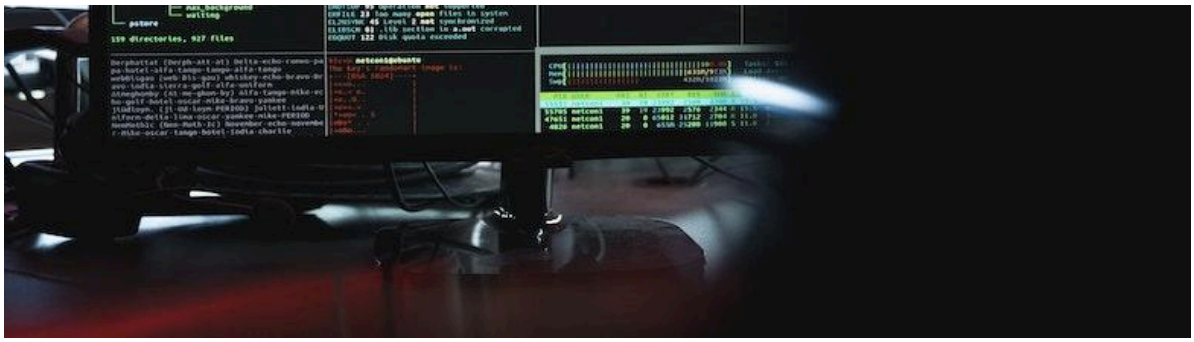

In our digitally connected and technology-dependent world, cyber-attacks on critical infrastructure such as electric power grids, water treatment facilities, and industrial control systems have far-reaching safety and security consequences. When these attacks are directed at civilian targets in an armed conflict, they can and should be considered war crimes.

Since Russia's full-scale invasion of Ukraine in February 2022, the world has witnessed the worst horrors of war, shocking the conscience of the global community. However, unlike the bombardment of civilians in Syria, imprisonment of Uighurs in China, or violent crackdown on protesters in Iran, multiple forums exist for adjudicating war crimes committed in Ukraine. These include the International Criminal Court (ICC), Ukraine's national courts, the national courts of other countries pursuant to the principle of universal jurisdiction, and possibly a new hybrid or international tribunal that could be established by the United Nations General Assembly.

The numerous avenues for accountability for international crimes committed in the Russia-Ukraine conflict allow for creative thinking about how to achieve many goals of the international criminal justice system. In addition to the specific objectives of establishing the truth, holding the perpetrator accountable, and compensating the victim with reparations, international judicial bodies can crystalize norms, strengthen legal protections for civilians, and set innovative legal precedents that advance and modernize international law.

As an early conflict to feature a major cyber power's deployment of cyber means and methods of warfare, this conflict presents a unique opportunity to achieve these broader objectives. In March 2023, Berkeley Law's Human Rights Center filed a second "article 15 communication" with the ICC Prosecutor on cyber war crimes in Ukraine. The submission presents the case for charging five Russian cyber-attacks against Ukraine's critical infrastructure as war crimes. This post summarizes the key legal questions raised in the submission, namely: what constitutes "attacks," "objects," and "military objectives" in cyberspace?

What Constitutes an "Attack" in Cyberspace?

A threshold issue is whether a cyber operation constitutes an "attack" under international humanitarian law (IHL) and article 8 of the Rome Statute. Russian cyber operations against Ukraine encompass a range of

be *physically* violent or result in *physical* consequences, although that is now many legal traditionalists interpret it.

This narrow interpretation of the law, however, is at odds with the object and purpose of IHL, as well as with society's broadening interpretation of the word "violence," which has come to be used to describe acts that are not just physical, but psychological and emotional, economic, or digital. Thus, in 2023, it is appropriate to adopt a broad interpretation of the term "violence."

The issue of what constitutes an "attack" gets more complicated when applied in cyberspace. It is widely accepted by States and academics that cyber operations expected to cause death, injury, or physical damage constitute attacks under IHL. Rule 92 of the ***Tallinn Manual 2.0*** reflects this position. However, a growing contingent of scholars and States has recognized cyber operations that cause a loss of functionality (without physical damage) as attacks. Under this approach, loss of functionality occurs "where the targeted equipment or systems no longer provide the service for which they were implemented, whether temporarily or permanently, reversibly or not." The ICRC and key ICC member States such as Japan, Germany, and France have adopted this position. The Human Rights Center's submission similarly concludes that treating loss of functionality as an attack is most consistent with the object and purpose of IHL's rules on the conduct of hostilities, and strongly advocates that the ICC adopt this approach.

What Constitutes an "Object" in Cyberspace?

A second issue is whether the attack was directed at "civilian objects," which raises the question of whether electronic data constitute an object. During this conflict, Russian perpetrators have deployed more than 15 types of wipers, a type of malware designed to destroy data and systems. Given that the target of cyber-attacks is often civilian, we must consider whether such data qualify as objects under IHL and the Rome Statute.

