سال‌نمای امنیت‌ملی جمهوری‌اسلامی‌ایران

تحولات راهبردی ۱۳۹۳

چشم‌انداز ۱۳۹٤

زیر نظر شورای نویسندگان

پژوهشکده مطالعات راهبردی

غیرانتفاعی

امنیت سایبری

مقدمه

امنیت سایبری یا امنیت مجازی عبارت است از نبودِ تجاوز یا هنجارشکنی یا تهدید به آن نسبت به یکی از پنج موضوع داده‌ها و اطلاعات، شبکه‌ها و سیستم‌های رایانه‌ای و مخابراتی، کاربران و مشترکین اینترنتی، ارائه‌دهندگان خدمات اینترنتی و در نهایت، موضوعات بیرون از محیط سایبر مانند بهداشت یا خدمات ضروری عمومی که کارکرد آنها وابسته به سامانه‌های رایانه و مخابراتی است. امنیت سایبری در دو مفهوم مضیق و موسع به کار می‌رود. در مفهوم مضیق، منظور اتخاذ تدابیر فنی و پیش‌گیرانه برای تأمین امنیت شبکه‌ها و اطلاعات است. در این مفهوم، اقدامات غیر فنی جایگاهی نداشته و اشخاص موضوع مستقیم تدابیر امنیتی نیست، همچنانکه تأمین امنیت فراتر از محیط سایبر را در بر نمی‌گیرد. در مفهوم موسع، امنیت سایبری دو گونه از تدابیر اصلی و واسطه‌ای را در بر می‌گیرد که تدابیر اصلی برای تأمین امنیت درون‌شبکه‌ای و تدابیر واسطه‌ای برای تأمین امنیت برون شبکه‌ای به کار می‌رود.

امنیت سایبری مفهومی وابسته به بستر یا فضای سایبری است. این بستر یا فضا در حالت نخستین، چهره‌ای جهانی دارد و مرزهای سرزمینی در آن کم‌رنگ است؛ ولی به جهت سیاست و قوانین ملی کشورها در حوزه سایبر و نیز کنترل‌پذیری مبادلات اطلاعاتی از سوی دولت‌ها، چهره ملی امنیت سایبری حتی از چهره بین‌المللی آن برجسته‌تر است و به عنوان یکی از شاخص‌های قدرت ملی دانسته می‌شود؛ چندان‌که دولت آمریکا، گسترش فضای سایبر و نیز آزادی اینترنت را به عنوان یکی از الگوهای مهم در سیاست برون‌سرزمینی خود می‌شناساند. در همین راستا، بایسته

اســت امنیت سایبری ایران در سال ۱۳۹۳ بررسی گردد تا فرصت و تهدیدهای آن روشن شود و چراغی برای آینده سیاست‌های دولت در این زمینه گردد.

برآورد ۱۳۹۳

فضای سایبر بســتر تبادل اطلاعات به اندازه بزرگی جهان فیزیکی است. بنابراین، امنیت سایبری در گــرو یک پیش‌انگاره اســت و آن دوفضایی‌بــودن زندگی اجتماعی شــهروندان ایرانی همانند شــهروندان دیگر کشورهاســت: فضای فیزیکی و فضای ســایبری. امنیت این فضای بزرگ و باز در حال بزرگ‌شــدن در ایران، وابسته به بررســی چهار گام است: گستره فضای سایبر، پیوند این فضا با امنیت ملی، قدرت ایران در این فضا و تهدیدهای این فضا بر ضد ایران که به نوبت به آنها پرداخته می‌شود.

گســتره فضای مجازی در ایران: برابر آمارهای منتشــره، ایران در زمره بیست کشور نخست جهان از جهت بهره‌گیری شــهروندان از اینترنت اســت که رتبه ســیزدهم جهان را در اختیار دارد. گســترش بهره‌گیری از اینترنت در ایران حتی از دیگر کشــورها باشتاب‌تر بوده است. در حالی که در ســال ۲۰۰۰ تنها ۲۵۰ هزار تن ایرانی از اینترنت اســتفاده می‌کردند، در آغازه ســال ۲۰۱۴ به ۴۵ میلیون تن رسیده است. بهره‌گیری از اینترنت در ایران، رشد نه درصدی در سال داشته است. در کشــورهای پیشرفته در سال ۲۰۱۳، ۷۷ درصد جمعیت و در کشورهای در حال پیشرفت ۳۱ درصد جمعیت از اینترنت استفاده کرده‌اند که ایران مابین کشورهای پیشرفته و در حال توسعه بوده و پنجاه‌وپنج درصد از جمعیتش از اینترنت استفاده می‌کند. ایران در میان کشورهای استفاده‌کننده از گوشــی همراه، رتبه سیزده را دارد که کشورهای بالاتر از ایران همگی جمعیتی به مراتب بیشتر از ایران دارند و ایران در بین کشــورهای زیر نود میلیون جمعیت، رتبه دوم پس از آلمان را دارد. تعداد شــماره‌های پیوندی مخابراتی تا ســال ۲۰۱۳، ۹۶ میلیون اســت که بیست میلیون بیش از جمعیت کشور است.

سال	۱۳۸۷	۱۳۸۸	۱۳۸۹	۱۳۹۰	۱۳۹۱	۱۳۹۲	۱۳۹۳
درصد ضریب نفوذ کاربران در ایران	۲۱/۸	۲۶/۲۹	۲۹/۶۳	۴۲/۲۴	۶۱/۰۶	۴۹/۱۳	۵۳/۴۰

رونــد ضریــب نفــوذ اینترنت پهنــای باند در پنــج شــیوه اتصــالات Cell، Dialup، Adsl، Wimax، phone و Fiber در سال‌های اخیر از روند صعودی برخوردار است.

