

GRILI WORKING PAPER NO.15

Forthcoming in the Military Law and Law of War Review 2025(2)



THE INVISIBLE BATTLEFIELD: APPLYING THE RULES OF INTERNATIONAL HUMANITARIAN LAW ON THE CONDUCT OF HOSTILITIES TO JAMMING AND SPOOFING OPERATIONS

December/ 2025

Maxime Nijs

Ghent Rolin-Jaequemyns International Law Institute (GRILI), Ghent University

THE INVISIBLE BATTLEFIELD: APPLYING THE RULES OF INTERNATIONAL HUMANITARIAN LAW ON THE CONDUCT OF HOSTILITIES TO JAMMING AND SPOOFING OPERATIONS

by *Maxime Nijs**

Abstract

This article examines the international legal framework governing electromagnetic warfare in situations of armed conflict. It first considers whether and to what extent international telecommunications law continues to apply between belligerents in wartime, before turning to international humanitarian law. The article then analyses how the rules of international humanitarian law governing the conduct of hostilities apply to electromagnetic warfare, with a particular focus on the jamming of enemy communication systems and the jamming and spoofing of Global Navigation Satellite Systems that guide enemy weapon systems. It clarifies when such operations qualify as 'attacks' within the meaning of Article 49(1) of the 1977 First Additional Protocol and assesses how the principles of distinction, proportionality and precautions in attack operate in this context, thereby highlighting the specific legal challenges posed by such operations. The article further examines the constraints applicable to electromagnetic operations that fall below the attack threshold, including the obligation of constant care and the special protection afforded to medical services.

Keywords

Electromagnetic warfare – jamming – spoofing – international humanitarian law – conduct of hostilities

1 Introduction

Ever since electronic devices were first introduced on the battlefield, electromagnetic warfare (EW) has played a vital role in military operations. One of the earliest recorded uses of such technology in combat dates back to the Russo-Japanese War (1904-1905), when Russian forces successfully jammed Japanese radio communications preventing over 60 shells from striking the Russian Fleet at the port of Lüshunkou (also known as 'Port Arthur') in China.¹ While EW can therefore hardly be considered a 'new' technology of warfare, it has continuously evolved – from primarily interfering with enemy telecommunications and radar systems in the beginning of the 20th century to becoming an umbrella term for a wide array of activities across the electromagnetic spectrum (EMS or the spectrum) to attack the

* Assistant and PhD Researcher at the Ghent Rolin-Jaequemyn International Law Institute, Ghent University, Belgium. <https://orcid.org/0000-0001-9908-5937>. Email: maxime.nijs@ugent.be. The author wishes to thank Tom Ruys, Marten Zwanenburg, Michael Schmitt, and the peer reviewers for their helpful comments on previous drafts of this article.

¹ Olga R Chiriac and Thomas Withington, 'Russian Electronic Warfare: From History to Modern Battlefield' (*Irregular Warfare Initiative*, 21 March 2024) <<https://irregularwarfare.org/articles/russian-electronic-warfare-from-history-to-modern-battlefield/>>.

enemy, to protect own forces and to support other military operations across all domains.² This evolution has been driven in large part by the advanced electrification and digitalization of the battlefield: Today virtually all military equipment depends on the EMS – from communication and positioning tools indispensable for command and control to advanced weapon systems.³

Moreover, as societies continue to digitalize, the EMS has become indispensable to our daily lives.⁴ We rely on it for seemingly ordinary activities, such as listening to the radio, browsing the internet on a smartphone or navigating with a car's satellite-based system. Beyond these everyday uses, telecommunications and positioning systems are essential to the functioning of critical services and infrastructure such as health care, water supply and electricity.⁵ These technologies likewise play a crucial role in shipping, aviation, emergency response and humanitarian action. As the spectrum grows increasingly congested, the risk of military operations interfering with civilian uses of the spectrum has heightened, with potentially far-reaching consequences for the civilian population.

The ongoing armed conflicts in the Middle East and the war between Russia and Ukraine illustrate both the vital importance of EW to modern militaries and the particular risk it poses to civilians. To counter the threat posed by precision-guided munitions (PGMs) and attack drones, belligerents have increasingly relied not only on traditional kinetic means but also on EW measures designed to jam or spoof the communication and navigation systems of such weapons – causing some to miss their intended targets and crash.⁶ While in certain circumstances such measures may be employed to protect civilians from the effects of hostilities, they can also entail significant risks, such as when disrupted or redirected weapons land in populated areas causing civilian harm. In addition, such EW operations have regularly interfered with civilian uses of the spectrum, such as the navigation systems of civilian aircraft and maritime vessels, thereby heightening the risk of accidents.⁷

² Malte von Spreckelsen, 'Electronic Warfare: The Forgotten Discipline' (2018) 27 *The Journal of the JAPCC* 41, 44–45; Ulrik Graff and Iben Yde, 'Elektronisk Krigsførelse i Folkeretligt Perspektiv' (University of Copenhagen, InterMil Project 2023) 7 <https://www.fak.dk/globalassets/fak/dokumenter/2023/-elektronisk_krigsforelse_report_enkeltidet_web-.pdf>.

³ Jack Watling and Sylvia Noah, 'Competitive Electronic Warfare in Modern Land Operations' (RUSI 2025) 3 <https://static.rusi.org/competitive-electronic-warfare-in-land-operations_1.pdf>.

⁴ Eve Massingham, 'Automation of the Spectrum, Automation and the Spectrum: Legal Challenges When Optimising Spectrum Use for Military Operations' 3 *Law, Technology and Humans* 91, 91.

⁵ Stephanie Halwa and Lydia Harriss, 'Electromagnetic (Electronic) Warfare' (UK Parliament Post Note 2025) 15 <<https://researchbriefings.files.parliament.uk/documents/POST-PN-0749/POST-PN-0749.pdf>>.

⁶ Thomas Withington, 'Jamming JDAM: The Threat to US Munitions from Russian Electronic Warfare' (RUSI 2023) <<https://www.rusi.org/explore-our-research/publications/commentary/jamming-jdam-threat-us-munitions-russian-electronic-warfare>>; See also: Ruben Stewart, 'The Shifting Battlefield: Technology, Tactics, and the Risk of Blurring Lines in Warfare' (*Humanitarian Law & Policy Blog*, 22 May 2025) <<https://blogs.icrc.org/law-and-policy/2025/05/22/the-shifting-battlefield-technology-tactics-and-the-risk-of-blurring-lines-of-warfare/>>.

⁷ Tom Whipple, '1,000 Flights a Day Have Signals Jammed over War Zones' *The Times* (London, 5 October 2024) <<https://www.thetimes.com/uk/technology-uk/article/1000-planes-a-day-have-signals-jammed-as-they-fly-over-war-zones-swtdflkqc>>; Anna Hirstenstein, 'Oil Tankers near Iran Appear to Be in Rural Russia as Signals Jammed' *Reuters* (18 June 2025) <<https://www.reuters.com/world/middle-east/oil-tankers-near-iran-appear-be-rural-russia-signals-jammed-2025-06-17/>>; The growing number of jamming and spoofing incidents affecting the Radio Navigation Satellite Service (RNSS), which is essential for the navigation of civil aircraft, maritime vessels and humanitarian assistance vehicles, has prompted the Secretaries-General of the

The purpose of this article is to clarify whether and how the rules of international humanitarian law (IHL) governing the conduct of hostilities (CoH) apply to such jamming and spoofing operations. These rules aim to protect civilians and, albeit to a far more limited extent, combatants against the effects of hostilities.⁸ They are mainly codified in the First and Second Additional Protocol of 1977 to the 1949 Geneva Conventions (AP I and AP II).⁹ While the Additional Protocols are not universally ratified and despite AP II's rudimentary regulation of the CoH, the CoH-rules enshrined in AP I are widely regarded, save for a few exceptions, to reflect customary international law applicable in both international armed conflicts (IACs) and non-international armed conflicts (NIACs).¹⁰

After providing a concise technical introduction to the EMS and the principal electromagnetic capabilities employed in contemporary conflicts, this article examines the international legal framework governing jamming and spoofing operations in the context of armed conflict. It first considers whether international telecommunications law continues to apply in wartime, before turning to IHL. The article then analyses the applicability and concrete application of the rules governing the CoH to EW, with particular emphasis on the interpretation of the concept of 'attack' within this legal framework. It examines when jamming and spoofing operations reach this threshold and how the relevant IHL rules regulate such operations, thereby highlighting the specific legal challenges they raise. Importantly, the article also explores how EW operations that remain below the threshold of an attack are nonetheless constrained by IHL. To structure this analysis, the article distinguishes between two scenarios in which jamming and spoofing are regularly employed on the battlefield: first, the jamming of enemy communications (such as radio communications), and second, the jamming and spoofing of Global Navigation Satellite Systems (GNSS) that guide weapon systems.

International Telecommunication Union (ITU), the International Civil Aviation Organization (ICAO) and the International Maritime Organization (IMO) to issue a joint statement expressing their concern and calling for stronger protection of the RNSS against harmful interference. Secretary General of the ITU, Secretary General of the ICAO, Secretary General of the IMO, 'Protection of the Radio Navigation Satellite Service from Harmful Interference' (18 March 2025) <<https://www.itu.int/en/mediacentre/Documents/2025/ICA0-IMO-ITU-Joint-Statement.pdf>>.

