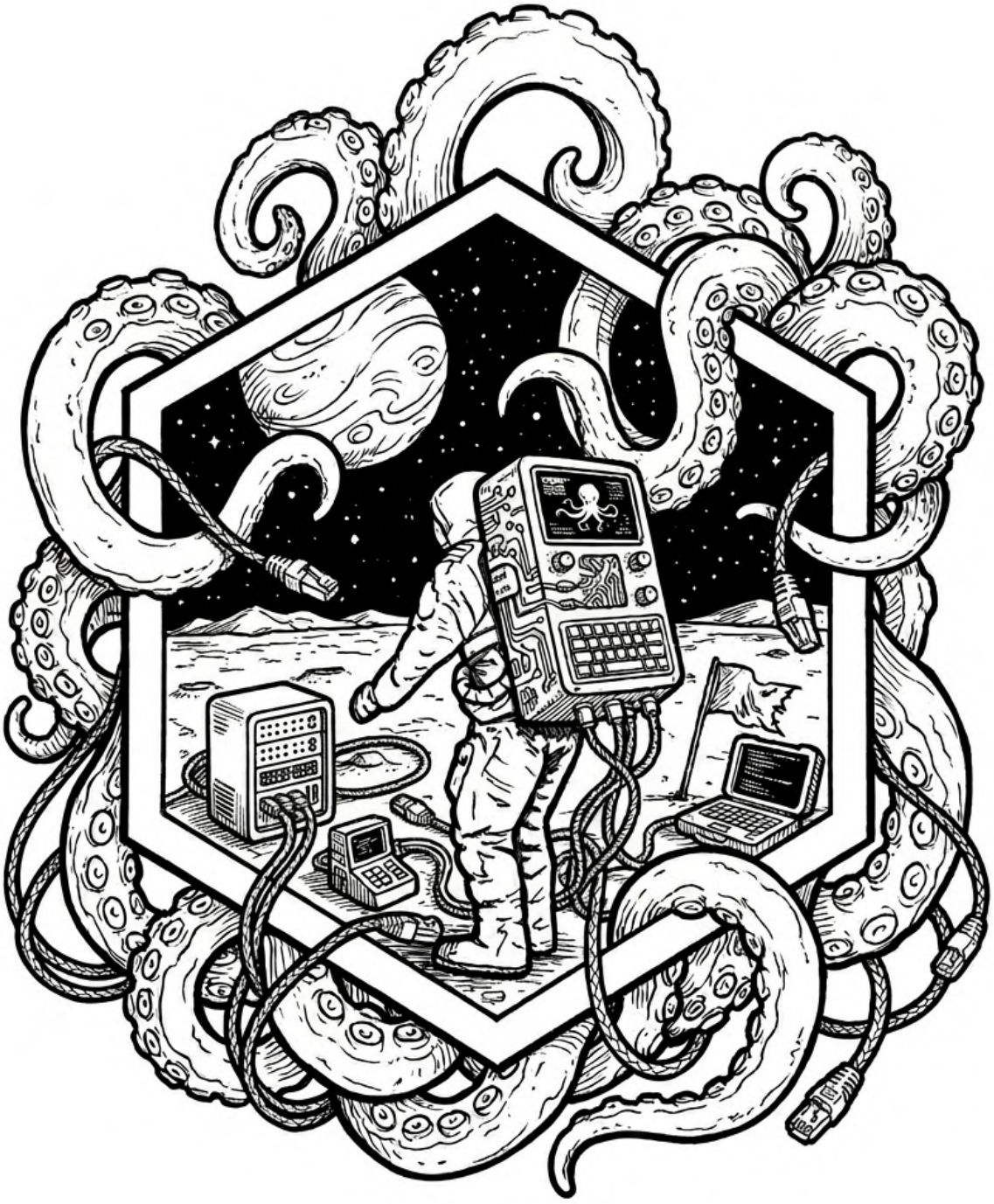
IL SERVER CHIAMATO "PARANOIA"



DIFENDERE AUTISTICI/INVENTATI PRIMA DEL 25 SETTEMBRE 2026

Da venticinque anni, un collettivo di hacker italiani sta costruendo un'infrastruttura comunicativa progettata per resistere alla censura, alla sorveglianza e alle retate della polizia. Il 26 agosto, gli Stati Uniti l'hanno designata come organizzazione terroristica. Il periodo di liquidazione termina il 25 settembre.

Testo originale in inglese di

Sabot Media

https://sabotmedia.noblogs.org

Traduzione a cura di

The BlackWave Collective

blackwave.noblogs.org

Avrebbe dovuto essere una notte buia e tempestosa in un hacklab italiano.
Invece, con grande fastidio, era una bellissima domenica soleggiata.

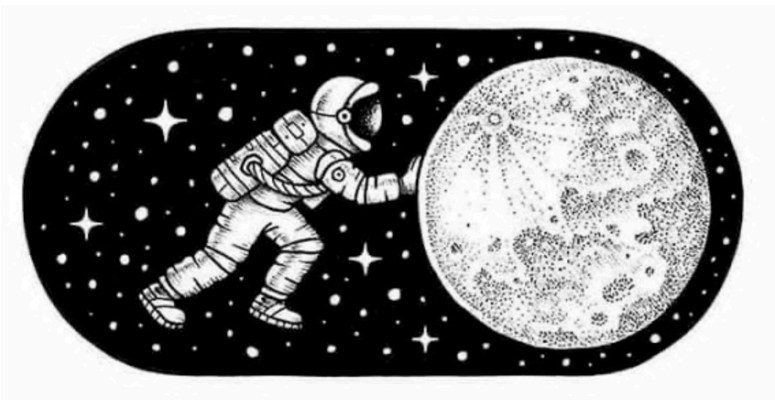
Il 3 marzo 2001, una decina di persone si riunirono all'hacklab LOA di Milano attorno a un computer assemblato con componenti di scarto. Una banca aveva venduto loro un vecchio server al prezzo simbolico di 15.000 lire, circa otto dollari. Lo ampliarono con componenti di recupero, tra cui un disco rigido prelevato dal computer di casa di qualcuno. Nessuno arrivò con un progetto formale. I pacchetti software venivano valutati uno alla volta. Ogni decisione veniva discussa finché tutti non erano d'accordo. Di proposito, la persona con meno esperienza tecnica veniva messa alla tastiera. Il processo richiese molto più tempo del necessario perché l'efficienza non era l'unico obiettivo. Tutti dovevano capire cosa stavano costruendo. Quel giorno, come ricordò in seguito uno dei partecipanti, fu quando dichiararono: «L'A/I ora esiste».

Chiamarono la macchina Paranoia. Il mese successivo entrò in rete, ospitando due domini e due storie intrecciate: Autistici.org e Inventati.org. Venticinque anni dopo, il 26 agosto 2026, gli Stati Uniti designarono Autistici/Inventati come «Organizzazione terroristica globale appositamente designata» e la inserirono nella lista delle «Persone particolarmente pericolose e bloccate».

La distanza tra questi due eventi — da un computer riciclato in un hacklab milanese all'apparato dello Stato americano di sicurezza nazionale — è la storia di un collettivo che ha trascorso un quarto di secolo a sostenere con forza una tesi pericolosa:

Le persone dovrebbero poter comunicare senza doversi prima sottomettere alle multinazionali o ai governi.

La minaccia immediata ora ha una data. Il 25 settembre scade l'autorizzazione temporanea concessa dagli Stati Uniti alle istituzioni per interrompere i propri rapporti con A/I. Banche, aziende tecnologiche, provider di hosting e altre istituzioni stanno ricevendo l'ordine di recidere ciò che resta. A/I ha costruito la propria infrastruttura per sopravvivere alla scomparsa di un server. Gli Stati Uniti stanno ora tentando di rendere il collettivo economicamente e tecnologicamente intoccabile. Unitevi a noi per esplorare cos'è A/I, la sua storia e cosa potrebbe significare questo nuovo attacco per il collettivo tecnologico autonomo e per la più ampia comunità radicale.