سال	۱۳۸۷	۱۳۸۸	۱۳۸۹	۱۳۹۰	۱۳۹۱	۱۳۹۲	۱۳۹۳
درصد ضریب نفوذ پهنای باند	بسیار ناچیز	بسیار ناچیز	۱۰/۱۴	۱۵/۳	۲۱/۷۱	۱۷/۷۷	۳۱/۱۶

به گزارش آمار جهانی اینترنت، خاورمیانه با ۱۱۱ میلیون تن کاربر اینترنتی، تنها ۳/۷ درصد از اینترنت جهانی را به کار می‌گیرد. برابر این آمار و جدول زیر، ایران ۴۵ میلیون تن کاربر دارد که از جهت تناسب جمعیت و بهره‌گیری از اینترنت رتبه دهم در منطقه را دارد.

کاربران اینترنتی خاورمیانه				
کشورها	جمعیت در سال ۲۰۱۴	شمار کاربران در دسامبر ۲۰۰۰	شمار کاربران در تابستان ۲۰۱۴	ضریب نفوذ به نسبت جمعیت
بحرین	۱.۳۱۴.۰۸۹	۴۰.۰۰۰	۱.۲۹۷.۵۰۰	٪۹۸/۷
امارات متحده عربی	۹.۲۰۶.۰۰۰	۷۳۵.۰۰۰	۸.۸۰۷.۲۲۶	٪۹۵/۷
قطر	۲.۱۲۳.۱۶۰	۳۰.۰۰۰	۲.۰۱۶.۴۰۰	٪۹۵/۰
کویت	۳.۲۶۸.۴۳۱	۱۵۰.۰۰۰	۳.۰۲۲.۰۱۰	٪۹۲/۵
اردن	۶.۵۲۸.۰۶۱	۱۲۷.۳۰۰	۵.۷۰۰.۰۰۰	٪۸۷/۳
لبنان	۴.۱۳۶.۸۹۵	۳۰۰.۰۰۰	۳.۳۳۶.۵۱۷	٪۸۰/۷
عمان	۳.۲۱۹.۷۷۵	۹۰.۰۰۰	۲.۵۸۴.۳۱۶	٪۸۰/۳
اسرائیل	۷.۸۲۱.۸۵۰	۱.۲۷۰.۰۰۰	۵.۹۲۸.۷۷۲	٪۷۵/۸
عربستان سعودی	۲۷.۳۴۵.۹۸۶	۲۰۰.۰۰۰	۱۸.۳۰۰.۰۰۰	٪۶۶/۹
ایران	۸۰.۸۴۰.۷۱۳	۲۵۰.۰۰۰	۴۵.۰۰۰.۰۰۰	٪۵۵/۷
عراق	۳۲.۵۸۵.۶۹۲	۱۲.۵۰۰	۲.۹۹۷.۸۸۴	٪۹/۲
فلسطین	۲.۷۳۱.۰۵۲	۳۵.۰۰۰	۱.۶۸۷.۷۳۹	٪۶۱/۸
سوریه	۲۲.۵۹۷.۵۳۱	۳۰.۰۰۰	۵.۹۲۰.۵۵۳	٪۲۶/۲
یمن	۲۶.۰۵۲.۹۶۶	۱۵.۰۰۰	۵.۲۱۰.۵۹۳	٪۲۰/۰

بهره‌گیری فراوان ایرانیان از اینترنت در حالی است که بسیاری از شبکه‌های اجتماعی و تارنماها در ایران پالایش شده‌اند. با این حال، شمار استفاده‌کنندگان از این تارنماها بالاست تا

جایی که به گفته وزیر فرهنگ و ارشاد در اسفند ۹۲، چهار میلیون ایرانی عضو فیس بوک‌اند.

بهره‌گیری از اینترنت در سال ۹۳ به طور ویژه، گرایشی آشکار به سمت شبکه‌های مجازی قابل نصب در گوشی‌های همراه داشته است. عرضه گسترده گوشی‌های تلفن هوشمند ارزان‌قیمت با پردازشگرهای دو هسته‌ای و حافظه چند گیگا بایتی توسط بسیاری از شرکت‌های تولیدکننده این گوشی‌ها، سبب شده شبکه‌های اجتماعی چون توئیتر، فیسبوک، گوگل پلاس و فرندفید را با وجود قدمت و گستردگی امکانات بروزشان کنار زده و عمده فعالیت کاربران عادی فضای مجازی به سمت شبکه‌های موبایلی معطوف گردد. حتی در این میان، استفاده از پست‌های الکترونیکی مانند جی میل و یاهو میل نیز کاهش چشمگیر داشته است. این امر سبب شده غول‌های فناوری را وادار به سرمایه‌گذاری در ابزارهای موبایلی نموده است؛ به طوری که شرکت فیس بوک با پرداخت رقم ۲۲ میلیارد دلار شرکت پیام‌رسان واتس آپ را خرید.

برابر آمارهای منتشره، ایران در زمره بیست کشور نخست جهان از جهت بهره‌گیری شهروندان از اینترنت است که رتبه سیزدهم جهان را در اختیار دارد. گسترش بهره‌گیری از اینترنت در ایران از دیگر کشورها پرشتاب‌تر بوده است

امنیت مجازی و امنیت ملی ایران: پیوند میان امنیت ملی و فضای سایبر، به ویژه با آغاز قرن بیست‌ویکم و رایانه‌ای‌شدن امور، شفاف‌تر شده است.

ارتباط فضای سایبر و امنیت ملی ایران از جهت مثبت و منفی قابل توجه است: ارتباط مثبت در نتیجه طبیعی کارکرد فناوری اطلاعات است. فناوری اطلاعات برای تأمین امنیت ملی کارکردهایی فراتر از اطلاع‌رسانی دارد. برخی دولت‌ها با استفاده از تکنیک پنهان‌نگاری[1] در محیط رایانه سعی در حفظ اطلاعات مرتبط با امنیت ملی نموده‌اند. رمزنگاری تکنیک کدگذاری اطلاعات در حین انتقال آنهاست تا احتیاطات لازم برای عدم دسترسی به آنها فراهم شود. در ابتدا این شیوه توسط آژانس امنیت ملی آمریکا برای محافظت از اطلاعات امنیت ملی فراهم گردید اما در ادامه طبق دستور العمل تصمیم‌گیری در مورد امنیت ملی مشهور به ان اس دی دی ۱۴۵[2] آژانس با نام امنیت ملی یا حفاظت از داده‌های حساس مبادرت به کنترل رمزنگاری داده‌های اشخاص نمود بدون آنکه در طبقه‌بندی خاصی از داده‌های مورد کنترل ارایه دهد. همین طور دولت‌ها از فناوری اطلاعات برای تأمین امنیت داخلی نیز بهره برده و برای مبارزه با مجرمین و بزهکاران از طریق خبرگیری از آنها به کار می‌برند.

