی نیز مرکز توجه چنین عملیاتی بوده اند، از جمله «مؤسسه امریکن انترپرایز» (American Enterprise Institute) و شورای روابط خارجی آمریکا (Council on Foreign Relations) که از سوی چندین عامل تهدیدکننده به عنوان هدف حملات انتخاب شدند. همان ایرانیانی که بنیاد اوراسیا را در دسامبر ۲۰۱۵ هدف قرار دادند، با جعل هویت مدیران شبکه های چندین مؤسسه سیاست خارجی در واشنگتن دی سی که از منتقدان حکومت ایران به شمار می رفتند، موجب لو رفتن کارمندان آن مؤسسات شدند.

این تلاش ها صرفاً متوجه منتقدان ایران نمی شود. سازمان های حامی بهبود روابط با ایران و پژوهشگران غیرسیاسی نیز بطور مرتب هدف قرار گرفته اند. به نظر می رسد وجه مشترک آنها صرفاً توجه به سیاست گذاری های مربوط به امور ایران بوده است.

نتیجه گیری و پیشنهادها

در حالی که اجرای عملیات سایبری تهاجمی ایران مستلزم منابع چندانی نبوده است، اما این امکان را برای تهران به وجود آورده تا خود را به عنوان یک قدرت سایبری در حال ظهور نشان دهد که قادر است صدمات قابل توجهی به رقبای خود بزند. حکومت امنیتی این کشور از این منابع سود برده تا توانایی خود در مواجهه با براندازی سیاسی و تلافی حملات علیه زیرساخت های خود را به رخ مخاطبان داخلی و بین المللی بکشد. با وجود آنکه این فعالیت ها ایران را- شاید حتی بیش از توانایی های واقعی اش- به عنوان یک نیروی قابل ملاحظه در مرکز توجه جهانی قرار داده، اما در عین حال آنچنان مبهم بوده اند که این کشور بتواند خود را قربانی اقدامات سرکوب گرانه کشورهای خارجی بنمایاند.

بر اساس شواهد موجود در خصوص هماهنگی بین فعالیت های سازمان های امنیتی و عملیات سایبری مشهود، می توان نتیجه گرفت که عاملان تهدیدکننده ایرانی تقریباً بطور قطع رابطه مستقیمی با نهادهای دولتی، بویژه سپاه پاسداران انقلاب اسلامی و وزارت اطلاعات دارند. با توجه به این همسویی و همدستی، عاملان تهدیدکننده ایرانی در اینجا مورد حمایت دولت توصیف شده اند. با این همه، از آنجا که عاملان تهدیدکننده معمولاً پیمانکاران خصوصی در شرکت های کوچک امنیتی هستند، این روابط گاه نامشخص هستند و عاملان درون نیروهای حکومتی ادغام نشده اند.

عملیات های سایبری ایران اغلب بازتاب رفتار مرسومی است که مجریان قانون در دیگر کشورها در واکنش به پیشرفت فن آوری های اطلاعاتی- از قبیل هک کردن دستگاه ها به منظور شنود ارتباطات اینترنتی کدگذاری شده- انجام می دهند. انجمن های استانداردهای بین المللی و فروشندگان تجهیزات مخابراتی، احتمال وقوع استراق سمع قانونی ارتباطات را موجه کرده اند. دولت ایران نیز با همان چالش های دیگر کشورها در زمینه تأمین امنیت داخلی علیه سازمان های تروریستی و جنایات مواجه است. این منافع اغلب خود را در قالب کمپین هایی نشان می دهد که شامل جمع آوری اسناد در زمینه هدف قرار دادن مستمر سازمان های ستیزه جو- هم داخلی و هم منطقه ای- است که دشمن حکومت ایران به شمار می روند. در این میان می توان به جدایی طلبان بلوچی و داعش اشاره کرد.

