Defend Autistici/Inventati Before September 25 – Sabot Media

For twenty-five years, an Italian hacker collective has built communications infrastructure designed to survive censorship, surveillance and police raids. On August 26, the United States designated it a terrorist organization. On September 25, the wind-down period ends.

It should have been a dark and stormy night in an Italian hacklab.

It was, annoyingly, a beautiful sunny Sunday.

On March 3, 2001, roughly ten people gathered at the LOA hacklab in Milan around a computer assembled from discarded machinery. A bank had sold them an old server for the symbolic price of 15,000 lire, about eight dollars. They expanded it with scavenged components, including a hard drive pulled from someone's home computer. Nobody arrived with a formal blueprint. Software packages were considered one at a time. Every decision was discussed until everyone agreed. Deliberately, the least technically experienced person was placed at the keyboard. The process took far longer than necessary because efficiency was not the only objective. Everyone was supposed to understand what they were building. That day, one participant later recalled, was when they declared: "A/I now exists."

They named the machine **Paranoia**. The following month it went online, carrying two domains and two intertwined histories: Autistici.org and Inventati.org. Twenty-five years later, on August 26, 2026, the United States designated Autistici/Inventati a Specially Designated Global Terrorist and placed it on the Specially Designated Nationals and Blocked Persons list.

The distance between those two events—from a recycled machine in a Milan hacklab to the machinery of the American national-security state—is the history of a collective that has spent a quarter century insisting upon one dangerous proposition:

People should be able to communicate without first surrendering themselves to corporations or governments.

The immediate threat now has a date. On September 25, the temporary U.S. authorization for institutions to wind down their relationships with A/I expires. Banks, technology companies, hosting providers and other institutions are being instructed to sever what remains. A/I built its infrastructure to survive the disappearance of a server. The United States is now attempting to make the collective economically and technologically untouchable. Join us as we explore what A/I is, its history, and what this newest attack might mean for the autonomous tech collective and the wider radical community.

Before A/I: Italy's underground internet

Autistici/Inventati did not appear from nowhere. Its roots run through more than a decade of Italian autonomous organizing, pirate radio, bulletin-board systems, squatted social centers, anti-capitalist movements and experimentation with computers as political tools. During the 1990s, networks such as the European Counter Network and Isole nella Rete provided online space for social movements when the internet remained unfamiliar to much of the public. Italy's Hackmeetings brought programmers, activists, artists and the technologically curious together inside self-managed spaces. Hacklabs appeared in occupied social centers, where people could learn Linux, build networks and approach technical knowledge as something to be shared rather than sold. The future members of A/I came from several parts of this world. In Milan, people associated with the LOA hacklab used the name **Autistici** to describe their intense fascination with technology and their desire to expose the politics concealed inside it. In Florence, the **Inventati** project was more oriented toward communication, publishing and movement organizing. Its projects included *Stampa Clandestina*, a newspaper intended to be pasted directly onto city walls, and *Spia la Spia*, an effort to map surveillance cameras in public places.

People from Bologna and elsewhere were also involved. Many participated in the early development of Indymedia Italy, part of the international open-publishing network that allowed protesters and ordinary participants to report events without waiting for professional journalists to mediate them. The different groups shared a problem. Movements increasingly needed websites, mailing lists and private email, but independent infrastructure remained scarce. The existing European Counter Network was carrying too much of that burden. Commercial providers offered greater capacity, but at the price of money, dependence, surveillance and eventual censorship. In November 2000, Inventati sent the Milanese hackers an encrypted email asking to meet. The message was treated like something out of an amateur spy film: PGP keys, carefully arranged recognition instructions, a secret time and place. Then the Florentines arrived two hours late in a legendary rust bucket called the General Lee, honking outside the squat while police monitoring the building watched in bewilderment.

The agreed-upon historical fact is that everyone eventually ate at a pizzeria called La Balena. Over dinner, the Florentines revealed their allegedly seditious plan:

Build another autonomous server.