وجه ارتباط منفی میان امنیت ملی با فضای سایبر در تهدیدات یا رفتارهای مجرمانه سایبری ضد امنیت ملی است. فضای سایبر، محیطی امن و با امکانات برای ناقضان هنجارهای آن محسوب می‌شود و هر آنچه ارتکابش در محیط بیرون مخاطره‌آمیز به نظر می‌رسد، در فضای سایبر راحت و

1. Cryptography
2. NSDD 145 (National security decision directive)

پنهانی تلقی می‌شود. پیوند امنیت ملی با فضای سایبر، بازخوردی از ایده‌های امنیت ملی در محیط بیرون است و رابطه امنیت ملی ایران و فضای سایبر نیز از همین دریچه نگریسته می‌شود. در واقع، درک امنیت ملی ایران و فضای سایبر در نوع نگرش وجوه امنیتی این فضاست. این سبب می‌شود فضای سایبر، بخشی گسترده از امنیت ملی ایران تلقی شود که با وجوه منفی و مثبت همراه است. وجوه منفی این فضا با جاسوسی و اقدام‌های تروریستی سایبری شروع می‌شود که مشهورترین تهدیدات امنیتی فضای سایبراند. طبق گزارش نهادهای مرتبط با امنیت سایبری، ایران در سال ۲۰۱۴ قربانی بیشترین تهدیدات سایبری از نوع جاسوسی و اقدام تروریستی بوده است. جدا از این، وقتی نگرش به ناامنی در فضای سایبر در حوزه اجتماعی نیز لحاظ می‌شود، تهدیدهای دیگری نیز وجود دارد از جمله تنزل عیار اخلاق برخی کاربران ایرانی و افزایش عواقب اخلاقی این شبکه‌ها در تبدیل‌شدن به گفتمان بی‌اخلاقی؛ «ماجرای حمله کاربران ایرانی به فیس‌بوک مسی و لیما، مدل برزیلی» و استفاده روزافزون کاربران از الفاظ مستهجن در توئیتر و ابزارهای موبایلی، افزایش ۶۰ برابری ارزش پول مجازی (بیت کوین) و زیرزمینی‌شدن ارتباطات هکرها، قاچاقچیان و ... به دور از نظارت دولت‌ها به همت این پول، گسترش فعالیت‌های پولی مضر در شبکه‌های اجتماعی و نیز عدم پرداخت مالیات برای فعالیت‌های پرسود تجارت الکترونیکی، افزایش چشم‌گیر شکل‌گیری روابط اجتماعی جدید در فضای مجازی و نبود برنامه‌ریزی فرهنگی برای بهره‌برداری از این خدمات نوین، افزایش جرایم رایانه‌ای و به تبع، افزایش کمی پرونده‌های پلیس فتا با رشد دسترسی به اینترنت، توسعه پرشتاب استفاده بدون تأمل از شبکه‌های ارتباطی تحت موبایل همچون وایبر، لاین، تلگرام، واتس‌اپ و تانگو در میان نوجوانان و جوانان به طور گسترده و آثار زیان‌بار آن، رشد بی‌سابقه استفاده از وی پی ان و پالایه‌شکن برای دورزدن فیلترینگ و افزایش سایت‌ها برای فروش یا ارایه نرم‌افزارهای فیلترینگ، افزایش تخریب و توهین به مقدسات مسلمانان و موج اسلام‌هراسی و افزایش فعالیت‌های اقتصادی مخرب در فضای مجازی، افزایش فروش موارد مخدر با استفاده از شبکه‌های اینترنتی.

تهدیدهای بالا نگران‌کننده‌اند، ولی نباید همه این موارد به عنوان تهدید ضد امنیتی تلقی شود و می‌بایست قدرت امنیت ملی در برابر تهدیدهای سایبری افزایش داده شود تا تنها تهدیدهای ویژه مد نظر قرار گیرد. از سوی دیگر، تهدیدهای پیش‌گفته را نباید موردی و مقطعی دانست که با محدودسازی اینترنت یا پالایش تارنماها و شبکه‌ها بتوان در حذف آنها گام برداشت.

برجسته‌ترین تهدید بر ضد فضای سایبر در سال ۹۳ تهدید هویت سایبری ایران بود که بر پایه آن نام دامنه با پسوند کشوری ایران در آستانه مصادره قرار گرفت

قدرت مجازی ایران: اینترنت و فراتر از آن فضای سایبر، بستری است که هر ساله بیش از پیش از سوی دولت‌ها کنترل می‌شود. دولت ایران نیز در این زمینه کوشیده نیروی کنترلی