PRIMA DI A/I: L'INTERNET UNDERGROUND ITALIANO

Autistici/Inventati non è nato dal nulla. Le sue radici affondano in oltre un decennio di organizzazione autonoma italiana, radio pirata, BBS (bulletin board system), centri sociali occupati, movimenti anticapitalisti e sperimentazione con i computer come strumenti politici. Negli anni '90, reti come l'European Counter Network e Isole nella Rete fornivano spazi online ai movimenti sociali, quando Internet era ancora sconosciuto a gran parte del pubblico. Gli Hackmeeting italiani riunivano programmatori, attivisti, artisti e curiosi di tecnologia all'interno di spazi autogestiti. Gli hacklab sorsero nei centri sociali occupati, dove le persone potevano conoscere e imparare ad utilizzare Linux, a costruire reti e a considerare la conoscenza tecnica come qualcosa da condividere piuttosto che da vendere. I futuri membri di A/I provenivano da diverse parti di questo mondo. A Milano, le persone legate all'hacklab LOA usavano il nome **Autistici** per descrivere il loro intenso fascino per la tecnologia e il desiderio di smascherare le dinamiche politiche nascoste al suo interno. A Firenze, il progetto **Inventati** era più orientato alla comunicazione, all'editoria e all'organizzazione dei movimenti. Tra i suoi progetti figuravano *Stampa* , un giornale pensato per essere affisso direttamente sui muri della città, e *Spia la Spia*, un'iniziativa volta a mappare le telecamere di sorveglianza nei luoghi pubblici.

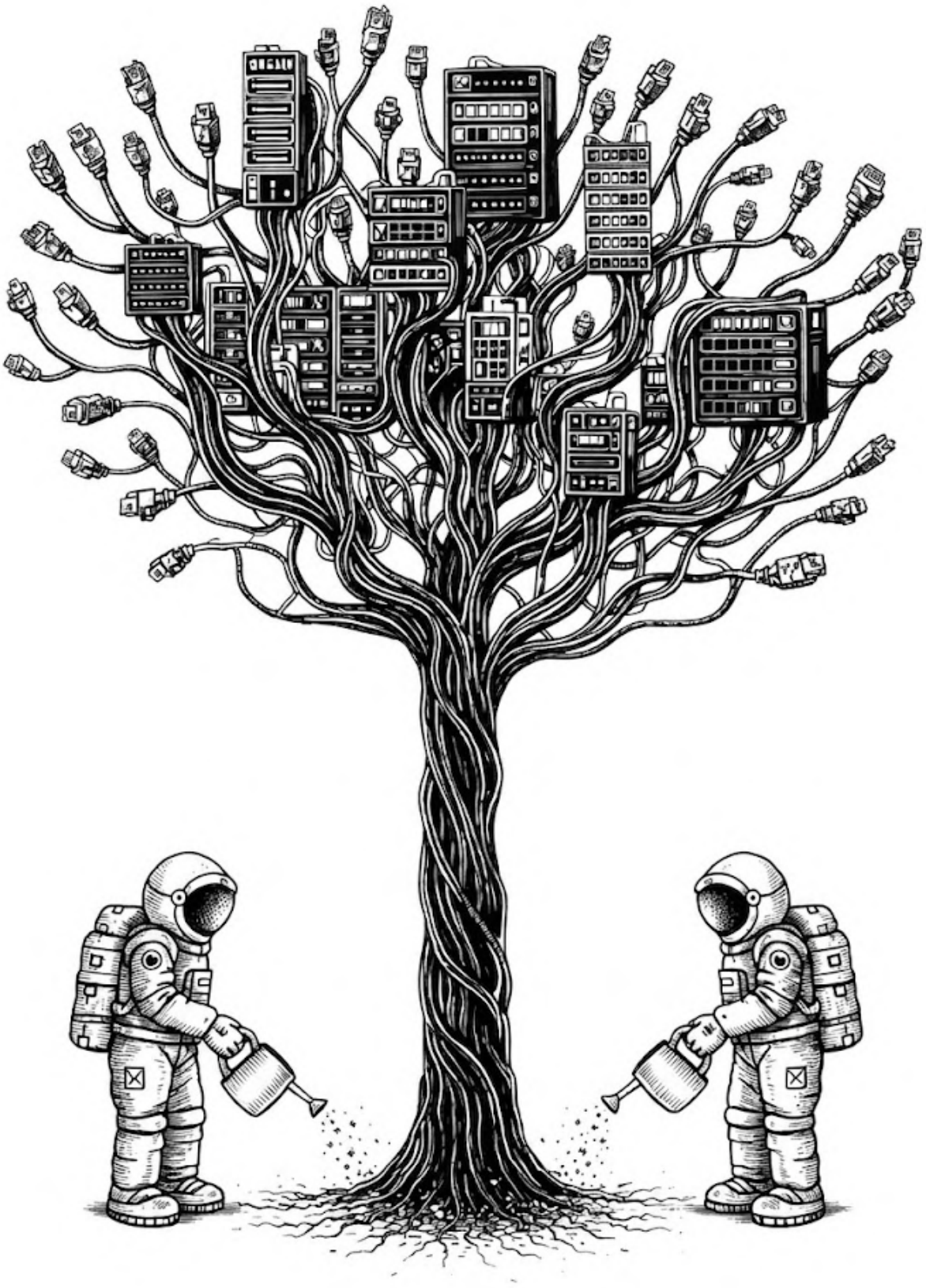
Erano coinvolte anche persone provenienti da Bologna e da altre località. Molti hanno partecipato allo sviluppo iniziale di Indymedia Italia, parte della rete internazionale di editoria aperta che consentiva ai manifestanti e ai semplici partecipanti di riferire sugli eventi senza dover attendere che fossero i giornalisti professionisti a mediare tali informazioni. I diversi gruppi condividevano un problema comune: i movimenti avevano sempre più bisogno di siti web, mailing list e posta elettronica privata, ma le infrastrutture indipendenti rimanevano scarse. L'esistente European Counter Network stava sostenendo un carico eccessivo. I provider commerciali offrivano una maggiore capacità, ma il prezzo da pagare era il denaro, la dipendenza, la sorveglianza e l'eventuale censura. Nel novembre 2000, Inventati inviò agli hacker milanesi un'e-mail crittografata chiedendo un incontro. Il messaggio fu gestito come se fosse tratto da un film di spionaggio amatoriale: chiavi PGP, istruzioni di riconoscimento accuratamente predisposte, un'ora e un luogo segreti. Poi i fiorentini arrivarono con due ore di ritardo a bordo di una leggendaria carretta arrugginita chiamata Generale Lee, suonando il clacson davanti allo squat mentre la polizia che sorvegliava l'edificio osservava sconcertata.

Il fatto storico concordato è che alla fine tutti mangiarono in una pizzeria chiamata La Balena. Durante la cena, i fiorentini rivelarono il loro piano, ritenuto sedizioso:

Costruire un altro server autonomo.

L'intenzione non era quella di sostituire l'infrastruttura esistente del movimento con un nuovo provider centrale. Era quella di moltiplicarla. Se ci fossero state migliaia di server autonomi, ragionavano, nessuna singola retata o sequestro avrebbe potuto interrompere le comunicazioni di tutti. Autistici fornì gran parte delle conoscenze tecniche. Inventati apportò la propria esperienza nell'editoria, nel lavoro culturale e nella comunicazione del movimento. Insieme divennero Autistici/Inventati, solitamente abbreviato in A/I.

L’associazione legale del collettivo si chiamava Investici, ma A/I non divenne mai un’organizzazione convenzionale. Non aveva un coordinatore, un leader ufficiale o un portavoce permanente. Le decisioni venivano prese collettivamente piuttosto che a maggioranza. Nessuno veniva pagato. Le sue risorse provenivano da donazioni volontarie, eventi di beneficenza e dal lavoro delle persone che lo gestivano. Il doppio nome era intenzionale. A/I era una creatura dal volto di Giano: un volto tecnico, l’altro comunicativo; uno rivolto verso la macchina, l’altro verso i movimenti che ne avevano bisogno.



IL SERVER CHE SI È ESCLUSO DA SOLO

La nascita non è stata del tutto gloriosa. Il secondo giorno di vita di Paranoia, qualcuno ha inserito un comando firewall invertito e ha accidentalmente ordinato alla macchina di respingere ogni connessione che non provenisse da se stessa.

Il server poteva comunicare solo con se stesso.

Il collettivo ha ritenuto che questo fosse talmente in linea con gli ideali del gruppo da stampare l'errore su una maglietta. Quella combinazione di serietà tecnica e rifiuto dell'autocompiacimento è diventata parte integrante del carattere di A/I. I server successivi hanno ricevuto nomi quali Chernobyl, Astio — «Rancore» — Rivolta, Contumacia e Latitanza: Rivolta, Contumacia e Vita in fuga. Dietro alle battute si celava una posizione politica ben definita. La comunicazione dovrebbe essere libera e accessibile. La conoscenza cresce attraverso la condivisione. Il software non è neutrale semplicemente perché opera in un mondo apparentemente virtuale. I sistemi attraverso i quali le persone parlano determinano chi può parlare, chi può ascoltare, chi possiede la registrazione e chi può essere messo a tacere. A/I iniziò a fornire siti web, posta elettronica privata, mailing list, newsletter e chat. I suoi servizi si ampliarono fino a includere Noblog, condivisione di file, conferenze audio e video, streaming, remailing anonimo e altri strumenti di comunicazione — il tutto senza pubblicità né estrazione di dati a fini commerciali.