The intention was not to replace existing movement infrastructure with a new central provider. It was to multiply it. If there were thousands of autonomous servers, they reasoned, no single raid or seizure could shut down everyone's communications. Autistici supplied much of the technical knowledge. Inventati brought its experience with publishing, cultural work and movement communication. Together they became Autistici/Inventati, usually shortened to A/I. The collective's legal association was called Investici, but A/I never became a conventional organization. It had no coordinator, official leader or permanent spokesperson. Decisions were made collectively rather than by majority vote. Nobody was paid. Its resources came from voluntary donations, benefit events and the labor of the people maintaining it. The dual name was deliberate. A/I was a Janus-faced creature: one face technical, the other communicative; one facing the machine, the other facing the movements that needed it.

The server that locked itself out

The birth was not entirely glorious. On the second day of Paranoia's existence, someone entered an inverted firewall command and accidentally instructed the machine to reject every connection not originating from itself.

The server could communicate only with the server.

The collective found this so perfectly on-brand that it printed the mistake on a T-shirt. That combination of technical seriousness and refusal of self-importance became part of A/I's character. Later servers received names including Chernobyl, Astio—"Grudge"—Rivolta, Contumacia and Latitanza: Revolt, Contumacy and Life on the Run. Behind the jokes was a developed political position. Communication should be free and accessible. Knowledge grows through being shared. Software is not neutral simply because it operates in a supposedly virtual world. The systems through which people speak determine who can speak, who can listen, who owns the record and who can be silenced. A/I began

providing websites, private email, mailing lists, newsletters and chat. Its services eventually expanded to include Noblogs, file sharing, audio and video conferencing, streaming, anonymous remailing and other communications tools—all without advertising or commercial data extraction.

Its manifesto describes the project in explicitly political terms. A/I is antifascist, anti-capitalist and antimilitarist. It promotes free software, encryption, pseudonymity and the independent circulation of knowledge and cultural work. It reserves its limited, volunteer-run resources for people and projects broadly compatible with those principles rather than businesses, political parties, organized religions or institutions already possessing the means to make themselves heard. A/I was never a politically neutral commercial host. But providing infrastructure is not the same act as authoring everything transmitted through it. Political affinity is not operational control. Giving someone an email account does not mean writing every message they later send. That distinction is central to the attack now being made against it.

Genoa: infrastructure under fire

Only months after Paranoia went online, the G8 came to Genoa. Many A/I participants were also involved with Indymedia Italy. They helped construct the movement's media center, laying cables, configuring servers and building workstations through which protesters could report what was happening across the city. What followed was historic: enormous demonstrations, the police killing of Carlo Giuliani, indiscriminate beatings in the streets, torture and abuse inside the Bolzaneto barracks and the nighttime raid on the Diaz school. Official narratives competed with photographs, recordings and firsthand testimony transmitted through independent infrastructure. Genoa became one of the earliest major demonstrations to be documented from nearly every direction by its participants rather than exclusively through institutional media.

For A/I, it was also what the collective later called a "traumatic communion." Its members experienced the same violence together while maintaining systems through which evidence of that violence could escape. After Genoa, A/I was no longer merely an interesting technical experiment. It had become trusted movement infrastructure. Demand grew rapidly. By 2003, A/I hosted more than 2,000 users, 205 websites and 269 discussion lists. Hosting those services for free was becoming unsustainable, while commercial hosting would cost thousands of euros annually. The collective answered with the KAOS tours: traveling gatherings combining benefit events, parties, public discussions and practical workshops. A/I members taught people how to configure servers, encrypt communications, edit and distribute video, create digital archives and stream audio.

The tours raised money, but their deeper purpose was political education. The collective did not want to become a group of invisible experts performing magic for passive users. It wanted the community to understand the machinery upon which it increasingly depended.

Every subsequent attack on A/I would produce a variation on this response:

Disclose what happened. Repair the damage. Share the lesson. Build something harder to destroy.