خود را بر این فضا بگستراند. به سخن دیگر، قدرت مجازی به عنوان یکی از سنجه‌های مهم برای اعمال قدرت ملی است که به دو صورت نمود می‌یابد؛ تحقق اینترنت یا اینترانت ملی و کنترل اینترنت جهانی. اینترنت ملی یا شبکه ملی اطلاعات برنامه‌ای است که دولت ایران از چندین سال پیش آن را دنبال می‌کند. ایمنی در برابر یورش‌های سایبری، کاهش هزینه‌های ارزی و رونق کسب‌وکار اینترنتی از دلایلی است که دولت ایران برای به راه انداختن این شبکه دنبال می‌کند. شبکه ملی اطلاعات از طریق خدمات‌رسانی وزارت ارتباطات و فناوری اطلاعات است که به طور کامل از سوی دولت کنترل‌شدنی است. در همین راستا، هم‌زمان با دهه فجر سال ۹۳، دو موتور جستجو به عنوان اولین موتورهای جستجوی ملی رونمایی شد. این دو موتور جستجو، پارسی‌جو و گُرگُر نام دارند. بیش از ۱۷۰ میلیارد تومان برای حمایت وزارت ارتباطات از موتورهای جست‌وجو بودجه پیش‌بینی شده که بخشی از این بودجه تا کنون اختصاص یافته و بخش دیگری از آن نیز به مرور زمان به این طرح‌ها تخصیص داده خواهد شد». موتور جستجوی پارسی‌جو نیز یکی از نخستین موتورهای جستجوی فارسی است که از سال ۸۷ راه‌اندازی شد و نسخه ۳ آن در سال ۹۳ با پوشش ۲۰۰ میلیون صفحه روی وب قرار گرفت. سایت الکسا، پارسی‌جو را در رتبه ۶۶۵ پربازدیدترین سایت‌های ایرانی قرار می‌دهد. با این حال، بر اساس آمار الکسا، گوگل و یاهو هنوز پربازدیدترین سایت‌ها در ایران هستند.

همین طور، رشد شبکه‌های اجتماعی ایرانی همچون کلوب، فیس نما، فارس توئیتر، آپارات، افسران و تبیان در سال ۹۳ چشمگیر بوده است. برای نمونه، شبکه افسران، با هدف مقابله با جنگ نرم دشمن راه‌اندازی شده تا ضمن ایجاد بستر هم‌فکری و بیان دیدگاه‌ها، شبکه توزیع برای بیشتر دیده‌شدن محتوا، انتشار سریع آن، طرح ایده‌ها یا اطلاع‌رسانی، بسترسازی برای آزمون ایده‌های نو قبل از اجرا و توانمندسازی افسران جوان بپردازد.

نسبت به اینترنت جهانی، پیروزی یا پیشرفت در جنگ سایبری و رویارویی موفق به جرایم سایبری دو شاخص قدرت سایبری ایران است. سال ۱۳۹۳ از جهت جنگ سایبری در سنجش با سال‌های پیشین، سال موفقی برای ایران به شمار می‌رود. در این سال یکی از مسئولان نظامی کشور آشکارا از بنیادگیری ارتش سایبری ایران سخن گفت و آن را دومین ارتش سایبری جهان دانست. کارکرد ارتش سایبری به طور طبیعی در جاسوسی و خرابکاری رایانه‌ای به عنوان جنگ سایبری است.

در این سال همچنین، شمار یورش‌های سایبری به زیرساخت‌های حیاتی ایران کاهش یافته و از سوی دیگر گفته می‌شود ایران توان جنگ سایبری در رویارویی با قدرت‌های سایبری جهان

را یافته است. اسنودن پیمانکار پیشین سازمان امنیت ملی آمریکا (ان اس ای)، فاش کرد که ایران یورش استاکس نت در سال ۲۰۱۰ را با یورش وایپر در سال ۲۰۱۴ پاسخ داده است. به گفته اسنودن، ایرانیان وایپر (برف‌پاک‌کن) را به شرکت سعودی آرامکو فرستادند که البته در مقایسه با دیگر ویروس‌ها در کارزارهای هک سایبری، کوچک است. این ویروس به طور خودکار خود را در سراسر شبکه ارتباطی داخلی تکثیر می‌کند و در نهایت کارکرد همه تجهیزات را مختل می‌کند. این اقدام ایران هرچند به طور رسمی از سوی مقام‌های ایرانی تأیید نشده، ولی زمینه‌ساز عرفی دفاع مشروع در جنگ‌های سایبری است؛ یعنی به طور مشروع امکان دفاع در برابر تجاوز سایبری از سوی دولت‌های دیگر وجود دارد.

در رویارویی با بزه‌های سایبری، به جهت پالایش گسترده محتوای اینترنتی و نیز وجود چندین نهاد گوناگون در پیگیری بزه‌های سایبری، نرخ کشف و پیگرد بزه‌کاران سایبری بالاست. به گفته رئیس پلیس فتا، پلیس سایبری ایران قدرت کشف ۹۰ درصدی پرونده‌های ارجاعی، علی الخصوص در پرونده‌های مهم را ظرف زمانی ۷۲ ساعت دارد. به گفته وی در سال ۹۳، آزمایشگاه‌های پلیس فتا در استان‌های کشور توسعه یافته و تقویت شده و پلیس فضای تولید و تبادل اطلاعات با استناد به ادله کافی از ارتکاب جرم و نیز فراگیری و کسب دانش فارنزیک، قادر به جمع‌آوری ادله دیجیتال در فضای مجازی است.

وزارت اطلاعات نیز در زمینه تهدیدات نرم به عنوان نهاد قانونی دیگر، پیگیر تهدیدات و سایبری است، به ویژه آنکه طبق بند ب ماده ۲۰۵ قانون برنامه پنجم توسعه، پیش‌گیری و مقابله با فساد و اختلال در امنیت اقتصادی، جرائم سازمان‌یافته ضد امنیتی، اقدامات تروریستی و تهدیدات نرم امنیتی در مقام ضابط دادگستری از وظیفه‌های وزارت اطلاعات است.

نهاد دیگر که قانون برای آن جایگاهی پیش‌بینی نکرده، مرکز بررسی جرایم سازمان‌یافته سایبری سپاه است که به طور گسترده درباره تارنماهای غیر اخلاقی فعالیت می‌کند. یکی از واپسین برنامه‌های این مرکز، اجرای پروژه «عنکبوت» با هدف ناامن‌سازی شبکه‌های اجتماعی غربی برای تولیدکنندگان محتوای غیر اخلاقی، مبتذل و مستهجن است که طبق مرکز مقابله با جرائم سازمان‌یافته سایبری سپاه پاسداران در بهمن ۱۳۹۳، گردانندگان شبکه‌های غیر اخلاقی در فیس بوک را بازداشت و تارنماهای آنان را از میان برده است. برنامه‌های سایبری سپاه از ارتش سایبری و مرکز مقابله با جرایم سازمان‌یافته سایبری فراتر رفته گاه به طور مستقیم از سوی نهادهای زیرین مانند قرارگاه ثارالله پیگیری می‌شود؛ از جمله دستگیری چند تن از گردانندگان صفحات فیس بوک توسط این نهاد. همین طور، گردانندگان وب‌سایت نارنجی که اخبار کامپیوتری و تکنولوژیک منتشر می‌کرد نیز توسط سپاه کرمان دستگیر شده‌اند.