Il suo manifesto descrive il progetto in termini esplicitamente politici. A/I è antifascista, anticapitalista e antimilitarista. Promuove il software libero, la crittografia, lo pseudonimato e la circolazione indipendente della conoscenza e delle opere culturali. Riserva le sue risorse limitate, gestite da volontari, a persone e progetti ampiamente compatibili con tali principi, piuttosto che ad aziende, partiti politici, religioni organizzate o istituzioni che già dispongono dei mezzi per farsi sentire. A/I non è mai stato un host commerciale politicamente neutrale. Ma fornire un'infrastruttura non equivale a redigere tutto ciò che viene trasmesso attraverso di essa. L'affinità politica non è controllo operativo. Fornire a qualcuno un account di posta elettronica non significa scrivere ogni messaggio che invierà in seguito. Questa distinzione è centrale nell'attacco che ora le viene sferrato.

GENOVA: L'INFRASTRUTTURA SOTTO TIRO

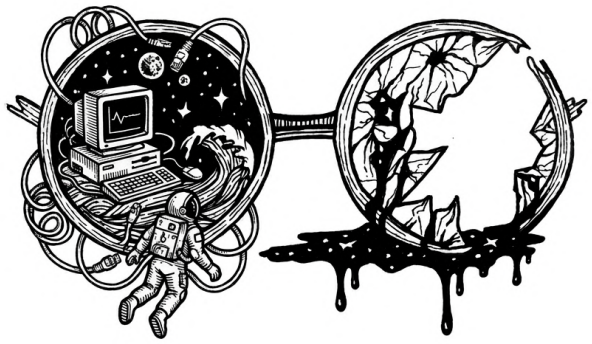
A pochi mesi dalla messa online di Paranoia, il G8 arrivò a Genova. Molti partecipanti di A/I erano coinvolti anche con Indymedia Italia. Aiutarono a costruire il centro media del movimento, posando cavi, configurando server e allestendo postazioni di lavoro attraverso le quali i manifestanti potevano riferire ciò che stava accadendo in tutta la città. Ciò che seguì fu storico: manifestazioni enormi, l'uccisione di Carlo Giuliani da parte della polizia, percosse indiscriminate per le strade, torture e abusi all'interno della caserma di Bolzaneto e il raid notturno alla scuola Diaz. Le narrazioni ufficiali si scontrarono con fotografie, registrazioni e testimonianze di prima mano trasmesse attraverso infrastrutture indipendenti. Genova divenne una delle prime grandi manifestazioni ad essere documentata da quasi ogni angolazione dai suoi partecipanti, piuttosto che esclusivamente attraverso i media istituzionali.

Per A/I, fu anche ciò che il collettivo definì in seguito una «comunione traumatica». I suoi membri vissero insieme la stessa violenza, mantenendo al contempo in funzione i sistemi attraverso i quali le prove di quella violenza potevano trapelare. Dopo Genova, A/I non era più solo un interessante esperimento tecnico. Era diventata un'infrastruttura affidabile per il movimento. La domanda crebbe rapidamente. Nel 2003, A/I ospitava più di 2.000 utenti, 205 siti web e 269 liste di discussione. Ospitare quei servizi gratuitamente stava diventando insostenibile, mentre l'hosting commerciale sarebbe costato migliaia di euro all'anno. Il collettivo rispose con i tour KAOS: incontri itineranti che combinavano eventi di raccolta fondi, feste, dibattiti pubblici e workshop pratici. I membri di A/I insegnavano alle persone come configurare i server, crittografare le comunicazioni, montare e distribuire video, creare archivi digitali e trasmettere audio in streaming.

I tour raccoglievano fondi, ma il loro scopo più profondo era l'educazione politica. Il collettivo non voleva diventare un gruppo di esperti invisibili che compivano magie per utenti passivi. Voleva che la comunità comprendesse i meccanismi da cui dipendeva sempre di più.

Ogni successivo attacco contro A/I avrebbe prodotto una variante di questa risposta:

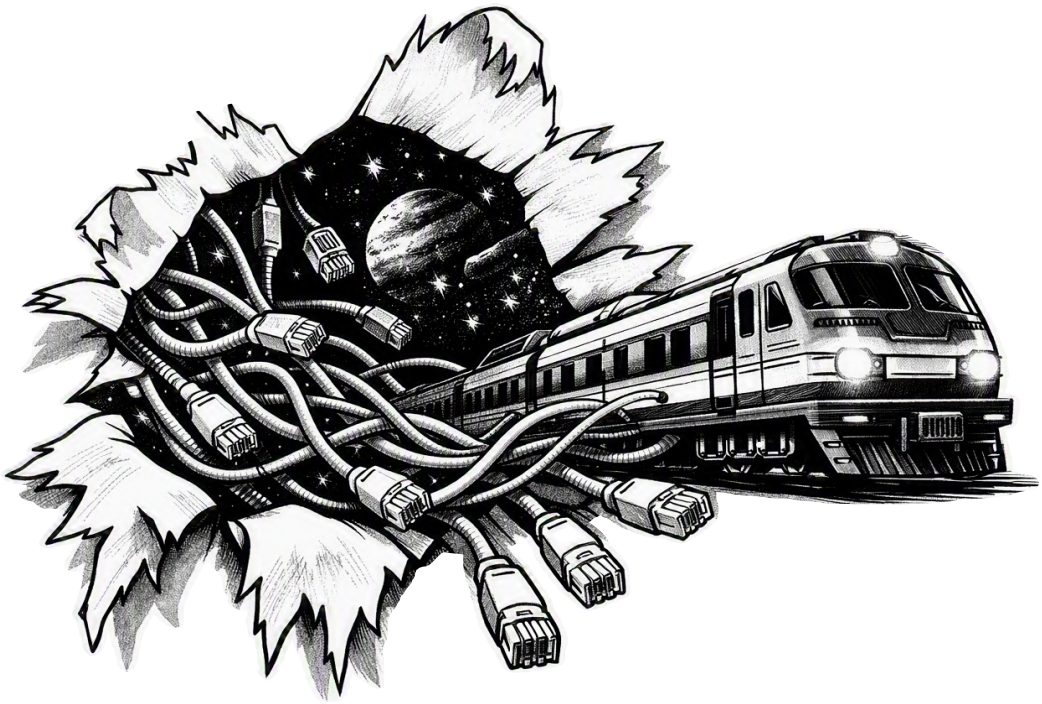
Diffondere ciò che è accaduto. Riparare il danno. Condividere la lezione appresa. Costruire qualcosa che sia più difficile da distruggere.



TRENITALIA SCOPRE L'EFFETTO STREISAND

Il primo grande scontro legale di A/I risale al 2004. Un collettivo di designer chiamato Zenmai aveva creato un sito web che parodiava la compagnia ferroviaria italiana Trenitalia. Il sito riproduceva l'aspetto del sito ufficiale dell'azienda, denunciando al contempo il coinvolgimento di Trenitalia nel trasporto di carri armati e altre forniture militari durante l'invasione dell'Iraq. Trenitalia chiese la rimozione della pagina, il risarcimento dei danni e la pubblicazione di avvisi su due importanti quotidiani, con un costo stimato di circa 20.000 euro. Inizialmente un tribunale ordinò ad A/I di rimuovere la parodia. Il web reagì riproducendola ovunque.

Trenitalia chiese quindi ad A/I di rimuovere anche i link alle pagine mirror — un'argomentazione che sollevava l'assurda possibilità che il semplice collegamento a materiale contestato potesse rendere qualsiasi motore di ricerca responsabile di esso. A/I presentò ricorso. Il 14 settembre 2004, il tribunale stabilì che il sito web rappresentava una satira protetta, fondata su una controversia fattuale. La pagina tornò online e a Trenitalia fu ordinato di pagare le spese legali di A/I. Fu una vittoria straordinaria per un piccolo collettivo di volontari. Ma mentre A/I combatteva la censura palese in tribunale, un'operazione più pericolosa era in atto a sua insaputa.

