جرایم کامپیوتری در ایران

رفتارهای اینترنتی مخاطره آمیز

گزارش کشوری

۲۰۱۵

آرتیکل ۱۹

Free Word Centre

60 Farringdon Road

London,

EC1R 3GA

United Kingdom

تلفن 2500 7324 20 44+

فاکس 0566 7490 20 44+

ایمیل info@article19.org

وب‌سایت www.article19.org

توئیتر @article19org

فیس‌بوک facebook.com/article19org

شابک 978-1-910793-17-6

فهرست

فهرست اصطلاحات و کلمات اختصاری

فهرست اصطلاحات و کلمات اختصاری

بی‌سی‌سی (رونوشت کاربنی ناپیدا): یکی از سه بخشی که حاوی فهرست دریافت‌کنندگان در هدر یک ایمیل است و در مواردی بکار می‌رود که ایمیل به دریافت کنندگانی خاص فرستاده می‌شود که وجود و هویتشان از دیگر دریافت کنندگان ذکر شده در بخش‌های "به" (گیرنده) و "سی سی" (رونوشت کاربنی) پنهان می‌ماند.

رمزنگاری (انکریپشن): رمزنگاری، عملی که با تبدیل اطلاعات به یک فرمت غیرقابل خواندن، از آن اطلاعات حفاظت می‌شود. رمزنگاری پیام‌ها روندی است که به این وسیله فقط طرفین مجاز قادر به خواندن پیام‌ها و یا اطلاعات خواهند بود.

فتا: پلیس سایبری ایران.

نمودار جستجو (گراف سرچ): یک موتور جستجوگر که با نمودارهای اجتماعی فیس‌بوک در هم ادغام شده است و با پردازش پرسش‌های زبان طبیعی، اطلاعاتی از شبکه‌های اجتماعی دوستان و آشنایان کاربر و غیره را به او باز می‌گرداند.

هویت بین المللی دستگاه تلفن همراه یا شماره سریالی (IMEI): شماره خاصی که برای شناسایی هر دستگاه تلفن همراه بکار می‌رود. هر تلفن همراه یک شماره هویت بین‌المللی خاص دارد که همیشه قابل ردیابی است.

آی‌اس‌پی: شرکت خدمات اینترنتی: آی‌اس‌پی شرکتی است که معمولاً در ازای دریافت پول، دسترسی به اینترنت را امکان‌پذیر می‌سازد.

فیشینگ: تلاش برای کسب اطلاعات حساس، مثل نام کاربری رمز عبور ، از طریق پهنان شدن پشت نام یک نهاد قابل اعتماد در ارتباطات الکترونیکی.

گرداب: فرماندهی پدافند سایبری سپاه پاسداران انقلاب اسلامی.

سیم کارت: یا ماژول شناساننده مشترک، کارتی هوشمند است که برای مشترکین تلفن‌های همراه در شبکه‌های GSM اطلاعات ذخیره می‌کند. این اطلاعات می‌تواند شامل هویت کاربر، محل و شماره تلفن او، کلیدهای امنیتی شخصی، فهرست تماس و پیامک‌های ذخیره شده باشد.

جاسوس افزار (اسپای ور): نرم‌افزاری که از طریق آن یک کاربر می‌تواند اطلاعات مخفی درباره فعالیت‌های کامپیوتر یک شخص دیگر بدست آورد. این کار با انتقال مخفیانه اطلاعات از هارد دیسک او میسر می‌شود.

صدا روی پروتکل اینترنت VoIP: یک روش و آندسته از فناوری‌هایی که برای انتقال ارتباطات صوتی و جلسات چندرسانه‌ای روی شبکه‌های پروتکل اینترنت(IP) ، مثل اینترنت، است.

شبکه خصوصی مجازی (وی‌پی‌ان): یک گروه کامپیوتر (یا شبکه‌های مجزا) که از طریق یک شبکه عمومی- عمدتاً اینترنت- به یکدیگر مرتبط می‌شوند. وی‌پی‌ان‌ها به عنوان ابزارهای اساسی کاربران اینترنت در ایران برای دور زدن و گریز از سیستم فیلترینگ این کشور شکل گرفت.

بدافزار (مال ور): بدافزار برنامه‌های رایانه‌ای هستند که معمولاً کاربر را آزار می‌دهند یا خسارتی بوجود می‌آورند.

شنود: شنود به معنای این است که اشخاص یا ارگان اطلاعاتی

ارتباطات شهروندان از قبیل مکالمه‌ها، پیامک‌های نوشتاری و تصویری، ارتباط اینترنتی مورد نظارت و تجسس قرار دهند.

تاریخچه (لاگ): در این متن تاریخچه به فعالیت‌های آنلاین و تلفنی (شامل موبایل) گفته می‌شود.

برنامه مدیریت رمز عبور (پسورد منجر): ابزاری راحت و قدرتمند که تمامی رمزهای عبور کاربر را در یک بانک اطلاعاتی بسیار مطمئن ذخیره و مدیریت می‌کند.

رندوم: بصورت تصادفی، اتفاقی، بدون برنامه ریزی قبلی.

پیش گفتار

پیش‌گفتار

طی دهه‌های متوالی، دولت‌ها از طریق احکام مجوزهای مخابراتی و ضوابط فنی که مردم را ملزم به تحویل اطلاعات تلفن‌های خود به مراکز اجرای قانون می‌کند، به ارتباطات محرمانه عموم مردم دسترسی بدون محدودیت داشته‌اند. اینترنت این توقع تاریخی و هنجار جهانی را ناگهان به چالش کشید. مکالمه‌های مردم، چه عادی و چه ضد حکومت، از کانال‌های ارتباطی محلی به پایگاه‌های خارج از دسترس حکومت‌ها تغییر مکان داده‌اند، به صورتی که معمولاً رمزنگاری شده و دیگر کشورها میزبان این مکالمات هستند. همزمان، دولت‌ها به لحاظ اقتصادی، حداقل به صورت ظاهری هم که شده ملزم به ایجاد ظرفیت‌های ارتباطی شدند، چرا که همان شبکه‌هایی که به زیر سؤال کشیدن عرف‌های تحمیلی حکومت‌ها را تسهیل می‌کردند، خود لازمه پیشرفت‌های مدرن و کسب و کار بین المللی شده بودند.

ساز و کار مبارزه با "جنگ نرم[1]" که فراتر از سانسور علنی و آشکار می‌رود، به شکل "فرماندهی پدافند سایبری سپاه پاسداران" و "پلیس سایبری ایران" نسبتاً دیر در ایران تأسیس شد. دستگاه امنیتی کوشیده است تا اهمیت خود را در این زمینه اثبات کرده و با پیگرد قانونی تقلب‌های دیجیتالی در داخل کشور و در عین حال جنگ سایبری در خارج از کشور به شکلی کارآمد عمل کند. دستگیری کنشگران اینترنتی به طرز فزاینده‌ای با اعترافات تلویزیونی و همچنین اظهارات

---

۱ اصطلاحی که سید علی خامنه‌ای، رهبر جمهوری اسلامی ایران، ساخت تا جنگ مداوم دیجیتالی غرب علیه ایرانیان استفاده کند.

مقامات همراه است، از جمله این که: "کسانی که گمان می‌کنند این فضا برای آنها امن است، باید به فعالیت‌های خود خاتمه دهند" (فوریه ۲۰۱۵)، یا "مردم باید بدانند که ما می‌توانیم پیام‌های آنان را بخوانیم" (سپتامبر ۲۰۱۴) و یا "ما قطعاً این افراد را شناسایی و با آنها مقابله خواهیم کرد" (مه ۲۰۱۴). حکومت از طریق این ادعاهای مبهم و اغراق آمیز به دنبال آن بوده است که کاربران اعتماد خود را نسبت به حریم خصوصی خود در فضای اینترنتی از دست دهند. زمانی که کاربران اینترنت بر این باور باشند که به رغم تمام اقدام‌های احتیاطی، مقامات قادر خواهند بود ارتباطات و مکالمه‌های آنان را شنود کنند، به همان رفتارهایی که خارج از فضای اینترنت دارند، یعنی خودسانسوری و شیوه‌های منفعلانه امنیتی، روی می‌آورند.

لفاظی با واقعیت تفاوتی بسیار دارد. در نتیجه استفاده از فناوری‌های اطلاعاتی، سازمان‌های امنیتی در سراسر دنیا با مانع مواجه یا اغلب به حاشیه رانده شده‌اند. اگر رمزنگاری‌ها و ابزار قوی در زمینه حریم خصوصی علیه سازمان‌های اطلاعاتی آمریکایی و اروپایی مؤثر واقع شده‌اند، بدون تردید فراتر از دسترس دستگاه‌های نظارتی ایران نیز هستند. نیروهای امنیتی که مورد تهدید قرار گرفته و قدرت خود را از دست داده‌اند در پی آن بوده‌اند که از طریق به نمایش گذاشتن قدرت خود که شباهت چندانی به امکانات واقعی آنان ندارد، کنترل خود را بر ارتباطات مدرن اعمال کنند. همانگونه که مطالعات موردی در این گزارش نشان می‌دهد، این ادعاهای گزاف حاصل عقده حقارت دیوان سالاری و مملو از رقابت‌های داخلی و نبود مهارت‌های تکنولوژیکی است. هر حکومتی که قادر به نظارت موفقیت‌آمیز محتوای ارتباطات اینترنتی است، نفع چندانی در ابراز توانایی‌های خود به شیوه‌های تهاجمی و علنی که مقامات ایرانی بکار می‌گیرند ندارد. بلکه چنین حکومت‌هایی بایستی به اندازه کافی انگیزه و مشوق داشته باشند که

در سکوت به جمع آوری اطلاعات مورد نظر خود بپردازند.

از آنجا که مقامات به هیچ وجه دانای کل نیستند، اساساً متکی به این هستند که کاربران هنگام ارتباط و حفظ اطلاعات شخصی اقدامات احتیاطی لازم را انجام نمی‌دهند. مقامات و وابستگان آنها به جای حمله به نقاط ضعف در رمزنویسی یا سوءاستفاده از آسیب‌پذیری‌های زیربنایی، معمولاً از سرشت اساسی انسان‌ها بهره‌برداری می‌کنند. یک موضوع مکرر در روایت‌های زیر دیده می‌شود: غرور کاربران شبکه‌های اجتماعی آنان را تشویق می‌کند تا خود را معرفی کنند، از امیال جنسی کاربران استفاده می‌شود تا با نرم افزارهای جاسوس افزار (اسپای ور) به دستگاه‌های آنها نفوذ کنند، و کاهلی کاربران باعث می‌شود تا از دستگاه‌های خود با رمز عبورهای مناسب حفاظت نکنند. هیچگونه روند یادگیری جمعی وجود ندارد: وخامت تصمیم‌های ظاهراً کوچک فقط زمانی درک می‌شوند که اطلاعات شخصی یک فرد علیه خود او در دادگاه استفاده می‌شود. از کوتاهی و قصور یک فرد استفاده می‌شود تا شبکه‌های گسترده‌تر آشنایان او مورد آزار و اذیت قرار بگیرند، و یک بازجویی منجر به ده‌ها دستگیری می‌شود. این افراد به عنوان شواهدی دال بر قدرت مقامات در اینترنت، در معرض نمایش گذاشته می‌شوند تا به این ترتیب حس عدم تقارن اطلاعاتی که مهمترین تدبیر یک حکومت سرکوبگر است ایجاد شود.

این پژوهش، مشاهدات من و دیگر محققان را درباره رفتار اغلب به لحاظ فنی ابتدایی و به لحاظ اجرایی ضعیفی که سازمان‌های امنیتی ایران در کارزار سرکوب مخالفان اینترنتی خود داشته‌اند، بیشتر تأیید می‌کند. طی چندین سال گذشته این اقدام‌های سرکوبگرانه مستند شده‌اند: اقداماتی که در کاربرد بدافزارهای مخرب علیه ایرانیان در جریان‌های پیش از انتخابات و همچنین در حملات به سیستم عامل‌های

بین المللی که میزبان رسانه‌های مستقل فارسی زبان بوده‌اند، دیده شده است. بر اساس این تجربه‌ها، می‌توان شروع به رفع ابهام از عملیات اطلاعاتی کرد و بیشتر به مسائل مشترک درباره رفتار کاربران که هرگز مستقیماً به آن توجه نشده پرداخت. این تحقیق برای نظام زیستی سازمان‌ها، پدیدآورندگان و افراد علاقمند به امنیت دیجیتال و آزادی اینترنت در ایران، آماری از شکست‌های روشمند است که هم توضیح می‌دهد چرا تمرکز صرف بر ابزار کافی نیست و هم روشنگر محدودیت‌هایی است که با آن مواجه می‌شویم. علاوه بر این، این تحقیق به طرز نگران کننده‌ای حاکی از آن است که بی کفایتی حکومت ناشی از موضوعاتی قابل حل است، و اینکه مقامات همزمان با رشد جامعه مدنی، از رویکردهای پیشرفته‌تر نظارتی استفاده خواهند کرد.