تهدیـد فضـای مجازی در ایران: تهدیـدات فضای مجازی در سـال ۱۳۹۳ را می‌توان از دو جایگاه امنیت خود فضای سایبر و امنیت بیرون از فضای سایبر بررسی کرد. امنیت فضای سایبر هم ناظر به هویت آن و هم ناظر به بستر تبادل اطلاعات است. برجسته‌ترین تهدید بر ضد فضای سایبر در سال ۹۳ تهدید هویت سایبری ایران بود که بر پایه آن نام دامنه با پسوند کشوری ایران در آستانه مصادره قرار گرفت. دولت ایران نام دامنه خود را در سال ۱۹۹۴ زیرِ نشانه.ir از آیکان دریافت کرد. مسـئول ثبت زیردامنه‌های با این پسوند، پژوهشـگاه دانش‌های بنیادی است که به گزارش این پژوهشگاه تا سال گذشته نزدیک به سیصد و پنجاه هزار دامنه اینترنتی تحت پسوند ir ثبت شده است. پژوهشگاه دانش‌های بنیادی نخستین مرکز علمی در ایران است که به اینترنت وصل شده و واحد ثبت نام دامنه با پسوند اختصاصی ایران نیز در همین پژوهشگاه مستقر است. دریافت این پسوند با دشواری‌هایی همراه بوده و به جهت پیوند سیاسی تیره میان ایران و آمریکا، آیکان نیز در سـاخت و ثبت دامنه کشـوری برای ایران با رئیس پیشین پژوهشگاه که در راه ثبت آن تلاش‌های فراوانی داشـته، همکاری بایسته روا نمی‌داشت. این پسوند، شناسه‌ای برای معرفی اینترنتی ایران اسـت که نشانی‌های سطح دوم و سـوم آن به عنوان زیردامنه‌های فعال آن به طور ویژه با عبارت ac.ir برای دانشگاه‌ها و مراکز علمی، co.ir برای شرکت‌های تجاری و gov.ir برای نهادهای دولتی شناخته می‌شود.

سال‌های ۱۳۹۲ و ۱۳۹۳ از جهت امنیت سایبری همسانی‌های بسیاری دارنـد. در واقـع، نـگاه حاکمیـت بـه فضـای سـایبر، به گونه‌ای بوده کـه در سـال‌های اخیر فضـای سـایبر و امنیـت آن در یـک مسـیر قرار داشته است

جدا از مسدودکردن دارایی‌های ایران در آمریکا از سوی دولت این کشور، دستگاه قضایی آمریکا مرجعی برای تملک دارایی‌های ایران تبدیل شده است. دادگاه‌های آمریکایی به استناد اینکه ایران به عنوان دولت حامی برخی اقدام‌های تروریسـتی اسـت، از باب تسبیب و حمایت، باید به جبران زیان بزه‌دیدگان اقدام‌های تروریسـتی بکوشد. بر همین اسـاس ایران در چندین پرونده به جبران زیان‌های هنگفت محکوم شد که خواندگان دعوی برای دریافت منابع مالی موضوع حکم، دسترسی متعارف به دارایی‌های ایران ندارند. از این رو، در یکی از واپسین پرونده‌ها، دادگاه آمریکایی دست بر پسـوند اختصاصی ایران یعنی .ir گذاشتند. طبق گزارش برخی رسانه‌های اسرائیلی در تابستان ۹۳، حکم دادگاه به طرفیت «سازمان ثبت اینترنتی نام‌ها و شماره‌های واگذارشده» یا آیکان صادر شده است. آیکان نهاد غیر انتفاعی آمریکایی با کارکرد بین‌المللی است که مدیریت دامنه‌های شبکه جهانی وب را بر عهده دارد. گفته شـده حکم دادگاه، برای بسـتن وب‌سایت‌های معمولی در ایران نیسـت، بلکه شاکیان را قادر می‌سـازد پول‌هایی را که ایران به آیکان می‌پردازد، تصرف کنند. این پرداخت‌ها را ایران بابت بازکردن وب‌سـایت‌های جدید یا وب‌سایت‌هایی که تجدید ثبت می‌شوند و در انتهای نشـانی خود علامت .ir دارند، به آیکان می‌پردازد. در همین حال، وکیلان این پرونده مدعی‌اند قصد دارند فقط سایت‌هایی را مسدود کنند که متعلق به حکومت ایران باشد.

به گفته مسئول ثبت دامنه اینترنتی .ir پژوهشگاه دانش‌های بنیادی، در صورتی که این حکم اجرایی شود، دامنه‌های اینترنتی با پسوند «آی آر» در عرصه بین‌المللی کار نخواهد کرد و مراجعه به دامنه ir در ایران و خارج از کشور امکان‌پذیر نخواهد بود. در این حکم که از سوی دادگاه محلی صادر شده، بحث منفعتی و مالی مطرح است؛ به این معنی که دامنه .ir و .ip نشانی‌هایی که به ایران تخصیص داده شده به عنوان یک نوع مایملک و دارایی کشور آمریکا تعیین شده که باید ضبط و به حراج گذاشته شود و عایدی آن به نفع بازماندگان قربانیان عملیات تروریستی استفاده شود. دامنه‌های دولتی به نسبت کل دامنه‌های فعال با پسوند.ir، کمتر از یک درصد است و فراوانی آن کمتر از یک هزار دامنه می‌شود، اما به نظر می‌رسد موضوع این حکم مربوط به دامنه‌های دولتی و غیر دولتی نباشد و بحث عواید مالی دامنه‌های اینترنتی مطرح است. در نگاه مسئولان ایرانی پسوند اختصاصی ایران به هیچ روی توقیف‌شدنی نیست؛ چرا که آیکان مؤسسه بین‌المللی است و تصمیماتی که در آن گرفته می‌شود به صورت بین‌المللی بوده و به نظر نمی‌رسد در مورد حکم یک دادگاه محلی، اعمال نظر خاصی انجام دهد. در ضمن آیکان بابت واگذاری دامنه‌ها پولی دریافت نمی‌کند و ایران از این منظر، پولی نزد آیکان ندارد که آنها بخواهند تصاحب کنند. دامنه‌های دات ای آر متعلق به دولت جمهوری اسلامی نیست و نود درصد این دامنه‌ها تحت مالکیت اشخاص به ثبت رسیده است. از طرفی، هیچ سرور دولتی خارج از کشور وجود ندارد که مسدود شود و اگر سرور سایت‌های شخصی نیز مسدود شود، انتقال آن به داخل کشور برای میزبانی به راحتی امکان‌پذیر خواهد بود.

