

در زمان قطعی اینترنت چگونه فعالیت کنیم؟

صدای امن
sv.khro.org

فهرست

- مقدمه
- فصل اول: بهداشت دیجیتال در شبکه‌های اجتماعی
- فصل دوم: شبکه‌سازی محلی در زمان قطعی کامل
- فصل سوم: پروتکل‌های تاب‌آور و ارتباطات ماهواره‌ای؛ شکستن حصار خاموشی
- فصل چهارم: شبکه‌سازی دستی و تاکتیک‌های غیردیجیتال
- سخن پایانی





مقدمه

در سال‌های اخیر، اقلیم اهواز (خوزستان) همواره یکی از نخستین مناطقی بوده است که در زمان بروز بحران‌های کارگری، محیط زیستی (مانند بحران آب) و اعتراضات مردمی، با قطع سراسری یا اختلالات شدید و هدفمند اینترنت مواجه شده است. قطع ارتباطات دیجیتال در اهواز، صرفاً یک اختلال فنی نیست، بلکه یک سلاح استراتژیک برای منزوی کردن جامعه، قطع جریان آزاد اطلاعات، و جلوگیری از سازمان‌دهی شبکه‌های مقاومت محلی است.

وابستگی مطلق به پلتفرم‌های ابری (مانند اینستاگرام و واتس‌اپ) یک خطای محاسباتی کشنده در زمان بحران است. فعالان اهوازی نیازمند تسلط بر شبکه‌ای از ابزارهای جایگزین (آفلاین و نظیربه‌نظیر) و بازگشت به تاکتیک‌های هوشمندانه غیردیجیتال هستند. این کتابچه، راهنمای گام‌به‌گام و عملیاتی برای عبور از سد خاموشی‌هاست.



فصل اول

بهداشت دیجیتال در شبکه‌های اجتماعی

تحقیقات نشان می‌دهد که بسیاری از بازداشت‌ها نه در کف خیابان‌های اهواز، بلکه در فضای پنهان شبکه‌های اجتماعی ریشه دارند. پاک‌سازی ردپای دیجیتال پیش از آغاز هرگونه بحران، دیگر یک توصیه ساده نیست، بلکه یک پروتکل امنیتی الزام‌آور برای بقای کنشگران است. در ادامه، حیاتی‌ترین اقدامات پیشگیرانه در این فضا بررسی شده است.

1. ذخیره‌سازی آفلاین:

نقشه‌های محلات اهواز را در گوگل‌مپس به صورت آفلاین دانلود کنید تا در صورت قطعی اینترنت بتوانید بدون جی‌پی‌اس مسیریابی کنید.



2. پاک‌سازی دستگاه (Wiping) و متادیتا:

عکس‌هایی که در محلات اهواز می‌گیرید، شامل مختصات جغرافیایی دقیق هستند. پیش از خاموشی، از برنامه‌هایی مثل Scrambled Exif برای حذف این متادیتا استفاده کنید. اگر قطعی اینترنت با حضور سنگین نیروهای امنیتی در خیابان همراه است، قبل از خروج از خانه، تمامی چت‌های حساس را از روی گوشی حذف کنید. در زمان قطعی اینترنت، تایمر پیام‌های ناپدیدشونده عمل نمی‌کنند.

3. کیف فارادی (Faraday Bag):

در زمان تجمعات، گوشی شما دائماً به دنبال اتصال به دکل‌های مخابراتی می‌گردد و موقعیت شما ثبت می‌شود. قرار دادن گوشی در کیف فارادی (یا پیچیدن آن در چند لایه فویل آلومینیومی ضخیم)، تمام سیگنال‌های آن را مسدود می‌کند.

4. دیوار دفاعی دوم؛ عبور از سد تأیید دو مرحله‌ای (2FA):

گزارش‌های مستند حاکی از آن است که تکیه بر پیامک (SMS) برای احراز هویت، یکی از بزرگترین حفره‌های امنیتی است که به راحتی توسط نهادهای ناظر شنود و رهگیری می‌شود. کارشناسان امنیت سایبری اکیداً توصیه می‌کنند که فعالان اهوازی برای قفل‌گذاری دوم حساب‌های شبکه‌های اجتماعی خود (مانند تلگرام، اینستاگرام و ایکس) تحت هیچ شرایطی از شماره موبایل استفاده نکنند؛ بلکه تنها از اپلیکیشن‌های تولید کد آفلاین نظیر Google Authenticator یا 2FAS بهره ببرند.



