KB LAW SCHOLARS JOURNAL
ISSN 3027-2440 (Online)
https://orcid.org/0009-0004-7341-0868
No. 2 The Laurels Dun An Oir Kanturk Co. Cork Republic of Ireland
Greenbelt Rd Lanham Md. 20706, Maryland, US

GoogleScholar GoogleAnalytics ORCID Open Research Europe
Zenodo.org OpenAire ResearchGate

PROTECTING CIVILIANS DURING CONDUCT OF HOSTILITIES IN URBAN AND CYBER WARFARES

▪**Theresa Uzoamaka Akpoghome** ▪▪**Nkechinyere Huomachi Worluh-Okolie**

[*Ph.D*, B.L] Professor of Law, Benson Idahosa University Benin City, Nigeria
<takpoghome@biu.edu.ng> [https://orcid.org./0000-0002-9296-0134]
[*Ph.D*, B.L] Senior Lecturer in Law, Benson Idahosa University Benin City, Nigeria
<nworluh-okolie@biu.edu.ng> [https://orcid.org./0009-0007-6794-7468]

DOI: 10.5281/zenodo.19415894

Abstract

Urban warfare is not a new method of warfare. Many cities have featured as a stage for violence since humans began building them. Similarly, the regime of cyber-attacks has been added to this trend of urban warfare. Consequent on the above, the paper examined the protection given to civilians in urban warfare as well as against digital threats. The paper argued that the major challenges in protecting civilians against the impact of war in cities is hinged on the lack of observance and obedience to the core tents of IHL, inclusive of lack of adherence to the principles of distinction, proportionality and precautions which results in incidental loss of lives and infrastructure belonging to civilians. The authors therefore maintained that it may be difficult in contemporary armed conflicts in cities to strictly adhere to the *core tenets* of IHL as civilian infrastructures are located closely or near military objectives. This distinction is also difficult to achieve in cyber operations, for instance, the lack of adherence to the rules in selecting means and methods of warfare redounds to devastating impacts on civilians as weapons that are indiscriminate are deployed without subjecting them to Article 36 API procedures. The paper then recommends the training of the members of the armed forces and the adoption of the rules of engagement in national legislations to be incorporated into the military manuals of the armed forces or the codes of conduct of armed groups. The paper therefore concluded that all parties to the conflict must remember that armed conflicts have limits and must endeavour to adhere to the rules of IHL and States should prosecute and punish persons who disregard the rules and target civilians or civilian objects as this is a crucial aspect of their due diligence obligation.

Key words- Urban warfare, Cyber-attacks, Distinction, Proportionality, Precaution

I. Introduction

> The harm and suffering caused in 2023 signal an alarming lack of compliance with international humanitarian laws and human rights law. And, if it is to have any real meaning for the millions of civilians affected by conflict it is time to go above and beyond compliances. To strive to the protection of civilian against the full range of harms they are suffering.[1]

The word 'civilian' is any person who does not belong to any of the categories of person listed in Article 4A (1)–(6) of the Third Geneva Convention and article 43 of the first Additional Protocol (AP I) to the Conventions. Civilians are defined negatively as anyone who is not a member of armed forces or armies of a state. The AP I defines a civilian thus: 'the civilian population comprises all persons who are civilians.'[2] The civilian population therefore is made up of individuals civilian i.e. person who do not belong to the various categories of combatants mention in article 4A of GC III. Under international humanitarian law, civilians in general are protected from dangers of military operations and certain categories of civilian are entitled to reinforced protection.[3] This protection is hinged on IHL's principle of distinction between the civilian and civilian objects and the combatants and military objective.[4]

Significantly, article 48 provides that:

> In order to ensure respect for the 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.

The use of the word 'shall' in the provision stated above imports compulsion. Those who conduct hostilities are under an obligation to ensure that the civilian population and their objects are not targeted or made the subject of any attack. This stipulation requires careful planning and delineation of civilian objects at all times and the avoidance of locating military objectives in the civilian areas. This distinction may not pose great

[1] Joyce Msuya: Assistant Secretary General for Humanitarian Affairs and Deputy Emergency Relief Coordinators
[2] Article 50(2) AP I.
[3] The women, children, sick, elderly and those *hors de combat* or those who do not take direct part in hostilities are afforded protection. See common Article 3 to the four Geneva Convention, Article 75 AP I and Article 4 AP II
[4] Article 48 AP I

challenge in international armed conflicts but in internal conflict. It could be challenging as the fighting forces are most often than not, civilians who have picked up arms against the armed forces of a high contracting party without due training in the conduct of hostilities. These civilians (fighters) dwell among the civilian population and are not identifiable by any fixed distinctive emblem. They are usually faceless and difficult to identify as they carry out attacks which may either be sporadic or concerted within the territory of a high contracting party. Article 49 AP I prohibits any attack on land, air or sea which may affect the civilian population or civilian objects[5] and the provision of Article 49 are additional to the rule concerning humanitarian protection contained in part II of GC4, and in other international agreements binding upon the High Contracting Parties as a well as other international rules relating to the protection of civilian and civilian objects.[6] Article 51 AP I further elaborated on the kind of protection which the civilian must enjoy unless for such time as they take a direct part in hostilities. The provision further noted that indiscriminate attack against the civilian population is prohibited and these include:

(a) Those which are not directed at a specific military objectives;
(b) Those which employ a method or means of combat which cannot be directed at a specific military objective or
(c) Those which employ a method or means of combat the effect which cannot be limited as required by this protocol, and consequently, in each such case, are of a nature to strike military objective and civilian or civilian objective and civilian or civilian objects without distinction.[7]

Laurent Gisel et al posit that "urban warfare is not a new phenomenon, premised on the fact that cities have featured as a stage for violence since human beings began building them and images in recent year-from Aleppo, Mosul, and Sana'a to Marawi, Mogadishu, Donetsk and Mekell-leave little room for doubts that towns and cities will remain primary battle ground for future armed conflicts. Laurent further observed the expectation for belligerents to continue using traditional methods such as sieges, tunnels, booby traps artillery, mortars and snipers and complement these with modern capabilities such as new

[5] Article 49(3) API
[6] Article 49(4) API
[7] Article 51(4) (a)-(c) AP I

technologies of warfare and precision.[8] Urban warfare has dire humanitarian consequences on the cities and their inhabitants, and must be regulated strictly for the benefit of humanity.

