نسخه خلاصه از ابزارها

ابزارهای ارتباط امن و همتا به همتا (P2P)

در زمینه ارتباطات امن و ابزارهای همتا به همتا (P2P)، نکته کلیدی این است که از ابزارهایی استفاده شود که قابل اعتماد، کاربرپسند و در برابر نظارت و رهگیری ایمن باشند. در اینجا برخی از پیشنهادها ارائه شده است:

اپلیکیشن‌های پیام‌رسان امن

این اپلیکیشن‌ها رمزگذاری سرتاسری ارائه می‌دهند و برای محافظت از ارتباطات حتی در محیط‌های پرخطر طراحی شده‌اند:

- **سیگنال:** یکی از امن‌ترین اپلیکیشن‌های پیام‌رسان موجود است که برای ارتباطات متنی، صوتی و ویدیویی رمزگذاری سرتاسری ارائه می‌دهد. این اپلیکیشن منبع‌باز است و در جامعه امنیتی به‌شدت مورد اعتماد است و استفاده از آن آسان است.
- **واتس‌اپ:** با وجود این که رمزگذاری سرتاسری ارائه می‌دهد و به‌طور گسترده استفاده می‌شود، به دلیل مالکیت آن توسط متا (Meta)، نگرانی‌هایی در مورد حریم خصوصی وجود دارد. با این حال، برای ارتباطات روزمره و در بسیاری از مناطق گزینه‌ای محبوب و نسبتاً امن است.
- **تلگرام:** ارتباطات رمزگذاری‌شده ارائه می‌دهد، اما تنها در حالت «چت محرمانه» (Secret Chat) این رمزگذاری فعال است. این اپلیکیشن به‌طور گسترده در مناطقی با سانسور اینترنت استفاده می‌شود، اگرچه رمزگذاری آن نسبت به سیگنال ضعیف‌تر است.

ابزارهای ارتباط همتا به همتا (P2P)

ابزارهای P2P در زمان قطع اینترنت اهمیت ویژه‌ای دارند، زیرا بدون نیاز به سرورهای مرکزی کار می‌کنند و در برابر کنترل‌های دولتی مقاوم‌تر هستند:

- **Briar** :یک اپلیکیشن پیام‌رسان P2P بسیار امن است که از طریق بلوتوث، وای‌فای یا اینترنت کار می‌کند. این اپلیکیشن برای فعالان و روزنامه‌نگاران طراحی شده و حتی زمانی که اینترنت قطع است با استفاده از شبکه‌های محلی کار می‌کند.
- **Bridgefy** : این اپلیکیشن به کاربران اجازه می‌دهد از طریق بلوتوث ارتباط برقرار کنند و یک شبکه مش ایجاد کنند که دستگاه‌ها را مستقیماً به هم متصل می‌کند. این ابزار در شرایطی که اینترنت در دسترس نیست اما کاربران در نزدیکی هم قرار دارند، مفید است.

- Delta Chat : این ابزار تلفیقی از قابلیت‌های ایمیل سنتی و پیام‌رسانی فوری است و به عنوان یک ابزار ارتباط امن در زمان قطع اینترنت بسیار مفید است.

سرویس‌های ایمیل امن

برای ارتباطات ایمیلی امن، به ویژه هنگام ارسال اسناد حساس:

- ProtonMail : این سرویس ایمیل مبتنی بر سوئیس رمزگذاری سرتاسری و حفاظت‌های قوی حریم خصوصی ارائه می‌دهد و گزینه‌ای مناسب برای ارسال اطلاعات حساس به‌صورت امن است.
- **Tutanota** : یک سرویس ایمیل امن دیگر که رمزگذاری سرتاسری ارائه می‌دهد، کاربرپسند است و ویژگی‌هایی مانند تقویم‌های رمزگذاری‌شده نیز ارائه می‌دهد.

شبکه‌های مش

شبکه‌های مش شبکه‌های غیرمتمرکزی هستند که حتی در زمان قطع اینترنت امکان ارتباطات را حفظ می‌کنند:

- **goTenna Mesh :** دستگاه‌های goTenna Mesh یک شبکه ارتباطی خصوصی و خارج از شبکه اینترنت با استفاده از امواج رادیویی برد بلند ایجاد می‌کنند. این دستگاه‌ها در مناطق بدون پوشش شبکه یا در زمان قطع اینترنت بسیار کارآمد هستند.
- **Serval Project :** این پروژه یک راه‌حل شبکه مش ارائه می‌دهد که می‌تواند دستگاه‌های اندروید را به بخشی از یک شبکه غیر متمرکز تبدیل کند، امکان برقراری تماس، پیام‌رسانی و اشتراک‌گذاری فایل را بدون نیاز به اینترنت فراهم می‌کند.

ارتباطات ماهواره‌ای

برای قطع کامل اینترنت یا در مناطقی که هیچ گونه ارتباطی وجود ندارد:

- Starlink **:** استارلینک، توسط اسپیس‌ایکس اداره می‌شود و خدمات اینترنت ماهواره‌ای ارائه می‌دهد. این یکی از پیشرفته‌ترین خدمات اینترنت ماهواره‌ای است و می‌تواند در حفظ دسترسی به اینترنت در مناطق دورافتاده یا قطع‌شده حیاتی باشد.
- **Inmarsat یا Iridium :** این شبکه‌های ارتباط ماهواره‌ای جهانی، خدمات صوتی و داده‌ای ارائه می‌دهند. اگرچه گران‌تر هستند، اما در مناطقی که روش‌های ارتباط سنتی در دسترس نیستند، قابل اعتماد هستند.
- Rostam media : رستم مدیا یک فناوری نوآورانه است که به کاربران امکان می‌دهد محتوای دیجیتال را از طریق ماهواره دریافت کنند، بدون نیاز به دسترسی به اینترنت. این فناوری برای دور زدن محدودیت‌ها و سانسور اینترنتی بسیار مفید است.

VPNها و ابزارهای ناشناس‌سازی

اگرچه VPNها P2P نیستند، اما برای دور زدن سانسور و تأمین امنیت فعالیت‌های آنلاین ضروری هستند:

- BeePass : یک VPN ساده و امن منبع‌باز است که برای حفظ حریم خصوصی کاربران و عبور از سانسور اینترنت طراحی شده است.
- Tor Browser : ترافیک اینترنت را ناشناس می‌کند و به محافظت در برابر نظارت کمک می‌کند. به‌ویژه در محیط‌هایی که فعالیت‌های مرور نیاز به محرمانگی دارد، مفید است.
- ProtonVPN : این سرویس VPN بسیار امن، حفاظت‌های حریم خصوصی قوی ارائه می‌دهد و با ProtonMail یکپارچه شده است.
- Psiphon : یک ابزار دور زدن محدودیت‌ها که ترکیبی از VPN، SSH و فناوری‌های پروکسی HTTP را ارائه می‌دهد و در کشورهایی با سانسور شدید اینترنت بسیار استفاده می‌شود.

- **MahsaNet** : این VPN برای ارائه تنظیمات قابل اعتماد از طریق سرور «مهسا» طراحی شده است. هدف آن ایجاد دسترسی آسان و اقتصادی به اینترنت برای تمام کاربران است.
- **Oblivion VPN**: یک اپلیکیشن خاص VPN است که با استفاده از فناوری Wiregaurd، ارتباطات را رمزگذاری می‌کند و با تنظیمات ویژه خود، به دور زدن سانسور اینترنت و حفظ حریم خصوصی کاربران کمک می‌کند. این ابزار با ترکیب ویژگی‌های برتر Wiregaurd و دیگر فناوری‌های مرتبط، دسترسی امن و آسان را به اینترنت آزاد فراهم می‌سازد. از اینجا می‌توانید به اوپن سورس این وی‌پی‌ان دسترسی داشته باشید.

