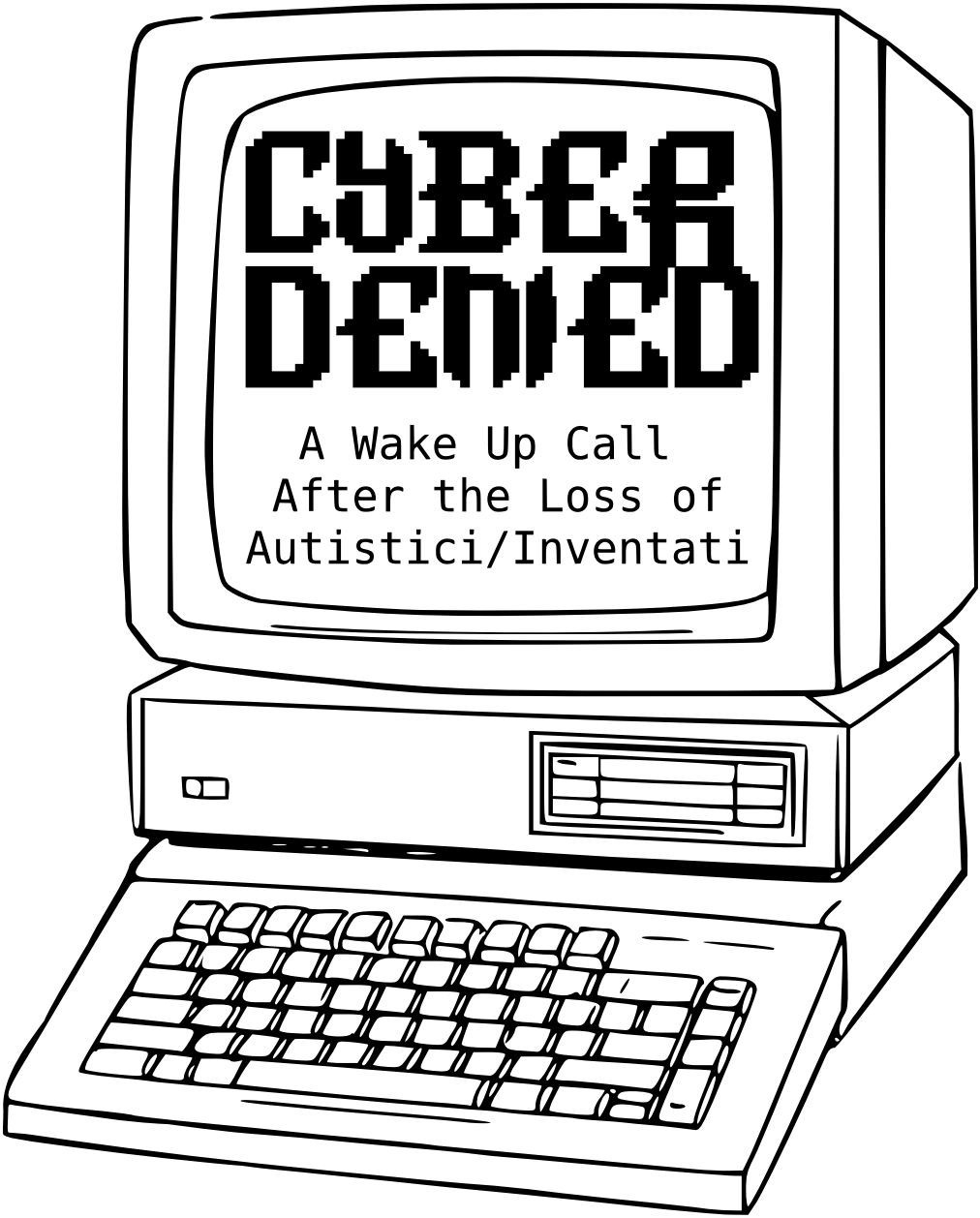

CYBER
DENIED
A Wake Up Call
After the Loss of
Autistici/Inventati

user@laptop:~$

We're your local anarchist nerds. You might know our faces and the sites we help run. You might have seen reporting based on our work. We've led Crypto Parties and digital security workshops. We've hosted FOSS and custom apps for anarchist projects, contributed to apps you've used. If you don't know us or our work, you know people just like us and work just like ours.

