https://doi.org/10.59862/k7m2x9q4r8/04

Chapter 4

Research Data during an Armed Conflict: An Overlooked Target?

ALEKSI KAJANDER
NATO Cooperative Cyber Defence Centre of Excellence,
Department of Law, Tallinn University of Technology
ORCID: 0000-0001-7164-2973

Abstract: The protection of digital data remains uncertain under international humanitarian law, with some states recognizing digital data as an object, while others do not. Current international humanitarian law primarily protects visible and tangible civilian objects, whereby digital data is not always recognized as an object and as such is subject to fewer protections than corporeal civilian objects. As a result, important civilian datasets may be at risk during an armed conflict, including research data held by educational institutions such as universities. This paper will examine the existing protections for civilian data under international humanitarian law, in particular under Articles 52, 57, and 58 of Additional Protocol I as well as current state positions on the status of data during armed conflict. Furthermore, this paper will offer practical recommendations to educational institutions on how to protect their research data during an armed conflict under current international humanitarian law.

Keywords: IHL, data, object, cyber warfare, cyber operations, research data, armed conflict

Modern armed conflicts, as demonstrated by the Ukraine war, incorporate a significant cyber component in them.[1] Ever since Stuxnet, it has become clear that cyber operations can deliver the same impact as conventional

[1] Lika Lagvilava, "The 2022–2023 Russia Ukraine War and Cyberspace Threats," *Future Human Image* 19 (2023), 43.

weapons and be considered armed attacks under international law.[2] However, while cyber operations can produce physical damage, often their impact is non-physical, such as the deletion or alteration of data. This creates the potential for a loophole in the protection provided by international humanitarian law (IHL) during an armed conflict, as while (physical) civilian objects are protected from attack, it is not quite clear whether data truly qualifies as an object. Although this may potentially affect many different types of data important for civilians, it is perhaps underappreciated that it can compromise significant scientific research data held at universities. This paper will examine the threat to research data during an armed conflict under IHL, and what measures may be recommended for research institutions to minimize their exposure.

Status of Universities under IHL

Under IHL, it is well established that civilian objects are protected and shall not be made the object of an attack under Article 52 of Additional Protocol I to the Geneva Conventions. Some objects, such as medical facilities are subject to additional protection with specific provisions that ensure that not only is it forbidden to attack them, but that they must be respected at all times and that their operation shall not be interfered with.[3] Similarly, objects essential for the survival of the populace,[4] cultural objects, and places of worship have[5] similar broad protections that go beyond merely not attacking. It may therefore be surprising that universities or other such research or educational institutions do not have a similar special protection.[6] Instead, universities and other places of learning or research are treated the same as any other civilian object.

---

[2] Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017), 342.

[3] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31, Article 19.

[4] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 54.

[5] Ibid, Article 53.

[6] Gregory Bart, "The Ambiguous Protection of Schools under the Law of War – Time for Parity with Hospitals and Religious Buildings," *Georgetown Journal of International Law* 40, no. 2 (2009), 427.

Initially, especially to a non-IHL lawyer, this may seem like trivial differences. However, with the advent of cyber operations during armed conflict, the lack of special protection has become increasingly significant. With cyber operations, the additional protections provided by broader wording such as "shall respect,"[7] "any acts of hostility,"[8] and "render useless"[9] has increased meaningfully. The prohibition against attacking only extends to civilian "objects," which are defined in the 1987 Commentary to Additional Protocol I as "visible and tangible."[10] While this was fine in 1987, since then, "immaterial" digital data, which one arguably cannot see or touch, has become incredibly important in many civilian contexts. As a result, a view that data is not an object under IHL has become prominent,[11] whereby civilian data could, as a result, be subject to a loophole where, as it is not an object, it could be attacked through cyber means, unlike physical civilian objects. Therefore, the previously mentioned broader protections have arguably increased in value as they are wide enough to encompass essentially any hostile activity aimed at them, and hence they arguably provide more protection against cyber operations.