ابزارهای ارتباط آفلاین

در شرایطی که حتی ابزارهای P2P ممکن است غیرقابل دسترس یا محدود شوند:

- **USB Dead Drops** : این روش شامل به‌اشتراک‌گذاری اطلاعات از طریق قرار دادن USBها در مکان‌های عمومی است که دیگران می‌توانند داده‌ها را از آن‌ها دریافت کنند. این روش که در مقایسه کمتر «تکنولوژیک» محسوب می‌شود برای توزیع اطلاعات در زمان قطع شدید اینترنت موثر است.
- **درایوهای USB رمزگذاری‌شده:** از درایوهای USB با رمزگذاری سخت‌افزاری برای ذخیره و انتقال امن اطلاعات حساس استفاده کنید. این ابزارها می‌توانند برای به اشتراک گذاشتن فایل‌های مهم به‌صورت حضوری و بدون اتکا به شبکه‌های دیجیتال استفاده شوند.
- **Ceno** : مرورگر (Cenoمخفف censorship.no!) یک مرورگر موبایل است که از روش‌های P2P برای عبور از سانسور استفاده می‌کند و به کاربران امکان می‌دهد اطلاعات وب را در مناطقی که اتصال اینترنت مختل شده است به اشتراک بگذارند.

رمزگذاری و مبهم‌سازی (Obfuscation)

رمزگذاری فرآیند تبدیل اطلاعات یا داده‌ها به کد است تا از دسترسی افراد غیرمجاز جلوگیری شود. رمزگذاری تضمین می‌کند که تنها افراد مجاز با کلید رمزگشایی صحیح می‌توانند به داده‌ها دسترسی داشته باشند و آن را بخوانند. این فرآیند برای ایمن‌سازی اطلاعات حساس مانند ایمیل‌ها، فایل‌ها، تراکنش‌های مالی و داده‌های شخصی استفاده می‌شود تا از دسترسی و درک آن توسط عوامل مخرب یا افراد غیرمجاز جلوگیری شود.

مبهم‌سازی (Obfuscation)، به نوبه خود، شامل مبهم‌سازی عمدی اطلاعات یا داده‌ها است، به‌طوری که حتی بدون تبدیل به قالب دیگر، فهم آن‌ها دشوار شود. برخلاف رمزگذاری، مبهم‌سازی نیازی به کلید رمزگشایی ندارد و فقط باعث می‌شود داده‌ها کمتر قابل خواندن و تفسیر باشند. هدف از مبهم‌سازی، پیچیده‌سازی داده‌ها برای جلوگیری از دسترسی غیرمجاز و دشوار کردن فهم آن است.

کاربردهای رایج رمزگذاری:

- ایمن‌سازی ایمیل‌ها برای جلوگیری از خواندن غیرمجاز.
- محافظت از فایل‌ها در برابر دسترسی غیرمجاز.
- حفظ امنیت تراکنش‌های مالی در برابر تقلب یا رهگیری.
- تضمین حریم خصوصی داده‌های شخصی در برابر سرقت یا سوءاستفاده.

کاربردهای رایج مبهم‌سازی:

- مخفی کردن منطق یک متن یا کد در نرم‌افزار برای حفاظت از مالکیت معنوی یا حریم خصوصی.
- کاهش خوانایی داده‌ها در هنگام انتقال برای جلوگیری از مشاهده تصادفی.

- افزودن پیچیدگی به فرمت‌های داده‌ها برای جلوگیری از تحلیل یا استخراج آسان.

ابزارهای رایج برای رمزگذاری و مبهم‌سازی:

- **PGP (Pretty Good Privacy)**: نرم‌افزار اولیه‌ای که GPG بر اساس آن ساخته شده است و برای ایمن‌سازی ارتباطات ایمیلی و رمزگذاری داده‌ها مورد استفاده قرار می‌گیرد.
- **VeraCrypt** : یک نرم‌افزار اوپن‌سورس محبوب برای رمزگذاری دیسک که امکان رمزگذاری فایل‌ها، پوشه‌ها یا کل درایو را فراهم می‌کند.
- **Nahoft** : یک اپلیکیشن مبهم‌سازی برای گوشی‌های اندروید و iOS است که به شما امکان می‌دهد پیام‌های خصوصی خود را به زنجیره‌ای از کلمات فارسی تبدیل کنید یا آن‌ها را در عکسی مخفی کنید و سپس از طریق هر اپلیکیشن پیام‌رسانی به‌طور ایمن ارسال کنید.

مخفی‌سازی داده‌ها (Data Hiding)

مخفی‌سازی داده‌ها یا استگانوگرافی به عملیاتی گفته می‌شود که در آن اطلاعات حساس درون فایل‌های غیر مشکوک مخفی می‌شود. برخی از ابزارهای امن و مؤثر برای مخفی‌سازی داده‌ها عبارتند از:

- **Steghide** : یک ابزار محبوب استگانوگرافی یا پنهان‌سازی است که به کاربران امکان می‌دهد داده‌ها را درون فایل‌های تصویری یا صوتی پنهان کنند. این ابزار از فرمت‌های مختلفی مانند BMP, JPEG, WAV و AU پشتیبانی می‌کند. داده‌های پنهان شده با استفاده از یک گذرواژه رمزگذاری می‌شوند، که یک لایه امنیتی اضافی فراهم می‌کند.
  - از چندین فرمت فایل پشتیبانی می‌کند.
  - از رمزگذاری قوی (AES) استفاده می‌کند.
  - امکان جاسازی و استخراج داده‌ها از فایل‌ها را به‌سادگی فراهم می‌کند.
- **SilentEye** : یک اپلیکیشن استگانوگرافی یا پنهان‌سازی دیگر است که به کاربران امکان می‌دهد داده‌ها را در فایل‌های تصویری و صوتی مخفی کنند. این اپلیکیشن دارای رابط کاربری گرافیکی ساده است که استفاده از آن را آسان می‌کند. SilentEye همچنین از رمزگذاری برای حفاظت از داده‌های مخفی‌شده پشتیبانی می‌کند.
  - رابط کاربری گرافیکی کاربر پسند.
  - پشتیبانی از فایل‌های تصویری BMP، JPG و صوتی WAV
  - رمزگذاری اختیاری برای داده‌های مخفی‌شده.
- **Crypture** : یک ابزار سبک و کاربردی برای استگانوگرافی است که داده‌ها را در قالب فایل‌های تصویری BMP مخفی می‌کند. این ابزار برای افرادی که به دنبال ابزاری بدون پیچیدگی‌های اضافه هستند، مناسب است.
  - سبک و ساده برای استفاده.
  - رمزگذاری داده‌های مخفی.
  - تمرکز بر روی فایل‌های تصویری BMP.
- **Stegano** : یک کتابخانه استگانوگرافی مبتنی بر پایتون است که می‌توان از آن برای مخفی‌سازی داده‌ها در تصاویر استفاده کرد. این ابزار بیشتر برای کاربرانی مناسب است که با برنامه‌نویسی آشنایی دارند، زیرا به دانش کدنویسی برای استفاده مؤثر نیاز دارد.
  - کتابخانه پایتون برای پیاده‌سازی سفارشی استگانوگرافی.
  - قابلیت ادغام در سایر برنامه‌ها.
  - پشتیبانی از مخفی‌سازی داده‌ها در فایل‌های PNG
- **Camouflage** : یک ابزار استگانوگرافی یا پنهان‌سازی است که فایل‌ها را در فایل‌های دیگر مانند اسناد یا تصاویر مخفی می‌کند. این ابزار همچنین داده‌های مخفی‌شده را فشرده و رمزگذاری می‌کند تا تشخیص آن‌ها سخت‌تر شود.

- مخفی‌سازی فایل‌ها درون فایل‌های دیگر مانند تصاویر و اسناد.
- فشرده‌سازی و رمزگذاری داده‌ها.
- رابط کاربری ساده برای استفاده آسان.

