

شماره هشتم | مرداد ۱۴۰۵ | دانشگاه صنعتی شریف

byte Magazine



انجمن علمی دانشکده مهندسی کامپیوتر
نشریه علمی فرهنگی **بایت**

سرمقاله؛

مـا مـر د م

تیم بایت

استار لینک

تیم بایت

دوربین‌هایی که علیه

صاحبان‌شان چرخیدند!

تیم بایت

هدایت ترافیک اینترنتی با

تاکتیک‌های شناخته‌و‌ناشناخته

سعید فراتی کاشانی

ماشین کشتار هوشمند

(بخش اول)

Steve Feldstein

قطعی بزرگ! (بخش اول)

سورنا کیا

اینترنت، حق مسلم!

سورنا کیا

چگونه در دنیای اینترنت

ناشناس بمانیم؟

Amnam

ماشین کشتار هوشمند

(بخش دوم)

Steve Feldstein

مهندسی مقاومت

در برابر سانسور...

فرزام کوهی

شورش در لایه چهارم

محراب مرادزاده

ماماندیم و اینترنت پرو!

سورنا کیا

مردم، مقابل مردم!

تیم بایت

کاسبان قطعی اینترنت،

خوش‌حالید؟

امیرحسین شهیدی

قطعی بزرگ! (بخش دوم)

تیم بایت

مدیر مسئول

امیرحسین شهیدی

سردبیر

آرش شاه‌حسینی

صاحب امتیاز

انجمن علمی دانشکده مهندسی کامپیوتر دانشگاه صنعتی شریف

صفحه آرایی و گرافیک

فاطمه نیلفروشان - امیررضا جعفری - محمد پارسا آرنی - نرگس کاری - امیررضا اینانلو - آرش شاه‌حسینی - امیرحسین محمدزاده

تحریریه

سورنا کیا - سعید فراتی کاشانی - امیرحسین محمدزاده - فرزام کوهی - صهیب صادقی - امیرحسین صوری - فاطمه نیلفروشان - نرگس کاری - آروین بقال اصل - امیررضا جعفری

نویسندگان

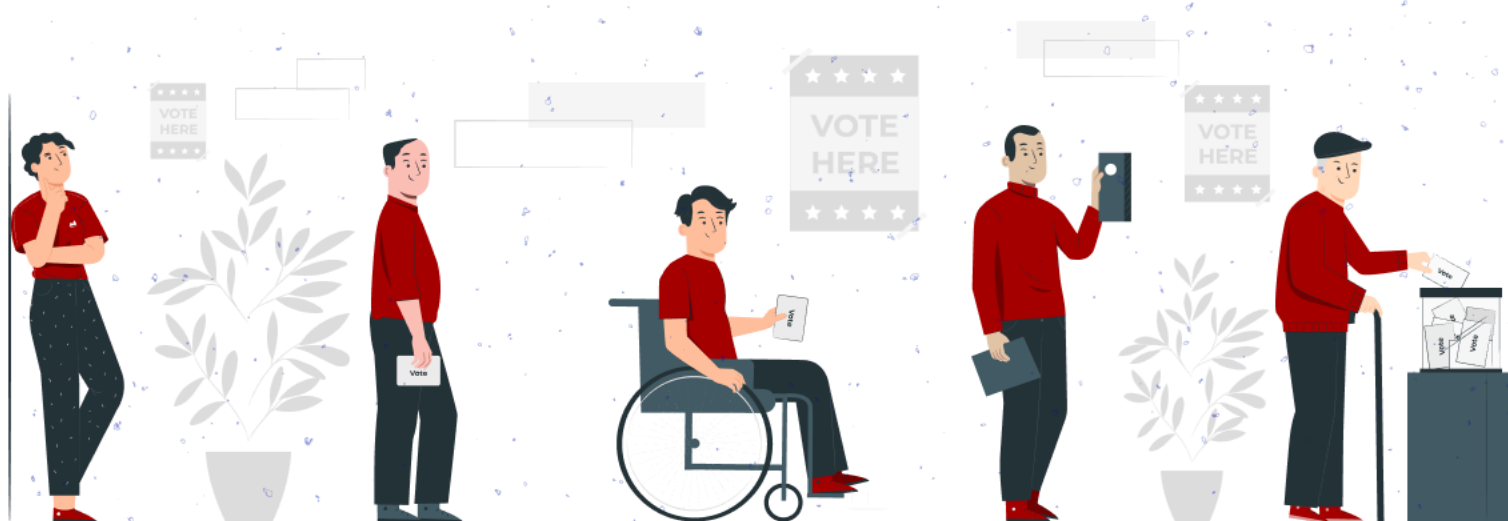
سعید فراتی کاشانی - سورنا کیا - Amnam - فرزام کوهی - محراب مرادزاده - امیرحسین شهیدی و تیم بزرگ بایت که از بردن نامشان در لیست تحریریه و نویسندگان معذوریم.

ویراستاری

امیرحسین صوری - صهیب صادقی - حسین زاهدی ادیب

فنی

معین آعلی



مردم

دانشگاه صنعتی شریف

تیم بایت

سانسور شدیم

b

۲ دقیقه

باز هم می‌گویند: «اکنون وقت گفت‌وگوست، وقت آرامش است. باید به شیوه درست اعتراض کرد!»

اما این پرسش‌های ساده، بی‌پاسخ باقی می‌مانند: وقتی قدرت، خود را در لباس مردم پنهان می‌کند؛ اعتراض دقیقاً خطاب به چه کسی است و باعث چه تغییری می‌شود؟

گفت‌وگو با چه کسی؟ و پس از چه چیزی؟

پس از این‌که دانشجورا «وحوش»، «قماش» و «یاغی» می‌نامید؟ وقتی اعتراض را «ارتداد» و مردم را مزدور دشمن می‌نامید؟

نمی‌توان دهه‌ها مردم را استثمار کرد و آینده‌شان را دزدید و بعد در نقش قربانی قرار گرفت و با تعجب پرسید: «چرا از ما متنفر هستید؟»

ما حرف داریم، اما نه باشما. آینده‌شان را دزدید و بعد در نقش قربانی قرار گرفت و با تعجب پرسید: «چرا از ما متنفر هستید؟»

برای آنان که صدایشان را بریدند؛ برای ستم‌دیدگان؛ برای مادرانی که هنوز چشم‌به‌راه عدالت‌اند؛ برای پدرانی که شرم فقر را هر شب با خود به خانه می‌برند؛ برای نسلی که آینده‌اش را گروگان گرفته‌اند.

ما سخن می‌گوییم برای این‌که بعد از آن همه

برای آن‌که خون ریخته‌شده، بذر آینده‌ای روشن‌تر شود.

ما می‌خواهیم از خود بپرسیم چگونه می‌شود ایدئولوژی‌ها چشم‌های ما را کور نکنند و حقیقت را قربانی شعار نکنیم.

آزادی را به بت تازه‌ای نفروشیم.

ما مثل شما نیستیم که عدالت‌خواهی را شعار کنیم و بعد گلوی مردم را با همان شعار بفشاریم. ما نه ستم را می‌پذیریم، نه ستم‌گر شدن را.

ما آزادی‌ای می‌خواهیم که اگر فرزندان روزی پرسید: «برای سرنوشت من چه کردی؟»

پاسخ دهیم: «کاری کردیم که تو خود، قلم تقدیرت را در دست بگیری؛ نه در سایه کسی زندگی کنی و نه در پرستش بتی تازه خم شوی.»

ما دنبال منجی نیستیم؛ ما دنبال انسانیم. هیچ قدرتی بالاتر از قانونی که مردم آن را نوشته‌اند، نفس نکشد.

زیرا قدرت تنها آن‌گاه حرمت دارد که از مردم برخیزد و به مردم بازگردد.

اگر قرار است از استبداد عبور کنیم، باید بیاموزیم چگونه عبور کنیم بی‌آن‌که استبداد دیگری بزاییم. این، شاید دشوارترین پرسش تاریخ ماست. اما تنها پرسشی است که اگر پاسخش را نیابیم، فردای ایران چیزی جز تکرار امروز نخواهد بود.

بدانید زمان صبور است ولی فراموش‌کار نیست و آه ستم‌دیده، حتی اگر در سکوت باشد، از هر بلندگویی رساتر است.

We the People

شاید برایتان جالب باشد که بدانید سرتیتر قانون اساسی کشور ایالات متحده آمریکا با عبارت «We the People» آغاز می‌شود؛ عبارتی که تأکید می‌کند منشأ مشروعیت، مردم‌اند نه حاکمان.

سخن اما از یک اصل ساده بود: (قدرت از مردم برمی‌خیزد و باید به مردم پاسخ دهد).

وقتی این اصل فراموش شود، قانون به ابزار سلطه بدل می‌شود.

واعراض،

تلاشی است

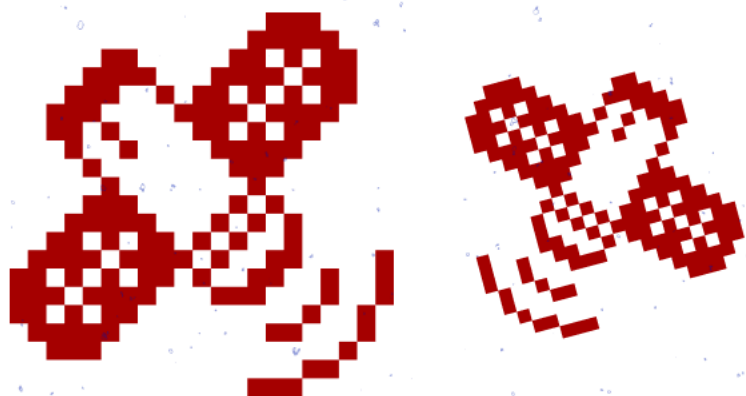
برای بازگرداندن

همان جمله نخست

به جایگاه حقیقی‌اش:

مأمردم.





استارلینک

جهان در عصر جدید، ایران در عصر حجر



در روزهای اخیر به دلیل قطع بی‌سابقه همه راه‌های ارتباطی و اینترنت در کشور، احتمالاً همگی نام استارلینک را شنیده‌ایم؛ شرکت و سامانه ارائه اینترنت ماهواره‌ای زیرمجموعه شرکت SpaceX ایلان ماسک که بخش بسیار گسترده‌ای از کره زمین از جمله ایران را پوشش داده و سرعت انتقال بسیار خوبی را هم فراهم می‌کند. در این مقاله می‌خواهیم نگاهی دقیق‌تر و فنی به نحوه کارکرد آن و توانایی ایجاد اختلال و شناسایی آن بیندازیم.

نبرد با Ping

در ابتدا باید توجه کنید که اینترنت ماهواره‌ای مقوله جدیدی نیست که ابداع‌کننده آن شرکت SpaceX باشد. پیش از این هم شرکت‌هایی وجود داشتند که اقدام به ارائه اینترنت ماهواره‌ای می‌کردند.

با این حال نوآوری اصلی شرکت SpaceX که نیازمند تلاش‌های مهندسی و علمی بسیار زیادی بوده، ارائه اینترنت در مدار LEO^۱ بوده‌است. اکثر ارائه‌دهندگان پیشین اینترنت، ماهواره‌ها را مدار زمین ثابت^۲ و در فاصله ۳۵٬۷۸۶ کیلومتری سطح زمین مستقر می‌کردند.

ویژگی خاص این فاصله این است که سرعت چرخش ماهواره‌ای که در این مدار قرار بگیرد به‌صورتی خواهد بود که عملاً همواره در بالای یک نقطه مشخص در زمین قرار دارد و لذا با مستقر کردن دریافت‌کننده‌ها در جهت ثابت، می‌توان به آن دسترسی پیدا کرد. ماهواره‌های مخابراتی نیز عموماً از این نوع هستند.

با این حال مدارهای زمین ثابت در زمینه ارائه اینترنت یک مشکل اساسی دارند و آن هم این است که انتقال داده‌ها صرفاً از ماهواره تا زمین و برگشت آن نیازمند زمان رفت و برگشتی حدود ۵۰۰ میلی‌ثانیه‌ای است. یعنی حتی با صرف‌نظر از تأخیرهای موجود در دستگاه‌ها، امکان دسترسی به تأخیر بهتر از ۵۰۰ میلی‌ثانیه به لحاظ قوانین فیزیک و سرعت نور وجود نخواهد داشت. از طرف دیگر، مدارهای Low Earth Orbit یا به اختصار LEO، به مدار ماهواره‌هایی با فاصله کمتر از ۲۰۰۰

کیلومتر در سطح زمین گفته می‌شود و واضح است که سرعت انتقال اطلاعات در این حالت بیش‌تر خواهد بود. به‌طور خاص ماهواره‌های استارلینک عموماً در فاصله ۵۵۰ کیلومتری سطح زمین قرار دارند و برنامه‌هایی برای ارسال بعضی ماهواره‌ها به مدار ۳۴۰ کیلومتری هم وجود دارد. این مدار امکان این که به تأخیری بین ۲۵ تا ۵۰ میلی‌ثانیه دست یابد را فراهم کرده که بسیار بهتر از اینترنت‌های قدیمی ماهواره‌ای است.

چالش‌های اینترنت ماهواره‌ای

با این حال چالش بزرگی که به وجود می‌آید، این است که دیگر ماهواره‌ها به لحاظ سرعت چرخش با سرعت چرخش زمین به دور خودش هماهنگ نخواهند بود و سرعت چرخش بسیار بیش‌تری خواهند داشت. هم‌چنین به دلیل نزدیک‌تر بودن به زمین، میدان دید کمتری هم دارند. لذا هر ماهواره نهایتاً می‌تواند زمانی بین ۳ تا ۱۵ دقیقه به یک کاربر ثابت روی زمین اینترنت‌رسانی کند. علاوه‌بر این، اگر تنها به کمک یک ماهواره بخواهیم ارتباط را برقرار کنیم، میدان دید ماهواره هم باید شامل کاربر و هم شامل سرورهای زمینی که با آن ارتباط برقرار کرده و دسترسی به اینترنت را فراهم می‌کنند، باشد که با توجه به فواصل این سرورها و هم‌چنین سرعت چرخش بالای ماهواره در اکثر اوقات امکان‌ناپذیر است.

راه‌حل استارلینک برای این موضوع، ارسال تعداد بسیار زیادی ماهواره به فضا است. طبیعتاً این راهکار هزینه اجرایی و عملیاتی بسیار بالایی دارد و امکان‌پذیر بودن آن از آن‌جا ناشی می‌شود که شرکت SpaceX عملاً خود به‌تنهایی امکان این که ارسال‌کننده ماهواره‌ها هم باشد را داشته است و با استفاده از موشک‌های Falcon ۹، می‌تواند هر بار تعداد زیادی ماهواره را به فضا منتقل کند. در نتیجه این موضوع، تا به حال بیش از ۱۰ هزار ماهواره استارلینک به فضا ارسال شده‌اند

و بخش بسیار گسترده‌ای از کره زمین را در پوشش خود قرار داده‌اند.

اما بعد از ارسال هم چالش‌های بسیار زیادی برای این ماهواره‌ها وجود دارد. از یک سو هماهنگی کاملی بین مانورهای مداری این ماهواره‌ها باید وجود داشته باشد و از سوی دیگر سامانه‌هایی گسترده برای مشخص کردن موقعیت آن‌ها برای سایر شرکت‌های فضایی و دولت‌ها باید تعیین بشود تا در پرتاب‌های خود، موقعیت این ماهواره‌ها را در نظر بگیرند. موضوعی که به‌خصوص با توجه به تعداد بالای آن‌ها در مداری با فاصله کم از زمین، از اهمیت ویژه‌ای برخوردار است.

علاوه‌بر آن، ماهواره‌هایی که در این ارتفاع قرار داشته باشند، در نهایت به‌دلیل مقاومت هوا حداکثر ۵ سال قابل استفاده هستند و بعد از آن در فرایندهای سقوط از پیش تعیین‌شده، وارد جو شده و منهدم می‌شوند. به‌طور خاص ماهواره‌های استارلینک از موادی ساخته شده‌اند که در هنگام ورود به جو زمین به‌طور کامل بسوزند و امکان برخورد بقایایی که امکان آسیب زدن به سازه‌ای در زمین را داشته باشد، بسیار کم بشود. ضمناً توجه کنید که هر چند در آن ارتفاع، فشار هوا بسیار کم‌تر است، اما هم‌چنان به شدت بیش‌تر از فشار هوا در ارتفاع ماهواره‌های زمین ثابت است.

حضور این ماهواره‌ها با این تعداد بالا در مدار نزدیک زمین، مشکلاتی را برای رصدخانه‌های زمینی نیز ایجاد می‌کند. به‌طور کلی ماهواره‌ها می‌توانند نور خورشید را بازتاب دهند و حتی هنگام شب در تصاویری که توسط تلسکوپ‌ها گرفته می‌شوند، اختلال ایجاد کنند.

خصوصاً این که این ماهواره‌ها حتی در بسیاری از اوقات با چشم غیرمسلح هم از روی سطح زمین به صورت نقاط نورانی در آسمان قابل مشاهده هستند. برای رفع این مشکل، استارلینک تحقیقات گسترده‌ای برای ساخت ماهواره از موادی با میزان انعکاس کم‌تر انجام داده و همچنین سامانه‌ها و API هایی برای اطلاع از موقعیت دقیق ماهواره‌ها ایجاد کرده‌است تا به رصدخانه‌ها در کاهش اثرات انعکاسی این ماهواره کمک کند، هر چند که همچنان انتقادات زیادی از سوی جوامع علمی نجومی نسبت به تأثیرات سوء تعداد زیاد ماهواره بر پروژه‌های رصدی وجود دارد.

ارتباط با زمین و مسیریابی

قسمت دیگر چالش‌ها، مسائل مربوط به علوم مخابرات و همچنین مهندسی و علوم کامپیوتر است.

با توجه به این که در فواصل زمانی چند دقیقه‌ای باید ارتباط با یک ماهواره جدید برقرار شود و ردیابی آن‌ها به صورت فیزیکی توسط گیرنده‌های زمینی کار دشوار و نیازمند انرژی زیادی است، در ترمینال‌های زمینی استارلینک که توسط کاربر استفاده می‌شود، از روشی موسوم به آرایه‌های اسکن فعال الکترونیکی (AESA) استفاده می‌شود که با استفاده از آرایه‌های فازی و به شکل الکترونیکی، می‌توانند جهت دریافت و ارسال امواج رادیویی را بدون نیاز به تغییر موقعیت فیزیکی، مداوم جهت‌دهی کنند.

خود ماهواره هم از سه محدوده فرکانسی موسوم به E-Band، Ku-Band، Ka-Band و استفاده می‌کند که Ku-Band مختص به ارتباط با کاربر بوده و دو محدوده دیگر که فرکانس بالاتری هم دارند برای ایجاد ارتباط با پهناهای باند بالا با سرورها و Gateway های زمینی که اتصال با اینترنت را برقرار می‌کنند، استفاده می‌شود.

ساختار استفاده‌شده در ترمینال‌های کاربران (یا به عبارت رایج‌تر دیش استارلینک) هم متشکل از فناوری‌های پیشرفته مخابراتی و همچنین پردازش سیگنال است.

ترمینال استارلینک یک برد مدار چاپی با قطر ۵۰ سانتی‌متر دارد که از شبکه‌ای از آنتن‌های شش ضلعی تشکیل شده‌است.

۶۳۲ میکروچیپ هر کدام با دو آنتن ارتباط داشته و توسط ۷۹ آرایه مشبک توپی (BGA) که محافظ‌های قوی دفع گرمایی دارند، کنترل می‌شوند. کل سامانه هم در نهایت توسط یک SoC مرکزی با سیستم‌های پیشرفته پردازش سیگنال کنترل می‌شود که براساس GPS^۳ داخلی دستگاه، می‌تواند به شکل مداوم محاسبات مربوط به ارتباط با ماهواره‌ها را انجام بدهد.

نکته مهم دیگر مسئله مسیریابی در شبکه است. پروتکل‌های رایج شبکه نظیر BGP^۴ و جداول مسیریابی ثابت، اساساً برای شبکه‌های فیزیکی رایجی که به ندرت به لحاظ فیزیکی تغییر مکان می‌دهند، طراحی شده‌اند. این موضوع برای ماهواره‌ای که با سرعت ۷/۵ کیلومتر در ثانیه (۲۷۰۰۰ کیلومتر در ساعت) در حرکت است، صادق نیست.

بسیاری از این پروتکل‌ها بر مبنای پیدا کردن کوتاه‌ترین مسیر یا کوتاه‌ترین تأخیر طراحی شده‌اند. با این حال، اجرای چنین روشی در مورد ارتباطات ماهواره‌ای می‌تواند منجر به این شود که ناگهان یک ماهواره به شدت مورد ازدحام درخواست قرار بگیرد و ماهواره‌های دیگر بدون استفاده باقی بمانند. به همین منظور الگوریتم‌های ویژه و اختصاصی طراحی شده‌اند که تحت چارچوبی به نام SKYLINK شناخته می‌شوند.

کلید اصلی SKYLINK اولویت دادن به ارتباطات بین ماهواره‌ای است. ماهواره‌های استارلینک از طریق شبکه پیشرفته‌ای از ارتباطات نوری که نزد بسیاری با عنوان لیزر فضایی شناخته می‌شود، ارتباط برقرار کرده و می‌توانند ترافیک را به یک دیگر انتقال بدهند.

نکته بسیار مهم این است که نور در فضا می‌تواند با سرعتی

بیش از ۴۰ درصد سرعت کابل‌های فیبر نوری زمینی انتقال پیدا کند. برای همین در بسیاری موارد می‌توان انتقال اطلاعات را در فضا سریع‌تر از انتقال آن به سرورهای زمینی و جابه‌جایی در فیبرهای نوری انجام داد؛ لذا در نظر گرفتن ارتباطات بین ماهواره‌ها و انتقال اطلاعات بین آن‌ها هم به لحاظ سریع‌تر بودن نسبت به شبکه‌های زمینی و هم به جهت کاهش ازدحام و بار شبکه اهمیت بالایی دارد و الگوریتم‌های طراحی‌شده برای استارلینک همه این موارد را در نظر می‌گیرند و بر آن اساس بهترین ماهواره برای برقراری ارتباط را انتخاب می‌کنند.

شناسایی استارلینک

در نهایت هم باید به روش‌هایی که می‌توانند باعث شناسایی یا ایجاد اختلال در استارلینک بشوند اشاره کرد. با توجه به این که مقالات آزاد زیادی در این مورد وجود ندارد، می‌توان فقط به برخی حدس و گمان‌ها و یا روش‌های تئوری که احتمال پیاده‌سازی دارند، اشاره کرد.

از جمله آن‌ها این است که برای شناسایی وجود ترافیک استارلینک در یک شبکه در صورتی که اتصال به یک کاربر برای مدت زیادی برقرار باشد، می‌توان به تغییرات در ping آن کاربر توجه کرد. به دلیل جابه‌جایی بین ماهواره‌های استارلینک در فاصله‌های چند دقیقه‌ای یا حتی بعضاً کمتر از یک دقیقه، معمولاً جهش‌های محسوسی در نرخ تأخیر در هنگام این جابه‌جایی ایجاد می‌شود که ناشی از انجام پردازش‌های تغییر به ماهواره جدید و استفاده از ماهواره دیگر با نرخ تأخیر متفاوت است.

این الگو در صورت رصد شدن به صورت نمودار دندانه‌ای^۵ قابل مشاهده است. به علاوه در فواصل نزدیک می‌توان با اسکن کردن فرکانس‌های Wi-Fi موجود و بررسی Mac Address دستگاه‌ها تا حدی متوجه حضور روترهای استارلینک در یک محدوده شد. هر چند چنین روش‌هایی عملاً نیاز به بررسی محله به محله و خیابانی دارد و به شکل گسترده به راحتی قابل استفاده نیستند.

