تحلیل

روندهای سایبری و امنیت جمهوری اسلامی ایران

دکتر قاسم ترابی*

اشاره:

فضای سایبر در حال تبدیل‌شدن به فضایی امنیتی و حتی جنگی برای آسیب‌رساندن به دیگران در شرایط جنگ و مهم‌تر صلح است. فضای سایبر به دلیل ویژگی‌های خاص و مثبت فراوان، ابزاری ایده‌ال برای کشورها و بازیگرانی شده که به شکلی به دنبال تضعیف و یا به دست‌آوردن اطلاعات حیاتی از جمهوری اسلامی هستند به گونه‌ای که ایران تبدیل به یکی از اصلی‌ترین اهداف اقدامات تخریبی سایبری و یکی از قربانیان اصلی این حوزه شده است. شاهد این موضوع هدایت نخستین جنگ سایبری رسمی جهان توسط آمریکا، رژیم صهیونیستی و برخی دیگر از دول غربی با ویروس «استاکس‌نت»[1] و «فلیم»،[2] علیه برنامه هسته‌ای ایران است. بر این اساس در ادامه ضمن بررسی و تحلیل مهم‌ترین روندها و رویدادهای سایبری مرتبط با ایران طی چند ماه گذشته، تلاش می‌شود پیشنهاداتی برای ارتقاء امنیت در این حوزه ارائه گردد.

مقدمه

رصد روندها و رویدادهای سایبری چند ماه گذشته نشانگر آن است که تهدیدات فضای سایبر همچون «جنگ سایبری»، «سایبرتروریسم»، «سایبرتروریسم دولتی»، «جاسوسی سایبری» و همچنین «جرائم سایبری» در حال تبدیل این عرصه به صحنه مقدم جنگ و دفاع هستند. طی این مدت بازیگران مختلف فعال در حوزه سایبر، از جمله دولت‌ها، تروریست‌ها، گروه‌های درگیر در جرایم سازمان‌یافته بین‌المللی و حتی هکرها به شکل فردی، از فضای سایبر به انحای مختلف برای آسیب‌رساندن به دیگران و کسب منافع استفاده نموده‌اند. از جمله می‌توان به استفاده نسبتاً گسترده گروه‌های تروریستی چون داعش از فضای سایبر اشاره نمود که عمدتاً با هدف بزرگنمایی اقدامات تروریستی، جذب مخاطب و پول و اصولاً نشان‌دادن و در متن قراردادن گفتمان خود، از این فضا استفاده می‌کنند. به همین شکل دولت‌های بزرگ نیز با توسل به امکانات فضای سایبر، حوزه‌ای جدید از رقابت و دشمنی را شکل داده‌اند که در چارچوب آن علیه همدیگر جاسوسی کرده و گه‌گاه با هک و تخریب همدیگر، قدرت علمی، فنی و در نتیجه جایگاه برتر خود در سلسله‌مراتب جهانی را به دیگری گوشزد می‌کنند. در این زمینه می‌توان به جاسوسی عمدتاً صنعتی چین از آمریکا که مدام با واکنش و تهدیدات مقامات آمریکایی مواجه می‌شود، جاسوسی گسترده برای رصد روندهای سیاسی، اقتصادی، اجتماعی و فرهنگی تقریباً تمامی کشورهای دنیا توسط آمریکا و اقدامات جسته و گریخته روسیه علیه کشورهای اروپایی و آمریکا از جمله اقدام اخیر در هک اطلاعات خانم کلینتون و مجمع سراسری حزب دموکرات، اشاره نمود.

همچنین می‌توان به پوشش رسانه‌های بین‌المللی در ارتباط با خبرهای حوزه سایبر اشاره نمود که طی چند سال گذشته به شدت روند صعودی داشته‌اند؛ به شکلی که اخبار مرتبط با تهدیدات فضای سایبر از حاشیه به متن درآمده‌اند. به عنوان نمونه طی چند سال گذشته اخبار مرتبط با جاسوسی سایبری آمریکا از مقامات اروپایی، جاسوسی سایبری رژیم صهیونیستی از مذاکرات هسته‌ای ایران و قدرت‌های جهانی، جاسوسی سایبری چین از آمریکا، خطر

1. Stuxnet
2. Flame

* همکار علمی پژوهشکده مطالعات راهبردی

جنگ سایبری روسیه علیه اوکراین و سایر کشورهایی اروپایی و آمریکا و در نهایت اقدامات سایبری ایران، رژیم صهیونیستی و عربستان علیه همدیگر بارها در صدر اخبار و تحلیل رسانه‌های شناخته‌شده بین‌المللی قرار گرفته‌اند. در روند مشابه دیگر تقریباً تمامی کشورهای پیشرو در فضای سایبر و حتی سازمان‌ها و پیمان‌های چون ناتو و اتحادیه اروپا برای مدیریت فضای سایبر و دفع تهدیدات و کسب منافع و فرصت‌ها، راهبردهای سایبری خود را مدون و منتشر نموده‌اند. تردیدی در این زمینه نیست که منتشر شدن راهبرد سایبری این بازیگران پیشرو، نشان‌دهنده امنیتی و حتی نظامی‌شدن فضای سایبر است. در حال حاضر تمامی اعضای ناتو و تمامی اعضای اتحادیه اروپا دارای راهبردهای سایبری مدون مطابق با اصول تصریح‌شده پیمان آتلانتیک شمالی و اتحادیه اروپا هستند. چین، روسیه و رژیم صهیونیستی نیز هرچند بنا به ملاحظات خود و همچنین ابهام راهبردی کلانی که دارند راهبرد سایبری منتشرشده مشخص و اختصاصی ندارند، با وجود این تردیدی در زمینه راهبرد سایبری آنها وجود ندارد. به هر حال این روندهای کلان نشان می‌دهند فضای سایبر به پیشانی رقابت بین کشورها و بازیگران مختلف برای کسب منافع و تعیین جایگاه در سلسله مراتب قدرت جهانی تبدیل شده است.