To convey how controversial the classification of data as an object currently is, the available state positions on the Cooperative Cyber Defence Centre of Excellence's (CCDCOE) CyberLaw Toolkit on cyber and international law provide a demonstration. Ten states have provided[12] a position that includes their view on whether data is an object or not under IHL. Six of these consider data as an object,[13] two consider that more discussions are

[7] Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31, Article 19.

[8] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 53.

[9] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, Article 54.

[10] International Committee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff Publishers, 1987), para. 2008.

[11] Ori Pomson, "'Objects'? The Legal Status of Computer Data under International Humanitarian Law," *Journal of Conflict & Security Law* 28, no. 2 (2023), 354.

[12] Cyber Law Toolkit, "Scenario 12: Cyber Operations Against Computer Data," accessed November 9, 2024, https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data.

[13] Austria (2024), Costa Rica (2023), Finland (2020), France (2019), Germany (2021), and Romania (2021) (preliminarily).

required and are thus undecided,[14] and finally, two do not consider data as an object.[15] The views of the two states that do not recognize data as an object are rather similar. In both cases, they do not consider data as an object by itself, although if a cyber operation foreseeably causes injury, death, or damage to (physical) objects, they would consider an "attack" under IHL and as such subject it to the applicable rules on targeting.

This miniature snapshot into state opinion is valuable for research facilities to be aware of, as the deletion of research data is unlikely to foreseeably result in a loss of life, injury, or damage to (physical) objects. As such, they must recognize that in the views of some countries it does not receive the same protection under IHL as physical objects, and therefore, they should not expect the same protection as they might for, for example, their buildings. Consequently, as discussions are still ongoing, it would be valuable for research facilities to make their opinions known and contribute to the discussion on the topic.

Lessons from the Ukraine War

With this in mind, the concern for research data becomes readily evident. Moreover, the ongoing armed conflict in Ukraine has already demonstrated that such cyber operations do in fact occur. The Main Directorate of Intelligence of Ukraine's Ministry of Defence reported that two petabytes (200 million gigabytes) of data were deleted from Russia's Far Eastern Scientific

[14] Federal Department of Foreign Affairs. (2021). Switzerland's position paper on the application of international law in cyberspace. https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf; United Nations General Assembly. (2021). Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, A/76/136, p. 23.

[15] Roy Schöndorf, "Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations," *US Naval War College International Law Studies*, 97 (2021), 401; Jeppe Kjelgaard and Ulf Melgaard, "Denmark's Position Paper on the Application of International Law in Cyberspace," *Nordic Journal of International Law*, 92(3) (2023), 455.

Research Centre of Space Hydrometeorology.[16] Among its other functions, the research center in question provides and handles satellite data and imagery to the Russian Ministry of Defence as well as other departments of the Russian state.[17] The operation raises an important observation that all research facilities should be aware of, that is to say, can they be construed as being "dual use," which may make them targetable from an IHL perspective?

While "dual use" is not technically a formal category of objects under IHL,[18] the concept is useful when discussing objects that have both a military and a civilian use. The appropriate assessment of an object from an IHL perspective is under Article 52 (2) whereby military objects are those which by their "nature, location, purpose, or use make an effective contribution to military action" and which if neutralized provides a "definite military advantage." As noted by the 1987 Commentary, establishments that produce civilian goods that can be used for the benefit of the army have a "dual function" whereby they may be attacked if the definite military advantage anticipated is proportional to the collateral to civilians. This is particularly relevant for research facilities that are expected to enable the production through research of either military technologies, services, or goods, or similar dual-use products that may benefit the armed forces in the future. In such situations, a research facility can be targetable under IHL regardless of the status of data as an object.

Furthermore, under Article 57 (2) of AP I, belligerents have an obligation to choose means and methods that minimize the expected collateral damage to civilians or objects. Therefore, a cyber operation that wipes the research data that may give rise to a military advantage in the future is immensely justifiable compared to kinetic methods, and as such, during an armed conflict might arguably be said to be the preferable means of dealing with such research facilities. For it is difficult to foresee a loss of civilian life when research data is deleted, and no physical damage is produced. As such, it could be argued

[16] Main Directorate of Intelligence (Ukraine), "Знищили ворожу 'планєту' – деталі кібератаки проти центру космічної гідрометеорології рф," January 24, 2024, https://gur.gov.ua/content/znyshchyly-vorozhu-planietu-detali-kiberataky-proty-tsentru-kosmichnoi-hidrometeorolohii-rf.html.