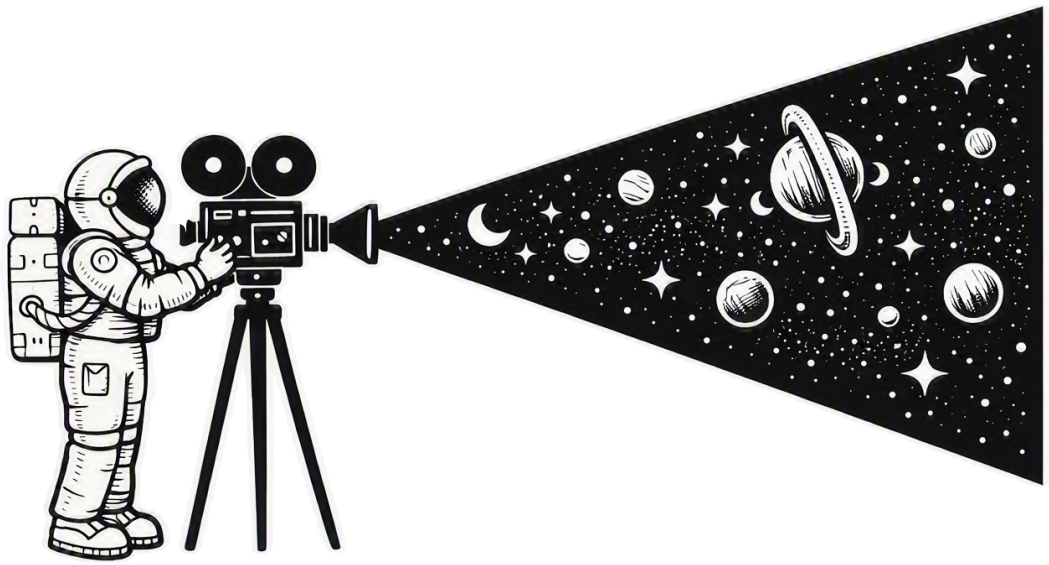


IL GIRO DI VITE CONTRO ARUBA

A quel tempo, il server di A/I era ospitato presso il provider commerciale Aruba ad Arezzo. Il 15 giugno 2004, la polizia italiana si presentò presso Aruba su ordine di un pubblico ministero di Bologna. I tecnici dell'azienda spensero il server di A/I e permisero alla polizia di copiare il materiale dai suoi dischi. Gli investigatori ottennero i certificati crittografici e probabilmente installarono apparecchiature in grado di intercettare il traffico. Ad A/I fu detto che l'interruzione era dovuta a un problema elettrico. Il collettivo scoprì la verità quasi un anno dopo, e solo per caso.

Nel maggio 2005, ad A/I fu ordinato di chiudere la casella di posta utilizzata dalla Croce Nera Anarchica italiana, nel corso di un'indagine su vasta scala che riguardava accuse di associazione a delinquere e sovversione anarchica. A/I ottemperò all'ordinanza del tribunale e richiese i documenti relativi al caso. Tali documenti contenevano messaggi che gli investigatori non avrebbero dovuto possedere. Nascosta in una nota a piè di pagina c'era la spiegazione: la polizia si era recata ad Aruba l'anno precedente e aveva ottenuto l'accesso al server di A/I. Un'operazione apparentemente incentrata su una sola casella di posta aveva potenzialmente compromesso migliaia di account e decine di migliaia di iscritti alle mailing list. Tra le persone coinvolte c'erano avvocati ed esperti tecnici che collaboravano con il Forum Legale di Genova. La polizia potrebbe quindi aver avuto accesso a comunicazioni riservate della difesa relative ai procedimenti penali scaturiti dalla condotta della polizia in occasione del G8. La violazione ha messo a nudo una cruda verità. A/I poteva gestire il proprio server, configurarlo con cura e rifiutarsi di conservare i log identificativi, ma la macchina fisica rimaneva nell'edificio di qualcun altro. Un provider commerciale poteva aprire la porta, consegnarne il contenuto e nascondere ciò che era accaduto.

A/I ha rimosso il server di Aruba, lo ha ripulito e ha ripristinato i servizi essenziali. Sono state sollevate interrogazioni parlamentari in Italia e a livello europeo. Il collettivo ha viaggiato in Italia e in Europa per spiegare la violazione. Ma soprattutto, ha ricostruito la rete.



PIANO R*: LA REPRESSIONE DIVENTA ARCHITETTURA

Il risultato è stato il Piano R*, lanciato nell'ottobre 2005: una rete di «comunicazione resistente». Anziché concentrare i servizi di A/I su un'unica macchina, il collettivo distribuì dati crittografati e funzioni su server situati in diversi paesi. I computer esposti al pubblico potevano essere sostituiti. I servizi potevano essere spostati quando l'hardware veniva sequestrato o un provider diventava ostile. La perdita di un nodo non avrebbe più esposto né messo a tacere l'intera comunità. R* significava replica, ridondanza, resistenza e altre parole che iniziano con la R. La sua architettura era concepita non solo per sopravvivere a guasti meccanici, ma anche per resistere ad attacchi politici. A/I non affermava di poter garantire una totale sicurezza. Al contrario, avvertiva ripetutamente gli utenti di non affidare mai ciecamente la propria sicurezza a nessun provider, compreso A/I. Riduceva al minimo i log e le informazioni identificative perché ciò che non esiste non può essere facilmente sequestrato. Incoraggiava gli utenti a crittografare le proprie comunicazioni perché nemmeno l'architettura server più robusta poteva sopperire a pratiche individuali non sicure.

Il collettivo trasformò un'operazione di sorveglianza segreta in una lezione di infrastruttura.

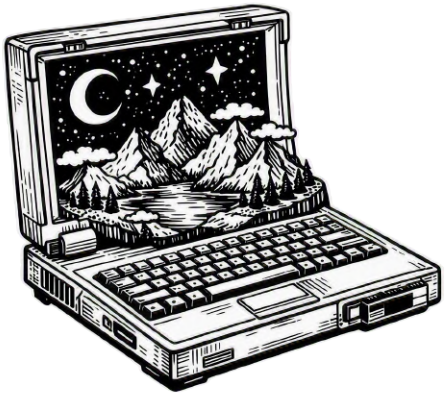
La repressione divenne architettura.

IL VATICANO, UN VIDEOGIOCO SATIRICO E LA NORVEGIA

La pressione continuò. Nel 2007, un politico italiano chiese che si intervenisse contro Operation: Pedopriest, un gioco satirico per browser che criticava gli sforzi della Chiesa cattolica per nascondere gli abusi sessuali commessi dal clero. Il suo creatore rimosse temporaneamente il gioco per proteggere il provider di hosting. A/I ne ospitò quindi una copia. A seguito di una denuncia da parte di un'organizzazione per la tutela dei minori non identificata, un provider americano disconnesse l'intero server di Noblogs. Dopo aver consultato i propri legali, il provider concluse che la satira era legale negli Stati Uniti e ripristinò il server. Il Piano R* mantenne accessibile altrove il materiale contestato e limitò l'interruzione su più ampia scala. A quel punto, A/I era diventato un importante rifugio dal nascente social web commerciale. Noblogs offriva la possibilità di pubblicare in modo indipendente senza pubblicità, data mining o l'obbligo per gli utenti di associare la propria identità legale a tutto ciò che dicevano.Tra i suoi utenti figuravano organizzazioni di movimento, scrittori indipendenti, dissidenti, artisti e operatori di ONG che operavano in contesti pericolosi. Nel 2008, A/I ricevette il premio italiano «Eroe della Privacy» Winston Smith per aver creato un'infrastruttura di comunicazione libera e resistente alla censura, nonostante le scarse risorse, gli attacchi tecnici e i ripetuti interventi giudiziari. Poi, il 6 novembre 2010, la polizia norvegese ha copiato i dischi rigidi di un server di A/I su richiesta dell'Italia. L'indagine aveva avuto origine da minacce e graffiti antifascisti rivolti ai membri dell'organizzazione neofascista CasaPound. Le autorità cercavano informazioni relative a una casella di posta elettronica. A/I aveva già spiegato di non possedere né le identità degli abbonati né i registri delle attività, ma a quanto pare gli investigatori volevano accertarsi che fosse vero.

Nel corso dell'operazione sono stati copiati migliaia di account.

Plan R* ha ripristinato i servizi interessati altrove nel giro di circa due ore. Entro ventiquattro ore, la rete funzionava normalmente. I dischi sequestrati erano crittografati e non hanno fornito alcuna informazione utile all'identificazione. L'operazione è diventata uno scandalo pubblico in Norvegia. Avvocati, giornalisti e organizzazioni tecnologiche hanno contestato il motivo per cui la polizia norvegese avesse copiato le comunicazioni private di migliaia di persone in risposta a una richiesta straniera spiegata in modo inadeguato. L'indagine italiana alla base dell'operazione fu infine archiviata. Laddove un'altra organizzazione avrebbe potuto interpretare le ripetute irruzioni come prova dell'impossibilità del proprio progetto, A/I le interpretò come conferma della sua necessità. La sua storia è documentata nel libro del collettivo, +KAOS: Ten Years of Hacking and Media Activism, e nella sua stessa storia del collettivo.