وضعیت سایبری ایران

بر اساس آمارهای موجود داخلی و بین‌المللی، ایران یکی از کشورهای با ضریب نفوذ متوسط اینترنت در سطح جهان به حساب می‌آید. براساس آمار ارائه شده اطلاعات سامانه مدیریت ضریب نفوذ اینترنت، تعداد کاربران بر مبنای جمعیت ۷۵ میلیون و ۱۴۹ هزار نفر، ۴۳ میلیون و ۲۶ هزار و ۲۷۹ نفر برآورد می‌شود. بر اساس گزارش‌ها، بیشترین اتصالات کاربران ایرانی مربوط به اینترنت، گوشی‌های تلفن همراه است و پس از آن اینترنت ADSLبیشترین کاربر را در کشور به خود اختصاص داده است. ضریب نفوذ اینترنت ADSL در کشور در حدود ۲۲.۰۷ درصد برآورد می‌شود و تعداد کاربران این فناوری، ۱۶ میلیون و ۵۸۲ هزار و ۵۳ کاربر و تعداد مشترکان آن ۶ میلیون و ۶۳۲ هزار و ۸۲۱ مشترک اعلام شده است. همچنین ضریب نفوذ اینترنت گوشی تلفن همراه، با توسعه 3G به ۳۸.۶۷ درصد رسیده است. این بدان معناست که ۲۹ میلیون و ۵۸ هزار و ۷۱۹ ایرانی با تلفن‌های همراه خود به اینترنت متصل می‌شوند. برآوردها از سایر شاخص‌های اتصالات در کشور نشان می‌دهد که همچنان شش میلیون و ۹۳۴ هزار و ۷۶۰ نفر در ایران از اینترنت دایل‌آپ استفاده می‌کنند. بنابراین ضریب نفوذ این فناوری منسوخ‌شده با احتساب سه میلیون و ۴۶۷ هزار و ۳۸۰ مشترک، ۹.۲۳ درصد است. در این ارزیابی‌ها، ضریب نفوذ اینترنت وایمکس ۴.۰۳ درصد برآورد شده که این امر نشان می‌دهد سه میلیون و ۲۸ هزار و ۳۹۸ نفر از طریق این فناوری به شبکه اینترنت متصل می‌شوند. شمار مشترکان اینترنت وایمکس نیز یک میلیون و ۲۱۱ هزار و ۳۵۹ مشترک می‌باشد. همچنین در ایران ۶ میلیون و ۱۰۶ هزار کاربر از طریق فناوری فیبر به اینترنت دسترسی دارند و ضریب نفوذ این فناوری با احتساب ۲ میلیون و ۶۵۶ هزار کاربر، ۸.۱۳ درصد برآورد می‌شود. ضریب نفوذ اینترنت باندپهن نیز به ۴۸.۳۷ درصد رسیده است. براساس ارزیابی‌های انجام شده، ضریب نفوذ اینترنت باندپهن در کشور که تا پایان سال ۹۳ حدود ۳۲.۳۱ درصد اعلام شده بود، به ۴۸.۳۷ درصد رسیده است.

آمار منتشرشده در عرصه بین‌المللی اندکی با آمارهای رسمی ایران متفاوت است. بر اساس داده‌های سایت «آمار زنده اینترنت»[1] در سال ۲۰۱۶ تعداد کاربران اینترنت در ایران ۳۹۱۴۹۱۰۳ نفر برآورد شده است. این بدان معناست میزان نفوذ اینترنت در ایران حدوداً ۴۹ درصد و بالاتر از متوسط جهانی با حدود ۴۶ درصد است، یعنی از هر دو نفر ایرانی یکی به اینترنت دسترسی دارد. بر اساس آمار همچنان ۴۰۸۹۴۰۴۳ نفر به اینترنت دسترسی ندارند که البته رقم بالایی محسوب می‌شود. همچنین این آمار و ارقام نشان می‌دهد طی چند سال گذشته در ایران اقدامات گسترده‌ای برای دسترسی بهتر و آسانتر به اینترنت صورت گرفته است.