- **DeepSound:** ابزاری برای مخفی‌سازی داده‌ها در فایل‌های صوتی است. این ابزار قابلیت جاسازی فایل‌های مخفی‌شده در آهنگ‌های صوتی را بدون تغییر محسوس کیفیت صدا دارد که تشخیص آن را دشوار می‌کند.
  - تخصص در فایل‌های صوتی.
  - پشتیبانی از فرمت‌هایی مانند FLAC، WAV و سایر فرمت‌ها.
  - دارای رمزگذاری AES
- **Outguess:** یک ابزار پیشرفته استگانوگرافی یا پنهان‌سازی است که بر روی تصاویر تمرکز دارد. این ابزار طوری طراحی شده است که داده‌ها را بدون ایجاد تغییرات محسوس در تصویر مخفی کند و گزینه خوبی برای کسانی است که به امنیت و عدم شناسایی بالا نیاز دارند.
  - تمرکز بر مخفی‌سازی داده‌ها در تصاویر.
  - تغییرات حداقلی در تصویر حامل.
  - پشتیبانی از فرمت‌های فایل JPEG و PNM
- Tella : یک اپلیکیشن موبایل امن است که برای فعالان، روزنامه‌نگاران و مدافعان حقوق بشر طراحی شده است تا اطلاعات حساس را در محیط‌های چالش‌برانگیز مستندسازی و محافظت کند. این اپلیکیشن به طور خودکار عکس‌ها، ویدئوها و ضبط‌های صوتی را رمزگذاری کرده، آن‌ها را از گالری معمولی گوشی مخفی می‌کند و به کاربران اجازه می‌دهد برای حفاظت بیشتر از پین یا رمز عبور استفاده کنند. Tella همچنین از جمع‌آوری داده به‌صورت آفلاین پشتیبانی می‌کند و با پلتفرم‌هایی مانند Uwazi و Kobotoolbox یکپارچه می‌شود. این اپلیکیشن رایگان، چند زبانه، منبع‌باز است و برای مقابله با سرکوب فیزیکی و دیجیتالی طراحی شده است.
  - محافظت از سرکوب فیزیکی و دیجیتالی در هنگام جمع‌آوری و ذخیره اطلاعات حساس.
  - محافظت از داده‌ها در برابر سانسور، دست‌کاری، رهگیری و تخریب.
  - تولید مستندات با کیفیت بالا، که می‌توان از آن برای تحقیقات، دفاع و عدالت انتقالی استفاده کرد.
  - رمزگذاری فایل‌ها: این اپلیکیشن به محض ثبت عکس‌ها، ویدئوها و ضبط‌های صوتی، آن‌ها را به‌طور خودکار رمزگذاری می‌کند.
  - مخفی‌سازی فایل‌ها در دستگاه: فایل‌های شما از گالری و فایل اکسپلورر معمولی گوشی در دسترس نیستند و فقط در داخل اپلیکیشن قابل مشاهده‌اند.
  - قفل‌گذاری فایل‌ها: برای حفاظت از فایل‌ها یک پین یا رمز عبور تنظیم کنید. وارد کردن قفل صحیح تنها راه رمزگشایی فایل‌های ذخیره‌شده در Tella است.
  - پنهان‌سازی ظاهر اپلیکیشن: ظاهر Tella را تغییر دهید تا برای افرادی که گوشی شما را جستجو می‌کنند، مخفی بماند.
  - دوربین و ضبط‌کننده داخلی: عکس بگیرید و ویدئوها و فایل‌های صوتی را مستقیماً در Tella ضبط کنید تا فایل‌ها بلافاصله رمزگذاری و در داخل اپلیکیشن مخفی شوند.
  - Tella با Uwazi، Kobotoolbox و Tella Web یکپارچه و هماهنگ می‌شود. پلتفرمی را انتخاب کنید که به بهترین شکل با نیازهای شما همخوانی دارد و داده‌ها را مستقیماً در Tella جمع‌آوری کنید.
  - حالت آفلاین: در مناطق با اینترنت محدود یا قطع‌شده، داده‌های خود را ذخیره کنید و در زمانی که به اتصال اینترنت مطمئن دسترسی دارید، آن‌ها را ارسال کنید.

حذف فراداده‌ها

در زمان قطع اینترنت، فراداده‌ها نقش مهمی دارند و اغلب به‌اندازه محتوای ارتباطات اهمیت دارند. فراداده‌ها اطلاعاتی درباره داده‌ها هستند، مانند اطلاعات مربوط به ارتباط افراد با یکدیگر، زمان برقراری این ارتباطات بدون فاش

کردن محتوای اصلی آن ارتباطات. حتی اگر محتوا رمزگذاری شده باشد، فراداده‌ها همچنان قابل ردیابی هستند و اطلاعات ارزشمندی را فاش می‌کنند.

در ادامه اهمیت فراداده‌ها در زمان قطع اینترنت توضیح داده شده است:

- **ردیابی الگوهای ارتباطی**
  - **پایش شبکه‌های اجتماعی:** حتی اگر محتوا به‌وسیله رمزگذاری پنهان شود، فراداده‌ها (مانند فرستنده، گیرنده، و زمان ارتباط) می‌توانند ارتباطات بین افراد را آشکار کنند. مقامات امنیتی و انتظامی می‌توانند از این طریق شبکه‌های فعالان، روزنامه‌نگاران یا اعضای مخالف را شناسایی کنند که می‌تواند به سرکوب هدفمند منجر شود.
  - **تکرار و زمان‌بندی ارتباطات:** فراداده‌ها نشان می‌دهند که فرد چقدر ارتباط برقرار می‌کند، چه ساعاتی از روز فعال است و با چه کسانی در ارتباط است. در دوره‌های حساس سیاسی، افزایش ارتباطات بین افراد یا گروه‌های خاص می‌تواند برای مقامات هشداردهنده باشد.
- **ردیابی موقعیت مکانی**
  - **فراداده‌های مکان‌یابی (ژئولوکیشن):** بسیاری از خدمات، به‌ویژه اپلیکیشن‌های موبایل یا مرورگرهای وب، به‌صورت خودکار اطلاعات مکانی کاربران را به عنوان بخشی از فراداده جمع‌آوری می‌کنند. حتی در شرایط محدودیت اینترنت، برخی از خدمات ممکن است همچنان قادر به ردیابی و گزارش مکان فیزیکی کاربران باشند. این مسئله در رژیم‌های سرکوبگر که به دنبال سرکوب اعتراضات و تجمعات هستند، بسیار خطرناک است.
  - **شناسایی VPN و پروکسی‌ها:** حتی اگر کاربران سعی کنند با استفاده از VPN یا پروکسی‌ها از قطع اینترنت عبور کنند، فراداده‌ها می‌توانند نشان دهند که شخصی از این ابزارها استفاده می‌کند و همچنین مکان سرور VPN یا پروکسی مورد استفاده را فاش کنند. این می‌تواند افرادی را که در تلاش برای دور زدن محدودیت‌ها هستند در معرض خطر قرار دهد.
- **نظارت بدون دسترسی به محتوا**
  - **تحلیل روابط:** در زمان قطع اینترنت، مقامات ممکن است نیازی به دیدن محتوای اصلی پیام‌ها نداشته باشند تا به اطلاعات مفید دست یابند. در این شرایط ماموران امنیتی یا ضابطین قضایی با بررسی فراداده‌ها و بررسی ارتباطات افراد، می‌توانند روابط را استنباط کنند، شبکه‌ها را ترسیم کنند و حتی اقدامات آینده را پیش‌بینی کنند. این به حکومت اجازه می‌دهد تا افراد کلیدی در جنبش‌های مدنی، سیاسی، اجتماعی را شناسایی کنند، حتی اگر محتوای ارتباطات رمزگذاری شده باشد.
  - **ساختن پروفایل:** فراداده‌های جمع‌آوری‌شده در طول زمان می‌توانند برای ساختن پروفایلی جامع از رفتار، روابط و برنامه‌های روزمره فرد استفاده شوند. در زمان قطع اینترنت، این نوع نظارت می‌تواند برای پایش تهدیدات احتمالی یا مخالفان افزایش یابد.
- **دور زدن رمزگذاری**
  - **محتوای رمزگذاری‌شده، فراداده‌های قابل مشاهده:** در حالی که رمزگذاری محتوای پیام‌ها را پنهان می‌کند، همیشه نمی‌تواند فراداده‌ها، مانند فرستنده و گیرنده پیام، طول پیام یا زمان و تکرار ارسال پیام‌ها را مخفی کند. در زمان قطع اینترنت، مقامات ممکن است تنها روش‌های ارتباطی محدودی (مانند ایمیل یا پیامک) را مجاز بدانند که در آن فراداده‌ها حتی اگر محتوا رمزگذاری شده باشد، قابل مشاهده باقی می‌مانند.
- **خطرات قانونی و اجتماعی**
  - **جرم به واسطه ارتباط:** فراداده‌ها می‌توانند افراد را از طریق ارتباطاتشان در معرض خطر قرار دهند. حتی اگر شخصی به‌طور فعال در فعالیت‌های مخالفان درگیر نباشد، ارتباط با افرادی که تحت نظارت هستند می‌تواند او را در معرض خطر قرار دهد. به‌عنوان مثال، اگر فراداده‌ها ارتباطات مکرر با فعالان شناخته‌شده را فاش کنند، مقامات امنیتی و قضایی ممکن است آن فرد را در فعالیت‌های سیاسی یا اجتماعی مقصر بدانند.
  - **چالش‌های پنهان‌سازی از نظارت:** در زمان قطع اینترنت، پنهان‌سازی فراداده‌ها بسیار دشوار است. ابزارهایی مانند VPN یا شبکه‌های ناشناس‌سازی مانند Tor کمک می‌کنند تا فراداده‌ها مبهم شوند، اما