⁸ Stuart Casey-Maslen and Steven Haines, *Hague Law Interpreted: The Conduct of Hostilities under the Law of Armed Conflict* (Hart Publishing 2018) 73; Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (2nd edn, Edward Elgar Publishing 2024) 28.

⁹ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609.

¹⁰ The ICRC's Customary IHL Study has found that in the regulation of the CoH most of the gaps left by AP II have largely been filled through State practice, which has led to the creation of rules parallel to those in AP I, but applicable as customary law to NIACs. Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law*, 1: Rules (Cambridge University Press 2005) XXXV; See also Sassòli (n 8) 28; However, it must be noted that the US has expressed concerns about the ICRC Study, and particularly, about the Study's assertion that many of the rules contained in AP I have achieved the status of customary law and are binding not only in the context of IACs but also in NIACs. John B Bellinger and William J Haynes, 'A US Government Response to the International Committee of the Red Cross Study "Customary International Humanitarian Law"' (2007) 89 *International Review of the Red Cross* 443, 447-448.

2 Military operations within the electromagnetic spectrum

2.1 *The electromagnetic spectrum in technical and military terms*

The EMS encompasses the entire range of electromagnetic radiation, classified according to frequency or wavelength. Although all electromagnetic waves travel at the speed of light in a vacuum, they vary widely in frequency, wavelength and the amount of energy they carry. In general, waves with longer wavelengths have lower frequencies and carry less energy, whereas those with shorter wavelengths have higher frequencies and greater energy. Arranged from the lowest to the highest frequencies (or, conversely, from the longest to the shortest wavelengths), the EMS includes radio waves, microwaves, infrared radiation, visible light, ultraviolet radiation, X-rays and gamma rays.¹¹

The frequency, wavelength and energy of an electromagnetic wave affect various properties, including its geographical range and the amount of information it can carry. For instance, low-frequency waves like radio waves can only carry limited amounts of data, but they can travel long distances and penetrate physical obstacles, which makes them appropriate for telecommunication. In contrast, microwaves, which have a higher frequency, can transmit more data but have a more limited range and can be disrupted by physical objects. As a result, microwaves are commonly used in radar systems and for satellite communications.¹²

US military doctrine describes the EMS as 'a manoeuvre space'. Just as in the physical domains and in cyberspace, military forces manoeuvre and conduct operations within the spectrum to achieve tactical, operational and strategic advantages over the enemy.¹³ Modern militaries rely on the EMS for a wide range of critical functions. Communication systems operating across broad portions of the spectrum enable forces to exchange information, transmit data, provide navigation and timing services, and exercise command and control over units worldwide. In addition, the EMS is vital for sensing and situational awareness of the operational environment, including for intelligence gathering and targeting purposes. The Russia-Ukraine conflict illustrates that even brief electromagnetic emissions by combatants can have lethal consequences: Ukrainian forces have reportedly been able to rapidly locate and target Russian senior officers by geolocating emissions from their personal cellular devices.¹⁴

¹¹ John R Hoehn, Jill C Gallagher, and Kelley M Sayler, 'Overview of Department of Defense Use of the Electromagnetic Spectrum' (Congressional Research Service 2021) 1–2 <<https://www.congress.gov/crs-product/R46564>>; See also: 'Electromagnetic Spectrum' (Encyclopaedia Britannica 2025) <<https://www.britannica.com/science/electromagnetic-spectrum>>.

¹² John R. Hoehn, 'Defense Primer: Military Use of the Electromagnetic Spectrum' (Congressional Research Service 2022) <<https://sgp.fas.org/crs/natsec/IF11155.pdf>>.

¹³ US Chairman of the Joint Chiefs of Staff, *Joint Electromagnetic Spectrum Operations* (Joint Publication 3-85, 2020) v. <https://irp.fas.org/doddir/dod/jp3_85.pdf>.

¹⁴ Charles Coventry, Luke Gigliotti, 'Distinction and the Rule of Perfidy within the Electromagnetic Spectrum' (*Articles of War*, 24 June 2024) <<https://lieber.westpoint.edu/distinction-rule-perfidy-electromagnetic-spectrum/>>.

2.2 Jamming, spoofing and other electromagnetic warfare capabilities

'Electromagnetic Warfare' (EW) refers to combat operations in the EMS to gain and maintain positions of relative advantage over the enemy. As already mentioned, EW can be considered an umbrella term for a wide array of activities across the spectrum to attack the enemy, to protect own forces and to support other military operations across all domains.¹⁵ A variety of EW technologies currently exist or are being developed.¹⁶ A first category of such capabilities are those which are designed to disrupt or deceive an enemy's military activities in the EMS.

A primary method of disrupting an enemy's access to the spectrum is by jamming its signals. Jamming is typically achieved by emitting interfering signals on the same frequency band as the target system, thereby overloading the receiver and preventing the intended transmission from being received.¹⁷ Jamming operations can, for example, target enemy communication networks to degrade command and control. Radar jamming has traditionally played a critical role in air operations, particularly for the suppression and destruction of enemy air defences.¹⁸ As already mentioned in the context of the Russo-Ukrainian armed conflict and the armed conflicts in the Middle East, the jamming of positioning, navigation and timing (PNT) signals necessary for GNSS and of radio communications has played a critical role in diminishing the effectiveness of PGMs and the reconnaissance and strike capabilities of drones.¹⁹

In addition to jamming, another key method of EW is 'spoofing', which does not entail the disruption of enemy signals, but involves the emitting of false signals to deceive receivers.²⁰ When applied to GNSS, spoofing can cause receivers to compute incorrect PNT data to redirect GNSS-guided systems to a different location. Such deception can disorient aircraft or naval vessels and may even lead them to crash if they rely solely on GNSS for navigation. Spoofing can also be used to divert drones or PGMs away from their intended targets. For example, in response to the threat posed by Hezbollah's long-range missiles, Israel has reportedly deployed a widespread spoofing system, which has also

¹⁵ Malte von Spreckelsen (n 2) 44–45; US military doctrine defines EW as 'military actions involving the use of electromagnetic and directed energy to control the EMS or to attack the enemy'. US Chairman of the Joint Chiefs of Staff (n 13) 1–5; US Department of the Army, *Cyberspace Operations and Electromagnetic Warfare* (FM 3-12, 2021) 2–8 <https://armypubs.army.mil/ProductMaps/PubForm/Details.aspx?PUB_ID=1022713>; John R. Hoehn, 'Defense Primer: Electronic Warfare' (Congressional Research Service 2022) <<https://www.congress.gov/crs-product/IF11118>>.

¹⁶ See also Report of the Secretary-General, 'Current developments in science and technology and their potential impact on international security and disarmament efforts' (2024) UN Doc A/79/224 12.

¹⁷ Robert Lawless and Hitoshi Nasu, 'Electronic Warfare and the Law of Armed Conflict' (*Articles of War*, 28 October 2024) <<https://lieber.westpoint.edu/electronic-warfare-law-armed-conflict-2/>>; Watling and Noah (n 3) 8–9.

¹⁸ Ulrik Graff and Iben Yde (n 2) 9–10.

¹⁹ Thomas Gibbons-Neff and Yurii Shyvala, "'Jamming": How Electronic Warfare Is Reshaping Ukraine's Battlefields' *The New York Times* (New York, 12 March 2024) <<https://www.nytimes.com/2024/03/12/world/europe/ukraine-drone-russia-jamming.html>>; Matthew N Slusher, 'Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience' (CSIS 2025) 6–7 <<https://www.csis.org/analysis/lessons-ukraine-conflict-modern-warfare-age-autonomy-information-and-resilience>> accessed 21 May 2025.

²⁰ Robert Lawless and Hitoshi Nasu (n 17); Watling and Noah (n 3) 9.

interfered with the GNSS reception of civilian aircraft.²¹ In the context of the war in Ukraine, Ukrainian forces have likewise reportedly employed spoofing to redirect Russian 'kamikaze' drones back toward Russia and Belarus.²²

As these technologies of EW continue to further develop and advance, so too do the countermeasures designed to defeat them. For example, aircraft, naval vessels, drones or weapon systems are often equipped with complementary navigation systems, such as inertial navigation systems, to reduce the impact of jamming and spoofing. Other protective techniques include frequency-hopping, which mitigates the risk of jamming by rapidly shifting communication frequencies in a pseudorandom pattern, making it harder for adversaries to disrupt transmissions.²³ Moreover, the war in Ukraine illustrates how both older and new technologies are being deployed to counter the threat from jamming and spoofing. For instance, Russian forces have increasingly replaced wireless drones with wired models equipped with spools of fibre-optic cable, providing a secure, unjammable connection between the drone and its operator.²⁴ Other drones have been outfitted with guidance systems powered by artificial intelligence (AI), allowing them to continue functioning autonomously once they are locked on to their target.²⁵

In addition to capabilities designed to disrupt and deceive enemy operations within the EMS, States have also developed weapon systems that utilize concentrated electromagnetic energy, as opposed to a physical projectile, to cause physical harm to enemy systems and personnel. These so-called 'directed-energy weapons' include high-power radiofrequency systems – such as microwave and millimetre wave weapons – and high-energy lasers.²⁶ High-power microwave weapons can degrade or destroy the circuits of a wide array of electronic systems, ranging from mobile phones to drones and missiles.²⁷ Millimetre wave weapons, such as the 'Active Denial System', are anti-personnel weapons that use millimetre wave energy to heat up water molecules in the subcutaneous layers of the skin, causing a painful burning sensation. While such weapons are generally classified as non-lethal, their radiation effects depend on several factors such as the power setting used, range and exposure duration.²⁸ High-energy lasers, which are

²¹ Matt Berg, 'GPS "Spoofing" Thickens the Fog of War' [2023] *Politico* <<https://www.politico.com/newsletters/digital-future-daily/2023/10/24/gps-spoofing-thickens-the-fog-of-war-00123284>>; Selam Gebrekidan, 'An Israeli Air Base Is a Source of GPS "Spoofing" Attacks, Researchers Say' *The New York Times* (3 July 2024) <<https://www.nytimes.com/2024/07/03/world/europe/an-israeli-air-base-is-a-source-of-gps-spoofing-attacks-researchers-say.html>>.