We say this not to speak with authority, but to show that the critique is coming from inside the house. We're not primitivists or anti-civ, not blanket anti-information-technology. We're deep in this and are trying to be pragmatic.

Oh, and we too lost e-mail addresses and access to NoBlogs sites we liked to read. This all hits very close to home.

On August 26th 2026 the US government classified the technology collective Autistici/Inventati as a Specially Designated Global Terrorist. This designation meant heavy sanctions on them and all those who support them. As a result of this, their domains were seized, and their bank accounts were frozen, among other things. This effectively ended their ability to operate, and the organization has since officially disbanded. Autistici/Inventati was a key host of services for radical anticapitalist and anarchist projects, including e-mail, mailing lists as well as the very popular managed WordPress service NoBlogs that had over 22,000 blogs.

What did we think was going to happen?

Anarchists oppose all forms of domination and hierarchy, so anarchists are enemies of the State from first principles. The State is the largest single oppressor and depriver of freedom, and as such it takes the lion's share of our attention. Similarly speaking, the United States is roughly the largest dominator on the global stage today, and so it too receives a large portion of criticism. Why is it then that anyone is surprised when the US regime (during a particularly fascist incarnation) has turned its attention on the open hosting of seditious and outright criminal material?[1] And why is it surprising that with Europe's descent into further authoritarianism that governments and financial institutions here would enthusiastically go along with US policy?

It's worth reading the State Department's "fact sheet" on the SGDT classification because it cites several well-known communiqués that were published on NoBlogs.[2] The words "terrorism" and "extremist" are semantically flexible enough to be useless, but you can always expect the State to sprinkle some theatrical language over its show of force. But also, let's be real. The anarchist movement is extreme compared to the majority of society being technocratic statists whose only ideas of change are twiddling the knobs controlling tax rates or swapping out who's in charge. The "fact sheet" is not off the mark when it comes to the specifics. The Trump regime read the websites that people intentionally published and has acted accordingly. The shocking thing here should actually be that it didn't happen sooner! One could even (cynically) hypothesize that the reason why is that

[1] Or, why is a surprise that this happened to a collective in Italy under a fascist prime minister? What favor did Trump buy from Meloni by doing so?

[2] See the Appendix where the "fact sheet" has been reproduced in full.

we are actually not enough of a threat to matter most of the time, and now was just a convenient moment for the fascists to whip up easy propaganda.

The internet was never really ours.

Among some techy-flavored radicals, cypherpunks, and the like, this has been long known and critiqued, though this critique never reached widespread awareness among the tech-literate much less the average user of the internet.[3]