به رغم سرمایه‌گذاری در نرم‌افزارهای ارتباطی و ساختار زیربنایی امن، کاربران همچنان تصمیم‌هایی می‌گیرند که به لحاظ حفظ حریم خصوصی منطقی نیستند، و این موضوع به این دلیل است که یا به نحوی مشوق و انگیزه آنها برای گرفتن چنین تصمیمات نادرستی بسیار زیاد است، و یا درک آنها از خطرات موجود با انتظارات ما متفاوت است. افزون بر این، باید اذعان کنیم که تناسبی بین الزامات ناشی از آموزش و فناوری که برعهده کاربرانِ در معرض تهدید است، با رفتارهای اینترنتی عادی وجود ندارد، و حتی کاربران به لحاظ تکنولوژیکی آگاه و ماهر در خارج از ایران یا کسانی که ادعای تخصص در مسائل امنیتی دارند هم معمولاً از چنین شیوه‌هایی استفاده نمی‌کنند، و غالباً با موانعی از سوی خود سیستم عامل‌ها مواجه می‌شوند. ما مرتب افرادی را می‌بینیم که در معرض خطر قرار می‌گیرند و به دلایل قابل پیشگیری دستگیر می‌شوند و آنچه برای آنها اتفاق می‌افتد گواهی است بر اینکه رسانه‌های مستقل، جوامع اقلیت‌ها، مخالفان سیاسی و

کنشگران اجتماعی همچنان به خاطر فعالیت‌های اینترنتی خود تحت پیگرد قانونی قرار خواهند گرفت.

بدون یک تحقیق متکی به حقیقت، روایت‌های غیرواقعی و تضعیف کننده‌ای که دست اندرکاران کوته فکر به رواج آن می‌پردازند، درک مردم را از اینترنت به عنوان یک فضای امن برای صداهای به حاشیه رانده شده تهدید می‌کند. این تحقیق را اگر با توجه به این مسئله بررسی کنیم، به بینشی نامعمول و کمیاب درباره چگونگی تلاش دولت‌ها برای سرکوب مخالفان خود در اینترنت دست می‌یابیم. این تحقیق نشانگر تأثیرات رعایت نکردن نکات ایمنی از سوی کاربران و همچنین محدودیت تلاش‌های امنیتی است. از منظری خوش بینانه، این تحقیق هم گواهی مهم بر محدودیت‌های حکومت است و هم نشانگر قدرت افراد در حمایت از حقوق بشر بنیادین خود به شکلی بی سابقه است.

کالین اندرسن

مقدمه

مقدمه

"اگر به خاطر آن اطلاعاتی (متن، عکس، یادداشت و اَپ‌های باز) که پس از دستگیری روی تلفنم پیدا کردند نبود، مقامات هیچ مدرک سفت و سختی برای محکوم کردن من نداشتند."[1]

در حال حاضر چه ارتباطی میان رفتار آنلاین و آفلاین شهروندان ایران و احتمال دستگیری آنها در ایران وجود دارد؟ این گزارش به طور اخص پاسخی به این پرسش است.

اینترنت در سال ۱۹۹۳ در ایران آغاز به کار کرد و طی سال‌ها مرتباً تعداد فزاینده‌ای از کاربران را به خود جذب کرده است. بین سال‌های ۲۰۰۱ و ۲۰۰۹- سال انتخابات ریاست جمهوری مورد مناقشه- استفاده از اینترنت هر سال حدود نیم برابر افزایش یافت. در سال ۲۰۱۴، تعداد کاربران اینترنت در ایران بیش از ۲۲ میلیون نفر، افزون بر ۲۸ درصد جمعیت کشور، تخمین زده شده است.

در دهه ۱۹۹۰ و اوایل دهه ۲۰۰۰، دسترسی به اینترنت هزینه بالایی در بر داشت و عمدتاً یکی از امکانات تجملی تلقی می‌شد. اما با افزایش محبوبیت اینترنت، قیمت آن هم مناسب تر شد و نقش اینترنت در زندگی روزمره ایرانیان به تدریج شکل گرفت.

---

۱ مصاحبه با آرتیکل ۱۹

در سپتامبر ۲۰۰۱، حسین درخشان- روزنامه نگار جوان ایرانی- یکی از اولین وبلاگ‌های منتقد حکومت را به زبان فارسی به راه انداخت. یکی از خوانندگان کنجکاو او را تشویق به نوشتن یک راهنمای ابتدایی وبلاگ نویسی کرد که به ایرانیان داخل کشور کمک کرد تا برای بیان عقاید خود، روز به روز بیشتر به اینترنت روی آورند و به این ترتیب وبلاگستان فارسی شکل گرفت. در آن زمان، وبلاگستان فارسی یکی از بزرگترین و فعالترین وبلاگستان‌های جهان بود و مقامات ایرانی را که تا آن زمان بدون رقیب انحصار کامل اطلاعات را در اختیار داشتند، دچار چالشی جدی کرد. عباس معروفی، نویسنده و وبلاگ نویس معروف ایرانی، استفاده از این تریبون نویافته را برای آزادی بیان و نظرپردازی اینگونه توصیف کرد:

"پیام‌هایی در بطری‌های سپرده به باد."

دولت با آغاز اقدامات سرکوبگرانه که به شدت آزادی بیان و اطلاعات را برای وبلاگ نویسان محدود می کرد، به سرعت و با قدرت به این جریان واکنش نشان داد: همان سالی که وبلاگستان ایران به راه افتاد، علی خامنه‌ای، رهبر کشور، حکم داد که فقط نهادهای مجاز حکومتی به وب دسترسی داشته باشند.

علاوه بر این، از سال ۲۰۰۱ شورای عالی انقلاب فرهنگی شروع به اجرای مجموعه‌ای از مقررات کرد که بر اساس آن، شرکت‌های خدمات اینترنتی (آی‌اس‌پی‌ها) موظف به نصب سیستم‌های فیلتر کردن سایت‌ها، شنود و ثبت فعالیت‌های اینترنتی مشتریان و همچنین برداشتن تمام وبسایت‌های ضد دولتی و ضد اسلامی از سرورهای خود شدند[1].

---

۱ http://www.Iranhrdc.org/English/English/publications/reports/3157-ctrl-alt-delete-iran-039-s-response-to-the-internet.html?p=1

این اقدامات سرکوبگرانه مداوم در سال ۲۰۰۸، درست پیش از انتخابات ریاست جمهوری ۲۰۰۹ به اوج خود رسید و بسیاری از وبلاگ‌نویسان را وادار کرد تا از شیوه‌های دیگر تبادل اطلاعات، از جمله پایگاه‌های شبکه‌های اجتماعی جدید، استفاده کنند[۱]. همان سال مقامات با فیلتر کردن اینترنت و دست زدن به اقدامات قانونی هدفمند به این مسئله واکنش نشان دادند.

در دسامبر ۲۰۰۸، امیدرضا میرصیافی[۲] متهم شد که در وبلاگ‌های خود به رهبران مذهبی اهانت کرده و به اشاعه تبلیغات علیه جمهوری اسلامی ایران پرداخته است و متعاقباً به دو سال و شش ماه زندان محکوم شد. او در ۱۸ مارس ۲۰۰۹ جان خود را در زندان از دست داد. میرصیافی اولین وبلاگ‌نویسی بود که در زندان جان سپرد. او به رغم مشکلات جسمی و روحی و همچنین درخواست کارمندان درمانگاه زندان، تحت درمان پزشکی خارج از زندان قرار نگرفت.

استفاده مخالفان حکومت از شبکه‌های اجتماعی، بویژه طی انتخاباتِ به شدت بحث برانگیز ریاست جمهوری در سال ۲۰۰۹ واضح و آشکار بود. کاربران شبکه‌های اجتماعی، موسوم به "شهروند-روزنامه نگار"، نقشی اساسی در سازماندهی و هماهنگ سازی اعتراضات ایفا کردند؛ فیلم‌های ویدیویی و عکس‌های غیرحرفه‌ای فوراً در اینترنت آپلود می‌شدند. تجمع‌های مردم هم عقیده از طریق ابزاری چون فیس بوک و توییتر آسانتر و در مدت زمانی کوتاه میسر می‌شد[۳]. اما نه تنها کنشگران ، بلکه مقامات ایرانی هم متوجه ظرفیت شبکه‌های اجتماعی به عنوان ابزاری برای بسیج‌های اجتماعی-سیاسی شده بودند.

---

۱ مثل فیس بوک و توییتر

۲ http://www.theguardian.com/world/2009/mar/20/omidreza-mirsayafi-iran-blogger-rouznegar

۳ http://news.bbc.co.uk/1/hi/world/middle_east/8099579.stm

از آن زمان به بعد، حکومت ایران جنگی مستمر علیه اینترنت به راه انداخته تا قابلیت‌های آن را برای تسهیل جنبش‌های اعتراضی محدود سازد. این جنگ به شکل قوانین، سیاست‌ها و اقدام‌های جدید درآمده است که همچنان طبق معیارهای جهانی حقوق بشر، خارج از محدودیت‌های مجاز آزادی بیان و اطلاعات قرار می‌گیرد[1]. سانسور اینترنت و نظارت بر آن به یک اولویت عمده تبدیل شده است. این نظارت تام از طریق تعدادی از برنامه‌های نظارتی دولت که به منظور اعمال نظارت بر ارتباطات اینترنتی طرح شده‌اند، شدت یافته است.

فعالیت‌های سایبری که با قواعد حکومت در تضاد قرار می‌گیرد، غیرقانونی اعلام شده که این نقض معیارهای جهانی است. در عین حال، توانایی‌های فنی مقامات بیشتر شده تا به طرز پیشرفته تر و جامع تری جلوی این فعالیت‌ها گرفته شود. در ژانویه ۲۰۱۰، قانون جرایم رایانه‌ای وضع شد که در قالب الفاظی مبهم، "اشاعه دروغ" یا انتشار مطالبی که به ضرر "اخلاق عمومی" بود را تخطی از قانون قلمداد می‌کرد[2]. یک سال بعد، پلیس سایبری ایران (فتا) تأسیس شد. نهادهای ایرانی سرکوبگر اینترنت، موسوم به "یگان‌های سایبری"، مثل "فرماندهی پدافند سایبری سپاه پاسداران انقلاب اسلامی (گرداب)" با حمایت مالی سپاه پاسداران ایران تأسیس شدند. در خبرها، گروه‌های دیگری مثل "ارتش سایبری ایران" هم به چشم می‌خورد، بویژه در فوریه ۲۰۱۱ زمانی که بنا بر گزارش‌های رسیده، رسانه‌های صدای

---

۱ در سال ۲۰۱۳ به دست اندرکاران و سیاستگزاران حکومت توصیه‌هایی مبنی بر چگونگی ترویج و حمایت از حقوق وبلاگ نویسان در داخل و خارج از کشور ارائه شد: «آرتیکل ۱۹، حق داشتن وبلاگ، ۲۰۱۳:

http://www.article19.org/data/files/medialibrary/3733/Right-to-Blog-EN-WEB.pdf

۲ آرتیکل ۱۹: جرائم رایانه‌ای در ایران: سرکوب اینترنتی در عمل

آمریکا و بی بی سی را هک کردند[1]. دولت هیچگاه رسماً رابطه خود با آنها را تأیید یا تکذیب نمی‌کند. گروه‌های بخش خصوصی، مانند "آشیانه"، "سیمرغ" و "شبگرد" هم بنا به گزارش‌های رسیده با مقامات کار کرده‌اند. گفته می‌شود که این گروه‌ها مثل "یگان‌های سایبری" که قبلاً به آنها اشاره شد، در نظارت، هک کردن، فرستادن پیام‌های تهدیدآمیز، تولید و بسط محتوا، ترویج فناوری‌های مخصوص ایران مثل سیستم‌ها و مرورگرهای عامل و همچنین فیشینگ دست داشته است.

مقامات ایران سرمایه گذاری سنگینی در پیشبرد توانایی‌های اجرایی، حقوقی و تدارکاتی خود کرده‌اند تا آزادی بیان و اطلاعات را به دلیل آنچه که آنها تهدیدات مربوط به فناوری‌های ارتباطی تلقی می‌کنند، محدود سازند. در مارس ۲۰۱۲، رهبر ایران، آیت الله خامنه‌ای، شورای عالی فضای مجازی را- که یک ارگان سیاست گذاری متشکل از اعضایی چون رئیس جمهور ایران، رئیس قوه قضاییه، وزیر اطلاعات، وزیر فرهنگ و دیگر مقامات مجری قانون- بنیان نهاد تا استفاده از اینترنت در ایران را زیر نظر بگیرد[2]. این شورا فقط یکی از گروه‌های نظارتی است که هدفشان محدودسازی دسترسی آزاد به اینترنت است[3]. یکی دیگر از این گروه‌ها، کمیته تعیین مصادیق محتوای مجرمانه است که سایت‌هایی را که محتوای غیرقانونی دارند شناسایی کرده و مسئول اخذ تصمیم نهایی در مورد مسدود شدن یا نشدن آنها به علت محتوایشان است.

تسلط مقامات ایران بر فضای اینترنت این کشور به طرزی گسترده

---

۱ همان منبع

۲ همان منبع

۳ همان منبع

گـزارش[1] شـده اسـت[2]. در مـورد تعـداد بـی شـمار کاربـران اینترنـت کـه دسـتگیر شـده یـا همچنـان دسـتگیر می‌شـوند هـم گزارش‌هـای بسـیاری در دسـت است[3].