به استثنای عربستان سعودی، ایران ظاهراً موفقیت چندانی در نفوذ به نهادهای مقاوم دولتی یا سازمان هایی که تحت محافظت خوبی قرار دارند، نداشته است. پس از دو دهه جرائم سایبری، دولت ها و شرکت های خصوصی هم سیاست های امنیتی اتخاذ کرده و هم روابط مبتنی بر همکاری با سازمان های امنیتی بیرونی (مثل تیم های آمادگی اضطراری کامپیوتری یا CERT) برقرار کرده اند تا بتوانند از خود در برابر این حملات دفاع کنند. شرکت ها در محیط اداری منابع فنی اختصاصی فراهم می کنند، دستگاه ها را تحت کنترل مرکزی قرار می دهند، کاربران را آموزش می دهند و از تجهیزات محافظتی برای شبکه ها استفاده می کنند که میزان خطرات را کاهش می دهد. چنین منابعی، بخش خصوصی و دولت ها را قادر می سازد تا در برابر تهدیدات واکنش از خود نشان دهند و بطور جمعی بر آگاهی خود بیفزایند.

شرکت های خصوصی تهدیدات امنیتی و نهادهای دولتی، از جمله دیده بان سایبری (CyWatch) سازمان اف بی آی، مرتباً گزارش هایی پیرامون خطرات معمول امنیتی در اختیار شرکت ها قرار می دهند که شامل اطلاعات درباره ابزارهای ثبت شده و زیرساخت حمله کننده هاست. سازمان اف بی آی اطلاعیه هایی در خصوص فعالیت های نفوذی ایران برای صنایع تهیه کرده که براساس گزارش های بخش خصوص فراهم آمده اند. نهادهای دولتی ایالات متحده نیز بدافزارهای ایرانی را از طریق اطلاعات برگرفته از شرکت های تهدیدات امنیتی شناسایی کرده اند. هنگامی که چندین کامپیوتر در بخش فارسی صدای آمریکا تحت تاثیر یک بدافزار ایرانی به نام Infy قرار گرفتند، مدیران شبکه منشاء آن را از طریق یک گزارش محرمانه که یک شرکت تهدیدات امنیتی تهیه کرده و در اختیار این سازمان قرار داده بود، شناسایی کردند.

دسترسی به چنین منابعی ساده نیست، بویژه برای ساکنان ایران که هنگام هدف قرار گرفتن از سوی حتی ساده ترین عامل تهدیدکننده، خود را تنها و بدون آمادگی قبلی می یابند. در حالی که بانک های آمریکایی به سرعت در زمینه اقدامات متقابلی که تأثیر حملات DDoS در «عملیات ابابیل» را محدود می کرد، سرمایه گذاری کردند؛ پلتفرم های رسانه های اجتماعی فارسی زبان و سازمان های رسانه ای که در معرض همان حملات قرار داشتند، عموماً استفاده از آن خدمات را متوقف کردند و حاضر به پرداخت هزاران دلار هزینه پهنای باند نشدند. در یک اطلاعیه سازمان اف بی آی که به بخش خصوصی فرستاده شد، پروفایل های جعلی ثبت شده بود که در زمان هدف قرار دادن جامعه بهایی نیز مورد استفاده قرار گرفته بودند. با این همه، سازمان اف بی آی و شرکت های امنیتی سایبری معمولاً به جوامعی که در معرض خطر قرار دارند، درباره ایمنی و حریم خصوصی آنها اطلاع نمی دهند. این اختلاف و محرومیت نشانگر تفاوتهایی است که در ارائه فرصت ها به اهداف غیردولتی و غیرشرکتی عاملان تهدیدکننده هماهنگ با حکومت وجود دارد.

توجه فزاینده شرکت های فن آوری اطلاعات به امنیت کاربران در سال های اخیر، مستقیماً به نفع هدف های ایران تمام شده است. سواد دیجیتالی به زبان فارسی و همچنین برنامه های آموزشی امنیت اطلاعات، از طریق کمک های خارجی تسهیلاتی را برای مخاطبان در معرض خطر فراهم کرده اند و مفاهیمی از قبیل مدیریت رمز عبور و چگونگی شناسایی مدیریت اجتماعی را به آنان آموخته اند. برخی از ویژگی های حساب های کاربری که بطور گسترده در دسترس است، از قبیل تأیید دو مرحله ای که از کاربر می خواهد کدی را که از طریق پیامک یا یک اپلیکیشن ارسال شده، هنگام ورود به حساب خود ارائه دهد، به وضوح سرقت نام و پسورد حساب های کاربری را برای ایرانیان بسیار دشوارتر کرده است. شرکت های خصوصی مانند گوگل و کلاودفلر (Cloudflare) و همچنین سرمایه گذاران دولتی از خدمات کاهش حملات DDoS پشتیبانی کرده اند- این خدمات منابعی دفاعی در سطح شرکت ها در اختیار سازمان های جامعه مدنی می گذارند تا بدون هیچ هزینه ای در برابر اینگونه حملات از خود دفاع کنند. همین امر منجر به کاهش چشمگیر تعداد آنها شده است.