ممکن است همچنان نشانه‌هایی باقی بگذارند یا در محیط‌های تحت نظارت شدید شک‌برانگیز باشند.

- **مسدود سازی دسترسی به منابع خارجی**
  - **شناسایی و مسدود سازی ترافیک:** حتی اگر کاربران سعی کنند از طریق ابزارهای ارتباطی خارجی (مانند VPN، پروکسی‌ها، یا اپلیکیشن‌های پیام‌رسان رمزگذاری‌شده) محدودیت‌های قطع اینترنت را دور بزنند، فراداده‌ها می‌توانند این تلاش‌ها را آشکار کنند. مقامات می‌توانند با تحلیل الگوهای فراداده و شناسایی ابزارهای مورد استفاده، این روش‌ها را مسدود کنند.

حفاظت از فراداده‌ها در زمان قطع اینترنت

در حالی که رمزگذاری محتوای پیام‌ها بسیار ضروری است، روش‌هایی نیز برای حفاظت از فراداده‌ها وجود دارد:

- **استفاده از شبکه‌های Tor یا I2P :** این ابزارهای ناشناس‌سازی با مسیریابی ترافیک از طریق چندین گره، فراداده‌ها را مبهم کرده و ردیابی مبدا یا مقصد ارتباط را برای مقامات دشوار می‌کنند.
- **VPNها و پروکسی‌ها:** با اینکه کامل نیستند، VPN ها می‌توانند برخی از انواع فراداده‌ها مانند آدرس IP کاربر را از طریق مسیریابی ترافیک از سرورهای خارجی پنهان کنند. با این حال، خود استفاده از VPN نیز ممکن است قابل ردیابی باشد.
- **تاخیر عمدی در ارسال پیام‌ها:** ابزارهایی مانند «شبکه‌های میکس» تأخیرهایی به پیام‌ها اضافه می‌کنند تا فراداده‌های زمانی را مبهم کرده و ارتباط بین فرستنده و گیرنده را دشوار کنند.

در شرایط قطع اینترنت، فراداده‌ها می‌توانند نقشه دقیقی از اینکه چه کسی با چه کسانی، چه زمانی و از کجا ارتباط دارد، حتی بدون دسترسی به محتوای پیام‌ها، به مقامات ارائه دهند. بنابراین، حفاظت از فراداده‌ها به‌اندازه ایمن‌سازی محتوای ارتباطات اهمیت دارد، به‌ویژه برای افرادی که در فعالیت‌های حساسی مانند اعتراضات، روزنامه‌نگاری یا دفاع از حقوق بشر مشغول هستند.

ابزارهای ساده و کاربردی برای حفاظت از فراداده‌ها:

- **MAT2 (ابزار ناشناس‌سازی فراداده‌ها)**
  - **کارکرد:** MAT2 یک ابزار رایگان و ساده برای حذف فراداده از اسناد، تصاویر، فایل‌های PDF و انواع دیگر فایل‌ها است. این ابزار از فرمت‌های گسترده‌ای پشتیبانی کرده و فراداده‌های حساس مانند نام نویسنده، اطلاعات مکان و تاریخچه تغییرات را حذف می‌کند.
  - **نحوه استفاده:** دارای رابط کاربری گرافیکی است که با قابلیت کشیدن و رها کردن فایل‌ها به کاربران غیر فنی کمک می‌کند فایل‌های خود را پیش از اشتراک‌گذاری پاک‌سازی کنند.
  - **امکان استفاده:** در سیستم‌عامل‌های لینوکس، قابل استفاده از طریق خط فرمان و در برخی توزیع‌های لینوکس نسخه‌های کاربر پسند موجود است.
- **ExifTool (برای تصاویر و ویدیوها)**
  - **کارکرد:** ExifTool ابزاری قدرتمند برای حذف فراداده‌ها، به‌ویژه از فایل‌های تصویری و ویدیویی است که ممکن است داده‌های GPS، اطلاعات دوربین یا زمان‌بندی‌ها را شامل شود.
  - **نحوه استفاده:** به‌طور پیش‌فرض فنی‌تر است، اما رابط‌های کاربرپسند مانند "ExifCleaner" برای کاربران غیر فنی فرآیند را ساده کرده و امکان کشیدن و رها کردن فایل‌ها برای حذف فراداده‌ها را فراهم می‌کنند.
  - **امکان استفاده:** قابل استفاده در سیستم‌عامل‌های ویندوز، macOS و لینوکس.
- **VLC Media Player (برای فراداده‌های ویدیوها)**
  - **کارکرد:** VLC که یک پخش‌کننده چندرسانه‌ای رایج است و ابزارهای داخلی برای ویرایش یا حذف فراداده‌ها از فایل‌های ویدیویی را دارد. کاربران می‌توانند به‌سادگی یک ویدیو را باز کرده، فراداده‌ها را ویرایش یا به‌کلی حذف کنند.
  - **نحوه استفاده:** ویدیو را باز کرده، به قسمت «ابزارها» > «اطلاعات رسانه» بروید و فیلدهای فراداده را به‌صورت دستی ویرایش یا پاک کنید. این روش برای کاربران غیر فنی ساده است.
  - **امکان استفاده:** برای ویندوز، macOS و لینوکس.

