IMUN 2026 Research Report

Human Rights Council #1: The question of safeguarding digital communication infrastructure during armed conflict.

Global conflicts continuously emerge; however, an increasing number involve warfare on digital as well as physical fronts. cyberwarfare and cyber defense systems. The International Committee of the Red Cross (ICRC) defines cyberwarfare as "means and methods of warfare that rely on information technology and are used in situations of armed conflict" ("Cyber Warfare"). The dangers of cyberwarfare stem from its potential destruction of unprotected and essential civilian infrastructure, including telecommunications, transportation, governmental, financial systems which rely on functioning Information and Communication Technologies (ICTs) ("Cyber Operations"). International Humanitarian Law (IHL), also known as the laws of war, aims to "…protect civilian populations and other protected persons and objects, including against the risks arising from ICT activities" (Zhou). These laws were catalyzed by Estonia's 2007 suffering of a 'distributed denial of service (DDoS) attack, the resolution of which troubled the International Community because regulations had been written for physical weapons only. As a result, the modified frameworks prohibit targeting civilians and civilian objects, and apply to all types of warfare, including cyberwarfare. However, it is exceedingly difficult to classify cyberattacks as violations of IHL due to the indirect nature of digital disruptions on vital civilian systems and physical infrastructure (Zhou). Furthermore, with the rapid development of modern technologies, it has become challenging to apply laws to ongoing wars. Specifically, it is difficult to establish who is responsible for launching the attack, and to differentiate between civilian and military computer networks, considering the prevalence of dual-use infrastructure. According to the ICRC, cyberattacks are controversial considering the 54th Customary Rule which states that

“Attacking, destroying, removing or rendering useless objects indispensable to the survival of the civilian population is prohibited” (“Customary IHL – Rule"). Particularly, cyberattacks on communication infrastructure can legally be considered an ‘attack’ considering that “an operation causing violent effects can be an attack even if the means used to cause those effects are not violent” (“Communication Blackouts”). The international community continues to debate questions of protecting civilian data, the risks that arise when civilian infrastructure is incorporated into warfare, and how medical and humanitarian aid can be safeguarded against ICT activities and cyber-attacks.

Despite difficulty enforcing restrictions on cyberwarfare, recent conflicts have highlighted civilian vulnerabilities to attacks on digital communication infrastructure. In the Russo-Ukrainian war the Security Service of Ukraine (SSU) has neutralized more than 16,000 Russian cyberattacks on telecommunications providers, government institutions, defense structures, while causing disruptions to internet services (Katsimon). The resulting inaccessibility to online navigation, emergency services, and humanitarian assistance raises grave concerns about the role of organizations such as the United Nations in limiting impact on human lives. For instance, recurring attacks on Ukrainian communication infrastructure damaged and deactivated localized electronic air raid alert systems, compromising the awareness and well-being of citizens. Similarly, seen in the Gaza conflict with Israeli cyberattacks against civilians. Specifically, Israel regulates Palestinian Information and Communication Technologies (ICTs), recurringly imposing communication blackouts and internet shutdowns on the civilian population of the Gaza Strip. This is partially caused by the absence of electricity and fuel, considering that internet providers are unable to generate power for network maintenance. It is vital to consider that physical attacks also pose threats to digital infrastructure, and in addition, pose direct danger

to civilian populations. By December 2023, Israeli forces had demolished all of Gaza's communication networks, implementing a siege and blockade of critical lifeline supplies and infrastructures which leaves 1.9 million people internally displaced ("Communication Blackouts"). These attacks have been hotly objected to by the Electronic Frontier Foundation, Human Rights Watch, and the World Health Organization, among other international organizations, leading to disputes about the legality of imposing communication blackouts under international humanitarian law (IHL). Similar discourse is required to address the roles of occupying powers regulating internet services and their access within occupied territories.

Consequently, delegates should focus on the devastating security, social and humanitarian, economic consequences of cyberoperations against critical information infrastructure, formulating definitions, regulations, and punishments for violating states. Consider differentiating between physical attacks on digital communications and cyberattacks. Also, discuss prevention frameworks and strategies that aim to protect civilian data, isolate networks to stop attackers from moving laterally, relocating critical communication data to outside active combat zones.

Works Cited

"Communication Blackouts: Israeli Cyberattacks Against Civilians in Gaza." *OpinioJuris*, 20 Mar. 2024, opiniojuris.org/2024/03/20/communication-blackouts-israeli-cyberattacks-against-civilians-in-gaza/. Accessed 2 July 2026.

"Customary IHL - Rule 54." *International Humanitarian Law Databases*, ihl-databases.icrc.org/en/customary-ihl/v1/rule54. Accessed 2 July 2026.

"Cyber Operations During Armed Conflicts." *International Committee of the Red Cross*, 11 Oct. 2021, www.icrc.org/en/document/cyber-warfare. Accessed 24 May 2026.

"Cyber Warfare." *Casebook ICRC*, casebook.icrc.org/a_to_z/glossary/cyber-warfare. Accessed 24 May 2026.

Katsimon, Olha. "Russia has carried out over 16,000 cyberattacks against Ukraine. Italy has announced new aid for cyber projects." *Liga*, 1 July 2026, news.liga.net/en/war/news/russia-has-carried-out-over-16-000-cyberattacks-against-ukraine-italy-has-announced-new-aid-for-cyber-projects. Accessed 2 July 2026.

Zhou, Wen. "Upholding IHL protections against the risks of ICT activities in armed conflict." *ICRC Blog*, 23 Apr. 2026, blogs.icrc.org/law-and-policy/2026/04/23/upholding-ihl-protections-against-the-risks-of-ict-activities-in-armed-conflict/. Accessed 25 May 2026.