در کنار همه این‌ها باید توجه کرد که در صورت استفاده از VPN، آی‌پی استارلینک در بازه مشخصی قرار دارد.



دانستنی‌های رندوم!

Iran built a vast camera network to control dissent. Israel hacked it

تیتروژنامه Los Angeles Times در مورد دسترسی اسرائیل به دوربین‌های نظارتی در ایران

نفوذ سایبری اسرائیل به شبکه دوربین‌های کشور، از نظارت ترافیک تا عملیات هدف‌گذاری هوشمند

در سال‌های اخیر، افشاگری‌های متعدد از سوی رسانه‌های معتبر بین‌المللی، پرده از یکی از گسترده‌ترین و حساس‌ترین عملیات‌های سایبری علیه زیرساخت‌های شهری ایران برداشته است. اسناد و گزارش‌هایی که توسط خبرگزاری‌هایی نظیر آسوشیتدپرس، اسرائیل تایمز و شبکه سی‌ان‌ان منتشر شده، همگی حاکی از آن است که رژیم اسرائیل موفق شده است تا برای سال‌ها به شبکه گسترده دوربین‌های نظارت ترافیکی و شهری در ایران نفوذ کرده و از آن به عنوان یک ابزار اطلاعاتی پیشرفته استفاده کند.

ابعاد فنی و عملیاتی نفوذ

بر اساس گزارش‌های تأییدشده، این نفوذ که گاه از آن به عنوان دسترسی سطح بالا یاد می‌شود، تقریباً تمامی دوربین‌های ترافیکی مستقر در معابر و تقاطع‌های اصلی تهران را در بر می‌گرفته است. یک مقام ارشد اطلاعاتی اسرائیل در گفت‌وگو با Times Of Israel اذعان کرده که تیم‌های سایبری این کشور، سال‌ها پیش موفق به نفوذ به این شبکه شده‌اند و تهران را به اندازه شهر اورشلیم برای خود شناخته‌شده و شفاف ساخته‌اند. وی اشاره می‌کند که داده‌های تصویری جمع‌آوری شده به صورت لحظه‌ای به سرورهای اسرائیل منتقل شده و با استفاده از الگوریتم‌های پیشرفته هوش مصنوعی پردازش می‌شوند.

کاربرد راهبردی: ردیابی و هدف‌گذاری

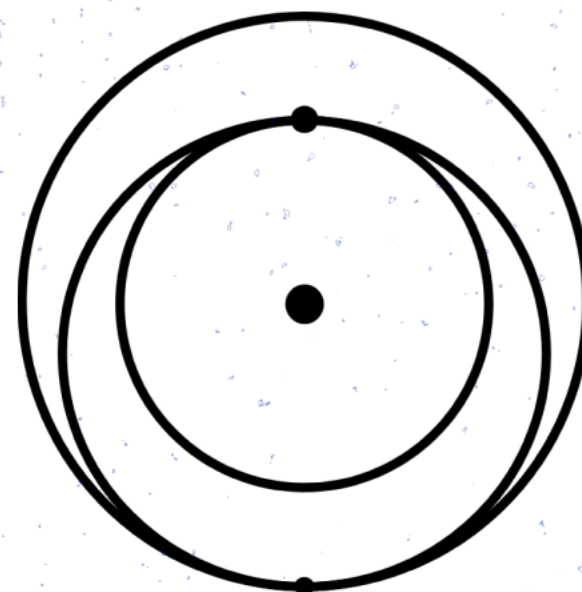
مهم‌ترین دستاورد این عملیات سایبری برای طرف اسرائیلی، قابلیت ردیابی بی‌وقفه محافظان و خودروهای حامل مقامات ارشد نظامی و امنیتی ایران بوده است. نشریه Wired و شبکه NPR در تحلیل‌های خود، این سامانه را به عنوان یک دستگاه تولید هدف مبتنی بر هوش مصنوعی توصیف کرده‌اند که حجم عظیمی از ویدیوها را غربال کرده و الگوهای حرکتی و رفتاری اهداف موردنظر را استخراج می‌کند. این قابلیت، نقشی حیاتی در عملیات‌های ترور و انهدام هدفمند چهره‌های کلیدی در خاک ایران و منطقه داشته است.

علت اصلی آسیب‌پذیری

تحلیل‌گران امنیتی در لس‌آنجلس تایمز، علت اصلی موفقیت این نفوذ گسترده را به سه عامل کلیدی نسبت داده‌اند؛ نخست، **تحریم‌های بین‌المللی** که تأمین تجهیزات به‌روز و مطمئن امنیت سایبری را برای ایران با دشواری مواجه ساخته و منجر به استفاده از سیستم‌های قدیمی یا غیراستاندارد در زیرساخت‌های شهری شده است؛ دوم، وجود نداشتن به‌روزرسانی‌های منظم امنیتی در این شبکه‌های نظارتی که عملاً درهای ورودی را برای حملات سایبری پیچیده گشوده است؛ و سوم، شبکه گسترده و رده‌بالای جاسوسان اسرائیلی که در فروش قطعات سخت‌افزاری و حتی برنامه‌های تشخیص چهره آلوده به سازمان‌های امنیتی تأثیرگذار بوده‌اند.

آنچه از مجموع گزارش‌های معتبر بین‌المللی برمی‌آید، تصویر روشنی از یک شکاف امنیتی جدی و طولانی‌مدت در یکی از حساس‌ترین زیرساخت‌های شهری ایران است که به نظر می‌رسد ریشه‌هایش به دوران استاکس‌نت باز می‌گردد. هک دوربین‌های رسمی دولتی و حتی خصوصی توسط اسرائیل، نمونه‌ای بارز از تبدیل یک ابزار ساده شهری به سلاحی قدرتمند در عرصه جنگ‌های مدرن و اطلاعاتی محسوب می‌شود. این رویداد، نه تنها ابعاد نظامی و امنیتی دارد، بلکه نشان‌دهنده تغییر رویکرد از جنگ‌های سنتی به سمت بهره‌گیری از داده‌های کلان در عرصه رویارویی‌های بین‌المللی است. وجود مدل‌های زبانی پیشرفته و کاهش زمان موردنیاز برای تحلیل میلیاردها داده، بار دیگر ثابت می‌کند که امنیت سایبری و حفاظت از داده‌ها تا چه حد اهمیت حیاتی دارد.

که به راحتی قابل تشخیص است و هر چند از طریق آن نمی‌توان به مکان روتر دست یافت، ولی می‌توان متوجه شد که فردی از طریق استارلینک از سایت یا سرویس مدنظر بازدید کرده است.



STARLINK

اختلال در استارلینک

برای مسدودسازی استارلینک، روش‌های ایجاد نویز و جَمینگ روی فرکانس‌های مورد استفاده آن می‌تواند به عنوان یکی از روش‌ها مورد استفاده قرار بگیرد.

هر چند با توجه به این که استارلینک در بازه فرکانسی Ku-band که بین ۱۰٫۷ تا ۱۲٫۷ گیگاهرتز است، فعالیت می‌کند و این بازه با بازه مورد استفاده در برخی سیستم‌های نظامی هوایی تداخل دارد، ایجاد نویز و جَمینگ روی آن نیازمند استفاده از جمرهای نظامی قدرتمند است و نمی‌تواند به شکل گسترده مورد استفاده قرار بگیرد.

روش دیگری که می‌تواند مورد استفاده قرار بگیرد و به نظر می‌رسد در قطعی‌های اخیر هم از آن استفاده شده بود - حال یا برای ایجاد اختلال در استارلینک یا به دلایل دیگری که به شکل ثانویه روی استارلینک اثر گذاشت - ایجاد اختلال در سامانه‌های موقعیت‌یاب و GPS است.

با توجه به اتکای استارلینک به این سامانه‌ها برای شروع به کار و برقراری ارتباط اولیه، در صورتی که اختلال شدیدی در GPS وجود داشته باشد این موضوع می‌تواند باعث بروز مشکل در ایجاد ارتباط اولیه شود. هر چند که اثر این موضوع بعد از برقراری اتصال اولیه کمتر می‌شود، اما به طور کلی می‌تواند به عنوان یک روش مؤثر برای جلوگیری از اتصال استفاده شود.

هدایت ترافیک اینترنتی با تاکتیک‌های شناخته‌ناشناخته

دانشگاه صنعتی شریف

سعید فراتی کاشانی

۴ دقیقه

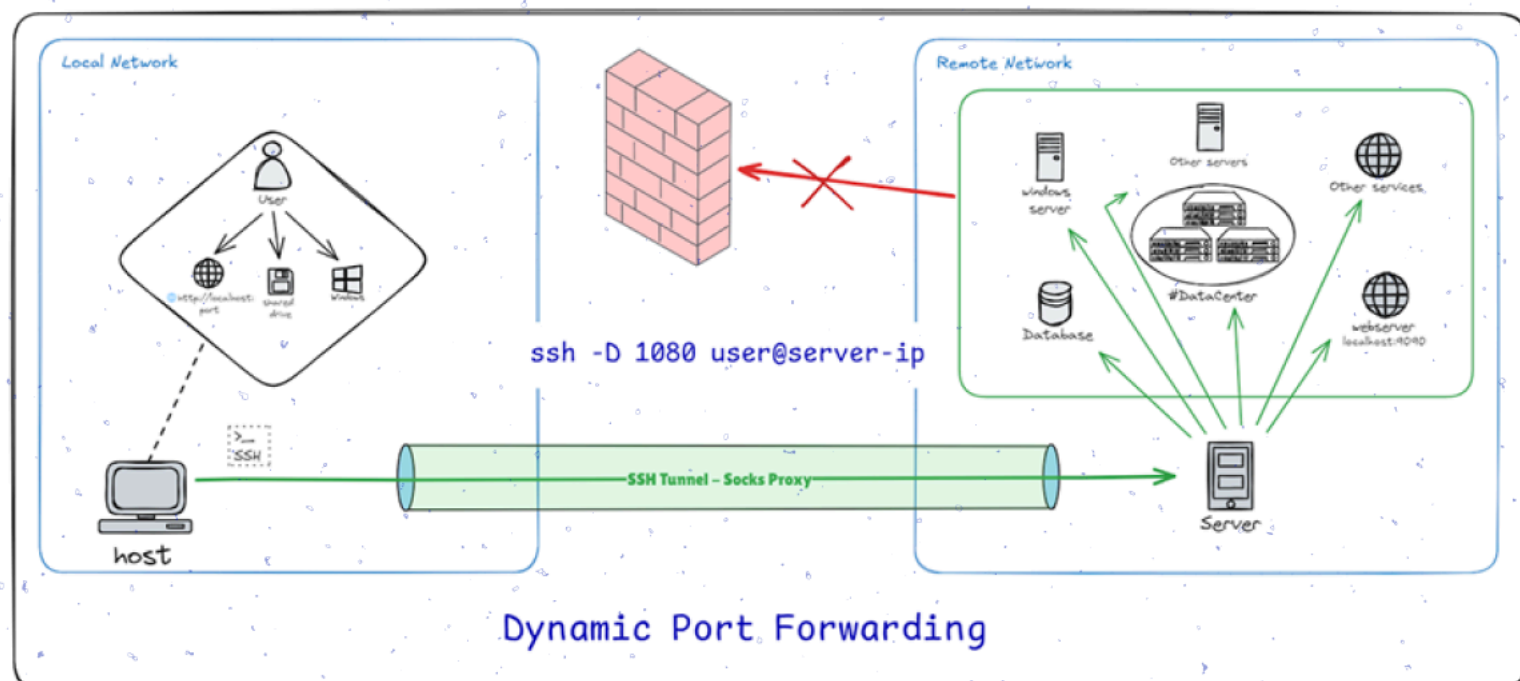
کارشناسی ۱۴۰۱



در دنیای امروز، گاهی محدودیت‌های اینترنتی باعث می‌شوند دسترسی به سرویس‌ها و اطلاعات مورد نیاز دشوار شود. در چنین شرایطی، هدایت ترافیک اینترنت از مسیرهای غیرمستقیم و امن، راهکاری مؤثر برای حفظ دسترسی و امنیت است. ابزارهایی مانند پروکسی‌ها و تونل‌های SSH یا VPN به داده‌ها اجازه می‌دهند بدون آن‌که مسیر و محتوای آن‌ها به سادگی قابل رهگیری باشد، ابتدا از یک نقطه واسط عبور کنند و سپس به مقصد نهایی برسند. به این ترتیب، کاربران می‌توانند هم از اطلاعات خود محافظت کنند و هم از محدودیت‌های شبکه عبور کنند؛ روش‌هایی که در ادامه با مثال و ترندهای عملی به آن‌ها خواهیم پرداخت.

تونل‌سازی با SSH؛ روشی برای عبور امن ترافیک

به قول یکی از اساتیدمان، «SSH is all you need!». یکی از روش‌های ساده و امن برای هدایت ترافیک اینترنتی از مسیرهای غیرمستقیم، استفاده از SSH است. SSH به‌طور معمول برای دسترسی به سرورها و مدیریت از راه دور استفاده می‌شود، اما افزون بر این، می‌تواند برای تونل‌سازی و هدایت داده‌ها از طریق یک مسیر امن نیز به کار رود. مزیت مهم SSH در نگاه ساده این است که تقریباً به‌صورت پیش‌فرض روی اکثر سرورهای مجازی و VPS‌ها نصب و فعال است، نیاز به راه‌اندازی پیچیده یا نرم‌افزار خاصی ندارد و از رمزنگاری قوی و امتحان پس‌داده‌ای استفاده می‌کند. در این روش، شما از یک سرور میانه (معمولاً یک سرور قابل دسترسی از طریق SSH) برای هدایت ترافیک اینترنتی خود استفاده می‌کنید و داده‌ها به‌صورت رمزگذاری شده از دستگاه شما عبور می‌کنند. همین در دسترس بودن، سادگی و امنیت مناسب باعث شده SSH برای بسیاری از



پس‌زمینه) و -p (تعیین پورت اتصال به سرور SSH) هم در سناریوهای تونل‌سازی بسیار کاربردی هستند.

اگر هم رابطه خوبی با ترمینال ندارید، می‌توانید از نرم‌افزارهایی مانند NetMod برای ویندوز یا Nekobox برای اندروید استفاده کنید و مشخصات سرورتان را به‌صورت دستی به‌عنوان SSH، اضافه کنید. حالا اگر به این روش علاقه‌مند شدید، می‌توانید درباره آن بیشتر مطالعه کنید. مطالعه پیرامون روش‌های مرتبط با تونل معکوس (Reverse SSH Tunnel) را به شما پیشنهاد می‌کنم.

اشتراک‌گذاری اینترنت با پروکسی در شبکه داخلی

گاهی اوقات ممکن است بخواهید اینترنت گوشی یا لپ‌تاپ خود را با دیگر دستگاه‌ها در شبکه محلی به اشتراک بگذارید. این کار زمانی می‌تواند مفید باشد که شما نیاز دارید به منابع یا سرویس‌هایی دسترسی داشته باشید که فقط از طریق یک پروکسی خاص قابل دسترسی هستند.

برخی نرم‌افزارها، مانند V2Ray یا NekoBox، به‌طور پیش‌فرض یک پراکسی SOCKS روی پورت‌های خاص (مثلاً ۱۰۸۰۸ برای V2Ray یا ۲۰۸۰ برای NekoBox) روی دستگاه شما ایجاد می‌کنند. این پروکسی‌ها برای هدایت ترافیک اینترنت به‌طور امن و رمزگذاری شده طراحی شده‌اند. اما نکته‌ای که می‌تواند مفید باشد این است که اکثر این برنامه‌ها داخل تنظیمات خود، گزینه‌ای به نام Allow connections from LAN دارند. اگر این گزینه را فعال کنید، دستگاه‌های دیگر در شبکه محلی می‌توانند از پروکسی SOCKS شما استفاده کنند. آن‌ها کافیست با وارد کردن آدرس IP دستگاه شما (مثلاً IP گوشی شما یا لپ‌تاپی که پروکسی را

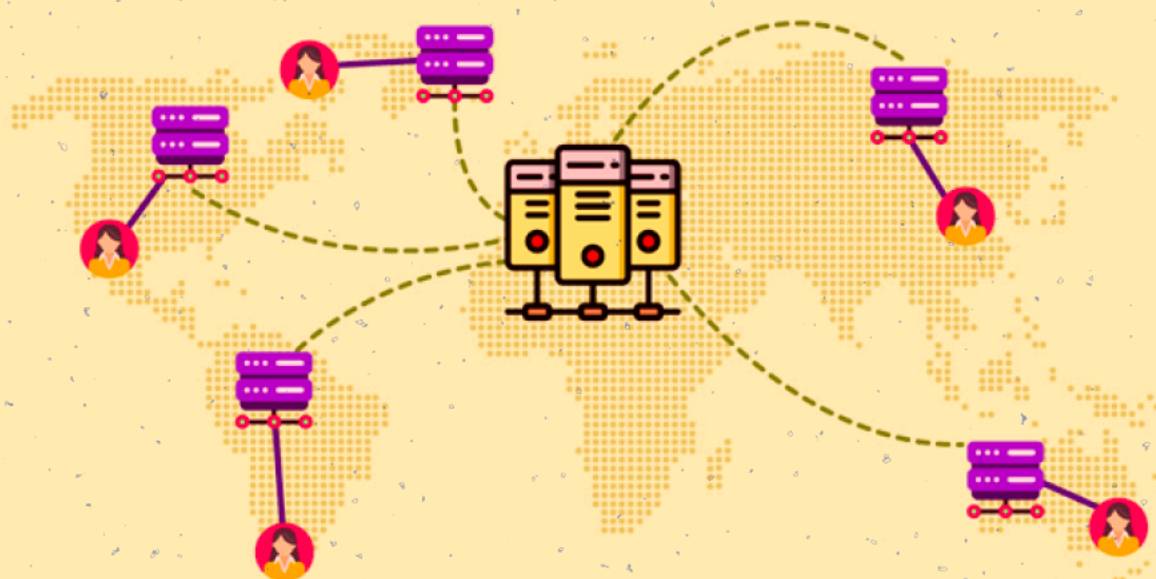
کاربران، اولین و دم‌دست‌ترین ابزار تونل‌سازی باشد.

یکی از رایج‌ترین انواع تونل‌سازی با SSH، تونل پویا (Dynamic Forwarding) است. در تونل پویا، یک پورت محلی روی سیستم شما باز می‌شود که به‌طور خودکار داده‌ها را از طریق سرور SSH به مقصد نهایی هدایت می‌کند. برای مثال، با استفاده از فرمان زیر، یک تونل پویا روی پورت ۱۰۸۰ ایجاد می‌کنید که از طریق آن می‌توانید از پروکسی SOCKS برای استفاده از اینترنت بهره ببرید:

```
ssh -D 1080 user@server
```

در این حالت، با تنظیم پروکسی در مرورگر یا برنامه‌هایی که از SOCKS پشتیبانی می‌کنند (مثل تلگرام یا فایرفاکس)، ترافیک اینترنتی شما از طریق سرور میانه هدایت می‌شود و تمام اطلاعات بین شما و سرور رمزگذاری می‌شود. این را هم بگوییم که در این حالت، باید آدرس سرور را برابر با localhost قرار دهید، از پورت ۱۰۸۰ استفاده کنید و نام کاربری و گذرواژه را نیز خالی بگذارید. افزون بر فلگ -D که برای تونل پویا استفاده می‌شود، چند فلگ رایج دیگر هم در SSH وجود دارد؛ به‌عنوان مثال، -L برای Local Port Forwarding است و یک پورت روی دستگاه شما را به یک مقصد مشخص در سمت سرور یا شبکه پشت آن متصل می‌کند (مثلاً دسترسی به پایگاه داده داخلی). -R برای Remote Port Forwarding یا همان تونل معکوس است و یک پورت روی سرور باز می‌کند تا به سیستم محلی شما وصل شود (مناسب وقتی که پشت NAT هستید). -J یا Jump Host برای اتصال زنجیره‌ای از طریق یک یا چند سرور واسط استفاده می‌شود تا بدون ورود جداگانه، به مقصد نهایی برسید. همچنین فلگ‌هایی مثل -N (اجرا نشدن پوسته shell- و فقط ایجاد تونل)، -f (ارسال SSH به

Content Delivery Networks



راه اندازی کرده‌اید) و پورت مربوطه (مثلاً پورت ۸۰۸۰ یا ۲۰۸۰)، ترافیک خود را از طریق پروکسی شما عبور دهند.

برای کاربران اندروید، یکی دیگر از راه‌های محبوب برای اشتراک‌گذاری اینترنت، استفاده از نرم‌افزار Every Proxy است. این برنامه به شما این امکان را می‌دهد که پس از تونل کردن تمام ترافیک گوشی با نرم‌افزاری دیگر، یک پروکسی SOCKS یا HTTP محلی ایجاد کنید. با این کار، می‌توانید از گوشی خود به عنوان یک Gateway اینترنتی برای دیگر دستگاه‌های موجود در شبکه محلی استفاده کنید.

امنیت و خطرات احتمالی

گاهی اوقات برای کاربران این پرسش به وجود می‌آید که آیا استفاده از کانفیگ‌های موجود در بسترهای عمومی، امنیت آن‌ها را به خطر می‌اندازد؟ در ادامه به پاسخ این پرسش می‌پردازیم. ابزارهایی مانند V2Ray به طور کلی امنیت بالایی دارند و با استفاده از رمزگذاری قوی، از داده‌های شما در برابر شنود محافظت می‌کنند. حتی اگر سرور را خودتان راه‌اندازی نکرده باشید، مدیر سرور ممکن است به متادیتا (مانند آدرس‌های IP و زمان‌های اتصال) دسترسی داشته باشد، اما این به معنای شنود محتوای ترافیک نیست، چون ارتباطات معمولاً به صورت رمزگذاری شده منتقل می‌شوند. علاوه بر این، بیشتر سایت‌هایی که ما به آن‌ها مراجعه می‌کنیم، به‌ویژه سایت‌های بانکی و خدماتی، از پروتکل HTTPS برای رمزگذاری ارتباطات استفاده می‌کنند، بنابراین حتی در صورت استفاده از این ابزارها، نگرانی جدی‌ای بابت امنیت وجود ندارد.

وقتی شانس، در خانه را می‌زد

در برخی دوره‌ها، با وجود محدودیت شدید دسترسی به اینترنت، سرویس‌هایی مانند ChatGPT در دسترس قرار می‌گرفتند. در این حالت، یک راه خلاقانه نیز قابل استفاده می‌شود. دلیل اصلی این موضوع، استفاده این سرویس‌ها از زیرساخت‌هایی مانند Cloudflare بود. Cloudflare به عنوان یک CDN^۱، به صورت واسطه‌ای میان کاربر و سرور اصلی عمل می‌کند و بسیاری از دامنه‌های مختلف را روی مجموعه‌ای از IP های مشترک

یکی دیگر از مواردی که جالب است درباره آن بدانیم، ECH^۵ است. ECH بخشی از TLS به حساب می‌آید که نام دامنه مقصد را در handshake اولیه رمزگذاری می‌کند و باعث می‌شود شناسایی سرویس‌ها با DPI به دلیل مخفی شدن SNI، دشوار شود. اگر علاقه‌مند هستید، می‌توانید جزئیات بیشتر آن را در منابع تخصصی مطالعه کنید.

جست‌وجو آزاد!