در نتیجه، یک کاربر آموزش دیده با تأیید دو مرحله ای و یک دستگاه iOS، هدف دشوارتری برای نفوذ به از سوی عاملان تهدیدکننده ایرانی است. با این همه، با وجود آنکه گزینه های تکنولوژیکی برای محافظت از حساب ها و دستگاه ها در سال های اخیر پیشرفت کرده؛ در نهایت، کاربر همچنان آسیب پذیرترین بخش این قضیه است.

پنهان کاری های حکومت ایران درباره فعالیت هایش و همچنین جغرافیای سیاسی نامعلوم این کشور، پیش بینی آینده عملیات سایبری اش را محدود می کند. همچون بسیاری از کشورها، ایران نیز ظاهراً خط مشی مشخصی ندارد که چه وقت دست به عملیات مختل کننده بزند و در فضای سایبری به اقدامات تلافی جویانه بپردازد. احتمالاً این خط مشی را اتخاذ هم نخواهد کرد. تهران در همسویی با استراتژی های نامتقارن جنگ های سنتی، از این ابهام اغلب سود برده است. شاید به همین دلیل است که عملیات نسبت داده به خود را انکار می کند و عاملان تهدیدکننده را نیز مستقیماً در دستگاه نظامی خود نگنجانده است.

از آنجا که ایران خود هدف جاسوسی سایبری مستمر و حملات تخریبی بوده، ملزم به کسب همان توانایی هایی است که علیه این کشور بکار گرفته شده است. این توانایی ها فرصت هایی را برای تهران فراهم می آورد تا طی عملیات جنگی احتمالی هزینه هایی تحمیل کند. به نظر نمی رسد ایران بتواند حملات چند مرحله ای همزمان را هر جا که می خواهد اجرا کند، اما این کشور می تواند در کمپین های تلافی جویانه اهداف ساده را بطور مکرر بکوبد. با شروع مجدد خصومت بین ایران و آمریکا، می توان انتظار داشت که سیستم های خدمات دولتی، غیرنظامی و اقتصادی آسیب پذیر از طریق تخریب داده ها، DDoS و دیگر حملات مختل کننده مورد هدف قرار بگیرند. با تصوراتی که اکنون درباره توانایی های تهاجمی سایبری ایران وجود دارد، مشخص نیست که این کشور آمادگی و توان اجرای حملات علیه شبکه برق یا سیستم های کنترل صنعتی- مانند حملاتی که علیه اوکراین صورت گرفت- را داشته باشد. در عوض، حملات متوجه اهدافی خواهد شد که از مقاومت کمتری برخوردارند، مثل دولت های محلی و ایالتی به جای زیرساخت های دولت فدرال، یا بخش های غیرآماده ای که پیش از این هدف قرار نگرفته اند، از جمله حمل و نقل و پشتیبانی به جای خدمات مالی. تلاش های یک ایرانی در جهت دخالت در یک سد محلی در نیویورک و دیگر گزارشات درباره نفوذ به ادارات دولتی، نشانگر فرصت های فراوانی است که ایران برای اقدامات تلافی جویانه علیه ایالات متحده دارد.

افزون بر این، به رغم آنکه ایران را یک بازیگر منطقی توصیف می کنند، اما این بازیگر فاقد یکپارچگی است: تداخل عملیاتی و همچنین نظارت های درون دولتی از سوی وزارت اطلاعات و سپاه پاسداران گواهی بر این مدعاست. انگیزه ها، هماهنگی و تصویب کمپین های هماهنگ با حکومت ایران شاید به لحاظ مواضع سیاست گذاری با دیگر قوای حکومت متفاوت باشد و استفاده از توانایی های تهاجمی سایبری نیز کمتر از تجهیز کردن سربازان برای ناظران مشهود باشد. دستگاه امنیتی ایران می تواند به آسانی در فضای مجازی به اجرای عملیات خصمانه بپردازد بی آنکه نیازی به توافق یا آگاهی سایر ارکان حکومت داشته باشد.