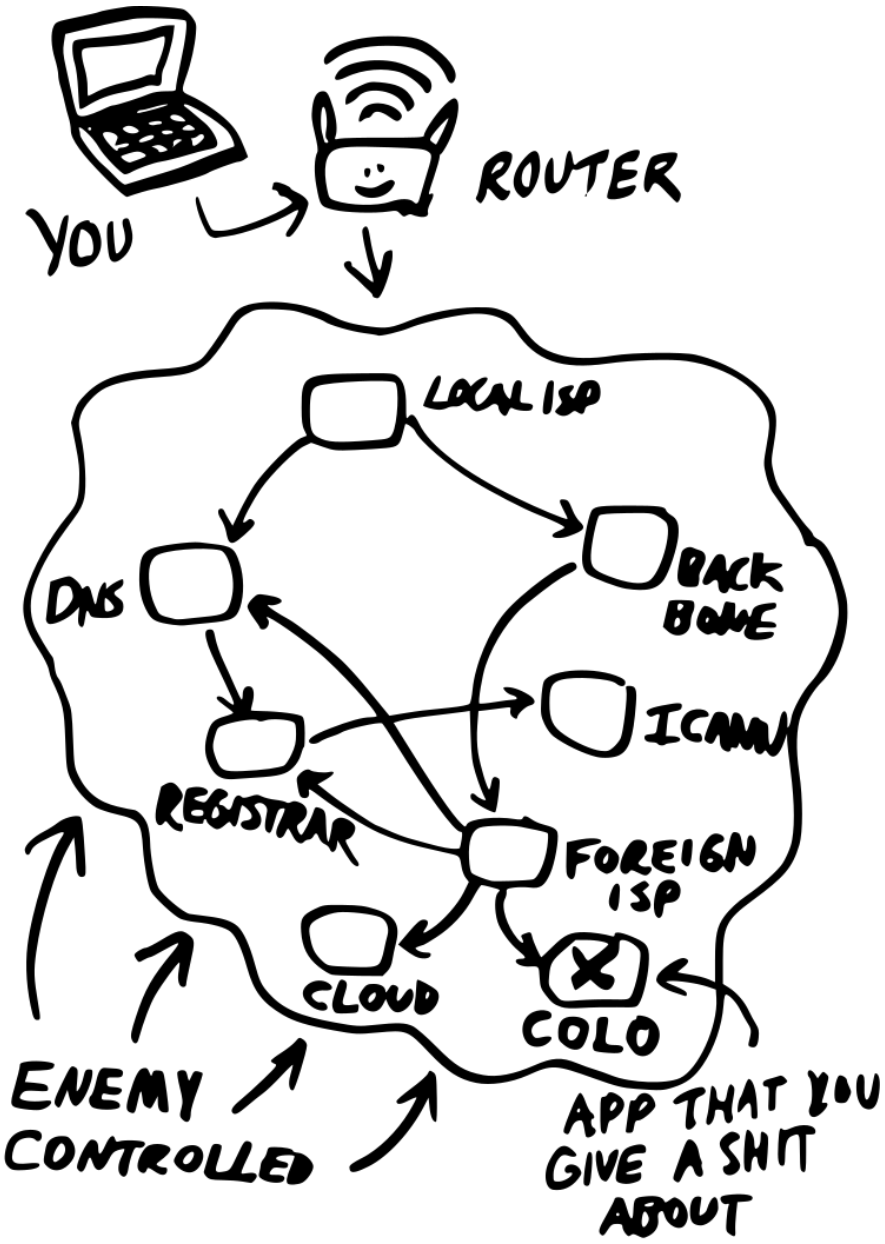
Why do we say isn't it ours? Those seeking liberation don't control the substrate of the internet. The internet is protocols and specifications built on physical infrastructure that is run by States and corporations. There might be some actors like A/I who are quite ideologically aligned with us and some allies who dream of a free internet (maybe only in the shit right-libertarian sense). But there is a monumental amount of pieces that all have to come together for Party A to host a website that Party B can view, and we control almost none of them.

It should obvious now that the commercial social media platforms are hostile to radical organizing. Wave after wave of bans have flushed out Facebook, Twitter, and Instagram. People migrated to newer copycat platforms like Bluesky that promise something different, or to entirely different formats like Telegram announcement channels or blogs like Medium and Substack. As all of these are effectively centrally controlled, and political projects there continue to suffer. The authorities on those large platforms actively hate us, and even if they don't, they don't give a fuck about us. At their scale, they only respond to economic incentives or the whims of their billionaire owners. They will not defend us against the State, that is, if they don't voluntarily kick us off (not only in cases where they're preempting a government order!) for any number of reasons for which there is no recourse. This is true not only for consumer-facing social apps but for nearly all providers of internet infrastructure.

One response is the call for self-hosting, for running servers hosting various websites and apps, where we are the administrators. This is exactly what Autistici/Inventati has been doing for the last twenty years, and has been reflected in newer projects like the anarchist-run Mastodon server kolektiva.social.

---

[3] *A Declaration of Independence of Cyberspace* was woefully wrong, yet even those who critiqued it continued to yearn for the utopia described within.


YOU
ROUTER
LOCAL ISP
DNS
BACK BONE
ICANN
REGISTRAR
FOREIGN ISP
CLOUD
COLO
ENEMY CONTROLLED
APP THAT YOU GIVE A SHIT ABOUT

Let a thousand identical flowers bloom!

The response to A/I's sanctions and shuttering has been one of defiance. Good.