در برخی مقاطع محدودسازی اینترنت، مشاهده می‌شد که سرویس جست‌وجوی گوگل همچنان در دسترس است، در حالی که سایر خدمات گوگل مانند Gmail، Google Drive یا Google Accounts مسدود بودند. دلیل این رفتار، تفاوت در نحوه ریزالو شدن نام دامنه‌ها (DNS resolution) و سیاست‌های مسدودسازی مبتنی بر دامنه بود. در این شرایط، دامنه‌هایی مانند google.com به یک یا چند IP مشخص پاسخ می‌دادند که در لایه فیلترینگ مسدود نشده بودند و امکان برقراری اتصال TCP به آن‌ها وجود داشت. وقتی DNS به صورت عادی ریزالو نمی‌شود یا پاسخ متفاوتی برمی‌گرداند، می‌توان نام دامنه‌های دیگر گوگل را به صورت دستی به همان IP مجاز نگاشت کرد. این کار باعث می‌شود سیستم عامل، بدون پرس‌وجوی DNS، مستقیماً به آن IP متصل شود؛ در نتیجه اگر مسدودسازی صرفاً در لایه DNS یا دامنه باشد، اتصال برقرار می‌شود. برای این کار کافی است فایل hosts سیستم را ویرایش کنید.

میزبانی می‌کند. در چنین شرایطی، برخی دامنه‌ها در لایه اینترنت کشور، مجاز تلقی می‌شدند و اتصال به آن‌ها مسدود نمی‌شد. پیش از ورود به این بحث، بد نیست سه مفهوم کلیدی را خیلی خلاصه مرور کنیم. TLS^۲ پروتکل رمزنگاری‌ای است که ارتباط بین کاربر و سرور را امن می‌کند و همان چیزی است که پشت HTTPS قرار دارد. در ابتدای برقراری این ارتباط، بخشی به نام SNI^۳ ارسال می‌شود که نام دامنه مقصد را مشخص می‌کند. از سوی دیگر، DPI^۴ روشی برای بازرسی عمیق بسته‌های شبکه توسط فایروال‌ها یا سامانه‌های فیلترینگ است که می‌تواند بر اساس اطلاعاتی مثل SNI، نوع ترافیک یا الگوهای خاص، اتصال‌ها را شناسایی و مسدود کند.

در این میان، مفهوم SNI نقش مهمی دارد. همان‌طور که گفته شد، SNI بخشی از فرآیند آغازین ارتباط TLS است که در آن نام دامنه مقصد پیش از رمزگذاری کامل ارسال می‌شود. برخی کاربران با تنظیم کانفیگ‌هایی مانند VLESS به گونه‌ای که SNI در آن برابر با دامنه‌هایی مانند ChatGPT باشد، موفق می‌شدند مرحله اولیه اتصال را بدون انسداد پشت سر بگذارند. از آن‌جا که Cloudflare ترافیک را پس از این مرحله به صورت رمزگذاری شده عبور می‌دهد، این اتصال می‌توانست عملاً به مسیری برای دسترسی گسترده‌تر به اینترنت تبدیل شود؛ رویکردی که از نظر مفهومی به تکنیک‌هایی مانند domain fronting شباهت دارد، هرچند معمولاً موقتی است و با تغییر سیاست‌ها از کار می‌افتد.

در ویندوز:

C:\Windows\System32\drivers\etc\hosts

و در لینوکس و مک:

/etc/hosts

و دامنه‌های موردنظر را به IP ای که برای گوگل باز است، نگاشت کنید. مثلاً در تصویر زیر، چند مورد آورده شده است.

```
216.239.38.120 drive.google.com
216.239.38.120 docs.google.com
216.239.38.120 sheets.google.com
216.239.38.120 forms.google.com
```

Chisel و GOST؛ طراحی مسیر، نه فقط ساخت تونل

گاهی مسئله فقط «داشتن پروکسی» نیست، بلکه ساختن یک مسیر هوشمند بین دو نقطه است. فرض کنید یک دستگاه دارید که به اینترنت بین‌الملل متصل است و دستگاهی دیگر که فقط به شبکه داخلی دسترسی دارد. هدف این است که اینترنت سیستم اول، به نوعی در اختیار سیستم دوم قرار بگیرد. در چنین سناریویی، ابزارهایی مانند Chisel و GOST می‌توانند نقش یک پل ارتباطی منعطف را ایفا کنند.

در یک سناریوی رایج، سیستم داخلی (که محدود است) اجازه دارد اتصال خروجی برقرار کند، اما از بیرون نمی‌توان به‌طور مستقیم به آن وصل شد. این دقیقاً همان حالتی است که تونل معکوس (Reverse Tunnel) معنا پیدا می‌کند. روی سیستم دارای اینترنت آزاد، Chisel را در حالت سرور اجرا می‌کنیم و اجازه ایجاد تونل معکوس می‌دهیم. سپس روی سیستم داخلی، کلاینت Chisel اجرا می‌شود و به سرور متصل می‌شود. نکته مهم این‌جاست که اتصال از داخل آغاز می‌شود؛ بنابراین حتی اگر سیستم داخلی پشت NAT یا فایروال باشد، مانعی برای برقراری تونل ایجاد نمی‌شود.

پس از اتصال، می‌توان روی سیستم داخلی یک پروکسی SOCKS محلی ایجاد کرد. در این حالت، کافی است مرورگر یا نرم‌افزارهای دیگر را روی SOCKS تنظیم کنیم تا تمام ترافیک آن‌ها

از طریق تونل به سرور خارجی هدایت شود.

حالا اگر Chisel را یک تونل ساده و کارآمد بدانیم، GOST بیشتر شبیه یک جعبه ابزار شبکه است. سناریوی پایه همان است: یک سرور خارج از کشور با اینترنت آزاد، و یک کلاینت داخل شبکه محدود. اما GOST اجازه می‌دهد نوع انتقال، نحوه کپسوله‌سازی و حتی زنجیره پروکسی‌ها را خودمان طراحی کنیم. مزیت مهم GOST این است که می‌توان این ارتباط را داخل Websocket، TLS یا حتی چند لایه متوالی کپسوله کرد. برای مثال، می‌توان ترافیک را به صورت SOCKS داخل TLS اجرا کرد تا از دید شبکه شبیه یک ارتباط HTTPS معمولی باشد، یا حتی چند پروکسی را زنجیره‌ای کرد تا مسیر ترافیک چندمرحله‌ای شود.

آیا ترافیک ما قابل تشخیص است؟

یکی از پرسش‌های رایج پیرامون ابزارهای تونل‌سازی این است که آیا ترافیک آن‌ها از دید شبکه یا اپراتور قابل تشخیص است یا نه. پاسخ کوتاه این است که بله، اغلب قابل تشخیص‌اند؛ اما میزان و دقت تشخیص متفاوت است. این تفاوت به نوع پروتکل، الگوی ترافیک و میزان شباهت آن به ترافیک عادی اینترنت بستگی دارد. OpenVPN به‌طور پیش‌فرض الگوی نسبتاً مشخصی دارد. اگر روی UDP و پورت‌های غیرمعمول اجرا شود، تشخیص آن برای سیستم‌های DPI ساده‌تر است، زیرا ساختار بسته‌ها و handshake آن با ترافیک وب معمولی تفاوت دارد. اجرای OpenVPN روی TCP و پورت ۴۴۳ می‌تواند تشخیص را سخت‌تر کند، اما همچنان در بسیاری از موارد، الگوی رفتاری آن (packet size، timing و renegotiation) قابل تمایز است. به همین دلیل، OpenVPN از نظر امنیت رمزنگاری قوی است، اما از نظر «استتار ترافیک» چندان ایده‌آل نیست.

در مقابل، پروتکل‌هایی مانند VMess و VLESS (به‌ویژه وقتی روی TLS و CDN اجرا می‌شوند) طوری طراحی شده‌اند که ترافیک آن‌ها تا حد زیادی شبیه HTTPS معمولی به نظر برسد. در این حالت، تشخیص دقیق نیازمند تحلیل‌های عمیق‌تری در لایه‌های بالاتر یا بررسی الگوهای رفتاری طولانی‌مدت است. با این حال،

حتی این روش‌ها هم کاملاً نامرئی نیستند؛ استفاده از SNI خاص، الگوی اتصال مداوم یا مسیرهای غیرعادی می‌تواند نشانه‌هایی برای تشخیص ایجاد کند. تفاوت اصلی این‌جاست که هزینه و پیچیدگی تشخیص آن‌ها بالاتر است.

WireGuard نیز یک پروتکل VPN مدرن، سریع و از نظر رمزنگاری بسیار امن است؛ اما برخلاف تصور رایج، از دید DPI، نامرئی محسوب نمی‌شود. در عمل، WireGuard الگوی مشخصی دارد: پکت آغازین کلاینت و پاسخ اولیه سرور (handshake) ساختار ثابتی دارند و اگر این پکت‌ها بدون پوشش اضافی روی شبکه دیده شوند، به راحتی می‌توان آن‌ها را از سایر ترافیک‌ها تفکیک کرد. به همین دلیل، تشخیص WireGuard در حالت خام برای تجهیزات تحلیل ترافیک کار پیچیده‌ای نیست.

یکی از راه‌ها برای کاهش این قابلیت تشخیص، افزودن یک لایه پوشاننده روی WireGuard است؛ برای مثال، قرار دادن آن داخل Websocket، TLS یا روش‌هایی مانند SWGP^۲. در SWGP، پکت‌های WireGuard پیش از ارسال، داخل یک پراکسی رمزگذاری شده کپسوله می‌شوند و از دید شبکه، به جای الگوی مشخص WireGuard، ترافیکی شبیه ارتباطات عادی TLS دیده می‌شود. در چنین حالتی، DPI دیگر به handshake واقعی WireGuard دسترسی مستقیم ندارد و تشخیص به تحلیل‌های رفتاری پیچیده‌تر محدود می‌شود. در نتیجه، WireGuard ذاتاً استتارپذیر نیست، اما با ابزارهایی مانند SWGP می‌تواند از یک پروتکل قابل تشخیص، به ترافیکی سخت‌تحلیل تبدیل شود؛ هرچند حتی در این سناریو هم «غیرقابل تشخیص مطلق» وجود ندارد و فقط هزینه تشخیص بالا می‌رود.

تونل SSH نیز وضعیت بینابینی دارد. خود SSH رمزنگاری قوی دارد، اما handshake و الگوی ترافیکی آن برای تجهیزات شبکه آشناست. اگر SSH روی پورت ۲۲ اجرا شود، تشخیص آن بسیار ساده است؛ حتی روی پورت‌های دیگر هم معمولاً می‌توان آن را از HTTPS واقعی تفکیک کرد. بنابراین SSH برای امنیت و سادگی عالی است، اما از نظر پنهان‌سازی ترافیک، محدودیت دارد.



عبور از تونل‌ها و گذر از دیوارها

هدف در روز
رسید.»

پیامدهای ناخواسته^۵ راهبرد
نامتقارن ایران و جنگ مبتنی
بر هوش مصنوعی آمریکا بر
حفاظت از غیرنظامیان

ماشین کشتار هوشمند: بخش اول



در بیست و چهار ساعت اول جنگ با ایران، ایالات متحده به بیش از ۱۰۰۰ هدف حمله کرد، یعنی به طور میانگین ۴۲ هدف در هر ساعت. تا زمان برقراری آتش‌بس، نیروهای آمریکایی بیش از ۱۳۰۰۰ هدف را منهدم کرده بودند. (اوضاع به جایی رسیده بود که برنامه‌ریزان پنتاگون عملاً لیست اهداف بارزش ایران را تقریباً خالی کرده بودند.) این سرعت بی‌سابقه در حملات، بدون به کارگیری یک ابزار جدید ممکن نبود: سامانه هوشمند میون^۱ که تحت نظارت شرکت پالانتیر^۲ است و در حال حاضر از هوش مصنوعی کلاد^۳ شرکت آنتروپیک نیرو می‌گیرد. پروژه^۴ Maven پاسخ به یک مشکل پیچیده بود.

تا اواسط دههٔ ۲۰۱۰، پنتاگون در حجم عظیمی از داده‌های نظارتی غرق شده بود؛ داده‌هایی که از تصاویر پهپادها، رهگیری سیگنال‌ها، تلفن‌های همراه و ترافیک اینترنت جمع‌آوری می‌شدند. اما این سازمان هیچ روش کارآمدی برای پردازش این اطلاعات و تبدیل آن‌ها به اهداف عملیاتی نداشت. در جنگ‌های گذشته، مانند جنگ عراق در سال ۲۰۰۳، پنتاگون برای تولید حدود ۲۰ هزار حمله به دو هزار نفر نیروی ترسیده‌شده نیاز داشت



قطعی بزرگ!

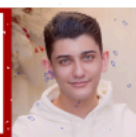
مروری بر زندانی کردن جهان آزاد در ایران

دانشگاه صنعتی شریف

سورنا کیا

۷ دقیقه

کارشناسی ۱۴۰۳



۳۲ سال قبل، هنگامی که اینترنت به صورت همگانی در اختیار کاربران ایرانی قرار گرفت، کمتر کاربری در کشور تصور می کرد که این پدیده نوظهور به مسئله ای امنیتی تبدیل شود. پدیده ای که روزی وصل، قطع یا محدود کردن آن در بالاترین نهاد سیاسی-امنیتی کشور، یعنی شورای عالی امنیت ملی تصمیم گیری شود. پدیده ای که از روز اول به بهانه های مختلف گروگان گرفته شد، تا بین ایران و جهان آزاد دیواری بکشند.

مردم ایران قطعی تعمیدی اینترنت را کم تجربه نکرده اند؛ اولین بار در آبان سال ۱۳۹۸ طعم آن را چشیدند و در پاییز ۱۴۰۱ نیز بار دیگر آن را تجربه کردند. اما امسال را شاید بتوان سال قطعی نامید. ابتدا در جنگ ۱۲ روزه شاهد قطعی بودیم و حال در زمستان ۱۴۰۴ و بهار ۱۴۰۵ شاهد سنگین ترین، طولانی ترین و بی سابقه ترین قطعی اینترنت تاریخ ایران بودیم. خفقانی که حتی با قطعی های خطوط تلفنی و پیامکی در سال ۱۳۸۸ نیز قابل مقایسه نیست. این قطعی نه تنها در تاریخ ایران بی سابقه است، بلکه اگر نگوییم بی سابقه، در تاریخ جهان نیز کم سابقه است. پیش از بررسی ابعاد اقتصادی و اجتماعی این قطعی خوب است آن چه بر ما گذشت را برای آیندگان مکتوب کنیم. در بخش اول به قطعی دی ماه و بهمن ماه ۱۴۰۴ می پردازیم.

تایم لاین قطعی اینترنت در ایران

پنجشنبه، ۱۱ دی

سایت زومیت در این روز مدعی می شود که از کاربران خود گزارشاتی مبنی بر اختلال در اینترنت دریافت کرده است، از این رو یک نظرسنجی با پرسش «آیا اینترنت در شهر شما اختلال دارد؟» منتشر می کند که در نتیجه آن ۷۵ درصد از ۴۲۲ کاربر شرکت کننده در این نظرسنجی پاسخ «بله» می دهند. ر این روزها هیچ کس فکر نمی کرد یکی از بزرگ ترین قطعی های اینترنت در جهان در شرف وقوع باشد.

پنجشنبه، ۱۸ دی

۲۰:۳۵

چهار صرافی «نوبیتکس»، «والکس»، «آبان تر» و «تبدیل» در اطلاعیه هایی جداگانه از کاربران خود می خواهند تا مدیریت ریسک را در دستور کار خود قرار دهند و از معاملات پرخطر بپرهیزند، چرا که احتمال انجام نشدن معاملات به دلیل قطعی ها بالاست. اطلاعیه هایی که احتمال اعمال محدودیت های بیشتر در ساعات و یا روزهای آتی می داد.

۰۹:۳۳

داده های netblocks نشان می دهد اینترنت در کرمانشاه به طور کامل قطع شده است؛ این قطعی به عنوان اولین قطعی کامل اینترنت یک شهر در جریان اعتراضات شناخته می شود.^۱ همچنین مطابق ادعای سایت زومیت، کاربران از ملی شدن اینترنت در شهرهای تهران و خوزستان خبر می دهند. در ادامه مطابق گفته پژوهش گرانی که این سایت با آن ها ارتباط داشته است، در نتیجه قطع پروتکل IPV6 اختلالات اینترنت افزایش یافته است.^۲

۲۰:۳۰

گزارشات netblocks حاکی از شروع قطعی کامل اینترنت در ایران است.^۳

۲۲:۰۰

اینترنت به طور کامل قطع شده است و حتی برای اولین بار شبکه ملی اطلاعات نیز در دسترس نیست. پیامک ها مختل می شوند و حتی برای ساعاتی ارتباطات خطوط تلفن نیز محدود شده و امکان برقراری تماس فراهم نیست. خدمات بانکی نیز مختل شده اند و امکان انجام هیچ عملیات بانکی و خدماتی اینترنتی وجود ندارد. به نظر می رسد این بار ابزارهای فیلترینگ کافی نبوده اند و عملاً زیرساخت های اینترنت را به صورت فیزیکی قطع کرده اند. به طور ساده تر می توان گفت اینترنت را از برق کشیدند. **ایران را خاموشی بی سابقه فرا گرفته است.^۴**

جمعه، ۱۹ دی

از ساعات ابتدایی روز ۱۹ دی خطوط تلفن به حالت عادی باز می گردد اما امکان تماس با خارج از کشور فراهم نیست. همچنین اینترنت و پیامک ها قطع هستند. از بعد از ظهر این روز، به صورت محدود بعضی از اپلیکیشن های

مربوط به امور بانکی بازگشایی می شوند.^۴ اما بقیه خدمات متصل نیستند. خبرگزاری مهر در خبری اعلام می کند که حتی ارائه خدمات ضروری مانند صدور گذرنامه در اداره پلیس مهاجرت و گذرنامه فراجا تا اطلاع ثانوی و وصل شدن اینترنت امکان پذیر نیست.^۵

ساعت ۱۳:۲۹ این روز، وزارت ارتباطات و اطلاعات فناوری، در اطلاعیه ای اعلام می کند «تصمیم راجع به قطعی مذکور توسط مراجع امنیتی ذیصلاح و به دلیل شرایط پیش آمده در کشور اخذ شده و وزارت ارتباطات مجدانه در حال پیگیری برقراری ارتباط و از سرگیری خدمات مذکور است و نتایج اقدامات متعاقباً اطلاع رسانی خواهد شد.»^۶ اطلاعیه ای که شاید بتوان از آن به عنوان اولین وعده بازگشایی اینترنت نام برد.

یکشنبه، ۲۱ دی

مرتضی کوهنورد، نایب رئیس کمیسیون اتاق واردات ایران در مصاحبه ای با ایسنا اعلام می کند: «روند کار در حوزه تجارت خارجی و تجارت داخلی به شدت مختل شده و به طور کلی شرایط کسب و کارها و امور اداری دچار مشکل شده است. ما شاهد هستیم که سامانه های گمرک، استاندارد، پست و... مختل شده و به درستی کار نمی کنند.»^۷

دوشنبه، ۲۲ دی

با وجود آن که روز پر خبری طی می شود، اما باز هم خبری از تغییر در شرایط اتصالات نیست. عباس عراقچی، وزیر امور خارجه، در دیدار با تعدادی از رؤسای نمایندگی های خارجی مقیم تهران، ضمن تأکید بر تلاش همکارانش برای بازگشایی هرچه زودتر اینترنت در سفارت خانه های خارجی، وعده باز شدن اینترنت با استقرار کامل امنیت را می دهد.^۸ گویی قطعی و خسارت ایرانیان ارزش کمتری دارد و در کشور خودمان شهروند درجه دو هستیم که اتصال سفارت های خارجی قرار است سریع تر برقرار شود!

اما این تنها وعده دوشنبه دولت نیست و از طرفی ستار هاشمی نیز در مصاحبه با ایسنا ذکر می کند که به صورت جدی در حال پیگیری هستند تا در **اسرع وقت** ارتباطات مردم برقرار شود.^۹

البته که وزیر ارتباطات چیزی جز یک نقش خیالی نبوده و جز تعیین درصد افزایش قیمت اینترنت کار خاصی نمی تواند انجام دهد!

یکشنبه، ۲۸ دی

سرانجام پس از مدتی طولانی که مردم فقط امکان مشاهده اخبار از طریق خبرگزاری‌های داخلی بسیار بسیار معتبر را داشتند، قابلیت ارسال پیام در پیام‌رسان‌های داخلی و همچنین ارسال فایل با محدودیت ۳۰۰ کیلوبایتی فراهم می‌شود. اما هنوز امکان ارسال پیام در گروه‌ها و کانال‌ها فراهم نیست.

محمد سراج، نماینده مجلس اعلام می‌کند «احتمالاً تا فردا، دوشنبه، یا حداکثر پس فردا یعنی سه‌شنبه، اینترنت به‌طور کامل وصل می‌شود و مردم مثل سابق به اینترنت جهانی دسترسی خواهند داشت.»^۵ اما این تنها وعده امروز نیست. مسعود پزشکیان، رئیس شورای عالی امنیت ملی - شورایی که طبق گفته مسئولین، قطعی اینترنت به دستور این شورا صورت گرفته است- می‌گوید «با توجه به ضرورت تسهیل امور کسب‌وکارهای اینترنتی و کاهش محدودیت‌های ارتباطاتی به آقای لاریجانی توصیه کردم که در اسرع وقت، محدودیت‌های اینترنتی برطرف شود.» اسرعی که مشخص نیست به چه زمان اشاره دارد.

دوشنبه، ۲۹ دی

بالاخره امکان ارسال پیام در گروه‌ها و همچنین ارسال فایل فراهم می‌شود. پس از مشخص شدن مشکلات فراوان موتورهای جست‌وجوی داخلی، سرانجام شاهد اتصال گوگل هستیم. منتها این اتصال به معنای اتصال Gmail و یا دیگر خدمات گوگل و یا حتی دسترسی به سایت‌های خارجی نیست. حسین افشین، معاون علمی ریاست جمهوری، وعده اتصال تا آخر هفته را می‌دهد، اما در ادامه اضافه می‌کند «البته این مکانیزم را در نظر داریم که اگر قطعی ادامه پیدا کند، بتوانیم به شرکت‌های بزرگ که آی‌پی ثابت دارند خدمات بدهیم.»^۶ گویی صحبت از اینترنت طبقاتی در میان مسئولین کشور عادی شده و مشکلی با اتصال اینترنت برای عده‌ای خاص به واسطه شغل‌شان ندارند!

سه‌شنبه، ۳۰ دی

آخرین روز دی ماه خونین فرا می‌رسد و تغییری در وضعیت اینترنت بین‌الملل مشاهده نمی‌شود. افشین، امروز نیز مصاحبه‌ای انجام می‌دهد و می‌گوید «سکوی ملی هوش مصنوعی تنها سکویی بوده که

به صورت خصوصی ممکن نیست. مسئولان در پاسخ به پرسش زمان وصل شدن اینترنت غالباً یک جمله را تکرار می‌کنند: «تصمیم‌گیری در این زمینه توسط نهادهای مسئول انجام می‌شود.»

پنج‌شنبه، ۲۵ دی

خبرگزاری مهر در گزارشی به نقل از ستاد توسعه اقتصاد دانش‌بنیان دیجیتال، اتصال‌پذیری و ارتباط معاونت علمی، می‌گوید که رایزنی‌هایی برای رفع یا کاهش محدودیت‌های دسترسی برخی شرکت‌های بزرگ فناوری اطلاعات دیجیتال انجام شده است.^۳ ادعایی که در تأیید بخشی از ادعاهای سه روز قبل زومیت و یکی از اولین زنگ‌های خطر اینترنت طبقاتی به‌طور رسمی به شمار می‌رود.