[17] Ibid.

[18] Oona Hathaway, Azmat Khan and Mara Revkin, "The Dangerous Rise of Dual Use Objects in War," *Duke Law School Public Law & Legal Theory Series*, no. 2024–56 (2024), 17.

that the belligerents should if, possible, prefer cyber means in such situations due to Article 52 (2) of AP I over conventional kinetic alternatives to preserve civilian life. Therefore, the cyber threat to research facilities during an armed conflict is significant.

Recommendations for Research Facilities

An often-overlooked aspect of IHL is the obligation for both parties to take precautions against the effects of attacks, as codified under Article 58 of AP I. The passive precautions noted in Article 58 are intended to provide an additional layer of protection to civilians by pre-emptively placing away from harm's way during military operations. In particular, sub-paragraph (b) which requires parties to the "maximum extent feasible" "avoid locating military objectives within or near densely populated areas," should be considered by research facilities. If a research facility is dedicated to such lines of research that can be assessed to give a definite military advantage to the armed forces, they should, where possible, be located away from other parts of such centers that are purely civilian in function and purpose. As per the commentary of 1987,[19] it is clear that this applies to the physical buildings that constitute the potential military object.

However, in the modern context, it would be advisable to extend the interpretation of this obligation not only to the physical building, but also its digital infrastructure. For, if either military or dual-use type research data is located, processed, and stored separately from non-military research data, this in effect translates 58 (b) to the modern environment. This separation would serve as a passive protective measure against a cyber operation targeting research data during an armed conflict. For, if the adversary would conduct a cyber operation intended to alter or wipe data, it would be limited to the separate network or storage that houses the dual-use or military data. Thus, the civilian research should be left unharmed, at least with an adversary who respects the principle of distinction under Article 48 of AP I.

Moreover, even if the data would not be recognized as an object, as it wo-

[19] International Committee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff Publishers, 1987), para. 2251.

uld take extra effort that must purposefully be targeted towards the civilian data, this would likely violate the "constant care" obligation a belligerent has under Article 57 (1). Under Article 57(1) a belligerent must, in their "military operations," take "constant care to spare the civilian population, civilians, and civilian objects." The word "military operations" is notable as it is broader than the protection against "attacks," which again in the modern context is valuable. For cyber operations may not always be attacks, but they are always "military operations" as this term includes, as per the commentary,[20] "other activities whatsoever carried out by the armed forces," which cyber operations will inevitably fall under.

Thus, it is arguably not possible to justify a purposeful effort to harm civilian data on separate infrastructure or network when the military or dual -purpose data is separate and independent of it. By contrast, if they are housed on the same network, infrastructure, or storage, they are immediately at more risk than if they are housed separately. For an adversary could relatively easily justify wiping all the data they encounter in the system of a research facility that is providing a definite military advantage through its data as being proportionate. This would be due entirely to the fact that no civilian lives or damage to civilian (physical) objects would occur. Furthermore, if an adversary does not recognize data as an object, they may similarly argue that it is not protected under IHL and as such its loss is of no consequence.

Therefore, a practical solution for any research facility is to ensure separation, where possible, between data that may legitimately be targetable due to the provision of a military advantage and purely civilian research data. Moreover, this type of arrangement would be consistent with the requirements of Article 58 of AP I, for those countries that recognize data as an object, and analogously, for those that do not. Consequently, if this is considered in the planning and design of the digital infrastructure in advance, it serves a potent passive precaution against the loss of research data during an armed conflict, even if data itself would not be considered an object.

[20] International Committee of the Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff Publishers, 1987), para. 2191.