26 AGOSTO 2026

L'ultimo attacco è di tutt'altro ordine. Il 26 agosto, il Dipartimento di Stato degli Stati Uniti ha designato Autistici/Inventati come «Specially Designated Global Terrorist» (SDGT) [associazione terroristica di pericolo globale]. Contemporaneamente, l'Ufficio per il Controllo dei Beni Stranieri (OFAC) del Dipartimento del Tesoro ha inserito A/I nell'elenco dei «Specially Designated Nationals and Blocked Persons» (SDN) [persone straniere considerate di pericolo pubblico] ai sensi dell'Ordine Esecutivo 13224. Non si tratta semplicemente di una dichiarazione di condanna da parte del governo. Si attiva così uno dei sistemi di esclusione economica più potenti al mondo. Gli Stati Uniti sostengono che A/I fornisca architetture digitali specializzate, comunicazioni criptate e servizi di hosting a gruppi antifascisti e altri movimenti radicali, comprese organizzazioni già designate dagli Stati Uniti.

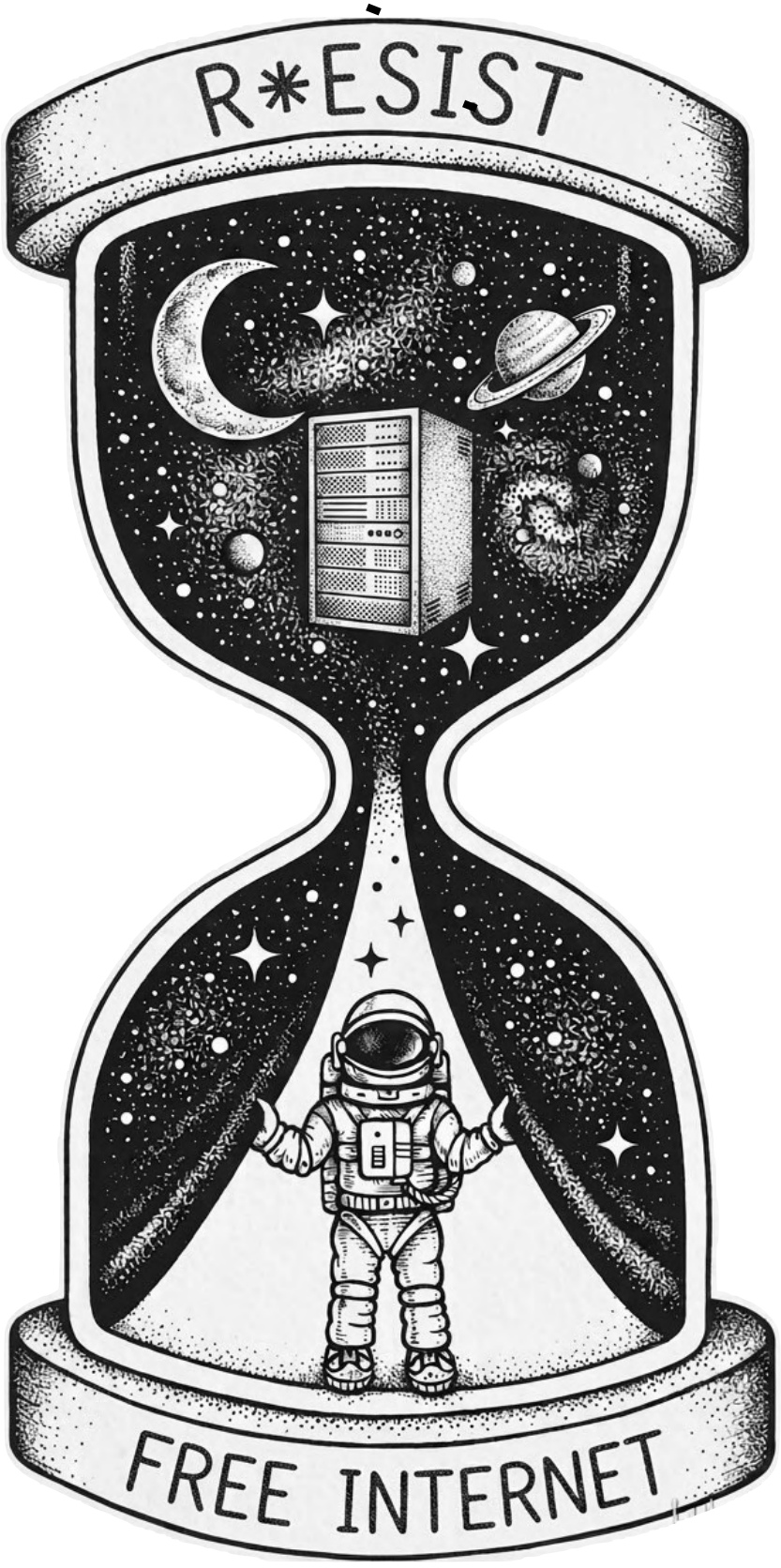
L'annuncio pubblico del Tesoro si concentra sui servizi forniti da A/I: siti web ospitati all'estero, posta elettronica crittografata, chat, videoconferenze e l'architettura digitale a supporto di Noblogs. Descrive l'orientamento politico antifascista e antimilitarista di A/I, la sua prassi di selezionare progetti compatibili con tale orientamento e la fornitura di infrastrutture utilizzate dal PKK. Il Tesoro considera quindi la fornitura di tali infrastrutture come un sostegno materiale o tecnologico al terrorismo. (Annuncio del Tesoro degli Stati Uniti) Il fascicolo di accompagnamento del Dipartimento di Stato va oltre, presentando attacchi, comunicati e pubblicazioni che, secondo quanto affermato, sarebbero transitati attraverso l'infrastruttura di A/I. Tra gli esempi citati figurano presunti sabotaggi a ferrovie e oleodotti in Europa, attacchi alle infrastrutture energetiche, Rose City Antifa, la resistenza al progetto di centro di addestramento della polizia ad Atlanta, Jane's Revenge e pubblicazioni contenenti dichiarazioni attribuite a organizzazioni armate. (Designazione del Dipartimento di Stato) Le dichiarazioni pubbliche del governo non dimostrano che A/I abbia pianificato tali azioni, selezionato gli obiettivi, trasferito armi, diretto i gruppi citati o redatto il materiale ospitato sui propri sistemi. Non stabiliscono quando A/I sia venuta a conoscenza di un atto specifico né se ne fosse a conoscenza prima che avvenisse.

La designazione avanza invece una tesi più ampia e dalle conseguenze più gravi:

La creazione di infrastrutture di comunicazione per movimenti radicali può essere di per sé considerata un atto di terrorismo.

Tale teoria annulla la distinzione tra fornitore e utente; tra affinità politica e controllo operativo; tra tutela della privacy e occultamento di un reato; tra la gestione di una piattaforma di pubblicazione e la paternità di tutto ciò che vi viene pubblicato. A/I non ha mai affermato di essere politicamente neutrale. Ha costruito l'infrastruttura proprio perché

i movimenti radicali avevano bisogno di uno spazio dove esprimersi, pubblicare e organizzarsi al di fuori del controllo delle aziende e dello Stato. Gli Stati Uniti stanno ora utilizzando proprio tale scopo come prova a suo carico.



COSA È SUCCESSO IL 25 SETTEMBRE 2026

Poiché A/I figura ora nell'elenco SDN, tutti i suoi beni o partecipazioni in beni situati negli Stati Uniti — o posseduti o controllati da un soggetto statunitense — devono essere congelati e segnalati all'OFAC. Salvo in caso di esenzione o licenza, ai soggetti e alle istituzioni statunitensi è generalmente vietato fornire o ricevere fondi, beni o servizi che coinvolgano A/I. Le restrizioni possono riguardare anche le transazioni che transitano attraverso gli Stati Uniti, anche quando le parti hanno sede altrove. L'OFAC ha rilasciato una licenza temporanea che consente le transazioni normalmente necessarie per liquidare i rapporti esistenti con A/I fino alle 00:01 (ora della costa orientale) del 25 settembre 2026. I pagamenti dovuti al collettivo non possono essere semplicemente versati a favore dello stesso; devono essere depositati su conti bloccati. Dopo la scadenza, le transazioni soggette a restrizioni richiedono un'altra autorizzazione applicabile. Il 25 settembre è quindi la data entro la quale le aziende e i cittadini statunitensi sono tenuti a separarsi da A/I.

- Le conseguenze possono includere la perdita di:
- Conti bancari e servizi di elaborazione dei pagamenti.
- Donazioni e servizi di raccolta fondi collegati agli Stati Uniti.
- Servizi di hosting, infrastruttura cloud e servizi di rete a monte.
- Registrazione dei domini e servizi tecnici correlati.
- Certificati, sicurezza e account per la consegna della posta elettronica.
- Software e servizi di comunicazione.
- Rapporti con fornitori non statunitensi spaventati dalle sanzioni secondarie americane.
- Accesso per le persone negli Stati Uniti che attualmente utilizzano i servizi di A/I.