این در حالی است که در همین روز، حاجی میرزایی، مدیرعامل بنیاد ملی بازی‌های رایانه‌ای می‌گوید که حتی بازی‌های داخلی که امکان چت داشتند، به‌طور کامل قطع شده‌اند. وی در ادامه به این موضوع اشاره می‌کند که برخی از شرکت‌های بازی‌سازی ناچار به اعزام نیروهای فنی خود به خارج از کشور شده‌اند تا کارهای فنی پشتیبانی را انجام دهند.^۴

جمعه، ۲۶ دی

NetBlocks گزارشی از اتصال بسیار محدود و کم‌تر از ۲ درصدی می‌دهد. اتصالی که مشخص نیست از طریق خلأهای سیستم فیلترینگ است یا اتصال گزینشی بعضی سیم‌کارت‌های خاص. با توجه به تداوم قطعی پیامک‌ها، گزینه دوم را می‌توان محتمل‌تر دانست.

شنبه، ۲۷ دی

سرانجام پس از ده روز، قطعی سرویس پیامک به پایان می‌رسد؛ قطعی‌ای که پس از سال ۱۳۸۸، به‌عنوان طولانی‌ترین قطعی این سرویس شناخته می‌شود؛ قطعی‌ای که مشکلات بسیار زیادی را برای تمامی اقشار جامعه ایجاد کرده بود. از ناتوانی در ورود به سرویس‌های داخلی مختلف به دلیل دریافت نکردن کد ورود گرفته تا نبود امکان استفاده از خدمات بانکی. با وجود اتصال این سرویس، در وضعیت اینترنت تغییری ایجاد نمی‌شود و همچنان هیچ‌کس نه قطعی‌ها و نه وصل شدن‌ها را گردن نمی‌گیرد!

در مقابل، زومیت با انتشار مقاله‌ای مدعی می‌شود لیست محدودی از داخل برخی دیتاست‌های کشور انتخاب شده و به این گروه منتخب اینترنت داده شده است. در ادامه به نقل از منبعی آگاه بازگو می‌کند «محدوده آی‌پی این کسب‌وکارها از سرور را انتخاب کرده و به آن‌ها دسترسی بین‌المللی داده‌اند که از این محدودیت‌ها عبور کنند.» به گفته این منبع آگاه زومیت، سرورهای یک ارگان (قوه قضاییه) اینترنت بین‌الملل دارد. همچنین بر اساس اظهارات منابع مورد بررسی زومیت، خبرگزاری فارس و مهر به‌همراه چند رسانه غیررسمی از اینترنت بین‌الملل برخوردارند. در ادامه، این رسانه مدعی می‌شود که وزارت ارتباطات با برخی از بازیگران بزرگ اقتصاد دیجیتال در ارتباط است و قصد دارد دسترسی مجزای آن‌ها به اینترنت را فراهم کند تا مشکل‌شان برای ادامه فعالیت حل شود. مسیری که به نظر می‌آید در ادامه همان طبقاتی شدن اینترنت باشد!

از طرف دیگر خبرگزاری فارس در مقاله‌ای با عنوان شکست استارلینک از ایران، به نقل از نشریه فوربس مدعی می‌شود «ایران اولین کشوری است که خدمات‌دهی استارلینک را از کار انداخته و دسترسی‌ها را تا این میزان مختل کرده است.»

سه‌شنبه، ۲۳ دی

این روز با تداوم محدودیت‌ها و البته ابراز امیدواری سخنگوی دولت مبنی بر احقاق هرچه زودتر حق دسترسی مردم به اینترنت آزاد شروع می‌شود.

محمدرضا عارف در این روز جلسه ستاد توسعه فناوری و کاربرد هوش مصنوعی را در شرایط قطعی مطلق اینترنت برگزار کرد! جلسه‌ای که مطابق گزارش ایسنا در آن هیچ اشاره‌ای به وضعیت ارتباطاتی کشور نشده است.^۲

چهارشنبه، ۲۴ دی

با گذشت یک هفته، بعضی از سایت‌ها و اپلیکیشن‌های داخلی در دسترس قرار گرفته‌اند. موتورهای جست‌وجوی داخلی همچون ذره‌بین و گردو به‌عنوان جایگزین به مردم معرفی شده‌اند. ولی خبری از بازگشایی اینترنت نیست. پیامک‌ها همچنان مسدود هستند و در پیام‌رسان‌های داخلی نیز امکان ارسال پیام چه به‌صورت گروهی و چه

توانسته خدمات هوش مصنوعی را به صورت پایدار ارائه دهد.^۱ سکویی که اطلاعاتی از توانمندی‌های آن در دسترس نیست و مشخص نیست به چه اندازه مؤثر و قابل استفاده عملی است.

■ چهارشنبه، ۱ بهمن

بهمن ماه بدون اینترنت بین‌الملل فرا می‌رسد. این بار نشانه‌هایی از اینترنت طبقاتی را از زبان رئیس دانشگاه تهران می‌شنویم. «گفت‌وگوهایی با وزیر محترم صورت گرفته است و مکاتباتی برای تسهیل دسترسی کاربران دانشگاهی انجام شده است.»^۲ روز گذشته حسین دلیریان، سخن‌گوی مرکز ملی فضای مجازی نیز گفته بود که در صدد ایجاد دسترسی بازرگانان به اینترنت آزاد با فراغ بال و خیال راحت هستند!^۳

در پی این سخنان، زومیت گزارشی از صف طولانی تاجران برای دسترسی به اینترنت آزاد را منتشر می‌کند. گزارشی که نکات عجیب دیگری نیز دارد. به طور مثال، رئیس کمیسیون فاوای اتاق بازرگانی در واکنش به اظهارات حسین دلیریان می‌گوید «خبر ایجاد دسترسی به اینترنت آزاد برای بازرگانان و تجار تا این لحظه به هیچ‌وجه صحت ندارد.»

در این گزارش اشاره می‌شود که مطابق گفته تعدادی از بازرگانان عضو اتاق، سازوکار محدودی برای این دسترسی ویژه در حال اجراست. بر اساس این گزارش، بازرگانان دارای کارت بازرگانی، پس از ایستادن در صف طولانی تا ۴۵ دقیقه، می‌توانند به اینترنت آزاد دسترسی داشته باشند. امکانی که بر اساس گفته یکی از بازرگانان با مشقت اداری و محدودیت زمانی و دادن امضاء و تعهد سوء استفاده نکردن همراه است.^۴

■ پنج‌شنبه، ۲ بهمن

اگر چه طی چند روز گذشته تعدادی از کاربران با مشقت و سختی‌های فراوان توانسته‌اند اتصالی محدود و کوتاه به اینترنت بین‌الملل تجربه کنند، اما هم‌چنان غالب جمعیت ایران امکان بهره‌مندی از این حق را ندارند.

یک عضو اتاق بازرگانی اعلام می‌کند که منظور از اینترنت آزاد تاجران صرفاً این است که آن‌ها می‌توانند با حضور در اتاق‌های بازرگانی به ایمیل خود دسترسی داشته باشند.^۵ مردم با خود می‌گویند: **کره شمالی را شنیدیم! ایران را دیدیم!**

■ جمعه، ۳ بهمن

دولتی که روزی با وعده اینترنت آزاد و کاهش فیلترینگ بر سر کار آمده بود، حالا سابقه بزرگ‌ترین قطعی تاریخ ایران را در کارنامه خود به ثبت رسانده است و هر روز شایعاتی در خصوص اینترنت طبقاتی تن و جان مردم کشور را می‌لرزاند و گویی اعصاب و روان مردم بازیچه دست عده‌ای تمامیت‌خواه شده است. در همین حین، خبرگزاری فارس اعلام می‌کند که اینترنت بین‌الملل تا ۲۴ ساعت آینده به طور کامل در تمامی استان‌ها بازگشایی می‌شود.^۶

■ شنبه، ۴ بهمن

در اواسط روز، برخی دیتاسنترهای کشور به اینترنت متصل می‌شوند. اتصالی که امید برقراری اینترنت بین‌الملل را زنده می‌کند، اما این اتصالات بسیار ناپایدار هستند و بعد از چند دقیقه دوباره قطع می‌شود. شاید بهترین توصیف برای اتصال این روزهای اینترنت ایران، قطره‌چکانی باشد. با وجود قطعی اینترنت بین‌الملل برای عموم مردم، سازمان نظام صنفی رایانه‌ای کشور اعلام می‌کند: «در پی پیگیری‌های مستمر سازمان نصر کشور، اتصال IP تعدادی از کسب‌وکارهای عضو این سازمان به اینترنت بین‌الملل برقرار شد.»^۷ اما نصر، آخرین سازمانی نیست که اتصال آن برقرار شده است. اتاق تعاون ایران نیز اعلام می‌کند که اینترنت آزاد را برای فعالان حوزه خود در محیط اتاق‌های تعاون استان‌ها فراهم آورده است.^۸ اینترنت طبقاتی دیگر تنها یک شایعه نیست، بلکه بیش از هر زمان به واقعیت نزدیک شده است. فارس که روز گذشته مدعی اتصال اینترنت تا امروز شده بود، حالا علت متصل نشدن را مشکلات فنی می‌داند.

■ یک‌شنبه، ۵ بهمن

با وجود متصل نشدن اینترنت، مجله تازه‌های اقتصاد مصاحبه‌ای با معاون سیاست‌گذاری و برنامه‌ریزی توسعه اقتصاد دیجیتال وزارت ارتباطات انجام می‌دهد. در این مصاحبه احسان چیت‌ساز معتقد است که تبدیل سیاست‌های اضطراری و کوتاه‌مدتی نظیر فیلترینگ به یک رویه عمومی و پایدار، کارکرد این ابزار را در زمان بحران از بین برده است. وی هشدار می‌دهد که تداوم این رویکرد اشتباه نه تنها نهادهای مسئول را ناچار به قطع کامل ارتباطات می‌کند، بلکه با سوق دادن مردم به سمت ابزارهای جایگزین، اثربخشی این نوع

محدودیت‌ها را در آینده با چالش جدی مواجه خواهد کرد، تا جایی که در آینده قطع اینترنت دیگر جواب‌گو نخواهد بود و نهادهای مسئول ناچار به قطع برق خواهند شد.^۹ وزارت ارتباطات نیز ادعای چند روز پیش فارس را رد می‌کند.^{۱۰}

■ دوشنبه، ۶ بهمن

با وجود اتصالات‌های کوتاه روزهای گذشته، بر اساس گزارش NetBlocks اتصال مجدد به صفر رسیده است. وزیر ارتباطات در جلسه مشترک با معاون علمی رئیس جمهور مطرح می‌کند که قطعی‌های اخیر، روزانه حداقل ۵ همت به اقتصاد کلان کشور خسارت وارد کرده است و به طور مستقیم و غیرمستقیم اشتغال حدود ۱۰ میلیون نفر را در حوزه اقتصاد دیجیتال مختل کرده است. وی همچنین تصریح می‌کند لطمه‌های وارده از این قطعی، ممکن است پیامدهای اجتماعی و امنیتی به همراه داشته باشد. در ادامه اضافه می‌کند «برآوردها نشان می‌دهند میانگین تاب‌آوری شرکت‌ها و کسب‌وکارهای اینترنتی حدود ۲۰ روز است و کشور در حال نزدیک شدن به این نقطه است، بنابراین باید با استفاده از ظرفیت‌های موجود، برای کاهش آسیب‌ها اقدام کرد.»^{۱۱} ۲۰ روزی که رو به اتمام است و البته تا همین زمان، تعداد زیادی از کسب‌وکارها از نقطه غیرقابل بازگشت ورشکستگی عبور کرده‌اند.

■ سه‌شنبه، ۷ بهمن

شرق اعلام می‌کند دسترسی به اینترنت در ایران ۸ سطح دارد که سطح ۸ به معنای قطع کامل و سطح ۱ به معنای دسترسی عادی به اینترنت است (مشخص نشده است دسترسی عادی به معنای دسترسی پیش از ۱۸ دی است یا دسترسی بدون فیلتر). وی در ادامه اضافه می‌کند که به گفته برخی از منابع آگاه، دسترسی به اینترنت قرار است تا ظهر از سطح ۵ به ۲ ارتقاء پیدا کند. با این حال، واتساپ فیلتر باقی می‌ماند.^{۱۲} تعداد بیشتری از وب‌سایت‌ها و اپلیکیشن‌ها مانند گیت‌هاب و اپ‌استور در دسترس قرار می‌گیرند، اما سطح فیلترینگ بر روی پیام‌رسان‌های خارجی هم‌چنان سنگین است و وضعیت اینترنت کشور در همین حالت تثبیت می‌شود.

جالب است بدانید **جهنم ۷ طبقه دارد و اینترنت در ایران از جهنم هم بدتر است.** ادامه دارد....

اینترنت، حق مسلم!

خلاصه‌ای از خسارات قطعی اینترنت



شاید سخن گفتن از خسارات قطعی اینترنت بر اقتصاد دیجیتال و تأثیرات روانی ناشی از آن پس از آن‌چه که در این مدت تجربه کردیم، مسخره و بی‌اهمیت به نظر بیاید، اما همین قطعی که امروزه برای ما مردم ایران طبیعی و کم‌اهمیت به نظر می‌رسد، در جهان امری ناشناخته است و حتی تجربه چندساعته آن‌چه ما فقط از ابتدای سال گذشته، نزدیک به ۱۰۰ روز تجربه کرده‌ایم، در دیگر نقاط جهان می‌تواند به اعتراضات گسترده‌ای تبدیل شود و سالیان سال از آن سخن گفته شود. پس آن‌چه رخ داد را مکتوب کرده‌ایم تا اگر روزی قطع کردن آنی اینترنت کشور، دیگر امری عادی برای مسئولان کشور نبود؛ اگر روزی اینترنت پرو آن‌قدر مسئله‌ای عادی شناخته نمی‌شد و اگر روزی دسترسی عموم مردم به اینترنت آزاد، به رسمیت شناخته می‌شد، بازگردیم و به یاد آوریم که چه خسارت‌هایی بر کشور و ملت ما تحمیل شد. واقعیت تلخ این است که قرار نیست هیچ اعتراض و سخنی در سیاست‌های قطعی اینترنت تأثیری بگذارد، چون این قطعی ناشی از آگاهی نداشتن مسئولان به عواقب زیان‌بار این عمل نیست، بلکه ناشی از اولویت دادن به سرکوب جامعه در مقایسه با اقتصاد و آرامش روانی مردم است. به‌طور فراوان شاهد این بوده‌ایم که مسئولان با نام امنیت، اینترنت را بر روی مردم بسته‌اند، اما آن‌چه که می‌تواند مورد پرسش واقع شود این است که آیا امنیت بدون رشد اقتصادی و آرامش روانی، معنایی دارد؟!

ابعاد اقتصادی

باید ابتدا به بخش کوچکی از آمار و بعد اقتصادی ماجرا بپردازیم. مطابق آمار اعلامی از سوی خبرگزاری ایسنا در مهر ۱۴۰۳، ۸ درصد از تولید ناخالص ملی (GDP) ایران را اقتصاد دیجیتال تشکیل داده است.^۱ GDP ایران در سال ۲۰۲۵ میلادی، ۴۳۸/۶۶ میلیارد دلار بوده است. از این رو، سهم روزانه اقتصاد دیجیتال چیزی در حدود ۹۶ میلیون دلار است.

مطابق ادعای نامداری، مدیرعامل کارنامه، این سهم از بازار صرفاً شامل لایه اول یا همان لایه هسته می‌شود.^۳ این ادعا به معنای این است که این ۸ درصد، تنها لایه‌های فناوری پایه و زیربنایی، یعنی فعالیت شرکت‌های تجهیزات مخابراتی و شبکه، خدمات اینترنت، نرم‌افزارهای پایه و اپراتورهای ایرانی و خارجی را شامل می‌شود. به عبارتی، در این ۸ درصد، سهم خدمات ابری، سامانه‌های پرداخت دیجیتال، اپ‌استورها، پیام‌رسان‌ها، شرکت‌های حمل‌ونقل آنلاین، فروشگاه‌های آنلاین، پلتفرم‌های سرگرمی و محتوا و بسیاری دیگر از حوزه‌های کسب‌وکار دیجیتال که بخش بزرگی از اقتصاد دیجیتال را تشکیل می‌دهند، به‌شمار نیامده‌اند. در واقع، ما آمار دقیق و رسمی از میزان سهم این نوع شرکت‌ها در اختیار نداریم تا بتوانیم حجم خسارت وارده را محاسبه کنیم، اما باید همین ۹۶ میلیون دلار روزانه را در نظر بگیریم. مطابق آمارهای ارائه‌شده توسط نامداری و بسیاری دیگر از کارشناسان حوزه فناوری اطلاعات، هر روز قطعی اینترنت بین‌الملل تقریباً بین ۵۰ تا ۷۰ درصد از این ۹۶ میلیون دلار را از بین می‌برد. یعنی روزانه ۵۰ تا ۷۰ میلیون دلار ضرر اقتصادی! با توجه به قیمت دلار در زمان نگارش این متن (۱۸۰۰۰۰۰ ریال)، روزانه ۱۲/۶ همت خسارت به اقتصاد کشور وارد شده است؛ آماري که با عدد اعلام‌شده از سوی رئیس کمیسیون دانش‌بنیان اتاق ایران نیز تطابق دارد.^۴ اگر خسارت روزانه را به‌طور متوسط ۱۰ همت در نظر بگیریم، با توجه به ۱۲ روز قطعی در جنگ ۱۲ روزه، حدود ۲۰ روز در دی‌ماه و بهمن‌ماه ۱۴۰۴ و همچنین بیش از ۸۰ روز قطعی در پی جنگ اخیر، خسارتی بیش از هزار همت به اقتصاد کشور وارد شده است. لازم به ذکر است که این آمار همچنان بسیار حداقلی است.

برای درک بزرگی این عدد باید ذکر کنیم که بودجه سالانه وزارت ارتباطات در سال آینده ۳/۲ همت^۵ و بودجه امسال دانشگاه ۱/۲ همت^۶ است. هزینه ساخت یک مدرسه ۱۲ کلاسه در شهرستان خاش سیستان و بلوچستان ۳۰ میلیارد تومان است^۷، گویی خسارتی معادل تخریب ۳۳ هزار مدرسه به اقتصاد کشور وارد شده است. یکی از خساراتی که نباید آن را فراموش کرد، خسارات وارده بر کسب‌وکارهای کوچک در بستر پلتفرم‌های متفاوت است. مطابق گزارش تابناک در شهریور ۱۴۰۱، بیش از ۱۱ میلیون ایرانی از طریق

شبکه‌های اجتماعی کسب درآمد می‌کردند که از این بین، بستر شغلی ۹ میلیون نفر اینستاگرام بوده است.^۸

اگر فرض کنیم این ۹ میلیون نفر به‌طور متوسط یک خانواده ۲ نفره را پوشش دهند، حدود ۱۸ میلیون نفر در اثر این قطعی دچار خسارات مالی سنگین شده‌اند و زندگی‌شان دچار تغییرات جدی شده است. از طرفی اگر هر یک از این کسب‌وکارها روزانه ۵۰۰ هزار تومان هم درآمد خالص داشته باشند، با این قطعی، روزانه نزدیک به ۵ همت خسارت به آنلاین‌شاپ‌های مستقر در پیام‌رسان‌ها وارد شده است؛ اما این پایان خسارت وارده بر آنلاین‌شاپ‌ها نیست. این ۵ همت خسارت از بابت کسب نکردن درآمد است؛ نکته دیگر، کوچک شدن سهم این کسب‌وکارها و از دست رفتن اعتماد عمومی به آن‌هاست. روندی که در این اقتصاد رانتي و الیگارش، به حذف کسب‌وکارهای کوچک سرعت می‌بخشد.

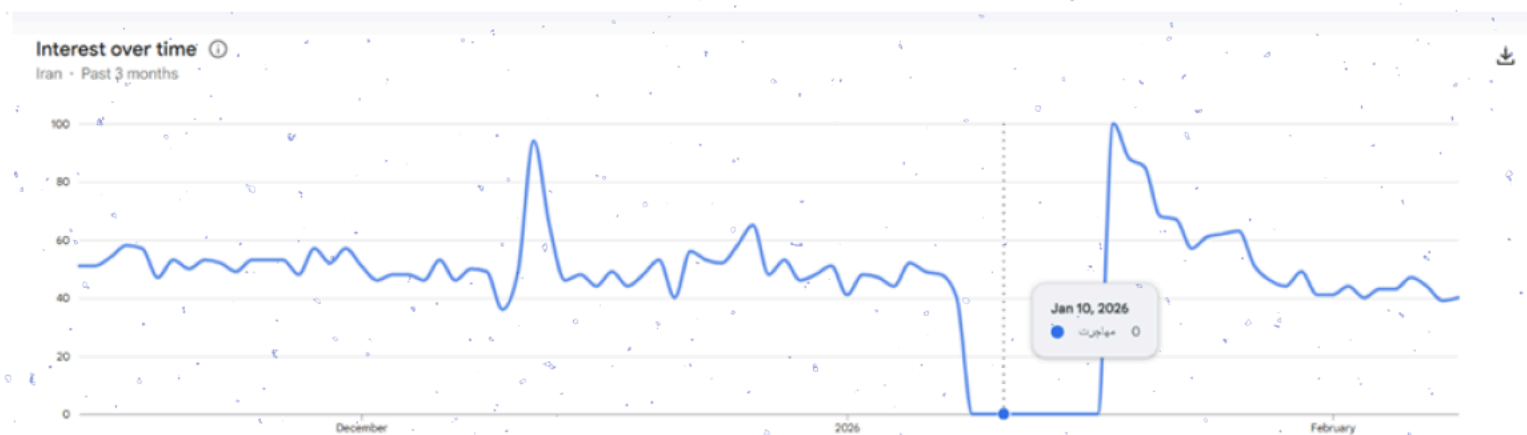
علاوه بر همه این‌ها باید به این نکته توجه کرد که اقتصاد، یک زنجیره است و مختل شدن یک بخش از آن، تمام آن را دچار اختلال می‌کند. قطعی اینترنت کشور علاوه بر کسب‌وکارهای مبتنی بر پلتفرم‌های آنلاین، بر بسیاری از صنایع و کسب‌وکارهایی که به‌ظاهر ربطی به اینترنت ندارند هم تأثیر می‌گذارد. به‌طور مثال در صنعت فولاد، بسیاری از اجزاء مختلف کار، بر پایه اپلیکیشن‌های تخصصی هستند که با قطع اینترنت از دسترس خارج می‌شوند یا صرافیه‌ها برای اعلام قیمت نیاز به دسترسی به بازارهای جهانی دارند.

در همین قطعی، گمرکات مرزی کشور نیز دچار مشکل شده است و واردات و صادرات کشور مورد آسیب واقع شد.^۹

بخش دیگر خسارت، خسارت مربوط به SEO^{۱۰} است. وب‌سایت‌هایی که سال‌ها با زحمات‌های بسیار توانسته بودند خود را در رتبه‌بندی گوگل بالا بکشند، حالا با نبود دسترسی اینترنت و نبود امکان به‌روز شدن، مرحله به مرحله جایگاه خود را از دست می‌دهند. خسارتی که برای جبران آن شاید زمان و هزینه زیادی نیاز باشد.

از طرف دیگر، شاهد قطعی پیامک‌ها نیز بودیم؛ این قطعی و ارسال نشدن OTP^{۱۱}، باعث ناتوانی در ورود به حساب‌های کاربری می‌شود که خساراتی از سوی دسترسی نداشتن بخشی از کاربران پدید می‌آورد.

شده است؛ امری که کسی حق نقد یا اعتراض به آن را ندارد، زیرا پدیده‌ای کاملاً طبیعی است! خشم حاصل از این تبعیض در کنار ناامیدی، می‌تواند موجب افزایش آمار مهاجرت شود. از این رو، بررسی تعداد دفعات جست‌وجوی کلمه «مهاجرت» پس از اتصال کوتاه اینترنت در دی‌ماه می‌تواند جالب باشد.