فعالیت های اخلال گرانه عاملان تهدیدکننده ایرانی، از زمان توافق موقت هسته ای، معروف به برجام، که در نوامبر ۲۰۱۳ امضاء شد، کاهش یافته است. زبان مسئولان نظامی و دولتی نیز طی زمان متحول شده است. در سال های اخیر، بویژه در دوره دولت روحانی، کمتر از گذشته بیانیه های پر سر و صدا و تهاجمی پیرامون عملیات سایبری ایران صادر شده است. در حالی که احتمال دخالت تهران در عملیات مختل کننده زیرساخت های آمریکایی و اروپایی کمتر است، اما این کشور به جاسوسی سایبری پرداخته و این کار را همچنان ادامه خواهد داد. از آنجا که ایران کمپین های پیشین خود را موفق تلقی می کند، عملیات تهاجمی سایبری را بیش از پیش وسیله ای مؤثر برای ادامه عملیات جاسوسی و نظارت بر دشمنان منطقه ای و مخالفان سیاسی خود می داند.

اما ایران تا مدت ها دچار محدودیت منابع خواهد بود. به نظر می رسد تهران به ندرت قادر بوده عملیات استخراج داده های تجاری یا دولتی را در مقیاس گسترده ای به اجرا بگذارد. این قضیه به عنوان مثال با تلاش چینی ها در جهت ربودن اسرار صنعتی شرکت بوئینگ یا پایگاه های داده ها از اداره مدیریت پرسنل ایالات متحده کاملاً تفاوت دارد. علاوه بر این، میزان دشواری نفوذ به چنین اهدافی طی زمان افزایش می یابد و مشخص نیست که توانایی های ایران نیز به همان نسبت بهبود بیابد.

فرار گسترده مغزها از ایران که طی آن بسیاری از تیزهوش ترین مهندسان کشور به دلایل سیاسی و اقتصادی آنجا را ترک می کنند، محدودیت های بیشتری بر ایجاد توانایی های سایبری این کشور اعمال می کند. طبق برآورد وزیر علوم، تحقیقات و فن آوری، ۱۵۰ هزار نفر از افراد بسیار مستعد هر سال از ایران مهاجرت می کنند که سالانه موجب زیان اقتصادی ۱۵۰ میلیارد دلاری می شود. هنگامی که مهندسان ایرانی کشور را به سوی Silicon Valley و اروپا ترک می کنند، قابلیت های ایران برای عملیات تهاجمی و دفاعی سایبری نیز همراه آنان از دست می رود.

به دلیل فقدان تشابه در سوابق عملیات سایبری ایران، اتفاقات جدید یا ظهور گروه های جدید اغلب به اشتباه به عنوان بهبود چشمگیر ظرفیتی تلقی می شود. به رغم چالش های سیستماتیک ناشی از اختلالات اداری و سرمایه گذاری ناکافی در عرصه امنیت سایبری، ایران دارای پتانسیل لازم برای اجرای عملیات مؤثرتری است. تلاش های حکومت، دانشگاه ها و بخش خصوصی در جهت ایجاد یک جامعه امنیتی سایبری حرفه ای، مثل میزبانی تورنمنت Capture the Flag، ناگزیر منجر به گردآوری بیشتر استعدادها خواهد شد. مشاهده سایر بازیگران دولت-ملت، مجموعه ای از معیارها را فراهم می آورد که می تواند شاخصی معتبر برای بهبود یا تغییر موقعیت به شمار رود. این معیارها عبارتند از:

- هماهنگی عاملان تهدیدکننده، بهبود یکپارچه تر بدافزارهای تولید داخلی و توسعه ابزارهای ساخته شده با منظور خاص که می تواند نشانگر استحکام ظرفیت، تخصصی شدن پرسنل، و حتی ادغام در حکومت باشد؛
- سرمایه گذاری در امنیت عملیاتی- شامل کاهش میزان اطلاعات در دسترس گردانندگان و همچنین افزایش سرمایه گذاری در پنهان کاری (مثل شبکه کمکی Magic Kitten)

- بهبود تحقیقات درباره پیشینه و توانایی های زبان خارجی در خلال عملیات، از قبیل خصوصی سازی بیشتر تلاش های مهندسی اجتماعی که نشانگر گنجاندن کارکنان پشتیبانی غیر فنی باشد؛ و
- اجرای عملیات، شامل حملات اکسپلویت های روز صفر یا هدف گرفتن زیرساخت های اصلی (به عنوان مثال، نفوذ به دستگاه های شبکه، ربودن پروتکل مسیریابی، و دستکاری در علامت دهی های مخابراتی). این گونه عملیات حاکی از سرمایه گذاری بیشتر در منابع لازم برای عملیات سایبری سیستماتیک است.

به رغم اینکه ایران در حال حاضر ابزار فنی پیچیده در اختیار ندارد، ابزار ساده نیز می تواند در تحمیل هزینه های سیاسی و اقتصادی مؤثر باشد. دلیل این مدعا، نفوذ موفقیت آمیز روسیه و متعاقب آن، درز کردن ارتباطات داخلی نهادها و گردانندگان حزب دموکرات پیش از انتخابات سال ۲۰۱۶ در ایالات متحده است. برخی از زیانبارترین مطالب استفاده شده در این عملیات از طریق نفوذی ساده به یک حساب جی میل وارد شد- فرصتی که در دسترس همگان است. این امر همچنین چالش تشخیص قصد و نیت را نیز تشدید می کند، و آنچه ابتدا جاسوسی به نظر می رسد می تواند بعدها به یک حمله تبدیل شود.

با توجه به اکوسیستم پراکنده عاملان تهدیدکننده ایران، بازداشتن تهران از شرکت در عملیات های تهاجمی سایبری به همان میزان چالش برانگیز است که دیگر تلاش ها در جهت پرداختن به مسائل امنیتی این کشور. احتمال اینکه فعالیت های سایبری منجر به بی ثباتی های منطقه ای شود از تهدیدات غیر اینترنتی ایران کمتر است. همچنین، به لحاظ تاریخی، حملات مختل کننده تهران علیه اهداف غیر ایرانی، اقدامات تلافی جویانه طی عملیات جنگی بوده است تا تحریک درگیری های جدید. به منظور حفظ اعتبار در زمانی که فعالیت های نظارتی غرب از طریق درز کردن اسناد محرمانه افشا می شود، سیاست گذاری مؤثر در این زمینه باید بین جاسوسی یا علامت دهی و خرابکاری یا نقض حقوق بشر- اعمالی که هنجارهای بین المللی را زیر پا می گذارد- تفاوت قائل شود. همچنین دانستن اینکه عملیات تهاجمی سایبری ایران نیازی به انتقال فن آوری یا پشتیبانی دیگر دولت ها ندارد، حائز اهمیت است. اعضای عاملان تهدیدکننده ایرانی- که عمدتاً توسعه دهندگان نرم افزارهای نازل هستند و برای تعداد معدودی شرکت کار می کنند- همچنان به سختی قابل شناسایی هستند، تحت پیگرد قانونی قرار می گیرند و یا مجازات می شوند.

اعلام اسامی و بی آبرو کردن افراد شاید موجب ترس از مشارکت در عملیات هماهنگ با حکومت شود، بویژه در مورد افراد با استعدادی که مایلند از ایران خارج شوند یا خارج از کشور تحصیل کنند. با این همه، مشخص نیست که شرکت کنندگان در «عملیات ابابیل» یا دیگر کمپین ها پس از اینکه هویت شان آشکار شد، تغییری در نحوه دخالت خود در اینگونه کمپین ها داده باشند. افزون بر این، گروه های کوچک و کم اهمیت تر اهدافی مقرون به صرفه برای عملیات سایبری تلافی جویانه محسوب نمی شوند. در خاتمه باید عنوان کرد که ایران برای اجرای کمپین های ساده دارای مجموعه ای کافی از برنامه ریزان توانمند است. بنابراین، افشای عملیات سایبری و گردانندگان آن شاید منجر به تنزل یا تعویق توسعه توانایی های سایبری شود، اما این کشور را بطور کامل از چنین اقداماتی باز نخواهد داشت.

