



IMAGE: HUGO CLEMENT VIA UNSPLASH/PHOTOMOSH

James Reddick
September 8th, 2026

- Cybercrime
- Government
- IndustryNews
- Privacy



Know what matters.
Act first.

In today’s fast-paced threat landscape, sorting the signal from the noise can be overwhelming.

Get started



Italian tech collective Autistici/Inventati shuts down after US terrorist designation

The Italian technology collective Autistici/Inventati (A/I) announced Sunday it will shut down operations after the U.S. government declared it a terrorist organization and imposed sanctions.

The volunteer-run collective was founded in 2001 on the principles of an open internet free from corporate and government control and was explicitly anti-capitalist and anti-fascist. Its free privacy-focused services had grown to host about 16,000 email addresses, 1,500 websites, 5,500 mailing lists and a network of some 10,000 blogs, all while pledging to protect its users' data.

On August 26, the State Department **labeled** A/I an “extremist group” operating infrastructure for “far-left militants across the world” and announced that anyone engaging with the group financially risked exposure to sanctions.

“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,” the agency claimed.

They alleged leftist groups relied on the collective’s digital infrastructure to plot violent attacks, citing examples of sabotage attacks on rail and energy systems in Europe, bombings of crisis pregnancy centers in the U.S., and protests against the Atlanta Public Safety Training Center, known among activists as “Cop City.” The State Department did not accuse the collective itself of organizing any such activity.

A/I was initially defiant, **saying** in response the U.S. had “unjustly designated us as terrorists.”

“It would like to freeze our servers and our accounts with the stroke of a pen from Washington,” they wrote. “They’re trying to wipe us out with a unilateral decree — an arbitrary one.”

The terrorist designation had a nearly immediate impact, with the operator of the .org domain — the U.S.-based Public Interest Registry — suspending the group’s domain on August 28. The same day, the collective’s Italian bank, Banca Etica, suspended its account over the sanctions risks **while saying** it “strongly condemns the use of OFAC listings for political purposes.”

On Sunday, A/I **announced** it would shut down, but would instruct users on how to back up content from blogs, mailboxes and websites.

“The possibility that our work may cause legal and financial consequences to those who are close to us — or even only have something to do with us — leaves us no choice,” they said. “Under these circumstances, we are no longer able to maintain our original mission — offering secure and non-commercial digital tools.”

An online home

Well before the emergence of social media and the tech behemoths of today, A/I arose from the idea that information on the internet should be democratized, said Mallory Knodel, executive director of the Social Web Foundation.

“The imagination was that we can use the web and the internet to build global solidarity in service of the anti-globalization movement, and we can build people power with these tools,” she said.

The need for platforms protected from government surveillance only became more acute over time, she said, especially after classified documents leaked by National Security Agency whistleblower Edward Snowden revealed the extent of the agency’s information dragnet.

“That was very mobilizing, especially in Europe, for the average person to realize the corporate infrastructure that’s based in the U.S. is obviously going to cooperate with the U.S.,” Knodel said.

Although A/I was not well known outside of certain activist circles, Knodel said the loss of the collective’s popular blogging platform, Noblogs, was “staggering.”

Anne Roth, a digital policy advisor for the leftist party at the German Parliament, started a blog on the platform in 2007 after her partner was accused of terrorism. Her nearly two decades of posts are still readable but she cannot access the administration tools. She first met some of A/I’s founders in 2001 during anti-globalization protests at the G8 summit in Genoa and trusted their mission.

“It feels like someone is sort of just stealing my home from me — my online home,” she said.

The State Department decree has also exposed rifts between the U.S. and Europe over tech hegemony and digital sovereignty. In a **statement** in support of A/I before the collective shut down, the European Digital Rights advocacy group said the sanctions undermine European sovereignty after “months of attacks on EU’s digital laws.”

The case, they said, “creates a dangerous precedent for non-commercial hosts, registrars and privacy-preserving services across Europe.”

For Roth, the fact that entities like the Public Interest Registry immediately capitulated to threats from the U.S. government should raise alarm bells for everyone.

“Just because the U.S. decides that someone is a terrorist — without any judicial procedure, without anything that one can legally go against — so just a decision by the State Department, and then all this internet governance structure falls apart,” she said. “I think that opens a lot of questions.”



Know what matters.
Act first.

Get started



Previous article

← ‘White hat’ hackers take \$47 million bounty after...

Next article

Russian suspect in bank account takeovers is...

→

James Reddick

has worked as a journalist around the world, including in Lebanon and in Cambodia, where he was Deputy Managing Editor of The Phnom Penh Post. He is also a radio and podcast producer for outlets like Snap Judgment.