5. آرشیوهای خطرناک؛ لزوم پاک‌سازی حافظه اینترنت

فضای مجازی فراموش نمی‌کند. ردپای به جا مانده از کامنت‌ها و لایک‌های قدیمی می‌تواند به عنوان اسناد جرم گذشته‌نگر علیه شهروندان استفاده شود. بررسی‌های فنی نشان می‌دهد که نهادهای سایبری از ابزارهای هوشمندِ خزش (Crawling) برای یافتن کلمات کلیدی در کل وب استفاده می‌کنند. جستجوی نام مستعار خود در اینترنت و پاک‌سازی هرگونه اظهارنظر، لایکِ مکان‌نما یا پُستِ دردسرساز قدیمی، برای جلوگیری از تشکیل پرونده الزامی است.

6. تله مکان‌نمایی؛ خطرات پنهان لوکیشن زنده

در روزهای ملتهب اهواز، انتشار موقعیت مکانی زنده (Live Location) در استوری‌ها یا تگ کردن افراد در تصاویر، به مثابه ارسال یک سیگنال ردیابیِ مستقیم برای نهادهای امنیتی است. گزارش‌ها نشان می‌دهد که هوش مصنوعی قادر است از طریق تطبیق پس‌زمینه‌ها، زاویه تابش آفتاب و تابلوهای شهری در تصاویر، موقعیت فعالان را شناسایی کند. رعایت اصل «استتار بصری» و پرهیز از انتشار فوری تصاویر، یک اصل تخطی‌ناپذیر در روزنامه‌نگاری شهروندی به شمار می‌رود.

7. هویت‌های سایه‌وار؛ ضرورت تفکیک مرزهای دیجیتال

خبرنگاران بحران و فعالان میدانی نباید تحت هیچ شرایطی از نام حقیقی، تاریخ تولد یا چهره واقعی خود در حساب‌های مبارزاتی استفاده کنند. استفاده از آواتارهای گرافیکی و اسامی مستعاری که فاقد هرگونه پیوند با زندگی شخصی فرد باشند، اولین خط دفاعی در برابر ماشین‌های تشخیص چهره و سیستم‌های احراز هویت دولتی است. علاوه بر این، ایمیل ثبت‌شده برای این حساب‌ها باید کاملاً ناشناس و اختصاصی باشد.



فصل دوم

شبکه‌سازی محلی در زمان قطعی کامل

هنگامی که دسترسی به سرورهای جهانی مسدود می‌شود، باید از شبکه‌های محلی و درهم‌تنیده استفاده کرد که نیازی به زیرساخت‌های دولتی و اینترنت ندارند. در این بخش، سه ابزار کلیدی برای این منظور معرفی می‌شود:

- بریر (Briar)؛ برای طلایی پیام‌رسانی آفلاین
- بریج‌فای (Bridgefy)؛ برای تجمعات متمرکز
- مرورگر سِنو (Ceno)؛ گردش اطلاعات به روش تورنت



برایـــــــر (Briar)

- **برایر (Briar)** یک اپلیکیشن پیام‌رسان با رمزنگاری سرتاسری و متمرکز بر حریم خصوصی است. این برنامه مجهز به تکنولوژی شبکه مِش (Mesh Network) بوده و به طور خاص برای کنشگران مدنی، روزنامه‌نگاران و شهروندان در شرایط بحرانی (مانند خاموشی اینترنت یا سرکوب امنیتی) طراحی شده است. برخلاف پیام‌رسان‌های مرسوم، Briar برای کار کردن به سرور مرکزی یا اتصال دائم به اینترنت جهانی وابسته نیست.
- **الف) مکانیزم عملکرد:** ارتباط بدون اینترنت بزرگترین قدرت بریر، توانایی برقراری ارتباط بدون نیاز به دکل‌های مخابراتی است.
در زمان قطعی اینترنت: برنامه از طریق «بلوتوث» (برای فواصل نزدیک) و «وای‌فای محلی» (بدون نیاز به مودم اینترنت) پیام‌ها را مستقیماً بین گوشی‌ها همگام‌سازی می‌کند. با این اتصال نقطه‌به‌نقطه (P2P)، یک شبکه درهم‌تنیده شکل می‌گیرد.