رویکردهای سیاست گذاری در خصوص تهدیدات سایبری ایران

گزینه های محدودی در زمینه سیاست گذاری باقی مانده است که عمدتاً عبارتند از: ۱) استفاده از ساختارهای موجود برای تحریم های هدفمند یا کیفرخواست، ۲) افزایش اطلاع رسانی در خصوص تهدیدات در سرتاسر جوامع و ۳) پشتیبانی از ابتکار عمل ها در جهت افزایش امنیت اطلاعات.

نظام تحریم های جامع علیه ایران احتمالاً دخالت عمده ای در توسعه توانایی های تهاجمی سایبری این کشور نخواهد داشت. ایرانیان معمولاً از سرورهای خارج از کشور استفاده می کنند که نوعاً در شبکه های موجود در اروپا و روسیه قرار دارند و به دیگر شبکه های جرائم سایبری (Bulletproof hosting) سرویس می دهند یا با استفاده از اطلاعات جعلی ثبت شده اند. از آنجا که منابع لازم برای افزایش ظرفیت ها بیشتر به توسعه حرفه ای و سازمانی بستگی دارد تا کامپیوترها یا زیرساخت، جلوی میزان اندکی از موارد یا خدمات فنی را می توان گرفت. افزون بر این، نظام تحریم های بسیار گسترده که به دنبال جلوگیری از فعالیت های سایبری مخرب است، به احتمال زیاد صدمات جانبی عمده ای به جریان آزاد اطلاعات به ایران خواهد داشت- موضوعی که جامعه مدنی ایران بطور مفصل درباره آن بحث کرده است.

آنجا که تحریم ها مناسبند، دفتر کنترل دارایی های خارجی در وزارت خزانه داری ایالات متحده از برنامه های هدفمندی حمایت می کند که می توان علیه نهادهای بین المللی که توانایی ایران در زمینه نظارت بر مردم خود را افزایش می دهند (دستورالعمل اجرایی ۱۳۶۰۶) و همچنین علیه کسانی که مسئول عملیات سایبری ضد زیرساخت های آمریکا هستند (دستورالعمل اجرایی ۱۳۶۹۴) بکار گرفته شوند. از تحریم ها و دیگر مکانیسم های مالی می توان به منظور جلوگیری از حمایت کشورهای خارجی و دیگر عوامل از عملیات تهاجمی سایبری ایران استفاده کرد. دستورالعمل اجرایی ۱۳۶۰۶ نمونه ای از اختیارات خود مبنی بر تعیین هر نهادی که در ایران یا جاهای دیگر در زمینه «مختل کردن، نظارت و ردیابی شبکه و کامپیوتر» تسهیلاتی برای حکومت ایران فراهم می کند، ارائه داده است. در حالی که این دستورالعمل بر حقوق بشر تمرکز دارد، زبان مشابهی می تواند بر حملات تهران علیه زیرساخت های حیاتی و جاسوسی تمرکز داشته باشد. تعمیم دقیق این اختیارات می تواند به تضمین اینکه عملیات سایبری ایران از انتقال فن آوری یا کمک های خارجی بهره نبرد، کمک کند؛ آن هم در زمانی که تهران در حال گسترش روابط تجاری و امنیتی خود، بویژه با کشورهایی چون روسیه و چین است.

علاوه بر این، وزارت دادگستری کیفرخواست هایی علیه ایرانیان متهم به همکاری در کمپین های مختل کننده صادر کرده است (همان افرادی که گفته می شود مسئول عملیات ابابیل بودند و در دستورالعمل اجرایی ۱۳۶۹۴ مشخص شده بودند) و موفق شده است تا حکم استرداد هکری را که در سرقت اسرار نظامی دست داشت از کشور ثالث بگیرد. به دلیل جای پای کوچک عملیاتی این گروه ها، تحریم های هدفمند یا دعواهای حقوقی بیشتر نمادین هستند تا مختل کننده، اما در عین حال فرصت های معدودی وجود دارد تا افرادی که در چنین عملیاتی شرکت می کنند عواقب اعمال خود را ببینند.

