گزارش دیده‌بان هکری

چالش مشروعیت جمهوری اسلامی به دست هکرها

فیلتربان
دی ۱۴۰۱ ـ خرداد ۱۴۰۲ / ژانویه ـ ژوئن ۲۰۲۳

فشرده

حمله‌های سایبری و درز اطلاعات از دی ۱۴۰۱ تا آخر خرداد ۱۴۰۲ (نیمه اول سال ۲۰۲۳ میلادی) همچون گذشته ادامه پیدا کرد. هدف نخست کنشگران هکری، دولت ایران بود. هکرهای متعددی موفق شدند وبسایت‌های رسمی را تغییر صورت دهند، در شبکه‌های داخلی نفوذ کنند و اسناد فوق‌محرمانه را برملا سازند. با آنکه هویت بسیاری از این گروه‌ها و نوع وابستگیِ آنها شناخته نیست، همه یک انگیزه دارند: استفاده از اینترنت همچون سلاحی علیه یکی از قدرت‌های سایبری در حال ظهور در جهان برای آنکه انتقام سرکوب مردم ایران را از دولت بگیرند. اسنادی که به دست هکرها افتاده، فساد و سرکوب و روش‌های غیرقانونی برای حفظ قدرت را برملا می‌کنند.

در هر کشوری این میزان حمله سایبری و درز اطلاعات یک تهدید برای امنیت ملی به شمار آمده و باعث انجام تحقیقات وسیع برای شناسایی و رفع آسیب‌پذیری‌ها می‌شود. اما دولت ایران تاکنون فقط دست به انکار این حمله‌ها زده‌است. گمانه‌زنی درباره وابستگی گروه‌های هکری ادامه دارد. در بهترین حالت، هکرها خود شهروندان ناراضی هستند که در همدردی با معترضان دست به عمل می‌زنند. این احتمال هم وجود دارد که حمله‌های سایبری و درز اطلاعات به دست دولت‌های در تقابل با جمهوری اسلامی در مسابقه میان سازمان‌های اطلاعاتی رخ داده باشد تا در بزنگاه ناآرامی‌ها اسرار مهم دولتی را فاش کنند. اعتراضات مردمی به سبب سرکوب فزاینده، آرام آرام به حالت زیرزمینی در می‌آید و احتمالا به همان نسبت حمله‌های سایبریِ انتقام‌جویانه هم شدت می‌گیرد.

پیش‌گفتار

طی چند سالِ گذشته در ایران، گروه‌های هکری متعددی پدید آمده‌اند که هدف‌ها، انگیزه‌های سیاسی و اهداف گوناگونی را پی می‌گیرند. فهمیدن اینکه این گروه‌ها به کجا وابسته‌اند، تقریبا غیرممکن است. برخی با هدف افشای اسرار دولت ایران عمل می‌کنند و برخی دیگر دشمنان جمهوری اسلامی مثل اسراییل و ایالات متحده را هدف می‌گیرند. از سال ۱۳۹۹ تعداد این عملیات از هر دو طرف بیشتر شده و بیش از پیش نیز در معرض آگاهی عموم قرار گرفته‌اند، به نحوی که رقابت دو سویه در فضای سایبری به وضوح نمایان است.

به دنبال جنبش «زن، زندگی، آزادی» که در شهریور ۱۴۰۱ آغاز شد، چند گروه هکری حمله‌های خود به رژیم ایران را آغاز کردند. آنها اسناد محرمانه درباره برنامه هسته‌ای را افشا و پخش زنده برنامه صدا و سیما را مختل کردند، همچنین چندین وبسایت دولتی را تغییر چهره دادند. هر گروه برای خود شخصیتی جداگانه به وجود آورده، شعار خاص خود را دارد و هر بار حوزه عملیات و اهدافش را وسیع‌تر می‌کند. شهروندان ناراضی از این فعالیت‌ها استقبال می‌کنند و دولت سعی می‌کند آنها را جدی نگیرد. تصویری که از اسناد افشا شده به دست آمده، حاکی از وجود یک زیرساخت پر پیچ و خم برای دور زدن تحریم‌های اقتصادی، نبرد جناح‌ها بر سر قدرت است، شاخه‌های گسترده سپاه پاسداران و جاه‌طلبی‌های سیاسیِ فزاینده‌اش را روایت می‌کند و حضور دستگاه‌های درهم‌تنیده سرکوب و نظارت بر مردم را به نمایش می‌گذارد.

این گزارش «دیده‌بان هکری» فعالیت‌های هکرها علیه جمهوری اسلامی را در نیمه اول سال ۲۰۲۳ میلادی، یعنی از دی‌ماه ۱۴۰۱ تا پایان خرداد ۱۴۰۲ پوشش می‌دهد. به این دلیل که تعداد گروه‌های هکری و حجم اسناد فاش شده در این دوره قابل‌توجه بوده، این گزارش بیشتر تمرکز خود را روز موضوعات ذکر شده گذاشته است. مجموع این فعالیت‌ها چشم‌اندازی در حال تحول را ترسیم می‌کنند که در آن مشروعیت نظام بیش از پیش به چالش گرفته می‌شود.

ناشناس (Anonymous)

گروه هکری «ناشناس» در سال میلادی ۲۰۲۳ همچنان به فعالیت ادامه داد. در ۲۶ دی ۱۴۰۱، «ناشناس» بیش از بیست‌هزار ایمیل متعلق به بزرگ‌ترین شرکت پتروشیمی ایران را افشا کرد. این ایمیل‌ها پیام‌های محرمانه، ارتباطات، اسناد تجاری و سندهای دیگری را شامل می‌شد که در فاصله مرداد ۱۳۹۹ تا مهر ۱۴۰۱ ارسال شده بودند. این ایمیل‌ها

تصویر ۱، نقشه‌ای که به ادعای «ناشناس» نشانگر پایگاه‌های سپاه در مرز غربی ایران است.

روشن می‌کردند که چگونه جمهوری اسلامی از طریق شرکت‌های خصوصی مثل شرکت تجارت صنعت پتروشیمی خلیج فارس تحریم‌های اقتصادی ایالات متحده آمریکا را دور می‌زند. طبق اسناد افشا شده، دولت ایران با استفاده از شبکه وسیعی از شرکت‌های صوری دست به صدور نفت و محصولات پتروشیمی می‌زند. کشور چین واردکننده اول است. پس از چین، کشورهای هند، عراق، ترکیه، و امارات متحده عربی از واردکنندگان اصلی هستند.[۱] طی بیش از دو سال، جمهوری اسلامی ۹.۴ میلیارد دلار نفت به چین صادر کرده است.