بهبود بخشیدن به امنیت فضای دیجیتالی در ایران

سـازمان آرتیـکل ۱۹ (Article 19) گزارش‌هایـی در سـال‌های ۲۰۱۲[4] و ۲۰۱۳[5] منتشـر کـرده کـه در آن محتـوای قانـون جرایـم رایانـه‌ای سـال ۲۰۱۰ ایـران و تأثیـرات آن بـر جامعـه اینترنتـی آن کشـور را مـورد تحلیـل قـرار داده اسـت. سـازمان آرتیـکل ۱۹ بـا تشـریح ایـن قانـون و مسـتند کـردن شـهادت قربانیـان آن، توصیه‌هایـی خطـاب بـه دسـت انـدرکاران، از متخصصـان فنـی و شـرکت‌های خصوصـی گرفتـه تـا دولـت ایـران، ارائـه داده تـا از حـق آزادی بیـان در ایـران حمایـت و آن را عملـی کنـد.

هنـوز بـه دشـواری می‌تـوان تعییـن کـرد کـه جامعـه اینترنتـی ایـران پیشـرفت محسوسـی در زمینـه حفاظـت از امنیـت دیجیتالـی خـود داشـته یـا نداشـته اسـت. گـزارش سـوم در ایـن مـورد بـه قصـد پـر کـردن ایـن خـلاء تهیـه شـده اسـت. ایـن گـزارش در پـی آن اسـت کـه تعییـن کنـد کاربـران اینترنـت در ایـران چـه پیشـرفتی -اگـر پیشـرفتی حاصـل شـده- در زمینـه حفـظ امنیـت دیجیتالـی خـود داشـته‌اند، و همچنیـن حوزه‌هایـی کـه نیـاز بـه

---

۱ https://globalvoicesonline.org/2015/03/23/internet-in-iran-evaluating-rouhanis-first-two-years-as-president

۲ https://cpj.org/reports/2012/05/10-most-censored-countries.php

۳ http://www.iranhumanrights.org/2015/03/facebook-users-arrested

۴ ایران: قانون جرائم رایانه‌ای (۲۰۱۲)
http://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB[4].pdf

۵ جرائم رایانه‌ای در ایران: سرکوب اینترنتی در عمل (۲۰۱۳)
http://www.article19.org/data/files/medialibrary/37385/Computer-Crimes-in-Iran-.pdf

تغییرات بیشتر رفتاری و فنی دارند کدامند.

این گزارش به منظور تحقق هدف خود بر پرسش‌های زیر تأکید می‌کند:

- مقامات ایران از کاربران اینترنت در این کشور چه اطلاعاتی در دست دارند؟
- آنها این اطلاعات را از چه طریق کسب کرده‌اند؟
- آنها در پی چه اطلاعات دیگری هستند؟
- آنها از چه شیوه‌هایی برای کسب اطلاعات بیشتر استفاده می کنند ؟

با تحلیل این یافته‌ها می‌توان روشن ساخت که کدام رفتارهای آنلاین و آفلاین منجر به افزایش میزان دستگیری‌ها می‌شود، و پاسخ به این پرسش به نوبه خود می‌تواند روشنگر بینشی مهم درباره این مسئله باشد که مقامات ایران چگونه اینترنت را شنود و بر آن نظارت می‌کنند. در پایان، این گزارش حاوی توصیه‌هایی مبنی بر این است که چه تغییرات رفتاری، برنامه‌های احتمالی و کمک‌های فنی لازم است، و اینکه چه حوزه‌هایی به تحقیقات بیشتر نیاز دارد.

روش شناسی

روش‌شناسی

هدف این گزارش آن است که ارتباط میان رفتار آنلاین و آفلاین کنشگران اینترنتی در ایران با احتمال دستگیری آنان در حال حاضر را بررسی کند. این گزارش راه‌هایی را توصیه می‌کند که از طریق آن بتوان خطر دستگیری این افراد را به میزان قابل ملاحظه‌ای کاهش داد.

اولین گام، شناسایی و مصاحبه با گروهی از افراد گوناگون بود که به دلیل فعالیت‌های آنلاین و آفلاین خود از سوی مقامات ایران مورد هدف قرار گرفته بودند. افرادی برای این بررسی واجد شرایط شناخته شدند که به دلیل فعالیت‌های اینترنتی خود تحت پیگرد قانونی قرار گرفته بودند. این شامل کسانی می‌شد که به علت‌های دیگر نیز دستگیر شده بودند، اما حضور آنان در اینترنت یکی از عوامل اصلی بازداشتشان به شمار می‌رفت. در مجموع، به منظور تهیه این گزارش اطلاعات ۲۵ پاسخ دهنده انتخاب و تحلیل شد.

این گروه متشکل از روزنامه نگاران، کنشگران حقوقی، افراد فعال در احزاب سیاسی زیرزمینی، اعضای گروه‌ها و اتحادیه‌های دانشجویی، کنشگران حقوق اقلیت‌ها و شهروندانی بود که از تریبون‌های شبکه‌های اجتماعی برای در میان گذاشتن عقاید خود با مخاطبان بیشتر استفاده می‌کردند. ترکیبی از کنشگران سرشناس و همچنین کمتر شناخته شده انتخاب شد تا بتوان تا حد امکان به یک ارزیابی متنوع از رفتار و عادات اینترنتی این افراد پی برد. این کار با دو هدف انجام شد: اول اینکه ببینیم آیا تفاوتی بین نظارت بر کنشگران سرشناس و کمتر شناخته

شـده وجـود دارد و دوم اینکـه ایـن تفـاوت خـود را چگونـه نشـان می‌دهـد.

بـه خاطـر حفـظ موضعـی بـی طرفانـه و غیرمتمرکـز، کسـانی کـه در شـهرهای کوچـک زندگـی می‌کردنـد بیشـتر از افـراد سـاکن تهـران مـورد توجـه قـرار گرفتنـد. هـدف از ایـن کار همچنیـن تشـویق بـه انجـام تحقیقـات بیشـتر در آینـده در مناطقـی خـارج از پایتخـت ایـران بـود کـه اغلـب در چنیـن مـواردی کمتـر در معـرض دیـد قـرار می‌گیرنـد.

در خاتمـه، ایـن مسـئله هـم مـورد توجـه قـرار گرفـت کـه مصاحبه‌هـا بـا مجموعـه ای متعـادل از افـرادی بـا سـنین، جنسـیت، تخصـص فنـی و جایـگاه اجتماعی-اقتصـادی متفـاوت صـورت پذیـرد.

مصاحبه‌هـا- و جمـع آوری بعـدی اطلاعـات- بـا تأکیـد بسـیار بـر مقـررات حریـم خصوصـی انجـام شـد تـا اسـامی پاسـخ دهنـدگان محفـوظ بمانـد. بعـلاوه، هـر گونـه اطلاعـات یـا جزئیـات شـخصی کـه امـکان داشـت امنیـت مصاحبـه شـوندگان را بـه خطـر بینـدازد از ایـن پژوهـش کنـار گذاشـته شـد. صـرف نظـر از چنیـن اقدامـات ایمنـی، اطلاعـات اسـتفاده شـده در ایـن پژوهـش بـدون تغییـر باقـی می‌مانـد.

از روش شناسـی تحقیقـی کیفـی اسـتفاده شـده تـا باورهـا، احساسـات، عقایـد، تجـارب و رفتارهـای پاسـخ دهنـدگان معیـن گـردد.

مصاحبـه کننـده از یـک فهرسـت مشـخص سـؤال اسـتفاده می‌کـرد، امـا سـاختار مصاحبـه بـه نحـوی بـود کـه در صـورت لـزوم پرسـش‌های خودانگیختـه و مربـوط بـه موضـوع هـم مطـرح شـود. پرسـش‌ها بـرای تعییـن مسـائل زیـر طراحـی شـده بودنـد: اول از همـه، اشـتباهات نوعـی کـه امنیـت اینترنتـی پاسـخ دهنـدگان را بـه خطـر انداختـه بـود؛ دوم، رایـج تریـن انـواع اطلاعاتـی کـه مقامـات بـه دنبـال آن بودنـد؛ و آخـر از همـه، روش‌هـای مـورد اسـتفاده بـرای اخـذ ایـن اطلاعـات. افـزون بـر ایـن، هـدف از طـرح پرسـش‌ها یافتـن ارتبـاط میـان کنشـگری آنلایـن و آفلایـن بـود. فهرسـت

کامـل ایـن پرسـش‌ها را در ضمیمـه یـک می‌تـوان یافـت.

اطلاعـات گـردآوری شـده بـه لحـاظ آمـاری تحلیـل و پاسـخ‌ها بـه رمـز درآورده شـد: حاصـل ایـن پژوهـش در فصـل بعـدی شـرح داده شـده اسـت.

یافته‌ها

یافته‌ها

رفع مسئولیت

این گزارش مستند با حسن نیت و بر اساس اطلاعات کسب شده از طریق مصاحبه‌های مفصل و دقیق محقق تهیه شده است. همانگونه که در "روش شناسی" (قسمت بالا) عنوان شد، یافته‌های این تحقیق به طور مشخص از اطلاعات جمع آوری شده از پاسخ دهندگان شرکت کننده در این تحقیق گرفته شده و جزئیات مربوط به آنها به دلایل امنیتی محرمانه می‌ماند. حقایق بیان شده در این تحقیق و نتیجه گیری‌های حاصل از آنها از منابعی قابل اعتماد به دست آمده‌اند، اما آرتیکل ۱۹ یا هیچ یک از اعضای وابسته به آن، هیچ گونه مسئولیتی درباره کامل بودن یا دقت آنها برعهده ندارند. در برخی موارد، آرتیکل ۱۹ مدارک این اظهارات را به دلیل آنکه امنیت پاسخ دهندگان را به خطر می‌اندازد منتشر نکرده است.

چگونه مقامات پیش از دستگیری افراد به جمع آوری اطلاعات می‌پردازند

بر اساس گفته‌های پاسخ دهندگان، دو نهاد اصلی که مسئول دستگیری‌ها و نظارت هستند عبارتند از: وزارت اطلاعات و سپاه پاسداران انقلاب اسلامی ایران. گفته می‌شود که وزارت اطلاعات بیشتر از شیوه‌های سنتی شنود و تجسس، مانند شنودخطوط تلفن ثابت، تلفن‌های همراه، محل‌های مسکونی، مکان‌های گردهم آیی یا

ادارات استفاده می‌کند و سپاه پاسداران از طریق تولید محتوا، عملیات نفوذی[1] و فیشینگ روش‌های پیشرفته تر نظارت را بکار می‌برد.

سپاه پاسداران انقلاب اسلامی ایران با تعداد بیشتر دستگیری‌ها و شیوه‌های خشونت آمیزتر معمولاً رفتاری تهاجمی تر از وزارت اطلاعات دارد[2]. اکثر نظارت‌ها و دستگیری‌های مربوط به اقلیت‌های نژادی و مذهبی و انتقاد از خامنه‌ای، رهبر ایران، به عهده سپاه پاسداران است.

تلفن‌های همراه

کنشگرانی که از ارسال پیامک و / یا تلفن برای بسیج دیگران یا سازماندهی محل ملاقات گروهی استفاده کرده‌اند بیشتر آسیب پذیر بوده‌اند. بسیاری از پاسخ دهندگان گزارش داده‌اند که تلفن‌های آنها از سوی سپاه پاسداران شنود می‌شده یا سوابق مکالمه‌های آنها طی چندین سال از ۲۰۰۹ تا ۲۰۱۴ مرتباً نظارت شده است. یکی از پاسخ دهندگان که مورد بازجویی قرار گرفته بود به یاد می‌آورد:

> "...من یک اتهام را رد کردم، *[و]* آنها به من تاریخچه پیامک‌هایم را که به دو سال قبل برمی گشت نشان دادند[3]."

ذخیره کردن عکس‌ها، پیامک‌ها، مدارک و انواع دیگر اطلاعات و داده‌ها در تلفن‌های همراه که با آنها می‌توان کسی را متهم کنند نیز خطرناک است. یکی از پاسخ دهندگان می گفت بدون اطلاعاتی

---

۱ به «عملیات نفوذی آنلاین» در زیر مراجعه کنید

۲ مصاحبه شوندگانی که با سپاه پاسداران سر و کار داشته‌اند گفته‌اند که حمله‌های خشونت آمیز به منازل یا ادارات، رفتارهای شدیدتر طی دستگیری یا دوران بازداشت و تهدیدهای تهاجمی تر و استفاده از زبان بی ادبانه و وقیح توسط سپاه صورت گرفته است.

۳ مصاحبه با آرتیکل ۱۹

که پس از دستگیری از تلفن همراهش بدست آوردند، "هیچ مدرک محکمی" برای محکوم کردن او وجود نداشت.