²² Henry Samuel, 'Ukraine "Redirecting" Iranian-Designed Kamikaze Drones Back to Russia' *The Telegraph* (London, 28 November 2024) <<https://www.telegraph.co.uk/world-news/2024/11/28/ukraine-redirect-iranian-designed-drones-to-russia/>>.

²³ Robert Lawless and Hitoshi Nasu (n 17); Matthew N Slusher (n 19) 6–7.

²⁴ 'How New Drones Are Sneaking Past Jammers on Ukraine's Front Lines' [2025] *The Economist* <<https://www.economist.com/europe/2025/05/05/how-new-drones-are-sneaking-past-jammers-on-ukraines-front-lines>>; David Kirichenko, 'A New and More Deadly Drone on Russia's Battlefields' (CEPA 2025) <<https://cepa.org/article/a-new-and-more-deadly-drone-on-russias-battlefields/>> accessed 21 May 2025.

²⁵ Tereza Pultarova, 'How Ukraine's Drones Are Beating Russian Jamming: Killer Drones Spot Landmarks as They Fly to Their Targets' [2025] *IEEE Spectrum* <<https://spectrum.ieee.org/killer-drones>>.

²⁶ Farah Sonde, 'Fact Sheet: Directed Energy Weapons' (Center for Arms Control and non-proliferation 2024) <<https://armscontrolcenter.org/fact-sheet-directed-energy-weapons/>>.

²⁷ Sarah Grand-Clément, 'Directed Energy Weapons: A New Look at an "Old" Technology' (UNIDIR 2022) <<https://unidir.org/directed-energy-weapons-a-new-look-at-an-old-technology/>>.

²⁸ Stuart Casey-Maslen, 'Non-Kinetic-Energy Weapons Termed "Non-Lethal": A Preliminary Assessment under International Humanitarian Law and International Human Rights Law' (Geneva Academy of International Humanitarian Law and Human Rights 2010) 62 <<https://www.geneva-academy.ch/joomlatools-files/docman-files/Non-Kinetic-Energy%20Weapons.pdf>>.

beginning to be deployed, are particularly effective against drones and incoming missiles.²⁹ Even at lower power settings, laser systems can be used to temporarily blind electro-optical sensors or the human eye.³⁰

Finally, States are also developing weapons which make use of electromagnetic energy to accelerate solid projectiles to a high velocity. These electromagnetically propelled weapons, such as rail or coil guns, could be capable of launching projectiles to greater distances and at greater speeds than chemical propellants.³¹

3 International Telecommunications Law: A peacetime legal regime?

Before turning to the legal framework of IHL, a preliminary question that must be addressed is whether jamming and spoofing operations in times of armed conflict are governed by international telecommunications law. The international legal framework governing telecommunications is administered by the International Telecommunication Union (ITU), which is the United Nations (UN) specialized agency for digital technologies. The ITU Constitution defines telecommunication as 'Any transmission, emission or reception of signs, signals, writing, images and sounds or intelligence of any nature by wire, radio, optical or other electromagnetic systems.'³²

Article 45(1) of the ITU Constitution expressly prohibits the causing of harmful interference to the radio services or communications of other Member States. Harmful interference is defined as 'Interference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating in accordance with the Radio Regulations'.³³ Moreover, Article 15 of the ITU's 2024 Radio Regulations (Radio Regulations) stipulates, among other things, that all radio stations are prohibited from making unnecessary transmissions or emitting superfluous, false, misleading or unidentified signals.³⁴ These prohibitions only apply to radio waves (including microwaves), defined in Article 1.5 of the Radio Regulations as 'Electromagnetic waves of frequencies arbitrarily lower than 3000 GHz, propagated in space without artificial guide', and do not extend to electromagnetic waves with higher frequencies. Accordingly, the jamming and

²⁹ William H. Boothby, 'The Drone Threat, the Laser Response, and the Law – Part II' (*Articles of War*, 13 January 2025) <<https://lieber.westpoint.edu/drone-threat-laser-response-law-part-ii/>>.

³⁰ Protocol IV to the Convention on Certain Conventional Weapons (CCW) prohibits the employment and transfer of laser weapons specifically designed, as their sole combat function or as one of their combat functions, to cause permanent blindness to unenhanced vision, that is to the naked eye or to the eye with corrective eyesight devices. As a consequence, laser weapons that merely cause temporary blindness or that cause permanent blindness incidentally are not prohibited by this protocol (see also: Article 3). Additional Protocol to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (Protocol IV, entitled Protocol on Blinding Laser Weapons) (adopted 13 October 1995, entered into force 30 July 1998) 2024 UNTS 163; Sarah Grand-Clément (n 27).

³¹ Report of the Secretary-General, 'Current developments in science and technology and their potential impact on international security and disarmament efforts' (2024) UN Doc A/79/224 12.

³² Constitution and Convention of the International Telecommunication Union (adopted 22 December 1992, entered into force 1 July 1994) 1825 UNTS 3 para 1014.

³³ *ibid* 1003.

³⁴ ITU, *Radio Regulations: Articles* (Edition of 2024).

spoofing of radio signals of another ITU Member State is generally prohibited under the ITU legal regime.³⁵ Consider, for example, Iran's jamming of a French EUTELSAT satellite in 2009 (and subsequently) which disrupted BBC broadcasts and which was found to constitute a violation of the prohibition of harmful interference by the ITU Radio Regulations Board (RRB).³⁶

Importantly, Article 48(1) of the ITU Constitution generally exempts military installations from the ITU's regulations as it provides that 'Member States retain their entire freedom with regard to military radio installations.'³⁷ However, as 'military radio installations' are not defined under the ITU Constitution, uncertainty remains as to the precise scope of this exemption. The Woomera Manual on the International Law of Military Space Operations³⁸ provides that the 'nature' of the installation itself determines the scope of the exemption, not the content or purpose of the radio communication that is transmitted via the installation.³⁹ This raises the question how one should determine the military nature of a radio installation. Should this depend on the ownership or the control of the object or rather on the purpose of the installation? As the former interpretation would allow States to easily circumvent the ITU legal regime by simply placing the installation under military control, the latter interpretation appears more persuasive. This reading also finds support in the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations,⁴⁰ which states that 'an installation operated solely for military purposes, such as a military communications satellite, is covered by the exemption'.⁴¹ Moreover, also certain non-military installations operated solely for military purposes, such as a reconnaissance satellite operated by a civilian intelligence agency to gather military intelligence, may be exempted. The Manuals' emphasis on the word 'solely' indicates, however, that military installations do not

³⁵ Sarah M Mountin, 'The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals' (2014) 90 *International Law Studies* 101, 135; Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn, Cambridge University Press 2017), 'The International Group of Experts agreed that unless peacetime jamming is conducted by a military radio station (Rule 64) or takes place and has effects entirely within that State's territory, it generally constitutes a violation of this Rule'.

³⁶ United Nations Office for Outer Space Affairs, 'Highlights in Space 2010' (2010) 100–101 <https://www.unoosa.org/pdf/publications/st_space_57E.pdf>.

³⁷ See also Article 6 ITU Constitution which provides that 'The Member States are bound to abide by the provisions of this Constitution, the Convention and the Administrative Regulations in all telecommunication offices and stations established or operated by them which engage in international services or which are capable of causing harmful interference to radio services of other countries, except in regard to services exempted from these obligations in accordance with the provisions of Article 48 of this Constitution'.

³⁸ The Woomera Manual was prepared by an international group of experts with the aim of identifying and clarifying the existing rules of international law applicable to military space activities and operations. Jack Beard and Dale Stephens (eds), *The Woomera Manual on the International Law of Military Space Operations* (Oxford University Press 2024).

³⁹ Jack Beard and Dale Stephens, 'Rule 19: ITU Harmful Radio Interference' in Jack Beard and Dale Stephens (eds), *The Woomera Manual on the International Law of Military Space Operations* (Oxford University Press 2024) 188–189 <<https://doi.org/10.1093/law/9780192870667.003.0024>> accessed 13 November 2025.

⁴⁰ The Tallinn Manual 2.0 reflects the opinions of the two international groups of experts that drafted the manuals as to the current state of the international law applicable to cyber operations. It must be noted that all modifications new additions to the original Tallinn Manual were also approved by the members of first international group of experts. Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35).