- اگر شما به دوستتان متصل شوید و او به شخص سومی وصل باشد، پیام شما از طریق گوشی دوستتان به نفر سوم می‌رسد، بدون آنکه محتوای پیام توسط او قابل خواندن باشد.
- **در زمان اتصال به اینترنت:** اگر اینترنت وصل باشد، Briar برای محافظت از شما در برابر شنود، تمامی ارتباطات را از شبکه مخفی و امن «تور» (Tor) عبور می‌دهد تا ردیابی موقعیت مکانی‌تان بسیار دشوار شود.



ب) امنیت و حریم خصوصی

بدون سرور مرکزی: پیام‌ها در هیچ کامپیوتری در دنیا ذخیره نمی‌شوند و منحصراً روی گوشی فرستنده و گیرنده می‌مانند.
ثبت‌نام بدون هویت واقعی: برای ساخت حساب نیازی به شماره تلفن، ایمیل یا سیم‌کارت نیست.
رمزنگاری کامل: مکاتبات چنان رمزگذاری می‌شوند که حتی توسعه‌دهندگان برنامه نیز قادر به خواندن آن‌ها نیستند.

ج) نصب و ایجاد حساب کاربری (اندروید) بریر را می‌توانید به سادگی از «گوگل پلی»، مارکت «F-Droid» یا از طریق دانلود مستقیم وب‌سایت رسمی Briar نصب کنید. در اولین ورود، یک نام مستعار و یک گذرواژه قوی (حداقل ۸ کاراکتر) انتخاب کنید.

⚠ **هشدار**: حساب کاربری شما فقط روی دستگاهتان ذخیره می‌شود. اگر برنامه را پاک کنید یا رمزتان را فراموش کنید، حسابتان به هیچ‌وجه قابل بازیابی نیست.

د) روش‌های امن برای افزودن مخاطب

از نزدیک (تأیید هویت حضوری): این امن‌ترین روش است. با زدن علامت (+) گزینه «افزودن مخاطب از نزدیک» را انتخاب کنید. دوربین را روی بارکد (QR Code) گوشی یکدیگر بگیرید تا جفت شوید. این کار نفوذ مأموران به شبکه شما را کاملاً غیرممکن می‌کند.
اگر امکان ملاقات ندارید، پیوند اختصاصی خود (شروع با briar://) را از یک راه امن برای طرف مقابل بفرستید تا او با وارد کردن آن به شما متصل شود.

هـ) سایر قابلیت‌ها علاوه بر چت دونفره، می‌توانید مخاطبان امن خود را به یکدیگر معرفی کنید یا گروه‌های خصوصی بسازید که پیام‌های آن نیز کاملاً رمزگذاری شده است (در گروه‌ها فقط سازنده می‌تواند عضو جدید اضافه کند).



بریج‌فای (Bridgefy)

این برنامه عملکردی مشابه بریر دارد اما شعاع بلوتوث آن بیشتر است (حدود ۱۰۰ متر). بریج‌فای برای تجمعات متراکم در خیابان‌های اهواز بسیار مناسب است؛ اما به یاد داشته باشید که امنیت آن کمتر از بریر است، بنابراین نباید برای هماهنگی‌های بسیار حساس (مانند ارسال اسامی واقعی و آدرس‌ها) از آن استفاده کرد.

مرورگر سِنو (Ceno)

سانسورچی می‌تواند سایت‌های خبری را فیلتر کند، اما نمی‌تواند جلوی اشتراک‌گذاری «کاربر با کاربر» را بگیرد. Ceno از پروتکل Ouinet استفاده می‌کند و به کاربرانی که موفق شده‌اند یک صفحه وب (مانند یک گزارش خبری حقوق بشری) را باز کنند، اجازه می‌دهد تا آن محتوا را به صورت آفلاین در شبکه محلی، با کسانی که اینترنت ندارند به اشتراک بگذارند.

در این بخش، به بررسی تخصصی و جزئی پروتکل‌هایی می‌پردازیم که در زمان «محاصره دیجیتال»، حکم شریان‌های حیاتی را برای کنشگران میدانی و شهروندان ایفا می‌کنند. این ابزارها برای دور زدن فیلترینگِ متمرکز و تأمین اتصال در زمان قطع کامل ستون فقرات اینترنت (Backbone) طراحی شده‌اند.