با توجه به ماهیت ابتدایی عملیات سایبری ایران، یک پاسخ حقوقی یا سیاسی محض که صرفاً متمرکز بر بازدارندگی ایران باشد، برای پرداختن به خطرات امنیت سایبری در کشور از کارآیی لازم برخوردار نیست. هر سیستمی که گروه های ایران بتوانند در آن رخنه کنند، به همان اندازه در معرض حملات دیگران (بویژه کره شمالی و حماس) با مجموعه ای از انگیزه های مشابه است. یک خط مشی مؤثر در برابر تهدیدات ایران بطور کلی باید متمرکز بر تأمین امنیت زیرساخت های حیاتی باشد.

به اشتراک گذاری اطلاعات یکی از مرسوم ترین استراتژی هایی است که ایالات متحده، اروپا و بخش خصوصی به منظور کاهش میزان تأثیر عملیات سایبری ایران اتخاذ کرده اند. پس از حمله آرمکو، ایالات متحده از برتری خود در نظارت و نسبت دادن این فعالیت ها به ایران سود برد تا مناسبات امنیتی با متحدان عرب خود در خلیج فارس را مستحکم کند. این امر منبعی بسیار ارزشمند است که در صورت امکان باید تعمیم یابد و پشتیبانی بیشتری برای متحدان منطقه ای فراهم آورد. به همین ترتیب، سازمان اف بی آی اطلاعیه هایی در خصوص کمپین های معین ایران برای بخش خصوصی تهیه و به اشتراک گذاری اطلاعات را تسهیل کرد. با وسعت بخشیدن به این تلاش ها می توان شرکای بیشتری را در بر گرفت و این داده ها را در اختیار سازمان های جامعه مدنی نیز قرار داد.

برخلاف مباحث امنیتی سنتی، اشخاص مستقل- به دلیل ماهیت مجازی و فراملیتی این تهدیدات- بیشتر در معرض عملیات سایبری قرار دارند. این موضوع پای افراد بیشتری را به میان می کشد که برای مراقبت از خود در برابر جرائم و جاسوسی تحت فشار بیشتری قرار می گیرند. مسئولیت حفاظت از این کاربران بطور مساوی بر عهده بخش خصوصی و دولت است. خوشبختانه پلتفرم های اینترنتی و خدمات وسایل ارتباطی، مانند فیس بوک و گوگل نقش مثبتی در تهیه ابزاری که به افراد در دفاع علیه حملات کمک می کند، ایفا کرده اند و حتی تا آنجا پیش رفته اند که کاربرانی که هدف کمپین های هماهنگ با دولت- شامل حملات از ایران- قرار گرفته اند را مطلع کرده اند. این ابتکار عمل ها کار مهاجمان را دشوار می کند و شرکت های فن آوری باید آنها را به عنوان تعهد اصلی خود مبنی بر حفظ ایمنی کاربران بکار گیرند.

مباحث مربوط به تأمین امنیت مخالفان کامل نخواهد بود، مگر اینکه بر نقش پیشرو دولت ایالات متحده و سازمان های توسعه در اروپا در فراهم آوردن ابزار ارتباطی ایمن برای کنشگران- که اغلب برنامه آزادی اینترنت نامیده می شود- تأکید شود. سرمایه گذاری مراحل اولیه از طریق بودجه دولتی در اختیار پژوهشگران و توسعه دهندگان قرار گرفته تا به تولید نمونه های اصلی و محصولات قابل پخش برای حفاظت از کنشگران و جامعه مدنی بپردازند که مورد توجه بخش خصوصی قرار نمی گیرند. بخش عمده- اگر نگوییم اکثریت- ایرانیانی که نظام سانسور را دور می زنند، این کار را با استفاده از ابزار مطمئن و معتبری انجام می دهند که بودجه اش از طرف وزارت امور خارجه آمریکا و هیئت رئیسه شورای اطلاع رسانی دولت آمریکا (Broadcasting Board of Governors) تهیه شده است. این دو همچنین از توسعه ابزار کدگذاری مثل Signal پشتیبانی کرده اند که شرکت های فن آوری در اپلیکیشن های پیام رسان خود مورد استفاده قرار داده اند و نشانگر اهمیت آزادی اینترنت به عنوان نوعی همکاری عمومی-خصوصی است.