⁴¹ *ibid* 299; See also Eve Massingham (n 4) 97.

encompass installations that are used for both civilian and military purposes. Consequently, dual-use systems such as the Global Positioning Systems (GPS) do not qualify as military installations for the purposes of this exemption.⁴²

While military radio installations are generally exempted from the ITU legal regime, Article 48(2) of the ITU Constitution stipulates that they must, 'so far as possible, observe statutory provisions relative to giving assistance in case of distress and to the measures to be taken to prevent harmful interference, and the provisions of the Administrative Regulations concerning the types of emission and the frequencies to be used, according to the nature of the service performed by such installations'. However, it has been argued that such a due diligence obligation does not preclude the use of military jamming and spoofing operations directed against the adversary in the context of an armed conflict, where required by military necessity.⁴³

More fundamentally, the question arises whether the ITU legal regime, and most notably the prohibition against harmful interference, continues to apply at all in times of armed conflict. The ITU Constitution contains no provision regulating its operation in such situations. In the absence of any express clause to that effect, Article 3 of the International Law Commission's (ILC) Draft Articles on the Effects of Armed Conflicts on Treaties provides that the outbreak of an armed conflict does not *ipso facto* terminate or suspend the operation of a treaty either between State parties to the conflict or between a State party to the conflict and a State that is not.⁴⁴

Accordingly, the ITU treaty regime principally continues to apply during armed conflict. Nevertheless, the prohibition of harmful interference is difficult to reconcile with the conduct of hostilities between belligerents in times of armed conflict. In such circumstances, the IHL rules governing the CoH operate as the *lex specialis* and consequently prevail over conflicting obligations stemming from the ITU framework. This understanding also finds support in the Woomera Manual, the Commentary to Rule 19 (Harmful Radio Interference) of which states that the rule 'does not apply between belligerents in the context of an armed conflict'.⁴⁵ Similarly, the Tallinn Manual 2.0 suggests that the prohibition of harmful interference is primarily a peacetime obligation and that the permissibility of jamming during armed conflict is instead assessed under IHL as *lex specialis*.⁴⁶

This position is also corroborated by State practice. Although States rarely articulate explicit legal justifications, their widespread and sustained employment of EW during armed conflict, combined with the absence of consistent protest framing such conduct as unlawful under the ITU regime, suggests a general acceptance that electromagnetic

⁴² Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35) 299.

⁴³ Sarah M Mountin, 'The Legality and Implications of Intentional Interference with Commercial Communication Satellite Signals' (2014) 90 *ILJ*, 138; See also Jack Beard and Dale Stephens (n 39) 189.

⁴⁴ International Law Commission, 'Draft Articles on the Effects of Armed Conflicts on Treaties, with Commentaries' <https://legal.un.org/ilc/texts/instruments/english/commentaries/1_10_2011.pdf>, Article 6 of the Draft Articles provides that in such cases the possibility of withdrawal and suspension depends inter alia on the nature of the convention and characteristics of the armed conflict.

⁴⁵ Jack Beard and Dale Stephens (n 39) 190.

⁴⁶ Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35) 298.

interference between belligerents may be permissible, provided that it complies with IHL.⁴⁷ At the same time, this does not imply that the ITU framework becomes wholly irrelevant in armed conflict. This regime, for example, continues to apply between belligerents and non-belligerent States (neutral States), except to the extent that it is incompatible with operations conducted in accordance with IHL.⁴⁸

4 The applicability and application of international humanitarian law to electromagnetic warfare

The previous section already alluded to the fact that IHL is applicable to EW. Although IHL contains no specific rules regulating such capabilities, it is well-accepted that – just as with other new technologies of warfare such as cyber operations⁴⁹ – IHL is applicable to and places limits on the use of EW with a nexus to an armed conflict. Indeed, the rules of IHL are technology-neutral and apply to all weapons or other means and methods of warfare.⁵⁰ This conclusion is supported by the findings of the International Court of Justice (ICJ) in the Nuclear Weapons Advisory Opinion, where it held that IHL ‘applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future’.⁵¹ However, recognizing that IHL as a body of law is applicable to EW is only a first step. The following two sections examine how the IHL rules governing the CoH apply to such capabilities.

5 Communications jamming and the conduct of hostilities rules

Consider the following scenario: States Alpha and Beta are engaged in an IAC. In support of a ground operation in a densely populated area, Alpha conducts a broadband jamming operation against communication networks to degrade the enemy’s command-and-control capabilities. Although the jamming successfully disrupts enemy radio

⁴⁷ See also Danish Ministry of Defence, *Military Manual on the International Law Relevant to Danish Armed in International Operations* (2016) 90 <<https://www.forsvaret.dk/globalassets/fko---forsvaret/dokumenter/publikationer/-military-manual-updated-2020-2.pdf>>, which provides that restrictions under the ITU legal regime must be respected by the Danish armed forces in international military operations outside of armed conflict.

⁴⁸ Jack Beard and Dale Stephens (n 39) 190.

⁴⁹ In 2021, the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security implicitly reached agreement that IHL applies to cyber operations during armed conflict, when it recognized the need to further study how and when certain IHL principles, including the principles of humanity, necessity, distinction and proportionality apply to the use of cyber operations by States: UNGA ‘Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security’ (14 July 2021) UN Doc A/76/135 para 71(f); This report was subsequently endorsed unanimously by the UNGA: UNGA Res 76/19 (8 December 2021) UN Doc A/RES/76/19; This has also been confirmed in the common positions of the European Union (EU) and the African Union (AU) and the national positions of: Australia, Brazil, Canada, Colombia, Costa Rica, Cuba, Israel, Japan, the Republic of Korea, New Zealand, Norway, Pakistan, Singapore, Switzerland, Thailand, the UK and the US. A helpful overview of these positions is provided by the Cyber Law Toolkit, which is continuously updated. ‘Common and National Positions’ (*Cyber Law Toolkit*) <https://cyberlaw.ccdcoe.org/wiki/List_of_articles#Common_and_national_positions>; See also: Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35) 375; ICRC, ‘International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper Submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security’ (2019) 4 <https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf>.

⁵⁰ Ulrik Graff and Iben Yde (n 2) 11.

⁵¹ *Legality of the threat or use of nuclear weapons* [1996] Advisory Opinion ICJ Rep 226 [86].

communications, it also incidentally affects mobile data networks relied upon by civilians. As a result, civilians in the affected area are unable to access mobile data services for several hours. How are such jamming operations regulated by the rules on the CoH? To answer this question, this section first examines whether this operation qualifies as an 'attack' before addressing the legal consequences that such a qualification would entail.

5.1 Interpreting the notion of 'attack' in Article 49(1) AP I

For the application of most of the CoH rules, the question arises whether a military operation can be qualified as an 'attack' in the sense of Article 49(1) AP I. This provision defines attacks as 'acts of violence against the adversary, whether in offence or in defence'. When a military operation crosses the threshold of an attack, it may not be directed against civilians or civilian objects (Articles 51(2) and 52(1) AP I). In addition, indiscriminate attacks, as defined in Article 51(4) AP I are prohibited. Indiscriminate attacks also encompass those that breach the principle of proportionality, which prohibits attacks that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated (Article 51(5)(b) AP I). Finally, most of the precautionary measures prescribed by Article 57 AP I must only be taken when an operation qualifies as an attack. In contrast, military operations that fall below this threshold are governed by a more limited set of regulations. Consequently, determining whether an EW operation qualifies as an 'attack' is a fundamental preliminary step when assessing the application of the CoH rules.

Two constitutive elements can be identified in the definition of attacks as contained in Article 49(1) AP I. First, an attack is an 'act of violence', which can be either offensive or defensive in nature,⁵² and second, it must be directed 'against the adversary'. Before turning to the interpretation of the term 'act of violence', it is important to clarify that the requirement that an act of violence is directed 'against the adversary' does not exclude acts of violence directed against civilians or civilian objects from the scope of attacks during the CoH. Indeed, such attacks would contravene one of IHL's most fundamental rules: the principle of distinction. Rather, this term serves to distinguish the rules of so-called 'Hague Law', which regulate the protection of persons and objects during CoH from those of 'Geneva Law', which concern the protection of persons and objects in the power of a party to the conflict. Acts of violence only qualify as attacks under IHL when they are directed at enemy combatants or military objectives, or at civilians or civilian objects – provided these persons or objects are not under the control of the attacking party.⁵³

In addition, some scholars have argued that the terms 'against the adversary' in the definition of an attack entail a subjective element. Corn *et al.*, for instance, argue that 'the motivation for executing the act must be to cause harm

⁵² As the ICRC Commentary clarifies, acts of violence against the adversary constitute attacks irrespective of their offensive or defensive nature as both can affect the civilian population. ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff Publishers 1987) para 1880.