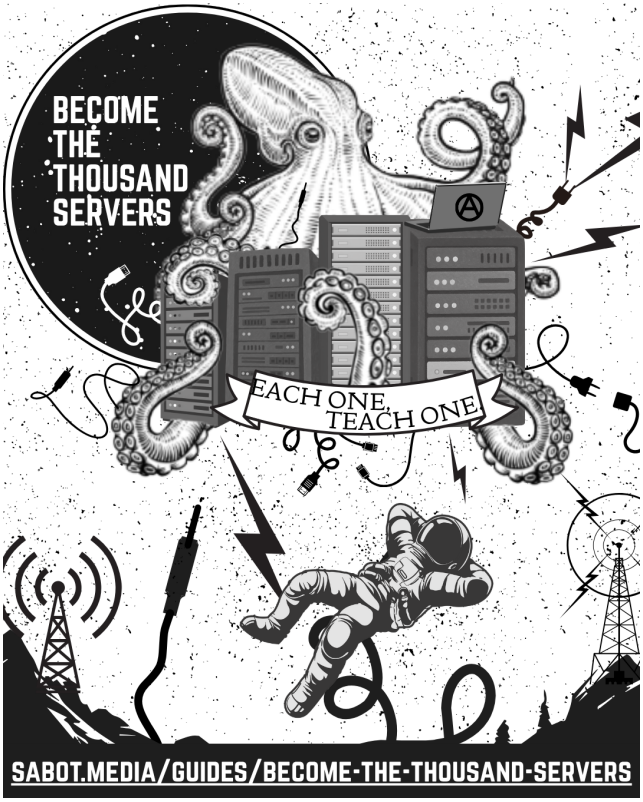
But let's not make the same mistakes again.

The dominant response from technologically inclined radicals has been to advocate for more decentralized self-hosting infrastructure. Not just one A/I, but ten, a hundred, a thousand. If A/I was one easy target where taking down one domain and one collective damaged the ability of thousands to communicate and tens of thousands more to read what they'd publicly written, then splitting to many sites means each takedown impacts fewer people. But it's not so simple. The move the government made against A/I created an uproar of sorts, but maybe ten people will give a fuck when whatever micro couterinfo WordPress site like literally-stab-every-cop.lol gets taken down, and in a month it will be forgotten by everyone.

This isn't even getting into what it requires to run internet infrastructure. What made A/I so valuable is their *scale* and *longevity*. Running a small fleet of servers reliably and securely is *hard* and time-consuming. It's 100 times more effort to run 100 A/I clones that serve 1/100th the number of users. Running a single website securely and reliably is no simple task. It requires significant techy background knowledge that takes time to learn, not to mention the perpetual janitorial upkeep of maintaining the infrastructure. There's a commonly cited number saying that it takes 10,000 hours of work to become an expert. Running a website is not a skill one can quickly pick up only to use on occasion in the same way that one can learn to cook for large groups at their local solidarity kitchen.[4]

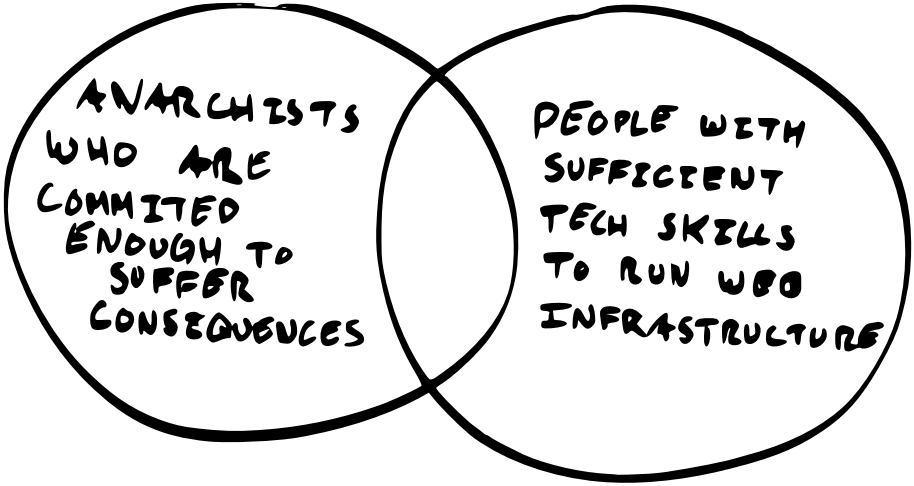
Self-hosting also changes the risk calculation for the individuals doing the hosting versus using services provided by collectives like A/I. In some sense, it really lets repression be focused. If a collective self-hosts, then the people running the website would be the same ones who engaged in the criminalized actions that would be posted to it. Large collectives like A/I (or other counterinfo sites) let anarchists (somewhat) launder their communiqués.

[4] This isn't a knock against professional chefs and the punks that cook at FNB. One, cooking has a definitive obvious use, and maybe many of these websites actually do nothing (maybe this zine does nothing). Two, we the authors have many times cooked at such kitchens including running them, so we're not talking out of our asses. And three, using dumpstered food to cook vegan food while listening to Pat the Bunny is clearly more fun than debugging Linux networking issues. Anyway...