Trenitalia discovers the Streisand effect

A/I's first major legal confrontation came in 2004. A design collective called Zenmai had created a website parodying the Italian railway company Trenitalia. It copied the appearance of the company's website while denouncing Trenitalia's involvement in transporting tanks and other military supplies during the invasion of Iraq. Trenitalia demanded the page's removal, damages and publication of notices in two major newspapers at a projected cost of approximately €20,000. A court initially ordered A/I to take the parody down. The internet responded by reproducing it everywhere.

Trenitalia then demanded that A/I remove links to the mirrors as well—an argument raising the absurd possibility that linking to disputed material could make any search engine responsible for it. A/I appealed. On September 14, 2004, the court ruled that the website was protected satire grounded in factual controversy. The page returned, and Trenitalia was ordered to pay A/I's legal expenses. It was an extraordinary victory for a small volunteer collective. But while A/I fought visible censorship in court, a more dangerous operation was taking place without its knowledge.

The Aruba crackdown

By then, A/I's server was housed at the commercial provider Aruba in Arezzo. On June 15, 2004, Italian police arrived at Aruba under orders from a Bologna prosecutor. The company's technicians shut down A/I's machine and allowed police to copy material from its disks. Investigators obtained its cryptographic certificates and may have installed equipment capable of intercepting traffic. A/I was told that the interruption resulted from an electrical problem. The collective discovered the truth almost a year later, and only by accident.

In May 2005, A/I was ordered to close the mailbox used by the Italian Anarchist Black Cross, Crocenera Anarchica, amid a sprawling investigation involving allegations of anarchist conspiracy and subversion. A/I complied with the court order and requested the underlying case documents. Those documents contained messages that investigators should not have been able to possess. Buried in a footnote was the explanation: police had gone to Aruba the previous year and acquired access to A/I's server. An operation purportedly concerned with one mailbox had potentially compromised thousands of accounts and tens of thousands of mailing-list subscribers. Among those affected were lawyers and technical experts working with the Genoa Legal Forum. Police may therefore have gained access to confidential defense communications concerning prosecutions arising from police conduct at the G8. The violation exposed a brutal truth. A/I could operate its own server, configure it carefully and refuse to retain identifying logs—but the physical machine remained in someone else's building. A commercial provider could open the door, surrender its contents and conceal what had happened.

A/I removed the machine from Aruba, cleaned it and restored essential services. Parliamentary questions were raised in Italy and at the European level. The collective traveled through Italy and Europe explaining the breach. Most importantly, it rebuilt the network.

Plan R*: repression becomes architecture

The result was Plan R*, launched in October 2005: a network of "resistant communication." Instead of concentrating A/I's services on one machine, the collective distributed encrypted data and functions across servers in several countries. Public-facing machines could be replaced. Services could move when hardware was seized or a provider became hostile. The loss of one node would no longer expose or silence the entire community. R* meant replication, redundancy, resistance and other words beginning with R. Its architecture was conceived not merely to survive mechanical failure but to withstand political attack. A/I did not claim it could guarantee perfect security. On the contrary, it repeatedly warned users never to entrust their safety blindly to any provider, including A/I. It minimized logs and identifying information because information that does not exist cannot easily be seized. It encouraged users to encrypt their own communications because even the strongest server architecture could not compensate for unsafe individual practices.

The collective transformed a covert surveillance operation into an infrastructure lesson.

Repression became architecture.

The Vatican, a satirical video game and Norway

The pressure continued. In 2007, an Italian politician demanded action against *Operation: Pedopriest*, a satirical browser game criticizing the Catholic Church's efforts to conceal sexual abuse by clergy. Its creator temporarily removed the game to protect the hosting provider. A/I then hosted a copy. Following a complaint from an unidentified child-protection organization, an American provider disconnected the entire Noblogs server. After consulting attorneys, the provider concluded that the satire was lawful in the United States and restored the machine. Plan R* kept the disputed material accessible elsewhere and limited the wider interruption. By then, A/I had become an important refuge from the emerging commercial social web. Noblogs offered independent publishing without advertising, data mining or demands that people attach their legal identities to everything they said.