طی دو ماه بعد نیز گروه «ناشناس» به کار خود ادامه داد. این گروه در ۱۳ بهمن ۱۴۰۱ اعلام کرد وبسایت رسمی وزارت فرهنگ و ارشاد اسلامی را تغییر چهره داده است. پس از قتل مهسا (ژینا) امینی به دست گشت ارشاد، این اداره به خاطر تحمیل باورهای مذهبی به جوانان مورد انزجار مردم قرار گرفت. در ۳۰ بهمن ۱۴۰۱ گروه «ناشناس» مدعی شد که وبسایت استانداری کرمان را تغییر صورت داده‌است. در ۶ فروردین ۱۴۰۲، گروه «ناشناس» نقشه‌ای از پایگاه‌های سپاه را به بیرون درز داد که در آن محل انبارهای سلاح و مهمات در حاشیه مرز غربی کشور مشخص شده بود (تصویر ۱).

بلک ریوارد (Black Reward)

در تاریخ ۳۰ دی ۱۴۰۱ گروه هکری «بلک ریوارد» که چند ماه پیش‌تر با سر و صدا آغاز به کار کرده بود[۲]، با مجموعه تازه‌ای از اسناد مربوط به یکی از دانشگاه‌های وابسته به سپاه به صحنه نبرد بازگشت. دانشگاه امام صادق پیش از انقلاب ۵۷ با نام دیگری به دست گروهی از دانش‌پژوهان تحصیل‌کرده در دانشگاه‌های هاروارد و ام‌آی‌تی تاسیس شده بود. هدف از ایجاد این دانشگاه، تربیت مدیران زبده و متخصص بود تا در بخش‌های دولتی و خصوصی به خدمت گرفته شوند. پس از انقلاب، این دانشگاه به دست اسلام‌گرایان افتاد و به محل آموزشِ مدیرانی تبدیل شد که می‌بایست از لحاظ سیاسی و ایدیولوژیک همسو با نظام اسلامی عمل کنند.

حمله هکری به دانشگاه امام صادق و درز اطلاعات آن از چند جهت اهمیت داشت. نخست، فاش می‌کرد که برنامه‌های دانشگاه برای کسب درآمد در بهترین حالت جای شک و شُبهه دارد. به ویژه فعالیت در زمینه استخراج ارز دیجیتال که به دلیل ناروشن بودن سیاست آن باعث شد شرکت‌های برق برای تامین نیروی مزرعه‌های استخراج رمزارز، به دلیل مصرف بالای برق، محدودیت قایل شوند. دانشگاه امام صادق برای

---

۱ وبسایت «ویکی‌ایران» که به چاپ اسناد افشاشده می‌پردازد در ماه‌های اخیر بخشی از این سندها را بایگانی کرده است. داده‌های قابل جستجو مربوط به ایمیل‌های شرکت تجارت صنعت پتروشیمی خلیج فارس نشان می‌دهد که محموله‌های پتروشیمی ایران به اروپا نیز صادر شده‌اند (در این داده‌ها ۶۵ بار این مقصد ذکر شده بدون آنکه از کشور خاصی نام آورده شود). به همین ترتیب «اتحاد کشورهای مشترک‌المنافع» که سابقاً عضو اتحاد جماهیر شوروی بودند (۲۹ بار) و آفریقا (دو بار) ذکر شده‌اند، بدون آنکه نام کشور معینی آورده شود. واردکنندگان دیگر عبارت‌اند از افغانستان، پاکستان، روسیه، سنگاپور، برزیل، عُمان، تایوان، و چند کشور دیگر.

۲ در فاصله شهریور تا آذر ۱۴۰۱ پس از شروع اعتراضات «زن، زندگی، آزادی» بلک ریوارد به تنهایی بیش از هر گروه هکری دیگری موفق شد اسناد محرمانه را به بیرون درز دهد. این اسناد متعلق به خبرگزاری فارس وابسته به سپاه، سازمان توسعه انرژی اتمی ایران، شرکت ملی نفت و گاز، و پرس تی‌وی، بازوی بین‌المللی صدا و سیما بود.

تحقیقات صنعتی، معدنی و تجاری موفق به کسب مجوز استخراج ارز دیجیتال از یک مقام محلی در استان خراسان رضوی شده بود. این مزرعه استخراج ارز در یک کارخانه نیمه‌متروک لباس به نام «کارخانه پوشاک جامعه» مستقر شده بود[۳] تا ضمن صرفه‌جویی در مصرف برق فعالیت‌اش را پنهان نگه دارد. اما شرکت برق به دلیل پرداخت نشدن بهای الکتریسیته از تامین انرژی خودداری کرده و کار این مزرعه را دچار وقفه کرد. کمی بعد، این مزرعه با حکم دادگاه کارش را از سر گرفت اما طبق مفاد اسناد فاش شده، دعوا با شرکت برق بر سر صورتحساب حل‌نشده باقی ماند.

دوم، این افشاگری‌ها نشان می‌داد، نهادهای مدافع رژیم نه تنها به دلایل عقیدتی بلکه به خاطر نفع مالی تا چه میزان در تحمیل حجاب اجباری نفع دارند. یکی از سندهای لو رفته نشان‌دهنده تمایل دانشگاه به همکاری با کسب‌وکارهای مشهد است که یکی از مراکز صنعت گردشگری مذهبی و زیارت شیعی به شمار می‌رود. هدف از این همکاری، تولید چادر مشکی برای فروش به زنان در مشهد بوده است. با توجه به محبوبیت چادر سیاه میان مومنان مشهدی و همچنین نیاز زیارت‌کنندگان زن به این پوشش برای ورود به حرم امام رضا، ریاست دانشگاه قصد کسب سود سرشار از این مدل کسب و کار را داشته است.

سوم، سندهای لو رفته نشان می‌دهند که در بالاترین سطوح هیات‌امنای دانشگاه، سومدیریت و شفاف نبودن در حسابداری و امور مالی حاکم است. یکی از این اسناد، جزییاتی از گزارش بازرسان حسابداری دانشگاه را فاش می‌کند. چندین خط از این گزارش شامل توصیه‌های حسابرسان برای تصحیح کمبودهای ثبت مدارک املاک و مستغلات دانشگاه است؛ موضوعی که سال‌ها مسکوت گذاشته شده و می‌تواند به وضع جریمه‌های مالیاتی کلان منجر شود.