آمار سه‌ماهه کلمه مهاجرت

همچنین، این مسئله تنها بر ایرانیان داخل کشور اثر نمی‌گذارد. مطابق آمار وزارت امور خارجه، ۵ میلیون ایرانی در خارج از کشور زندگی می‌کنند. این قطعی باعث قطع ارتباط این افراد با خانواده‌های خود می‌شود و آنان را نیز ناامید می‌کند. در این میان شاهد پدیده دردناک سفر ایرانیان به نقاط صفر مرزی برای دسترسی به اینترنت و معامله سیم‌کارت‌های افغانستان و عراق با قیمت‌های گزاف بودیم و در نهایت مردمی که به مدت نامعلوم به کشورهای همسایه سفر کردند تا چند روزی اینترنت داشته باشند.^۲

افرادی اختیار اتصال و قطعی اینترنت یک ملت را در دست گرفته‌اند که بخش عمده عمرشان را در دنیایی بدون اینترنت گذرانده‌اند و کوچک‌ترین درکی از نقش حیاتی آن در زندگی امروز جامعه ایران ندارند. در حالی که کشورهای منطقه مانند عربستان و امارات میلیاردها دلار در اقتصاد دیجیتال، هوش مصنوعی و زیرساخت‌های آینده سرمایه‌گذاری می‌کنند، ما همچنان درگیر پروژه‌ای به نام «شبکه ملی اطلاعات» هستیم؛ پروژه‌ای که نه برای جهش اقتصادی، نه برای

پیشرفت علمی، بلکه برای محدودسازی، مدیریت و خفه کردن صدای جامعه طراحی شده است. سال‌هاست هزینه‌های سنگین از جیب مردم صرف این شبکه شده است، اما خروجی آن چه بوده است؟ امروز پس از ۹۰ روز قطعی در کمتر از ۴ ماه، می‌توان به راحتی به این پرسش پاسخ داد. سیستمی ناکارآمد که حتی در زمان قطعی اینترنت هم نمی‌تواند خدمات پایه را پایدار نگه دارد و ذره‌ای اعتماد عمومی ایجاد کند. پیام‌رسان‌های داخلی که قرار بود جایگزین شوند، با کوچک‌ترین تنش مانند رعدوبرق و زلزله، یا به طور کل از دسترس خارج شدند، یا دچار اختلال می‌شوند. موتورهای جست‌وجویی که نام «جست‌وجو» را یدک می‌کشند، اما در عمل چیزی جز فیلتر کردن با چند RegEx ساده نیستند. سرویس‌های هوش مصنوعی که حتی از ابتدایی‌ترین اطلاعات بی‌خبرند و مسعود پزشکیان را با بازیکن فوتبال اشتباه می‌گیرند، اما قرار است نماد استقلال فناوری باشند!

اما به یاد داشته باشید، اینترنت یک امتیاز تشریفاتی یا هدیه حاکمیت به مردم نیست. اینترنت حق مردم است؛ همان‌طور که آب، برق و گاز حق مردم هستند؛ همان‌طور که خیابان‌ها و فضاهای عمومی حق مردم هستند. این حق را نمی‌توان سهمیه‌بندی کرد، نمی‌توان طبقاتی کرد، نمی‌توان مشروط به سلیقه و تصمیم چند نفر کرد. اینترنت را نمی‌شود به بهانه‌های مبهم از مردم گرفت و بعد همان را قطره‌چکانی به «قشر خاص» یا «زمان خاص» برگرداند. دسترسی به اینترنت برای تجارت حق است، برای پژوهش حق است، برای آموزش حق است، برای ارتباط با جهان حق است، همان‌طور که برای سرگرمی و اینستاگرام‌گردی هم حق است. هیچ‌کس حق ندارد تعیین کند کدام استفاده موجه است و کدام نیست. در یک کلام، اینترنت لطف دولت به مردم نیست که هر زمان بخواهد آن را قطع کند. **اینترنت حق مسلم مردم است؛ حتی که نه قابل‌مصادره است، نه قابل‌معامله، و نه قابل‌خاموش کردن با یک دکمه.**

آنچه گفته شد، تنها خسارات واردشده بود و سخنی از هزینه فرصت‌های ازدست‌رفته به میان نیامد. با این قطعی، شانس بسیاری از سرمایه‌گذاری‌ها در حوزه اقتصاد دیجیتال از دست رفت. از سمت دیگر این خسارات واردشده بر اقتصاد می‌توانند باعث پدیده تعدیل نیرو شوند؛ پدیده‌ای که از نگاه متخصصان و صاحبان مشاغل اصلاً دور از انتظار نیست. پیامدی که سال‌ها بر جامعه تأثیرگذار خواهد بود.

بحث دیگری که نباید از آن گذشت، بحث امنیت سایبری کاربران است. با قطعی اینترنت، امکان بسیاری از به‌روزرسانی‌ها از دست می‌روند. باگ‌های امنیتی برطرف‌شده بر دیگر دستگاه‌ها در جهان هم‌چنان بر روی سیستم‌های ما باقی می‌ماند و اگر در این مدت این باگ‌ها از سوی هکرها کشف شوند، در زمان اتصال اینترنت می‌تواند موجب آسیب غیرقابل‌جبران به سیستم‌های ما شود. در واقع این خود، تحریمی امنیتی است و موجب پایین آمدن سپرهای دفاعی کشور می‌شود و ریسک امنیت اطلاعات شهروندان را بالا می‌برد. البته در شرایط فعلی، سخن گفتن از امنیت اطلاعات شوخی‌ای بیش نیست!

ابعاد اجتماعی

بعد اقتصادی اینترنت را شاید بتوان با اعداد و ارقام توصیف کرد، اما آن‌چه نمی‌توان به راحتی توصیف کرد، بحث تأثیر این قطعی بر اجتماع و تأثیر آن بر روان جامعه است. متأسفانه آمار و نظرسنجی دقیق و معتبری از قطعی اینترنت بر روح و روان جامعه ایران وجود ندارد. امروزه، حضور در فضای مجازی همچون حضور در اجتماع است و قطع این محیط مانند حبس خانگی افراد و گرفتن حق سخن گفتن در اجتماع است. از این رو، این قطعی‌ها موجب «استرس انزوای دیجیتال» یا «اضطراب قطع اتصال» می‌شوند. تروماهای جمعی ایجاد می‌شوند و اضطراب در اجتماع فراگیر می‌شود. جامعه دچار سرخوردگی و افسردگی شدید می‌شود و انزوای پایداری می‌شود. در نهایت، در کنار عصبانیت حاصل از این قطعی، اقتصاد بیمار و تبعیض‌های متعدد، خشمی عمیق در جامعه نهادینه می‌شود. خشمی که با مطرح شدن اخباری مانند اینترنت طبقاتی و انتخابی تشدید می‌شود. هر روزی که سپری می‌شود، اینترنت پرو بدون هیچ‌گونه توضیحی، عادی‌سازی می‌شود. گویی سال‌ها وجود داشته و تبدیل به امری بدیهی



چگونه در دنیای اینترنت ناشناس بمانیم؟

دانشگاه صنعتی شریف
Amnam
کارشناسی ۱۴XX
۴ دقیقه

انسان‌ها در دنیای واقعی، به محض خروج از درب منزل، تحت نظر چشم‌ها هستند (به شرطی که لوازم الکترونیکی نقش ابزار جاسوسی را نداشته باشند و همچنین ابزار نظارتی خاصی در محیط، کارگذاری نشده باشد). این چشم‌ها می‌توانند الکترونیکی، مانند دوربین‌های مداربسته، یا انسانی، مثل مأمورهای دولتی باشند.

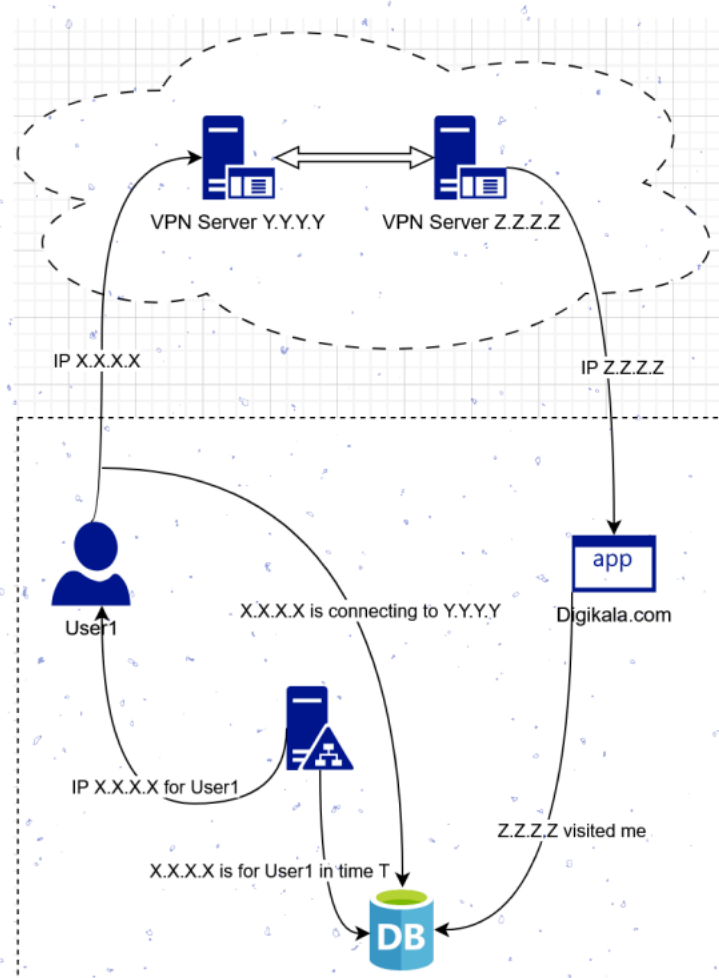
در دنیای دیجیتال اوضاع فرق می‌کند، تقریباً همه وقایع به صورت خودکار ثبت می‌شوند، برای مثال:

- زمان اتصال
- IP مبدأ (حتی IP های پویا)
- IP مقصد
- پرسش DNS^۲
- الگوی ارسال بسته‌ها

دولت‌ها و اپراتورها می‌توانند با داشتن این اطلاعات فعالیت کاربران را به طور کامل رصد کنند و هویت آن‌ها را پیدا کنند. تفاوت عمده ردپاها در دنیای دیجیتال با دنیای واقعی این است که وابسته به خصوصیات فیزیکی (مانند چهره) نیستند و با مجموعه‌ای از شناسه‌های فنی تعریف می‌شوند. با داشتن دانش کافی از معماری شبکه، می‌توان دانش دولت‌ها از کاربران را محدود کرد.

برای مثال، می‌دانیم که اپراتورها (ثابت و همراه) به کاربران IP تخصیص می‌دهند و تمامی فعالیت‌های آن IP در بازه تخصیصش در سطح زیرساخت ملی قابل ثبت و قابل پیگیری است. حال اگر با این IP به یک سرور خارجی متصل شویم و از آن سرور برای وب‌گردی استفاده کنیم، چه؟ در ظاهر، سایت مقصد فقط IP سرور خارجی را داشته و دسترسی به IP واقعی کاربر ندارد. اما در عمل، اپراتور داخلی می‌داند که شما در چه ساعتی به کدام سرور متصل شده‌اید و قسمت دیگری از دولت می‌داند که توسط یک IP، یک درخواست به داخل کشور آمده است. احتمالاً دولت می‌تواند حدس بزند این همان کاربری است که چندی پیش با IP داخلی خودش به آن سرور بسته می‌فرستاد.

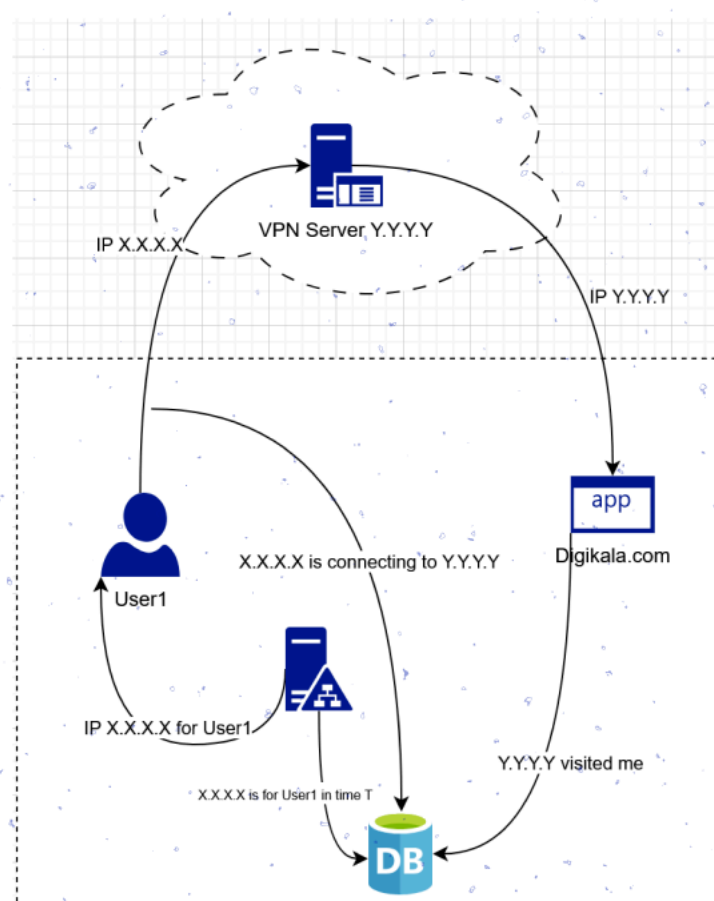
مسئله دوم که حتی مهم‌تر است، سشن^۳ و کوکی^۴ است. فرض کنید از طریق یک IP کاملاً



نصب افزونه‌های اضافی، تغییر تنظیمات مرورگر یا باز کردن فایل‌های دانلودی خارج از محیط ایمن می‌تواند IP واقعی را افشا کند. منظور از محیط ایمن، Sandbox و یک ماشین مجازی^۲ بدون اینترنت است.



در مورد VPN‌ها و کانفیگ‌های رایگان، بهتر است ابتدا یک پیش‌فرض ساده را بپذیریم: در اینترنت «خدمت رایگان بدون درآمد» تقریباً وجود ندارد. وقتی سرویسی هزینه زیرساخت، سرور و پهنای باند را پرداخت می‌کند، اما از کاربر پولی دریافت نمی‌کند، باید پرسید این هزینه از چه طریقی جبران می‌شود. در بسیاری از موارد، پاسخ در جمع‌آوری داده، فروش اطلاعات و یا بهره‌برداری‌های دیگر نهفته است. برخی افراد یا حتی مجموعه‌ها با اهداف مشخص، اشتراک‌های رایگان VPN را از طریق کانال‌های واسط، گروه‌های پیام‌رسان یا نرم‌افزارهایی با ظاهر عادی منتشر می‌کنند. کاربر تصور می‌کند صرفاً در حال تغییر IP است، در حالی که ممکن است تمام ترافیک او از زیرساختی عبور کند که به طور کامل تحت نظارت است. داده‌های تحت نظارت می‌توانند شامل IP واقعی، زمان اتصال، دامنه‌های بازدید شده و در صورت نبود رمزنگاری سرتاسری، حتی محتوای کامل تبادل داده باشند.



متفاوت و ناشناس (مانند چند لایه VPN^۵، شبکه TOR^۶، استارلینک و...) وارد سایتی مانند دیجی‌کالا شوید. اگر با حساب کاربری شخصی خود لاگین کنید، سرور با استفاده از Session ID و کوکی ذخیره‌شده در مرورگر، هویت شما را تشخیص می‌دهد. در این حالت، IP جدید هیچ اهمیتی ندارد، چون شما خودتان هویت‌تان را اعلام کرده‌اید. به جز نام کاربری، کاربران اثرانگشت‌های دیگری مانند فونت‌ها، رزولوشن مرورگر، WebGL و Canvas دارند که با کنار هم قرار دادن چنین اطلاعاتی می‌توان هویت کاربر را از پشت یک IP کاملاً ناشناس کشف کرد.

حال اگر دو سرور خارجی داشته باشیم، چه؟ به عنوان نمونه، کاربر ابتدا به Server A متصل شود، سپس از داخل آن به Server B تونل بزند و خروجی اینترنت از Server B انجام شود. در این سناریو، سرور دوم IP واقعی کاربر را نمی‌بیند و فقط IP سرور اول را می‌شناسد. اپراتور داخلی نیز فقط اتصال به Server A را مشاهده می‌کند. این معماری زنجیره تحلیل را پیچیده‌تر می‌کند و وابستگی به یک نقطه واحد را کاهش می‌دهد. با این حال، اگر کاربر از همان محیط مرورگر قبلی با کوکی‌های قدیمی یا حساب‌های شخصی استفاده کند، این لایه‌بندی فنی نیز بی‌فایده خواهد شد.

در مورد شبکه Tor نیز وضعیت مشابه است. Tor ترافیک را از ۳ گره ورودی، میانی و خروجی عبور می‌دهد تا مبدأ و مقصد از یک‌دیگر جدا باشند. گره ورودی IP اصلی کاربر را می‌بیند، ولی مقصد را نمی‌داند و گره خروجی نیز مقصد را می‌بیند، ولی IP واقعی را نمی‌داند. این طراحی برای کاهش امکان ردیابی مستقیم است. با این حال، ورود به حساب‌های شخصی از طریق Tor،

ریسک دیگر، خود نرم افزار است. برخی اپلیکیشن های VPN رایگان علاوه بر ایجاد تونل، دسترسی های غیرضروری به دستگاه درخواست می کنند یا حاوی کدهای تبلیغاتی و حتی ماژول های مخرب هستند. در چنین حالتی، کاربر نه تنها ناشناس نشده، بلکه یک نقطه دسترسی مستقیم به دستگاه خود اضافه کرده است. تا زمانی که از صحت چرخه کامل یک VPN - شامل مالکیت سرورها، سیاست نگهداری لاگ ها، کد نرم افزار و غیره -

اطلاع دقیق ندارید، استفاده از آن خطر قابل توجهی دارد. چنانچه به واسطه داشتن رن خوب، دسترسی به IP هایی دارید که از طریق آن می توانید بدون مواجهه با دیوار آتش ملی به تمامی خدمات بین الملل دسترسی داشته باشید، توصیه می کنیم حتماً از VPN یا پروکسی استفاده کنید تا سرویس های بین المللی از هویت و رن خوب مطلع نشوند تا مبادا حساب های کاربری شما بسته و یا محدود شود. کارهایی مانند جداسازی

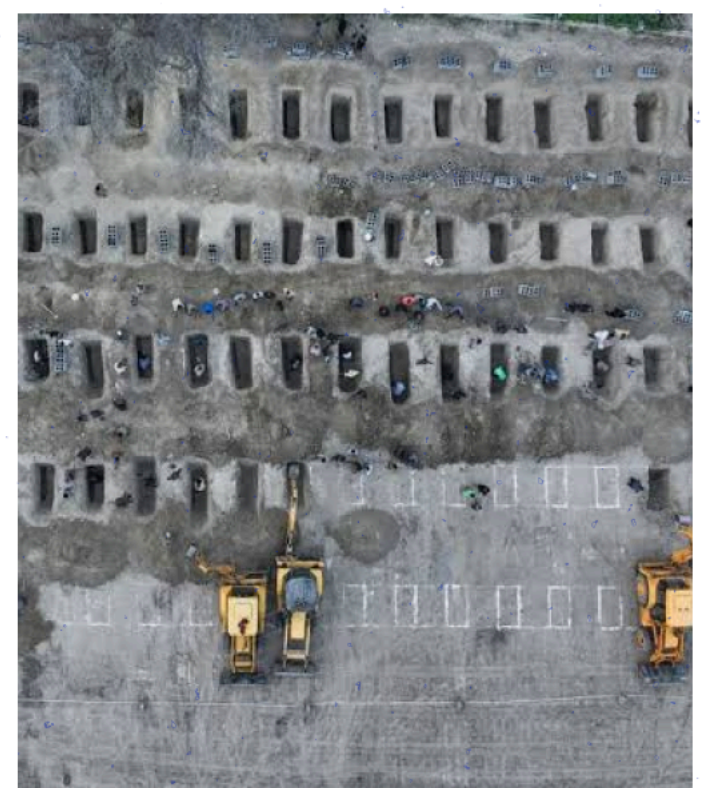
هویت های دیجیتال (داشتن چند ایمیل، حساب کاربری، مرورگر و...)، استفاده از محیط های مجزا (مثلاً ماشین مجازی یا سیستم عامل های موقت)، حذف منظم کوکی ها، کنترل نشد DNS و WebRTC و پرهیز از ترکیب هویت واقعی با زیرساخت ناشناس سازی از اصول پایه هستند. هر اشتباه کوچک، مانند یک لاگین ساده، می تواند تمام زنجیره فنی را بی اثر کند. اینترنت فراموش نمی کند، بلکه ذخیره می کند.

پیامدهای ناخواسته راهبرد نامتقارن ایران و جنگ مبتنی بر هوش مصنوعی آمریکا بر حفاظت از غیرنظامیان

ماشین کشتار هوشمند: بخش دوم



حذف این موانع از سوی پنتاگون، نه تنها کنترل های فرایندی را از میان برد، بلکه زمان اختصاص یافته برای تحلیل اطلاعات ورودی را نیز به شدت کاهش داد. وقتی سامانه تنها هفتاد ثانیه به افسران فرصت می دهد تا درباره ارسال یک بسته هدف گیری تصمیم بگیرند، طراحی سیستم به طور ذاتی آنان را به سمت تأیید حمله سوق می دهد، حتی زمانی که میزان اطمینان نسبت به اطلاعات پایین باشد. نتیجه چنین رویکردی روشن است: **اشتباهات بیشتر و آسیب گسترده تر به غیرنظامیان.**



دلایل موجهی برای نگرانی از تأثیرات استفاده از هوش مصنوعی نظامی وجود دارد. برای نمونه، ارتش اسرائیل سامانه هوش مصنوعی ای به نام Lavender توسعه داده است که نقش محوری در هدایت موشک ها و بمب ها در جنگ غزه ایفا کرده است. هدف این سامانه، شناسایی اعضای مشکوک حماس و جهاد اسلامی به عنوان اهداف بالقوه بود. تنها در هفته های نخست جنگ، Lavender حدود ۳۷ هزار فلسطینی را به عنوان گزینه های احتمالی حملات هوایی شناسایی کرد.

اما نیروهای ارتش اسرائیل زمان بسیار اندکی برای تأیید تصمیمات این سامانه در اختیار داشتند؛ در برخی موارد، تنها ۲۰ ثانیه برای هر بسته هدف گیری. نگران کننده تر آن که این سامانه در حدود ۱۰ درصد موارد دچار خطا می شد و افرادی را به عنوان هدف معرفی می کرد که تنها ارتباطی بسیار ضعیف، یا حتی هیچ ارتباطی، با گروه های مسلح نداشتند. با توجه به حجم بالای حملاتی که بر اساس پیشنهاد های Lavender انجام شد، نرخ خطای ۱۰ درصدی احتمالاً به این معناست که هزاران غیرنظامی به اشتباه زخمی یا کشته شده اند.

در مورد جنگ ایران نیز گزارش ها نشان می دهد که حملات آمریکا خسارات سنگینی به غیرنظامیان و زیرساخت های غیرنظامی وارد کرده است که برخی از این حملات مستقیماً نقض کنوانسیون ژنو بوده است.