Its users included movement organizations, personal writers, dissidents, artists and NGO workers operating in dangerous environments. In 2008, A/I received Italy's Winston Smith "Privacy Hero" award for creating free communications infrastructure resistant to censorship despite scarce resources, technical attacks and repeated judicial interventions. Then, on November 6, 2010, Norwegian police copied an A/I server's hard drives at Italy's request. The investigation originated with threats and antifascist graffiti directed at members of the neo-fascist CasaPound organization. Authorities were seeking information concerning one mailbox. A/I had already explained that it possessed neither subscriber identities nor activity logs, but investigators apparently wanted to determine whether that was true.

Thousands of accounts were copied in the process.

Plan R* restored the affected services elsewhere within approximately two hours. Within twenty-four hours, the network was operating normally. The seized disks were encrypted and yielded no useful identifying information. The operation became a public scandal in Norway. Lawyers, journalists and technology organizations questioned why Norwegian police had copied thousands of people's private communications in response to an inadequately explained foreign request. The underlying Italian investigation was eventually dropped. Where another organization might have interpreted repeated raids as proof that its project was impossible, A/I interpreted them as confirmation that the project was necessary. Its history is documented in the collective's book, *+KAOS: Ten Years of Hacking and Media Activism*, and its own history of the collective.

August 26, 2026

The newest attack is of a different order. On August 26, the U.S. State Department designated Autistici/Inventati a Specially Designated Global Terrorist. At the same time, the Treasury Department's Office of Foreign Assets Control placed A/I on the Specially Designated Nationals and Blocked Persons list under Executive Order 13224. This is not simply a condemnatory government statement. It activates one of the world's most powerful systems of economic exclusion. The United States alleges that A/I supplies specialized digital architecture, encrypted communications and hosting to antifascist groups and other radical movements, including organizations already designated by the United States.

Treasury's public announcement focuses upon the services A/I provides: foreign-hosted websites, encrypted email, chat, video conferencing and the digital architecture supporting Noblogs. It describes A/I's antifascist and antimilitarist politics, its practice of selecting projects compatible with those politics and its provision of infrastructure used by the PKK. Treasury then treats the provision of that infrastructure as material or technological support for terrorism. (U.S. Treasury announcement) The State Department's accompanying case goes further, presenting attacks, communiqués and publications that it says passed through A/I infrastructure. Its examples include alleged railway and pipeline sabotage in Europe, attacks on energy infrastructure, Rose City Antifa, resistance to Atlanta's proposed police-training center, Jane's Revenge and publications carrying statements attributed to armed organizations. (State Department designation) The government's public statements do not show that A/I planned those actions, selected targets, transferred weapons, directed the cited groups or authored the material hosted on its systems. They do not establish when A/I learned of any particular act or whether it knew about it before it occurred.

Instead, the designation advances a broader and more consequential proposition:

Building communications infrastructure for radical movements can itself be treated as terrorism.

That theory collapses the distinction between a provider and a user; between political affinity and operational control; between protecting privacy and concealing a crime; between maintaining a publishing platform and authoring everything published through it. A/I has never claimed to be politically neutral. It built infrastructure precisely because radical movements needed somewhere to speak, publish and organize beyond corporate and state control. The United States is now using that purpose as evidence against it.

What happens on September 25

Because A/I is now on the SDN list, all of its property or interests in property within the United States—or possessed or controlled by a U.S. person—must be blocked and reported to OFAC. Unless an exemption or license applies, U.S. people and institutions are generally prohibited from providing or receiving funds, goods or services involving A/I. The restrictions can reach transactions passing through the United States even when the parties are located elsewhere. OFAC has issued a temporary license allowing transactions ordinarily necessary to wind down existing relationships with A/I until **12:01 a.m. Eastern time on September 25, 2026**. Payments owed to the collective cannot simply be released to it; they must be placed in blocked accounts. After the deadline, covered transactions require another applicable authorization. September 25 is therefore the date by which American companies and individuals are expected to separate themselves from A/I.

