UKRAINE: Timeline of Cyberattacks

cyberpeaceinstitute.org/ukraine-timeline-of-cyberattacks

February 24, 2022

Against the backdrop of the military invasion of Ukraine, the CyberPeace Institute is tracking how cyberattacks and operations are, and have been, targeting critical infrastructure and civilian objects.

In recent weeks there has been a significant escalation in the number of reported cyberattacks against Ukrainian institutions, organizations, including humanitarian NGOs, and the wider population. Ukraine is no stranger to being on the receiving-end of cyberattacks and the timeline below tracks the most significant incidents to date.

The importance of tracking cyberattacks in Ukraine

The tracking of cyberattacks and incidents as they become public is important in order to record these attacks and identify – where possible – the harm and risks for civilian populations. Cyberattacks affect people and risk lives. 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.

Harm caused by cyberattacks during an armed conflict

The targeting of critical infrastructure raises particular concern as this infrastructure is essential for the survival of the civilian population. Attacks on infrastructure such as energy, water, healthcare, financial institutions, transport and communication services can have devastating consequences on the civilian population. NGOs responding to the humanitarian needs of the population in Ukraine and neighboring countries are targeted by cyberattacks in order to disrupt their activities.

Beyond the risks to critical infrastructure and civilian objects, cyberattacks sow distrust and limit access to accurate information or spread false information. They can also be highly disruptive and create a sense of fear and uncertainty and even lead to the eventual displacement of people.

Civilian populations are protected under international humanitarian law
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) have a direct bearing on cyber operations during armed conflicts in order to protect the civilian population against the effects of such operations.

Frequently Asked Questions on the laws of armed conflict with a focus on cyber.

Ukraine conflict and the work of the CyberPeace Institute
The CyberPeace Institute's mission is to reduce the scale and frequency of cyberattacks against vulnerable communities, provide assistance and advocate for respect of laws and norms. Thus, documenting cyberattacks is important to understand the harm caused to people. The CyberPeace Builders program is a trustworthy volunteer network designed to help humanitarian NGOs strengthen their cybersecurity.

Factsheet on Ukraine conflict and the work of the CyberPeace Institute.

Call for Support from the CyberPeace Institute
Crucial to the work of the Institute are open source research by our small team of experts. Can you support the Institute's data collection?

- If you have the capabilities to support our ongoing work to collect data on cyberattacks related to the armed conflict in Ukraine and/or cases of cyberattacks against the healthcare sector and humanitarian NGOs, we would appreciate hearing from you.
- We seek online volunteers who can dedicate a few hours of their time and expertise to support the work of the Institute.
- Find out more by contacting .