- **AnonAddy (برای فرادادههای ایمیل)**
  - **کارکرد:** AnonAddy یک سرویس ساده برای ارسال و دریافت ایمیل به‌صورت ناشناس است که آدرس ایمیل واقعی شما را مخفی کرده و فرادادههایی مانند آدرس IP را حذف می‌کند.
  - **نحوه استفاده:** کاربران می‌توانند از طریق ایجاد نام‌های مستعار ناشناس برای ایمیل خود، ایمیل‌ها را بدون نمایش اطلاعات شخصی یا فراداده ارسال و دریافت کنند.
  - **امکان استفاده:** با هر کلاینت ایمیلی سازگار است و از طریق مرورگر وب قابل دسترسی است.
- **OnionShare (برای اشتراک‌گذاری فایل به‌صورت ناشناس)**
  - **کارکرد:** OnionShare به کاربران امکان می‌دهد فایل‌ها را به‌صورت امن و ناشناس با استفاده از شبکه Tor به اشتراک بگذارند و فرادادههای مرتبط با فرآیند اشتراک‌گذاری را پنهان کند.
  - **نحوه استفاده:** کاربران غیر فنی می‌توانند OnionShare را نصب کرده، فایل‌های خود را به‌سادگی کشیده و رها کرده و یک لینک امن دریافت کنند که می‌توانند به گیرنده ارسال کنند.
  - **امکان استفاده:** برای ویندوز، macOS و لینوکس.
- **Tor Browser (برای وب‌گردی و ارتباطات)**
  - **کارکرد:** مرورگر Tor ترافیک اینترنتی کاربران را از چندین گره عبور داده و فرادادههایی مانند آدرس IP و عادت‌های مرور را مخفی می‌کند. این یکی از ساده‌ترین ابزارها برای کاربران غیر فنی است که از فعالیت‌های آنلاین خود محافظت کنند.
  - **نحوه استفاده:** مرورگر Tor را دانلود کرده و مانند یک مرورگر معمولی از آن استفاده کنید. این مرورگر به‌طور خودکار ترافیک شما را ناشناس می‌کند.
  - **امکان استفاده:** برای ویندوز، macOS، لینوکس و اندروید.
- **Simple PDF Metadata Remover (حذف فراداده PDF)**
  - **کارکرد:** این ابزار به‌صورت خاص برای حذف فراداده از PDFها طراحی شده و اطلاعاتی مانند نام نویسنده، تاریخ ایجاد سند و تاریخچه تغییرات را پاک می‌کند.
  - **نحوه استفاده:** کاربران می‌توانند فایل PDF خود را به‌سادگی کشیده و رها کرده و با یک کلیک فرادادهها را حذف کنند.
  - **در دسترس بودن:** به‌عنوان یک برنامه ساده برای ویندوز.
- **BleachBit (برای پاک‌سازی کلی فایل‌ها)**
  - **کارکرد:** BleachBit ابزاری کاربرپسند است که به حذف فرادادهها از انواع مختلف فایل‌ها و پاک‌سازی داده‌های غیرضروری از رایانه کمک می‌کند تا حریم خصوصی کاربران حفظ شود.
  - **نحوه استفاده:** رابط کاربری ساده‌ای ارائه می‌دهد که کاربران می‌توانند نوع فایل‌هایی را که می‌خواهند پاک‌سازی کنند (مانند تاریخچه مرورگر، فرادادهها و بیشتر) انتخاب کرده و با یک کلیک پاک‌سازی را انجام دهند.
  - **امکان استفاده:** برای ویندوز و لینوکس.
- **اپلیکیشن‌های حذف فراداده عکس (برای گوشی‌های هوشمند)**
  - **کارکرد:** این اپلیکیشن‌ها برای حذف فرادادهها از عکس‌های گوشی‌های هوشمند طراحی شده‌اند، مانند داده‌های EXIF که اطلاعات مکان و دوربین را شامل می‌شوند.
  - **نحوه استفاده:** کاربران فقط نیاز به آپلود عکس دارند و اپلیکیشن به‌طور خودکار فرادادهها را حذف می‌کند.
- **سیستم‌عامل Tails (برای حفظ کامل حریم خصوصی)**
  - **کارکرد:** Tails یک سیستم‌عامل متمرکز بر حریم خصوصی است که از طریق USB اجرا می‌شود و تمام فعالیت‌ها را ناشناس می‌کند. این سیستم‌عامل به‌صورت پیش‌فرض با ابزارهایی مانند Tor، ارتباطات رمزگذاری‌شده و حذف فراداده برای فایل‌ها بارگذاری شده است.
  - **نحوه استفاده:** نصب Tails ممکن است به دانش فنی مختصری نیاز داشته باشد، اما پس از راه‌اندازی، تمام ابزارها ساده و برای حریم خصوصی از پیش تنظیم شده‌اند، که آن را برای کاربران غیر فنی که به حفاظت جامع نیاز دارند، ایده‌آل می‌کند.
  - **امکان استفاده:** به صورت رایگان در دسترس است، اما به یک فلش USB برای نصب و اجرا نیاز دارد.

این ابزارها برای کاربران غیر فنی، روش‌های ساده و موثری برای حذف یا پنهان کردن فراداده‌ها ارائه می‌دهند و با رابط‌های کشیدن و رها کردن، پاک‌سازی با یک کلیک، و ابزارهای ناشناس‌سازی مانند Tor یا Tails پیچیدگی‌های فرآیند را به‌صورت خودکار انجام می‌دهند.

سناریوهای عملی و قابل اجرا

در اینجا به بررسی چهار سناریوی واقعی خواهیم پرداخت. در این سناریوها، نه تنها روش‌های مورد استفاده کاربران تحلیل خواهند شد، بلکه ریسک‌های امنیتی نیز بررسی شده و راه‌حل‌هایی برای کاهش این ریسک‌ها ارائه خواهد شد.

سناریوی اول: قطع کامل اینترنت و استفاده از ابزارهای ارتباطی داخلی

در زمان قطع اینترنت، من در تهران بودم در حالی که همسرم که شهروند ایالات متحده است در آنجا حضور داشت. برای چند روز هیچ راهی برای ارتباط با او نداشتم تا اینکه متوجه شدم می‌توانم از طریق خدمات ایمیل مبتنی بر اینترنت ملی با دامنه .ir ایمیل‌هایی به جیمیل ارسال و دریافت کنم. پس از چند روز سکوت، بالاخره توانستیم ارتباط برقرار کنیم، اما به دلیل نگرانی از اینکه ایمیل‌های .ir خوانده شوند، مکالمات ما بسیار رسمی بود. سعی می‌کردیم به صورت مبهم و غیرمستقیم صحبت کنیم، نگران از اینکه کسی ممکن است نظارت کند.

راه‌حل: حتی در زمان قطع اینترنت، برخی خدمات اینترنت ملی ممکن است فعال باقی بمانند (مانند ایمیل‌های با دامنه .ir). در این شرایط، می‌توان از رمزگذاری GPG بر روی این پلتفرم‌ها استفاده کرد تا محتوا برای افراد ثالث به راحتی قابل خواندن نباشد. همچنین می‌توان یک فایل یا پیام متنی رمزگذاری‌شده ایجاد کرده و از طریق کانال‌های دیگر مانند پیام‌رسان‌ها یا حتی پیامک ارسال کرد.

برنامه‌ریزی پیشگیرانه: قبل از قطع اینترنت، فرد و همسرش می‌توانند رمزگذاری GPG را برای ایمیل‌های خود تنظیم کنند. GPG امکان رمزگذاری پیام‌ها را فراهم می‌کند، به طوری که تنها گیرنده مورد نظر قادر به خواندن آن‌ها باشد. این زوج می‌توانستند کلیدهای عمومی GPG خود را از قبل رد و بدل کنند تا حتی در پلتفرم‌های تحت نظارت نیز بتوانند به صورت ایمن ارتباط برقرار کنند.

سناریوی دوم: قطع شبکه داده موبایل

در زمان قطع اینترنت در شهری بزرگ مانند تهران، مقامات با هدف اختلال در اینترنت موبایل (3G/4G) به‌ویژه در مناطقی مانند پارک لاله که اعتراضات در جریان بود، شبکه‌های مخابراتی (BTS) را هدف قرار دادند. همه سیم‌کارت‌ها از دسترسی به اینترنت، از جمله خدمات LTE، قطع شدند. با این حال، در حالی که اینترنت موبایل قطع شده بود، اینترنت ثابت خانگی (ADSL/TD-LTE) همچنان فعال بود.

با بهره‌گیری از این فرصت، با استفاده از VPN از طریق گوشی به شبکه اینترنت خانگی‌ام متصل شدم. از طریق ایجاد اتصال امن به وای‌فای خانگی‌ام از طریق VPN، توانستم قطع اینترنت موبایل را دور زده و به اینترنت دسترسی پیدا کنم. پس از اتصال، گوشی خود را به نقطه اتصال تبدیل کردم و امکان دسترسی به اینترنت را برای دیگران در اطرافم نیز فراهم کردم. در حالی که بسیاری از افراد دسترسی به اینترنت نداشتند من و اطرافیانم دسترسی کامل به اینترنت داشتیم.

