

Racing the Cyber Clock: Securing Civil Society Before the Mythos Window Closes

An Open Letter from Civil Society Leaders

We represent organisations deeply committed to the public good. Whether addressing humanitarian crises, ensuring access to clean water, combating hunger, providing healthcare in remote areas, fighting violence against women, or combating child sexual abuse and human trafficking, we all face common threats: cyberattacks and information manipulation. In 2024, through the [Nonprofits' Call for Cybersecurity](#), we called on governments, corporations, and philanthropies to recognise civil society as critical infrastructure and invest in its digital resilience. **Because of recent advances in frontier AI models, that call now has a deadline. We have a few months to act.**

AI models, such as Anthropic's Mythos, have shown that systems can identify software vulnerabilities and accelerate cyber operations at unprecedented speed and scale. Those capabilities are not yet widely available, but they eventually will be. This creates what we call the "Mythos Window": a brief 6-to-12-month period during which defenders have a temporary advantage. It is a rare opportunity to strengthen systems and deploy AI-powered defenses before comparable capabilities become widely available, including to cybercriminals. Major technology companies are already investing heavily in defensive AI. Civil society must too, or our organisations will be the least protected facing the fastest-growing threats.

Whilst cybercriminals and malicious state actors accelerate their adoption of AI, the digital resilience of our organisations remains underfunded. Data governance, AI implementation and cybersecurity are treated as overhead rather than essential capacity. In the age of AI, you cannot fund human impact without funding digital resilience.

We do welcome the AI industry initiatives to build the AI capacity of nonprofits. Still, helping nonprofits to use AI is not the same as protecting them from AI-enabled attacks. Our organisations need another level of ambition, both in speed and scale. The investments made over the next 6–12 months will determine whether thousands of nonprofits are equipped to defend themselves or remain vulnerable to AI-fueled threats.

It would be a civilisational failure to protect the world's largest companies with defensive AI while leaving the organisations protecting the world's most vulnerable people exposed. We therefore call on governments, philanthropies, AI companies, cybersecurity providers, and technology leaders to fund digital resilience, equip civil society for the age of AI, build shared defensive capabilities, and connect civil society to broader collective defense efforts.

1. Fund digital resilience as a core component of civil society organisational development

We call on donors to integrate digital resilience into their organisational development strategies and funding models, and we commit to making it a priority within our own organisations. Digital resilience is a strategic foundation for mission delivery, just as governance or financial sustainability. It is not an operational overhead or a technical afterthought. It is a strategic leadership decision that directly affects our ability to protect the people we serve, preserve trust, and deliver impact. Donors without ready-to-use organisational development strategies can use a dedicated funding instrument such as the [Common Good Cyber fund](#).

2. Strengthen civil society organisations for the age of AI

We call on donors, AI companies, and technology partners to help us strengthen our workforce, processes, governance, and operational resilience. We stand ready to lead this transformation. Adopting technology alone is not enough. With the right support, we will invest in cyber talent, modern resilience training, continuous testing and exercises, responsible and secure AI adoption, and stronger governance practices that help identify emerging risks such as unmanaged “Shadow AI”, insecure AI use, and the exposure of sensitive information.

3. Build shared cyber capabilities for civil society

We call on donors to invest in shared defensive capabilities that enable our organisations to identify vulnerabilities, exchange threat intelligence, detect attacks earlier, and respond more effectively. This includes strengthening and expanding Information Sharing and Analysis Centres (ISACs), trusted communities through which civil society organisations share threat intelligence, warnings, expertise, and incident response support. It also includes deploying AI-enabled capabilities that improve vulnerability management, accelerate incident response, and provide access to expertise and services that no single organisation can build or afford alone.

4. Connect civil society to collective digital defense

We call on public, private, and philanthropic partners to connect the civil society sector to collective defense ecosystems, including threat intelligence sharing communities, joint crisis exercises, and coordinated incident response efforts. As AI accelerates cyber threats, the value of collective defense is growing just as quickly. Governments, technology companies, cybersecurity providers, and critical infrastructure operators are increasingly sharing intelligence, coordinating responses, and building common defenses. Civil society must not be

left behind. When one organisation identifies a threat, hundreds of others should benefit from that knowledge. In the age of AI, resilience will increasingly depend not on how fast any one organisation can respond, but on how fast entire communities can learn and act together.

These calls aim to trigger urgent actions, and aim for a long term impact. **We do not start from scratch. Civil society invested in its digital resilience for years. We need to strengthen, connect, and scale what already works before the Mythos Window closes.**

The cost of inaction will be measured not only in compromised systems, but in disrupted humanitarian operations, weakened democratic institutions, threatened human rights defenders, and vulnerable communities left unprotected.

Together, we can ensure that the organisations protecting the world's most vulnerable people are not left defenseless in the age of AI.

Signatories

Chief Executive Officers, Executive Directors, Secretaries-General, and other leaders of civil society organisations committed to protecting the public good.

To sign the petition:

<https://tally.so/r/RGIN5j>