تهدید مهم دیگر، شبکه‌های اجتماعی مبتنی بر تلفن همراه‌اند که به طور گسترده مورد بهره ایرانیان قرار دارند. شبکه‌هایی مانند وایبر، واتس آپ، تانگو، اینستاگرام و لاین به بستری برای تبادل اطلاعات بیشتر بین ایرانیان تبدیل شده و تراکم سامانه‌های اتصال اینترنتی را از رایانه‌های شخصی به گوشی‌های همراه افزایش داده است.

تهدیددانستن گسترش شبکه‌های مجازی یا ندانستن آن خود چالشی در سال ۹۳ بود. در شهریور ۹۳، معاون اول رئیس قوه قضائیه، با ارسال نامه‌ای به وزیر ارتباطات ضمن اینکه خواستار فراهم‌آوری زمینه و بستر فنی مورد نیاز برای مسدودسازی و کنترل اطلاعاتی مؤثر شبکه‌های اجتماعی نظیر وآتس آپ، وایبر و تانگو ظرف یک ماه آینده شد، اعلام کرد در غیر این صورت، قوه قضائیه نسبت به این امر اقدام خواهد کرد. با مخالفت دولت در این زمینه، پالایش هوشمند محتوای اینترنتی جای خود را به پالایش عنوانی که کل تارنما یا نرم‌افزار را پالایش می‌کند، داد. با این حال، تارنماهایی برجسته‌ای مانند فیس بوک با آنکه همچنان فیلتر است، ولی از آن به عنوان تهدید جدی یاد می‌شود. در همین راستا، دادگاه انقلاب ۸ نفر از گردانندگان صفحات فیس بوکی را

در سال ۹۳، نگاه به پالایش تا اندازه‌ای بهبود یافته و پالایش تارنما یا نرم‌افزار و شبکه جای خود را تا اندازه کمی به پالایش محتوا داده است

مجموعا به ۱۲۷ سال حبس محکوم کرده است. «اجتماع و تبانی علیه امنیت ملی، فعالیت تبلیغی علیه نظام، توهین به مقدسات، توهین به سران قوا و توهین به اشخاص»، از اتهامات این افراد بوده است. طبق گزارش خبرگزاری ایرنا، قرارگاه ثارالله این افراد را از تیرماه سال گذشته در شهرهای تهران، شیراز، کرمان، یزد و آبادان مورد پیگرد قرار داده و بازداشت کرده و سپس رسیدگی اولیه به پرونده آنان در دادسرای اوین انجام گرفته است. احکام صادرشده از ۲۱ تا ۱۱ سال حبس را در بر می‌گیرد و دو نفر از متهمان علاوه بر حبس به مجازات نقدی و ۵۰ ضربه شلاق نیز محکوم شده‌اند.

بازی‌های رایانه‌ای، دیگر تهدید مجازی به ویژه برای کودکان و نوجوانان است. بیش از یک‌سوم ایرانی‌ها از بازی‌های رایانه‌ای استفاده می‌کنند که هشتاد درصد آنها در گروه سنی ۸ تا ۱۵ سال قرار دارند. بازی‌های رایانه‌ای و شبکه‌های اجتماعی مجازی هر دو همانند اینترنت‌اند که نمی‌توان به طور قطعی آنها را تهدید قلمداد نمود، ولی میزان استفاده از بازی‌های رایانه‌ای توسط کودکان و نوجوان هم از جهت فرهنگ‌پذیری‌های ناهنجار و هم به جهت آموزش‌های ناروا می‌تواند نگرانی‌هایی برای آینده نسل کم‌سن و سال ایرانی ترسیم کند.

از جهت سیاسی نیز فرمانده نیروی انتظامی ایران، نسبت به افزایش خطر «تروریسم در فضای مجازی» هشدار داده است. تروریسم سایبری به معنای اقدامات خرابکارانه نسبت به زیرساخت‌های حیاتی یا تارنماهای خدمات‌رسان عمومی است که به قصد بر هم زدن امنیت یا پریشانی اذهان عمومی انجام می‌شود. همین نگرانی را مشاور عالی‌مقام رهبری در امور دفاعی و نظامی نسبت به زیرساخت‌های حیاتی کشور که با فناوری اطلاعات در ارتباط هستند، اعلام کرده است.