در یک مورد دیگر، با یکی از مصاحبه شوندگان از یک کانال خبری فارسی زبان خارج از کشور به صورت تلفنی تماس گرفته بودند. فقط چند ساعت بعد از آن مکالمه، او برای بازجویی به وزارت اطلاعات احضار شده بود. "آنها تاریخچه مکالمات و تمام پیامک‌هایم را طی شش ماه گذشته نشانم دادند." این موضوع نه تنها نشانگر دامنه شنود تلفنی مقامات است، بلکه حاکی از آگاهی آنها از مکالمات تلفنی است که از سوی بعضی از شبکه‌های خبری مشخص صورت می گیرد.

یکی دیگر از باورهای رایج و اشتباه کنشگران ایرانی این است که می‌توانند با تغییر مستمر سیم کارت، رد پایی از خود به جا نگذارند. اما این درست نیست، چرا که تلفن‌های همراه از طریق شماره سریال[1] (IMEI) ، قطع نظر از سیم کارت استفاده شده قابل ردیابی است و این ناشی از آن است که شرکت نوکیا-زیمنس تجهیزات خاصی ویژه تلفن‌های همراه به مقامات ایران فروخته است[2].

فیشینگ و حمله با نرم افزارهای مخرب

فیشینگ یکی از راهکارهایی است که با هدف بهره برداری از سهل انگاری کنشگران و شهروندان عادی اغلب استفاده می‌شود.

---

۱ از طریق سیم کارت می‌توان شما را شناسایی کرد، اما تلفن همراه نیز می‌تواند شما را به دردسر بیندازد. هر تلفن همراه یک شماره ویژه، تحت عنوان هویت بین المللی دستگاه تلفن همراه یا شماره سریالی (IMEI)، دارد. این شماره تمام مدت قابل ردیابی است.

۲ نوکیا- زیمنس از قانون سرکوب در ایران ابراز تأسف می کنند، بلومبرگ، ۰۳/۰۶/۲۰۱۰. قابل دسترسی در اینترنت:
http://www.businessweek.com/globalbiz/content/jun2010/gb2010063_509207.htm [17.03.2015]

رایج ترین شیوه، استفاده از وعده محتوای سکسی (مثل عکس) است تا قربانی را به کلیک کردن روی یک تصویر وسوسه کنند. به صورت متناوب، به خبرنگاران فایل‌های قابل اجرا (مثل وُرد، پی دی اف یا تصاویر) در لفافه عنوان‌های خبری فوری فرستاده می‌شود. هنگامی که قربانی روی آن مطلب کلیک می کند، نرم افزار مخرب(Malware) دانلود و روی دستگاه او نصب می‌شود. این عمل میکرفن یا دوربین داخلی کامپیوتر را فعال و جاسوس افزار (اسپای ور) را نصب می کند تا اطلاعات کلیدی را به یک کاربر خارجی (از قبیل مقامات) بفرستد، یا یک صفحه ورود به سامانه ایمیل جعلی درست می کند تا رمز عبور قربانی را بدست آورد. این روش آخر ترکیبی از فیشینگ و عملی موسوم به "حمله فردی در میانه" (man-in-the-middle-attack) است که به وسیله آن یک شخص ثالث قادر می‌شود تا مکالمه بین دو نفر را بدون اطلاع آنان شنود کند[1].

عملیات نفوذی آنلاین

عملیات نفوذی گروهی آنلاین یکی از راهکارهای رایجی است که مقامات استفاده می کنند. آنها از شیوه‌های گوناگونی برای تشخیص هویت آفلاین افراد، مانند گردانندگان یا مدیران گروه‌های اینترنتی استفاده می کنند. شیوه‌های مورد استفاده متفاوت است و به سیستم عامل و پایگاه آن بستگی دارد. مثلاً فیس بوک سیستم عاملی است که مقامات اکثراً از آن استفاده کرده‌اند. روش‌هایی که برای جمع آوری اطلاعات و داده‌های شخصی استفاده شده به شرح زیر است:

- درست کردن نام کاربری جعلی به منظور فرستادن درخواست

---

۱ ان. دوپال، حمله فرد میانه، قابل دسترسی در اینترنت:
http://www.veracode.com/security/man-middle-attack (17.03.2015)

دوستی.

- نوشتن نظرات یا پیام‌های تحریک آمیز به منظور گرفتن پاسخ و به دام انداختن فرد در حال مکالمه[1]. این روش به تله انداختن افراد "آژان پرووکاتور" یا "عامل نفوذی" نامیده می‌شود.
- شنودروابط علنی کاربران به منظور شناسایی و مشخص کردن روندها. این عمل شامل استفاده از دیگر اعضای گروه برای جمع آوری اطلاعات راجع به افراد خاص می‌شود.

یکی دیگر از کارهایی که کاربران ایرانی را هنگام ارتباطات اینترنتی آسیب پذیر می‌کند، استفاده نکردن از روش "بی سی سی" (BCC) در ارسال ایمیل‌های انبوه است. این بدین معناست که اسامی افراد و آدرس‌های ایمیل تمام کسانی که در فهرست ایمیل بوده‌اند برای همگان، از جمله افراد غیرقابل اعتماد، قابل رؤیت می‌شود. زمانی که مقامات به این ایمیل‌های انبوه یا پیام‌های گروهی دسترسی پیدا می‌کنند،بدون نیاز به دسترسی به سرور ایمیل‌ها و یا استفاده روشهای پیچیده قادر خواهند بود اسامی افراد و آدرس‌های ایمیل آنها را بدست آورند. این مشکل بویژه در پیام‌های گروهی وایبر و فیس بوک متداول است[2].

هویت تعداد زیادی از مصاحبه شوندگانی که در گزارش ما شرکت

---

۱ شخصی که از نام کاربری تقلبی استفاده کرده مکالمه را آغاز میکند و کمی از جزئیات فردی و شخصی خود را در میان می‌گذارد تا توجه فرد مورد هدف را جلب و اعتماد او را کسب کند. پس از جلب اعتماد، فرد مورد هدف به راحتی جزئیات بیشتری درباره خود در میان می‌گذارد و داوطلبانه هویت و عقاید خود را به خطر می‌اندازد. تعدادی از مدیران گروه‌هایی که طی این تحقیق با آنها مصاحبه شد با این مسئله مواجه شده بودند.

۲ وایبر پرطرفدارترین اَپ پیام رسان فوری در ایران است که دارای قابلیت انتقال صدا روی اینترنت VoIP و رایگان است. فیس بوک هم بسیار پرطرفدار است. برای کسب اطلاعات و آمار بیشتر لطفاً به این صفحه که به زبان فارسی است مراجعه کنید:
http://www.amarestan.com/vdcjfaevzuqeo.sfu.html

داشـتند، هنـگام نفـوذ مقامـات در ایمیل‌هـای انبـوه و پیام‌هـای گروهـی کشـف شـده بـود.

استفاده از اسامی واقعی

تعـداد قابـل ملاحظـه‌ای از پاسـخ دهنـدگان در فضـای مجـازی از اسـامی واقعـی خـود اسـتفاده کـرده بودنـد بـا ایـن بـاور کـه در مقایسـه بـا نـام مسـتعار از تأثیـر و اعتبـار بیشـتری برخـوردار اسـت. انگیـزه دیگر ایـن افراد در اسـتفاده از نـام واقعـی، امیـد بـه شـهرت و محبوبیـت در آینـده بـوده اسـت. ایـن شـیوه نشـانگر آن اسـت کـه ایـن اشـخاص بـه هیـچ وجـه از خطـر دسـتگیری در اثـر چنیـن رفتـاری اطـلاع نداشـته‌اند، چـرا کـه فعالیت‌هـای اینترنتـی آنـان بـه راحتـی توسـط مقامـات قابـل ردیابـی اسـت.

فیس بوک

> "طـی بازجویـی ام متوجـه شـدم کـه تمـام اطلاعاتـی کـه مقامـات ادعـا می کردنـد از مـن بدسـت آورده‌انـد از صفحـه فیـس بـوک مـن یـا[صفحـات] دوسـتانم جمـع آوری شـده کـه در آن مـرا تـگ کـرده بودنـد[1]."

اگـر چـه سـایت فیـس بـوک در ایـران فیلتـر شـده اسـت، امـا تـا کنـون فیـس بـوک پرطرفدارتریـن پایـگاه شـبکه‌های اجتماعـی در ایـران بـوده اسـت، چـرا کـه از طریـق آن نسـبتاً بـه آسـانی می‌تـوان بـا تعـداد بسـیاری از افـراد و گروه‌هـای هـم عقیـده ارتبـاط برقـرار کـرد. افـزون بـر ایـن، فیـس بـوک بـرای وبـلاگ نویسـانی کـه وبلاگشـان را بسـته بودنـد یـا از تعـداد مطلـوب بازدیدکننـده برخـوردار نبودنـد، تریبـون جایگزیـن مناسـبی بـرای بیـان آزادانـه

---

۱ مصاحبه با آرتیکل ۱۹

عقاید خود بوده است.

در حالی که افزایش جریان اطلاعات و ترویج صداها و عقاید متفاوت مزایایی دارد، کاربران ایرانی معمولاً آگاه نیستند که چگونه می‌توان اطلاعاتی را که آنها با میل و رغبت در فیس بوک با دیگران در میان می‌گذارند بر علیه آنان استفاده کرد. مثلاً تنظیمات حریم خصوصی به درستی درک نشده‌اند، یعنی اینکه در میان گذاشتن اطلاعات و تگ کردن دیگران در عکس‌ها می‌توانند نه تنها برای خود کاربران بلکه برای دیگران نیز منجر به مزاحمت‌های قانونی از سوی مقامات شود.

آسیب پذیری‌های مشترکی که در تنظیمات حریم خصوصی فیس بوک به آن اشاره شد، عبارتند از:

- اجازه دادن به اینکه فهرست دوستان برای عموم مردم قابل دیدن باشد.
- توزیع دعوت‌های گروهی به برنامه‌ها و رویدادها.
- تشکیل دادن گروه‌های باز و عمومی که به همه اجازه ورود داده و آنها را قادر به مشاهده جزئیات تمام اعضای گروه و فعالیت‌ها می‌کند.

فیس بوک همچنین اخیراً یک گزینه "گراف سرچ" (یا نمودار جستجو) ایجاد کرده که از طریق آن جزئیات اطلاعات مربوط به فعالیت‌های عمومی یک عضو به سرعت و آسانی قابل دسترس می‌شود.

استفاده از کامپیوترها و چاپگرهای عمومی

بعضی از پاسخ دهندگان گفته‌اند که از طریق ثبت فعالیتشان در

کامپیوترهـا و چاپگرهـای عمومـی در مکان‌هایـی مثـل محیـط دانشـگاه یـا محـل کار شناسـایی شـده‌اند. کامپیوترهـای کافـی نت‌هـا نیـز اطلاعـات شـخصی و داده‌هـای مـرور مشـتریان خـود را ثبـت می‌کننـد[1].

شنود دائمی

بـر اسـاس یافته‌هـای ایـن تحقیـق، فعالیت‌هـای آنلایـن و آفلایـن اقلیت‌هـای نـژادی و مذهبـی (بویـژه بهائیـان و دراویـش) و همچنیـن اعضـای گروهـای سیاسـی سرشـناس بـه صـورت دائـم تحـت شـنود قـرار دارنـد. ایـن امـر بـه قصـد شـنود و سـرکوب آن دسـته از فعالیت‌هـای اعضـای ایـن گروه‌هـا صـورت می‌گیـرد کـه ممکـن اسـت باعـث بـه شناسـایی آنـان بشـود، و اغلـب بـه عهـده واحدهـای ویـژه سـرویس‌های اطلاعاتـی اسـت کـه مختـص نظـارت بـر کنشـگران اقلیت‌هـا هسـتند. شـیوه‌های مـورد اسـتفاده مقامـات شـامل فیلتـر کـردن مسـتمر وبسـایت‌ها و همچنیـن دسـتور دادن بـه دامنه‌هـای میزبـان بـه منظـور حـذف اطلاعـات گروه‌هـای خـاص و توقـف ارائـه خدمـات بـه آنـان اسـت[2].

آی اس پی‌ها و ارتباطات امن

از پاسـخ دهنـدگان دربـاره شـرکت‌های خدمـات اینترنتـی (آی اس پـی)

---

۱ قوانیـن کافه‌هـای مجـازی مقـرر می‌کنـد کـه کافـی نت‌هـا چـه خدماتـی در اختیـار مـردم بگذارنـد، بـه کاربـران اجـازه انتقـال چـه مطالبـی را از طریـق دسـتگاه‌های خـود بدهنـد و همچنیـن ایـن مکان‌هـا را موظـف می‌سـازد کـه هویـت و تاریخچـه مشـتریان خـود را «حداقـل بـه مـدت شـش مـاه» ثبـت و ذخیـره کننـد. گزارشـگر ویـژه سـازمان ملـل در مـورد ایـران در گـزارش سـوم خـود دربـاره وضعیـت حقـوق بشـر در جمهـوری اسـلامی ایـران کـه در ۱۳ سـپتامبر ۲۰۱۲ بـه کمیتـه سـوم مجمـع عمومـی سـازمان ملـل متحـد ارائـه کـرد، بـر ایـن عمـل بـه عنـوان محدودسـازی آزادی بیـان و حـق دسـتیابی بـه اطلاعـات بـرای ایرانیـان تأکیـد کـرد.