Le società straniere non sono automaticamente soggette a tutti i divieti imposti ai cittadini statunitensi. Tuttavia, l'OFAC avverte che gli istituti finanziari stranieri possono andare incontro a sanzioni secondarie qualora facilitino consapevolmente transazioni significative per conto di soggetti designati. Tale avvertimento può causare danni pari a quelli di un'applicazione diretta della legge. Una banca, un registro o un'azienda di hosting europea potrebbe non sapere con precisione cosa le richieda la legge statunitense. Il suo dipartimento di conformità potrebbe semplicemente decidere che mantenere un rapporto con un piccolo collettivo anarchico italiano non valga il rischio percepito. Spesso le istituzioni adottano misure di conformità eccessive. I fornitori possono chiudere conti o revocare infrastrutture anche quando la legge non lo impone chiaramente. Le organizzazioni possono rimuovere link, evitare corrispondenza o interrompere rapporti non correlati semplicemente perché il nome di A/I compare ora in una lista nera del terrorismo.

È così che le sanzioni statunitensi acquisiscono forza a livello mondiale: non solo attraverso la giurisdizione legale, ma anche attraverso il timore delle istituzioni.

IL BERSAGLIO PRINCIPALE È LA COMUNITA LEGATA AL SERVER

La designazione può essere rivolta ad A/I, ma i suoi effetti non si limiteranno alla collettività. L'infrastruttura di A/I è utilizzata da scrittori, organizzatori, ricercatori, artisti, testate del movimento e persone che l'hanno scelta proprio perché le piattaforme commerciali erano insicure, politicamente ostili o progettate per estrarre i loro dati. Questi utenti non vengono automaticamente sanzionati solo perché hanno un indirizzo A/I o pubblicano su Noblogs. Ma una volta che lo stesso provider viene inserito nella lista nera del terrorismo, la semplice associazione può trasformarsi in un segnale di rischio. Una banca potrebbe sottoporre a scrutinio un pagamento. Un provider di posta elettronica potrebbe ridurre la priorità o bloccare la consegna. Un datore di lavoro, un agente di frontiera o un investigatore potrebbe considerare un indirizzo come sospetto. Un giornalista potrebbe esitare a contattare una fonte. Un ricercatore potrebbe evitare un archivio. Un nuovo utente potrebbe decidere che aprire un account sia troppo pericoloso. Nulla di tutto ciò richiede che il governo persegua penalmente ogni persona coinvolta. La designazione può generare una propria sfera di paura.

Questo è uno dei motivi per cui questa mossa, altrimenti inspiegabile, potrebbe rivelarsi utile allo Stato anche se A/I rimanesse online. Gli attacchi precedenti cercavano di raggiungere la collettività attraverso macchine, caselle di posta e provider specifici. A/I ha risposto distribuendo i propri sistemi, crittografando i propri dischi e conservando meno informazioni. Tali pratiche hanno reso meno efficaci i sequestri e la sorveglianza convenzionali. Le sanzioni colpiscono un livello diverso: le relazioni che consentono all'infrastruttura di esistere. Anziché violare la crittografia, il governo può esercitare pressioni su banche, registrar, centri dati, aziende di software e utenti per isolare le persone che gestiscono il sistema. Anziché dimostrare in tribunale che ogni utente abbia commesso un reato, può rendere il mantenimento dei contatti costoso e giuridicamente incerto.

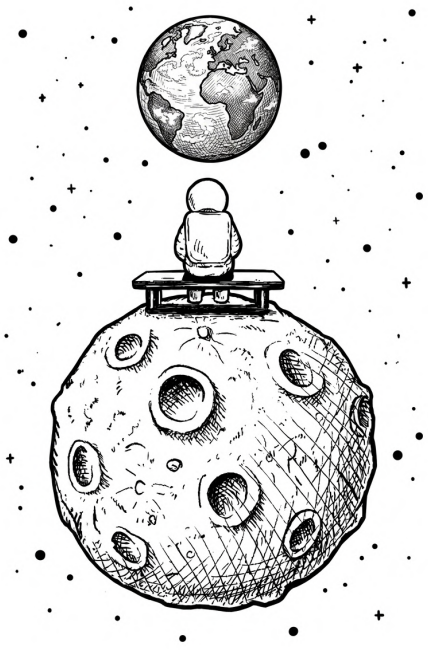
Si tratta del potere dello Stato di sorveglianza che opera attraverso intermediari privati. Il governo non ha bisogno di collocare un funzionario all'interno di ogni sala server quando i dipartimenti di conformità, i gestori dei pagamenti e le piattaforme possono essere indotti a sorvegliare la rete autonomamente. Ogni istituzione traccerà i propri confini difensivi, spesso più ampi di quanto richiesto dalla legge. Alcune potrebbero richiedere più documenti di identità, conservare più registri, monitorare i contenuti politici o rifiutare del tutto i progetti volti a tutelare la privacy. Altre potrebbero chiudere silenziosamente gli account senza offrire alcuna via di ricorso significativa. L'applicazione delle norme si disperde tra aziende le cui decisioni sono difficili da comprendere, contestare o persino documentare.

Il danno che ne deriva non si limita alla censura. Può modificare l'architettura della comunicazione del movimento. I piccoli fornitori autonomi potrebbero giungere alla conclusione che fornire servizi a comunità controverse comporti un rischio esistenziale. Le piattaforme più grandi potrebbero indicare tale designazione come un ulteriore motivo per espandere la verifica dell'identità, la moderazione automatizzata e la conservazione

dei dati. Gli utenti potrebbero migrare dalle infrastrutture fidate del movimento verso sistemi commerciali più facili da monitorare, sottoporre a mandato di comparizione e mappare. Lo Stato acquisisce potere anche quando non ottiene alcun testo in chiaro dai dischi crittografati dell'A/I: le persone si isolano, i fornitori raccolgono più informazioni e le relazioni sociali che circondano il dissenso diventano più facili da osservare.

Il precedente va oltre i progetti esplicitamente anarchici o antifascisti. Se l'allineamento politico con gli utenti, la tutela della privacy e l'hosting di pubblicazioni controverse possono essere assemblati in un caso in cui l'infrastruttura stessa costituisce un sostegno, allora i fornitori di posta crittografata, gli editori radicali, gli archivi comunitari, le VPN, i social network federati, i progetti di assistenza legale e altri host indipendenti hanno tutti motivo di prestare attenzione. I fatti e le leggi specifici variano di caso in caso. Il pericolo sta nella normalizzazione della categoria: un fornitore di servizi di comunicazione non è più considerato un semplice canale o un editore con diritti e responsabilità propri, ma un partecipante a ogni atto che il governo attribuisce a chiunque utilizzi i suoi sistemi.

Ciò non significa che la designazione riguardi segretamente ogni utente di A/I, né che si verificheranno tutte le possibili conseguenze. Il governo non ha spiegato pubblicamente la propria strategia interna al di là delle accuse contenute nei suoi comunicati. Ma la struttura dell'azione è evidente. Sostituisce un'accusa circoscritta contro una condotta identificabile con una sanzione generica contro l'infrastruttura; sposta l'applicazione della legge da un'aula di tribunale a una rete globale di istituzioni caute; e rende l'incertezza stessa uno strumento di controllo. L'obiettivo immediato potrebbe essere quello di impedire l'uso di A/I. L'effetto più ampio è quello di avvertire chiunque sviluppi sistemi di comunicazione al di fuori della supervisione aziendale e statale che il rifugio che essi offrono può essere trasformato in prova contro di loro.



A/I RIUSCIRÀ A SOPRAVVIVERE?

A/I ha visto arrivare la repressione dello Stato da lontano.

La sua intera infrastruttura parte proprio da questo presupposto: che la preparazione sia fondamentale. A/I ha sede in Italia, non negli Stati Uniti. La sua infrastruttura è distribuita a livello internazionale. I suoi servizi sono gestiti da volontari tecnicamente esperti. Evita di dipendere da un unico fornitore, riduce al minimo le informazioni identificative e vanta decenni di esperienza nel ripristino dei servizi durante le emergenze. Non ha azionisti, né sede centrale, né un libro paga convenzionale. I suoi costi operativi relativamente modesti e la struttura basata sul volontariato offrono allo Stato pochi punti di pressione conosciuti. Non c'è motivo di supporre che il sito web, il sistema di posta elettronica o Noblogs scompariranno semplicemente il 25 settembre. A/I potrebbe essere meglio attrezzata per sopravvivere al sequestro o alla disconnessione di una macchina rispetto a quasi qualsiasi altro progetto di comunicazione di dimensioni comparabili.