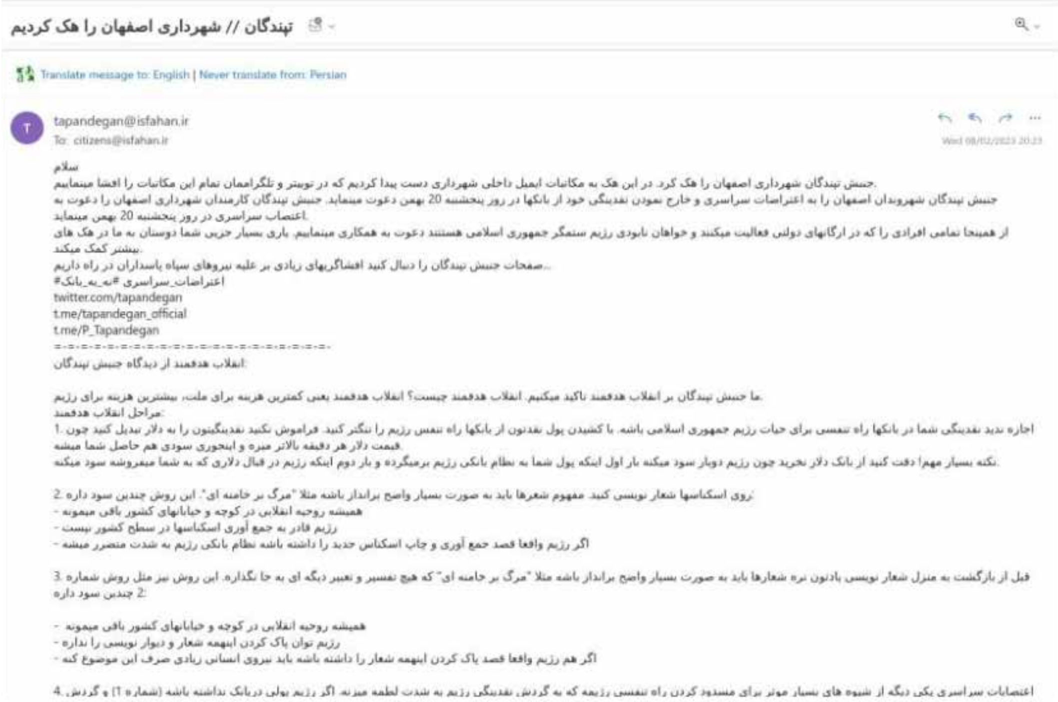
علاوه بر دانشگاه امام صادق، «بلک ریوارد» هدف‌های دیگری نیز داشت. در ۲۹ بهمن ۱۴۰۱، این گروه هکری اسناد تازه‌ای از خبرگزاری نیمه‌دولتیِ فارس - یک رسانه مهم وابسته به سپاه - منتشر کرد. بلک ریوارد قبلا در آبان ۱۴۰۱ با هک کردن خبرگزاری فارس یک رشته بولتن محرمانه را به بیرون درز داد که در آنها برنامه‌های رژیم برای سرکوب اعتراضات «زن، زندگی، آزادی» برشمرده شده بود. ظاهرا اسناد جدید هم بخش دیگری از همان فایل‌های آبان است. این مدارک اخیر در برگیرنده گزارش‌هایی است که خبرنگاران خبرگزاری فارس در سال‌های ۱۳۹۷ تا ۱۴۰۱ برای سران سپاه تهیه کرده بودند که شامل فایل‌های صوتی مصاحبه (چاپ شده و چاپ‌نشده) و بولتن‌ها (گزارش‌های اطلاعاتی و امنیتی) می‌شد.

بولتن‌های افشاشده به موضوعاتی چون داده‌های تحلیلی و آماری کاربران رسانه‌های اجتماعی و اوضاع اقتصادی می‌پرداختند. از آن میان یک سند ۲۴۷ کلمه‌ای[۴] قابل ذکر است که ظاهرا برای شورای عالی فضای مجازی تهیه شده‌است. این شورا مرجع اصلی نظارت بر فضای مجازی در ایران است. گزارش مورخ ۱۶ بهمن ۱۳۹۹ به محبوب‌ترین پیام‌های فارسیِ اینستاگرام در هفته پیش از آن تاریخ می‌پردازد. این پست‌ها بر حسب موضوع دسته‌بندی شده‌اند؛ از جمله کارهای روزانه سلبریتی‌ها، تولیدات موسیقی داخلی و تبعیدی، اخبار داخلی و خارجی، همچنین مطالبی که افراد سرشناس

---

۳ اسناد لو رفته نشان می‌دهد که این کارخانه پوشاک نیز بخشی از دارایی‌های دانشگاه امام صادق است.

۴ سند شماره ۹۹۱۱۰۴ شورای عالی فضای مجازی


تپندگان // شهرداری اصفهان را هک کردیم

Translate message to: English | Never translate from: Persian

tapandegan@isfahan.ir
To: citizens@isfahan.ir
Wed 08/02/2023 20:23

سلام
جنبش تپندگان شهرداری اصفهان را هک کرد. در این هک به مکاتبات ایمیل داخلی شهرداری دست پیدا کردیم که در توییتر و تلگراممان تمام این مکاتبات را افشا مینماییم.
جنبش تپندگان شهروندان اصفهان را به اعتراضات سراسری و خارج نمودن نقدینگی خود از بانکها در روز پنجشنبه 20 بهمن دعوت مینماید. جنبش تپندگان کارمندان شهرداری اصفهان را دعوت به اعتصاب سراسری در روز پنجشنبه 20 بهمن مینماید.
از همینجا تمامی افرادی را که در ارگانهای دولتی فعالیت میکنند و خواهان نابودی رژیم ستمگر جمهوری اسلامی هستند دعوت به همکاری مینماییم. یاری بسیار جزیی شما دوستان به ما در هک های بیشتر کمک میکند.
صفحات جنبش تپندگان را دنبال کنید افشاگریهای زیادی بر علیه نیروهای سپاه پاسداران در راه داریم...
اعتراضات_سراسری #نه_به_بانک#
twitter.com/tapandegan
t.me/tapandegan_official
t.me/P_Tapandegan
=-
انقلاب هدفمند از دیدگاه جنبش تپندگان:

ما جنبش تپندگان بر انقلاب هدفمند تاکید میکنیم. انقلاب هدفمند چیست؟ انقلاب هدفمند یعنی کمترین هزینه برای ملت، بیشترین هزینه برای رژیم.
مراحل انقلاب هدفمند:
1. اجازه ندید نقدینگی شما در بانکها راه تنفسی برای حیات رژیم جمهوری اسلامی باشه. با کشیدن پول نقدتون از بانکها راه تنفس رژیم را تنگتر کنید. فراموش نکنید نقدینگیتون را به دلار تبدیل کنید چون قیمت دلار هر دقیقه بالاتر میره و اینجوری سودی هم حاصل شما میشه.
نکته بسیار مهم: دقت کنید از بانک دلار نخرید چون رژیم دوبار سود میکنه بار اول اینکه پول شما به نظام بانکی رژیم برمیگرده و بار دوم اینکه رژیم در قبال دلاری که به شما میفروشه سود میکنه.

2. روی اسکناسها شعار نویسی کنید. مفهوم شعرها باید به صورت بسیار واضح برانداز باشه مثلا "مرگ بر خامنه ای". این روش چندین سود داره:
- همیشه روحیه انقلابی در کوچه و خیابانهای کشور باقی میمونه
- رژیم قادر به جمع آوری اسکناسها در سطح کشور نیست
- اگر رژیم واقعا قصد جمع آوری و چاپ اسکناس جدید را داشته باشه نظام بانکی رژیم به شدت متضرر میشه

3. قبل از بازگشت به منزل شعار نویسی یادتون نره شعارها باید به صورت بسیار واضح برانداز باشه مثلا "مرگ بر خامنه ای" که هیچ تفسیر و تعبیر دیگه ای به جا نگذاره. این روش نیز مثل روش شماره 2 چندین سود داره:

- همیشه روحیه انقلابی در کوچه و خیابانهای کشور باقی میمونه
- رژیم توان پاک کردن اینهمه شعار و دیوار نویسی را نداره
- اگر هم رژیم واقعا قصد پاک کردن اینهمه شعار را داشته باشه باید نیروی انسانی زیادی صرف این موضوع کنه

4. اعتصابات سراسری یکی دیگه از شیوه های بسیار موثر برای مسدود کردن راه تنفسی رژیمه که به گردش نقدینگی رژیم به شدت لطمه میزنه. اگر رژیم پولی در بانک نداشته باشه (شماره 1) و گردش

تصویر ۲، نمونه‌ای از یک ایمیل که «تپندگان» به ساکنان اصفهان ارسال کرد.

در مورد حقوق بشر و رفتار حاکمیت در اینستاگرام نشر داده بودند.[۵]

این سند به این دلیل اهمیت دارد که اولا میزان اطلاع‌رسانیِ خبرگزاری فارس به شورای عالی فضای مجازی طبعا نفوذ غیرمستقیم بر تصمیماتِ این شورا را نشان می‌دهد. دوما این گزارش نقش خبرگزاری فارس را در دستگاه وسیع جاسوسی و نظارتِ دولتی افشا می‌کند. این خبرگزاری با رصدکردن رسانه‌های اجتماعی و تهیه گزارش‌های سرشار از جزییات، نبض زندگیِ روزمره شهروندان را گرفته و اطلاعات آنان را در اختیار ارگان‌های تصمیم‌گیرنده می‌گذارد که در بهترین حالت، خبرچینی از مردم و در بدترین حالت جاسوسی رسمی امنیتی در فضای مجازی است.

تپندگان

۱۹ بهمن ۱۴۰۱، گروه هکری «تپندگان» دست به حمله تازه‌ای زد و این بار شهرداری اصفهان را هدف گرفت. پس از این رویداد، تپندگان یک پیامک جمعی به ساکنان اصفهان فرستاد و در آن از شهروندان خواست پس‌اندازها و سپرده‌های خود را از بانک‌ها بیرون بکشند تا با ایجاد کسری سرمایه، رژیم در آستانه سقوط قرار گیرد. پیامک‌های دیگری نیز از سوی تپندگان به مردم اصفهان، کارکنان شهرداری این شهر و گزارشگران داخلی و خارجی فرستاده شد.

در مهرماه ۱۴۰۱، گروه تپندگان به پایگاه اینترنتی دانشگاه دخترانه الزهرا نفوذ کرد. این دانشگاه به خاطر رعایت سختگیرانه قواعد مذهبی در خصوص حجاب و پذیرش دانشجو شهرت دارد.

---

۵ برای نمونه پیام‌های مسیح علی‌نژاد درباره حکم زندان یک فیلمساز مستقل و منع ورود زنان به استادیوم ورزشی ذکر شده. سند دیگر به یک نمایش استندآپ کمدی اشاره دارد که گوینده از هوای آلوده تهران صحبت کرده و ساکنان شهر را ترغیب می‌کند که مسوولان را مجبور به پاسخگویی کنند.

«واندر» (Wonder)

همزمان با حمله گروه تپندگان در ۱۹ بهمن ۱۴۰۱، یک شخصیت هکری دیگر به نام «واندر» اعلام موجودیت کرد. واندر اعلام کرد که در واکنش به اعدام‌های ناعادلانه چند پایگاه اینترنتی قوه قضاییه را پایین کشیده است.

عدالت علی

در تاریخ ۲۰ بهمن ۱۴۰۱، گروه هکری «عدالت علی» که پیش‌تر ویدیوهای دوربین‌های مداربسته زندان اوین را به بیرون درز داده بود، یک گزارش محرمانه از قوه قضاییه منتشر کرد که به سرعت جنجال آفرید. این گزارش با جزییات توصیف می‌کند چگونه دو عضو سپاه پاسداران - که یکی از آنها به اطلاعات سپاه تعلق داشته- دو زن جوان بازداشتی را مورد تعرض جنسی قرار می‌دهند. طبق این گزارش، دو مامور سپاه در یک پمپ بنزین پس از وارسی گوشی‌های همراه آن دو زن و یافتن «موضوعات معاند نظام» آنها را دستگیر می‌کنند. سپس به هنگام انتقال بازداشتی‌ها به یکی از مراکز «مستقلِ» سپاه (طبق گزارش)، در میان راه به آن دو زن تجاوز کرده و سپس آنها را رها می‌کنند.