گزارش روزنامه نیویورک تایمز آسیب وارد شده به دست کم ۲۲ مدرسه و ۱۷ مرکز درمانی را تأیید کرده است؛ از جمله مدرسه ای در شهر میناب که در یکی از حملات آمریکا بیش از ۱۵۰ کودک جان خود را از دست دادند.

همان گزارش تأکید می کند که ابعاد واقعی خسارات احتمالاً بسیار گسترده تر بوده است؛ زیرا جمعیت هلال احمر ایران، به عنوان اصلی ترین سازمان امداد رسانی کشور، آسیب دیدن دست کم ۷۶۳ مدرسه و ۳۱۶ مرکز درمانی را در طول جنگ ثبت کرده است.

این میزان حیرت آور از خسارت، پرسش های جدی و فوری درباره دقت عملکرد میون و همچنین میزان نظارت واقعی پنتاگون بر فرایند هدف گیری ایجاد می کند.

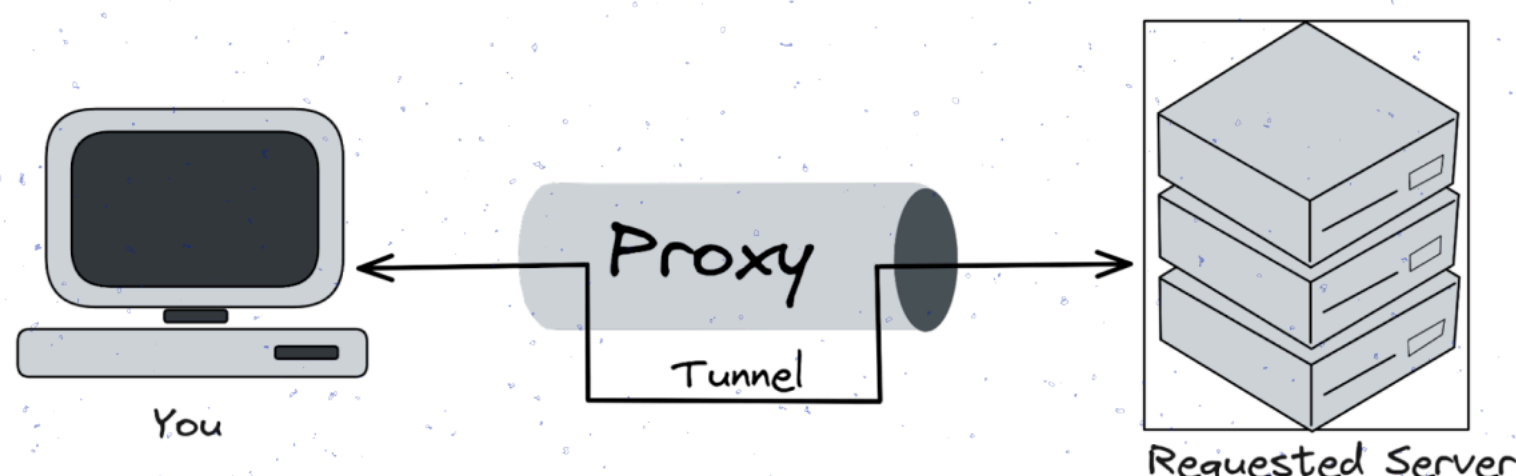
زمانی که زنجیره کشتار تا آن اندازه فشرده شود که نظارت معنادار انسانی عملاً به امری نمادین تبدیل شود، تعادل میان سرعت و دقت بیش از حد به سمت سرعت متمایل شده است؛ در چنین شرایطی، کاهش سرعت فرایندهای مبتنی بر هوش مصنوعی، ضرورتی اجتناب ناپذیر خواهد بود.

حداقل می توان گفت که سابقه نه چندان قابل اعتماد هوش مصنوعی نظامی، ادعاهایی را که می گویند استفاده از مدل های زبانی بزرگ در فرایند هدف گیری باعث افزایش دقت یا تشخیص بهتر غیرنظامیان از رزمندگان می شود، زیر سؤال می برد.

نگران کننده تر از آن، همان گونه که یک پژوهش گر حقوقی در مقاله ای اشاره می کند، سرعت و مقیاس هدف گیری مبتنی بر هوش مصنوعی این خطر را ایجاد می کند که میزان خسارات انسانی به سطحی بسیار فراتر از آنچه پیش تر تصور می شد برسد. این روند در نهایت، اصل بنیادین خویشتن داری در حقوق بین الملل بشردوستانه (IHL) را تضعیف می کند؛ اصلی که بر این ایده استوار است که نیروهای نظامی باید در شیوه جنگیدن خود محدودیت هایی را رعایت کنند تا از تحمیل رنج و آسیب غیرضروری جلوگیری شود.^۲

احراز هویت^۲، رمزنگاری^۳ و قالب پیام‌ها چگونه باشد و در نهایت لایه^۴ چهارم شبکه، یعنی لایه انتقال^۵ است که مشخص می‌کند ترافیک روی چه حامل شبکه‌ای (TCP^۵، UDP^۶ یا QUIC^۷) حرکت کند.

پروکسی، تونل زدن و کانفیگ



پروکسی یک واسطه است که بین کاربر و مقصد می‌ایستد و به جای این که سیستم، به طور مستقیم به سرور مقصد متصل شود، درخواست‌ها را به پروکسی می‌فرستد و پروکسی آن‌ها را به مقصد منتقل می‌کند. پروکسی معمولاً در لایه^۸ هفتم شبکه، یعنی لایه^۹ کاربرد^{۱۰} عمل می‌کند. از جمله اهداف رایج پروکسی زدن می‌توان به مخفی کردن IP کاربر، کنترل دسترسی، اعمال سیاست (مثلاً سیاست مسیریابی)، کش^{۱۱} و در بسیاری از سامانه‌ها، اضافه کردن لایه‌های امنیتی و رمزنگاری اشاره کرد. دقت شود که پروکسی لزوماً VPN^{۱۲} نیست. تونل زدن یعنی یک پروتکل یا جریان ترافیکی را داخل یک کانال دیگر کپسوله کنیم. گویی که داخل یک راهرو، یک راه دیگر بسازیم. تونل زدن عموماً برای ایجاد یک کانال امن با رمزنگاری و امنیت، عبور از محدودیت‌های شبکه، پایداری و کارایی ناشی از مدیریت بهتر Loss ها استفاده می‌شود. و در نهایت به کانفیگ می‌رسیم. کانفیگ‌ها فقط آدرس‌های سرورها نیستند، بلکه یک سند کامل سیاست و اتصال هستند که مشخص می‌کنند:

- ۱- به کجا وصل شویم؟ (شناسه‌های نقطه پایانی چیست؟)
 - ۲- با چه روشی وصل شویم؟ (پروتکل‌هایی مانند VLESS، VMess و...)
 - ۳- روی چه حامل شبکه‌ای اتصال را برقرار کنیم؟ (مانند پروتکل‌های لایه انتقال شامل TCP و UDP...)
 - ۴- چه چیزهایی کجا بروند؟ (قواعد مسیریابی، مستقیم یا از طریق تونل؟)
 - ۵- مشکلات اتصال و دریافت پاسخ از DNS چگونه حل شوند؟ (استراتژی DNS و جلوگیری از نشت)
 - ۶- و چطور اتصال، پایدار و بهینه باشد؟
- بنابراین کانفیگ یک پشته پروتکل-سیاست است که در ابزارهای اتصال، هم مسیر و قوانین را مشخص می‌کند و هم سیاست‌ها را تعیین می‌کند.

پروتکل‌ها، ابزار سیاست و اتصال

در ادامه قصد داریم به برخی از رایج‌ترین پروتکل‌های کانفیگ‌ها اشاره کنیم. برای هر پروتکل سعی شده که مطالب از مستند اصلی آن پروتکل استخراج شده باشد.

VMess

پروتکل VMess بومی V2Ray برای ارتباط بین کلاینت و سرور است و در مستندات رسمی به عنوان یک پروتکل stateless توصیف می‌شود؛ یعنی کلاینت و سرور می‌توانند داده را بدون یک handshake جداگانه منتقل کنند و هر تبادل داده، وابستگی مستقیمی به تبادل‌های قبل و بعد ندارد.

در مدل ارتباطی VMess، کلاینت آغازگر درخواست است و سرور در ابتدا تلاش می‌کند تشخیص دهد آیا درخواست از یک کلاینت معتبر آمده یا نه؛ اگر این اعتبارسنجی موفق باشد، درخواست به

مهندسی مقاومت در برابر سانسور

کالبدشکافی اکوسیستم کانفیگ‌های V2Ray/Xray

فرزام کوهی
کارشناسی ۱۴۰۱
دانشگاه صنعتی شریف
۶ دقیقه

هنگام استفاده از کانفیگ‌های V2ray، باید واژگانی نظیر VLESS، VMess و Trojan را دیده باشید. کانفیگ‌هایی که برای اتصال به پلتفرم‌های فیلترشده یا تحریم‌شده نظیر تلگرام، اینستاگرام، فیس‌بوک، یوتیوب و X استفاده می‌کنیم، بخشی از زندگی روزمره ما را تشکیل می‌دهند. این روزها اتصال پایدار به اینترنت به یکی از دغدغه‌های جدی هر شخص در ایران، به ویژه کسانی که به هر طریقی گذران زندگی روزمره‌شان به اینترنت وابسته است، تبدیل شده است. بنابراین شاید آشنایی با نحوه کارکرد برنامه‌هایی مانند NekoRay، V2RayN و به طور مشخص تر هسته آن‌ها مانند sing-box، Xray و V2Ray خالی از لطف نباشد.

اجزای اکوسیستم اتصال: Protocol و Client، Core

برای داشتن یک دید منسجم‌تر، بهتر است در ابتدا مفاهیمی را تعریف کنیم. به ابزارهایی مانند sing-box، Xray و V2Ray که نقش محوری و اصلی دارند؛ یعنی پردازش ترافیک، پیاده‌سازی پروتکل‌ها و اجرای سیاست‌های مسیریابی و DNS را انجام می‌دهند، هسته یا موتور می‌گوییم. در مقابل، به برنامه‌هایی نظیر V2RayN، V2RayNG، NekoBox و Nekoray که نقش یک رابط کاربری را ایفا می‌کنند و مدیریت پروتکل‌ها و کنترل یک هسته را ساده می‌کنند، کلاینت گفته می‌شود. نقش اصلی این کلاینت‌ها، ایجاد رابطی گرافیکی و ساده‌تر برای ارتباط با هسته است. در نهایت، همه این اسامی معروفی که تا به امروز با آن‌ها سروکار داشتید، یعنی Shadowsocks، VLESS، VMess و Trojan نام پروتکل‌هایی هستند که تعیین می‌کنند

Shadowsocks

Shadowsocks یک پروکسی رمز شده است که برای عبور دادن ترافیک TCP و UDP از طریق یک سرور واسط طراحی شده است؛ یعنی کلاینت به جای اتصال مستقیم به مقصد، داده را به سرور Shadowsocks می‌فرستد و سرور آن را به مقصد نهایی forward می‌کند. نسخه‌های مدرن Shadowsocks (به خصوص ۲۰۲۲) بر پایه AEAD^۶ ساخته شده‌اند؛ یعنی هم‌زمان محرمانگی و تمامیت داده را تضمین می‌کنند. ۲۰۲۲ Spec می‌گوید پروتکل از AEAD با یک کلید متقارن اشتراک‌گذاری شده از پیش^۷ برای حفاظت از داده استفاده می‌کند. این یعنی مدل اعتماد Shadowsocks ساده است: «هر کس کلید را دارد، مجاز است».

SOCKS5

پروتکل SOCKS (معمولاً SOCKS5) یک پروتکل پروکسی لایه کاربرد است که به کلاینت اجازه می‌دهد اتصال‌های TCP (و همچنین UDP در SOCKS5) را از طریق یک سرور واسط برقرار کند. در RFC^۸ رسمی SOCKS5 آمده که این پروتکل برای application-layer traversal of IP network firewalls طراحی شده؛ یعنی راهی استاندارد برای عبور دادن ارتباط‌های برنامه‌ها از یک واسطه یا فایروال. نکته کلیدی این است که SOCKS به‌تنهایی VPN یا تونل امن نیست؛ این پروتکل بیشتر نقش یک کانال‌دهنده را دارد: برنامه می‌گوید «به این مقصد وصل شو»، و سرور SOCKS اتصال را از طرف او برقرار می‌کند و داده را بین دو طرف رد و بدل می‌کند. در همان RFC تأکید شده که سطح امنیت بسیار وابسته به روش‌های احراز هویت و کپسوله‌سازی انتخاب‌شده در مذاکره وابسته است؛ یعنی خود SOCKS امنیت را تضمین نمی‌کند و این موضوع به انتخاب‌های جانبی بستگی دارد.

بنابراین، SOCKS یک استاندارد عمومی برای پروکسی کردن ترافیک است، اما Shadowsocks یک پروتکل پروکسی رمز شده با طراحی امنیتی مشخص؛ در نتیجه Shadowsocks اغلب کانال امن را خودش تعریف می‌کند، در حالی که SOCKS معمولاً به امنیت لایه‌های دیگر متکی است.

رمزنگاری ارائه نمی‌کند و برای کارکرد صحیح، فرضش این است که در یک اتصال TLS^۳ با پیکربندی درست به‌کار گرفته شود. VLESS در مستند V2Fly (شاخه v5) صراحتاً منسوخ‌شده اعلام شده و در معرض حذف توصیف می‌شود؛ یعنی از منظر نگهداری پروژه، ممکن است در آینده از این توزیع حذف شود. منسوخ بودن یک پروتکل معمولاً به معنی این است که توسعه‌دهندگان آن شاخه، تعهدی برای توسعه، رفع باگ و سازگاری آینده روی آن ندارند و به کاربران پیشنهاد می‌کنند به گزینه‌های دیگر مهاجرت کنند.

Trojan

Trojan یک پروتکل و سازوکار پروکسی مبتنی بر TLS است که ایده محوری آن شبیه‌سازی ترافیک HTTPS است. در مستندات رسمی Trojan آمده که این پروژه به جای اتکا به مبهم‌سازی تصادفی، تلاش می‌کند رفتار خود را تا حد ممکن مشابه HTTPS نگه دارد. همچنین طراحی پروتکل طوری است که اتصال‌هایی که ساختار درست یا گذرواژه معتبر ندارند به یک endpoint از پیش تعیین‌شده هدایت می‌شوند تا سرور در برابر کاوش‌گری^۴ مشکوک، رفتاری شبیه یک سرویس عادی (مثلاً HTTP) داشته باشد. این ویژگی‌ها Trojan را به نمونه‌ای جالب از رویکرد استار در قالب سرویس‌های رایج در بحث DPI و سانسور شبکه تبدیل می‌کند.

پروتکل Trojan را می‌توان در یک زنجیره ساده خلاصه کرد: کلاینت ابتدا یک TLS handshake کاملاً معمولی با سرور (معمولاً روی پورت ۴۴۳) برقرار می‌کند؛ دقیقاً شبیه زمانی که یک وب‌سایت HTTPS باز می‌شود. پس از احراز هویت، ترافیک پروکسی تونل شده در همان کانال TLS جریان پیدا می‌کند و نیازی به ایجاد تونل جداگانه با الگوی شروع متفاوت نیست. نتیجه این است که از دید ISP^۵ و فایروال، بسته‌ها عموماً شبیه ترافیک عادی مرور وب دیده می‌شوند و امضاء یا هدر اختصاصی واضحی برای علامت‌گذاری وجود ندارد. علاوه بر این، اگر تلاش برای کاوش یا درخواست غیرمجاز رخ دهد، سرور به جای خطای غیرعادی، یک پاسخ وب معتبر برمی‌گرداند؛ همین رفتار fail-safe شانس شناسایی خودکار را کاهش می‌دهد.



مقصد نهایی forward می‌شود و پاسخ دریافت‌شده دوباره به کلاینت بازگردانده می‌شود. این توصیف، VMess را در دسته پروتکل‌های پروکسی احراز هویت‌دار قرار می‌دهد که در آن مرحله تشخیص هویت/اعتبار، بخشی از خود پروتکل است.

VMess یک پروتکل وابسته به زمان است و برای کارکرد درست، ساعت کلاینت و سرور باید با هم هم‌گام باشند، یعنی هر دو با UTC هم‌گام باشند. این ویژگی، هم یک فرض طراحی است و هم می‌تواند در برخی سناریوها منبع خطا یا سطح حمله باشد. این پروتکل، یک پروتکل TCP-based است، یعنی در لایه انتقال از TCP استفاده می‌کند.

در نسخه مستند کانفیگ VMess در V2Fly نیز اشاره می‌شود که ترافیک VMess با رمزنگاری به شکل جریان‌های تصادفی دیده می‌شود (نوعی مبهم‌سازی از طریق رمزگذاری). این گزاره معمولاً در بحث DPI^۱ به عنوان رویکرد look-like-nothing مطرح می‌شود؛ یعنی ترافیک سعی می‌کند شبیه محتوای قابل تشخیص نباشد، هرچند پژوهش‌های امنیت شبکه نشان داده‌اند که حتی این سبک هم ممکن است با روش‌های تشخیص آماری/رفتاری، هدف قرار بگیرد.

VLESS

در مستند رسمی، VLESS به صورت صریح یک پروتکل stateless و lightweight معرفی می‌شود و به عنوان یک پل بین کلاینت و سرور Xray عمل می‌کند.

در همین منبع تأکید شده که برخلاف VMess، VLESS به زمان سیستم وابسته نیست و روش احراز هویت آن نیز UUID^۲ است. این توصیف، از نظر مهندسی یعنی هویت کاربر یا کلاینت با یک شناسه پایدار (UUID) معرفی می‌شود، اما طراحی پروتکل به جای تکیه بر اعتبار زمانی پیام‌ها، تلاش می‌کند سبک‌تر و با حساسیت کم‌تری نسبت به هم‌گام بودن ساعت باشد، نقطه‌ای که در برخی از محیط‌ها می‌تواند منبع خطا یا پیچیدگی باشد.

از منظر مدل لایه‌ای، VLESS بیشتر نقش پروتکل شناسایی و کنترل و حمل سبک را بازی می‌کند و معمولاً در یک پشته کنار لایه‌های دیگر معنا پیدا می‌کند. VLESS خودش به‌تنهایی

اهمیت چنین فایل‌هایی از زاویه مهندسی این جاست که آن‌ها یک لایه کم‌تر دیده‌شده در اکوسیستم اتصال را نمایندگی می‌کنند: لایه حمل‌ونقل دانش عملیاتی. یعنی علاوه بر این‌که خود پروتکل‌ها مشخص می‌کنند داده روی سیم چگونه رد و بدل می‌شود، این فایل‌ها مشخص می‌کنند کاربر چگونه آن دانش را ذخیره، منتقل و بازتولید می‌کند. یک فایل npv می‌تواند مجموعه‌ای از پروفایل‌ها و ترجیحات را یک‌جا جابه‌جا کند و به همین دلیل در فضای اشتراک‌گذاری کانفیگ‌ها محبوب می‌شود. چون تبدیل تنظیمات پیچیده به چیزی قابل حمل را ممکن می‌کند.

کلاینت‌ها، همراه همیشگی!

کلاینت‌ها در این اکوسیستم معمولاً نقش ظاهری یا مدیریتی دارند: یعنی به جای این‌که خودشان همه‌چیز را از صفر پیاده‌سازی کنند، کارشان مدیریت پروفایل‌ها، وارد یا خارج کردن کانفیگ‌ها، سوئیچ بین سرورها و کنترل یک هسته در پشت‌صحنه (مثل Xray یا sing-box) است. از این منظر، ابزارهایی مثل NekoRay (عموماً دسکتاپ) و V2rayNG (اندروید) و Happ (همه سیستم‌ها) بین کاربران محبوب هستند، چون تجربه کاربری ساده، مدیریت چند پروفایل و سازگاری با طیف وسیعی از پروتکل‌ها را فراهم می‌کنند. برخی کلاینت‌ها علاوه بر حالت پروکسی سیستم، گزینه‌هایی مثل TUN/VPN-mode هم ارائه می‌دهند تا ترافیک برنامه‌های بیشتری را پوشش دهند.

در کنار این‌ها، بعضی نام‌ها مثل V2Ray بیشتر به خود هسته اشاره دارند تا یک کلاینت رابط کاربری؛ اما در عمل کاربران با ابزارهایی سروکار دارند که یا مستقیماً V2Ray/Xray/sing-box را اجرا می‌کنند یا خروجی‌های استاندارد (مثل SOCKS/HTTP proxy) می‌دهند تا برنامه‌های دیگر از آن استفاده کنند. حتی Happ نیز، معمولاً در همین دسته قرار می‌گیرد، یک ابزار مدیریت اتصال که چند پروتکل را زیر یک رابط واحد جمع می‌کند. جمع‌بندی ساده این است: کلاینت خوب آن است که پشت‌صحنه هسته را درست و پایدار مدیریت کند، وارد یا خارج کردن مطمئن داشته باشد و بدون پیچیده کردن تجربه کاربری، پروفایل‌ها و سیاست‌های اتصال را قابل کنترل کند.

ساخته شده است. داک رسمی OpenVPN همچنین توضیح می‌دهد که بعد از این‌که نشست TLS برقرار و احراز شد، از همان کانال TLS برای تبادل موارد کلیدی استفاده می‌شود تا کلیدهای رمزنگاری یا تمامیت کانال داده ساخته شوند؛ ضمن این‌که OpenVPN می‌تواند روی UDP و همچنین TCP اجرا شود.

از پروتکل تا پروفایل؛ Npv چیست؟

شاید شما هم به تازگی با فایل‌های با فرمت npv آشنا شده باشید و از تونل Npv برای اتصال به اینترنت استفاده کرده باشید. اما این فایل‌ها دقیقاً چه هستند و حاوی چه اطلاعاتی هستند؟

تونل Npv (که گاهی با نام NapsternetV هم شناخته می‌شود) را می‌توان یک کلاینت چندپروتکلی دانست که هدفش ساده کردن استفاده از چند خانواده اتصال در یک برنامه واحد است. در توضیحات رسمی منتشرشده برای این برنامه اشاره می‌شود که از چند نوع روش و پروتکل رایج پشتیبانی می‌کند (از جمله خانواده V2Ray مانند VLESS یا VMess و نیز گزینه‌هایی مثل Trojan، Shadowsocks و SOCKS). همین چندپروتکلی بودن باعث می‌شود تونل Npv بیش‌تر از آن‌که یک کلاینت ساده باشد، نقش یک مدیر اتصال را بازی کند؛ جایی که کاربر پروفایل‌ها را نگه می‌دارد، بین آن‌ها جابه‌جا می‌شود و تجربه‌ای یکپارچه از چند فناوری متفاوت می‌گیرد.

در کنار خود برنامه، پسوند npv معمولاً به عنوان یک فایل پیکربندی و پروفایل برای همین ابزار مطرح می‌شود. نکته مهم این است که npv را نباید هم‌ردیف VMess یا VLESS دانست. npv پروتکل شبکه نیست، بلکه یک بسته‌بندی برای پروفایل‌ها و تنظیمات است که فرایند وارد/خارج کردن^۳ کانفیگ را ساده می‌کند. منابعی که پسوند فایل را معرفی می‌کنند هم npv را به عنوان فایل مرتبط با NapsternetV/Npv و در نقش فایل تنظیمات یا پروفایل دسته‌بندی می‌کنند.

Hysteria1 و Hysteria2

Hysteria (نسخه ۱) را می‌توان یک پروکسی مبتنی بر QUIC دانست که هدفش عملکرد خوب روی شبکه‌های ناپایدار و همچنین عبورپذیری در محیط‌های محدودشده است. در مستندات رسمی v1 صراحتاً گفته می‌شود پروتکل برای یک روش سریع، امن و قابل اعتماد جهت عبور از فایروال و سانسور طراحی شده و قابلیت استفاده روی TCP و همچنین UDP را دارد.