⁵³ *The Prosecutor v Bosco Ntaganda (Observations by Professor Roger O'Keefe, pursuant to rule 103 of the Rules of Procedure and Evidence)* [2020] ICC ICC-01/04-02/06 A2 3-4; Sassòli (n 8) 28.

to the adversary or other persons or objects in the conduct of hostilities'.⁵⁴ According to this view, such a subjective element would be necessary to distinguish attacks from other harmful acts, such as the provision of air-delivered humanitarian assistance that inadvertently causes injury or damage, manoeuvre damage to roads and fields, or the disposal of excess explosive ordnance in an unpopulated area. While such a motivational element might indeed be read into the words 'against the adversary', some have expressed doubts about such an interpretation, in particular as this would introduce a simple justification for not treating otherwise violent acts as attacks, which would significantly reduce the protection of civilians and civilian objects during the CoH.⁵⁵ Consequently, it can be argued that the definition of an attack should be understood as an objective characterization of conduct.⁵⁶

This brings us to the crux of the matter: how should the term 'act of violence' be interpreted? Nowadays, it is well-established that acts of violence are not confined to means or methods of warfare that release kinetic force. As numerous scholars note, the defining characteristic of 'violence' lies in its harmful consequences rather than the nature of the means employed.⁵⁷ What harmful consequences must a military operation cause to cross the threshold of an attack? Traditionally, the notion of violence has been associated with physical harm. For example, Rule 92 of the Tallinn Manual 2.0 defines a cyber attack as: 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.⁵⁸ Most States,⁵⁹ the ICRC,⁶⁰ and other experts⁶¹ agree that at least those cyber operations that cause effects similar to those of kinetic weapons – namely death, injury or physical damage – constitute attacks under IHL. This has also been confirmed outside the

⁵⁴ *The Prosecutor v Bosco Ntaganda (Observations by Professor Geoffrey S Corn et al, pursuant to rule 103 of the Rules of Procedure and Evidence)* [2020] ICC ICC-01/04-02/06 A2 5–6; See also Chris Jenks, 'Motive Matters: The Meaning of Attack Under IHL & the Rome Statute' (*Opinio Juris*, 26 October 2020) <<https://opiniojuris.org/2020/10/26/motive-matters-the-meaning-of-attack-under-ihl-the-rome-statute/>>; Dick Jackson, 'Motive and Control in Defining Attacks' (*Articles of War*, 11 November 2020) <<https://lieber.westpoint.edu/motive-control-attacks/>>; Michael N Schmitt, 'Naval War College Situations: Conflict in Gregoria and Tanaka: The Law of Targeting' (2024) 103 *International Law Studies* 44–45.

⁵⁵ Tsvetelina Van Benthem and Henning Lahmann, 'Scenario 27: Contesting and Redirecting Ongoing Attacks' *Cyber Law Toolkit* <https://cyberlaw.ccdcoe.org/wiki/Scenario_27:_Contesting_and_redirecting_ongoing_attacks>.

⁵⁶ Tsvetelina Van Benthem, 'The Redirection of Attacks by Defending Forces' (2020) 102 *International Review of the Red Cross* 875, 881–883.

⁵⁷ William H Boothby, *The Law of Targeting* (Oxford University Press 2012) 81, 384; Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35) 415; Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (4th edn, Cambridge University Press 2022) 2–3; Jeroen van den Boogaard, *Proportionality in International Humanitarian Law: Refocusing the Balance in Practice* (Cambridge University Press 2023) 138.

⁵⁸ Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35) r 92.

⁵⁹ A helpful overview of State positions on the interpretation of the notion of 'attack' in the cyber context is provided by the Cyber Law Toolkit. See particularly the positions of Australia, Austria, Canada, Colombia, Costa Rica, the Czech Republic, Denmark, France, Germany, Ireland, Israel, Italy, Japan, New Zealand, Norway, Pakistan, Sweden, Switzerland, the UK and the US: 'The Notion of Attack under International Humanitarian Law' (*Cyber Law Toolkit*) <[https://cyberlaw.ccdcoe.org/wiki/Attack_\(international_humanitarian_law\)](https://cyberlaw.ccdcoe.org/wiki/Attack_(international_humanitarian_law))>.

⁶⁰ ICRC, 'International Humanitarian Law and the Challenges of Contemporary Conflicts' (2015) 41–42 <https://www.icrc.org/sites/default/files/document/file_list/32ic-report-on-ihl-and-challenges-of-armed-conflicts.pdf>.

⁶¹ Cordula Droege, 'Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians' (2012) 94 *International Review of the Red Cross* 533, 557; Michael N Schmitt, "'Attack" as a Term of Art in International Law: The Cyber Operations Context' in Christian Czosseck, Rain Ottis, and Katharina Ziolkowski (eds), *Proceedings of the 4th International Conference on Cyber Conflict* (NATO CCD COE Publications 2012) 289–293; David Turns, 'Cyber War and the Concept of "Attack" in International Humanitarian Law' in Dan Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff Publishers 2013) 224–225; Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann, 'Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts' (2020) 102 *IRRC*, 312–313.

cyber-context. For example, the Pre-Trial Chamber (II) of the International Criminal Court (ICC) has held in Ntaganda that 'in characterizing a certain conduct as an "attack", what matters is the consequences of the act, and particularly whether injury, death, damage or destruction are intended or foreseeable consequences thereof'.⁶² Moreover, according to the ICRC, such physical harm need not be the direct consequence of the attack, but also harm due to the foreseeable indirect effects (often referred to as 'reverberating' effects) of a military operation is sufficient.⁶³ This position is also reflected in the national positions of several States.⁶⁴

This latter point is of particular importance with regard to EW. As was already noted, certain EW capabilities, such as directed energy weapons and electromagnetically propelled weapons, can directly inflict physical harm and their use therefore clearly constitutes an attack within the meaning of Article 49(1) AP I. By contrast, a jamming operation targeting enemy communications generally does not cause direct physical harm to the receiving devices.⁶⁵ Nevertheless, when such operations are reasonably expected to cause physical harm, including due to their foreseeable indirect effects, the operation will qualify as an attack.

Going a step further, the question arises whether mere interference caused by a jamming or spoofing operation can be regarded as (temporarily) 'disabling' the enemy's receiving devices. While there is broad consensus that an attack requires the infliction of physical harm, the question whether operations that impair or neutralize an object, without physically damaging or destroying it, constitute attacks has generated extensive debate, particularly with regard to cyber operations.⁶⁶ Although States and scholars diverge in their views on whether and to what extent disabling an object qualifies as an attack, there nonetheless appears to be agreement that not all military operations that merely interfere with communication systems fall within the scope of Article 49(1) AP I.⁶⁷

⁶² *The Prosecutor v Bosco Ntaganda (Decision on the Confirmation of Charges)* [2014] ICC (Pre-Trial Chamber II) ICC-01/04-02/06 [46]; Also the HPCR Manual takes the position that for a military operation to constitute an attack it must be intended to or result in death, injury, damage or destruction of persons or objects. Program on Humanitarian Policy and Conflict Research at Harvard, *HPCR Manual on International Law Applicable to Air and Missile Warfare* (Cambridge University Press 2013) 12–13.

⁶³ ICRC, 'International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper Submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security' (n 49) 7.

⁶⁴ See, for example, the national positions of Austria and Switzerland. 'The Notion of Attack under International Humanitarian Law' (n 59); Norwegian Ministry of Defence, *Manual of the Law of Armed Conflict* (2013) para 209 <https://usnwc.libguides.com/ld.php?content_id=47416967>; Danish Ministry of Defence (n 47) 677.

⁶⁵ However, in exceptional cases, the emission of high-power jamming signals can cause damage to the receiving device, such as by burning out its circuits. when causing such harm was reasonably foreseeable on the side of the attacker, such an operation qualifies as an attack within the meaning of Article 49(1) AP I. See also Watling and Noah (n 3) 8.

⁶⁶ Cordula Droege (n 61) 557–560; Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann (n 61) 313–316; Robin Geiss and Henning Lahmann, 'Protecting Societies: Anchoring A New Protection Dimension In International Law In Times Of Increased Cyber Threats' (Geneva Academy of International Humanitarian Law and Human Rights 2021) 9–12 <<https://www.geneva-academy.ch/joomlatools-files/docman-files/working-papers/Protecting%20Societies%20-%20Anchoring.pdf>>; Giacomo Biggio, 'Regulating Non-Kinetic Effects of Cyber Operations: The "Loss of Functionality" Approach and the Military Necessity-Humanity Balance under International Humanitarian Law' [2025] *Journal of Conflict and Security Law* 1, 10–13.

⁶⁷ Cordula Droege (n 61) 560; Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35) 418; Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann (n 61) 316; Terry D Gill, 'International Humanitarian Law Applied to Cyber-Warfare:

In this regard, the ICRC 2015 Challenges Report explicitly confirms that 'the jamming of radio communications or television broadcasts has not traditionally been considered an attack in the sense of IHL'.⁶⁸ Looking at the positions of States, The Danish Military Manual, for instance, provides that 'As far as damage to objects is concerned, the term covers any physical damage. However, the term does not cover temporary inoperability and other neutralization which does not involve physical damage (e.g., a digital freeze of a communication control system)'.⁶⁹ Similarly, the United States considers that military operations which merely cause brief disruptions to internet services or temporarily disable or interfere with communications fall outside the definition of an attack.⁷⁰ Also Israel argues that military operations only constitute attacks when they are expected to cause physical damage, expressly noting that certain forms of EW have not been regarded as attacks and are therefore not subject to the targeting rules.⁷¹

Also States that subscribe to a 'loss-of-functionality' approach exclude most military operations that merely interfere with communications. The French national position on international law applied to operations in cyberspace provides: 'Most cyberoperations carried out by the French armed forces in an armed conflict situation (mainly information-gathering) do not meet the definition of an attack. For example, altering the adversary's propaganda capabilities, and in particular making an influence site unavailable by saturation or denial of service – which is not prohibited by IHL by analogy with conventional jamming of radio communications or TV broadcasts – cannot be characterised as an attack'.⁷²

The view that most military operations which merely interfere with communications do not constitute attacks is further supported by the argument that such operations generally cause only 'inconvenience' rather than physical harm.⁷³ The concept of inconvenience is also used to identify which incidental effects on the civilian population need not be taken into account in the proportionality assessment.⁷⁴ For example, the US DoD Law of War Manual states

Precautions, Proportionality and the Notion of "Attack" under the Humanitarian Law of Armed Conflict' in Nicholas Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (2nd edn, Edward Elgar Publishing 2021) 465; Yoram Dinstein (n 57) 3.