The guide linked above was initially written with an "Artificial Intelligence" LLM. Even the people saying how easy and doable this kind of work can be were too tired of the work to put the time in to write the guides themselves! Part of why this happened, of course, is the horrendous quality and usability of free software, its documentation, and the whole ecosystem.

The phrase "Let a thousand flowers bloom!" has been used by many as a call to action on how we should respond to this repression, but like we've said. A thousand A/I clones takes roughly a thousand as many people to run them, and the overlap between anarchists who are committed enough to suffer consequences for supporting criminalized activity and people with sufficient tech skills to run web infrastructure is vanishingly small. This is because, on the average, those who are capable of cultivating such tech skills and maintaining them through constant use are those working for tech companies, which is to say privileged. This privilege is a set of golden handcuffs that limits the amount of risk they are willing to expose



themselves to.[5] Simply put, privileged people have less skin in the game, in part because they can opt-out of "politics" while others cannot.

Maybe think of it like this: How many middle class techies would set themselves up to go to prison so you could have a website where you post about firebombing ATMs?

And if you're reading this and are considering hosting such websites but you don't think this is a possibility, ask yourself what happens next. Why would the US government (or any government) stop with A/I? Who are they coming for next?

Given the costs in human labor and the increasing hosting costs because of "Artificial Intelligence" causing the prices of computer parts to skyrocket, we have to ask ourselves, what is the point of all this? Most online anarchist projects are to "get the word out."

Well, have we?

[5]We are not exempting ourselves from this either, at least not entirely. Each of us has over a decade "in the movement," but we can still wonder if we're not shying away from actions and causes.

Cybernetic Legibility

The way things are built now, there is no sovereign internet. Self-hosted websites are not the digital equivalent of homesteading or getting "off grid."

Remember, websites are all hosted on physical infrastructure that exists in the real world, and all of it can be tied back to a human who runs it. From the piece of hardware hosting the application that serves the HTML of a website to every piece of networking equipment that allows a request to reach it and a response to return: these all have human operators who work for corporations (or if we're lucky, collectives). There are companies that offer anonymously hosting websites like FlokiNET that are paid for in cash or (varyingly anonymous) cryptocurrencies.Even if the entity posting the content to the website is never known, a police raid could seize the physical server out of the data center or use legal means to halt the company's operation.[6]

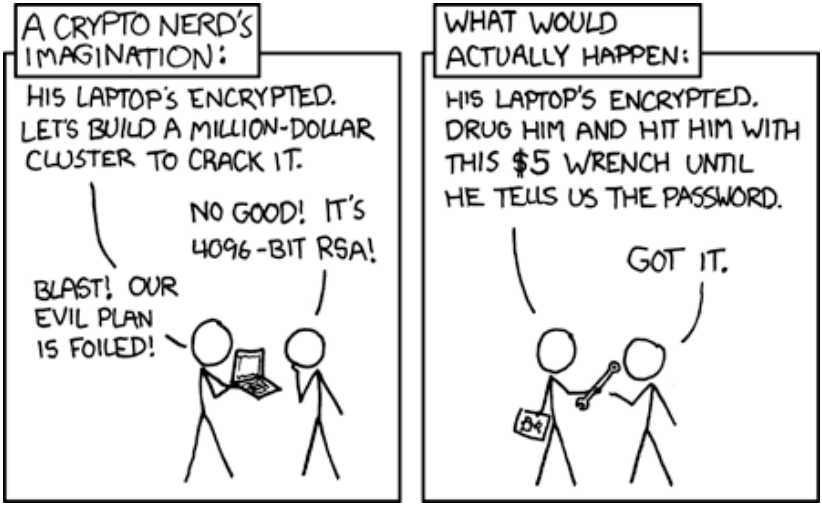
On the user's side technologies like VPNs and Tor are available to route around some kinds of censorship, but due to how the protocols of the internet work, to any network observer it is obvious that such technologies are in use. To some degree, it's a wonder these have been allowed to exist as long as they have. Tor is blocked in some countries we imagine as more repressive than "The West," and there are some mitigations for this, but requiring these mitigations still shuts out some users. In extreme cases, the internet is shut off entirely or regionally isolated.