While the Rome Statute refers to attacks on "objects" in several provisions, it does not define this term. AP I defines civilian objects simply as those that are "not military objectives," which is not helpful in addressing whether an intangible item of value fits the definition. In general, there are several alternative definitions for the term "object," some of which explicitly include the word "material" or "physical," but others that do not. One of the legal definitions provided describes an object as "something toward which thought, feeling, or action is directed." In our increasingly digitized world, removing the tangibility requirement is logical. Otherwise, a strict interpretation would lead to the contradictory outcome that, for example, hard copies of wills and medical files are protected, while their corresponding digital versions are not.

During the drafting of the *Tallinn Manual*, members of the International Group of Experts diverged on whether data constitute an object. However, in recent years, an increasing number of scholars has shifted its position to accept that, at least in some circumstances, data are objects. The *Tallinn Manual* conversations occurred before the full-scale Russian invasion of Ukraine and the aggressive, unprecedented use of wipers. This type of scenario was never offered as a hypothetical case during their debates. Now that we have a real-world example of how

Finally, the prosecution must prove that the civilian objects were not "military objectives." This is a challenging feat when dealing with digital systems that might support both civilian services and military operations. Article 52 of AP I defines military objectives as "objects which by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage." In addition, Article 52(3) specifies that, "In case of doubt whether an object which is normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used." Thus, there is a treaty-based presumption that objects enjoy civilian status.

The definition translates into a two-prong test. First, the object must, by its nature, location, purpose or use, make an effective contribution to military action. The "nature" of an object denotes its intrinsic character. It must be endowed with some inherent attribute which makes an effective contribution to military action, for example, a military base or weapons depot. The "purpose" of a military objective is concerned with the intended future use of an object, while that of "use" is concerned with its present function. The "location" of an objective concerns a specific land area that can be regarded *per se* as a military objective, for example, a mountain pass of strategic value. Critically, these factors are predicated on the reasonably anticipated intentions and actual activity of the adversary, not on hypothetical scenarios or guesswork. While military lawyers tend to take a permissive interpretation of "military objectives," overly broad interpretations that place military necessity over civilian protection are dangerous and undermine the object and purpose of AP I, which was intended to secure greater protections for civilians.

The second prong requires that the object's destruction, capture, or neutralization, in the circumstances ruling at the time, must offer a definite military advantage. Similarly, this turns on the interpretation of what constitutes a definite military advantage at the time. It has been observed that the Russian military intelligence (GRU) units involved in offensive cyber operations frequently engage in gratuitous cyber-attacks with little military advantage to be gained. As one U.S. Assistant Attorney General describes it, Russia weaponizes its cyber capabilities to "wantonly [cause] unprecedented damage to pursue small tactical advantages and to satisfy fits of spite."

This assessment gets more complicated in cyberspace, where civilian and military infrastructure are increasingly intertwined. While some objects support the dual uses of both military campaigns and ordinary civilian life, IHL does not formally recognize such a category, instead treating dual-use objects as military objectives subject to a proportionality analysis. Thus, even if an object is a military objective under IHL, armed forces must "take all feasible precautions in the choice of means and methods of attack" to avoid "incidental loss of civilian life, injury to civilians and damage to civilian objects." Thus, a related consideration when it comes to dual-use objects is how to apply a proportionality analysis to the cyber context.

Although dual-use objects have historically been viewed as legitimate military targets regardless of the degree to which they support civilian life, such interpretations are outdated in the Digital Age. They are also fundamentally

Human Rights Center's submission to the ICC is bigger than any one individual victim or perpetrator, and it is intended for greater impact beyond the borders of Ukraine. The submission addresses a new kind of malevolence that is in its infancy but presents a mounting threat to all mankind. Prosecuting cyber–attacks as war crimes would be an unprecedented but critically important step towards modernizing the laws of armed conflict—laws that are at risk of becoming obsolete if they cannot be interpreted broadly with due consideration for the evolution of technology, weapons, and warfighting.

***

Lindsay Freeman, JD, Adv LLM, is Director of Law and Policy of the Technology Program at the UC Berkeley Human Rights Center.

Photo credit: Pexels

RELATED POSTS

Symposium Intro: Ukraine-Russia Armed Conflict
by Sean Watts, Winston Williams, Ronald Alcala
February 28, 2022
–
Russia's "Special Military Operation" and the (Claimed) Right of Self-Defense
by Michael N. Schmitt
February 28, 2022
–
Legal Status of Ukraine's Resistance Forces
by Ronald Alcala and Steve Szymanski
February 28, 2022
–
Cluster Munitions and the Ukraine War
by William H. Boothby
February 28, 2022
–
Neutrality in the War against Ukraine
by Wolff Heintschel von Heinegg
March 1, 2022