Conclusions

Universities and research facilities do not have special protection during an armed conflict, rather they are protected against attacks the same as all other civilian objects. This creates an issue when it comes to research data, as it is still controversial whether data is an object or not, and therefore protected against attacks. As can be seen from state positions, especially when there are no physical consequences from a cyber operation against data, not all states agree that it would amount to an attack. Therefore, as research data has no special protection, unlike for example, medical data, it is vulnerable during an armed conflict as it is not clear if it is a civilian object. Until the status of data as an object under IHL is confirmed, it is recommended that universities protect their research data during wartime by ensuring, as far as possible, that military and dual-use data is stored separately from the rest of their data. Consequently, universities must recognize this risk to their data during peacetime, and make preparations accordingly in their systems, to avoid a rude awakening during an armed conflict.

Policy Recommendations

Research institutions are recommended to take precautions during peacetime to better ensure their data is safe during an armed conflict. Firstly, wherever possible, militarily relevant or dual-use data should, as far as possible, be isolated and stored separately from purely civilian data. This provides additional protection even though digital civilian data is not protected as such, as belligerents have a constant care duty for the civilian population, and as such must not go out of their way to cause harm to civilians. Consequently, a military operation that purposefully extends to civilian data stored separately from the militarily relevant data would likely violate this constant care obligation. Secondly, institutions should consider storing essential data physically on paper, as it is protected under IHL, unlike digital data. Finally, states should raise the issue internationally, such as during the UN's Open Ended Working Group discussions on international law, with an aim to close the loophole by evolving the interpretation of "civilian object" under IHL. Research institutions should ensure their

state's decisionmakers are aware of the issue and encourage them to take action on appropriate international fora as well as formulating and expressing their formal state opinion on the interpretation of IHL in a dedicated public document.

Bibliography

Bart, Gregory. "The Ambiguous Protection of Schools under the Law of War – Time for Parity with Hospitals and Religious Buildings." *Georgetown Journal of International Law* 40, no. 2 (2009).

Cyber Law Toolkit. "Scenario 12: Cyber Operations Against Computer Data." https://cyberlaw.ccdcoe.org/wiki/Scenario_12:_Cyber_operations_against_computer_data.

Federal Department of Foreign Affairs. "Switzerland's position paper on the application of international law in cyberspace." 2021, https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.

Federal Government of Germany. "On the Application of International Law in Cyberspace." March 2021, Position Paper of Germany.

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31.

International Review of the Red Cross. (1987) Commentary on the Additional Protocol.

Kjelgaard, Jeppe and Ulf Melgaard. "Denmark's Position Paper on the Application of International Law in Cyberspace." *Nordic Journal of International Law* 92, no. 3 (2023), 446-455.

Lagvilava, Lika. "The 2022–2023 Russia Ukraine War and Cyberspace Threats." *Future Human Image* 19 (2023), 43.

Lehto, Marja. "Finland's views on International Law and Cyberspace." *Nordic Journal of International Law* 92, no. 3 (2023), 456–469.

Main Directorate of Intelligence (Ukraine). Знищили ворожу "планету" – деталі кібератаки проти центру космічної гідрометеорології рф. 24 January 2024, https://gur.gov.ua/content/znyshchyly-vorozhu-planietu-detali-kibe-

rataky-proty-tsentru-kosmichnoi-hidrometeorolohii-rf.html.

Ministry of Foreign Affairs of Costa Rica. "Costa Rica's Position On The Application Of International Law In Cyberspace." 2021, Position Paper of Costa Rica.

Hathaway, Oona, Azmat Khan and Mara Revkin. "The Dangerous Rise of Dual-Use Objects in War." *Duke law School Public Law & Legal Theory Series*, (2024), 2024–56

Pomson, Ori. "'Objects'? The Legal Status of Computer Data under International Humanitarian Law." *Journal of Conflict & Security Law* 28, no. 2 (2023).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

Republic of Austria. "Position Paper of the Republic of Austria: Cyber Activities and International Law." April 2024, Position Paper of the Republic of Austria.

Schmitt, Michael. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press, 2017.

Schöndorf, Roy. "Israel's perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations." *US Naval War College International Law Studies* 97 (2021), 395–406.

United Nations General Assembly. Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266, A/76/136 (2021), 17–23 (Brazil), 75–79 (Romania).