بعد از این ماجرا، دو زن قربانی با رجوع به یک شعبه کلانتری تلاش می‌کنند شکایت‌نامه‌ای به ثبت برسانند اما با مداخله نمایندگان وزارت اطلاعات از این کار منع می‌شوند. با این حال، پافشاری شاکیان باعث شد که دفتر دادستان کل به شکل محرمانه موضوع را پی بگیرد. دادستانی نه تنها ماموران سپاه را مقصر دانست بلکه از منزل یکی از آن دو مدارکی نیز پیدا کرد. در میان یافته‌های دادستانی مقداری مواد مخدر، سلاح گرم و همچنین تعدادی لباس فرم فراجا (فرماندهی انتظامی جمهوری اسلامی ایران) و لباس روحانیت به قصد لاپوشانیِ عملیات سپاه کشف شد.

گزارش لو رفته از چند جهت قابل توجه است. این گزارش به صراحت رفتار مجرمانه ماموران سپاه علیه زنان ایران و همچنین ناراضیان را مستند می‌کند. به هنگام اعتراضات «زن، زندگی، آزادی»، بسیاری از شاهدان سپاه پاسداران را متهم کردند که با شلیک گلوله‌های ساچمه‌ای به دستگاه تناسلی زنان جوان و نیز تعرض جنسی، دست به سرکوب گسترده این معترضان زده است. دستگیرشدگان نیز بارها از وجود شکنجه، اخاذی، و رفتار خشن در بازداشتگاه‌ها شکایت کرده‌اند. در گزارش لو رفته که به وسیله بالاترین مقام‌های قوه قضاییه تهیه شده، این اتهام‌ها تأیید شده است. اما تهیه‌کنندگان گزارش هیچ قدمی برای جلوگیری از این جرایم برنداشتند. برعکس، نویسندگان گزارش توصیه می‌کنند که جرم صورت گرفته مخفی بماند و در معرض افکار عمومی قرار نگیرد، دو مامور متجاوز فقط از کار برکنار شوند و در گزارش‌های بعدی ذکری از وابستگی آنها به سپاه پاسداران به میان نیاید.

دو روز بعد از لو رفتن این گزارش، در ۲۲ بهمن ۱۴۰۱، گروه عدالت علی نامه‌ای را از قوه قضاییه برملا کرد که نشان می‌داد علیه خویشاوندان نزدیک علی خامنه‌ای رهبر نظام شکایتی به دادگاه رسیده است: در این سند از اختلاس و فساد مالی گسترده در یکی از شرکت‌های تجاری متعلق به آنها و پنهان کردن اسناد مالی به قصد گمراه کردن حسابرسان صحبت به میان آمده است.

یک گروه بدون هویت

روز تحویل سال نوی خورشیدی یک گروه هکری ناشناس وارد پخش زنده شبکه دو صدا و سیما شد. برنامه زنده ناگهان تبدیل به یک شوی خبری از سوی یک کانال جعلی به نام «دی بی سی» شد، که بازی با نام «بی بی سی» بود.[۶] هکرها برنامه زنده سال نو را به یک شوی سیاسی مضحک تبدیل کردند در یک قسمت فردی به تقلید از یکی از رهبران حزب کارگران کردستان (پ.ک.ک) می‌گوید، ما تجزیه‌طلب نیستیم؛ واکنشی طعنه‌آمیز به دعواهای اخیر میان اپوزیسیونِ رژیم که کنشگران اتنیکی را به جدایی‌طلبی به قصد تجزیه ایران متهم می‌کنند.

روزنامه «فرهیختگان» این واقعه را تایید کرد، اما هیچ گروهی مسوولیت هک کردن صدا و سیما را به عهده نگرفت و در پی آن، هیچ بیانیه‌ای نه به وسیله‌ی مقامات دولتی و نه گروه‌های مخالف، منتشر نشد.

لب‌دوختگان

لب‌دوختگان یکی از قدیمی‌ترین و فعال‌ترین گروه‌های هکری، در ادامه فعالیت‌هایش این‌بار در ماه‌های فروردین و اردیبهشت ۱۴۰۲ دست به افشای اسناد زد. سوم فروردین ۱۴۰۲، لب‌دوختگان مدارک دیگری به بیرون درز داد که موضوع آنها فناوری نظارت و جاسوسی، از جمله نرم‌افزارهایی برای ضبط صدا و شنود گوشی‌ها بود که یکی از شاخه‌های سپاه پاسداران و نیروی قدس به نام «واحد ۳۰۰» (DSPRI) از آنها استفاده می‌کرده است. اطلاعات بیشتر راجع به این واحد در کانال تلگرام لب‌دوختگان به تاریخ یکم تیرماه ۱۴۰۲ به چاپ رسید[۷]. در ۱۱ اردیبهشت، لب‌دوختگان هویت دو هکر جمهوری اسلامی را که با گروه «ایلیا نت گستر» وابسته به بخش سایبری سپاه همکاری داشتند، افشا کرد. ایلیا نت گستر (که همچنین با نام‌های شهید شوشتری، امام‌نت پاسارگاد، و امنیت پاسارگاد شناخته می‌شود) در بهمن ۱۴۰۰ مشمول تحریم‌های اقتصادی آمریکا شد، زیرا این گروه هکری در سال ۲۰۱۸ میلادی (۱۳۹۶خورشیدی) زیر عنوان «ارتش سایبری یمن» فعالیت کرده بود. در ۲۸ اردیبهشت ۱۴۰۲، لب‌دوختگان یک ویدیو منتشر کرد که در آن ظاهرا علی مهدویان، یکی از هکرهای ایلیا نت گستر مورد حمله واقع می‌شود. وزارت امور خارجه ایالات متحده جایزه‌ای به مبلغ ۱۰ میلیون دلار برای کسب اطلاعات راجع به علی مهدویان تعیین کرده است زیرا این هکر در انتخابات ریاست جمهوری ۲۰۲۰ آمریکا مداخله سایبری کرده و خود را به نام «پراود بویز» - که یک گروه افراطی آمریکایی است- جا زده بود. در روز ۲۸ خرداد، لب‌دوختگان دو شرکت صوری متعلق به سپاه را افشا کرد که ظاهرا تولیدکننده پهپاد شاهد۱۳۶- هستند؛ پهپادهایی که ایران به روسیه صادر می‌کند تا در جنگ با اوکراین مورد استفاده قرار گیرند[۸].