برآورد مقایسه‌ای

سال‌های ۱۳۹۲ و ۱۳۹۳ از جهت امنیت سایبری همسانی‌های بسیاری دارند. در واقع، نگاه حاکمیت به فضای سایبر، به گونه‌ای بوده که در سال‌های اخیر فضای سایبر و امنیت آن در یک مسیر قرار داشته است. در هر دو سال، نگرانی‌های مربوط به جاسوسی‌های رایانه‌ای، تروریسم سایبری، توهین به مقدسات و مقامات کشور و گسترش تارنماهای غیر اخلاقی وجود داشته و ممنوعیت استفاده از پالایه‌شکن مورد تأکید بوده است. با این حال، این حساسیت‌ها سبب موازی‌کاری و پریشانی در تصدی امنیت سایبری در کشور شده، به گونه‌ای که مسئول تأمین امنیت سایبری در ایران در نهایت روشن نیست. حتی برنامه‌های موازی فنی و قضایی از سوی نهادهای گوناگون برای امنیت سایبری در عمل خود سبب اختلال مدیریت در فضای سایبر شده است. در هر دو سال، ایران از جهت نرخ شتاب گردش اطلاعات و سرعت دسترسی به آنها در جایگاه

نامناسبی بوده و با وجود شمار قابل ملاحظه‌ای از کاربران، از جهت شتاب گردش اطلاعات و دسترسی به آن، در میان کشورهای جهان رتبه ۱۵۰ را دارد. با آنکه دولت اعلام کرده آهنگ افزایش چندبرابری شتاب اینترنتی را دارد، ولی رویکرد غالب آن است که به جای برقراری فضای آزاد و امن اطلاعات از طریق فنی بر سه راه دیگر برای امنیت سایبری تأکید شود. درگیرکردن نهادهای گوناگون نظامی، انتظامی، اطلاعاتی و اجرایی برای کنترل فضای سایبر، پالایش گسترده و پایین نگه‌داشتن شتاب دسترسی به اطلاعات. این سه راه‌کار نادرست، چندین سال است به عنوان راه‌کارهای امنیت‌سازی فضای سایبر استفاده می‌شوند و در دو سال ۹۲ و ۹۳ نیز دنباله داشته‌اند. با این حال در سال ۹۳، دولت گام مهمی برداشته تا از این پس از پالایش هوشمند بهره گیرد. پالایش هوشمند تنها جلوی گردش محتوای غیر قانونی را می‌گیرد و نرم‌افزار یا تارنما را به طور کلی مسدود نمی‌کند. به گفته وزیر ارتباطات و فناوری اطلاعات، دولت در مرحله فاز دوم یعنی سازمان‌دهی فیلترینگ هوشمند است که در گام اول، فیلترینگ هوشمند بر روی اینستاگرام پیاده شده که ۸۳ درصد از میزان فیلترینگ هوشمند موفق بوده است. در واقع در سال ۹۳، نگاه به پالایش تا اندازه‌ای بهبود یافته و پالایش تارنما یا نرم‌افزار و شبکه جای خود را تا اندازه کمی به پالایش محتوا داده است. پالایش هوشمند از آن رو نیز اهمیت دارد که به جهت قضایی، نهاد فیلترینگ که زیر نظر دادستانی کل کشور است، دستور پالایش چندین شبکه اجتماعی مجازی مانند واتس آپ و اینستاگرام را صادر کرده بود. این کمیته به موجب قانون باید مصداق‌های مجرمانه را بیابد و دستور پالایش بدهد، ولی در عمل پالایش معیاری اعمال می‌شود و بر پایه معیارهای از پیش تعیین‌شده، دستور پالایش می‌دهد. به واقع، فیلترینگ هوشمند در سال ۱۳۸۸ به موجب قانون جرایم رایانه‌ای پیش‌بینی شده و آن از ره‌گذر پالایش مصداقی بوده است، ولی کمیته پالایش معیاری را که به فیلترینگ گسترده اینترنتی می‌انجامد در دستور کار قرار داده است. دلیل رویارویی مجلس و دستگاه قضایی با دولت در همین نگاه معیاری و مصداقی به پالایش نهفته است. نمایندگان مجلس شورای اسلامی و نیز مسئولان نهاد فیلترینگ (بعضاً با استناد به فتاوای برخی فقها) می‌کوشیدند برنامه‌های پالایش هوشمند وزارت ارتباطات و فناوری اطلاعات را ناکارآمد جلوه دهند، ولی اجرای نهایی این برنامه و پالایش‌نشدن شبکه‌های اجتماعی، نشان از برتری نگرش پالایش مصداقی بر پالایش معیاری در سال ۹۳ است که می‌توان آن را مهم‌ترین گام پیشرفت در سنجش با سال ۹۲ دانست.

همین‌طور در دو سال ۹۲ و ۹۳، حضور دولتمردان در شبکه‌های مجازی سبب شده نگرش دولتی نسبت به فضای سایبر بهتر از پیش شود. این بهبودی در سال ۹۳ از آن رو برجسته‌تر است که رئیس جمهور نیز به تشویق شهروندان برای استفاده از شبکه‌های اجتماعی مجازی پرداخته است.

سال ۹۳ از جهت پیگرد بزه‌های رایانه‌ای نیز موفق‌تر از سال گذشته بوده است. طبق گفته «رئیس پلیس مبارزه با جرایم رایانه‌ای»، «کمیته ویژه‌ای در پلیس مبارزه با جرایم رایانه‌ای ایجاد شده که فضای اینترنت را رصد می‌کند». وظیفه این کمیته مبارزه با مواردی چون «فروش لوازم غیرمجاز و کلاه‌برداری» است و به موضوعات سیاسی نیز در صورتی که کار غیرقانونی صورت گرفته باشد، بنا بر قانون ورود پیدا می‌کند. کنترل اطلاعاتی در سال ۹۳ تا جایی پیش رفت که دولت لایحه‌ای را برای جرم‌انگاری ورود، معامله و نگهداری دستگاه‌ها و افزارهایی آماده کرد که برای ضبط محتوا (صوت و تصویر) به کار می‌آیند.

چشم‌انداز امنیت سایبری در ایران در سال آینده باز بر همین توازن وجوه منفی و مثبت فضای سایبر است. سنگینی وزنه به سمت مؤلفه‌های مثبت و کنترل مؤلفه‌های منفی است

پلیس فتا با آنکه در سال ۹۲ در حاشیه برخی برخوردهای جنجال‌برانگیز با وبلاگ نویسان بوده ولی به گونه‌ای نامحسوس گرایش به سمت بزه‌های رایانه‌ای عمومی مانند کلاه‌برداری و سرقت رایانه‌ای داشته و از سوی دیگر، برخورد با وبلاگ‌نویسان و نیز کنترل محتوای هرزه در اختیار نهادهای وابسته به سپاه قرار گرفته که هم چهره قضایی ندارند و هم جایگاه آنها در قانون پیش‌بینی نشده است. این برنامه می‌تواند نقدهای وارده به پلیس فتا را به نهادهای غیر مسئول در این زمینه انتقال دهد.