1. internet live stats

کاربران اینترنت در ایران ۲۰۱۶

سال	کاربران اینترنت	میزان نفوذ اینترنت	میزان جمعیت	عدم دسترسی به اینترنت	تغییرات سالیانه به درصد	تغییرات سالیانه به نفر	تغییرات جمعیتی
۲۰۱۶	۳۹,۱۴۹,۱۰۳	٪۴۸.۹	۸۰,۰۴۳,۱۴۶	۴۰,۸۹۴,۰۴۳	٪۷.۷	۲,۷۸۴,۸۳۱	٪۱.۱۸
۲۰۱۵	۳۶,۳۶۴,۲۷۲	٪۴۶	۷۹,۱۰۹,۲۷۲	۴۲,۷۴۵,۰۰۰	٪۱۸.۳	۵,۶۱۴,۷۴۸	٪۱.۲۴
۲۰۱۴	۳۰,۷۴۹,۵۲۴	٪۳۹.۴	۷۸,۱۴۳,۶۴۴	۴۷,۳۹۴,۱۲۰	٪۳۳.۱	۷,۶۴۲,۳۶۷	٪۱.۲۸
۲۰۱۳	۲۳,۱۰۷,۱۵۷	٪۳۰	۷۷,۱۵۲,۴۴۵	۵۴,۰۴۵,۲۸۸	٪۳۳.۵	۵,۷۹۶,۶۷۷	٪۱.۳۱
۲۰۱۲	۱۷,۳۱۰,۴۸۰	٪۲۲.۷	۷۶,۱۵۶,۹۷۵	۵۸,۸۴۶,۴۹۵	٪۲۱.۲	۳,۰۲۵,۴۵۹	٪۱.۲۹
۲۰۱۱	۱۴,۲۸۵,۰۲۱	٪۱۹	۷۵,۱۸۴,۳۲۲	۶۰,۸۹۹,۳۰۱	٪۲۱	۲,۴۷۸,۷۳۵	٪۱.۲۵
۲۰۱۰	۱۱,۸۰۶,۲۸۶	٪۱۵.۹	۷۴,۲۵۳,۳۷۳	۶۲,۴۴۷,۰۸۷	٪۱۶.۶	۱,۶۸۱,۰۹۱	٪۱.۲
۲۰۰۹	۱۰,۱۲۵,۱۹۶	٪۱۳.۸	۷۳,۳۷۰,۹۸۲	۶۳,۲۴۵,۷۸۶	٪۱۶.۱	۱,۴۰۷,۰۰۶	٪۱.۱۶
۲۰۰۸	۸,۷۱۸,۱۸۹	٪۱۲	۷۲,۵۳۰,۶۹۳	۶۳,۸۱۲,۵۰۴	٪۲۸.۴	۱,۹۲۶,۲۲۴	٪۱.۱۳
۲۰۰۷	۶,۷۹۱,۹۶۵	٪۹.۵	۷۱,۷۲۰,۸۵۹	۶۴,۹۲۸,۸۹۴	٪۹.۳	۵۷۹,۰۹۶	٪۱.۱۲
۲۰۰۶	۶,۲۱۲,۸۶۹	٪۸.۸	۷۰,۹۲۳,۱۶۴	۶۴,۷۱۰,۲۹۵	٪۹.۴	۵۳۲,۹۷۸	٪۱.۱۴
۲۰۰۵	۵,۶۷۹,۸۹۱	٪۸.۱	۷۰,۱۲۲,۱۱۵	۶۴,۴۴۲,۲۲۴	٪۹.۴	۴۸۷,۶۷۷	٪۱.۱۵
۲۰۰۴	۵,۱۹۲,۲۱۴	٪۷.۵	۶۹,۳۲۱,۹۵۳	۶۴,۱۲۹,۷۳۹	٪۹.۳	۴۴۱,۰۸۴	٪۱.۱۷
۲۰۰۳	۴,۷۵۱,۱۳۰	٪۶.۹	۶۸,۵۲۲,۰۷۴	۶۳,۷۷۰,۹۴۴	٪۵۱.۷	۱,۶۱۹,۳۶۳	٪۱.۲۲
۲۰۰۲	۳,۱۳۱,۷۶۷	٪۴.۶	۶۷,۶۹۶,۶۷۷	۶۴,۵۶۴,۹۱۰	٪۲۱۵.۸	۲,۱۴۰,۱۱۸	٪۱.۳۲
۲۰۰۱	۹۹۱,۶۴۹	٪۱.۵	۶۶,۸۱۲,۷۳۶	۶۵,۸۲۱,۰۸۷	٪۶۱.۲	۳۷۶,۴۸۴	٪۱.۴۶
۲۰۰۰	۶۱۵,۱۶۵	٪۰.۹	۶۵,۸۵۰,۰۶۲	۶۵,۲۳۴,۸۹۷	٪۱۵۰.۸	۳۶۹,۹۲۶	۱.۶۵

