

Ukraine conflict and the work of the CyberPeace Institute

The escalation of hostilities further to the 26 February 2022 invasion of Ukraine by the military forces of the Russian Federation has led to devastating humanitarian consequences for Ukraine's civilian population.


In this situation of international armed conflict, Ukraine is subjected to attacks from traditional weapons as well as cyberattacks and operations. Cyberattacks have taken the form of attacks which aim to disrupt institutions, infrastructure, and to limit access to information and/or spread disinformation.

The CyberPeace Institute is tracking how cyberattacks and operations are targeting civilians, civilian objects and infrastructure essential for the survival of the civilian population.

The importance of tracking cyberattacks in Ukraine

There has been a significant escalation in the number of reported cyberattacks against Ukrainian institutions, organizations and the wider civilian population. This is important in order to identify harm to the civilian population, and to infrastructure essential for the survival of the civilian population, including humanitarian non-governmental organizations carrying out critical services for people in need.

Attacks on infrastructure such as energy, water and sanitation facilities, healthcare, financial institutions, transport and communication services can have devastating consequences on the civilian population. Cyberattacks also sow distrust and limit access to accurate information or spread false information.



UKRAINE:
Timeline of Cyberattacks
on critical infrastructure
and civilian objects

On their own, and/or combined with kinetic attacks, cyberattacks can also be highly disruptive and create a sense of fear and uncertainty and accelerate violence and/or the displacement of people.

Information on cyberattacks can also be shared with the CyberPeace Institute for possible inclusion in the Timeline of Cyberattacks.

Call to respect international humanitarian law

The CyberPeace Institute calls upon all actors to spare civilians and other protected persons, civilian objects and infrastructure which are ensuring the delivery of essential services in line with international humanitarian law. This is an obligation of all parties to the armed conflict. Respecting this law is important to save lives and reduce suffering.

Like any other weapon used in armed conflict, the use of cyber tools is subject to restrictions. International Humanitarian Law (IHL) applies to cyber operations during armed conflicts. The important legal principles of distinction (distinguish at all times between military objectives and civilian objects) and proportionality (prohibit attacks expected to cause excessive civilian harm) must be respected. These principles also have a direct bearing on cyber operations during armed conflicts in order to protect the civilian population against the effects of such operations.

In the future, it will be important to use the information on cyberattacks to identify developments or clarifications of the law in relation to the use of cyber operations in armed conflicts, and for accountability including in any future judicial proceedings.

CyberPeace Builders




The CyberPeace Institute provides volunteers with practical ways to help vulnerable civilian communities to build resilience against cyberattacks through the **CyberPeace Builders**.



The [CyberPeace Builders](#) is a cybersecurity volunteer network operated by the CyberPeace Institute, created for the sole purpose to help humanitarian organizations elevate their cybersecurity resilience. The network is made of cybersecurity experts carefully selected from reputable companies, matched with selected NGOs for short-term punctual engagements.

The **CyberPeace Institute** is a non governmental organization whose mission is to reduce the harms from cyberattacks on people's lives worldwide, provide assistance to vulnerable communities, and call for responsible cyber behaviour, accountability and, ultimately, cyberpeace.

CyberPeace Institute
Campus Biotech Innovation
Park Avenue de Sécheron 15
1202 Geneva, Switzerland

 cyberpeaceinstitute.org
 @CyberPeace Institute
 @CyberpeaceInst