ایالات متحده باید همچنان از برنامه ها و ضابطه های دسترسی به اینترنت و امنیت سایبری پشتیبانی کند که اولویت شان جریان آزاد و ایمن اطلاعات در برابر چالش های موجود از سوی کشورهایی چون ایران، چین و روسیه است. این امر علاوه بر تهیه بودجه برای جامعه مدنی، ترغیب ارزش های دموکراتیک در ساختار های اداره اینترنت، مثل «شرکت اینترنتی برای نام ها و شماره های واگذار شده» (ICANN) و اتحادیه مخابرات بین المللی (ITU) را نیز دربر می گیرد. این موضوع همچنین بر اهمیت سیاست های داخلی در خصوص تلاش برای آزادی اینترنت تأکید دارد: پیشنهاد در زمینه تضعیف محصولات امنیت اطلاعات از قبیل اپلیکیشن های پیام رسان کدگذاری شده، به مردم کشورهایی که در آنها حکومت قانون ضعیف است و دسترسی پنهانی به شبکه های ارتباطات معمولاً برای سرکوب مورد استفاده قرار می گیرد، صدمه می زند.

براساس سابقه عملیات تهاجمی سایبری ایران، همان عاملانی که مسئول جاسوسی علیه بخش خصوصی هستند در نظارت بر مدافعان حقوق بشر نیز دخالت دارند که به دلیل محدودیت منابع این اهداف، بطور چشمگیری موفقیت آمیزتر بوده اند. اینگونه جوامع در خطر شاخصی هستند برای تاکتیک ها و ابزاری که علیه اهداف دیگر به کار گرفته خواهند شد، و تبادل فزاینده اطلاعات موجب آموزش و استراتژی های کاهشی مؤثرتر برای همگان خواهد شد. مدت مدیدی است که سیاست گذاران متوجه شده اند که تنها تغییر از درون می تواند ایران را به یکی از اعضای سازنده جامعه جهانی تبدیل کند. ایمنی و امنیت سازمان های جامعه مدنی ایران و صداهای دمکراتیک که هدف عملیات سایبری حکومت قرار می گیرند، باید به عنوان سهامداران مهم در مباحث امنیت سایبری و سیاست خارجی به رسمیت شناخته شده و مورد حمایت قرار گیرند.

فرهنگ اصطلاحات

کمپین: مجموعه ای از فعالیت ها که توسط عاملان تهدیدکننده با هدفی خاص صورت می پذیرد.

سرقت نام و پسورد حساب های کاربری: روند سرقت نام و پسورد حساب های کاربری وابسته به پلتفرم های اینترنتی.

DDoS: تلاش برای از دسترس خارج کردن یک سرویس اینترنتی از طریق ایجاد ترافیک سنگین از چندین منبع.

عملیات تهاجمی سایبری: عملیات فضای سایبری با هدف قدرت نمایی از طریق اعمال زور در فضای سایبری.

Sinkhole: تغییر مسیر ترافیک مخرب اینترنتی به منظور آنکه پژوهشگران امنیتی بتوانند آنرا ذخیره و تحلیل کنند.

فیشینگ هدفمند: حمله هدفمندی که با استفاده از یک ایمیل گمراه کننده صورت می گیرد تا دریافت کننده آن را فریب دهد و او رفتار خطرناکی به نفع دشمن انجام دهد.

حمله زنجیره: نفوذ استراتژیک به یک نهاد خاص، مانند یک فروشنده، با هدف نفوذ غیرمستقیم به یک هدف دیگر، همچون مشتریان آن فروشنده.

عامل تهدیدکننده: فرد یا گروهی که در فعالیت سایبری مخرب شرکت دارد.

حمله Watering hole: نفوذ به یک وبسایت منتخب به منظور اجرای حملات نفوذی از طریق انتقال بدافزار به بازدیدکنندگان وبسایت.