http//:www.internetlivestats.com/internet-users/iran/

روندها و رویدادهای سایبری

روندهـا و رویدادهـای سـایبری مرتبط با جمهوری اسـلامی را می‌توان در دو سـطح داخلـی و منطقـه‌ای یا جهانی تقسـیم‌بندی نمـود. در سـطح داخلی که عمدتاً توسـط افـراد بـه شـکل فـردی و بـا انگیزهایـی چـون کلاه‌بـرداری، نشـان‌دادن توانایی‌ها و کنجـکاوی صـورت می‌گیـرد، سـطح تهدیـدات چندان بالا نیسـتند. بـا این حال همین اقدامات ممکن است پیامدهای جدی و ناخواسته‌ای به دنبال داشته باشد. کما اینکه برخی از اقدامات این‌چنینی در کشـورهای دیگـر دارای عواقبـی ناخواسـته بوده‌انـد. بـه عنـوان نمونـه برخـی از ویروس‌هـا و بدافزارهای مورد استفاده هکرها نتایج و پیامدهای به دنبال داشته که از قبل قابل پیش‌بینی نبوده است. همچنین این گونه اقدامات می‌تواند پیامدهای سیاسـی و اجتماعی چون بی‌اعتمادی به دولت و سیسـتم مدیریت کشـور و کاهش اعتمـاد به عنوان یک سـرمایه اجتماعی را به دنبال داشـته باشـد. در این زمینه می‌توان به هکری اشاره نمود کـه چندی پیش با عنـوان «مافیا هکینگ تیم» برخی از سـایت‌های اصلی کشور مثل سایت سازمان ثبت اسناد، شرکت پست جمهوری اسـلامی ایـران و برخی از دانشـگاه‌ها را هک کـرد و به اطلاعات گسـترده‌ای دست یافت. موفقیت این هکر عملاً نشان داد بسیاری از سـایت‌های مهم و حساس کشور چندان در برابر اقدامات تخریبی و جاسوسی ایمن نیستند و باید در این زمینه اقدامات جدی در اولویت قرار گیرد. نگرانی اصلی در این زمینه هک‌شـدن اطلاعات گسترده این سـایت‌ها و قرار دادن آنهـا در اینترنت و در نتیجه ایجاد نگرانی در بین شهروندان است.

کاربران اینترنت در جهان ۲۰۱۶

سال	کاربران اینترنت	میزان نفوذ اینترنت	میزان جمعیت جهان	عدم دسترسی به اینترنت	تغییرات سالیانه به درصد	تغییرات سالیانه به نفر	تغییرات جمعیتی
۲۰۱۶	۳,۴۲۴,۹۷۱,۲۳۷	٪۴۶٫۱	۷,۴۳۲,۶۶۳,۲۷۵	۴,۰۰۷,۶۹۲,۰۳۸	٪۷٫۵	۲۳۸,۹۷۵,۰۸۲	٪۱٫۱۳
۲۰۱۵	۳,۱۸۵,۹۹۶,۱۵۵	٪۴۳٫۴	۷,۳۴۹,۴۷۲,۰۹۹	۴,۱۶۳,۴۷۵,۹۴۴	٪۷٫۸	۲۲۹,۶۱۰,۵۸۶	٪۱٫۱۵
۲۰۱۴	۲,۹۵۶,۳۸۵,۵۶۹	٪۴۰٫۷	۷,۲۶۵,۷۸۵,۹۴۶	۴,۳۰۹,۴۰۰,۳۷۷	٪۸٫۴	۲۲۷,۹۵۷,۴۶۲	٪۱٫۱۷
۲۰۱۳	۲,۷۲۸,۴۲۸,۱۰۷	٪۳۸	۷,۱۸۱,۷۱۵,۱۳۹	۴,۴۵۳,۲۸۷,۰۳۲	٪۹٫۴	۲۳۳,۶۹۱,۸۵۹	٪۱٫۱۹
۲۰۱۲	۲,۴۹۴,۷۳۶,۲۴۸	٪۳۵٫۱	۷,۰۹۷,۵۰۰,۴۵۳	۴,۶۰۲,۷۶۴,۲۰۵	٪۱۱٫۸	۲۶۲,۷۷۸,۸۸۹	٪۱٫۲
۲۰۱۱	۲,۲۳۱,۹۵۷,۳۵۹	٪۳۱٫۸	۷,۰۱۳,۴۲۷,۰۵۲	۴,۷۸۱,۴۶۹,۶۹۳	٪۱۰٫۳	۲۰۸,۷۵۴,۳۸۵	٪۱٫۲۱
۲۰۱۰	۲,۰۲۳,۲۰۲,۹۷۴	٪۲۹٫۲	۶,۹۲۹,۷۲۵,۰۴۳	۴,۹۰۶,۵۲۲,۰۶۹	٪۱۴٫۵	۲۵۶,۷۹۹,۱۶۰	٪۱٫۲۲
۲۰۰۹	۱,۷۶۶,۴۰۳,۸۱۴	٪۲۵٫۸	۶,۸۴۶,۴۷۹,۵۲۱	۵,۰۸۰,۰۷۵,۷۰۷	٪۱۲٫۱	۱۹۱,۳۳۶,۲۹۴	٪۱٫۲۲
۲۰۰۸	۱,۵۷۵,۰۶۷,۵۲۰	٪۲۳٫۳	۶,۷۶۳,۷۳۲,۸۷۹	۵,۱۸۸,۶۶۵,۳۵۹	٪۱۴٫۷	۲۰۱,۸۴۰,۵۳۲	٪۱٫۲۳
۲۰۰۷	۱,۳۷۳,۲۲۶,۹۸۸	٪۲۰٫۶	۶,۶۸۱,۶۰۷,۳۲۰	۵,۳۰۸,۳۸۰,۳۳۲	٪۱۸٫۱	۲۱۰,۳۱۰,۱۷۰	٪۱٫۲۳
۲۰۰۶	۱,۱۶۲,۹۱۶,۸۱۸	٪۱۷٫۶	۶,۶۰۰,۲۲۰,۲۴۷	۵,۴۳۷,۳۰۳,۴۲۹	٪۱۲٫۹	۱۳۲,۸۱۵,۵۲۹	٪۱٫۲۴
۲۰۰۵	۱,۰۳۰,۱۰۱,۲۸۹	٪۱۵٫۸	۶,۵۱۹,۶۳۵,۸۵۰	۵,۴۸۹,۵۳۴,۵۶۱	٪۱۲٫۸	۱۱۶,۷۷۳,۵۱۸	٪۱٫۲۴
۲۰۰۴	۹۱۳,۳۲۷,۷۷۱	٪۱۴٫۲	۶,۴۳۹,۸۴۲,۴۰۸	۵,۵۲۶,۵۱۴,۶۳۷	٪۱۶٫۹	۱۳۱,۸۹۱,۷۸۸	٪۱٫۲۴
۲۰۰۳	۷۸۱,۴۳۵,۹۸۳	٪۱۲٫۳	۶,۳۶۰,۷۶۴,۶۸۴	۵,۵۷۹,۳۲۸,۷۰۱	٪۱۷٫۵	۱۱۶,۳۷۰,۹۶۹	٪۱٫۲۵
۲۰۰۲	۶۶۵,۰۶۵,۰۱۴	٪۱۰٫۶	۶,۲۸۲,۳۰۱,۷۶۷	۵,۶۱۷,۲۳۶,۷۵۳	٪۳۲٫۴	۱۶۲,۷۷۲,۷۶۹	٪۱٫۲۶
۲۰۰۱	۵۰۲,۲۹۲,۲۴۵	٪۸٫۱	۶,۲۰۴,۳۱۰,۷۳۹	۵,۷۰۲,۰۱۸,۴۹۴	٪۲۱٫۱	۸۷,۴۹۷,۲۸۸	٪۱٫۲۷
۲۰۰۰	۴۱۴,۷۹۴,۹۵۷	٪۶٫۸	۶,۱۲۶,۶۲۲,۱۲۱	۵,۷۱۱,۸۲۷,۱۶۴	٪۴۷٫۳	۱۳۳,۲۵۷,۳۰۵	٪۱٫۲۸