یک هشدار نیز منتشر شده بود که به دلیل احتمال ردیابی، از آوردن تلفن همراه به محل اعتراضات خودداری کنید؛ اما راه‌حل من این امکان را فراهم کرد که با استفاده از شبکه امن خانگی‌ام، دسترسی به اینترنت را به روشی امن‌تر برای دیگران فراهم کنم.

راه‌حل: این روش بر این اساس استوار است که در حالی که شبکه‌های موبایل (BTS) قطع می‌شوند، خدمات اینترنت ثابت مانند ADSL یا TD-LTE ممکن است همچنان فعال بمانند. با اتصال به اینترنت ثابت از طریق VPN از دستگاه موبایل، می‌توان دسترسی به اینترنت را بازیابی کرد و با تبدیل گوشی به نقطه اتصال، این اتصال را با دیگران به اشتراک گذاشت.

اجرای این راه‌حل:

- **استفاده از اینترنت ثابت:** اگر اینترنت ثابت خانگی‌تان هنوز فعال است، از آن برای دسترسی به اینترنت جهانی استفاده کنید.
- **اتصال از طریق VPN:** یک VPN بر روی گوشی نصب و تنظیم کنید تا حتی در زمان قطع اینترنت موبایل، بتوانید به‌صورت ایمن به شبکه خانگی متصل شوید.
- **ایجاد نقطه اتصال:** پس از اتصال از طریق VPN، قابلیت نقطه اتصال گوشی را فعال کرده و اتصال اینترنت را با دیگران به اشتراک بگذارید.

این راه‌حل دسترسی مستمر به پلتفرم‌های آنلاین را در زمان اختلال شبکه‌های موبایل تضمین می‌کند و به شما امکان می‌دهد تا در لحظه متصل بمانید و به دیگران کمک کنید.

برنامه‌ریزی پیشگیرانه: جهت آماده‌سازی برای چنین شرایطی، ضروری است که پیش از قطع اینترنت، گام‌های مشخصی برداشته شود. در ادامه، نحوه برنامه‌ریزی را مشاهده می‌کنید:

تهیه ابزارهای لازم:

- **سرویس VPN :** یک سرویس VPN نصب کنید که امکان اتصال از راه دور به شبکه اینترنت خانگی را فراهم کند. اطمینان حاصل کنید که این سرویس بر روی گوشی و سایر دستگاه‌های شما نصب و تنظیم شده است.
- **اتصال اینترنت ثابت:** مطمئن شوید که اتصال اینترنت خانگی پایدار و قابل اعتمادی مانند TD-LTE یا ADSL دارید که می‌تواند در مواقع قطع شبکه موبایل استفاده شود.
- **قابلیت نقطه اتصال موبایل:** با قابلیت نقطه اتصال (هات‌اسپات) گوشی آشنا شوید و مطمئن شوید که این قابلیت فعال و تنظیم شده است.

هماهنگی با دیگران:

- به دوستان و خانواده اطلاع دهید که چه تنظیماتی انجام داده‌اید تا در صورت قطعی اینترنت، بتوانند به نقطه اتصال موبایل شما متصل شوند.
- آن‌ها را تشویق کنید تا تنظیمات مشابهی را برای پشتیبانی و کاهش بار راه‌اندازی کنند.

تهدیدهای احتمالی:

- **نظارت:** حتی در صورت استفاده از VPN برای رمزگذاری اتصال، مقامات همچنان ممکن است الگوهای ترافیک یا فراداده‌ها را پایش کنند، به‌ویژه اگر کنترل ISPهای محلی را در اختیار داشته باشند. استفاده از ابزارهای رمزگذاری مانند VPN یا Tor برای محافظت از داده‌ها ضروری است.
- **امنیت فیزیکی:** حمل موبایل با نقطه اتصال روشن ممکن است توجه را جلب کند، به‌ویژه اگر دسترسی شما به اینترنت مشهود باشد در حالی که دیگران قطع ارتباط دارند. مراقب باشید که اتصال خود را در کجا استفاده می‌کنید و از جلب توجه در مناطق با امنیت بالا یا اعتراضات خودداری کنید.
- **اختلال در خدمات:** با وجود اینکه خدمات اینترنت ثابت مانند TD-LTE یا ADSL ممکن است فعال بمانند، احتمال قطع آن‌ها نیز وجود دارد. هیچ تضمینی وجود ندارد که این اتصالات در طول قطعی‌های طولانی مدت نیز پایدار باقی بمانند.
- **تخلیه باتری:** استفاده از گوشی به‌عنوان نقطه اتصال می‌تواند باتری آن را به سرعت تخلیه کند، به‌ویژه در استفاده طولانی‌مدت. مطمئن شوید که شارژرهای قابل حمل یا منابع تغذیه در دسترس دارید تا اتصال را برای

مدت زمان طولانی‌تر حفظ کنید.

سناریوی سوم: قطع تقریباً کامل اینترنت و استفاده از زیرساخت‌های داخلی و رومینگ

در پاسخ به افزایش قطعی‌های اینترنت، گروهی به نام «ارتش مخفی» ایجاد کردیم تا راهی برای دور زدن این محدودیت‌ها و حفظ دسترسی به اینترنت پیدا کنیم. متوجه شدیم که می‌توانیم از سیم‌کارت‌های خارجی کشورهای مانند ترکیه و امارات، همچنین مراکز داده داخلی در ایران برای دسترسی به اینترنت استفاده کنیم.

استراتژی اصلی ما این بود که کاربران را از طریق VPN به سیم‌کارت‌های خارجی که از خدمات رومینگ در داخل ایران استفاده می‌کردند متصل کنیم. با این روش، ترافیک کاربران به شبکه‌های بین‌المللی منتقل شد و حتی در زمانی که شبکه‌های محلی قطع بودند، دسترسی به اینترنت را حفظ کردیم.

زمانی که خدمات رومینگ نیز مسدود شد، به روش دیگری سازگار شدیم و کاربران را به مراکز داده داخلی متصل کردیم. از طریق اتصال VPN، کاربران به این مراکز داده داخلی که هنوز به اینترنت جهانی متصل بودند دسترسی پیدا کردند. به این ترتیب، حتی در شرایط قطعی شدید، توانستیم ارتباطات و کانال‌های حیاتی اطلاعات را حفظ کنیم.

راه‌حل: راه‌حل در این سناریو بر دو استراتژی کلیدی متکی بود: استفاده از سیم‌کارت‌های خارجی با خدمات رومینگ و مراکز داده داخلی. این روش‌ها به کاربران امکان دادند که علی‌رغم اختلالات شبکه‌های محلی، به اینترنت متصل بمانند.

نحوه عملکرد:

- **استفاده از سیم‌کارت‌های خارجی برای رومینگ:** ما به کاربران دسترسی به سیم‌کارت‌های خارجی (مانند ترکیه و امارات) که همچنان خدمات رومینگ فعال در داخل ایران داشتند، ارائه کردیم. با اتصال به این سیم‌کارت‌ها از طریق VPN، کاربران توانستند محدودیت‌های اینترنتی ایران را دور بزنند و به خدمات اینترنت بین‌المللی دسترسی پیدا کنند.
- **اتصال به مراکز داده داخلی:** هنگامی که مقامات خدمات رومینگ را مسدود کردند، استراتژی خود را به مراکز داده داخلی تغییر دادیم. با مسیریابی ترافیک VPN از طریق این مراکز داده که به اینترنت جهانی متصل بودند، کاربران توانستند حتی در زمان قطعی گسترده اینترنت به خدمات آنلاین دسترسی داشته باشند.

هر دو روش به ما امکان دادند تا در لحظات بحرانی به کاربران دسترسی به اینترنت ارائه کنیم، به‌طوری که ارتباطات، به‌روزرسانی‌ها و تبادل اطلاعات علی‌رغم تلاش‌های دولت برای ایزوله‌سازی جامعه همچنان امکان‌پذیر باقی بماند.

