The application of international humanitarian law to non-kinetic cyber operations

by **Mariam Salukvadze**

In recent decades, technological innovation has expanded the battlefield into the digital realm, where operations can incapacitate systems and undermine societal stability without a single shot being fired. Under International Humanitarian Law (IHL), applicability is triggered once the threshold of armed conflict is reached, as clarified by international jurisprudence such as the International Criminal Tribunal for the former Yugoslavia's (ICTY) Tadić Decision, in particular the Appeals Chamber's decision in Prosecutor v. Duško Tadić (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 1995), which states that "an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups" (para. 70), thereby clarifying the threshold for the existence of an armed conflict and providing key criteria - namely the intensity of violence and the organization of the parties - for distinguishing between international and non-international armed conflicts.[1] Building on this, the *Tallinn Manual* - a non-binding but influential reference expert study on the application of international law to cyber warfare, developed under the auspices of the NATO Cooperative Cyber Defence Centre of Excellence - suggests that cyber operations causing physical damage or injury could qualify as armed attacks.[2] While it is generally accepted that cyber operations conducted in the context of an existing armed conflict fall under IHL, the crucial issue is whether cyber operations, in the absence of kinetic force, can independently reach the threshold required to trigger the application of IHL.

Article 49(1) of Additional Protocol I defines an *"attack"* as *"acts of violence against the adversary, whether in offence or defence."*[3] This has traditionally been interpreted by the International Committee of the Red Cross (ICRC) and tribunals such as the ICTY

[1] Prosecutor v Dusko Tadic (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1-AR72 (2 October 1995) para 70.

[2] Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd edn, CUP 2017) 415.

[3] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 49(1).

Technological innovation has expanded the battlefield into the digital realm, where operations can incapacitate systems and undermine societal stability without a single shot being fired

as requiring physical force.[4] However, the *Tallinn Manual* adopts a broader, effects-based approach, suggesting that the notion of *"acts of violence"* is not confined to physical harm but also includes actions with violent consequences.[5] Nevertheless, the experts involved in the Manual remain divided: some assert that only cyber operations resulting in physical damage constitute attacks under IHL, while others argue for recognizing intangible harms - such as severe data corruption - as sufficient.[6] The dominant kinetic equivalence theory, which links the definition of an attack to physical effects, has been criticised for its inability to capture the strategic objectives of contemporary cyber operations, which often aim to disrupt functionality rather than cause physical destruction of infrastructure.[7]

> **"The definition of an armed attack under IHL should encompass not only immediate physical effects but also broader, long-term consequences that may emerge over time, including economic disruption and environmental harm."[8]**

In the cyber domain, the impact of an operation can range from temporary inconveniences, such as a Distributed Denial of Service (DDoS) attack, to severe outcomes - such as triggering the physical destruction of critical infrastructure through manipulated digital commands.[9] Increasingly, modern conflict targets the functionality of infrastructure rather than its physical form, reinforcing the need for a broader interpretation of *"attack"* that includes the neutralization of key systems. However, expanding the definition of an *"attack"* to include non-physical effects also presents legal and ethical challenges. An overly broad interpretation risks undermining core IHL principles - namely, distinction and proportionality.[10] These principles are fundamental to maintaining the balance between military necessity and humanitarian protection. If every disruptive cyber operation is considered an *"attack,"* even those causing minor inconvenience, there is a danger that legal protections are applied too broadly or inconsistently, thereby diluting the normative clarity of IHL.[11] Nonetheless, this does not mean that cyber operations causing minor disruptions should be dismissed outright. While not all inconveniences meet the threshold of an attack, their cumulative effects - particularly when directed at critical civilian infrastructure - can escalate into significant harm. A

4 International Committee of the Red Cross, Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949 (Yves Sandoz et al eds, 1987) para 1880; Prosecutor v Pavle Strugar (Judgment) IT-01-42 (ICTY Appeals Chamber, 17 July 2008) para 270. See also Michael Bothe, Karl Josef Partsch, and Waldemar A Solf, New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949 (2nd edn, Martinus Nijhoff Publishers 2013) 329.

5 Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd edn, CUP 2017) 415.

6 Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (CUP, 2012) 199. Yoram Dinstein, T*he Conduct of Hostilities under the Law of International Armed Conflict* (3rd edn, CUP, 2016). See also Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd edn, CUP, 2017) 415-418. Michael Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework' (1999) 37 Colum Journal of Transnational Law 914-15.

7 Elizabeth Mavropoulou, 'Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks' (2015) 4(2) Journal of Law & Cyber Warfare 33.

8 Ido Kilovaty, 'Cyber Conflict and the Thresholds of War' (22 June 2021) forthcoming in Is the International Legal Order Unravelling? (David Sloss, ed, OUP 2022) 26.

9 Justina Nkechinyere Madubuike-Ekwe, 'Cyberattack and the Use of Force in International Law' (2021) 12 Beijing Law Review 636-637.

10 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3, art 48 and 51(5)(b). Kai Ambos, 'International Criminal Responsibility in Cyberspace' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015) 134.

11 Michael N Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' (2014) 96(893) Int. Rev. of the Red Cross 205.

nuanced and context-specific approach is necessary, where the functional impact, strategic intent, and civilian consequences of a cyber operation are assessed holistically.[12]

In conclusion, cyber operations challenge the traditional frameworks of IHL, particularly with regard to the definition of *"attack* "and the protection of civilian objects. While IHL has historically been grounded in kinetic violence, the digital nature of cyber warfare calls for a broader, effects-based interpretation that accounts for both immediate and long-term disruptions to functionality. Nevertheless, this expansion must be carefully managed to avoid undermining foundational principles such as distinction and proportionality. A context-specific approach that considers strategic intent, the severity of harm, and civilian impact provides a more appropriate framework for evaluating cyber operations under IHL.

"As cyber warfare continues to evolve, legal norms must keep pace – grounded in clear state practice, strengthened by legal consensus, and guided by a commitment to safeguarding humanitarian values in the digital domain."

[12] Justina Nkechinyere Madubuike-Ekwe, 'Cyberattack and the Use of Force in International Law' (2021) 12 Beijing Law Review 646. Michael Gervais, 'Cyber-Attacks and the Laws of War' (2012) 30 Berkeley Journal of International Law 525, 525-531. See also Michael N Schmitt, 'Rewired Warfare: Rethinking the Law of Cyber Attack' (2014) 96(893) International Review of the Red Cross 204.

About the Author

Mariam Salukvadze is a legal professional specializing in criminal law, cybercrime, and digital human rights. In her previous role in law enforcement, she supervised investigators, and oversaw high-priority cases including cybercrime, ensuring the quality of investigations, and safeguarding human rights. She has contributed to the development of national policies on cybercrime and rights-based policing. As a Chevening Scholar, she holds a master's degree in criminal justice from Queen Mary University of London, awarded with distinction. She also contributes her expertise as a NonResident Fellow with the EU Cyber Diplomacy Initiative, an EUfunded programme that supports the Union's international cyber diplomacy efforts by advancing research, capacity building, and global cooperation to strengthen the rulesbased order and resilience in cyberspace.

Download Issue 5

unicri
United Nations Interregional Crime and Justice Research Institute

1540 Compass

ISSUE FIVE: INTERVIEWS WITH

PERMANENT REPRESENTATIVE OF PANAMA TO THE UN

Eloy Alfaro de Alba

DIRECTOR, SECRETARIAT OF THE ASIA-PACIFIC GROUP ON MONEY LAUNDERING

Mitali Tyagi

FORMER COORDINATOR OF THE 1540 GROUP OF EXPERTS

Jonathan Brewer