۲ خانه آزادی، آزدای در شبکه - ایران:
https://freedomhouse.org/report/freedom-net/2012/iran#.VToNt47F_C8

مورد استفاده آنها سؤال شد تا مشخص شود آیا شرکت‌های مختلف در ایران سیاست‌های متفاوتی در خصوص مشترکین خود بکار می‌برند یا خیر. یافته‌های این پژوهش نشان می‌دهد که شرکت‌های خدمات اینترنتی در ایران معمولاً از اطلاعات شخصی مشترکین خود حفاظت نمی‌کنند. در واقع، شرکت‌های ایرانی به موجب قانون موظف هستند که هر گونه اطلاعاتی که مقامات درباره مشترکین آنها لازم دارند در اختیارشان بگذارند[1]. تمام شرکت‌های خدمات اینترنتی تحت کنترل شدید مقامات و تابع مقررات وضع شده از سوی آنها هستند و از سیاست‌های ملی در خصوص فیلتر کردن و سانسور پیروی می‌کنند[2]. در نتیجه، بعضی از کاربران اینترنت دست به اقداماتی می‌زنند تا به اینترنت دسترسی پیدا کنند بدون آنکه با وبسایت‌های فیلتر و مسدود شده توسط مقامات مواجه شوند، مثل به راه انداختن شبکه‌های مجازی خصوصی یا وی پی ان‌ها. استفاده از وی پی ان به دلیل نصب بسیار ساده آن متداول است. اما قابل اعتماد بودن آنها بعضی اوقات زیر سؤال بوده است؛ یکی از مصاحبه شوندگان بر این باور بود که وی پی ان مورد استفاده او - که آن را در اینترنت خریده بود- ایراد داشته است، و ادعا می‌کرد که مقامات به آن دسترسی داشتند. در بعضی از بازجویی‌ها، مقامات ادعا کرده بودند که اطلاعات خود را مستقیماً از وی پی ان‌های کاربران کسب کرده‌اند. این مسئله چه صحت داشته باشد و چه نداشته باشد، از اعتماد ایرانیان به وی پی ان‌ها کاسته است. ایرانیان همیشه به منبع وی پی ان مورد استفاده خود برای

---

۱ به بررسی قانون جرائم رایانه‌ای که توسط آرتیکل ۱۹ تهیه شده مراجعه کنید:
http://www.article19.org/resources.php/resource/2922/en/iran:-computer-crimes-law

۲ برای کسب اطلاعات بیشتر درباره سیاست‌های ملی در زمینه فیلتر کردن و سانسور و نقش شرکت‌های خدمات اینترنتی به گزارش آرتیکل ۱۹ در خصوص فیلتر کردن اینترنت در ایران (۲۰۰۹) مراجعه کنید:
https://opennet.net/sites/opennet.net/files/ONI_Iran_2009.pdf (15.02.2015)

دستیابی به وبسایت‌های فیلتر شده، مثل فیس بوک، توجه نمی‌کنند. در برخی موارد، مقامات وی پی ان‌های خود را ایجاد می‌کنند تا بتوانند اطلاعات کاربران را به یک مسیر تحت شنود هدایت کنند که همین باعث آسانتر شدن نظارت می‌شود.

روش‌های استفاده شده برای اخذ اطلاعات طی بازداشت و پس از آن

دسترسی فیزیکی به لپ تاپ‌ها و دیگر دستگاه‌ها (مصادره شده)

"همه چیز آنجا بود... همه اطلاعاتی که به من آسیب رساند، حاضر و آماده روی لپ تاپم بود. بدون رمزنگاری و یا رمز عبور[1]."

بررسی لپ تاپ‌ها و دیگر دستگاه‌های مصادره شده، ساده ترین راه برای اخذ اطلاعات از افراد بازداشت شده از سوی مقامات است. بنابر گفته مصاحبه شوندگان، اغلب اتفاق افتاده بود که اطلاعات اضافی جمع آوری شده از کامپیوترهای لپ تاپ مصادره شده آنها، پرونده‌های آنها را پس از بازداشت پیچیده تر و دشوارتر کرده بود. به عنوان مثال، در بسیار از موارد پاسخ دهندگان فقط پس از بازداشت متوجه می‌شدند چقدر اطلاعات حفاظت نشده بر روی دستگاه‌های کامپیوتر خود ذخیره کرده بودند. این موضوع متعاقباً طی روند دادرسی به آنها صدمه رسانده بود. اغلب پاسخ دهندگان اظهار می‌داشتند که اگر به خاطر بررسی دستگاه‌های مصادره شده آنها نبود، مدارک کافی برای محکوم کردن آنها وجود نمی‌داشت.

اکثریت پاسخ دهندگان برای حساب‌های آنلاین خود روی دستگاه‌های الکترونیکی و/یا کامپیوترهای شخصی شان، یا اصلاً رمز

---

۱ مصاحبه با آرتیکل ۱۹

عبورنداشتند، یا از رمز عبورهای ضعیف استفاده می‌کردند. در بیشتر موارد، پاسخ دهنده گان از فقط یک رمز عبور برای چندین حساب استفاده می‌کردند که همین موضوع دسترسی به حساب‌ها را برای مقامات آسان می‌کرد. یکی از شرکت کنندگان حتی اذعان کرد که همه رمزهایش را به دلیل حافظه ضعیف خود، بر روی دسکتاپ ذخیره کرده بود. هیچ یک از شرکت کنندگان از برنامه مدیریت رمز عبور استفاده نکره بودند.

برخی از پاسخ دهندگان بلافاصله رمز عبورهای خود را نزد مقامات افشا کرده بودند؛ با این تصور که یا چیزی برای پنهان کردن ندارند، یا اینکه در صورت همکاری، با آنها ملایم تر رفتار خواهد شد. با این همه، مصاحبه شوندگانی که این گونه رفتار کرده بودند - یعنی با این باور که مقامات با آنها رفتار کمتر سخت گیرانه خواهند داشت - به اشتباه خود پی برده بودند.

در مقابل، آندسته از پاسخ دهندگانی که طی بازجویی داوطلبانه رمزهای خود را به مقامات نداده، یا رمزعبورهای اشتباه داده بودند، موفق به حفظ ایمنی حساب‌های خود شده بودند.

هیچ یک از پاسخ دهندگان از نرم افزارهای ویژه رمزنگاری بر روی دستگاه‌های خود استفاده نکرده بودند. در چند مورد، داده‌های یافته شده بر روی کامپیوترهای افراد دستگیر شده منجر به شناسایی، به خطر افتادن و (در یک مورد در این تحقیق) دستگیری افراد دیگر شده بود. در یک مورد، یکی از پاسخ دهندگان که تاریخچه پیام‌های چت را حذف نکرده بود، سهواً هویت فردی را که با پشتکار و دقت تاریخچه چت‌ها را روی دستگاه خود حذف کرده بود، فاش کرده و همین موضوع منجر به بازداشت فرد دوم شده بود.

استفاده از اطلاعات پراکنده و ناقص

اطلاعات پراکنده‌ای که از سوی مقامات از منابع گوناگون جمع آوری شده بود، به عنوان وسیله‌ای برای ایجاد ارعاب مورد استفاده قرار گرفته بود، و همین باعث شده بود تا افراد اطلاعات بیشتری درباره خود - با این باور (غلط) که مقامات همه چیز را درباره فرد بازداشت شده می‌دانند - ارائه دهند[1].

این روش که جو رعب و وحشت غالب بر جامعه ایران آنرا تشدید می‌کند، بر رفتارهای اینترنتی برخی از پاسخ دهندگان تأثیر گذاشته بود، زیرا آنها بر این باور بودند که هر چقدر هم که بکوشند تا مواظب رفتار خود باشند، مقامات از همه جزییات زندگی آنان با خبر هستند. در نتیجه، آنها معتقد بودند که تدابیر امنیتی بی فایده‌اند.

فشار روانی

برخی از پاسخ دهندگان از تهدید مقامات خبر می‌دادند دال بر اینکه در صورت عدم همکاری آنها، اطلاعات خصوصی که موجب شرمساری آنان خواهد شد، در اختیار دیگران قرار خواهند داد. برخی دیگر شرح می‌دادند که برای اعمال فشار بیشتر بر آنان، تهدیداتی علیه اعضای خانواده آنها صورت گرفته بود. اعضای خانواده از سوی مقامات تهدید شده بودند که در صورت اعتراض علنی به زندانی شدن آنها، با بستگانشان به شدت بدرفتاری خواهد شد. در موارد گوناگون، مقامات به دروغ به اعضای خانواده قول داده بودند که اگر با آنها همکاری و اطلاعات لازم را نزد مقامات افشا کنند، همین موضوع باعث آسان تر شدن شرایط زندان برای عزیزانشان می‌شود.

---

۱ بنابر یافته‌های موجود در مصاحبه‌ها

شکنجه و دیگر شکل‌های بدرفتاری

بسیاری از پاسخ دهندگان شرح می‌دادند که طی دوره بازداشت، مقامات برای وادار کردن آنها به اعتراف از شکنجه و دیگر شکل‌های بدرفتاری استفاده کرده‌اند. پاسخ دهندگان در گزارش‌های خود به بازجویی‌های به شدت طولانی، ضرب و شتم مکرر از سوی مأموران مجری قانون، سیلی زدن، هتاکی، و نگه داشته شدن در شرایط بازداشت - که می‌تواند رفتاری سبعانه، غیرانسانی و تحقیرآمیز تلقی شود -اشاره کرده‌اند.

بازجویی به عنوان منبع اصلی اطلاعات

طی بازجویی‌ها، از همه پاسخ دهندگان خواسته شده بود تا رمز عبورها و اطلاعات درباره همه تماس‌ها، شبکه‌ها و سازماندهان تجمعات یا جنبش‌های اعتراضی را ارائه دهند. از برخی از پاسخ دهندگان کمتر شناخته شده خواسته بودند تا همه اطلاعات خود درباره برخی از دوستان، همکاران و دیگر تماس‌ها را بنویسند. یکی از مصاحبه شوندگان اظهار داشت که "بخش بزرگی" از بازجویی‌ها شامل نوشتن همه اطلاعاتی می‌شد که آنها درباره تک تک جزییات تماس‌های ذخیره شده بر روی موبایل‌هایشان در اختیار داشتند.

این روش اخیر نوعاً هنگامی از سوی مقامات مورد استفاده قرار می‌گرفت که آنها یک فرد را نشان کرده بودند، اما اطلاعاتی در مورد آنها در اختیار نداشتند[1]. این بدین معنی است که مقامات معمولاً توان دسترسی به حساب‌های آنلاین را پیش از دستگیری (جدا از چند مورد فیشینگ اتفاقی و معدود) ندارند و بنابراین، از بازجویی‌ها و بازداشت‌ها

---

۱ این تاکتیک جدا کردن فرد (یا «تک نویسی») نامیده می‌شود که فرد بازداشت شده را وادار می‌کند تا درباره یکی از اعضای خاص (معمولاً عالی رتبه) از شبکه خود بنویسند.

به عنوان شیوه‌های اصلی جمع آوری اطلاعات استفاده می‌کنند[1].

تاثیر بر جامعه آنلاین در ایران

کنترل اجتماعی

از احضاریه‌ها، بازداشت‌ها و دستگیری‌های موقت در جهت حفظ کنترل اجتماعی و همچنین اشاعه رعب و وحشت میان کاربران اینترنت و جوامع کنشگران استفاده می‌شود. مشخص است که از نظر مقامات، این ابزارها و روش‌ها در ترغیب خودسانسوری بیانات مشروع در میان این گروه‌ها مؤثر بوده است.

در شهرهای کوچک، این تأثیر براساس میزان شناخته شدن کنشگران تغییر می‌کرد. کنشگران کمتر شناخته شده شرح می‌دادند که فعالیت‌های آنلاین خود را بطور کامل متوقف کرده بودند. از سوی دیگر، آن دسته از کنشگرانی که بیشتر شناخته شده به شمار می‌رفتند، فعالیت‌های آنلاین و آفلاین خود را فقط بطور موقت قطع کرده بودند.

وضعیت در تهران فرق می‌کرد. پاسخ دهندگان اعتقاد داشتند ایجاد ارعاب و وحشت بطور قابل ملاحظه‌ای در پایتخت کمتر مؤثر بوده است، زیرا جمعیت بزرگ این شهر و نبود منابع کافی، پیگیری تهدیدات پس از ایجاد رعب و وحشت را برای مقامات بطور چشمگیری دشوار می‌کرد.

احضاریه‌ها و اخطارهایی که با حکم زندان همراه نبودند به عنوان عامل بازدارنده از سوی مقامات استفاده می‌شد، اما چنین مواردی فقط

---

۱ برای اطلاعات بیشتر درباره زیرساخت و توان‌های اینترنتی در ایران، به گزارش سیاست‌ها و زیرساخت اینترنتی ایران از سوی «اسمال مدیا» مراجعه کنید:
http://smallmedia.org.uk/sites/default/files/reports/IIIP02.pdf

در شهرهای کوچک گزارش شده بود.