http://www.internetlivestats.com/internet-users/iran/

در سطح منطقه‌ای و جهانی سطح تهدیدات قابل قیاس با عرصه داخلی نیستند. ایران بر اساس آمار بین‌المللی از جمله قربانیان و اهداف اصلی مهم‌ترین و مخرب‌ترین حملات سایبری بوده است. دلیل اصلی این امر نیز مخالفت‌ها و دشمنی‌های کشورهای غربی، عربی و رژیم صهیونیستی با ایران به دلیل ماهیت خاص آن و تداوم برنامه هسته‌ای بوده است. البته به شکل کلی با توافق جامع هسته‌ای از سطح تهدیدات سایبری علیه زیرساخت‌های هسته‌ای و غیرهسته‌ای ایران به خصوص از سوی غرب و آمریکا کاسته شد. با وجود این، با گسترش اختلافات در سایر حوزه‌ها و به خصوص گسترش جنگ نیابتی در سطح منطقه، کشورهای چون عربستان و رژیم صهیونیستی مدیریت تهدیدات سایبری علیه ایران را به دست گرفته‌اند. بر این اساس اقدامات اخیر سایبری عربستان سعودی علیه ایران، که به باور برخی از تحلیل گران با حمایت و پشتیبانی رژیم صهیونیستی صورت می گیرد باید در چارچوب رقابت کلان منطقه‌ای بین دو کشور ارزیابی شود. بنابراین اقدامات سایبری عربستان سعودی علیه ایران را باید در کنار سایر اقدامات دو کشور از جمله جنگ نیابتی در سوریه، عراق، یمن، اختلافات جدی در بحرین و تلاش عربستان برای نزدیکی با اپوزیسیون ایرانی خارج کشور و برخی از گروه‌ها و اقلیت‌های مذهبی و قومی در داخل ایران ارزیابی نمود. در این زمینه می‌توان به حملات سایبری به چند سایت ایرانی از جمله سایت مرکز آمار و ثبت احوال ایران اشاره نمود که به گفته مقامات مسئول ایرانی از داخل خاک عربستان سعودی صورت گرفته است. گروهی با عنوان داعس مسئولیت این حمله را بر عهده گرفت که در ابتدا با توجه به نزدیکی اسم آن با داعش، گمانه‌زنی‌ها را به سوی این گروه تروریستی برد. با این حال بعداً معلوم شد که داعس گروهی نزدیک به عربستان و بعثی‌های عراق است. این گروه در صفحه سایت، تصویری از صدام حسین را به نمایش گذاشت.

رژیم صهیونیستی نیز از جمله کشورهایی است که انگیزه فراوانی برای رقابت سایبری و انجام اقدامات جاسوسی و خرابکارانه علیه جمهوری اسلامی ایران دارد. عمده تمرکز سایبری رژیم صهیونیستی برنامه هسته‌ای جمهوری اسلامی ایران است. بر اساس اطلاعات موجود می‌توان گفت رژیم صهیونیستی یکی از بازیگران اصلی فعال در ساخت ویروس استاکس‌نت بوده است. به باور تحلیل‌گران بین‌المللی استفاده از این ویروس علیه تأسیسات هسته‌ای ایران، نخستین جنگ سایبری واقعی در سطح جهان به شمار می‌آید. رژیم صهیونیستی همچنین یکی از فعال‌ترین کشورها در زمینه جاسوسی از مذاکرات هسته‌ای ایران با قدرت‌های بزرگ بود. در این زمینه گزارش شرکت روسی «کاسپرسکی» نشان می‌دهد که سازمان‌های اطلاعاتی رژیم صهیونیستی از ویروس پیشرفته‌تر «دکو» استفاده نموده‌اند تا در جریان ریز مذاکرات قرار گیرند. البته هنوز جزئیات خاصی از این برنامه منتشر نشده است، ولی دولت‌های سویس و اتریش به عنوان کشورهای میزبان مذاکرات در حال تحقیق در این باره هستند؛ نتیجه تحقیقات قرار است بعد از طی مراحل نهایی و قانونی منتشر شود.