⁶⁸ ICRC, 'International Humanitarian Law and the Challenges of Contemporary Conflicts' (n 60) 41–42.

⁶⁹ Danish Ministry of Defence (n 47) 290.

⁷⁰ US Department of Defense, *Law of War Manual* (Updated version 2023, 2015) para 16.5.2 <<https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF>>.

⁷¹ Roy Schöndorf, 'Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations' (2021) 97 *International Law Studies* 395.

⁷² France, 'International Law Applied to Operations in Cyberspace: Paper Shared by France with the Open-Ended Working Group Established by Resolution 75/240' (2021) 12 <<https://perma.cc/8KKK-P4HU>>; By contrast, Germany appears to adopt a particularly broad interpretation, defining a cyber attack as 'an act or action initiated in or through cyberspace to cause harmful effects on communication, information or other electronic systems, on the information that is stored, processed or transmitted on these systems, or on physical objects or persons'. Such an interpretation could arguably encompass communications jamming. Federal Government of Germany, 'On the Application of International Law in Cyberspace' (2021) 8 <<https://www.auswaertiges-amt.de/resource/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf>>.

⁷³ Boothby (n 57) 362, 370; Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35) 418; Sassòli (n 8) 582.

⁷⁴ International Law Association Study Group on the Conduct of Hostilities in the 21st Century, 'The Conduct of Hostilities and International Humanitarian Law: Challenges of 21st Century Warfare' (2017) 93 *International Law Studies* 322, 354; van den Boogaard (n 57) 160.

that 'In assessing incidental injury or damage during cyber operations, it may be important to consider that remote harms and lesser forms of harm, such as mere inconveniences or temporary disruptions, need not be considered in assessing whether an attack is prohibited by the principle of proportionality.'⁷⁵

However, it must be noted that the term inconvenience is not contained in primary IHL norms and that its meaning remains unsettled.⁷⁶ While temporary interferences with communications, as in the present scenario, might indeed constitute mere inconveniences that are not expected to result in physical harm, it has already been noted that telecommunication has become indispensable for civilian life in the 21st century. During armed conflict, civilian dependence on telecommunications is even greater as mobile phones and computers might be the only way of seeking life-saving information or medical or humanitarian assistance.⁷⁷ Consequently, it is conceivable that in certain cases communications jamming might be expected to cause physical harm to persons or objects, such as when jamming operations result in prolonged disruptions of medical communications.⁷⁸ In such cases, the jamming operation would be subject to the full range of rules governing the CoH, including the principles of distinction, proportionality and precautions in attack.

Nevertheless, as noted, most jamming operations targeting enemy communications will fall below the threshold of an attack. Therefore, the next section will examine the CoH rules that apply not only to attacks, but more broadly to all 'military operations'.

5.2 IHL rules governing all military operations

5.2.1 The principle of distinction

While many of rules governing the CoH are indeed formulated with reference to the notion of 'attacks', certain provisions are phrased in arguably broader terms. Notably, Article 48 of Additional Protocol I, which codifies the principle of distinction, provides that: In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.

Article 48 AP I refers to the notion of 'operations', or as the ICRC Commentary notes 'military operations', rather than 'attacks'. The term 'military operations' also appears in other provisions of the same the section (Part IV. Section I), which deals with the general protection of the civilian population against the effects of hostilities. For example,

⁷⁵ US Department of Defense (n 70) para 16.5.1.1.

⁷⁶ Cordula Droege (n 61) 560; Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35) 418.

⁷⁷ Cléa Thounin, 'Offline and in Danger: The Humanitarian Consequences of Connectivity Disruptions' (*Humanitarian Law & Policy Blog*, 1 July 2025) <<https://blogs.icrc.org/law-and-policy/2025/07/01/offline-and-in-danger-the-humanitarian-consequences-of-connectivity-disruptions/>>.

⁷⁸ See also Robert Lawless and Hitoshi Nasu (n 17).

Article 51(1) AP I provides that 'The civilian population and individual civilians shall enjoy general protection against dangers arising from military operations', and Article 57 AP I, which codifies the principle of precaution in 'in attack', stipulates in its first paragraph that 'In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians and civilian objects.'

While the ICRC Commentary initially appears to equate 'operations' with 'attacks', stating that 'The word "operations" should be understood in the context of the whole of the Section; it refers to military operations during which violence is used',⁷⁹ this reference primarily serves to distinguish operations of a military nature from other activities carried out by the armed forces, such 'ideological, political or religious campaigns'.⁸⁰ Indeed, the Commentary subsequently relies on a dictionary definition of military operations which is broader than that of 'attacks', namely, any movements, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat or related to hostilities.⁸¹ This interpretation is widely supported.⁸²

While acknowledging the differing terminology used in AP I, Schmitt argues that the principle of distinction only applies to attacks and not to military operations falling below this threshold. This is also the position taken by the group of experts that drafted the Tallinn Manual 2.0⁸³ and in some military manuals⁸⁴. Drawing on an interpretation of Article 48 AP I in its context, Schmitt argues that the principle of distinction ought to be operationalized through the application of the various attack-related CoH rules, such as the prohibition against making civilians or civilian objects the object of attack (Articles 51(2) and 52(1) AP I) or the prohibition against indiscriminate attacks (Article 51(4) and (5) AP I).⁸⁵ A similar line of reasoning is advanced in relation to the obligation to take constant care under Article 57(1) AP I.⁸⁶ However, such an interpretation would render Article 48 AP I and the other provisions relying on the term 'military operations' superfluous. This would run counter the principle of effectiveness and the corollary

⁷⁹ Michael N Schmitt, 'Wired Warfare: Computer Network Attack and Jus in Bello' (2002) 84 *International Review of the Red Cross* 365, 366–367; Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 177–178.

⁸⁰ ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (n 52) para 1875; Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012) 199–200.

⁸¹ See the Commentary to Articles 48, 51(2) and 57(1). ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (n 52) paras 1875, 1936, 2191.

⁸² UK Chiefs of Staff, *The Joint Service Manual of the Law of Armed Conflict* (2004) para 5.32, fn 187 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/27874/JSP3832004Edition.pdf>; 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) 325–326, 408; Program on Humanitarian Policy and Conflict Research at Harvard (n 62) 10; International Law Association Study Group on the Conduct of Hostilities in the 21st Century (n 74) 380–381.

⁸³ Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35) 421–422; See also: Marco Roscini (n 79) 178–179.

⁸⁴ Norwegian Ministry of Defence (n 64) 210; US Department of Defense (n 70) para 16.5.2.

⁸⁵ As Schmitt notes, Article 51(1) AP I, which begins by noting that '[t]he civilian population and individual civilians shall enjoy general protection against dangers arising from military operations', operationalizes this provision by stating that 'to give effect to this protection, the following rules, which are additional to other applicable rules of international law, shall be observed in all circumstances.' Michael N Schmitt, "'Attack' as a Term of Art in International Law: The Cyber Operations Context' (n 61) 289.

⁸⁶ Michael N Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' (2012) 87 *International Law Studies* 89, 92.

presumption against redundancy, which mandates that every phrase or provision in a treaty must be presumed to have its own independent meaning and effect.⁸⁷

Another argument presented by Schmitt is that some non-violent 'military operations' may be directed against civilians, such as psychological operations or propaganda.⁸⁸ However, as Droege points out, this argument rests on a misunderstanding of the concept of military operations. While it is true that some operations, such as psychological operations, can be directed at the civilian population, this is because they do not qualify as 'military operations' as understood by the drafters of the 1977 Additional Protocols, i.e., activities carried out by the armed forces that are related to hostilities.⁸⁹

Recognizing that this remains a controversial issue, there nevertheless are compelling reasons to apply the principle of distinction to military operations that fall below the attack threshold, unless they are not closely related to the conduct of hostilities, as may be the case with propaganda or certain non-physical psychological operations.⁹⁰ Moreover, it must also be noted that even States that reject this approach consider that limitations on such military operations might also arise under the principle of 'military necessity'. For example, the US DoD Law of War Manual provides that military cyber operations that do not constitute attacks should comport with the general principles of the law of war and must not be directed against enemy civilians or civilian objects unless the operations are militarily necessary. Furthermore, such operations should not be conducted in way that causes unnecessarily causes inconvenience to civilians or neutral persons.⁹¹

Nevertheless, it must be acknowledged that applying the principle of distinction in the electromagnetic spectrum presents challenges. Jamming operations typically affect a broad geographic area and, by their very nature, cannot easily distinguish between military and civilian uses of the same frequency bands. The EMS is heavily relied upon by dual-use systems, such as GPS, which serve both civilian and military purposes simultaneously. Furthermore, as illustrated by the Russia-Ukraine conflict, armed forces are increasingly using civilian cellular networks for military purposes.⁹² Consequently, operations directed at military uses of the spectrum may at times cause incidental interference with civilian communications and services.⁹³ Nonetheless, as will be demonstrated in the following

⁸⁷ Alexander Orakhelashvili, *The Interpretation of Acts and Rules in Public International Law* (Oxford University Press 2008) 422.

⁸⁸ While such activities do not fall within the notion of 'military operations', they are not beyond the scope of other IHL norms. For example, such operations may violate the prohibition of acts or threats of violence the primary purpose of which is to spread terror among the civilian population. ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' (2019) 28–29 <<https://shop.icrc.org/download/ebook?sku=4427/002-ebook>>.

⁸⁹ Cordula Droege (n 61) 556.

⁹⁰ *ibid*; See also Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann (n 61) 325.