فصل سوم

پروتکل‌های تاب‌آور و ارتباطات ماهواره‌ای

قطع اینترنت در زمان بحران‌ها، به ندرت یک «خاموشی مطلق و صد درصدی» است؛ بلکه در واقع یک «محاصره دیجیتال» و انتقال اجباری کاربران از اینترنتِ آزاد به یک شبکه داخلی (اینترانت) است تا سیستم‌های بانکی، بیمارستانی و دولتی از کار نیفتند. دستگاه سرکوب دیواری به دور اقلیم اهواز می‌کشد، اما لاجرم روزنه‌هایی را برای تنفسِ سیستمِ خودش باز می‌گذارد.

هنر یک کنشگر حرفه‌ای و آموزش‌دیده، تبدیل کردنِ همین روزنه‌ها به تونل‌های ارتباطی است. این فصل به شما می‌آموزد که چگونه از پروتکل‌های «تاب‌آور» استفاده کنید؛ ابزارهایی که پیام‌های مبارزاتی شما را در لباسِ ترافیکِ مجاز و عادی (مثل ایمیل‌های اداری) پنهان کرده و از دیوارهای هوشمند فیلترینگ عبور می‌دهند.

در گام بعدی، زمانی که کابل‌ها و زیرساخت‌های زمینی به طور کامل به روی مردم بسته می‌شوند، تنها مسیر فرار، نگاه به بالا است. در این بخش تشریح می‌کنیم که چگونه با رعایت سخت‌گیرانه‌ترین اصول استتار و امنیت، انحصار حکومت بر جریان اطلاعات را در هم بشکنید و با استفاده از ارتباطات ماهواره‌ای، آسمان را به تنها مرزِ غیرقابل‌سانسور برای رساندن صدای خود تبدیل کنید.



دلتـــــا چت (Delta Chat)؛ استتار در شبکه‌های اداری

زمانی که نهادهای نظارتی دسترسی به پیام‌رسان‌های مشهوری مانند تلگرام یا واتس‌اپ را مسدود می‌کنند، معمولاً زیرساخت‌های «ایمیل» (پروتکل‌های IMAP و SMTP) را باز می‌گذارند؛ چرا که از کار افتادن ایمیل به معنای فلج شدن سیستم‌های بانکی، اداری و مکاتبات دولتی است.

دلتا چت یک «انگلِ هوشمند» در بستر ایمیل است. این برنامه ظاهر و راحتیِ یک پیام‌رسان مدرن را دارد، اما در پشت صحنه، هر پیام شما را به صورت یک ایمیلِ رمزنگاری شده ارسال می‌کند. از دید سیستم‌های فیلترینگ، شما در حال انجام یک مکاتبه ساده ایمیلی هستید.

نکات امنیتی حیـــاتی

- **انتخاب سرویس‌دهنده:** هرگز از سرویس‌های داخلی یا جی‌می‌ل (Gmail) برای کارهای حساس استفاده نکنید. بهترین گزینه، استفاده از سرویس‌های امن و ناشناس مانند ProtonMail است.
- **رمزنگاری خودکار:** دلتا چت از استاندارد Autocrypt استفاده می‌کند. یعنی اولین پیامی که بین دو نفر رد و بدل می‌شود، کلیدهای رمزنگاری را تبادل کرده و تمام پیام‌های بعدی کاملاً ناخوانا می‌شوند.
- **عدم وابستگی به شماره:** برای ثبت‌نام نیاز به سیم‌کارت ندارید، که این موضوع خطر ردیابی هویت را از طریق اپراتورهای داخلی (همراه اول/ایرانسل) از بین می‌برد.



2. استارلینک (Starlink)

استارلینک نه تنها یک ابزار تکنولوژیک، بلکه یک «سپر دفاعی» در برابر قطع سراسری اینترنت است. با این حال، استفاده از آن در مناطق حساس امنیتی مانند اهواز، نیازمند رعایت پروتکل‌های حفاظتی بسیار سخت‌گیرانه است.