اتهامات نسبت به فعالیت‌های سایبری ایران، بخش دیگری از مسائل سایبری را دربرمی‌گیرد. در این باره می‌توان به گزارشی اشاره کرد که توسط نهادها و مراکز امنیتی رژیم صهیونیستی درباره جاسوسی سایبری ایران از سایر کشورها منتشر شده است. بر اساس این گزارش، ایران یکی از فعال‌ترین کشورهای جهان در زمینه جاسوسی سایبری به حساب می‌آید و عربستان سعودی و رژیم صهیونیستی، بیشترین تمرکز جاسوسی سایبری ایران را به خود اختصاص داده‌اند. بر اساس این ادعا، عربستان سعودی هدف در حدود ۴۴درصد و رژیم صهیونیستی ۱۴درصد جاسوسی سایبری ایران بوده‌اند.

با نهایی‌شدن توافق هسته‌ای اقدامات تخریبی آمریکا علیه برنامه هسته‌ای ایران کاهش یافت زیرا یکی از تعهدات ضمنی آمریکا در برجام به شکلی پایان‌دادن به اقدامات تخریبی علیه برنامه هسته‌ای ایران بوده است؛ ضمن اینکه با توافق و با توجه به اجرای پروتکل الحاقی، اصولاً نیاز به اقدامات تخریبی آمریکا در این حوزه کاهش یافته است.

با توجه به اختلافات موجود در منطقه و به خصوص فراگیری جنگ نیابتی بین ایران و عربستان که به شکلی رژیم صهیونیستی نیز در حمایت از سعودی‌ها وارد آن شده است، می‌توان این سطح از تمرکز را در چارچوب جنگ و رقابت منطقه‌ای ایران و عربستان ارزیابی نمود. ضمن اینکه یمن با ۱۱ درصد و ونزوئلا نیز با ۸ درصد کشورهای بعدی هستند. در مرتبه بعدی نیز عراق، انگلستان، افغانستان، کویت، مصر، امارات، ترکیه، سوریه، اردن، کانادا، اسپانیا، مراکش و پاکستان قرار دارند. نکته مهم در مورد این گزارش عدم اشاره به جاسوسی سایبری ایران از آمریکا و قرارنگرفتن این کشور در لیست کشورهای هدف جمهوری اسلامی ایران است. به هر حال این انتظار می‌رفت که با توجه به تنش‌ها و دشمنی‌های گسترده موجود، آمریکا یکی از اهداف اصلی جاسوسی احتمالی

ایـران باشـد، در حالیکه در لیسـت کشـورهای هدف جاسوسـی سـایبری ایران، نامی از آمریکا برده نشده است که دلیل آن چندان مشخص نیست. نکته آخر اینکه بدون توجه به واقعی بودن یا نبودن اطلاعات این گزارش، اصل این موضوع نشـان می‌دهد تا چه میزان رژیم صهیونیسـتی اقدامات ایران در حوزه سایبری را مورد رصد و تجزیه و تحلیل قرار می‌دهد.

با توافـق جامـع هسـته‌ای از سـطح تهدیدات سـایبری علیه زیرسـاخت‌های هسـته‌ای و غیرهسـته‌ای ایـران کاسـته شـد؛ با وجود این، با گسـترش اختلافات در سـایر حوزه‌ها و به خصوص گسـترش جنگ نیابتی در سـطح منطقه، کشورهای چـون عربسـتان و رژیـم صهیونیسـتی مدیریت تهدیدات سایبری علیه ایران را به دست گرفته‌اند.

در مورد روندها و رویدادهای سایبری مرتبط با آمریکا و ایران، چند نکته قابل توجه هسـتند. اول اینکه با نهایی‌شدن توافق هسته‌ای اقدامات تخریبی آمریکا علیه برنامه هسته‌ای ایران کاهش یافت. به واقع یکی از تعهدات ضمنی آمریکا در برجام به شـکلی پایان‌دادن بـه اقدامات تخریبی علیه برنامه هسـته‌ای ایران بوده اسـت. ضمن اینکـه با توافق و با توجه به اجـرای پروتکل الحاقی، اصولاً نیاز به اقدامات تخریبی آمریکا در این حوزه کاهش یافته اسـت. بنابراین به شـکل کلی طی چند ماه گذشـته تحول خاصی در زمینه جنگ یا جاسوسی سـایبری از سوی آمریکا علیه ایران رخ نداده است. با این حال باید به این موضوع اشـاره نمود که بر اساس گزارش‌هایی که اخیراً منتشـر شـده‌اند، آمریکایی‌ها برنامه‌ای کلان برای ایجاد تخریب‌های گسـترده در ایران با توسـل به امکانات فضای سـایبر داشـته‌اند. هدف از ایـن برنامه‌ها تخریب‌های گسـترده در مراکز هسـته‌ای و غیرهسـته‌ای ایران در صورت ناموفق بودن مذاکرات هسته‌ای عنوان شده است. بر اساس گزارش نیویورک‌تایمز این طرح که «نیترو زئوس»[1] نام داشته، قرار بود تـا در صورت عـدم توافق بـه مرحله اجرا درآید. یک از اهداف نیترو زئوس تخریب کامل سـامانه‌های دفاع هوایی ایران بود. بر اساس گزارش این رسـانه، با غیرفعال‌شدن و تخریب سـامانه‌های دفـاع هوایی ایران، آمریکا و هر کشـور دیگری توان ورود به فضای هوایی کشـور و انجام هرگونه اقدام آفندی را پیدا می‌کردند. همچنین طراحان این برنامه قصد داشـتند تا در صورت عدم توافـق با نفوذ به شـبکه بـرق، مخابرات و سیسـتم مالی عملاً آنهـا را با اختلال جدی مواجه سـازند. قرار بر این بوده تا همه این خرابکاری‌ها به شـکل همزمان آغاز شوند تا به شـکلی مسـئولان دچار سردرگمی و کشـور با بی‌ثباتی و شورش مواجه شود. به گفته یکی از تحلیل‌گران مطلع آمریکایی، در صورت اجـرای این طـرح، بزرگترین حملـه سـایبری جهـان بـه مرحلـه اجـرا درمی‌آمد و جهان نسـبت بـه توانایی‌های سایبری آمریکا مطلع می‌شد.