قیام تا سرنگونی

در تاریخ ۱۷ اردیبهشت ۱۴۰۲، گروه هکری «قیام تا سرنگونی» ادعا کرد که سِروِرهای

---

۶ بی بی سی فارسی از کانال‌های خبری پربیننده در میان ایرانیان است.

۷ بخشی از این افشاگری‌ها نشان می‌داد که تعدادی از دانشگاه‌های مهم مثل دانشگاه تهران با واحد ۳۰۰ سپاه قدس همکاری دارند.

۸ این دو شرکت عبارت‌اند از: شرکت چکاد صنعت فراز آسیا و شرکت سدید سازه پرواز شریف.

وزارت امور خارجه ایران را هک کرده و ۲۱۰ دامنه اینترنتی و وبسایت را تغییر صورت داده است.[۹] این وبسایت‌ها تصویرهایی از رهبران سازمان مجاهدین خلق را به نمایش گذاشتند. خبر این اقدام نیز در یکی از سایت‌های مجاهدین منتشر شد. هکرها سپس به تدریج مجموعه‌ای از اسناد وزارت خارجه را درباره موضوعات مختلف متعلق به اواخر ۱۳۹۸ تا فروردین ۱۴۰۲ منتشر کردند. در میان این اسناد تصاویری از رهبران بالارتبه‌ای که عضو بسیج بودند[۱۰] - مثل وزیرخارجه فعلی، حسین امیرعبداللهیان - و اطلاعات مربوط به گذرنامه مقاماتی نظیر دبیرکل شورای عالی امنیت ملی وجود داشت.
اسناد لو رفته همچنین برخی از حساسیت‌های سیاست خارجی نظام را به نمایش می‌گذارد. نخست، توجه ویژه به سازمان مجاهدین خلق و حضور آنها در کشور آلبانی به چشم می‌خورد. وزارت امور خارجه به صورت پیاپی درگیر نامه‌نگاری با دولت و اعضای پارلمان آلبانی بوده تا به پذیرش سازمان «تروریستی» مجاهدین در آن کشور اعتراض کند. ارجحیت دیگر، مساله اسدالله اسدی، دیپلمات ایرانی در بلژیک بود که در سال ۲۰۲۱ میلادی به جرم مشارکت در طرح بمب‌گذاری در کنفرانس سالانه مجاهدین در فرانسه دستگیر و به ۲۰ سال حبس محکوم شده بود. دولت ایران به شدت تلاش داشت اسدی را آزاد کند و سرانجام موفق شد از طریق معاوضه زندانیان با بلژیک در ماه مه ۲۰۲۳ او را به ایران بازگرداند.

گروه قیام تا سرنگونی در ۸ خرداد ۱۴۰۲ اسناد تازه‌ای را افشا کرد و در تلگرام مدعی شد که، «کل شبکه داخلی شدیدا حفاظت شده نهاد ریاست‌جمهوری رییسی جلاد در تهران تسخیر و از دسترس خارج شد.» طی سه ساعت بعد، هر چند دقیقه یکبار، قیام تا سرنگونی فایل‌ها، تصاویر، و ویدیوهای جدیدی منتشر کردکه همگی دسته‌بندی‌شده و برای پخشِ سریع آماده بودند. کم و بیش در همان ساعات، وبسایت سازمان مجاهدین خلق با انتساب این حمله به گروه قیام تا سرنگونی گزارش داد که، «ناراضیان ایرانی سِرورهای به شدت محافظت شده متعلق به ریاست جمهوری رژیم را تسخیر کردند.»

قیام تا سرنگونی ادعا کرد که کنترل ۱۲۰ سرور و مخزن‌های اطلاعاتی کلیدی مرتبط با شبکه داخلی دفتر ریاست جمهوری و بیش از ۱۳۰۰ کامپیوتر در این شبکه را به دست گرفته و به مکاتبه‌های محرمانه ریاست جمهوری و هیات وزیران دسترسی پیدا کرده است. اسناد محرمانه و فوق محرمانه، نقشه داخلی ساختمان دفتر ریاست جمهوری، آی‌پی‌ها یا آدرس‌های اینترنتیِ ارگان‌های مرتبط با رییس‌جمهور و دیگر سران دولت و نهادهای مهم دولتی مثل وزارت کشور، وزارت اطلاعات و نیروی بسیج، از جمله مدارکی بودند که به دست گروه قیام تا سرنگونی افتاد.

مدارک لو رفته برخی از ارجحیت‌های رژیم را در یک سلسله مسایل حساس مثل سازوکار کنترل اطلاعات نشان می‌داد. در نامه‌ای مورخ ۲۰ دی[۱۱] ۱۴۰۱، سرلشگر حسین سلامی، فرمانده قرارگاه ثارالله سپاه پاسداران که مسوول امنیت تهران است، اصرار کرد که در روز برگزاری کنکور ورودی دانشگاه‌های، اینترنت باید مسدود شود. این تصمیم - که گفته می‌شد از طرف وزیر علوم گرفته شده، ظاهرا به منظور جلوگیری از تقلب

---

۹ قیام تا سرنگونی در تاریخ ۶ بهمن ۱۴۰۰ در پیام‌رسان تلگرام اعلام موجودیت کرد. از همان روزهای نخست پیام‌های آن همسو با سازمان مجاهدین بود که نوعی از وابستگی را نشان می‌دهد. این گروه قبلاً به نهادهای دولتی نظیر دوربین‌های مداربسته‌ی شهرداری تهران و اطلاعات خصوصی بیش از ۳۰۰۰ تن از کارکنان قوه قضاییه دسترسی پیدا کرده بود.

۱۰ بسیج یک تشکیلات شبه‌نظامی متعلق به سپاه است.

۱۱ سند موسوم به «سلام _ ۰۷» منتشر شده به وسیله‌ی قیام تا سرنگونی در ۸ خرداد ۱۴۰۲.

و توزیع سوآل‌های کنکور قبل از روز امتحان بوده است. اما این تصمیم در حقیقت نشان‌دهنده این باور عمومی است که راه‌حل رژیم برای هر تنش اجتماعی یا سیاسی خاموش کردن اینترنت است؛ اعم از اینکه این تنش ناشی از اعتراضات سیاسی باشد یا برگزاری بدون دشواری آزمون سراسری.