الف) شیوه استفاده صحیح و عملیاتی

- **مکان‌یابی هوشمند:** دیش استارلینک (Dishy) باید دید مستقیم به آسمان داشته باشد، اما هرگز نباید به تنهایی روی یک پشت‌بامِ خالی قرار گیرد. بهترین مکان، استتار میان انبوهی از اشیاء دیگر (مانند کولرها، مخازن آب یا تجهیزات رها شده) است تا از دیدرسِ مستقیم خارج شود.
- **اتصال کابلی به جای وای‌فای:** سیگنال‌های وای‌فای به راحتی توسط دستگاه‌های جهت‌یابِ امنیتی قابل شناسایی هستند. اکیداً توصیه می‌شود از آداپتور اترنت (Ethernet Adapter) استارلینک استفاده کرده و اینترنت را منحصراً با کابل LAN به داخل ساختمان منتقل کنید.
- **اشتراک‌گذاری امن:** اگر نیاز دارید اینترنت را با هسته‌های دیگر به اشتراک بگذارید، از مودم‌های ثانویه با بُردِ کم استفاده کنید و نام شبکه (SSID) را حتماً روی حالت مخفی (Hidden) قرار دهید.

ب) خطرات شناسایی و بازداشت

- **شناسایی بصری:** پهپادهای نظارتی به طور مداوم به دنبال اشکال هندسی منظم (دیش‌های سفید و چهارگوش) روی پشت‌بام‌ها هستند.

- **ردیابی فرکانسی (رادیوگونیومتری):** دستگاه‌های ردیاب می‌توانند سیگنال‌های ارسالی دیش به سمت ماهواره (Uplink) را شناسایی کنند. اگرچه این کار از نظر فنی دشوار است، اما فعالیت مداوم و طولانی‌مدت، احتمال شناسایی مکانِ دقیق دیش را به شدت افزایش می‌دهد.

- **بازرسی‌های خانه‌به‌خانه:** نگهداری فیزیکی تجهیزات استارلینک به دلیل ممنوعیت‌های قانونی، همواره یک ریسک امنیتی بزرگ محسوب می‌شود.

ج) پروتکل‌های حفاظتی و نکات ایمنی تکمیلی

- **استتار فیزیکی دیش:** می‌توانید از رنگ‌های پلاستیکی مات (که مطلقاً فاقد ذرات فلزی باشند) برای رنگ‌آمیزی دیش مطابق با بافت و رنگ پشت‌بام استفاده کنید. همچنین، پوشاندن دیش با پارچه‌های بسیار نازک نخی یا کیسه‌های پلاستیکی تیره مانع عبور سیگنال نمی‌شود، اما آن را از دید پهپادها پنهان می‌کند.

- **مدیریت زمان اتصال (استراتژی اتصال ضربتی):** دیش را ۲۴ ساعته روشن نگذارید. از استراتژی «اتصال ضربتی» استفاده کنید؛ یعنی صرفاً در ساعات مشخص و خلوت شبانه‌روز (مثلاً ۳ بامداد) دیش را روشن کنید، داده‌ها و گزارش‌ها را به سرعت ارسال یا دریافت کنید و سپس بلافاصله آن را خاموش، جمع‌آوری و مخفی سازید.

در صورت امکان از پنل‌های خورشیدی یا پاوربانک‌های بزرگ و استاندارد استفاده کنید تا نوسانات برق شهری یا قطع هدفمند برق توسط نهادهای امنیتی، فعالیت ارتباطی شما را مختل نکند.





3.توشـــــه (Toosheh)؛ کتابخانه دیجیتال آفلاین

توشه یک راهکار یک‌طرفه اما فوق‌العاده امن برای دریافت اطلاعات حجیم در زمان قطع کامل اینترنت است.

چرا توشه نفوذناپذیر به شمار می‌آید؟
چون شما هیچ سیگنالی «ارسال» نمی‌کنید. شما فقط مانند تماشای تلویزیون، داده‌ها را «دریافت» می‌کنید. بنابراین هیچ ردیابیِ فرکانسی برای شناسایی شما وجود ندارد.

روش استفاده:رسیور ماهواره خود را روی فرکانس شبکه توشه (معمولاً در ماهواره یاه‌ست) تنظیم کنید.
یک فلش مموری به پورت USB رسیور وصل کنید.
در زمان پخش بسته‌های دیتا (معمولاً شب‌ها)، گزینه ضبط (Record) را بزنید.
پس از اتمام، فلش را به لپ‌تاپ متصل کرده و با نرم‌افزار مخصوص توشه، بسته‌ها را باز کنید.

محتوا: این بسته‌ها شامل فیلترشکن‌های جدید، ویدیوهای آموزشی امنیتی، اخبار سانسورنشده و حتی نسخه‌های آفلاین ویکی‌پدیا هستند. این روش برای «تغذیه اطلاعاتی» شبکه‌های محلی در زمان خاموشی طولانی‌مدت اینترنت در اهواز بی‌نظیر است.