برنامه‌ریزی پیشگیرانه: برای اطمینان از اینکه این روش در قطعی‌های اینترنت آینده به‌خوبی کار کند، ضروری است که از قبل برنامه‌ریزی و آماده‌سازی انجام شود. در ادامه مراحل آماده‌سازی ذکر شده است:

- **تهیه سیم‌کارت‌های خارجی**
  - اطمینان حاصل کنید که شما یا افراد مورد اعتماد به سیم‌کارت‌های خارجی از کشورهایی مانند ترکیه یا امارات دسترسی دارند. این سیم‌کارت‌ها را از قبل تست کنید تا مطمئن شوید می‌توانند از طریق رومینگ در ایران متصل شوند.
  - برای توزیع این سیم‌کارت‌ها به کاربران مورد اعتماد در مواقع قطعی گسترده اینترنت، یک برنامه پشتیبان داشته باشید.
- **راه‌اندازی زیرساخت VPN**
  - سرورهای VPN را راه‌اندازی و پیکربندی کنید تا بتوانند ترافیک را از طریق سیم‌کارت‌های خارجی یا مراکز داده داخلی مسیریابی کنند. اطمینان حاصل کنید که VPN با این سیم‌کارت‌ها تست شده و می‌تواند اتصالات امن برقرار کند.
  - چندین پیکربندی VPN آماده داشته باشید تا در صورت مسدود شدن یک سرور یا روش، گزینه‌های دیگری در دسترس باشد.
- **ایجاد ارتباط با مراکز داده داخلی**

- مراکز داده داخلی را شناسایی کنید و ارتباطات امنی با آن‌ها برقرار کنید که حتی در زمان قطعی‌های جزئی همچنان به اینترنت جهانی دسترسی دارند. در صورت امکان، با افراد مورد اعتماد در این مراکز داده ارتباط برقرار کنید تا اتصال به اینترنت حفظ شود.
- اطمینان حاصل کنید که VPN می‌تواند ترافیک را به‌راحتی از طریق این مراکز داده مسیریابی کند اگر خدمات رومینگ قطع شدند.

- **تست منظم سیستم‌های پشتیبان**
  - به‌طور منظم کل تنظیمات را تست کنید، از اتصال VPN گرفته تا عملکرد سیم‌کارت‌های خارجی و مراکز داده. اطمینان حاصل کنید که کاربران می‌دانند در مواقع نیاز چگونه به این سیستم‌ها متصل شوند.
  - یک کانال ارتباطی امن و خصوصی ایجاد کنید تا به کاربران آموزش دهید چگونه به VPN متصل شده و در زمان قطعی اینترنت دسترسی را حفظ کنند.

تهدیدات احتمالی: در حالی که این روش می‌تواند دسترسی به اینترنت را در شرایط قطعی شدید فراهم کند، خطراتی نیز به همراه دارد:

- **نظارت و شناسایی:** مقامات ممکن است ترافیک سیم‌کارت‌های خارجی یا مراکز داده داخلی را پایش کنند، به‌ویژه اگر مشکوک شوند که افراد از این روش‌ها برای دور زدن قطعی اینترنت استفاده می‌کنند. استفاده از رمزگذاری (مانند VPN،Tor و غیره) ضروری است تا خطر نظارت و شناسایی به حداقل برسد.
- **امنیت فیزیکی:** در اختیار داشتن سیم‌کارت‌های خارجی یا دسترسی به مراکز داده داخلی ممکن است در مناطق با امنیت بالا یا تحت نظارت دولت شک‌برانگیز باشد. اطمینان حاصل کنید که افراد درگیر از خطرات احتمالی آگاه بوده و می‌دانند چگونه در چنین شرایطی رفتار کنند.
- **قطع مراکز داده:** اگر دولت تشخیص دهد که از مراکز داده داخلی برای دور زدن محدودیت‌ها استفاده می‌شود، ممکن است دسترسی به این مراکز را نیز مسدود کند. داشتن چندین سرور VPN یا روش‌های جایگزین ضروری است تا اتصال امن حفظ شود.
- **ازدحام روی سیم‌کارت‌های خارجی:** اگر تعداد زیادی کاربر به تعداد محدودی سیم‌کارت خارجی متصل شوند، شبکه ممکن است دچار ازدحام شده و باعث کاهش عملکرد یا ایجاد مشکلات اتصال شود. داشتن سیم‌کارت‌ها و سرورهای VPN متعدد برای توزیع بار شبکه ضروری است.

سناریوی چهارم: استفاده از پلتفرم‌های بازی و کسب‌وکار برای ارتباطات

پس از حادثه اسقاط هواپیمای اوکراینی و محدودیت‌های اینترنت در سراسر کشور، به روش‌های قدیمی ارتباطی مانند فکس و پیامک برای اطلاع‌رسانی درباره برگزاری نمایشگاه برگشتیم، این وضعیت یادآور اوایل دهه ۲۰۰۰ بود. اینترنت دیگر هرگز مثل قبل نبود. ما مجبور شدیم به سیستم‌های ارتباطی منسوخ مانند ارسال نامه با پیک موتوری تکیه کنیم.

در زندگی شخصی من، قطع اینترنت ارتباطم را با دنیای بیرون کاملاً قطع کرد. احساس می‌کردم در جزیره‌ای گیر افتاده‌ام و هیچ راهی برای ارتباط با جهان بیرون یا فرار ندارم. گرچه این قطع ارتباط لزوماً زندگی روزمره را مختل نمی‌کرد، اما احساس ناامنی شدیدی داشت. برای دسترسی به اخبار مجبور شدیم به سایت «پیوندها»، صفحه سانسور اینترنت ایران، سر بزنیم. بدون دسترسی به تلویزیون یا ماهواره، تلاش می‌کردیم از منابع خبری داخلی حقیقت را کنار هم بگذاریم. به دلیل نگرانی از پروتکل‌های مربوط به حفاظت ا حریم خصوصی، به اپلیکیشن‌های داخلی اعتماد نداشتم. از سوی دیگر مطالبی در رابطه با اینترنت ماهواره‌ای شنیده بودم اما قیمت آن خیلی بالا بود. در نتیجه، بسیاری از ما به VPNها متوسل شدیم تا سعی کنیم دوباره به اینترنت جهانی دسترسی پیدا کنیم. گاهی اوقات اتاق‌های خبر رسانه‌ها «امتیازهای» اینترنت محدود و بسیار کمی ارائه می‌دادند که عمدتاً برای عکاسان بود و حس می‌کردیم که بسیار تحت کنترل و دستکاری‌شده است.

پس از اعتراضاتی که با جان‌باختن مهسا آغاز شد، اینترنت در برخی مناطق قطع شد تا ارتباطات مختل و از سازماندهی جلوگیری شود. اما ما راه‌های جایگزینی برای ارتباط پیدا کردیم، از جمله استفاده از پلتفرم‌های بازی و اپلیکیشن‌های داخلی مانند دیوار که احتمال کمتری برای نظارت بر آنها وجود داشت.

در سپتامبر ۲۰۲۲، این وضعیت تشدید شد. دیگر برای جلوگیری از گسترش نظارت دولت خیلی دیر شده بود و مهم‌ترین اولویت این بود که فعالیت‌های‌مان جان دیگران را به خطر نیندازد. گروهی در محله ما در اکباتان یک تجمع اعتراضی سازماندهی کرده بودند، اما زمانی که به آنجا رسیدیم، منطقه پر از نیروهای بسیجی بود.

ما کدهایی برای ارتباط ایمن ایجاد کرده بودیم. ابتدا ساکت می‌ماندیم و فاصله می‌گرفتیم تا شرایط را بسنجیم. همچنین کانال‌های پشتیبان ارتباطی داشتیم، از جمله گروه خاصی در تلگرام با اعضای مشترک که زبان و کدهای خاصی را برای انتقال اطلاعات می‌دانستند.. بسیاری از این افراد طراح بازی بودند و بازی‌هایی ایجاد کرده بودند که به‌طور مخفیانه برای سازماندهی استفاده می‌شد؛ در واقع کسی بازی نمی‌کرد، بلکه این پلتفرم‌ها به‌عنوان ابزاری برای ارتباطات به کار می‌رفتند.