مهاجرت اجباری

اکثر پاسخ دهندگان که با قید وثیقه آزاد شده بودند، کشور را ترک کردند. بطور چشمگیری تقریباً نیمی از آنها کشور را بین سال‌های ۲۰۱۰ و ۲۰۱۲ ترک کردند. فاصله‌های طولانی بین تاریخ دادگاه‌ها این فرصت را برای آنها فراهم می‌کرد تا با عبور از مرز - با پای پیاده یا با وسایلی که مورد ردیابی قرار نمی‌گرفتند - به کشورهای همسایه بروند. این موضوع چنین القا می‌کند که پذیرفتن وثیقه و فاصله‌های طولانی بین تاریخ دادگاه‌ها می‌تواند یک استراتژی برنامه ریزی شده از سوی مقامات باشد تا به این ترتیب به جای نگاه داشتن کنشگران در زندان، به آنها اجازه ترک کشور را بدهند. چنین استراتژی ضمن کم کردن هزینه‌ها برای مقامات[1]، توان کنشگران برای بسیج کردن دیگران را نیز کاهش می‌دهد و همچنین موجب تضعیف مشروعیت و احساس اتحاد میان آندسته از کنشگران می‌شود که تصمیم به ماندن در ایران می‌گیرند. اکثریت پاسخ دهندگانی که ایران را ترک کردند، دیگر فعالیت‌های آنلاین را متوقف کرده‌اند. یافته‌ها خاطر نشان می‌سازد که این موضوع به خاطر روند تعدیل دوباره و اسکان مجدد در کشوری است که به آن پناه برده‌اند و همچنین به دلیل احساس انزوا است.

---

۱ دولت ایران معمولاً به فشارهای بین المللی درخصوص سابقه خود در زمینه حقوق بشر واکنش نشان می‌دهد. پس از مناقشات انتخابات ریاست جمهوری در سال ۱۳۸۸، تعداد افراد در زندان به شدت افزایش یافت و ایران برای حجم بالای بازداشت‌هایش، در مرکز توجهات بین المللی قرار گرفته بود. به نظر می‌رسد هنگامی که مردم از فرصت بیرون بودن از زندان با قید وثیقه استفاده کرده و کشور را ترک می‌کردند، دولت چشم خود را بر این موضوع بسته بود.

"من اکنون نسبت به درخواست‌های دوستی بر روی فیس بوک بیشتر حساس هستم، همچنین نسبت به تنظیمات حریم خصوصی خودم بر روی پایگاه‌های رسانه‌های اجتماعی نیز حساس تر شده‌ام[1]."

بسیاری از پاسخ دهندگان برای بسیج یا تماس با دیگران دیگر از تلفن‌های موبایل خود استفاده نمی‌کنند. اکثر آنها می‌کوشند از رمز عبورهای قوی تر استفاده کنند و آنها را روی مرورگرها و دستگاه‌های خود ذخیره نمی‌کنند. آنها همچنین سعی می‌کنند تا تاریخچه چت‌ها/ مکالمات خود را بطور مرتب حذف کنند. پاسخ دهندگان به اعتبار رمزنگاری‌های موجود در برخی از سیستم عامل‌ها اطمینان دارند، اما اکثر آنها به دلیل پیچیدگی رمزنگاری اضافی، از آن در ارتباطات خود استفاده نمی‌کنند.

پاسخ دهندگان همچنین شرح دادند که از ابزارهای ارتباطی که به باور آنها کمتر ایمن بود (از جمله پیامک‌ها و اپلیکیشن‌هایی از قبیل تانگو و وایبر) به آنچه از نظر آنها سیستم عامل‌های امن تر و قابل اطمینان تر به شمار می‌رفت (مانند آی مسیج، واتساپ، فیس تایم و اسکایپ) رو آورده بودند. با این همه، پاسخ دهندگان اذعان می‌کردند که رو آوردن به سیستم امل‌های امن تر در واقع با انگیزه سهولت استفاده بود تا امنیت بیشتر. پاسخ دهندگان هیچگاه به استفاده از اپلیکیشن‌های خصوصاً امن همچون چت سکیور[2] و تکست سکیور[3]

---

۱ مصاحبه با آرتیکل ۱۹

۲ برای اطلاعات بیشتر به این صفحه مراجعه کنید:
https://chatsecure.org/

۳ برای اطلاعات بیشتر به این صفحه مراجعه کنید:
https://securityinabox.org/en/guide/textsecure/android

اشـاره‌ای نکردنـد.

تجربه‌های مشترک

تقریبـاً همـه پاسـخ دهنـدگان کوشـیده بودنـد تـا پـس از آزاد شـدن، درس‌هایـی را کـه آموختـه بودنـد بـا همتایـان خـود شـریک شـوند. بـا ایـن همـه، آنهـا می‌گوینـد کـه جامعـه ایرانیـان بـه دلیـل بـی دقتـی و یـا بـی حوصلگـی، رغبـت چندانـی از خـود در خصـوص جـدی گرفتـن اقدامـات امنیتـی آنلایـن نشـان نمی‌دهـد. همچنیـن ایـن درک وجـود دارد کـه امنیـت امـری پیچیـده اسـت و در نتیجـه بـه زحمتـش نمـی‌ارزد. بسـیاری از افـراد بـر ایـن باورنـد کـه بـا وجـود اسـتفاده از هـر گونـه روش امنیتـی، مقامـات ایـران همچنـان خواهنـد توانسـت در امنیـت دیجیتالـی آنهـا نفـوذ کننـد، بطـور غیـر قانونـی بـر فعالیت‌هـای آنلایـن آنهـا نظـارت کـرده، و اطلاعـات شـخصی آنهـا را بطـور غیرقانونـی جمـع آوری کننـد. چنیـن نگرش‌هایـی بازتابـی اسـت از نبـود درک و فهـم درسـت از فرصت‌هـای موجـود جهـت امـن تـر کـردن رفتارهـای دیجیتـال.

کنشگری آنلاین و آفلاین

از نظـر پاسـخ دهندگانـی کـه مـورد مصاحبـه قـرار گرفتنـد، کنشـگری آنلایـن و آفلایـن یکسـان اسـت. زندگـی یـک کنشـگر، خصوصـاً کسـی کـه از هویـت واقعـی خـود اسـتفاده می‌کنـد، در هـر دو حـوزه رخ می‌دهـد. متعاقبـاً تمرکـز و توجـه مقامـات ایرانـی و همچنیـن شـیوه‌های مـورد اسـتفاده آنهـا در زمینـه نظـارت و عملیـات نفـوذی آنلایـن و آفلایـن بـا یکدیگـر تطابق دارد.

بـا ایـن همـه، اکثریـت پاسـخ دهنـدگان از ایـن خبـر دادنـد کـه آنهـا ابتـدا

به دلیل فعالیت‌های آفلاین شان از سوی مقامات مورد شناسایی قرار گرفته بودند. فقط پس از شناسایی شدن در فضای آفلاین بود که نظارت بر فعالیت‌های آنلاین آنها آغاز گشته بود. این موضوع می‌تواند چنین القا کند که مقامات توان لازم برای شنود گسترده آنلاین را در اختیار ندارند و در عوض ترجیح می‌دهند تا فعالیت‌های خود را ابتدا بر روی رفتارهای تحریک آمیز آفلاین متمرکز کنند.

آندسته از معدود پاسخ دهندگانی که بدون در نظر گرفتن پیشینه شان، صرفاً به دلیل فعالیت‌های آنلاین خود احضار شده بودند، یا خامنه‌ای رهبر ایران را مورد انتقاد قرار داده، یا تجمعات را سازماندهی کرده، و یا در اینترنت از تعداد پیروان قابل ملاحظه‌ای برخوردار بودند. این بدین معنی است که فقط انتقادات سیاسی، سازماندهی تجمعات بدون مجوز، و یا داشتن تعداد زیادی از پیروان آنلاین، فعالیت‌های اینترنتی محسوب می‌شوند که از نظر مقامات ایران ارزش نظارت و تحقیق و رسیدگی را دارند.

موارد عمده دلواپسی‌های مقامات

مقامات به هرگونه فعالیت‌های گروهی و به هرگونه عمل یا فراخوان‌های عمومی و خصوصی[1] که از سوی شبکه یا گروهی سازماندهی می‌شود به شدت واکنش نشان می‌دهند. مقامات هنگام کشف یک شبکه، تلاش می‌کنند تا با مرتبط ساختن آن با کشورها یا پول‌های خارجی باعث خدشه دار شدن اعتبارش و آن را تهدیدی

۱ منظور هرگونه فراخوانی برای آکسیون‌های عمومی، تظاهرات و یا اعتراض است

علیه امنیت ملی نشان دهند[1]. اشتغال ذهنی آنها با کشف یک شبکه و وابستگی‌ها آن با کمک‌های خارجی، امری بسیار متداول است. نخستین پرسش‌هایی که مقامات طی بازجویی‌ها می‌پرسند، به دنبال تعیین دو موضوع است: ابتدا افراد یا سازمان‌هایی خارج از ایران که "شبکه" این کنشگر را تشکیل می‌دهند و سپس منابع مالی او.

پاسخ دهندگان همچنین اظهار داشتند که روی تریبون‌های آنلاین، مقامات توجه خاصی به مبارزه مسلحانه و "تجزیه طلبی" در برخی از مناطق که اقلیت‌های قومی متمرکز شده‌اند معطوف می‌کنند. اما یکی دیگر از حوزه‌های حساس برای مقامات تجمعات در دانشگاه‌ها است. به منظور اشاعه ترس از آزار و اذیت و همچنین جلوگیری از تجمعات و بسیج گروهی، بطور منظم از احضاریه‌ها و همچنین سرکوب‌های سیستماتیک دانشجویان و اتحادیه‌های آنان استفاده می‌شود. در سال ۲۰۱۱، چهار عضو از اتحادیه دموکراتیک دانشجویان کرد بازداشت و چند نفر دیگر به دفاتر اطلاعاتی و امنیتی احضار شدند[2].

توان تکنیکی واقعی مقامات

"بازجوی من بهم گفت "حالا دیگه توی دردسر افتادی!
توی خانه‌ات اینترنت پیدا کرده‌ایم!" نمی‌دانستم بخندم

---

۱ سازمان عفو بین المللی بازداشت شش نفر - فیلمسازان مستند و یک تولید کننده فیلم - را در ایران محکوم می‌کند:
http://www.amnestyusa.org/news/press-releases/amnesty-international-condemns-arrest-of-six-individuals-documentary-filmmakers-and-a-film-producer

۲ بیانیه مشترک در خصوص حق تحصیل و آزادی آکادمیک در ایران:
http://www.iranhrdc.org/english/news/press-statements/1000000163-joint-statement-on-the-right-to-education-and-academic-freedom-in-iran.html

یـا گریه کنـم.[1]"

اظهـارات مقامـات ایرانـی دال بـر تـوان آنهـا در اجـرای شـنود فراگیـر، بـا شـواهد و مـدارک موجـود - کـه نشـاندهنده الگـوی بازداشـت و پـس از آن توقیـف تجهیـزات تکنیکـی اسـت- مغایـرت دارد. پاسـخ دهنـدگان اشـاره می‌کردنـد کـه گاهـی مقامـات بطـور رنـدوم افـرادی را دسـتگیر می‌کننـد و سـپس می‌کوشـند تـا پرونـده‌ای را علیـه فـرد دسـتگیر شـده بـر اسـاس آنچـه کـه بـر روی کامپیوتـر و یـا دیگـر دسـتگاه‌های او می‌یابنـد تشـکیل دهنـد. معمـولاً بـه دنبـال دسـتگیری‌های رنـدوم، جریمه‌هـای سـنگینی وضـع می‌شـود کـه بـر اسـاس قانـون جرائـم رایانـه‌ای می‌باشـد.

بـر اسـاس گفته‌هـای مصاحبـه شـوندگان، اطلاعـات تکنیکـی واقعـی بازجویـان بسـیار محـدود اسـت، هرچنـد گفتـه می‌شـود کـه اطلاعـات بازجویـان سـپاه پاسـداران انقـلاب اسـلامی بیشـتر از بازجویـان وزارت اطلاعـات اسـت. بازجویـان نتواسـته بودنـد کامپیوتـر هیـچ یـک از پاسـخ دهنـدگان را هـک کننـد؛ بلکـه دسترسـی بـه رمـز عبورهـا فقـط در نتیجـه اشـتباه یـا بـی دقتـی فـردی میسـر گشـته بـود و یـا ایـن اطلاعـات زیـر فشـار بـه مقامـات داده شـده بـود.

بـا ایـن همـه، روندهـای موجـود نشـان می‌دهـد کـه از سـال ۲۰۰۹ بـه بعـد، معلومـات تکنیکـی و منابـع مقامـات افزایـش یافتـه اسـت[2]. مجـدداً ایـن موضـوع منطبـق بـا ایـن درک آنهـا اسـت کـه تریبون‌هـای آنلایـن قـدرت بسـیج کـردن افـراد را دارد. هنگامـی کـه مقامـات بـه چنیـن درکـی رسـیدند، آنهـا سـرمایه گـذاری هنگفتـی در ظرفیـت سـازی و اسـتخدام متخصصـان

---

۱ مصاحبه با آرتیکل ۱۹

۲ بـرای اطلاعـات بیشـتر دربـاره زیرسـاخت و توان‌هـای اینترنتـی کنونـی ایـران بـه «گـزارش سیاسـت‌ها و زیرسـاخت اینترنتـی ایـران»از سـوی اسـمال مدیـا مراجعـه کنیـد:
http://smallmedia.org.uk/sites/default/files/reports/IIIP02.pdf

و کارشناسانی [1] کردند که یا اغلب ترسانده شده‌اند یا مشوق‌های سخاوتمندانه‌ای به آنها پیشنهاد شده است.