The consequences may include the loss of:

- Bank accounts and payment processing.
- U.S.-linked donations and fundraising services.
- Hosting, cloud infrastructure and upstream network services.
- Domain registration and related technical services.
- Certificate, security and email-delivery accounts.
- Software and communications services.
- Relationships with non-U.S. providers frightened by American secondary sanctions.
- Access for people in the United States who currently use A/I's services.

Foreign companies are not automatically governed by every prohibition imposed upon Americans. But OFAC warns that foreign financial

institutions can face secondary-sanctions exposure for knowingly facilitating significant transactions on behalf of a designated entity. That warning may do as much damage as direct enforcement. A European bank, registrar or hosting company may not know precisely what American law demands of it. Its compliance department may simply decide that maintaining a relationship with a small Italian anarchist collective is not worth the perceived risk. Institutions frequently over-comply. Providers may close accounts or withdraw infrastructure even when the law does not clearly require them to do so. Organizations may remove links, avoid correspondence or terminate unrelated relationships merely because A/I's name now appears on a terrorism blacklist.

That is how American sanctions acquire worldwide force: not only through legal jurisdiction, but through institutional fear.

The wider target is the community around the server

The designation may be directed at A/I, but its effects will not stop at the collective. A/I's infrastructure is used by writers, organizers, researchers, artists, movement publications and people who chose it precisely because commercial platforms were unsafe, politically hostile or designed to extract their data. Those users are not automatically sanctioned because they have an A/I address or published on Noblogs. But once the provider itself is placed on a terrorism blacklist, ordinary association can be converted into a risk signal. A bank may scrutinize a payment. An email provider may downgrade or block delivery. An employer, border agent or investigator may treat an address as suspicious. A journalist may hesitate to contact a source. A researcher may avoid an archive. A new user may decide that opening an account is too dangerous. None of this requires the government to prosecute every person involved. The designation can produce its own perimeter of fear.

That is one reason this otherwise inexplicable move may be useful to the state even if A/I remains online. Earlier attacks tried to reach the collective through particular machines, mailboxes and providers. A/I answered by distributing its systems, encrypting its disks and retaining less information. Those practices made conventional seizure and surveillance less productive. Sanctions attack a different layer: the relationships that allow infrastructure to exist. Rather than breaking the encryption, the government can pressure banks, registrars, data centers, software companies and users to isolate the people operating it. Rather than prove in court that each user committed an offense, it can make continued contact costly and legally uncertain.

This is surveillance-state power operating through private intermediaries. The government does not need to place an officer inside every server room when compliance departments, payment processors and platforms can be induced to police the network themselves. Each institution will draw its own defensive boundary, often wider than the law requires. Some may demand more identity documents, retain more logs, monitor political content or refuse privacy-preserving projects altogether. Others may quietly close accounts and provide no meaningful avenue of appeal. Enforcement becomes dispersed across companies whose decisions are difficult to see, challenge or even document.

The resulting harm is not limited to censorship. It can change the architecture of movement communication. Small autonomous providers may conclude that serving controversial communities invites existential risk. Larger platforms may point to the designation as another reason to expand identity verification, automated moderation and data retention. Users may migrate from trusted movement infrastructure to commercial systems that are easier to monitor, subpoena and map. The state gains leverage even when it gains no plaintext from A/I's encrypted disks: people separate themselves, providers collect more information and the social relationships surrounding dissent become easier to observe.

The precedent also reaches beyond explicitly anarchist or antifascist projects. If political alignment with users, privacy protections and the hosting of controversial publications can be assembled into a case that infrastructure itself constitutes support, then encrypted mail providers, radical publishers, community archives, VPNs, federated social networks, legal-support projects and other independent hosts all have reason to pay attention. The immediate facts and laws would differ in every case. The danger lies in normalizing the category: a communications provider no longer treated as a conduit or publisher with its own rights and responsibilities, but as a participant in every act the government attributes to anyone using its systems.