به عنوان عکاس، همواره نگران حفاظت از خود و کارم بودم و به روش‌های سنتی بازگشتم تا امنیت بیشتری داشته باشم. در دو یا سه روز اول اعتراضات، من و بسیاری از همکارانم، دوربین‌هایمان را به خیابان بردیم تا وقایع را مستند کنیم. اما وقتی دستگیری‌ها و ضبط دوربین‌ها شروع شدند، استفاده از تلفن همراه را متوقف کردم. به جای آن، از یک دوربین سونی قدیمی بدون لنز و با یک کارت SD کوچک استفاده کردم که به اینترنت متصل نبود. زمانی که در نهایت کارت SD را از بین بردم، هیچ اثری از کارهایم باقی نماند. همواره در قاب‌بندی عکس‌ها مراقب بودم تا چهره افراد را محو کنم و هویت آن‌ها را حفظ کنم.

راه‌حل: برای کاهش تاثیرات قطع اینترنت، به ویژه برای افرادی که در حوزه‌های حساس یا خلاقانه و هنری فعالیت می‌کنند، یک راه‌حل چند لایه لازم است:

- **پلتفرم‌های ارتباطی جایگزین:** در زمان اعتراضات، افراد می‌توانند از پلتفرم‌های بازی یا اپلیکیشن‌های داخلی مانند دیوار به‌عنوان کانال‌های ارتباطی مخفی استفاده کنند. از آنجا که تمام این ارتباطات به صورت متنی انجام می‌شود، کاربران باید آدرس IP خود را پنهان کرده و تمام ارتباطات را رمزگذاری کنند.
- **ذخیره و انتقال داده‌های رمزگذاری‌شده:** استفاده از ابزارهای رمزگذاری قوی مانند GPG برای حفاظت از ارتباطات و داده‌ها، به ویژه برای روزنامه‌نگاران و هنرمندان، ضروری است. علاوه بر این، آن‌ها باید به‌طور منظم از کارهای خود نسخه‌های پشتیبان تهیه و به‌صورت آفلاین و رمزگذاری‌شده (مانند USB یا SSD) ذخیره کنند. این نسخه‌های پشتیبان می‌توانند از طریق سرویس‌های ابری یا راهکارهای ذخیره‌سازی غیرمتمرکز مانند IPFS در خارج از کشور نیز نگهداری شوند.
- **پلتفرم‌های غیرمتمرکز برای به اشتراک‌گذاری آثار و محتوا:** هنرمندان باید به پلتفرم‌های مبتنی بر بلاکچین برای نمایش آثار خود توجه کنند. فناوری‌های غیر متمرکز مانند NFTها می‌توانند به هنرمندان این امکان را بدهند که حتی در صورت مسدود شدن پلتفرم‌های مرکزی مانند اینستاگرام، آثار خود را به صورت جهانی به اشتراک بگذارند.

برنامه‌ریزی پیشگیرانه: برای آماده‌سازی جهت قطعی‌های احتمالی اینترنت در آینده، افراد و سازمان‌ها باید از پیش برنامه‌ریزی کنند:

- **شبکه‌های مش (Mesh Networks) :** ایجاد شبکه‌های محلی مش که به دستگاه‌های الکترونیکی امکان اتصال مستقیم بدون نیاز به اینترنت گسترده را می‌دهد، ضروری است. این شبکه‌ها برای حفظ ارتباطات در زمان قطعی‌های طولانی مدت، به‌ویژه در مناطق شهری متراکم، بسیار کاربردی خواهند بود.
- **پشتیبان‌گیری و مدیریت داده‌های آفلاین:** پشتیبان‌گیری منظم از داده‌ها در مکان‌های امن و آفلاین اطمینان می‌دهد که کارها و ارتباطات حتی در زمان قطعی‌ها قابل دسترسی باقی می‌مانند. استفاده از خدماتی مانند IPFS برای ذخیره‌سازی غیرمتمرکز یا فضای ابری امن بین‌المللی می‌تواند یک لایه حفاظتی برای داده‌های حساس فراهم کند.
- **آموزش سواد دیجیتال و امنیت:** آموزش روش‌های ارتباط امن به هنرمندان، فعالان و دیگر گروه‌های آسیب‌پذیر، از جمله استفاده از VPN، ابزارهای رمزگذاری و سیستم‌های پشتیبان‌گیری آفلاین، به آن‌ها کمک می‌کند که در مواجهه با قطعی اینترنت آمادگی بیشتری داشته باشند.

با پذیرش این راه‌حل‌ها و اجرای اقدامات پیشگیرانه، افراد، کسب‌وکارها و هنرمندان می‌توانند حتی در زمان قطع اینترنت، کار خود را با امنیت و اطمینان بیشتری ادامه دهند. این امر به محافظت از ارتباطات حیاتی، تداوم کارهای خلاقانه، هنری و حفظ آزادی بیان و سازماندهی کمک می‌کند.

بازی قطع اینترنت

بازی «قطع اینترنت» با دقت طراحی شده است تا تجربه‌ای جذاب و آموزشی پیرامون موضوع قطع اینترنت ارائه دهد. هدف اصلی آن، آشنا کردن شرکت‌کنندگان با تکنیک‌های مختلفی است که برای مختل کردن دسترسی به اینترنت به کار می‌روند و همچنین شامل راهبردهایی برای مقابله با این محدودیت‌ها است. این بازی با هدف برجسته‌سازی موضوع مهم سانسور اینترنت ساخته شده است و به بررسی انگیزه‌های پشت این قطعی‌ها و تأثیرات آن‌ها بر حقوق بشر می‌پردازد. با استفاده از این بازی با قابلیت مشارکت فعال یا گیم‌پلی تعاملی، افراد و سازمان‌ها می‌توانند دانش قابل توجهی در رابطه با روش‌های دولت‌ها برای مسدود کردن دسترسی به اینترنت پیدا کنند و راه‌های مؤثری برای حفاظت از آزادی دیجیتال بیاموزند.

این بازی در گردهمایی‌های حضوری و آنلاین قابل استفاده است و به‌عنوان یک ابزار چندکاره برای گروه‌های متنوع عمل می‌کند و شامل دستورالعمل‌های دقیق برای تسهیل‌گران، دینامیک‌های بازی و منابعی مانند نقشه‌ها و کارت‌ها برای افزایش کیفیت تجربه‌ی بازی است. در یک جلسه ۱۲۰ دقیقه‌ای، بازیکنان به جنبه‌های فنی قطع اینترنت می‌پردازند، با سناریوهای واقعی مواجه می‌شوند و با استفاده از کارت‌های «دور زدن» روش‌های مختلف برای عبور از محدودیت‌ها را بررسی می‌کنند. با بهره‌گیری از مجوز اشتراک‌گذاری آزاد(creative commons license)، این بازی به کاربران اجازه می‌دهد محتوا را متناسب با نیازهای خود تغییر دهند، درک عمیق‌تری از زیرساخت اینترنت به دست آورند و توانایی خود برای مقابله و مقاومت در برابر قطع اینترنت را تقویت کنند.

محتویات فایل‌های بازی:

- **راهنمای بازی:** شامل دستورالعمل‌هایی برای کمک به تسهیل‌گران در سازماندهی جلسات آموزشی؛ هم به‌صورت آنلاین و هم به صورت حضوری.
- **۱۳ سناریوی مسدودسازی:** برای انتخاب سناریوهای مرتبط با مخاطب و اهداف مورد نظر.
- **ارائه‌ها و تصاویر قابل ویرایش:** برای تطبیق مطالب با نیازها و ویژگی‌های مخاطب.

توجه داشته باشید که این بازی برای یادگیری شخصی درباره قطع اینترنت طراحی نشده است و نیازمند حضور تسهیل‌گر و تعامل با دیگران است.