Hysteria2 (نسخه ۲) همین ایده را با یک تأکید پررنگ‌تر روی نقاب زدن^۱ HTTP/3 و مشخصات رسمی‌تر ادامه می‌دهد: در v2 آمده که برای یک شخص ثالث بدون اعتبارنامه (از جمله مرد میانی یا کاوش‌گر فعال)، سرور Hysteria2 باید مثل یک وب‌سرور استاندارد HTTP/3 رفتار کند و همچنین ترافیک رمزشده بین کلاینت و سرور در ظاهر شبیه ترافیک عادی HTTP/3 دیده شود. علاوه بر این، مستند v2 تأکید می‌کند که پروتکل باید بر پایه QUIC (استاندارد RFC 9000) پیاده‌سازی شود؛ یعنی حمل‌ونقل زیرین آن QUIC است و همین باعث می‌شود ویژگی‌های QUIC (مثل Multiplexing و رفتار مناسب‌تر روی مسیره‌های ناپایدار) نقش پررنگی در کارکرد پروتکل داشته باشند.

OpenVPN و Wireguard

WireGuard و OpenVPN، برخلاف پروکسی‌های قبلی که مطرح شدند، هر دو در خانواده VPN/Tunnel قرار می‌گیرند، اما فلسفه طراحی‌شان متفاوت است. WireGuard یک تونل شبکه مدرن با طراحی مینیمال است که طبق مستندات رسمی از Noise_IK handshake استفاده می‌کند و تمام بسته‌ها را روی UDP می‌فرستد؛ همچنین در مقاله رسمی WireGuard روی ایده نگاشت ساده «کلید عمومی همتا ↔ هویت تونل» و یک تبادل کلید یک‌رفت و برگشتی^۲ تأکید می‌شود.

در مقابل، OpenVPN یک VPN قدیمی‌تر و بسیار رایج است که طبق مستندات رسمی می‌تواند هم در حالت کلید ایستا و هم در حالت SSL/TLS (با گواهی‌های کلاینت یا سرور) کار کند و بر پایه رابط‌های مجازی TUN/TAP

شورش در لایه چهارم

عبور از فیلترینگ با نقض استانداردهای TCP



چکیده: در این مقاله به بررسی فنی دو پروژه ساختارشکن GFW-Knocker و paquet می‌پردازیم که با رویکردی کاملاً متفاوت از ابزارهای رایج، سامانه‌های فیلترینگ را دور می‌زنند. این پروتکل‌ها به جای تلاش برای مخفی شدن در لایه کاربرد، با نقض عمدی استانداردهای TCP و حذف مرحله دست‌تکانی سه‌مرحله‌ای^۲ در لایه انتقال^۳، نقطه ضعف و محدودیت‌های پردازشی فایروال‌های ملی را هدف قرار می‌دهند. در این مطلب خواهیم دید که چگونه برنامه‌نویسان با استفاده از سوکت‌های خام^۴ و تزریق مستقیم داده‌ها به بسته‌های ACK، توانسته‌اند سد سانسور اینترنت را به جای دور زدن، به شکلی بنیادین بشکافند.

مقدمه: در دنیای شبکه‌های کامپیوتری، همواره یک موش‌وگربه‌بازی جذاب بین سامانه‌های سانسور اینترنت (مانند فایروال بزرگ چین یا همان GFW^۵) و توسعه‌دهندگان ابزارهای دور زدن فیلترینگ وجود دارد. اگر به ابزارهایی که تا امروز استفاده کرده‌ایم (مثل Trojan، V2Ray یا انواع VPN‌ها) نگاهی بیندازید، متوجه می‌شوید که تمرکز اکثر آن‌ها روی مخفی کردن ترافیک در لایه کاربرد شبکه است. این روش‌ها سعی می‌کنند داده‌های شما را شبیه به یک وب‌گردی امن و عادی جلوه دهند. اما به تازگی پروژه‌ای در گیت‌هاب با نام gfw_resist_tcp_proxy رویکرد کاملاً جدیدی را معرفی کرده‌است: سوراخ کردن سد فیلترینگ در لایه انتقال.

فایروال‌های ملی چگونه IP ها را مسدود می‌کنند؟

قبل از بررسی راه‌حل، باید بدانیم در سطح کلان، سامانه‌های فیلترینگ چگونه کار می‌کنند. تصور کنید یک سرور مجازی^۶ مسدود شده‌است و فایروال باید جلوی ارتباط کاربران با آن IP خاص را بگیرد.

در حالت استاندارد، هر ارتباط TCP با سازوکاری به نام دست‌تکانی سه‌مرحله‌ای آغاز می‌شود:

۱. کلاینت یک بسته SYN برای سرور می‌فرستد (درخواست ارتباط).

۲. سرور با یک بسته SYN-ACK پاسخ می‌دهد (تأیید درخواست).

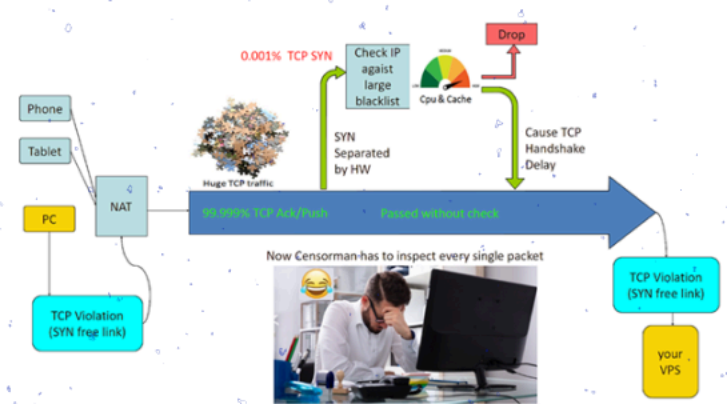
۳. کلاینت یک بسته ACK می‌فرستد و سپس ارسال داده‌ها آغاز می‌شود.

فایروال‌های ملی در درگاه‌های ورودی و خروجی کشور با حجم عظیمی از ترافیک (چندین ترابایت بر ثانیه) روبه‌رو هستند. بررسی تک‌تک بسته‌های عبوری برای پیدا کردن IP های لیست سیاه، نیازمند سخت‌افزارهای فوق‌العاده گران‌قیمت (میلیون‌ها دلار سرمایه‌گذاری) است و عملاً با نرم‌افزارهای معمولی قابل انجام نیست. بنابراین، فایروال‌ها یک میان‌بر پردازشی می‌زنند: آن‌ها فقط بسته‌های اولیه، یعنی SYN را بررسی می‌کنند. اگر IP مقصد بسته SYN در لیست سیاه باشد، آن بسته اصطلاحاً Drop می‌شود (یا با ارسال یک بسته جعلی TCP-RST، ارتباط قطع می‌شود) و ارتباط هرگز شکل نمی‌گیرد.

ایده اصلی پروتکل: نقض قوانین TCP^۷

اگر فایروال فقط بسته‌های SYN را مسدود می‌کند، چرا ما اصلاً برای شروع ارتباط بسته SYN نفرستیم؟! این پروتکل پیشنهاد می‌کند که مرحله دست‌تکانی سه‌مرحله‌ای را به طور کامل دور بزنیم. در این روش، کلاینت ارتباط را بدون ارسال بسته SYN و مستقیماً با فرستادن بسته‌های ACK یا PUSH آغاز می‌کند! بسته‌های ACK معمولاً حاوی داده‌های اصلی در میانه یک ارتباط هستند و تعداد آن‌ها در شبکه، صدها هزار بار بیشتر از بسته‌های SYN است.

فایروال‌های ملی معمولاً در برخورد با این بسته‌ها به صورت Stateless عمل می‌کنند؛ یعنی چون نمی‌توانند وضعیت میلیون‌ها ارتباط همزمان را در حافظه RAM خود نگه دارند، فرض را بر این می‌گذارند که این بسته ACK متعلق به ارتباطی است که قبلاً با موفقیت برقرار شده، پس به آن اجازه عبور می‌دهند! تلاش برای مسدود کردن تمام بسته‌های ACK، باعث افت شدید سرعت روترهای مرکزی و از هم پاشیدن کل شبکه اینترنت می‌شود. در نتیجه، داده‌های ما در قالب بسته‌های ACK به راحتی از فایروال عبور کرده و به سرور مسدود شده می‌رسند.



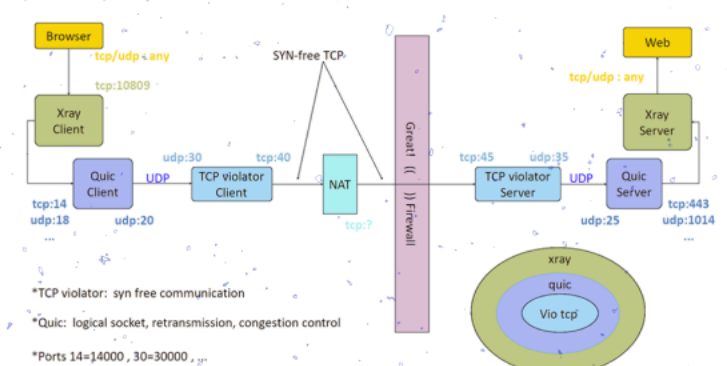
تصویر ۱ (معماری کلاسیک مسدودسازی): کلاینت در تلاش است با استاندارد TCP به سرور متصل شود. تجهیزات فیلترینگ (مثل GFW)، پورت و IP را شنود کرده و به محض رؤیت پرچم SYN، بسته را معدوم کرده و مانع از رسیدن آن به مقصد می‌شوند.

تغییر پارادایم: از مخفی شدن تا شکافتن سد

اکثر روش‌های ضدسانسور فعلی، سعی در مخفی شدن دارند. اما این پروتکل پارادایم فیلترینگ را تغییر می‌دهد. ما در این روش نیازی به مخفی شدن نداریم؛ بلکه با صدای بلند به همان IP مسدود شده متصل می‌شویم، اما از مسیری استفاده می‌کنیم که فایروال به دلیل محدودیت‌های سخت‌افزاری خود، توان پردازشی لازم برای مسدود کردن آن را ندارد. این یعنی شکافتن^۸ سد فیلترینگ به جای دور زدن آن. فرقی نمی‌کند لایه‌های بالایی از چه پروتکلی استفاده کنند، این روش در پایین‌ترین سطح ممکن، هر پورتهای سوراخ می‌کند.

چالش‌های فنی و نحوه پیاده‌سازی

طبیعتاً سیستم‌عامل‌های ما به برنامه‌ها اجازه نمی‌دهند که بدون ارسال SYN، ارتباط شبکه‌ای برقرار کنند. برای دور زدن این محدودیت، پروتکل از تکنیک سوکت‌های خام استفاده می‌کند و بسته‌های شبکه را بایت‌به‌بایت به صورت دستی می‌سازد (Packet Crafting).



تصویر ۲ (معماری دور زدن با نقض قوانین TCP): کلاینت با حذف پرچم SYN، داده را مستقیماً کپسوله می‌کند. فایروال این ترافیک را بی‌خطر تشخیص داده و عبور می‌دهد و سرور نیز برای دریافت و رمزگشایی این بسته‌های غیرمعمول آماده است.

در قطعه کد ساده شده زیر می بینیم که چگونه یک بسته TCP با پرچم های دستکاری شده ساخته می شود.

چه اتفاقی در این کد افتاد؟ در بخش دوم کد، ما صراحتاً پرچم ACK و PSH را true قرار داده ایم و هیچ پرچم SYN ای مقداری نمانده است. سپس با استفاده از SerializeLayers، این لایه های نرم افزاری را به همراه پیام اصلی خود به یک رشته خام از بایت ها تبدیل می کنیم. حالا این بسته غیرمتمعارف، از طریق سوکت های خام مستقیماً به کارت شبکه فرستاده می شود. فایروال با دیدن پرچم ACK تصور می کند این بسته متعلق به یک ارتباط از پیش تأیید شده است و اجازه عبور آن را صادر می کند!

نتیجه گیری

پروژه نقض قوانین TCP یک نمونه بی نظیر برای درک عمیق مدل OSI و رفتار پروتکل های شبکه است. این پروژه نشان می دهد که چگونه شناخت دقیق نقاط ضعف سیستم های کلان (مانند گلوگاه های پردازشی فایروال ها) می تواند منجر به خلق راهکارهایی شود که پیشرفته ترین فایروال های جهان را نیز فلج کند.

ارتباط با پایداری خیره کننده ای برقرار می ماند. پروژه paquet با بهره گیری از کتابخانه هایی مثل pcap (برای شنود بسته ها) و gopacket (برای ساخت دستی بسته ها)، مستقیماً با لایه های پایین سیستم عامل تعامل کرده و پشته استاندارد TCP/IP سیستم عامل را به کل دور می زند. این مخزن اثبات می کند که ایده سوراخ کردن فایروال از یک تئوری دانشگاهی فراتر رفته و در حال تبدیل شدن به ابزاری قدرتمند، پایدار و عملیاتی در لایه انتقال شبکه است.

دست به کد شویم

برای کالبدشکافی یک پکت دست ساز در زبان Go در پروتکل هایی مثل paquet، برنامه نویسی نمی تواند از توابع استاندارد شبکه در سیستم عامل (مانند net.Dial در زبان Go) استفاده کند؛ چرا که سیستم عامل به صورت خودکار یک بسته SYN را برای شروع ارتباط ارسال می کند که برخلاف هدف ماست. برای دور زدن این رفتار، توسعه دهندگان از کتابخانه هایی مانند gopacket استفاده می کنند تا بسته ها را بایت به بایت، به صورت دستی طراحی کنند (عملی که به آن Packet Crafting می گویند).

محدودیت بزرگ این روش

این پروتکل با وجود ایده نبوغ آمیزش، روی برخی شبکه های موبایل (مثل اپراتورهای 4G و TD-LTE) به مشکل می خورد. دلیل آن، وجود دستگاه های NAT پیشرفته (CGNAT) در شبکه های موبایل است. این روترها برای عبور ترافیک بین IP داخلی گوشی شما و اینترنت، باید جدول پورت ها را به روز کنند. اگر روتر NAT اپراتور موبایل، بسته SYN شما را نبیند، اصلاً پورت را باز نمی کند و به بسته های ACK ساختگی شما اجازه خروج نمی دهد. هم چنین نیاز به دسترسی Root باعث می شود اجرای این روش روی گوشی های موبایل هوشمند برای کاربران عادی بسیار دشوار باشد.

تکامل ایده: از مفهوم اولیه تا پروژه paquet (نسخه Go)

همان طور که اشاره شد، مخزن gw_resist_tcp_proxy، بیش تر نقش یک اثبات مفهوم^۱ را ایفا می کند تا نشان دهد این روش ساختار شکنانه امکان پذیر است. اما دنیای متن باز به سرعت این ایده خام را پرورش داد. نتیجه این تکامل، تولد پروژه دیگری به نام paquet است که دقیقاً از همین سازوکار (یعنی نقض استانداردهای TCP و دور زدن دست تکانی سه مرحله ای) استفاده می کند، اما با معماری بسیار بهینه و با زبان Go توسعه یافته است. ورود زبان Go و باز نویسی این پروتکل در مخزن paquet، دو مزیت حیاتی به همراه داشته است:

- سرعت و مدیریت هم زمانی^۲: زبان Go ذاتاً برای پردازش های سنگین شبکه ای طراحی شده است. به همین دلیل، paquet می تواند هزاران اتصال هم زمان را بدون افت عملکرد و با مصرف بهینه منابع سرور (CPU و RAM) مدیریت کند.
- تلفیق با پروتکل KCP: توسعه دهندگان paquet به جای اتکای صرف به بسته های خام، پروتکل KCP را روی این بسته های دستکاری شده TCP پیاده سازی کرده اند. پروتکل KCP برای شبکه هایی با افت بسته^۳ بالا بهینه سازی شده است. این یعنی حتی در اینترنت های پر از اختلال، خطاهای شبکه با سرعت جبران شده و

```
package main
import (
    "net"
    "github.com/google/gopacket"
    "github.com/google/gopacket/layers"
)
func main() {
    // 1. Creating Network Layer (IP)
    ipLayer := &layers.IPv4{
        SrcIP:    net.ParseIP("192.168.1.10"), // Client IP
        DstIP:    net.ParseIP("203.0.113.50"), // Filtered Server IP
        Version:  4, Protocol: layers.IPProtocolTCP
    }
    // 2. Creating Transport Layer (TCP) - Magic is here!
    tcpLayer := &layers.TCP{
        SrcPort: layers.TCPPort(43210),
        DstPort: layers.TCPPort(443),
        ACK:     true, // Activating ACK (Without SYN!)
        PSH:     true, // PSH Flag for sending data immediately
        Window:  1500
    }
    // Calculating checksum to avoid packets from being dropped by routers
    tcpLayer.SetNetworkLayerForChecksum(ipLayer)
    // 3. Capsulate and convert layers to bytes (Serialization)
    buf := gopacket.NewSerializeBuffer()
    opts := gopacket.SerializeOptions{ComputeChecksums: true, FixLengths: true,}
    // Mix IP and TCP layers (Payload)
    gopacket.SerializeLayers(buf, opts, ipLayer, tcpLayer,
        gopacket.Payload([]byte("Secret Data Request!")))
    // Ready to inject to network card
    packetBytes := buf.Bytes()
}
```


مامانندیم و اینترنت پرو!

بعضی چیزها زود فراموش می‌شوند.



سورنا کیا

کارشناسی ۱۴۰۳

دانشگاه صنعتی شریف

۴ دقیقه

در دی‌ماه سال گذشته که متن‌های «قطعی بزرگ» و «اینترنت، حق مسلم» را می‌نوشتیم، نقل‌قول‌ها و نشانه‌هایی از اینترنت پرو و طبقاتی را با تعجب ذکر می‌کردم و آن را برای جامعه خطرناک می‌دانستم؛ اما اگر بخواهم واقعیت را بگویم، هیچ‌گاه تصور نمی‌کردم که به این زودی جامعه عمل به خود بپوشد و عملیاتی شود، هیچ‌گاه فکرش را هم نمی‌کردم که به این زودی دوباره دست‌به‌قلم شوم تا متنی چنین دردناک از بار مسئولیتی به این حد سنگین که بر دوش ما نهاده شده، به تحریر در بیاورم. آن زمان که حتی ۱۰۰ روز هم از آن نمی‌گذرد، تصور می‌کردیم که بزرگ‌ترین قطعی اینترنت تاریخ را تجربه کرده‌ایم و سال‌ها قرار نیست مانند آن را ببینیم؛ اما پیش از آن که متن‌ها به مرحله چاپ برسند، قطعی به مراتب بزرگ‌تر را تجربه کردیم؛ قطعی‌ای که دیگر فقط قطعی نبود، بلکه اتصالی هولناک برای عده‌ای خاص به نام «اینترنت پرو» را به همراه داشت.

اما اکنون که اینترنت پرو به میان آمده و گاهی در بازار سیاه معامله می‌شود، و ابزارهای خاص اتصال مانند VPN^۱ شریف نیز گاهی در دسترس قرار می‌گیرند، شاید یک پرسش بیش از پیش خودنمایی کند: «**وظیفه ما چیست؟**». آیا ما اعضای جامعه نیز، مسئولیتی در قبال استفاده از این اینترنت طبقاتی ناعادلانه داریم یا باید تمام مسئولیت ناشی از این پدیده را متوجه دولت و نهادهای تصمیم‌گیر بدانیم و خود، به راحتی از آن استفاده کنیم و به آن مشروعیت ببخشیم؟ یا آن که نسخه‌ای برای همه جامعه بیچیم که نباید از این اینترنت استفاده کنید، ولو اگر خسارات سنگینی متحمل شوید؟

باید ابتدا کمی به این مقوله ناخوشایند، یعنی پیدایش اینترنت پرو بپردازیم. سال‌ها صحبت از پدیده‌ای به نام «سیم‌کارت سفید» در میان بود، اما هیچ‌گاه به‌طور علنی تأیید نشد و سازوکار استفاده از آن نیز مشخص نشد. در دی‌ماه سال ۱۴۰۴، شایعاتی مبنی بر ایجاد سیم‌کارت‌هایی که عادی نیستند و **پرو** نام دارند، به میان آمد. در اوایل اسفندماه همان سال، بعضی از گروه‌های تلگرامی آگهی‌هایی از فروش آن منتشر کردند و

مشترک گرامی؛

به دلیل بروز اشکال فنی در بروزرسانی سامانه کد دستوری، سرویس اینترنت پرو که در مرحله آزمایش بوده، به اشتباه در اختیار برخی مشترکان قرار گرفته و فعالسازی توسط شما انجام شده است.

این سرویس غیرفعال شده و هزینه پرداختی به شما عودت گردید. همچنین وضعیت اینترنت شما به حالت قبل برگشته است.

از شکیبایی و همراهی شما سپاسگزاریم.

شده است و به صورت آشکار یک نظام طبقاتی ساخته است که در آن افراد ثروتمند حق دسترسی بیشتری نسبت به باقی جامعه به اینترنت دارند؟! آیا نباید از اپراتورهای مربوطه بپرسیم که در حال ارائه چه خدمات اضافه‌ای هستند که آن قدر اختلاف قیمت نسبت به اینترنت در دسترس عموم وجود دارد؟!!

هرچه که هست، گوشی به سخنان ما بدهکار نیست. قرار نیست که گفته‌های ما موجب اتصال اینترنت عموم و از میان برداشته شدن طرح اینترنت پرو شود، همان‌طور که ایجاد آن به خواسته ما نبوده است. در این جا به پرسش اصلی این متن برمی‌گردیم. آیا این اختیار نداشتن ما، نشانه‌ای از سلب مسئولیت ما در برابر ایجاد این نظام طبقاتی است که ثروتمند را ارجح بر نیازمند، دانشجو را مقدم بر آحاد جامعه و پزشک را برتر از بیمارانش بر می‌شمارد؟!!

بی‌شک، شانه خالی کردن است اگر فقط بگوییم که هیچ مسئولیتی نداریم. **ما هم مسئولیم.** هر گیگابایت اینترنتی که خریداری می‌شود و یا هر VPN ای که به سبب دانشجو بودن مان به ما اختصاص داده می‌شود، در واقع مهر تأییدی است بر این رانت. همان‌طور که وقتی عده‌ای خاص به سبب ارتباطات‌شان می‌توانند خودروها را با قیمت بسیار پایین‌تر از قیمت بازار از کارخانه خریداری کنند، در ذهن ما تصویری از ناعدالتی نقش می‌بندد؛ اگر اتصال به اینترنت حق است، داشتن خودرویی به قیمت تمام‌شده کارخانه هم حق است. اگر این‌گونه استدلال کنیم که اتصال به اینترنت

امکان خرید آن برای عده‌ای فراهم شد^۲. پس از شروع جنگ، در روز ۱۲ اسفند، یک کد دستوری منتشر شد که با شماره‌گیری آن و پرداخت ۴۰ هزار تومان به ازای هر گیگابایت، استفاده از اینترنت با محدودیت کمتر از حد معمول ممکن می‌شد - با آن که تمامی پلتفرم‌ها هنوز رفع فیلتر نشده بودند، اما بسیاری از آن‌ها مانند تلگرام، اینستاگرام، توئیتر و یوتیوب بدون محدودیت اجرا می‌شدند. اما این سرویس بعد از چند ساعت از دسترس خارج شد و اپراتورهای مربوطه بیان کردند که به دلیل بروز اشکال فنی در بروزرسانی سامانه کد دستوری، سرویس اینترنت پرو به اشتباه در اختیار کاربران قرار گرفته است.