Censorship versus evasion is a game of cat-and-mouse, but in the end the State controls both ends of the line. In europe Chat Control legislation is constantly knocking at the door, the descendent of some of the battles of the original Crypto Wars of the likes of the Clipper Chip. Age verification has arrived with shocking speed in a few countries, and certainly forms of this will be rolled out elsewhere. In most meaningful ways, net neutrality is long dead. What is going to happen to your Tor connection or Onion Service when age verification is required by your ISP to get on the internet at all? Again, even if that data flowing over the wire is encrypted, they know someone using your internet is connecting to a well-known anonymization network.

[6]For example, Lavabit suspending operations in 2013 while under a gag order, and at the time this was assumed to be because they provided e-mail hosting for leaker Edward Snowden. A legal company was dismantled by legal means.

There are other experimental technologies like offline-first peer-to-peer applications or multi-transport networks like Reticulum which do seem to offer some unique advantages. There's some good reasons to hope that these technologies work out, but wherever they touch the real world through internet-bridging or radio broadcast, they become opportunities for the State to interfere.

A lot of what's envisioned here in terms of censorship evasion still relies on a static and predictable model of repression that follows laws *as they are written now*. First, the law can change lightning fast. Second, we know police don't follow the law (because it was never meant to bind them). As we slip into more authoritarianism, we can see our future here in other regimes. Many countries with sophisticated internet-wide filtering still allow the use of VPNs, not because they don't understand them but because they don't need to care. Think of Iranian police going door to door and executing people who were visibly injured after protests because injury was enough "evidence" of being an enemy suitable for elimination.



Playing out an intense series of legal games in your mind is not going to help when the police decide to grab random people off the street based on how they dress. These are the real consequences we're facing when actually resisting the State.

One could continue to go "more underground," but doing so is still the re-

pression working. Plus, once one has gone far enough underground, there is a qualitative change in in one's actions and their effects. There might be networks that are disconnected from The Internet where one can browse websites hosted on a neighbor's laptop that are not top-to-bottom part of a cybernetic control structure that reports everything back to the State and corporations. There's a cyberpunk utopianism in dreaming of this. Yes, we the authors still make zines and distribute them, but this is *nothing* in comparison to Rupert Murdoch and Elon Musk being able to beam fascist slop directly into hundreds of millions of minds.

We as anarchists are uniquely constrained in how communicate with the public about our ideas. We have virtually no budget and never will. We cannot legally say the majority of things we believe. We cannot legally report on the majority of things we do. An anarchist society is far from the current one that describing it is both seditious and is an endeavor to communicate it to someone unfamiliar with its outline.[7]

Digital communication gives us scale, but it's also more traceable. Going offline doesn't solve our problems either, even as we lose reach. Look at how print media in the form of zines were used in the Prarieland case in the US to sentence anti-ICE protesters to decades in prison. Look at the case against the Zündlumpen in Germany and Austria. At Bezmotivny in Italy.

[7] This argument is expanded in "Asymmetric Speech Constraints Around Anarchism" by William Gillis. See: https://humaniterations.net/2026/09/19/asymmetric-speech-constraints/.

To Change the Material World

Imagine this. You and all your comrades have magic phones that only be unlocked by their owners' totally uncoerced free will. They are untraceable by any human means. You and your comrades all have magic servers buried on the moon that are uncensorable and can reached by anyone on Earth at any time.

So what?

Given all the powerful tools we have now, we're doing very little with them. A lack of tools and websites is not the problem. But also, the goal is not to just *have* unbreakable cryptography or unblockable websites. The goal is to change our material conditions. To change society. To change the world. Tools might help us along the way, but also they might not. They might be a distraction. The spores of change might begin to grow in cyberspace, and mycelium networks might expand there, but like the mushroom, we must break through the surface and reach the physical world. The most perfect communication and media technologies alone are only tools. We have to get out there and make the change.

In the recent past, the cost-benefit analysis of hosting counterinfo sites and running anarchist infrastructure was highly in favor of doing so. There was little repression, so even if there was little effect, it did no harm. But, the repression is mounting, and our effects are *not*. The effects we have are not primarily a result of our sick tech stacks, but rather the result of humans on the ground doing the fucking work. Putting their bodies on the line. Facing real repression.[8]

We lost Autistici/Inventati. What's next? RiseUp? Indymedia? The Anarchist Library? Kolektiva.social? Various CryptPad instances? LibCom.org? Signal?