رویداد دیگـر مرتبط با ایـران، اعلان جـرم دادگسـتری آمریـکا علیـه چنـد ایرانی اسـت که با عکس و اسـم به عنوان اخلال‌گـران امنیت آمریکا معرفی شـدند. اتهـام این هفت ایرانی، اختلال در سیسـتم مالی و یکی از سـدهای نزدیک نیویورک عنوان شده اسـت. همچنین در دادخواست دادسـتانی، آنها افـرادی کارآزموده مورد حمایـت دولت ایـران معرفی شـده‌اند که

1. Nitro Zeus

در استخدام شرکت «آی‌تی‌سک‌تیم»[1] و «مرصاد» هستند. نکته قابل توجه اینکه در کنار اعلان جرم سایبری علیه چند شهروند چینی، تقریباً این نخستین‌بار در جهان است که دادگستری آمریکا از شهروندان کشوری دیگر به اتهام انجام جرایم سایبری اعلان جرم می‌کنند. هدف آمریکا از این کار نیز اعمال فشار بیشتر بر ایران و به خصوص بر نخبگان حوزه سایبر است تا با دولت ایران همکاری نکنند. به تعبیری آمریکا با اعلان دادخواست علیه این چند نفر عملاً به دیگران هشدار می‌دهد که همکاری با دولت ایران می‌تواند آنها را در فهرست تحت پیگرد دولت آمریکا در سرتاسر جهان قرار دهد و اینکه خروج از کشور می‌تواند به دستگیری و انتقال آنها به آمریکا منجر شود. به هر حال این روندها نشان می‌دهند که تهدیدات فضای سایبری در حال ایجاد تغییرات کلان در سطح جهان و حتی در قواعد و مقررات ملی هستند، که این امر می‌تواند در روابط کشورهای مختلف مسائل و مشکلات جدیدی به وجود آورد.

در رویدادی دیگر می‌توان به خبر هک‌شدن تلگرام ۱۵ میلیون ایرانی اشاره کرد که باعث ایجاد نگرانی بین شهروندان کشور شده است. بنا به اطلاعات موجود از ۱۰۰ میلیون کاربر تلگرام ایرانی‌ها با ۲۳ میلیون کاربر رکوردار هستند، که البته در حال حاضر با نگرانی از این رسانه اجتماعی استفاده می‌کنند. البته در مورد اینکه هکرها به چه اطلاعاتی دسترسی یافته‌اند اتفاق‌نظر وجود ندارد. با این حال فارغ از اینکه دسترسی در حد شماره تلفن بوده یا کلیه اطلاعات موجود در نرم‌افزار از جمله متن‌ها، عکس‌ها و فیلم‌ها هک شده‌اند، این رویداد به نگرانی‌ها در میان شهروندان و همچنین دولت دامن زده است. شهروندان طبیعتاً نگران منتشرشدن اطلاعات شخصی هستند، امری که در آینده می‌تواند در موارد دیگر آسیب‌های اجتماعی جدی به دنبال داشته باشد. اما در سطح ملی این رویداد نشان داد باید مسئله دسترسی به اطلاعات شهروندان توسط بیگانگان جدی‌تر گرفته شود. نیازی به گفتن نیست که اطلاعات جمع‌شده توسط همین شبکه‌ها در نهایت در اختیار دولت‌هایشان قرار می‌گیرد و یا حتی به کشورهای دیگر فروخته می‌شود. در این زمینه می‌توان به اطلاعات منتشرشده سایت «ویکی‌لیکس» و افرادی چون «جولیان آسانژ» و «ریچارد اسنودن» اشاره نمود که به خوبی این موضوع را تأیید می‌کنند. بر اساس اطلاعات منتشرشده این افراد، دولت آمریکا رابطه نزدیکی با شرکت‌های فعال در حوزه سایبر دارد و اطلاعات مورد نیاز را از آنها می‌گیرد. ضمن اینکه این رابطه را نباید رابطه‌ای بین دو بازیگر ارزیابی نمود، بلکه ماهیت و عمق همکاری در سطحی است که می‌توان دولت و برخی شرکت‌های فعال در حوزه سایبر را در یک جبهه دید.

