WORK AND DIGITALISATION 04.02.2026 | Hanna Voss & Mani Mostofi & Fereidoon Bashar

Lethal blackout

Iran's blackout – and the killing it facilitated – has been a tragedy for its people. It should also serve as a warning to Europe

On 8 January 2026, as millions of Iranians took to the streets to protest, the Iranian regime engineered an internet shutdown of unprecedented scale and sophistication. The communication blackout was near-total, severing international access, domestic network connectivity, mobile data, and landline services. Under the shield of the most comprehensive communications blackout in the country's history, Iranian security forces unleashed a bloody wave of state-sanctioned violence.

The world is still learning the full extent of what happened over the past weeks. As of 27 January, the Human Rights Activists News Agency (HRANA) has confirmed that over 5900 protesters and bystanders were killed, including 100 children. The numbers continue to rise, with more than 17000 known cases still under investigation. Authorities arrested at least 42000 protesters and activists, including 325 children. Lawyers, activists, journalists, and ordinary citizens are being detained or killed, with evidence of shots to the head and the enforced disappearance of wounded protesters inside hospitals – all while most of the country remains cut off from the outside world.

The Islamic Republic's internet shutdown did more than silence Iranians. It enabled the state violence that followed.

Spreading repression

For over a decade, the Islamic Republic has spent billions of euros on an internet built not for openness, but for surveillance, censorship, and centralised control. What Iranian policymakers call the National Information Network (NIN), inspired by China's Great Firewall, was deliberately designed through public–private ventures to give the state decisive control over internet access and telecommunications. As a result, millions of websites are blocked in Iran, including platforms such as Instagram and Telegram, while citizens are pushed onto surveillance-

equipped domestic applications like Rubika for basic services such as education, payments, and banking.

This control is structural. Iran's domestic network connects to the global internet through just two government-controlled gateways, allowing authorities to throttle or sever international connectivity while maintaining limited internal services. Combined with tools such as deep packet inspection, nationwide manipulation of mobile networks, and targeted disruption of encrypted traffic, the NIN enables the state to isolate society with remarkable precision – minimising economic fallout while maximising political control.

With this infrastructure in place, the Islamic Republic routinely shuts down the internet at moments of perceived crisis, from protest movements to elections to war. The January 2026 blackout revealed the logical endpoint of this system. What is used daily to filter information and survey citizens became a tool for mass violence. With communication cut, protesters were isolated, journalists silenced, and evidence suppressed, creating conditions in which security forces could act with near-total impunity. As the UN Special Rapporteur on human rights in Iran has warned, the resulting abuses may amount to crimes against humanity. For Europe, there should be no confusion: digital authoritarianism is deadly.

Digital authoritarian practices, once proven effective, do not remain confined to distant crises. They spread.

It is also transnational. Iran's model of digital repression does not exist in isolation. Authoritarian governments are closely observing one another, sharing technologies, strategies, and lessons learned. China exports its censorship infrastructure abroad, while Iran and Russia exchange know-how on shutdowns, surveillance, and information manipulation. Each successful iteration pushes the boundaries of what can be done without triggering meaningful international consequences.

This poses a growing threat to European democracy and security. Digital authoritarian practices, once proven effective, do not remain confined to distant crises. They spread. Iran, for instance, deploys coordinated disinformation networks and conducts foreign interference operations aimed at shaping political debates within European countries. Transnational cyber repression is also on the rise, with even German Members of the European Parliament becoming targets of Iranian state-sponsored hacking campaigns. As digital isolation and state control over communication become tools of state violence, these practices

increasingly fuel instability far beyond Iran's borders.

Iranians have long lived under censorship and have become experts in circumvention. Every Iranian knows how to use VPNs to bypass state controls and often prefers encrypted messaging apps over government-promoted platforms. During internet shutdowns, informal 'helper communities' emerge, deploying ad hoc infrastructure to use tools such as DeltaChat and, where possible, connect through limited networks of Starlink terminals. These communities are not spontaneous. They are built on years of trust, technical knowledge-sharing, and community capacity-building.

Beyond statements of concern, Europe should develop a coherent digital rights strategy that institutionalises sustained support for the technologies and communities that keep people connected under repression.

Local communities in Iran and elsewhere rely on technologies and resources developed by the global internet freedom and digital rights ecosystem. This community – composed of civil society organisations, technologists, researchers, and small firms – develops anti-censorship tools and privacy-preserving technologies that disrupt digital authoritarian tactics. These efforts are essential for civilian protection, independent reporting, and early warning of mass atrocities. Yet this ecosystem remains chronically underfunded and increasingly exposed to state repression, precisely at a moment when such tools are no longer optional.

Supporting those who resist digital authoritarianism requires a holistic, multistakeholder strategy centred on resilience through diversity. This means investing in a broad portfolio of imperfect but complementary tools: decentralised messaging applications, more adaptive VPN technologies, digital security support, satellite connectivity, and sustained community capacity-building. Digital authoritarians cannot block every channel at once. A diversified approach raises the cost of censorship exponentially and forces regimes to spend increasing political and financial capital to maintain control.

Germany and the European Union are well positioned to act. Beyond statements of concern, Europe should develop a coherent digital rights strategy that institutionalises sustained support for the technologies and communities that keep people connected under repression. This includes funding the maintenance of existing tools, supporting research into emerging censorship techniques, and strengthening the communities that make these technologies usable in practice.

Iran's blackout – and the killing it facilitated – has been a tragedy for its people. It should also serve as a warning to Europe.



Hanna Voss

Hanna Voss was an editor for taz am Wochenende and now works in the international office of the Friedrich-Ebert-Stiftung in Beirut.



Mani Mostofi

Mani Mostofi is a lawyer, international legal expert and human rights activist with many years of experience in international human rights work. Among other things, he has led advocacy and research projects for UN-related initiatives and Human Rights Watch, and is now the director of Miaan.



Fereidoon Bashar

Fereidoon Bashar is the executive director of *ASL19*, a technology and exile media organisation dedicated to fighting digital authoritarianism. He works to combat threats to civil society in Iran by designing and developing solutions with and for various communities.