Things that are critical infrastructure for us could be fucking *gone* with the snap of some fascist's fingers. We make the mistake of treating digital infrastructure and spaces like physical ones. A dozen evictions means a dozen police operations that can be disrupted. Riot cops have to physically show up where they could face consequences, and small number of committed radicals could bring the city to a halt. A dozen domain seizures means a dozen pushes of a button done

[8] A collective one author belongs to was raided for their IT work. We know this isn't repression free. Likewise, we understand the irony that this zine will be posted online which itself might invite repression.

anonymously from the safety of an office, and there is nothing we can do about that at this time.

We're not saying go dark. Don't shut your website down. Don't skip spinning up a new website to replace a lost NoBlogs. Don't drop off the public internet. Or maybe do all these things actually. Regardless of what choices you make, be sure you can justify them given the risks you face. Ask yourself whether the effort of setting up an e-mail sever or WordPress and the repression you might face for doing so are justifiable given the effects you hope to have.

The title of this zine came from the 2024 article "Clandestine communications in cyber-denied environments: numbers stations and radio in the 21st century" in the *Journal of Policing, Intelligence and Counter Terrorism*. It is a thought experiment by cops on how criminals might communicate and coordinate without using the internet on the assumptions that such criminals might in the near future find that malware and surveillance make use of the internet untenable (or, simply blunt repression and restriction). Cops are toying with the idea that repressed groups might leave the internet. We might want to game out such scenarios as well as every intermediate step before reaching such a point. Many of us grew up on the internet, some of us in its golden era. Losing it seems unfathomable, but we need to imagine that such a time might come.

Autistici/Inventati was shut down, and the response is to make a 1,000 copies. Maybe this is the right move. Maybe not. There are so many things we could do, and it seems unlikely that as conditions become more hostile that simply cloning Autistici/Inventati and hoping for different results is the right one.

Remember: we are more than just a series of anarchist media projects.

Appendix: Designation of Autistici/Inventati as a Specially Designated Global Terrorist

Source: https://www.state.gov/releases/office-of-the-spokesperson/2026/08/designation-of-autistici-inventati-as-a-specially-designated-global-terrorist/

Today, the Department of State, in partnership with the Department of the Treasury, is announcing the designation of Autistici/Inventati as a Specially Designated Global Terrorist.

Autistici/Inventati (A/I Collective) is an Italy-based extremist group that builds and operates the digital infrastructure for violent Antifa cells and other far-left militants across the world. A/I's cadre of radical hackers and tech developers provide a full spectrum of services — including encrypted chats and email, web hosting, secure video conferencing and streaming, anonymity shields, and a suite of other technological tools — to Marxist, anarchist, and other left-wing extremist groups in the United States, Europe, and elsewhere. These tools are specifically designed to support the operations of far-left terrorist networks, built to enable them to organize, recruit, communicate, disseminate propaganda, share target information and tactics, and carry out violent attacks – all while remaining anonymous, untraceable, and beyond the reach of the law.

The A/I Collective exclusively offers its tools and services to radical left-wing actors and manually vets all potential users for ideological affinity before granting them access to its infrastructure. The group has become a key node in a transnational campaign by violent and criminal far-left networks to destabilize the United States and its partners across Europe, the Western Hemisphere, and beyond. It currently claims to host roughly 16,000 mailboxes, 1,500 websites, 5,500 mailing lists, and 10,000 "blogs" on its custom-built platform, which militants frequently use to disseminate target information, tactical manuals and techniques, and communiqués about recent attacks.

As a result of today's action, all property and interests in property of the designated entity that are subject to U.S. jurisdiction are blocked, and all U.S. persons are generally prohibited from engaging in any transactions with them. Financial institutions and other persons may risk exposure to sanctions for engaging

in certain transactions or activities involving the designated entities, with prohibitions to include the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of the designated entities. Engaging in certain transactions involving the designated entities may also risk the imposition of secondary sanctions on participating foreign financial institutions. Violations of U.S. sanctions may result in the imposition of civil or criminal penalties on U.S. and foreign persons.

Today's action is being taken pursuant to Executive Order 13224, as amended, which targets entities and persons for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods and services to or in support of, an act of terrorism. This designation is part of a broader U.S. government effort to address the threat of transnational far-left terrorism.