فصل چهارم

شبکه‌سازی دستی و تاکتیک‌های میدانی

تکیه مطلق بر فناوری، پاشنه آشیل هر جنبش مدنی است. سناریوی محتمل در بحران‌های شدید امنیتی، از کار افتادن تمامی زیرساخت‌های الکترونیکی است. در این «نقطه صفر»، هسته‌های مقاومت باید به سرعت به روش‌های سنتی، فیزیکی و غیرقابل‌شنود بازگردند.



1.گوشی‌های سوخته (Burner Phones)؛ ارتباطات

یک‌بارمصرف استفاده از گوشی‌های هوشمند و خطوط اصلی برای هماهنگی میدانی، به معنای خودکشی امنیتی است. راهکار جایگزین، تهیه گوشی‌های ساده (دکمه‌ای) و ارزان‌قیمت با سیم‌کارت‌های بی‌نام یا ثبت‌شده به نام افراد غیرمرتبط است. این دستگاه‌ها نباید هرگز در خانه روشن شوند. آن‌ها را تنها در مواقع اضطراری، در مکانی دور از خانه و صرفاً برای ارسال یک پیامکِ کدگذاری‌شده (مثلاً: "فردا برای خرید کتاب می‌آیم") روشن کنید. بلافاصله پس از ارسال پیام، گوشی باید خاموش شده و باتری آن خارج شود تا امکان ردیابی موقعیت شما توسط دکل‌های مخابراتی به صفر برسد.

2.شب‌نامه و تراکت‌نویسی دوزبانه (عربی/فارسی)

رسانه‌های کاغذی در قلب خاموشی دیجیتال در اهواز، توزیع شبانه و مویرگیِ تراکت‌های چاپِ خانگی، شریان اطلاع‌رسانی را زنده نگه می‌دارد.

این برگه‌ها باید در ساعات تاریک در صندوق‌های پستی یا زیر درِ منازل توزیع شوند. پوشیدن دستکش نخی (برای جلوگیری از ثبت اثر انگشت روی کاغذ) و پوشاندن کامل چهره (برای استتار در برابر دوربین‌های مداربسته شهری و خانگی) یک قانون تخطی‌ناپذیر است.

3.گرافیتی‌های نشان‌دار؛ زبان خیابان‌ها

دیوارنویسی در این مرحله، از نوشتن شعارهای طولانی به ثبتِ «نشانه‌های بصری» تغییر ماهیت می‌دهد. با استفاده از شابلون و یک اسپری رنگ، می‌توانید نمادهای اعتراضی را در سطح شهر حک کنید.

4. شبکه قاصدان انسانی؛ انتقال فیزیکی داده‌ها

انتقال پیام‌های بسیار حساس یا فایل‌های ویدئویی مستند از اعتراضات، باید از طریق افرادِ امین انجام شود.

استفاده از گروه‌هایی که کمتر در رادار امنیتی هستند و سوءظن ایجاد نمی‌کنند (مانند افراد مسن یا نوجوانان) بهترین گزینه است. این قاصدها می‌توانند پیام‌های شفاهی یا فلش‌مموری‌های رمزنگاری‌شده (با نرم‌افزارهایی نظیر VeraCrypt که در صورت دستگیری



سخن پایانی

دستگاه سرکوب می‌پندارد که با کشیدن دوشاخه اینترنت و خاموش کردن دکل‌های مخابراتی، قادر است صدای یک جامعه را در گلو خفه کند؛ اما تجربه نشان داده است که یک شبکه آگاه و آموزش‌دیده، همواره مسیر خود را از میان موانع پیدا خواهد کرد.
تلفیق هوشمندانه فناوری‌های نوین (همچون ارتباطات آفلاین با اپلیکیشن بریر و پنهان‌نگاری با نهفت) در کنار بازگشت استراتژیک به تاکتیک‌های کلاسیک و کاغذی، این تضمین را ایجاد می‌کند که کنشگران اهوازی همواره یک قدم از سیستم‌های نظارتی جلوتر حرکت کنند. ارتباطات امن، برنده‌ترین سلاح ماست؛ سلاحی که حتی در تاریک‌ترین روزها نیز بر زمین گذاشته نخواهد شد.



صـــدای امن

Secure Voice

cs.khro.org
info@khro.org