اشتباهی که نشان از عزم آنان، جهت ساخت مسیری برای تبعیض آشکار در اتصال بود. پس از آن، هر روز اخبار جدیدی از فعال شدن اینترنت پرو برای عده‌ای به گوش می‌رسید و این اینترنت طبقاتی مشروعیت بیشتری به خود می‌بخشید؛ تا آن جا که در نهایت با تأیید مسئولین دولتی همراه شد؛ تا جایی که در ۲۲ اردیبهشت، مهاجرانی - سخنگوی دولتی که با وعده برخورد با اینترنت طبقاتی که آن زمان اینترنت سفید نام داشت، به روی کار آمد- در پاسخ به پرسش‌های خبرنگاران در خصوص اینترنت پرو می‌گوید که اینترنت پرو، مصوبه شورای عالی امنیت ملی را دارد که آقای رئیس‌جمهور، رئیس آن شورا هستند. در ادامه نیز ذکر می‌کند که این اینترنت، مخصوص کسب‌وکارهاست. مشخص نیست هنگامی که عموم مردم دسترسی به اینترنت ندارند، صاحبان کسب‌وکار چگونه می‌توانند محصولات یا خدمات خود را به مردم معرفی کنند. در ادامه خانم مهاجرانی می‌گویند که کشور در شرایط جنگی است و این اقتضاء شرایط جنگی است که امنیت مردم در اولویت نسبت به همه چیز قرار بگیرد^۳. اما در این هنگام باید به یک پرسش بنیادین و سخت پاسخ داده شود: اتصال اینترنت زندگی مردم را در خطر بزرگ‌تری قرار می‌دهد یا قطعی آن؟!!

با تمامی این کشمکش‌ها، هم‌چنان اتصال عموم مردم قطع است و طرح اینترنت پرو استوار است؛ طرحی که باعث ایجاد بازار سیاهی آشکار شده و به راحتی در دسترس بسیاری قرار گرفته است. پرسش دیگری که باید مطرح شود این است که آیا اتصال تا این اندازه گسترده، باعث در خطر افتادن امنیتی که خودشان می‌گویند، نمی‌شود؟! آیا غیر از این است که امکان اتصال برای افرادی که از تمکن مالی بالاتری برخوردار بودند، فراهم

«ضروری است!» هست یا نیست؟ اگر هست، آیا «ضروری است!» دیگری وجود دارد که در مقابل آن باشد؟ آن گاه کدام یک را باید برگزید؟ حقیقت این است که هر یک از ما یک بار زیسته‌ایم و این بدین معناست که به واقع زیسته‌ایم، پس هیچ‌کس نمی‌تواند بگوید که چه درست است و چه غلط. کدام انتخاب ما اثر مثبت‌تری خواهد داشت.

آری، پرسش ما همان پرسشی است که پارمنیدس^۲ از خود پرسید. **سنگینی یا سبکی؟** سنگینی بار مسئولیت و تعهد ناشی از قبول این نوع اتصال، یا سبکی حاصل از رد آن؟ شاید این سبکی و سنگینی با یک‌دیگر متضاد باشند، اما به‌واقع بسیار به هم شبیه هستند.

هر دو به‌گونه‌ای تحمل‌ناپذیر هستند و هیچ‌یک بر دیگری برتر نیست. هر کدام از ما باید در خود بنگریم و این را از خود بپرسیم: **«سبکی رد این اتصال، یا سنگینی پذیرش آن؟»**



سیستم برای این‌که مردم علیه هسته مرکزی قدرت متحد نشوند، بازی حذف افقی راه می‌اندازد. در یک حالت طبیعی، وقتی فساد، تبعیض یا فقر در جامعه‌ای بالا می‌رود، نگاه مردم به سمت بالا (یعنی حکومت، سیاست‌گذاران و هسته مرکزی قدرت) معطوف می‌شود و جامعه متوجه می‌شود که ریشه مشکلات در تصمیمات ساختار قدرت است. این حالت برای حکومت‌ها بسیار خطرناک است، زیرا باعث می‌شود پیکان اعتراضات به سوی آن‌ها گرفته شود. حکومت‌های هوشمند برای فرار از تقابل عمودی، ساختار بازی را تغییر می‌دهند و آن را افقی می‌کنند. یعنی با توزیع هدفمند رانت، امتیازات انحصاری یا مجوزهای خاص به یک قشر، صنف یا گروه مشخص، کاری می‌کنند که مردم به جای نگاه کردن به بالا، به بغل‌دستی خود نگاه کنند. «توتالیتریزم تنها به نابودی قابلیت‌های سیاسی انسان‌ها بسنده نمی‌کند؛ بلکه انزوای اجتماعی را به یک تجربه روزمره تبدیل می‌کند. مأموریت اصلی این سیستم‌ها، ویران کردن تمام روابط اصیل میان انسان‌هاست؛ به گونه‌ای که هر فرد، هم‌شهری خود را نه یک شریک یا همراه، بلکه یک رقیب بالقوه برای بقا یا یک تهدید برای امتیازات ناچیز خود ببیند.»

لازم است ذکر کنم که دسترسی به اینترنت برای عموم مردم، طبق منشور سازمان ملل، یکی از حقوق اولیه بشری شناخته می‌شود، مانند آب! در نظر داشته باشید که یک «اما» مطرح است: «اما»یی بنیادین و اساسی.

چه کسی به ما حق قضاوت دیگران را داده است؟ چه کسی به ما این حق را داده است که برای جامعه‌ای به این بزرگی یک نسخه واحد بپیچیم و بدون در نظر گرفتن شرایط هر فرد به او بگوییم «تو حق استفاده از این مقوله را نداری»؟ اگر زندگی فردی با این اینترنت گره خورده بود، آن وقت چه؟

اما آیا فقط در این حالت حق استفاده از اینترنت را به افراد می‌دهیم؟ مرز استفاده از این نوع اینترنت کجاست؟ آیا ما می‌توانیم تعیین کنیم؟ میلان کوندرا^۱ در کتاب «بار هستی»، وقتی دوره‌های مهم زندگی را ترسیم می‌کند، انتخاب را با «ضروری است!» موجه می‌سازد. حال ما نیز در یک دوره‌ای قرار داریم و وقت آن است که با خود بیندیشیم که آیا این اتصال یک

یک امر ضروری است، اما خودروی ارزان نه، باید از خود بپرسیم که آیا واقعاً این‌طور است؟ آیا ما حقوقی داریم که یکی بر دیگری ضرورت دارد؟ آیا می‌توان از حق خودرو چشم پوشید و از اتصال اینترنت برای خودمان، نه؟

آیا اتصال ما دانشجویان یا پزشکان و یا صاحبان کسب‌وکارها مهم‌تر از دیگر اعضای جامعه است؟ چون این اقشار جامعه فعالیت‌های به‌ظاهر مهم‌تر از دیگران انجام می‌دهند، صلاحیت بیشتری دارند؟

حال اگر فردی نیاز مبرم به اتصال برای دسترسی به فعالیت‌های به‌ظاهر کم‌اهمیت‌تر، مانند وقت‌گذرانی در اینستاگرام، دیدن ویدیو از یوتیوب و بسیاری از امور به‌ظاهر کوچک دیگر که آرامش ذهنی او را فراهم می‌کند، داشته باشد و به‌دلیل قطعی دچار مشکل حاد روانی شود، بخشی از مسئولیتش با مایی که آسوده با این عنوان که حق بیشتری داریم، نیست؟! آیا اتصال من کم‌خطرتر از اتصال پدربزرگم است، که به من این حق داده شده است، اما به او نه؟

مردم، مقابل مردم!

توتالیتریزم چطور روح جمعی را می‌کشد؟



یکی از قدیمی‌ترین شیوه‌های حفظ قدرت، آن چیزی است که در ادبیات سیاسی از آن با عنوان «تفرقه بینداز و حکومت کن» یاد می‌شود. گاه تنها کافی است منافع گروه‌های مختلف به شکلی تنظیم شود که هر گروه، بقای خود را در بقای سیستم و در تضاد با دیگر مردمان ببیند. هانا آرنت به خوبی توضیح می‌دهد که حکومت‌های تمامیت‌خواه چگونه با اعطای موقعیت‌های انحصاری به یک گروه، آن‌ها را از بدنه جامعه جدا کرده و روبه‌روی هم‌شهری‌هایشان قرار می‌دهند. وی در کتاب توتالیتریزم می‌گوید: «ساختار توتالیتر، جامعه را به لایه‌های بی‌شماری از امتیازات منحصربه‌فرد تقسیم می‌کند. این سیستم به گونه‌ای طراحی شده که هر فرد، در هر رتبه‌ای که هست، احساس کند نسبت به لایه پایینی خود دارای یک امتیاز ویژه و انحصاری است؛ امری که باعث می‌شود او برای حفظ

این جایگاه کوچک، مأمور کنترل و سرکوب دیگران شود.» آرنت در بحث خود درباره افول ملت-دولت‌ها اشاره می‌کند که چطور حکومت‌ها مفهوم شهروندی و منافع ملی یکسان را نابود می‌کنند و به جای آن، مدل امتیاز بر اساس وفاداری را جایگزین می‌کنند: «در دولت‌های توتالیتر، دولت دیگر به‌عنوان نماینده قانون و منافع مشترک همه شهروندان عمل نمی‌کند، بلکه به ابزاری در دست یک جنبش یا قشر خاص تبدیل می‌شود. در این حالت، رفاه و امتیازات تنها به کسانی تعلق می‌گیرد که بخشی از این بدنه وفادار باشند و مابقی جامعه به حاشیه رانده می‌شوند.» یکی از عمیق‌ترین تحلیل‌های آرنت این است که حکومت‌ها برای تضمین وفاداری اقشار خاص، آن‌ها را در منافع حاصل از ظلم یا رانت شریک می‌کنند. وقتی شما از یک سیستم فاسد، رانت یا امتیاز ویژه‌ای بگیرید که حق دیگران است، عملاً هم‌سرنوشت آن سیستم می‌شوید. «راز موفقیت این سیستم‌ها در این است که توانسته‌اند توده‌ها را در جنایت‌ها و منافع خود شریک کنند. آن‌ها فضایی خلق می‌کنند که در آن، افراد احساس می‌کنند پل‌های پشت‌سرشان خراب شده و بقای شخصی‌شان کاملاً به بقای رژیم گره خورده است.»

۱. تأمین‌کنندگان سرویس‌های قطع و محدودسازی اینترنت

۲. فروشندگان اینترنت پرو (اینترنت طبقاتی و آیارتاید)

۳. بازیگران بزرگ سرویس‌های دور زدن فیلترینگ

۴. بازار خانگی و خرده‌فروشان کافه‌فینگ

در این میان، بازیگران کوچک و خانگی نیز در بازار حضور دارند که می‌توان آن‌ها را به بازیگران جزء در صنعت مافیایی خودرو تشبیه کرد. اگر فرض کنیم با یک مافیای بزرگ اینترنت مواجه هستیم، طبیعی است که برای ساکت نگه‌داشتن افکار عمومی، باید سهم کوچکی از بازار را به خود

برگردیم؛ پیش‌بینی دقیق درآمد این شرکت‌ها ممکن نیست. تنها داده موجود، گزارشی از خبرگزاری تسنیم (به‌عنوان یک رسانه حاکمیتی) است که با تخمین ۳ میلیون مصرف‌کننده برای طرح پرو، درآمد یک‌ساله کاسبان را ۵۰۰ میلیون دلار برآورد کرده بود. این شرکت‌ها پیش از معرفی «اینترنت پرو»، از طریق فروش خطوط سفید نیز درآمدزایی می‌کردند و چه‌بسا هزینه خدمات به‌ظاهر باکیفیت خود را از بودجه عمومی و بیت‌المال تأمین کرده باشند. تنها راه دسترسی به آمار دقیق این گروه و گروه اول، افشای اسناد محرمانه شرکتی و دولتی است.

گروه سوم و چهارم: فروش فیلتر شکن‌های خط سفید، استارلینک و تجهیزات ماهواره‌ای

غیررسمی‌ترین بخش صنعت قطعی اینترنت در این لایه نهفته است. تخمین سرمایه عظیم در گردش در این بخش، کاری دشوار اما ممکن است؛ به‌ویژه آن‌که بازیگران بزرگی مانند آقازادگان فروشنده وی‌پی‌ان یا قاچاق‌چیان تجهیزات استارلینک حضور پررنگی در آن دارند؛ موضوعی که محاسبه درآمد این افراد را به امری پرمخاطره تبدیل می‌کند. محاسبه درآمدهای بازیگران خانگی نیز به دلیل گستردگی، دشواری‌های زیادی دارد. با این حال، آمارها و برآوردهایی از گردش مالی این بخش وجود دارند که قابل تأمل هستند.

- نرخ‌های نجومی در دوران پیک قطعی: در جریان تنش‌ها و قطعی‌های دی‌ماه و قطعی‌های اسفند تا اردیبهشت، مبالغ شگفت‌آوری برای هر گیگابایت اینترنت آزاد مطرح می‌شد. نرخ تعادلی بازار برای کانفیگ‌های استارلینک از ۲ تا ۴ میلیون تومان و برای کانفیگ‌های معمولی از ۳۰۰ تا ۷۰۰ هزار تومان متغیر بود. در زمان اوج محدودیت‌ها، تنها یکی از کیف پول‌های دیجیتال شناسایی‌شده در حوزه فروش فیلتر شکن توانست رکوردی میلیون دلاری ثبت کند.

ارقام فروش کانفیگ در اواخر دوره محدودیت‌ها و با کاهش نسبی سخت‌گیری‌ها، حدود ۳۰ تا ۴۰ درصد افت کرد. در این وضعیت آن سوال همیشگی

گروه دوم: فروش اینترنت پرو (اینترنت طبقاتی و آپارتاید)

در این بخش، اپراتورهای تلفن همراه، بهترین نمونه برای بررسی هستند. از آن‌جا که از میان اپراتورهای اصلی، تنها یک اپراتور در بورس تهران عرضه شده‌است، صرفاً می‌توان داده‌های همین شرکت را ارزیابی کرد.

طبق بررسی‌های صورت‌گرفته در سامانه کدال، این شرکت با وجود تمام چالش‌های ناشی از قطعی اینترنت در ماه‌های اخیر، روند درآمدی مطلوبی را حفظ کرده‌است. این امر با توجه به قطعی اینترنت بین‌الملل و تعرفه پایین‌تر ترافیک داخلی و همچنین گرایش بیشتر مردم به استفاده از خطوط اینترنت ثابت، منطقی به نظر نمی‌رسد؛ به‌ویژه در شرایطی که شرکت‌های مشابه در حوزه اینترنت ثابت، با افت محسوس درآمدهای خود نسبت به سال گذشته مواجه شده‌اند، تا جایی که شایعه ورشکستگی برخی از آن‌ها نیز مطرح شد.

به دلیل وجود نداشتن شفافیت لازم در صورت‌های مالی این شرکت‌ها، امکان دسته‌بندی دقیق درآمدها وجود ندارد و این بنگاه‌ها می‌توانند درآمدهای حاصل از فروش سیم‌کارت‌های «سفید» را در بخش‌هایی مانند فروش کلی اینترنت و خدمات، پنهان کنند.

از سوی دیگر، شواهد نشان می‌دهد که بساط فروش پنهانی اینترنت طبقاتی حتی پیش از تنش‌های اخیر نیز برقرار بوده‌است. سیم‌کارت‌هایی موسوم به «سفید» که به خبرنگاران، آقازادگان، چهره‌های سیاسی و نزدیکان آن‌ها اعطا شده بود و برای مدتی طولانی پنهان نگاه داشته شد. پنهان‌کاری چهره‌های سیاسی و صاحبان رانت طبیعی است، اما این‌که خبرنگاران وابسته و غیروابسته به دولت، این رانت بزرگ را مدت‌ها کتمان کرده بودند، لکه ننگ بزرگی بر پیشانی آنان است و بیش از پیش نشان می‌دهد که چرا افکار عمومی به خبرگزاری‌ها اعتمادی ندارند. چه تضمینی وجود دارد که این افراد قلم خود را به بهایی ناچیز نفروشد و به مردم دروغ تحویل ندهند؟ از حاشیه خارج شویم و به بحث اصلی

مردم واگذار کنند. مافیاهای بزرگ اینترنت می‌دانند که بهترین ضامن بقای فساد، توزیع و همگانی کردن آن است. جوانانی که باید استعدادشان در پروژه‌های علمی و صنعتی ملی استفاده می‌شد اما اکنون بیکار هستند، باید چنین حس کنند که در سیستم شما از طریق کانفیگ‌فروشی آینده‌ای خواهند داشت!

این دسته از جوانان یا این کار را به‌عنوان شغل اصلی و فرعی ادامه می‌دهند، یا از این چرخه خارج شده و مهاجرت می‌کنند تا از دانش خود در مسیر مفیدی بهره ببرند و یا این‌که به مرور زمان به مافیاهای اینترنتی جدیدی تبدیل می‌شوند. در هر صورت، سیستم فاسد طراحی‌شده برنده است؛ شما به‌عنوان یک بازیگر بزرگ به درآمدهای دلاری خود می‌افزایید، کانفیگ با قیمت نجومی به دست مردم می‌رسد و آن بازیگر کوچک نیز با ترس و لرز فراوان، درآمد ناچیزی کسب می‌کند. مردم می‌بازند و فساد برنده می‌شود...

بررسی گردش مالی کاسبان فیلترینگ

بررسی ابعاد مالی این حوزه، عمق فاجعه را بیشتر نمایان می‌کند. در ادامه به تفکیک گروه‌ها، به این موضوع می‌پردازیم.

گروه اول: شرکت‌های ساختار یافته و پیمانکار

متأسفانه قراردادهای رسمی قابل‌استنادی در درگاه‌های دولتی برای این موضوعات وجود ندارد؛ چرا که شفافیت قراردادهای دولتی در کشور ما صرفاً در آستانه انتخابات مطرح می‌شود. پس از آن، با طرح بهانه‌های امنیتی، شرایط تحریم و این‌که شفافیت به‌مثابه «پاس گل به دشمن» است، این مفهوم به حاشیه رانده می‌شود و در نتیجه منبع رسمی‌ای در این خصوص در دسترس نیست.

مشخص نیست که این افراد خدمات خود را گران فروخته‌اند یا صرفاً با انگیزه‌های ایدئولوژیک فریب خورده‌اند. با این حال، امیدواریم اگر مخاطب این متن هستند

(There is an Imposter among us) دیدگاهی برآوردی نسبت به گردش مالی آقازاده‌ها و اینترنت سفیدفروشان پیدا کنند و دست‌کم کمی از حاشیه سود آن‌ها بکاهند و خود را ارزان بفروشند!

اینترنت توسط فرد، سازمان، نهاد یا هر چیزی که هیچ کس نمی داند چه کسی یا چه چیزی است، قطع شد. سکوهای داخلی که عملاً بهترین فرصت را برای خودنمایی در این شرایط داشتند، دائم دچار اختلال بودند و تازه وقتی همه از آن ها استفاده کردند، فهمیدند چه مشکلات زیرساختی و حتی محصولی بزرگی

تخمین دقیق اعداد و ارقام در این حوزه به

بعضی‌ها می‌گویند اینترنت بالاخره وصل شده‌است، اما بهتر آن است که بگوییم فیلترشکن‌ها بالاخره وصل شدند؛ چون محدودیت‌ها آن‌قدر بدتر شده که بدون فیلترشکن نمی‌توان حتی استفادهٔ روزمره‌ای از فناوری داشت. اما داستانی که ما گفتیم، داستان اینترنت نبود.

به هر حال، مسئله این نیست که چه کسی و با چه اهدافی ما را به اینترنت آزاد وصل کرد، مسئله این است که چرا از ابتدا اینترنت آزاد نداشتیم...

اینترنت دم‌دستی‌ترین بهانه برای ما بود تا از رنجی که برای رسیدن به حقوق اولیه خود می‌کشیم، بگوییم. از اینترنت گفتیم تا یادمان نرود چه دروغ‌هایی شنیدیم و می‌شنویم و چطور یکی از بدیهی‌ترین نیازهای زندگی‌مان آن قدر گره‌اش کور شد که دیگر هیچ‌کس نمی‌تواند از لابه‌لای این همه فساد، رانت و امنیتی‌بازی آن را نجات دهد. اینترنت قربانی شد؛ همان‌طور که نیازهای اولیه دیگر، مثل زندگی، عشق، آزادی و دیگر دل‌خوشی‌های خوب‌مان که ما مردم معمولی برای زنده ماندن به آن‌ها نیاز داشتیم، قربانی شدند. ما حتی تعریف دقیقی هم از دل‌خوشی‌های خوب‌مان نداشتیم و همین کوتاهی ما راه را برای قاتلان باز کرد. دل‌خوشی‌هایمان همه قربانی شدند و ما ماندیم، تک و تنها، روبه‌روی ارتش سیاهی. تازه فهمیدیم آن قربانی‌هایی که برایشان نجنگیدیم، هر یک، عنصری از حیات ما بودند. آری، دیگر این فقط اینترنت و این چیزهای کوچک نیستند که قربانی شده‌اند؛ ما قربانی شدیم، خوبی قربانی شد، زندگی قربانی شد...

1 Magazine

در پاییز ۱۹۳۹، درست در آستانه شروع جنگ جهانی دوم، دانشجویان دانشگاه آکسفورد دچار سردرگمی شدید شده بودند. آن‌ها فکر می‌کردند در حالی که سایه جنگ روی سرشان است، درس خواندن و کار کردن روی پروژه‌های شخصی کاری بی‌هوده است و باید همه چیز را متوقف کنند. سی. اس. لوئیس در کلیسای دانشگاه آکسفورد خطاب به آن‌ها سخنرانی معروفی کرد. آن سخنرانی هنوز هم مثل نوری باریک، به جوامعی که در عمق تاریکی اند نیرو می‌بخشد:

«زندگی انسان هواره بر لبه پرتگاهی زیسته است. فرهنگ انسانی هواره ناچار بوده است در سایه چیزی که از خود او بی‌نهایت مهم‌تر است، وجود داشته باشد. اگر آدمیان جست‌وجوی دانش و زیبایی را تا زمانی که از همه چیز در امان باشند به تعویق می‌انداختند، این جست‌وجو هرگز آغاز نمی‌شد. اما بشر مدت‌ها پیش، از این دلیل‌های قانع‌کننده چشم پوشید. آنان دانش و زیبایی را همین حالا می‌خواستند و منتظر زمان مناسبی نبودند که هرگز نمی‌رسد.

به نظر من، همه وظایف سیاسی و نظامی از این جنس‌اند که در صورت نیاز باید برایشان مرد، اما نباید برایشان زندگی کرد. ممکن است مردی لازم باشد برای کشورمان جان بدهد؛ اما هیچ‌کس نباید، به معنایی انحصاری، برای کشورش زندگی کند. کسی که بی‌هیچ قید و شرطی خود را تسلیم خواسته‌های زمانی یک ملت، یا یک حزب می‌کند، به امپراطور آن چیز را می‌دهد که به طور آشکارتر از همه از آن خداست: خودش. بحران‌ها و جنگ‌ها شرایط جدیدی خلق نمی‌کنند؛ آن‌ها فقط به ما یادآوری می‌کنند که زندگی همیشه ناپایدار است. پس کارهای خود را آغاز کنید و پیش ببرید، گویی هیچ اتفاقی در جریان نیست؛ چرا که زمان منتظر صلح ایده‌آل شما نمی‌ماند.»

انتقادات و پیشنهادات خود را
بامادر میان بگذارید



SSC
STUDENTS' SCIENTIFIC CHAPTER
انجمن علمی دانشکده مهندسی کامپیوتر
دانشگاه صنعتی شریف