عدم هماهنگی و شکاف اطلاعاتی

یافته‌های این گزارش نشان می‌دهد که بطور مشخص شکاف اطلاعاتی بین سازمان‌ها و ادارات متفاوت مقامات ایران وجود دارد.

روال برخوردها بر اساس مکان جغرافیایی

بسیاری از پاسخ دهندگان شاهدی بر وجود این روند بودند که اکثر بازداشت‌ها و تهدید و ارعاب در تهران و سپس با اندکی فاصله، در استان فارس رخ داده بودند. چنین پنداشته می‌شود که مقامات استان فارس کوشیده بودند تا، توان امنیتی و اطلاعاتی خود را با ترکیبی از بازداشت‌های رندوم همراه با اتهامات سنگین، حجم بالای بازداشت‌های گروهی و میزان چشمگیری از کنترل اجتماعی نشان دهند. پاسخ دهندگان بر این باورند که این امر یا به دلیل اختلافات جناحی درون سیستم امنیتی است، و یا وجود مشوق‌های ترفیعی برای واحدهای درگیر در این موضوع.

بازداشت‌ها، اتهامات و زندان

در اکثر موارد، شواهد و مدارک در پرونده یک فرد بر اساس چیزهایی است که بر روی دستگاه‌های دیجیتالی مصادره شده او یافت

---

۱ گزارش آرتیکل ۱۹ با عنوان «جرائم اینترنتی در ایران: سرکوب آنلاین در عمل (۲۰۱۳) را ببینید:
http://www.article19.org/resources.php/resource/37385/en/computer-crimes-in-iran:-online-repression-in-practice

می‌شود. قوانین و مقررات مبهمی که در قانون جرائم رایانه‌ای یا قانون مجازات عمومی آمده است، وارد کردن اتهامات سنگین به شهروندان را برای مقامات تسهیل می‌کند.

اکثریت پاسخ دهندگان با حکمی در محل سکونت خود دستگیر شده بودند. گروهی از آنها پس از دریافت حکم بازداشت، خود را تحویل داده بودند. معدودی از آنها پیشتر نیز برای فعالیت‌های خود دستگیر شده بودند، و برخی هم ماه‌ها پیش از دستگیری شان، جلسات توجیهی مکرری با یک مأمور امنیتی تعیین شده داشته بودند.

متداول ترین اتهامات عبارتند از: تبلیغ علیه نظام، اقدام علیه امنیت ملی، توهین به رهبر ایران آیت الله خامنه‌ای، تجزیه طلبی و مشارکت در مبارزه مسلحانه (برای کنشگران اقلیت‌های قومی)، نشر اکاذیب و اقدام علیه عفت و اخلاق عمومی.

به رغم اشاره نه چندانی که به این موضوع در مصاحبه‌ها شده بود، تقریباً همه این اتهامات مبهم مطابق با و تحت پوشش قانون جرائم رایانه‌ای و قانون مجازات عمومی هستند. این موضوع خاطر نشان می‌سازد که اگرچه بر طبق شواهد موجود در مصاحبه‌ها بازداشت‌ها همچنان خودسرانه رخ می‌دهند، اما مقامات ایرانی اطمینان حاصل می‌کنند که این بازداشت‌ها بر اساس قوانین ملی ایران که در حال شکل گیری است صورت گیرند.

تحت چنین قوانینی، افرادی که می‌کوشند از حقوق بشر بنیادین خود - از قبیل حق آزادی بیان، برگزاری تجمعات و جمعیت‌های مسالمت آمیز، آزادی مذهب، و تلاش برای دسترسی و به مشارکت گذاشتن اطلاعات مشروع روی اینترنت استفاده کنند، با مجازات‌های کیفری سنگینی روبه رو می‌شوند.

تحلیل نهایی و نتایج

تحلیل نهایی و نتایج

مقامات ایران توانسته‌اند جو ارعاب و وحشت و سؤظن را با موفقیت در جامعه اینترنتی ایران بوجود آورند. میزان بالای بازداشت‌های کسانی که در فعالیت‌های آنلاین شرکت داشته‌اند (از جمله بازداشت‌های رندوم که به مجازات‌های سنگین منجر می‌شود)، به مقامات این اجازه را داده‌است تا کنترل اجتماعی خود را حفظ کنند، و همین امر موجب محدود شدن استفاده مشروع از حق آزادی بیان و اطلاعات شده است. با این همه، پس از بررسی دقیق شیوه‌های عملکرد مقامات - بویژه نحوه شنود و جمع آوری اطلاعات از سوی آنها - مهارت‌ها و منابع آنها در زمینه حفظ نظارت و شنود جامع و موفقیت آمیز در سرتاسر کشور را نه می‌توان اثبات کرد و نه رد.

بر اساس پژوهش ما، آرتیکل ۱۹ بر این باور است که شهروندان ایرانی - مدافعان حقوق بشر، کنشگران، خبرنگاران و وبلاگ نویسان - همچنان بر اساس قوانین جرائم سایبری، از سوی مقامات ایران شناسایی، تحت نظارت و هدف قرار خواهند گرفت. دریافت‌های حاصله از پژوهش ما نشان می‌دهد که آندسته از کاربران اینترنت که برخی از ویژگی‌های زیر را نشان می‌دهند، بیش از دیگران در معرض خطر بازداشت غیرقانونی، شکنجه و دیگر بدرفتاری‌ها و محاکمه ناعادلانه قرار دارند:

- آنهایی که در فعالیت‌های آفلاین شرکت می‌کنند و لینک‌های شناخته شده به هویت و سوابق آنلاین آنها موجود است.

- آنهایی که در شهرهای بسیار کوچک زندگی می‌کنند و به آسانی می‌توان آنها را شناسایی کرد.
- آنهایی که از نفوذ اینترنتی برخوردارند و به دلیل میزان مخاطبانشان و سطح حمایت از آنها، توان دسترسی به میزان قابل ملاحظه‌ای از افراد را دارند.
- آنهایی که فقط از کمترین میزان و یا هیچ اقدامات امنیتی استفاده می‌کنند.

آرتیکل ۱۹ معتقد است که جامعه آنلان ایرانی متواند با تقویت امنیت آفلان خود باعث تقویت امنیت آنلاین خود نیز باشد. جامعه اینترنتی ایران هنوز اهمیت امنیت دیجیتالی را بخوبی درک نکرده است. برخورد کاربران اینترنت در ایران با مسئله امنیت آنلاین خود بیشتر منفعلانه است تا پیشگیرانه. تا جاییکه اتفاقی برای خود آنها رخ نداده است، آنها به دلیل کاهلی، بی دقتی و یا این باور که چنین کاری بی فایده است، نسبت به تغییر عادات آنلاین خود بی میل و رغبت هستند.

پژوهش ما همچنین نشان می‌دهد که بسیاری از کاربران اینترنت در ایران خود را مقید به استفاده از فناوری‌های ایمن تر (اپلیکیشن‌ها، سیستم عامل و پایگاه‌ها، کتاب‌های راهنماها، کتابچه‌ها و دیگر ابزارها) نمی‌کنند، زیرا از نظر آنها استفاده از این فناوری بیش از حد پیچیده است.

میزان دانش و منابع مقامات هنوز تعیین نشده است، چرا که بر اساس مقیاس این پژوهش، داده‌هایی که درباره این موضوع در اختیار آرتیکل ۱۹ قرار گرفته، نظری و حداقل به شمار می‌رود. با این همه، آرتیکل ۱۹ تصدیق می‌کند که برخی از شکاف‌های شناسایی شده

نشـان می‌دهـد کـه داشـتن طرح‌هـای احتمالـی چنـد بخشـی[1] بـه منظـور حمایـت از آندسـته از کسـانی کـه در معـرض خطـر قریـب الوقـوع هسـتند بسـیار ضـروری اسـت.

۱ رویکـردی کـه در آن تعـداد کثیـری از سـازمان‌هایی بـا تخصص‌هـای گوناگـون مثـلاً در زمینـه فنـاوری، شـرکت‌های تجـاری، سـازمان‌های غیردولتـی، سـازمان ملـل متحـد و غیـره مداخلـه می‌کننـد.

راه پیش رو: توصیه‌ها

راه پیش رو: توصیه‌ها

توصیه‌هایی به جمهوری اسلامی ایران

- ایران باید هدف قرار دادن کنشگران شنود فعالیت‌های آنها را متوقف کند. همه شنودهای هدفمند باید مطابق با بند ۱۷ میثاق بین المللی حقوق مدنی و سیاسی باشد. شنود جمعی (یا "جمع آوری فله‌ای اطلاعات") اساساً مداخله نامتناسب در حقوق بشر[1] به شمار می‌رود، و جمهوری اسلامی ایران باید اطمینان حاصل کند که در این زمینه از معیارهای بین المللی حقوق بشر پیروی می کند.
- اقداماتی که با حمایت حکومت ایران در زمینه سانسور انجام می‌شود - از جمله فیلترینگ سیستماتیک محتوای اینترنت- بایستی بی درنگ متوقف شود. هرگونه فیلترینگ از سوی دولت یا ارائه دهندگان خدمات اینترنتی تجاری که از سوی کاربر نهایی کنترل نمی‌شود، شکلی از سانسور از پیش به شمار می‌رود که محدودیتی بر آزادی بیان است و به همین

---

۱ «آرتیکل ۱۹، سازمان حریم خصوصی بین الملل، دیدبان حقوق بشر و دیگران»، مشاوره دفتر کمیسیون عالی حقوق بشر در رابطه با قطعنامه ۶۸/۱۶۷ از سوی مجمع عمومی سازمان ملل با عنوان حق حفظ حریم خصوصی در عصر دیجیتال، ۱ آوریل ۲۰۱۴، که در این آدرس در دسترس همگان است:
https://www.ef.org/files/2014/04/17/ngo_submission_final_31.03.14.pdf

دلیـل توجیـه پذیـر نیسـت[1].

- قانـون گـذاران جمهـوری اسـلامی ایـران بایـد قانـون جرائـم رایانـه‌ای را در تمامیـت آن لغـو کننـد، و در جهـت مشـروعیت بخشـیدن بـه اسـتفاده از حـق آزادی بیـان، اصلاحـات حقوقـی جامعـی را بـه اجـرا بگذارنـد.
- هرگونـه قانونـی از قبیـل قانـون جرائـم رایانـه‌ای کـه مسـئولیتی روی شـرکت‌های ارائـه دهنـده خدمـات اینترنتـی (آی اس پـی) بـه دلیـل محتـوای مطالبـی کـه از طریـق سیسـتم‌های آنـان عبـور می‌کنـد تحمیـل می‌کنـد، بایـد بلافاصلـه لغـو شـود.

توصیه‌های برای سازمان‌های غیردولتی (NGOs) و پدیدآورندگان فناوری که روی حقوق دیجیتالی در ایران کار می‌کنند

- بایـد همـکاری فزاینـده‌ای بیـن سـازمان‌های غیردولتـی و پدیدآورنـدگان فنـاوری کـه در زمینـه حقـوق دیجیتالـی در ایـران کنشـگر هسـتند وجـود داشـته باشـد. بـا همـکاری بیشـتر، مـوارد زیـر بایسـتی اجـرا شـود:
  - همـه مطالـب و ابزارهایـی کـه از سـوی سـازمان‌های غیردولتـی و پدیـدآوردگان فنـاوری بوجـود می‌آینـد، بایـد قابـل دسـترس همـگان وقابـل اسـتفاده کاربرانباشـند. آنهـا بایـد بگونـه‌ای طراحـی شـوند کـه بـا ایجـاد تغییـرات فرهنگـی و رفتـاری

---

[1] همانگونـه کـه ایـن موضـوع در بیانیـه مشـترک در خصـوص آزادی بیـان و اینترنـت، از سـوی چهـار گزارشـگر ویـژه بیـن المللـی در زمینـه آزادی بیـان بـه وضـوح در سـال ۲۰۱۱ بیـان شـده اسـت: http://www.osce.org/fom/78309

مناسب، موجب تحقق امنیت اینترنتی - حتی برای کسانی که از حداقل دانش درباره فناوری مربوطه برخوردارند - می‌گردد.

» باید تحلیل و تحقیق دقیقی در خصوص توانایی‌ها و استراتژی‌های واقعی جمهوری اسلامی ایران در زمینه شنود و سانسور انجام شود. همچنین بسیار حائز اهمیت است که ساختار قدرت شنود و پلیس اینترنتی در ایران به منظور تأیید یافته‌های ارائه شده در این گزارش - دال بر اینکه مقامات مسئول نظارت و بازداشت‌ها نامتمرکز و ناهماهنگ هستند - بررسی و تحلیل شود.