BRIEFS

Japan Airlines warns of data breach as country grapples with multiple cyber incidents | October 28th, 2026

Nefilim, Hive ransomware operator given five-year-plus sentence after guilty plea | October 27th, 2026

FCC bans two devices with surveillance chips linked to Huawei | October 23rd, 2026

Quest Diagnostics warns of potential data theft after attack on lab service system | October 23rd, 2026

23andMe successor settles with California for \$6 million over cybersecurity failings | October 20th, 2026

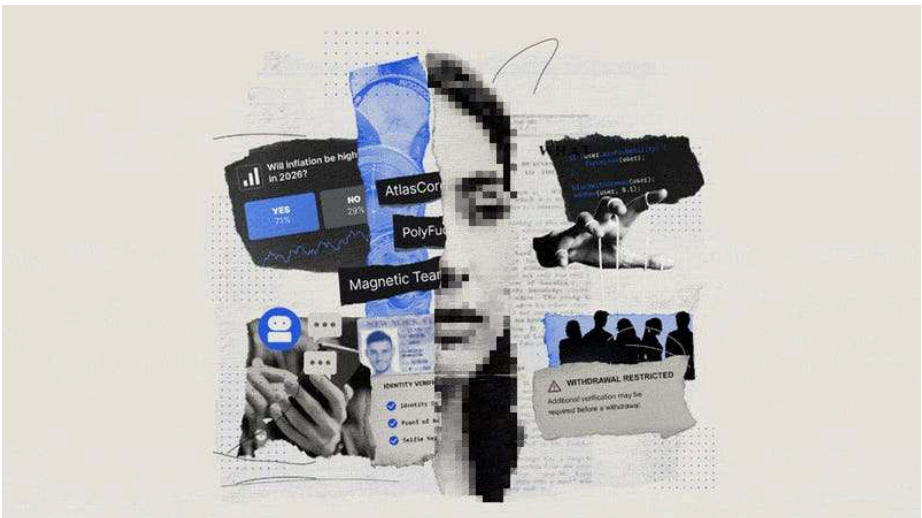
Ahold Delhaize confirms 'malicious actions' behind cyber outages affecting grocery brands | October 19th, 2026

Hackers steal customer data from major Russian hosting provider FirstVDS | October 19th, 2026

Proofpoint lines up \$6.3 billion deal for Varonis’ data security | October 16th, 2026

North Macedonian police arrest alleged administrator behind OLVX cybercrime market | October 14th, 2026

PREDICTION MARKETS EMERGE AS A NEW VERTICAL FOR TRAFFER TEAMS



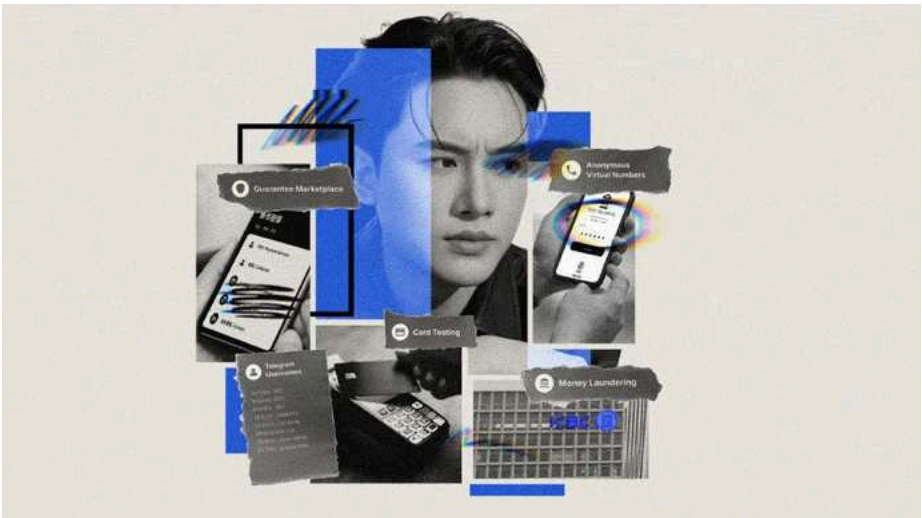
RUSSIA IS TIGHTENING INTERNET CONTROLS, LEADING TO OPERATIONAL RISKS



JAPAN ADOPTS PROACTIVE CYBER DEFENSE STRATEGY



TAJIN GROUP: GUARANTEE MARKETPLACE VENDOR INVOLVED IN PHISHING AND CHINESE MONEY LAUNDERING GROUP



H1 2026 MALWARE VULNERABILITY TRENDS