⁹¹ US Department of Defense (n 70) para 16.5.2; See also Commonwealth of Australia, Department of Foreign Affairs and Trade and Trade, 'Australia's International Cyber and Critical Tech Engagement Strategy' (2021) 98 <<https://www.dfat.gov.au/sites/default/files/international-cyber-critical-technology-engagement-strategy-2021.pdf>>.

⁹² Matthew Ford, 'From Innovation to Participation: Connectivity and the Conduct of Contemporary Warfare' (2024) 100 *International Affairs* 1531, 1542.

⁹³ Watling and Noah (n 3) 11–12.

section, belligerents are required to exercise constant care to avoid and, in any event, to minimize such incidental interference with civilian uses of the EMS.

5.2.2 *Constant care*

In contrast to the principle of distinction, there is broad agreement among States⁹⁴ and in scholarly literature⁹⁵ that the precautionary obligation to take constant care to spare the civilian population, individual civilians and civilian objects also applies to military operations that fall below the threshold of an attack.

Although often described as a preambular statement to the more specific precautionary measures set out in the subsequent paragraphs of Article 57 AP I,⁹⁶ the general obligation to exercise constant care enshrined in Article 57(1) is recognized as a binding norm in its own right.⁹⁷ On this understanding, the precautionary duties laid down in Article 57(2)-(5) AP I should be seen as concrete applications or specific manifestations of the overarching obligation contained in the first paragraph. While these provisions can be derived from and partially overlap with the general obligation of constant care, they do not exhaust its broader normative scope.

The term 'constant care' is not explicitly defined in IHL. However, like all precautionary obligations, this obligation is best understood as an obligation of conduct, namely, a positive and continuous obligation aimed at risk mitigation and harm prevention, the fulfilment of which requires the exercise of due diligence. As such the obligation is relative in nature. What precisely the obligation requires depends on the circumstances of each specific case.⁹⁸ Despite the fact that Article 57(1) does not refer to the 'feasibility' qualifier, as the other more specific precautions in attack, the constant care obligation must be understood in the same way. The obligation to take 'feasible' precautions has been

⁹⁴ UK Chiefs of Staff (n 82) para 5.32, fn 187; French Ministry for Armed Forces, *Manual of the Law of Military Operations* (2022) 117 <[https://www.defense.gouv.fr/sites/default/files/sga/French%20Manual%20of%20the%20Law%20of%20Military%20Operations.pdf#:~:text=This%20Military%20Operations%20Law%20Manual%20presents%2C%20in%20a,in%20national%20territory%20for%20intervention%20outside%20war%20situations.](https://www.defense.gouv.fr/sites/default/files/sga/French%20Manual%20of%20the%20Law%20of%20Military%20Operations.pdf#:~:text=This%20Military%20Operations%20Law%20Manual%20presents%2C%20in%20a,in%20national%20territory%20for%20intervention%20outside%20war%20situations.;)>; With regard to cyber operations, see: Jeppe Mejer Kjelgaard and Ulf Melgaard, 'Denmark's Position Paper on the Application of International Law in Cyberspace' [2023] *Nordic Journal of International Law* 446, 455.

⁹⁵ Jean-François Quéguiner, 'Precautions under the Law Governing the Conduct of Hostilities' (2006) 88 *International Review of the Red Cross* 793, 796–797; Eric Talbot Jensen, 'Cyber Attacks: Proportionality and Precautions in Attack' (2013) 89 *International Law Studies* 198, 202; International Law Association Study Group on the Conduct of Hostilities in the 21st Century (n 74) 279–381; Noam Neuman, 'A Precautionary Tale: The Theory and Practice of Precautions in Attack' in Yoram Dinstein (ed), *Israel Yearbook on Human Rights*, vol 48 (Martinus Nijhoff Publishers 2018) 28; Chris Jenks and Rain Liivoja, 'Machine Autonomy and the Constant Care Obligation' (*Humanitarian Law & Policy Blog*) <<https://blogs.icrc.org/law-and-policy/2018/12/11/machine-autonomy-constant-care-obligation/>>; Asaf Lubin, 'Lieber Studies Big Data Volume – Algorithms of Care: Military AI, Digital Rights, and the Duty of Constant Care' (*Articles of War*) <<https://lieber.westpoint.edu/algorithms-care-military-ai-digital-rights-duty-constant-care/>>; As already mentioned, this position is rejected by Schmitt. Michael N Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' (n 86) 92.

⁹⁶ The ICRC Commentary, for example, provides: 'Even though this is only an enunciation of a general principle which is already recognized in customary law, it is good that it is included at the beginning of this article in black and white, as the other paragraphs are devoted to the practical application of this principle.' ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (n 52) para 2191.

⁹⁷ Jean-François Quéguiner (n 95) 796–797.

⁹⁸ International Law Association Study Group on the Conduct of Hostilities in the 21st Century (n 74) 381.

interpreted by many States as being limited to those precautions which are practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations.⁹⁹

Accordingly, with respect to communications jamming and, by extension, other forms of EW such as GNSS jamming and spoofing, it can be argued that the obligation of constant care requires belligerents to take all feasible precautionary measures to avoid, or at least minimize, incidental interference with civilian uses of the EMS. Whenever feasible, such measures might include the employment of localized EW operations rather than area-wide operations and frequency-specific EW operations.¹⁰⁰ More generally, during the planning and employment phase of EW, belligerents should continuously monitor the electromagnetic operational environment to distinguish frequencies and spectral bands used for military purposes from those relied upon by civilians. This requires, among other things, the collection of signals intelligence to identify military and civilian uses of the spectrum. Such monitoring should form an integral component of electromagnetic spectrum management activities, which armed forces already carry to ensure that spectrum-dependent military systems function as intended and to prevent unintended interference with friendly systems.¹⁰¹

5.2.3 The special protection of medical services

Given the fundamental importance of health care for all those affected by armed conflict, IHL provides specific protection to both military and civilian medical services. Article 19 of the First Geneva Convention of 1949 (GC I) provides that 'Fixed establishments and mobile medical units of the Medical Service may in no circumstances be attacked, but shall at all times be respected and protected by the Parties to the conflict'.¹⁰² Civilian hospitals and certain means of transport for wounded and sick civilians are similarly protected on the basis of the Fourth Geneva Convention of 1949 (GC IV)¹⁰³ (Articles 16 and 18-22), as well as AP I (Articles 8(e) and 12-13).

As the ICRC Commentary clarifies, the obligation to respect medical services goes beyond the prohibition of attacking them: 'As regards the obligation to respect, the explicit mention of the prohibition of attack before the obligation is stated implies that it encompasses broader commitments than simply to refrain from attack in the context of the

⁹⁹ Amended Protocol on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on 3 May 1996 (Protocol II) annexed to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (adopted 3 May 1996, entered into force 3 December 1998) 2048 UNTS 93, Article 3(10); Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects (with Protocols I, II and III) (adopted 10 October 1980, entered into force 2 December 1983) 1342 UNTS 137, Article 1(5) Protocol III; Julie Gaudreau, 'Les Réserves Aux Protocoles Additionnels Aux Conventions de Genève Pour La Protection Des Victimes de La Guerre' [2003] *International Review of the Red Cross* 143, 163.

¹⁰⁰ See also G Blair Kuplic and Jonathan Sawmiller, 'Humanity on the Final Frontier: Challenges in Applying International Humanitarian Law to Modern Military Space Operations' (2025) 107 *International Review of the Red Cross* 200, 235.

¹⁰¹ See US Chairman of the Joint Chiefs of Staff (n 13) 1-9.

¹⁰² Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85.

¹⁰³ Geneva Convention Relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287.

conduct of hostilities. To respect medical units also means not interfering with their work in order to allow them to continue to treat the wounded and sick in their care.¹⁰⁴ This special protection is of particular importance in the present context, especially in light of the ongoing controversy as to whether military operations falling below the attack threshold are subject to the principle of distinction.

According to the ICRC, this obligation of non-interference also extends to medical communications. Consequently, it is argued that connectivity disruptions must not be directed against the communication systems dedicated to medical missions.¹⁰⁵ Further support for this position can be found in the Tallinn Manual 2.0, with regard to military cyber operations. The Manual, for instance, states that a cyber operation which alters the positioning system of a medical helicopter to misdirect it would be prohibited, even though such an operation does not qualify as an attack.¹⁰⁶ By analogy, spoofing operations directed against medical services would likewise fall within the scope of this prohibition.

However, the Manual also emphasizes that the obligation to respect medical communications does not extend to incidental interference, such as the general disruption of enemy communication systems in which medical communications are affected. This clarification is equally relevant in the context of EW. Still, even in cases of incidental interference, the party conducting the operations remains bound by the duty to take constant care to avoid, or at least minimize, adverse effects on protected medical services, to the extent feasible under the circumstances.

6 Jamming and spoofing enemy weapon systems and the conduct of hostilities rules

Having examined how jamming operations affecting communications are to be assessed under IHL, this section turns to the application of the CoH rules to jamming and spoofing operations that interfere with the GNSS of weapon systems. Consider the following scenario, which appears far from hypothetical in light of contemporary armed conflicts:

States Alpha and Beta remain engaged in an IAC. Alpha's radar systems detect several GNSS-guided loitering munitions (for example, so-called 'kamikaze drones') launched by State Beta en route to its territory. Alpha's military intelligence assesses it highly likely that the attack is directed against the State's military headquarters. In response, Alpha initiates a widespread GNSS jamming campaign aimed at disrupting the munitions' positioning and navigation capabilities, with the objective of causing at least some of them to deviate from their intended trajectory and crash

¹⁰⁴ ICRC, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (Cambridge University Press 2016) para 1799; See also US Department of Defense (n 70) para 7.10.1.