چشم‌انداز ۱۳۹٤

چشم‌انداز امنیت سایبری در ایران پیرو نوع نگرش به فضای سایبر است. به سخن دیگر، امنیت سایبری در ایران بر پایه مؤلفه‌های منفی و مثبت، هر دو است که گاه هر یک از این مؤلفه‌ها برجسته می‌شود. نگرش متوازن در این زمینه و احتیاط دائمی نسبت به فضای سایبر سبب شده ضریب نفوذ اینترنتی و شتاب دسترسی به اطلاعات در ایران پایین‌تر از سطح مطلوب باشد. پالایش گسترده محتوای اینترنتی، مؤلفه دیگر امنیت‌سازی است که از الگوی علمی و کارشناسی‌شده پیروی نمی‌کند. همین طور، تعدد نهادهای امنیت‌ساز در فضای سایبر که برخی جایگاه قانونی ندارند، سبب شده قوانین و مقررات داخلی و بین‌المللی در فضای سایبر ایران، به درستی اجرا نشوند. حتی تعدد نهادهای سیاست‌گذار در زمینه فضای سایبر مانند وزارت ارتباطات و فناوری اطلاعات یا شورای عالی مجازی که برخی نیز جایگاه قانونی ندارند، سیاست‌های حاکم بر فضای سایبر را سردرگم نشان می‌دهد.

چشم‌انداز امنیت سایبری در ایران در سال آینده باز بر همین توازن وجوه منفی و مثبت فضای سایبر است. سنگینی وزنه به سمت مؤلفه‌های مثبت و کنترل مؤلفه‌های منفی است. مؤلفه‌های مثبت بر سه دسته‌اند: نخست قانون‌گرایی. فضای سایبر در ایران از طریق قانون‌های گوناگون هنجارمند شده است. بنابراین، اجرای این قوانین به طور بایسته سبب امنیت‌سازی فضای سایبر می‌گردد. در

برابر می‌توان برنامه‌ها یا اظهار نظرهای خلاف قانون را دید که از این مؤلفه دور است؛ مانند آنچه بر خلاف قانون بیان می‌شود: «استفاده از وی پی ان جرم است». استفاده از پالایه‌شکن و وی پی ان با هیچ یک از عنوان‌های مجرمانه سازگار نیست و به همین دلیل نیز طرحی برای جرم‌انگاری آن در مجلس نوشته شده، ولی تا زمان قانون‌شدن این طرح نباید از جهت استفاده از وی پی ان و فیلترشکن از تعبیر غیر قانونی یا جرم استفاده کرد.

دوم، تمرکزگرایی به این معنا که نهادهای امنیت‌ساز برای فضای سایبر نه تنها باید در قانون پیش‌بینی شده باشند، بلکه به طور متمرکز و هدفمند فعالیت کنند. کنترل هدفمند فضای سایبر هم سبب شفاف‌سازی در این زمینه می‌شود و هم پاسخ‌گویی را به همراه دارد. این دو ویژگی سبب می‌شوند شهروندان بدانند نگاه مثبت ولی هدفمند نسبت به تهدیدهای فضای سایبر وجود دارد.

سوم، برقراری تراز میان میزان کاربران اینترنتی و استفاده از فضای سایبر با شتاب دسترسی به اینترنت و دسترسی آزاد و قانونی به آن. تا زمانی که ایران از جهت شمار کاربران و استفاده اینترنتی رتبه برجسته‌ای در جهان دارد، ولی نرخ نفوذ اینترنتی و نیز شتاب دسترسی به اطلاعات پایین باشد، این فاصله فرجامی جز ناهنجاری فضای سایبر در آینده نخواهد داشت؛ زیرا شمار کاربران اینترنتی با کاهش نرخ نفوذ کاسته نمی‌شود، بلکه خود سبب روی‌آوردن راه‌های جایگزین در فضای سایبر می‌شود که هر ساله پدید می‌آیند. در واقع، فضای سایبر همچون موجی فراگیر همه جامعه را در برگرفته و هر ساله نیز با سرعت و قوت این موج افزوده می‌شود. بنابراین، امکانات ارایه‌شده دولتی باید متناسب با شمار کاربران باشد.

باید یادآوری کرد که دولت باید میان امنیت سایبری درون‌سرزمینی و برون‌سرزمینی فرق بگذارد و این دو را در هم تنیده نداند. آسیب‌ها و کاستی‌های امنیت سایبری ایران، چهره درون‌سرزمینی دارد که محدودسازی فضای سایبر در عمل به زیان شهروندان ایرانی می‌انجامد. پس باید نگرش به امنیت سایبری درون‌سرزمینی جاذبه‌محور باشد، ولی از جهت برون‌مرزی، دولت باید همواره سازوکارهای جنگ سایبری و دفاع سایبری را مد نظر داشته باشد. در اینجا، نقش دولت یا عامل بیگانه مطرح است، به گونه‌ای که ایران در سال‌های اخیر تهدیدهای واقعی سایبری را از این راستا آزموده است. پس، هر گونه اقدام سایبری برای دفع یورش‌های سایبری و جاسوسی‌های رایانه‌ای در قالب دفاع مشروع سایبری باید به عنوان برنامه و سیاست در این زمینه لحاظ شود و در هر حال، دولت باید قدرت خود را در این زمینه افزایش دهد و در برابر از کنترل‌های درون‌سرزمینی بکاهد.

آسیب‌ها و کاستی‌های امنیت سایبری ایران، چهره درون‌سرزمینی دارد که محدودسازی فضای سایبر در عمل به زیان شهروندان ایرانی می‌انجامد. پس باید نگرش به امنیت سایبری درون‌سرزمینی جاذبه‌محور باشد، ولی از جهت برون‌مرزی، دولت باید همواره سازوکارهای جنگ سایبری و دفاع سایبری را مد نظر داشته باشد