That does not mean the designation is secretly about every A/I user, or that every possible consequence will occur. The government has not publicly explained its internal strategy beyond the allegations in its announcements. But the structure of the action is visible. It replaces a narrow accusation against identifiable conduct with a broad penalty against infrastructure; shifts enforcement from a courtroom to a global web of cautious institutions; and makes uncertainty itself an instrument of control. The immediate objective may be to disable A/I. The wider effect is to warn anyone building communications beyond corporate and state supervision that the shelter they provide can be recast as evidence against them.

Can A/I survive this?

A/I has seen state repression coming for miles.

Its entire infrastructure assumes that:

- Servers will be seized.
- Providers will cooperate with police.
- Governments will demand information about users.
- Corporations will disconnect controversial material.
- Individual machines and locations will become unavailable.
- Data and services must therefore be encrypted, distributed and replaceable.

That preparation matters. A/I is based in Italy, not the United States. Its infrastructure is internationally distributed. Its services are maintained by technically sophisticated volunteers. It avoids dependence on any single provider, minimizes identifying information and has decades of experience restoring services during emergencies. It has no shareholders, corporate headquarters or conventional payroll. Its relatively modest operating costs and volunteer structure give the state fewer familiar pressure points. There is little reason to assume that the website, mail system or Noblogs will simply disappear on September 25. A/I may be better equipped to survive a seized or disconnected machine than nearly any communications project of comparable size.

But this is not another server raid.

Plan R* was built to survive machines disappearing. It cannot, by itself, prevent banks from blocking money, registrars from suspending domains or companies around the world from withdrawing services because they fear American penalties.

The designation targets the connective tissue around the servers:

- Banking.
- Donations.

- Domains.
- Data-center contracts.
- Bandwidth.
- Certificates.
- Software dependencies.
- International institutional relationships.

A/I has survived technical isolation before. The United States is now attempting financial and institutional excommunication. Its core services may be resilient. Its ability to fund them, replace infrastructure and participate in the broader technological system is at considerably greater risk. What happens after September 25 will therefore depend not only upon the architecture surrounding A/I's data, but upon the solidarity surrounding A/I itself.

September 25 is not a deadline for silence

The designation is designed to isolate. The answer must be informed, independent and disciplined solidarity. People in the United States should not improvise donations, disguise payments or route resources through another person, organization, currency or country. That could create sanctions exposure for the supporter, the intermediary and A/I itself. The prohibitions can also extend beyond money. Coordinated technical assistance, translation, advocacy, event organization or other services provided to a designated entity may create legal risk.

But September 25 is not a deadline for silence. Independent reporting, criticism, protest, education and political advocacy remain possible. People can tell A/I's history, examine and challenge the government's claims, contact journalists and civil-liberties organizations, preserve public materials and independently organize against the criminalization of resistant communications infrastructure. The practical distinction is between speaking and acting independently about A/I and providing funds or coordinated services to A/I. The exact boundaries can be complicated. Anyone contemplating fundraising, replacement infrastructure, public mirroring or direct technical assistance should obtain qualified sanctions counsel. A February 2025 civil-liberties primer on material support and OFAC restrictions also warns that lawful or protected activity can still attract surveillance, investigation, immigration consequences or civil litigation. Supporters approached by law enforcement should decline to answer questions and speak with an attorney.

This article is reporting and political analysis, not legal advice.

What supporters can do before September 25

Tell the history. Share A/I's story: the hacklabs, Paranoia, Genoa, the KAOS tours, the Trenitalia victory, the Aruba breach, Plan R*, Noblogs and the Norwegian seizure. Do not allow the government's description to become the only publicly available account of what A/I is. **Build a public defense coalition.** Ask independent server collectives, digital-rights organizations, hacklabs, free-software projects, radical libraries, independent publishers, journalists, attorneys, researchers and former users to respond publicly. **Preserve the archive.** Servers can be seized. Domains can be suspended. Hosts can panic. Back up publicly accessible and historically valuable Noblogs writing, along with A/I's manifestos, technical documents, legal records and movement history. Record source URLs, authorship, publication dates and retrieval dates. Respect privacy, copyright and removal requests. Do not access private accounts or circumvent security. Personal preservation, research archiving and ordinary journalism are not the same as publicly operating replacement infrastructure; anyone considering a public mirror should first seek qualified advice.

