

18 February 2022

## **Cyberattacks on Ukraine's infrastructure and civil society violate human rights**

Cyberattacks targeting Ukraine's critical infrastructure are undermining people's human rights. The most recent attacks on [January 13-14](#) and [February 15, 2022](#) targeted essential public service infrastructure, including both major national banks and the e-governance platform Diia, which provides people with access to more than 50 public services ranging from supporting parents of newborns to opening a business to providing proof of COVID-19 vaccination. Cyberwarfare is an assault on human rights, and has devastating effects on people's privacy, freedom of expression, safety and security, and access to information. Cyberattacks can wipe essential systems such as electrical grids, hospitals, and governmental services offline, exacerbating tensions, worsening crises, and endangering lives.

Cyber operations [targeting](#) journalists, civil society organizations, and human rights defenders are particularly alarming and should be prohibited in all circumstances. Individuals who work in defense of civil liberties, rights, and democracy are themselves a form of critical infrastructure, often providing direct services and advocating for the needs of the most vulnerable.

### **CALL TO ACTION**

The international community must come together to provide additional support to Ukraine and its human rights defenders in increasing their resilience to ongoing cyber threats, as well as investigating prior attacks and holding perpetrators to account.

#### **1. PROVIDE DIRECT SUPPORT TO JOURNALISTS, CIVIL SOCIETY, AND HUMAN RIGHTS DEFENDERS**

There is a pressing need to provide Ukrainian civil society with technical means to protect both themselves and the sensitive data on their servers and devices, as well as to prevent future attacks. We urge **tech companies, nonprofits, and funders** to expand their support programs and provide Ukrainian activists with free and secure VPNs, antivirus programs, encryption, DDoS protection, and other essential digital tools, equipment, and services.

*Civil society organizations, human rights defenders, and journalists in need of digital security assistance can connect with Access Now's 24/7 [Digital Security Helpline](#) at [help@accessnow.org](mailto:help@accessnow.org).*

#### **2. ESTABLISH AND UPHOLD CLEAR, PEOPLE-FIRST CYBERSECURITY STANDARDS**

**UN bodies and other international organizations** advancing cybersecurity and cybercrime law and norms should center human rights in their work, take a human-centric approach, and condemn those who permit or perpetrate cyberattacks.

**States** participating in the upcoming 49th Session of the UN Human Rights Council should condemn cyberwarfare as a threat to human rights in Ukraine, call for an investigation of their human rights impacts, and take steps to hold perpetrators accountable. Further, they should ensure that resolutions on human rights defenders, disinformation, and related topics all strengthen protections for digital rights and raise the human rights impacts of surveillance, censorship, and disruptions to connectivity.

### **3. GUARD AGAINST ATTEMPTS TO ESCALATE AND EXPLOIT CURRENT TENSIONS**

**Social media platforms** and other technology firms must make the investments necessary to prevent the spread of [disinformation campaigns](#) designed to escalate tensions in the conflict between Russia and Ukraine.

Likewise, both **policymakers and internet service providers** should refrain from using misinformation as a justification for restricting access to the internet or communications platforms. Limiting [free expression](#) and access to information is particularly [dangerous](#) for vulnerable individuals in moments of unrest and uncertainty, and only puts them further at risk.

**Governments and technology firms** must also vigilantly guard against rogue actors seeking to exploit current tensions to camouflage their disruptive, criminal activities. It is essential to fully investigate any cyber attacks that undermine human rights, even when some attacks may not be directly attributed to specific government actors, as leaving them unaddressed cultivates an overall environment of impunity.

---

## **SIGNATORIES**

Access Now  
Centre for Democracy and Rule of Law  
Digital Security Lab Ukraine  
European Digital Rights (EDRI)