- I server verranno sequestrati.
- I provider collaboreranno con la polizia.
- I governi richiederanno informazioni sugli utenti.
- Le aziende disattiveranno i contenuti controversi.
- Singoli server e sedi diventeranno inaccessibili.
- I dati e i servizi devono quindi essere crittografati, distribuiti e sostituibili.

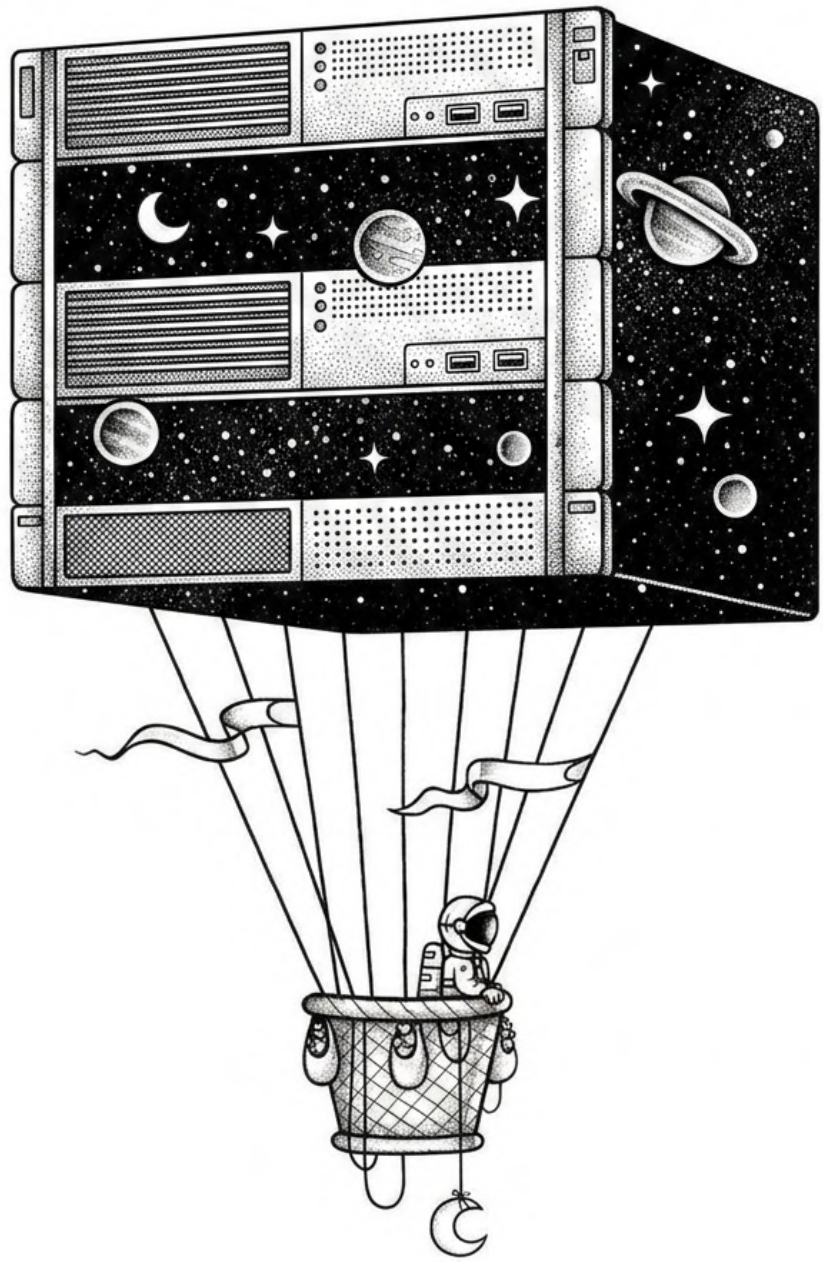
Ma questa non è l'ennesima retata ai server.

Il Piano R* è stato concepito per sopravvivere alla scomparsa dei server. Da solo, non può impedire alle banche di bloccare i fondi, ai registrar di sospendere i domini o alle aziende di tutto il mondo di sospendere i servizi per timore di sanzioni statunitensi.

La designazione prende di mira il tessuto connettivo attorno ai server: A/I è già sopravvissuta all'isolamento tecnico in passato. Gli Stati Uniti stanno ora tentando una scomunica finanziaria e istituzionale. I suoi servizi fondamentali potrebbero essere resilienti. La sua capacità di finanziarli, sostituire le infrastrutture e partecipare al più ampio sistema tecnologico è invece esposta a un rischio notevolmente maggiore. Ciò che accadrà dopo il 25 settembre dipenderà quindi non solo dall'architettura che circonda i dati di A/I, ma dalla solidarietà che circonda A/I stessa.

- Servizi bancari.
- Donazioni.
- Domini.
- Contratti relativi ai data center.
- Larghezza di banda.
- Certificati.
- Dipendenze software.
- Relazioni istituzionali internazionali.

A/I è già sopravvissuta in passato all'isolamento tecnico. Gli Stati Uniti ora stanno tentando l'isolamento finanziario e istituzionale. I suoi servizi fondamentali potrebbero rivelarsi resilienti. La sua capacità di finanziarli, di sostituire le infrastrutture e di partecipare al sistema tecnologico più ampio è invece esposta a un rischio notevolmente maggiore. Ciò che accadrà dopo il 25 settembre dipenderà quindi non solo dall'architettura che circonda i dati di A/I, ma anche dalla solidarietà che circonda A/I stessa.

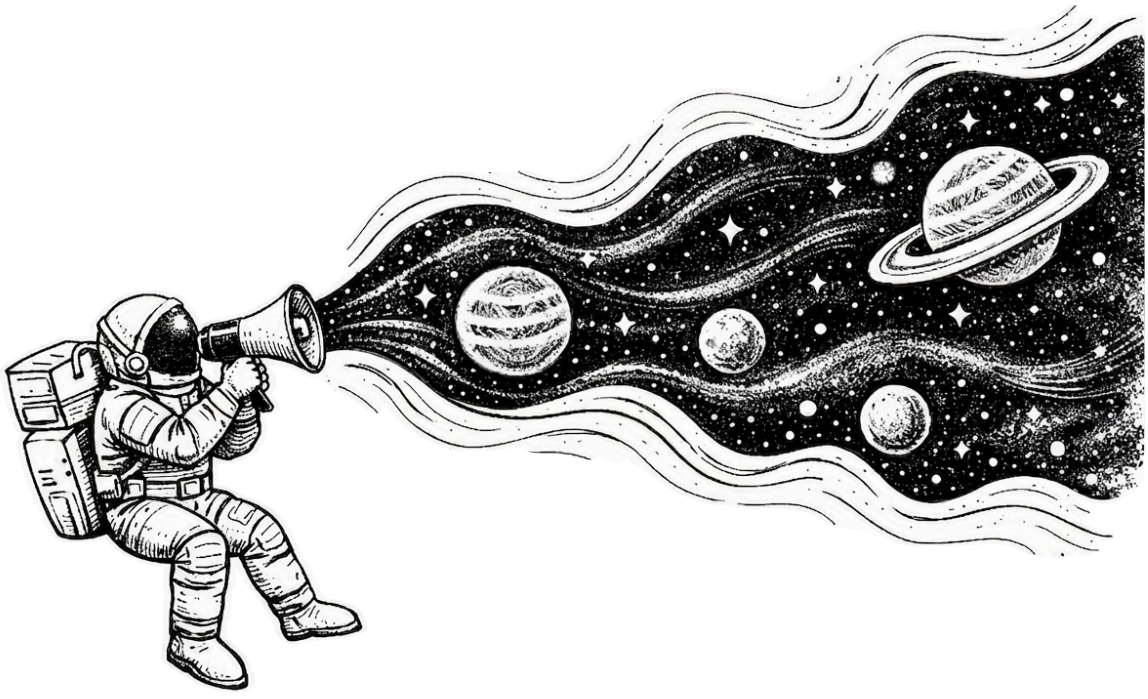


IL 25 SETTEMBRE NON È UNA SCADENZA PER IL SILENZIO

La designazione ha lo scopo di isolare. La risposta deve essere una solidarietà consapevole, indipendente e disciplinata. Chi vive negli Stati Uniti non dovrebbe improvvisare donazioni, mascherare pagamenti o convogliare risorse attraverso un'altra persona, organizzazione, valuta o paese. Ciò potrebbe esporre a sanzioni il sostenitore, l'intermediario e la stessa A/I. I divieti possono estendersi anche oltre il denaro. L'assistenza tecnica coordinata, la traduzione, l'attività di advocacy, l'organizzazione di eventi o altri servizi forniti a un'entità designata possono comportare rischi legali.