دومین سند مهم افشا شده نامه فوق محرمانه فرمانده قرارگاه سایبری و تهدیدات جدید سپاه مورخ ۱۰ فروردین ۱۴۰۲ خطاب به رییس‌جمهور ابراهیم رییسی بود. در این نامه توصیه شده که، ترکیب اعضای شورای عالی فضای مجازی به نفع اعضای منتخب از سپاه تغییر کند. در این نامه همچنین پیشنهاد شده نقش نیروهای نظامی به ویژه سپاه پاسداران در زمینه نظارت بر درگاه‌های فضای مجازی کشور افزایش یابد. این سند تا بدانجا پیش می‌رود که اختیارات قوه مجریه، به ویژه وزارت اطلاعات و فناوری ارتباطات، را محدود سازد. در عوض، فرمانده سایبری سپاه توصیه می‌کند که نیروهای نظامی و امنیتی بهتر می‌توانند از درگاه‌های ارتباط اینترنت که راه ارتباط ایران با اینترنت بین‌المللی است محافظت کنند. به عبارت دیگر، سپاه پاسداران به دنبال آن است که بالاترین مرجع تصمیم‌گیری و سیاستگذاری فضای مجازی در ایران باشد. این تلاش در حالی صورت می‌گیرد که «طرح صیانت» که نظارت بر اینترنت را به سپاه می‌سپرد، در مجلس ناکام ماند.

سندهای لو رفته همچنین روشن می‌کنند که رژیم نسبت به اعتراضات دانشجویی بسیار حساس است و سپاه پاسداران در سرکوب جنبش‌های اعتراضی مثل جنبش دانشجویی تا حد زیادی دخالت دارد. در چندین سند، جزییات بحث‌های درونی واحدهای اطلاعاتی و امنیتی سپاه برای برخورد با اعتراض‌های دانشجویان و استادان مطرح شده است. در نامه‌ای به تاریخ ۱۱ مهر ۱۴۰۰، رییس‌جمهور از هیات وزیران می‌خواهد با استفاده از هشتگ‌هایی چون «#ایران_یکپارچه» در رسانه‌های اجتماعی به مقابله با تمایلات تجزیه‌طلبانه بپردازند. این یکی از موارد نادر و انکارنکردنی از دخالت دولت در روایت‌سازی توسط حساب‌های کاربری مدافع رژیم در رسانه‌های اجتماعی است. در پاسخ به این افشاگری‌ها، دولت بدون آنکه دلیلی برای این ادعا بیاورد، این مدارک را غیرواقعی دانست.

در تاریخ ۳۰ خرداد ۱۴۰۲، کمتر از یک ماه بعد از حمله به ساختمان ریاست‌جمهوری آلبانی، پلیس این کشور به اردوگاه مجاهدین خلق در نزدیکی ماینتس، شهر کوچکی در ۳۰ کیلومتری تیرانا پایتخت کشور، یورش برد. در این حمله ۱۵۰ دستگاه کامپیوتر که گویا مرتبط با فعالیت‌های سیاسی بودند به دست پلیس افتاد و تعدادی از اعضای مجاهدین و ماموران پلیس آلبانی مجروح شدند. بنا به اخبار منتشر شده، دولت آلبانی تحقیقاتی را درباره فعالیت‌های سیاسی اعضای سازمان مجاهدین آغاز کرده است. طبق توافقی که در سال ۱۳۹۲ خورشیدی میان مجاهدین و دولت آلبانی برای پناه دادن به مجاهدین صورت گرفته بود، اعضای این سازمان از فعالیت سیاسی منع و موظف به رعایت قوانین کشور شده بودند. فعالیت‌های سیاسی مجاهدین که سبب حمله پلیس شد - چنانچه به اثبات برسد- نقض آن توافق‌نامه به حساب می‌آید. دولت ایالات متحده آمریکا که یک دهه قبل بانی انتقال مجاهدین از عراق به آلبانی بود، در این درگیری جانب دولت آلبانی را گرفت و از حق حاکمیت ملی این کشور در اجرای قوانین‌ش دفاع کرد.

اعضای سازمان مجاهدین با افتخار به گزارشگران محلی اظهار داشته‌اند که چگونه به سیستم‌های ارتباطی نهادهای دولتی ایران و شهرداری تهران نفوذ کرده‌اند. روشن

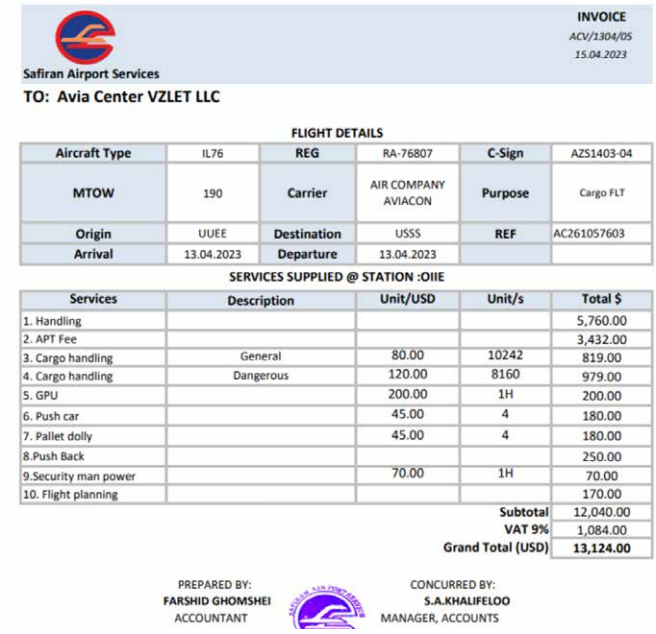
نیست منظور آنها فعالیت‌های «قیام تا سرنگونی» باشد. اما زمان و شرایط یورش به قرارگاه مجاهدین قابل تامل است. این یورش درست یک ماه پس از حمله‌های گسترده سایبری از سوی «قیام تا سرنگونی» به شبکه‌های دولتی در ایران صورت گرفت. طبق مدارک درز کرده از سوی این گروه هکری، دولت ایران از حضور مجاهدین در آلبانی نگران بوده و از راه‌های گوناگون تلاش کرده تا توافق میان دولت آلبانی و مجاهدین آسیب ببیند.