A/I Collective's Support for Violent Far-Left Extremist Groups

The A/I Collective provides encrypted tools and services to numerous violent far-left extremist groups operating in the United States and around the world. Many of these groups have relied on the A/I Collective's digital infrastructure to plot or incite violent attacks, recruit others to engage in criminal activity, publish official communiqués by U.S.-designated foreign terrorist organizations, and disseminate maps of critical infrastructure, along with instructions for building improvised explosive and incendiary devices — all routed through a network of foreign servers intended to conceal criminal activity from law enforcement.

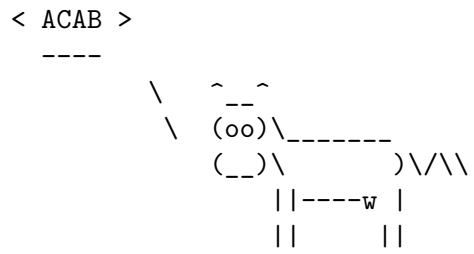
- The anarchist cells responsible for sabotaging rail systems across France, Italy, Germany, and the Netherlands in 2026, relied on A/I Collective tools and services to claim responsibility for the attacks, publish official communiqués, and disseminate manuals for constructing improvised incendiary devices to target railways and other critical infrastructure.
- The anarchist cell responsible for sabotaging the Transalpine Pipeline (TAL) in March 2026, which temporarily halted crude oil flows to Austria, Germany, and the Czech Republic, relied on A/I Collective tools and services to claim responsibility for the attack and publish official communiqués, as well as to disseminate a manifesto calling for additional attacks on critical infrastructure and referring adherents to another A/I

Collective platform, which provides detailed sabotage manuals as well as maps of vulnerable critical infrastructure across North America.

- The far-left extremist network responsible for multiple arson attacks and acts of sabotage against Germany's rail and energy infrastructure between 2011 and 2026, including a January 2026 attack on Berlin's power grid that cut power to 45,000 households and resulted in a fatality, relied on A/I Collective tools and services to claim responsibility for attacks, publish official communiques, and disseminate a manifesto calling for additional attacks on energy infrastructure worldwide.
- A far-left extremist media group claiming to be a "tool" for global militants to share "essential information" to be "acted upon," relies on A/I Collective tools and services to publish official communiqués and calls to action for U.S.-designated foreign terrorist organizations such as Armed Proletarian Justice, Informal Anarchist Federation and International Revolutionary Front (FAI/FRI), the Islamic Revolutionary Guard Corps (IRGC), Hamas, Hizballah, National Liberation Army (ELN), New People's Army (NPA), Popular Front for the Liberation of Palestine (PFLP), Palestinian Islamic Jihad (PIJ), and Revolutionary Class Self-Defense. This same group was recently cited in a federal criminal complaint against a domestic terrorist who was sentenced to 19 years in prison for targeting a federal building and police car with improvised explosive devices.
- Oregon-based Rose City Antifa has relied on A/I Collective tools and services to organize and incite violent and criminal acts domestically, including an attack on Customs and Border Patrol helicopters that led to a federal indictment. Rose City Antifa also used A/I Collective tools and services to disseminate doxing lists and release illegally obtained personal information of Federal Immigration and Customs Enforcement, along with calls for targeted attacks on ICE agents in the streets and "in their homes."
- The anarchist cell responsible for waging a violent campaign to prevent the construction of a law enforcement training center in Atlanta, Georgia, relied on A/I Collective tools and services to claim responsibility for violent attacks on law enforcement officers, disseminate doxing lists and illegally obtained private information, threaten government officials and business owners, and circulate instructions for making improvised explo-

sive and incendiary devices to be used against government buildings and local businesses. The cell remains active and still uses A/I Collective tools and services to incite violent and criminal acts against government officials, law enforcement, and critical infrastructure.

- The violent far-left extremists, "Jane's Revenge," who waged a firebombing campaign against crisis pregnancy centers across the United States, relied on A/I Collective tools and services to publish official communiqués and claims of responsibility for violent and criminal acts and to incite copycat attacks. Four members of the group were later charged for violating federal law and engaging in a "conspiracy against rights" through threats of force and intimidation.


< ACAB >
\ ^__^
\ (oo)_______
(__)\ )\/\\
||----w |
|| ||



Scrappy Capy Distro

October 2026

scrappycapydistro.info · scrappy-capy-distro@riseup.net

Posted on the internet with full self-awareness.
Don't worry. We know.