Document over-compliance. Record companies, banks, registrars, platforms and institutions terminating services or removing material. Preserve notices and correspondence. The public record should show how far the designation reaches beyond its formal language. **Demand answers.** Ask digital-rights groups, European institutions and public officials whether they will permit American sanctions to dismantle an Italian communications collective. Ask what protection exists for European infrastructure, users and archives. **Organize independently.** Hold public discussions about autonomous infrastructure, sanctions, surveillance and material-support law. Publish explainers. Teach encryption. Support independent civil-liberties work opposing expansive terrorism designations. **Prepare lawful material support.** A/I has historically survived through voluntary donations, but U.S. supporters should not send or reroute money while the designation applies without a clear authorization. Digital-rights and legal organizations can independently investigate lawful support mechanisms, licensing and potential delisting proceedings.

Listen carefully to A/I's public response while keeping advocacy legally independent. The collective's statement should inform how its history and circumstances are described. Any coordinated campaign, fundraising channel or direct service requires separate legal consideration. The immediate objective is to make A/I impossible to quietly disappear.

The network called solidarity

A/I has survived corporations demanding censorship, covert police access, confiscated disks, hostile providers, parliamentary attacks and international investigations. The Trenitalia case produced mirrors and a legal victory. The Aruba breach produced Plan R*. Provider censorship produced redundancy.

The Norwegian seizure demonstrated that the network could recover in hours. Each attempt to isolate the collective spread knowledge about how censorship and surveillance operate. Each attack became an opportunity to teach more people how to protect one another. The United States has now transformed that history into a global test. At stake is not only the survival of one Italian hacker collective. It is whether maintaining infrastructure for radical movements can itself be treated as terrorism; whether privacy can be redefined as concealment; whether refusing to collect identifying information can be presented as obstruction; and whether a provider can be held politically and legally responsible for every text, tactic and claim transmitted through its machines.

A/I has spent twenty-five years preparing for the day when a server disappears. It knows how to replace a machine, move a service, restore encrypted data and continue operating after police or providers pull a plug. The United States is attempting something different. It is trying to frighten banks, hosts, registrars, infrastructure providers and supporters around the world into abandoning the collective. Whether that succeeds will depend partly upon A/I's architecture.

It will also depend upon us.

Between now and September 25, preserve the history. Share the story. Build the coalition. Document the isolation. Teach the tools. Prepare a lawful defense. Do not allow the state to quietly establish that building privacy-preserving infrastructure for dissent is itself an act of terrorism. Twenty-five years ago, ten people gathered around a recycled machine and deliberately took too long configuring it because everyone in the room was supposed to learn. That remains the lesson. Do not leave the knowledge with experts.

Do not leave the infrastructure in one place. Do not leave the targeted to stand alone.

The first server was called **Paranoia**.

The network it created was called **solidarity**.

Public statement from Autistici/Inventati:

Today we were made aware that the US Government has targeted a small, volunteer-run, technology collective from Italy with disproportionate sanctions as anyone can read in the Treasury Department Statement, the State Department Statement and the related Executive Order.

We deny all allegations included in the statements, while we strongly affirm our dedication to providing a platform of tools for digital self-defense, addressing the need of free communication for activists and other individuals, groups and associations.

We will not back down, we will keep doing what we have been doing all these years and we will do whatever is in our possibility to counter the false allegations made by a politically desperate administration with the sole intention of swaying people and media attention away from their own violence and warmongering.

Antifascism and anticapitalism are not terrorism. Protesting is not terrorism. And everyone has the right to speak out and to struggle for humanity.

Autistic/Invented Collective — "Socializing knowledge without establishing power"

Stay human.

Download the A/I book , +KAOS, on the history of the collective's work, available for free.

Download our Media Kit for social media graphics, archival guides, press briefs, templates, and flyers if you or your organization would like to show solidarity with A/I or learn more.