آتش‌سوزی‌های سریالی که طی چند هفته گذشته در پتروشیمی یا خطوط انتقال گاز کشور اتفاق افتاده‌اند، یکی دیگر از شائبه‌های مهم حملات سایبری را رقم زده است. آتش‌سوزی مهیب در پتروشیمی امام خمینی در ۱۶ مرداد در حالی بود که در بامداد همان روز یکی از لوله‌های انتقال گاز در نزدیکی شهر گناوه در استان بوشهر دچار حریق شد، که بر اساس گزارش‌ها یک کشته و چندین مصدوم به دنبال داشت. مجتمع پتروشیمی بوعلی سینا و همچنین پتروشیمی بیستون کرمانشاه نیز طی چند هفته گذشته با آتش سوزی‌های مشابهی مواجه شده‌اند. به هر حال سریالی‌بودن و زمان نزدیک بین این آتش‌سوزی‌ها باعث شده که احتمال خرابکاری و به ویژه خرابکاری سایبری یکی از گزینه‌های مورد توجه در این زمینه باشد. ضریب این احتمال با توجه به اینکه دولت طی چند سال گذشته به دلیل تحریم‌ها مجبور شده بود تا قطعات مورد نیاز پتروشیمی را از بازار سیاه و دلالان بین‌المللی خریداری نماید، افزایش می‌یابد. در این راستا اخیراً دبیر شورای عالی فضای مجازی خبر از ایجاد تیمی ویژه برای بررسی احتمال خرابکاری سایبری در

2. ITSec Team (ITSEC)

مجتمع‌های پتروشیمی مختلف را مطرح کرده است. قرار است این تیم پس از تحقیق گزارش کاملی درباره علت این رویدادها و در صورت سایبری بودن در مورد بدافزار، عوامل و کشورهای عامل آن ارائه دهند.

نتیجه‌گیری

انقلاب سایبری در حال دگرگون‌کردن زندگی انسان و سامان سیاسی، اقتصادی، فرهنگی و نظامی کشورهای مختلف است. بر این اساس به نظر می‌رسد جهان در کلیه ابعاد در حال پوست‌اندازی و از تن خارج‌کردن نظم گذشته و به تن‌کردن نظم و شاید بی‌نظمی جدیدی با ماهیت سایبری باشد. در این راستا، تأثیرات انقلاب سایبر را نباید دست کم گرفت و باید تلاش کرد ضمن همراه‌شدن با آن در مقام راهبر و نه لزوماً کاربر بود. بر این اساس کشورهایی که موضوع سایبر را در سطح تهدیدات و فرصت‌ها جدی گرفته‌اند، در سالیان آینده نه تنها از امنیت سایبری و به شکل کلی امنیت در ابعاد مختلف بهره‌مند خواهد بود، بلکه در سلسله مراتب قدرت جهانی در مقام‌های بالاتر خواهد نشست. در مقابل عدم دریافتن فرصت‌های سایبری، عقب‌ماندگی در ابعاد مختلف را به دنبال خواهد داشت که خود واجد تهدیدات جدی است. بر این اساس کلید موفقیت در آینده سرمایه‌گذاری گسترده دیروز و امروز بر حوزه سایبر است. در این راستا و بر اساس تجربیات سایر کشورهای پیشرو و راهبردهای سایبری سایرین محورهای زیر راه‌گشا می‌آیند:

- نهادها و مراکز فعال در حوزه سایبر مطابق تحولات جدید به روز شوند؛
- سرمایه‌گذاری بیشتر بر رشته‌های مرتبط با حوزه سایبر در اولویت قرار گیرد؛
- مراکز و پژوهشکده‌های جدیدی در حوزه تحقیق و پژوهش سایبری ایجاد گردند؛
- کشور با سرمایه‌گذاری در ابعاد علمی، پژوهشی و نیروی انسانی از کاربری فضای سایبر در حوزه‌های نرم‌افزاری و سخت‌افزاری بکاهد؛
- همکاری سایبری در ابعاد مختلف با کشورهای دیگر افزایش یابد؛
- تلاش برای گسترش آگاهی‌های عمومی در بین شهروندان، مؤسسات و مراکز خصوصی و دولتی در اولویت قرار گیرد؛
- همکاری بیشتر و ساماندهی‌شده بخش خصوصی، دولتی، دانشگاه‌ها و مراکز علمی و پژوهشی بیش از گذشته مد نظر قرار گیرد؛
- بورس دانشجویان در دانشگاه‌های خارج از کشور برای کسب دانش به روز سایبری در اولویت قرار گیرد؛
- هر سال رزمایش‌هایی برای شناسایی نقاط ضعف و افزایش آمادگی سایبری برگزار گردد؛
- اضافه‌شدن دروسی با هدف آگاه‌سازی در دوران ابتدایی و دروس مقدماتی سایبری با هدف آماده‌کردن شرایط برای ورود دانش‌آموزان به رشته‌های مرتبط با فضای سایبر در دانشگاه‌ها می‌تواند راه‌گشا باشد؛
- شرایط برای تهیه و تدوین یک راهبرد سایبری جامع و منسجم مطابق توانایی‌ها و ضعف‌های کشور در فضای سایبر و تحولات سریع جهانی در این حوزه فراهم گردد.