Ma il 25 settembre non è una scadenza per il silenzio. Il giornalismo indipendente, la critica, la protesta, l'educazione e l'attività di advocacy politica rimangono possibili. È possibile raccontare la storia di A/I, esaminare e contestare le affermazioni del governo, contattare giornalisti e organizzazioni per le libertà civili, preservare materiali di dominio pubblico e organizzarsi in modo indipendente contro la criminalizzazione delle infrastrutture di comunicazione di resistenza. La distinzione pratica sta tra il parlare e agire in modo indipendente riguardo ad A/I e il fornire fondi o servizi coordinati ad A/I. I confini esatti possono essere complessi. Chiunque stia valutando di raccogliere fondi, sostituire infrastrutture, creare mirroring pubblici o fornire assistenza tecnica diretta dovrebbe rivolgersi a un consulente legale qualificato in materia di sanzioni. Una guida sulle libertà civili del febbraio 2025 relativa al sostegno materiale e alle restrizioni dell'OFAC avverte inoltre che anche attività lecite o protette possono comunque essere oggetto di sorveglianza, indagini, conseguenze in materia di immigrazione o contenziosi civili. I sostenitori avvicinati dalle forze dell'ordine dovrebbero rifiutarsi di rispondere alle domande e rivolgersi a un avvocato.

Questo articolo è un resoconto e un'analisi politica, non una consulenza legale.



COSA POSSONO FARE I SOSTENITORI PRIMA DEL 25 SETTEMBRE

Raccontate la storia. Condividete la storia di A/I: gli hacklab, Paranoia, Genova, i tour KAOS, la vittoria su Trenitalia, la violazione di Aruba, Plan R*, Noblogs e il sequestro norvegese. Non permettete che la descrizione del governo diventi l'unica versione pubblicamente disponibile di ciò che è A/I. **Costruite una coalizione di difesa pubblica.** Chiedete a collettivi di server indipendenti, organizzazioni per i diritti digitali, hacklab, progetti di software libero, biblioteche radicali, editori indipendenti, giornalisti, avvocati, ricercatori ed ex utenti di rispondere pubblicamente. **Preservate l'archivio**. I server possono essere sequestrati. I domini possono essere sospesi. Gli host possono farsi prendere dal panico. Eseguite il backup degli scritti di Noblogs accessibili al pubblico e di valore storico, insieme ai manifesti di A/I, ai documenti tecnici, agli atti legali e alla storia del movimento. Registrate gli URL di origine, la paternità, le date di pubblicazione e quelle di recupero. Rispettate la privacy, il diritto d'autore e le richieste di rimozione. Non accedete ad account privati né aggirate le misure di sicurezza. La conservazione personale, l'archiviazione a fini di ricerca e il giornalismo ordinario non equivalgono alla gestione pubblica di un'infrastruttura sostitutiva; chiunque stia valutando la creazione di un mirror pubblico dovrebbe prima richiedere una consulenza qualificata.

Documentare il rispetto eccessivo delle norme. Registrare le aziende, le banche, i registrar, le piattaforme e le istituzioni che interrompono i servizi o rimuovono materiale. Conservare le notifiche e la corrispondenza. Il registro pubblico dovrebbe mostrare fino a che punto la designazione si estenda oltre il suo linguaggio formale. **Esigere risposte**. Chiedere ai gruppi per i diritti digitali, alle istituzioni europee e ai funzionari pubblici se permetteranno che le sanzioni americane smantellino un collettivo di comunicazione italiano. Chiedere quali protezioni esistano per le infrastrutture, gli utenti e gli archivi europei. **Organizzarsi in modo indipendente**. Promuovere dibattiti pubblici su infrastrutture autonome, sanzioni, sorveglianza e leggi sul sostegno materiale. Pubblicare guide esplicative. Insegnare la crittografia. Sostenere il lavoro indipendente a difesa delle libertà civili che si oppone alle designazioni di terrorismo estese. **Preparare forme di sostegno materiale lecite**. A/I è storicamente sopravvissuta grazie a donazioni volontarie, ma i sostenitori statunitensi non dovrebbero inviare o reindirizzare denaro mentre la designazione è in vigore senza una chiara autorizzazione. Le organizzazioni per i diritti digitali e quelle legali possono indagare in modo indipendente su meccanismi di sostegno leciti, licenze e potenziali procedure di cancellazione dalla lista.

Ascoltare attentamente la risposta pubblica di A/I mantenendo l'attività di advocacy giuridicamente indipendente.La dichiarazione del collettivo dovrebbe chiarire come vengono descritte la sua storia e le circostanze. Qualsiasi campagna coordinata, canale di raccolta fondi o servizio diretto richiede una valutazione giuridica separata. L'obiettivo immediato è rendere impossibile che A/I scompaia silenziosamente.

LA RETE CHIAMATA SOLIDARIETÀ

A/I è sopravvissuto alle multinazionali che esigevano censura, all'accesso segreto delle forze dell'ordine, alla confisca di dischi, a provider ostili, ad attacchi parlamentari e a indagini internazionali. Il caso Trenitalia ha prodotto server mirror e una vittoria legale. La violazione di Aruba ha dato origine al Piano R*. La censura dei provider ha generato ridondanza.

Il sequestro norvegese ha dimostrato che la rete poteva riprendersi in poche ore. Ogni tentativo di isolare il collettivo ha diffuso la conoscenza di come funzionano la censura e la sorveglianza. Ogni attacco è diventato un'opportunità per insegnare a più persone come proteggersi a vicenda. Gli Stati Uniti hanno ora trasformato quella storia in una prova globale. La posta in gioco non è solo la sopravvivenza di un collettivo di hacker italiani. Si tratta di stabilire se il mantenimento di infrastrutture per movimenti radicali possa essere di per sé considerato terrorismo; se la privacy possa essere ridefinita come occultamento; se il rifiuto di raccogliere informazioni identificative possa essere presentato come ostruzionismo; e se un provider possa essere ritenuto politicamente e legalmente responsabile di ogni testo, tattica e rivendicazione trasmessa attraverso i suoi server.

A/I ha trascorso venticinque anni a prepararsi al giorno in cui un server fosse scomparso. Sa come sostituire un server, spostare un servizio, ripristinare dati crittografati e continuare a operare dopo che la polizia o i provider ne abbiano interrotto il funzionamento. Gli Stati Uniti stanno tentando qualcosa di diverso. Stanno cercando di spaventare banche, host, registrar, fornitori di infrastrutture e sostenitori in tutto il mondo affinché abbandonino il collettivo. Il successo di questa strategia dipenderà in parte dall'architettura di A/I.

Dipenderà anche da noi.

Da oggi al 25 settembre, conservate la storia. Condividete la storia. Costruite la coalizione. Documentate l'isolamento. Insegnate gli strumenti. Preparate una difesa legale. Non permettete allo Stato di stabilire silenziosamente che costruire un'infrastruttura che preservi la privacy per il dissenso sia di per sé un atto di terrorismo. Venticinque anni fa, dieci persone si sono riunite attorno a un computer riciclato e hanno deliberatamente impiegato troppo tempo a configurarlo perché tutti i presenti nella stanza dovessero imparare. Questa rimane la lezione. Non lasciate la conoscenza solo agli esperti. Non concentrate l'infrastruttura in un unico luogo. Non lasciate soli coloro che sono presi di mira.

Il primo server si chiamava **Paranoia**.

La rete che ha creato si chiamava **solidarietà**.

DICHIARAZIONE PUBBLICA DI AUTISTICI/INVENTATI:

Oggi siamo venuti a sapere che il governo degli Stati Uniti ha preso di mira un piccolo collettivo tecnologico italiano gestito da volontari con sanzioni sproporzionate, come chiunque può leggere nella dichiarazione del Dipartimento del Tesoro, nella dichiarazione del Dipartimento di Stato e nel relativo ordine esecutivo.

Neghiamo tutte le accuse contenute nelle dichiarazioni, mentre affermiamo con forza il nostro impegno a fornire una piattaforma di strumenti per l'autodifesa digitale, rispondendo all'esigenza di comunicazione libera per attivisti e altri individui, gruppi e associazioni.

Non ci tireremo indietro, continueremo a fare ciò che abbiamo fatto in tutti questi anni e faremo tutto ciò che è in nostro potere per contrastare le false accuse mosse da un'amministrazione politicamente disperata, con l'unico intento di distogliere l'attenzione della gente e dei media dalla propria violenza e dal proprio bellicismo.

L'antifascismo e l'anticapitalismo non sono terrorismo. Protestare non è terrorismo. E tutti hanno il diritto di esprimersi e di lottare per l'umanità.

Collettivo Autistic/Invented — «Socializzare la conoscenza senza stabilire un potere»

Rimanete umani.