» برای همه افراد درگیر باید طرح‌های احتمالی مناسب ایجاد و طراحی شود تا بتوانند بلافاصله اقدامات لازم را برای افرادی که با بالاترین میزان ریسک و تهدید روبه رو هستند، انجام دهند.

- سازمان‌های غیردولتی باید بر آندسته از مدافعان حقوق بشر که کمتر شناخته شده‌اند - بویژه آنهایی که از گروه‌های اقلیتی هستند - بیشتر تأکید کرده و اطمینان حاصل کنند که آنها از حمایت برابر از سوی سازمان‌های غیردولتی و پدیدآورندگان فناوری برخوردار می‌شوند. همچنین باید ابزارها و کمک‌های لازم برای چنین گروه‌هایی فراهم شود تا آنها بتوانند از خود در برابر تهدیدات دیجیتالی حفاظت کنند.

توصیه‌هایی به کاربران اینترنت در ایران

- کاربران اینترنت باید اطمینان حاصل کنند که در جریان آخرین پیشرفت‌های امنیتی در زمینه ابزاری ارتباطی مورد استفاده

خـود قـرار دارنـد چـرا کـه ایـن کار تاثیـر بـه سـزا بـر امنیـت آنهـا و مخاطبانشـان دارد. ایـن مسـتلزم اهمیـت دادن و توجـه کـردن بـه کتاب‌هـای راهنمـا و بسـته‌های اطلاعاتـی اسـت کـه از سـوی سـازمان‌های غیردولتـی و پدیدآورنـدگان فنـاوری فراهـم می‌آیـد.

- کاربـران نـه تنهـا بایـد از سیسـتم عامل‌هـا و پایگاه‌هـای ایمـن تـر کـه دارای رمزنـگاری هسـتند اسـتفاده کننـد، بلکـه بایـد خـود را بـا رمزنگاری‌هـا اضافـه در زمینـه ارتباطـات آشـنا کـرده و از آنهـا اسـتفاده کننـد. ایـن امـر بایـد شـامل اسـتفاده از رمزنـگاری هـارد دیسـک شـود تـا حتـی در صـورت مصـادر کامپیوتـر یـا لپ تـاپ آنها از سـوی مقامـات، اطلاعـات و داده‌هـای آنهـا همچنـان حفاظـت شـود.
- افـراد شـرکت کننـده در کنشـگری اینترنتـی بایـد اطمینـان حاصـل کننـد کـه عادت‌هـای امنیتـی ضـروری و مقدماتـی را رعایـت می‌کننـد، از قبیـل: حـذف کـردن مکاتبـات خـود کـه ممکـن اسـت آنهـا و شـبکه شـان را درگیـر جرائـم آنلایـن بکنـد؛ خودداری از اسـتفاده از اسـامی واقعـی؛ اسـتفاده از رمـز عبورهـای مطمئـن؛ اسـتفاده از برنامه‌هـای مدیریـت رمـز عبـور؛ کاهـش ریسـک هنـگام اسـتفاده از تلفن‌هـای هوشـمند و تلفن‌هـای همـراه؛ حـذف کـردن تاریخچـه مرورگـر و چت‌هـا؛ و ایجـاد حـس پاسـخگویی مشـترک میـان افـرادی کـه در گروه‌هـای موجـود در حـوزه اینترنـت مشـارکت می‌کننـد.
- کاربـران اینترنـت هنـگام اسـتفاده از کامپیوترهـای عمومـی (بویـژه در کافـی نت‌هـا) و همچنیـن پرینترهـا عمومـی در مکان‌هایـی از قبیـل محوطـه دانشـگاه یـا محـل کار، بایـد بـه شـدت هوشـیار و گـوش بـه زنـگ باشـند. از آنجـا کـه اطلاعـات شـخصی آنهـا و

همچنین داده‌های مرور شده ثبت می‌شود، کاربران نباید از دستگاه‌های خود برای ارتباط برقرار کردن یا مرور اطلاعات حساس استفاده کنند.

- کاربران اینترنت هنگام تلاش برای دسترسی به وبسایت‌های فیلترشده، باید فقط از شبکه‌های مجازی خصوصی (وی‌پی‌ان) ایمن و یا نرم افزارهای که قابلیت ارتباط محرمانه را دارند استفاده کنند.
- کاربران فیس بوک باید اهمیت آسیب پذیرهای امنیتی تنظیمات حریم خصوصی فیس بوک را بخوبی درک کنند و از پروتکل‌های امنیتی مقدماتی و اساسی در فیس بوک پیروی کنند، از جمله:
  - » اطمینان حاصل کنند که "فهرست دوستان" آنها در معرض دید عموم نیست
  - » خودداری از استفاده از پست‌های همگانی. از گذاشتن پست‌های مربوط به موضوعات حساس که ممکن است توجه مقامات را به خود جلب کند، یا باید خودداری کرد، و یا باید این کار بطور خصوصی انجام داد.
  - » گزینش دقیق اعضای مورد اعتماد برای مشارکت در رویدادهایی که ممکن است از سوی مقامات تهدید تلقی شود، به جای فرستادن دعوت‌های دسته جمعی.
  - » هنگام ایجاد گروه‌های فیس بوکی پیرامون موضوع‌های حساس، باید این گروه‌ها بطور خصوصی تشکیل شوند تا به این ترتیب به توان از ایمن باقی ماندن محتوای مکالمات و گفتگوها اطمینان حاصل کرد و از اعضاء حفاظت شود.

- کاربـران اینترنـت هنـگام اسـتفاده از رسـانه‌های اجتماعـی، بایـد نسـبت بـه وجـود حسـاب‌های اینترنتـی جعلـی و "عوامـل نفـوذی" هوشـیار و آگاه باشـند. کسـانی کـه بیشـتر از همـه در معـرض قـرار دارنـد - از قبیـل گردانندگان و مدیـران گروه‌هـا - بایـد نسـبت بـه خطـرات فیشـینگ و کاربـرد فزاینـده عملیـات نفـوذی در اینترنـت از سـوی مقامـات آگاه و هوشـیار باشـند.
- کاربـران اینترنـت و اعضـای خانواده‌هـای آنهـا بایـد برنامه‌هـای احتمالـی جایگزیـن داشـته باشـند تـا در صـورت بازداشـت بلافاصلـه از آنهـا اسـتفاده کننـد:
  - از آنجـا کـه معمـولاً بیـن زمـان بازداشـت و برداشـتن محتـوا از روی دسـتگاه و حسـاب‌های آنلایـن شـخص فاصلـه‌ای وجـود دارد، یکـی از اقدامـات می‌توانـد ایـن باشـد کـه یـک شـخص ثالـث مـورد اعتمـاد رمـز عبورهـا را از راه دور تغییـر دهـد و/یـا اطلاعـات حسـاس را از روی دیسـک‌های سـخت حـذف کنـد.
  - در صـورت آنکـه دسـتگاه‌ها بلافاصلـه طـی رونـد بازداشـت مصـادره نشـوند، دوسـتان و اعضـای خانـواده بایـد بـی درنـگ دسـتگاه‌ها را بـه مکانـی امـن منتقـل سـازند.

رفتارهای اینترنتی مخاطره‌آمیز که می‌توانند شما را به زندان بیندازند

رفتارهای اینترنتی مخاطره‌آمیز که میتوانند شما را به زندان بیندازند.

استفاده همیشگی از وی پی ان های نا امن و آزمایش نشده

استفاده از موبایل برای تمام کارهای حساس

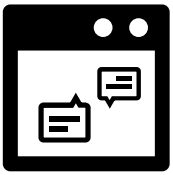
عدم برنامه ریزی برای پاک کردن رد پا دیجیتال در موقع مبادا و در صورت بازداشت

استفاده بی احتیاط از فیسبوک و دیگر شبکه های اجتماعی

عدم رمزنگاری هارد دیسک و یا ایمیل جهت محافظت از مکالمات و اطلاعات حساس

نا آگاهی از آخرین تحولات امنیتی

استفاده همیشگی از پسوردهای ساده



پاک نکردن ایمیل ها ، تاریخچه چت ها و مرورگر

ضمیمه یک: فهرست پرسش‌ها

ضمیمه یک: فهرست پرسش‌ها

۱. بطور مختصر کنشگری کنونی یا اخیر خود را شرح دهید. در صورت پاسخ منفی، لطفاً دلیل فعال نبودن خود را توضیح دهید.

۲. لطفاً شرایط بازداشت خود از سوی مقامات ایران را شرح داده و بطور تقریبی مکان، زمان و چگونگی آن را نیز توضیح دهید.

۳. چه اتهامی به شما وارد شد و آیا بازداشت شما به پیگرد قانونی نیز انجامید؟

۴. تا جایی که اطلاع دارید، مقامات پیش از بازداشتتان چه اطلاعاتی درباره شما داشتند، و این اطلاعات را چگونه جمع آوری کرده بودند؟

۵. آیا مقامات طی بازداشت شما، کوشیدند تا به زور از شما اطلاعات به دست آورند؟ در صورت پاسخ مثبت، لطفاً اطلاعاتی را که مایل به دانستن آن بودند، و همچنین شیوه‌هایی را که برای به دست آوردن آن بکار بردند، شرح دهید.

۶. به نظر شما، فعالیت‌هایتان روی شبکه اینترنت به چه صورت در دستگیری شما و/یا دشواری‌هایی که طی و پس از بازداشت و/یا پیگرد قانونی تجربه کردید، تأثیر گذاشته بود؟

۷. آیا هیچیک از فعالیت‌هایتان در اینترنت و یا هنگام استفاده از فناوری‌های دیجیتال را می‌توانستید به نحو دیگری انجام دهید یا از انجام آن خودداری کنید؟

۸. آیا فکر می‌کنید اطلاعاتی وجود داشته باشد که پیش از بازداشتتان در اینترنت به اشتراک گذاشته باشید و همین به ضرر پرونده تان تمام شده باشد؟

۹. طی و پس از دوران پیگرد قانونی شما، آیا با افرادی دیگری که به دلیل فعالیت‌های خود در اینترنت یا هنگام استفاده از فناوری‌های دیجیتالی تحت پیگیرد قانونی قرار گرفته بودند، تماس گرفتید؟ چه شباهت‌هایی (در صورتی که شباهتی وجود داشت) بین پرونده خود و دیگران یافتید؟

۱۰. آیا تجربه پیگرد قانونی هیچ یک از عادات شما را در هنگام استفاده از فناوری‌های دیجیتالی تغییر داد؟

۱۱. ۱۱. آیا شما به ارتباطات ایمن از قبیل رمزنگاری عقیده دارید و از آن استفاده می‌کنید؟ در صورت پاسخ مثبت، آیا همواره از آن استفاده می‌کنید؟

۱۲. برخی چنین استدلال می‌کنند که مقامات به دلیل فعالیت‌های آنلاین افراد، متوجه آنان می‌شوند و آنان را بازداشت می‌کنند، و این در حالی است که بر اساس نظر مخالف، کنشگران ابتدا به دلیل فعالیت‌های آفلاین خود شناسایی می‌شوند و سپس فعالیت‌های آنلاین آنها چارچوب لازم برای یافتن اطلاعات بیشتر درباره آنان را فراهم می‌آورد. نظر شما چیست؟

۱۳. در مقیاس یک تا پنج، میزان تخصص بازجو یا بازجویان شما در زمینه فناوری اطلاعات و فعالیت‌های اینترنتی چه بود؟ (پنج یعنی بسیار خبره و یک یعنی بی تجربه). لطفاً توضیح دهید.

۱۴. در مقیاس یک تا پنج، تا چه میزان توان مقامات در شنود فعالیت‌های اینترنتی و تشخیص هویت کنشگران آنلاین پیشرفته

است؟ لطفاً توضیح دهید.

۱۵. آیا هیچ پیشنهادی برای دیگر افرادی که از فناوری‌های دیجیتالی برای کنشگری سیاسی / اجتماعی استفاده می‌کنند دارید؟ چگونه تلاش کرده‌اید تا این موضوع را با دیگران در میان بگذارید و چه بازخوردی دریافت کردید؟

۱۶. چه توصیه‌هایی در زمینه ابزارها و منابعی که برای کمک به مردم در جهت بهبود امنیت اینترنت مورد نیاز است دارید؟ این ابزارها و منابع را از چه طریق باید توزیع کرد؟

۱۷. شرکت خدمات اینترنتی (آی اس پی) شما چه نام داشت؟

۱۸. لطفاً هرگونه نظر، پیشنهاد، یا اطلاعات دیگری که مایل به افزودن آن هستید، با ما در میان بگذارید.

۱۹. لطفاً انتخاب کنید: مرد، زن، ترجیح می‌دهم مشخص نکنم، نظرات دیگر.

۲۰. سن شما زمان بازداشت. لطفاً انتخاب کنید: زیر ۲۰ سال، ۲۵-۲۰، ۳۰-۲۵، ۳۵-۳۰، بالای ۳۵ سال.

دفاع از آزادی بیان و اطلاعات

آرتیکل ۱۹

Free Word Centre 60 Farringdon Road London EC1R 3GA

تلفن: 2500 7324 20 44+ فاکس: 0566 7490 20 44+

ایمیل: info@article19.org وبسایت: www.article19.org

توییتر: @article19org فیسبوک: facebook.com/article19org