¹⁰⁵ ICRC, *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (n 104) para 1804, 'The obligation to respect means that an intentional disruption of these units' ability to communicate for medical purposes with other components of the armed forces is also prohibited'; Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann (n 61) 328; Tilman Rodenhäuser, 'International Humanitarian Law and Connectivity Disruptions during Armed Conflict' (*Humanitarian Law & Policy Blog*, 3 July 2025) <<https://blogs.icrc.org/law-and-policy/2025/07/03/international-humanitarian-law-and-connectivity-disruptions-during-armed-conflict/>>.

¹⁰⁶ Michael N Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (n 35) 514.

before reaching their target. Alpha is, however, fully aware that the disruption of the munitions' GNSS is likely to result in some of them crashing into a nearby densely populated area, thereby causing harm to civilians and damage to civilian objects. In order to further enhance protection against Beta's attack, Alpha additionally conducts a GNSS spoofing operation designed to manipulate the position and navigation signals received by the munitions, with the aim of redirecting at least some of them away from their intended target and towards an enemy military base located on Beta's territory.

6.1 Jamming enemy weapon systems causing civilian harm

The first question to consider is whether the jamming operation qualifies as an attack in the sense of Article 49(1) of Additional Protocol I. As was already established, attacks are military operations that are reasonably expected to cause physical harm, such as death or injury to persons, or damage or destruction to objects, including through the operation's foreseeable indirect effects. While jamming the positioning systems of loitering munitions does not directly cause physical harm, it is expected to cause several of these munitions to crash, resulting in damage or destruction to the drones. This suggests that such an operation may indeed qualify as an attack. Moreover, the fact that the jamming operation is of a defensive nature, i.e., to protect the military headquarters against attack does not preclude this conclusion. Indeed, Article 49(1) considers that acts of violence against the adversary are attacks, irrespective of their offensive or defensive nature.

A more complex question concerns whether the jamming operation can be categorized as an attack 'against the adversary', given that at least some of the expected physical harm, particularly any civilian harm resulting from the loss of control of the munitions, would materialize on territory under the control of the State conducting the jamming operation. As already established, acts of violence against persons or objects under the control of the attacking party do not qualify as attacks within the meaning of Article 49(1) AP I. Accordingly, most destructive acts carried out by a State on its own territory will fall outside the scope of this notion as they are directed against persons or objects under that State's control.¹⁰⁷ Nevertheless, this is not invariably the case. By way of example, the placing of mines on a State's own territory in anticipation of a future offensive by the adversary is considered to constitute an attack directed against the adversary, since the laying of mines may reasonably be expected to cause physical harm to enemy combatants.¹⁰⁸ This is so even though civilians that might be incidentally affected by such an operation would typically be located within territory under the control of the party laying the mines.

In the same vein, the fact that the civilians and civilian objects harmed as a result of the jamming operation are under Alpha's control is not determinative in the present context. The operation is not directed against them, but rather

¹⁰⁷ ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (n 52) para 1890.

¹⁰⁸ See Stefan Oeter, 'Methods of Combat' in Dieter Fleck (ed), *The Handbook of International Humanitarian Law* (Oxford University Press 2021) 175; See also ICRC, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (n 52) para 1881.

against the enemy loitering munitions, which constitute military objectives by nature within the meaning of Article 52(2) AP I and which cannot be regarded as being under the control of the attacking State. By analogy, if Alpha would have used kinetic missile defence systems in the same scenario it would undisputedly qualify as an attack in the sense of Article 49(1) AP I. Consequently, the jamming operation can be considered to constitute an attack against the adversary and must comply with the full set of CoH rules, including the principles of distinction, proportionality and precautions in attack.

Following the reasoning that the jamming operation is directed against enemy drones, it can also be argued that the operation accords to the principle of distinction. However, in accordance with the principle of proportionality, such a jamming operation would be prohibited if it may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, that would be excessive in relation to the concrete and direct military advantage anticipated (Article 51(5)(b) AP I). Yet assessing proportionality in this context poses particular challenges. For example, there may be uncertainty as to what extent the jamming operation will be effective, as this depends, *inter alia*, on whether the loitering munitions are equipped with alternative navigation systems, which might not be known to the commander at the time of decision-making. Such uncertainty regarding the probability of obtaining the anticipated military advantage diminishes the concreteness of the advantage to be taken into consideration. Consequently, fewer expected incidental civilian harm will be tolerated in such cases.¹⁰⁹

Finally, the principle of precautions in attack, codified in Article 57 AP I, plays a crucial role in protecting the civilian population against the effects of hostilities in the circumstances at hand. Of particular relevance is the obligation to take all feasible precautions in the choice of means and methods of warfare with a view to avoiding, and, in any event, minimizing incidental civilian harm (Article 57(2)(a)(ii) AP I). This obligation may require the attacking party to opt for alternative means, such as surface-to-air missiles or less costly directed energy weapons, if these would be expected to cause fewer incidental civilian effects and if their use is feasible in the circumstances ruling at the time.

6.2 Spoofing and redirecting enemy weapon systems against the adversary

Turning to the spoofing operation from our scenario, it is evident this operation crosses the attack-threshold. By intentionally redirecting loitering munitions towards a military objective on Beta's territory (i.e., an object under Beta's control), the operation is reasonably expected to result in physical damage or destruction and potentially in loss of life. The fact that the physical effects are produced indirectly, through the manipulated functioning of the

¹⁰⁹ Laurent Gisel, 'The Principle of Proportionality in the Rules Governing the Conduct of Hostilities under International Humanitarian Law' (ICRC, Université Laval 2018) 18 <<https://www.icrc.org/en/document/international-expert-meeting-report-principle-proportionality?platform=hootsuite>>; Emanuela-Chiara Gillard, 'Proportionality in the Conduct of Hostilities: The Incidental Harm Side of the Assessment' (Chatham House 2018) 20 <<https://www.chathamhouse.org/sites/default/files/publications/research/2018-12-10-proportionality-conduct-hostilities-incident-harm-gillard-final.pdf>>; van den Boogaard (n 57) 145.

adversary's weapon systems, does not alter the operation's qualification as an attack within the meaning of Article 49(1). Indeed, what is determinative is that physical harm constitutes a foreseeable consequence of the operation.¹¹⁰

Consequently, the redirection operation must comply with the full range of rules governing the CoH, including the principles of distinction, proportionality and precautions in attack.¹¹¹ In the scenario at hand, the loitering munitions are redirected against the military headquarters of State Beta, which constitutes a military objective by nature within the meaning of Article 52(2) of AP I. As such, the redirection of the munitions towards that objective would not, in principle, raise concerns under the principle of distinction. Nevertheless, it must be emphasised that, in practice, redirecting GNSS-guided weapon systems to a predetermined target is often technically complex and subject to significant uncertainty. It depends, *inter alia* on whether the weapon-systems are fitted with complementary navigation systems, which may limit the effectiveness of spoofing. Consequently, the degree of control that the spoofing party can realistically exercise over the weapon system is therefore of critical importance. If, for example, State Alpha only would have the technical capability to redirect the loitering munitions away from their intended target towards the territory of State Beta, without being able to direct them towards a specific military objective the attack would violate the prohibition of indiscriminate attacks in Article 51(4)(a) AP I.

7 Conclusion

Electromagnetic warfare has become a defining characteristic of contemporary armed conflicts. The extensive use of jamming and spoofing operations in recent conflicts, such as in the war between Russia and Ukraine and the various armed conflicts in the Middle East illustrates both their vital importance for militaries and the serious risks they may pose to civilians. As military reliance on the EMS continues to expand, so too does the need for greater clarity concerning the limits that IHL poses to these operations. This article seeks to provide such clarity by examining how the IHL rules governing the CoH apply to EW, and particularly jamming and spoofing operations.

EW does not exist in a legal vacuum. Although the ITU's legal framework and the prohibition of harmful interference do not apply between belligerents in times of armed conflict, IHL as a technology-neutral legal framework is undoubtedly applicable to EW with a nexus to armed conflict. It was demonstrated that most EW operations affecting communications will fall below the attack-threshold. By contrast, EW directed at weapon systems generally does not. When jamming or spoofing operations are expected to cause physical harm, the operation constitutes an attack and must comply with the full range of CoH rules. Importantly, this article has also outlined obligations that apply to all

¹¹⁰ For a similar conclusion with regard to the redirection of weapon systems against the adversary through cyber means, see Tsvetelina Van Benthem (n 56) 881; Tsvetelina Van Benthem and Henning Lahmann (n 55).

¹¹¹ See also Yoram Dinstein and Arne Willy Dahl (eds), *Oslo Manual on Select Topics of the Law of Armed Conflict* (Springer 2020) 41–42, 'This Rule reflects that a cyber hacker who achieves control of the enemy's weapon system or its munition becomes responsible for his/her subsequent employment of the weapon. The hacker's employment of the weapon must comply with principles and rules of LOAC including distinction, discrimination and proportionality as well as the obligation to take precautions in attack'.

military operations in the EMS. In particular, States should take constant care to avoid and, in any event to minimize incidental interference with civilian uses of the spectrum. As the EMS has become an indispensable part of civilian life, the importance of such an obligation can hardly be overstated.