از یک دهه پیش که آلبانی تصمیم گرفت به مجاهدین پناه دهد، روابط میان جمهوری اسلامی و دولت آلبانی با تنش همراه بوده است. تابستان گذشته دولت آلبانی هدف حمله‌های سایبری قرار گرفت. دولت این کشور و شعبه تهدیدات سایبری مایکروسافت این حمله‌ها را به وزارت اطلاعات جمهوری اسلامی نسبت دادند. این حمله‌ها ظاهرا به تلافی حضور مجاهدین در خاک آلبانی صورت گرفت و متعاقب آن دولت این کشور روابط دیپلماتیک خود با ایران را قطع کرد. ایالات متحده نیز به خاطر این حمله‌ها تحریم‌های تازه‌ای علیه بعضی از مقامات ایرانی وضع کرد.

هوشیاران وطن

در تاریخ ۲۷ خرداد ۱۴۰۲، یک گروه هکری دیگر به نام «هوشیاران وطن» ایمیل‌های «شرکت خدمات فرودگاهی سفیران» را منتشر کرد. این گروه در کانال تلگرام خود نوشت که شرکت سفیران، «تسهیل‌کننده انتقال تسلیحات نظامی از سپاه به روسیه امپریالیستی است.»

گفته می‌شود شرکت سفیران که مرتبط با سپاه پاسداران است به تاجران و سرمایه‌دارن (به طور عمده روسی) و نهادهایی که معاملات مالی با سپاه دارند خدمات مسافرتی عرضه می‌کند و حتی محموله‌های نظامی را به روسیه منتقل می‌کند. برای این منظور، سفیران از شرکت‌های صوری در عمان و امارات متحده عربی استفاده می‌کند تا از



Safiran Airport Services

INVOICE
ACV/1304/05
15.04.2023

TO: Avia Center VZLET LLC

FLIGHT DETAILS

Aircraft Type	IL76	**REG**	RA-76807	**C-Sign**	AZS1403-04
MTOW	190	**Carrier**	AIR COMPANY AVIACON	**Purpose**	Cargo FLT
Origin	UUEE	**Destination**	USSS	**REF**	AC261057603
Arrival	13.04.2023	**Departure**	13.04.2023		

SERVICES SUPPLIED @ STATION :OIIE

Services	Description	Unit/USD	Unit/s	Total $
1. Handling				5,760.00
2. APT Fee				3,432.00
3. Cargo handling	General	80.00	10242	819.00
4. Cargo handling	Dangerous	120.00	8160	979.00
5. GPU		200.00	1H	200.00
6. Push car		45.00	4	180.00
7. Pallet dolly		45.00	4	180.00
8.Push Back				250.00
9.Security man power		70.00	1H	70.00
10. Flight planning				170.00
			Subtotal	12,040.00
			VAT 9%	1,084.00
			Grand Total (USD)	**13,124.00**

PREPARED BY:
FARSHID GHOMSHEI
ACCOUNTANT

CONCURRED BY:
S.A.KHALIFELOO
MANAGER, ACCOUNTS

تصویر ۳، سند لو رفته توسط هوشیاران وطن، صورتحساب شرکت سفیران به تاریخ ۱۵ آوریل ۲۰۲۳ که حمل بارها را «خطرناک» توصیف کرده است.

طریق پول‌شویی بتواند تحریم‌های بین‌المللی را دور بزند. این شرکت به مشتریان خود به طور اکید سفارش کرده که در تراکنش‌های مالی خود به هیچ‌وجه از نام شرکت استفاده نکنند تا از عواقب قانونی دور زدن تحریم‌ها در امان بمانند. اسناد لو رفته همچنین نشان می‌دهد میان این شرکت و نهادهای روسی بر سر پرداخت وجوه، مجادلاتی صورت گرفته است. هوشیاران وطن ادعا دارد که درآمد حاصل از این خدمات به حساب سپاه واریز می‌شود تا با آن اقلیت‌های اتنیکی را سرکوب کند.

تصویر ۳، سند لو رفته توسط هوشیاران وطن، صورتحساب شرکت سفیران به تاریخ ۱۵ آوریل ۲۰۲۳ که حمل بارها را «خطرناک» توصیف کرده است.
گروه هوشیاران وطن موارد متعددی از افشای معاملات شرکت‌های هواپیمایی دولتی با سپاه پاسداران و واحدهای برون‌مرزیِ آن مثل نیروی قدس را در کارنامه خود دارد.

نتیجه

گروه‌های هکری همچنان علیه نهادهای دولتی ایران به حمله‌های سایبری ادامه می‌دهند و ادعا دارند که عملیات آنها در همبستگی با معترضان ایران انجام می‌شود. اما برخی از وقایع اخیر، از جمله یورش به قرارگاه سازمان مجاهدین خلق در آلبانی، نشانه‌ی آن است که بعضی از این گروه‌ها احتمالا خاستگاه و ارتباطات دیگری دارند. باید منتظر بود تا معلوم شود دولت آلبانی در پایان تحقیقاتش راجع به عملیات سایبری مجاهدین، چه نوع شواهدی ارایه خواهد داد. در مورد سایر گروه‌ها هم از جمله «بلک ریوارد»، همین ابهام‌ها وجود دارد.

تحلیلِ انبوه اسناد لو رفته نشان‌دهنده حساسیت‌ها و ارجحیت‌های در هم تنیده جمهوری اسلامی در خصوص طیفی از مسایل اجتماعی، سیاسی، تکنولوژیک و سیاست خارجی است و نیز گسترش فعالیت‌های سپاه در حیطه حکمرانی، همراه با طرح‌های جاه‌طلبانه برای وسعت بخشیدن بیشتر این فعالیت‌ها.

اسناد فاش شده همچنین حاکی از نبردی است میان ناراضیان ایرانی و سمپات‌های (ظاهری) آنها در میان گروه‌های هکری از یک سو، و جمهوری اسلامی از سوی دیگر. در یک مبارزه نابرابر برای رسیدن به عدالت، معترضان از جانب هکرها حمایت می‌شوند؛ همان هکرهایی که احتمالا اهداف سیاسی خود را هم دارند. در نتیجه، میدانی از تعارض شکل گرفته که مدام شخصیت‌های تازه به آن گام می‌گذارند و شواهد بیشتری از فساد و سرکوب دولتی را افشا می‌کنند. در این میدان، گروه‌های هکری - و حامیان احتمالی آنها- تاکتیک‌های خود رژیم را همچون سلاح علیه آن به کار می‌گیرند.