He adduced reasons why urban centres are vulnerable to conflicts and these include the fact that cities have strategic value. As the core hub of people, power, economic activity, social institutions, history and culture, and embodiment of national identities controlling cities and their inhabitants is seen as strategically critical by belligerents. Secondly, the rapid rise in urbanization reinforces the strategic value of cities and thirdly, it maybe belligerent's strategy to draw the fighting into an urban area as the physical and human terrain of a city can offer advantage to the defender and mitigate the technological supremacy of a more powerful opponent. This also affords the attackers the opportunity to pin defenders down in a city to prevent their escape, or resort to siege warfare.[9]

In fact, the rise of cyber and information operation in the conduct of hostilities is not novel, premised on the fact that use of digital tools in warfare present increasing challenges such as the disruption of essential services such as medical, electrical, water and sanitation facilities.[10] The situation is more precarious as there is an increasing number of civilians involved in the digital battle field. This trend present a myriad of risk as it again blurs the core principle of IHL[11]-a distinction which requires that civilians must be distinguished from the combatant, with only the latter being lawful targets.[12] It is in view of these that this paper discusses the protection of civilians in urban warfare as well as against digital threats. There are five parts including the introduction; the core principles of IHL; the safeguards in protecting civilians in urban warfare and against digital threats; the problem of choice of means and methods of warfare and the dangers of digital threats to the civilian population and civilian infrastructure, and the conclusion.

---

[8] Laurent Gisel, Pilar Gimeno Sarciada. Ken Hume and Abby Zeith, 'Urban Warfare: An Age-old problem in need of new solutions', (April 27, 2021) <https://www.blogs.icra.org/lawand-policy/2021/04/27/urban-warfare/>accessed September 9, 2025.
[9] *Ibid.*
[10] ICRC, 'Protecting Civilian against Digital Threats ICRC's Humanitarian Cyber Diplomacy in the "EU Bubble" (26 Jan, 2024), <https://www.reliefweb.inter/world/protecting-civilians-against-digital-threats-icrcs-humanitarian-cyber-diplomacy-eu-bubble> accessed September 13, 2025
[11] [Hereafter, the International Humanitarian Law]
[12] *Ibid*

2. NATURE AND SCOPE OF CORE PRINCIPLES OF IHL IN THE CONDUCT OF HOSTILITIES

International humanitarian law or the law of armed conflict is designed to protect those who do not or are no longer fighting or those *hors de combat by reason of capture, sickness or injury*. This law does not apply in a vacuum. Its enforcement or implementation strategy is based on certain fundamental principles and these principles are Distinction, Precaution and Proportionality. These principles have been laid down to ensure accuracy in targeting and the reduction of collateral damage in the conduct of hostilities. But the reality on ground is that the very nature of urban settlement makes it near impossible for belligerents to effectively apply these principles of IHL particularly the principle of distinction.[13]

a. The principle of Distinction

This literally mandates that armed men or the fighting forces be distinguished from civilian population in addition to targeting only military objectives. In this regard, Article 48 AP I postulates that:

> In order to ensure respect and protection of the civilian population and civilian objects, the parties to the conflict shall at all-time distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operation only against military objectives.[14]

A combined reading of Articles 48 and 52(2) provides a mandatory framework which belligerents must comply with in combat. However, strict compliance to this rule is made difficult because urban centres or cities are by the their nature made up of civilian objects such as living houses, schools, hospitals, shops, markets, farmland etc. In addition to this, military objects such as military barracks, headquarters and air bases which are lawful targets are also cited in the cities making a clear distinction between these objects very difficult. This distinction becomes even more difficult in times of non-international armed conflict where armed groups stores their military hardware's in civilian dwellings

[13] Article 52(2) AP I provides that "Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage".
[14] The principle of distinction is tagged 'The basic rule'.

as has been witnessed in the ongoing Israeli-Hamas conflict leading to the destruction of civilian objects in order to neutralize the military forces or weapons of the enemy. These types of attacks cause incidental loss of civilian lives that far outweighs the military advantage being sought by the attacking force. For effectiveness there must be a level of intelligence report identifying precisely the location of these military objects that could be targeted. Identifying and targeting military objectives exclusively has been difficult because these military object are cited in places originally meant for civilian and are placed or located side by side or closely by civilian objects. One major challenge identified by Nathalie Durhin is the problem of dual use objects or facilities. These facilities by their very nature are civilian objects but used by both the civilian and the military.[15] Some of these dual objects include but not limited to bridges, roads, power stations and electricity distribution and transmission function.[16] The military here have a duty to gather accurate information on the use of these objects and how the facilities are shared by the civilians and the military. Natalie further noted that where the object is an oil refinery, it would be necessary to establish the amount of fuel being directly supplied to enemy troops and the precise impact the destruction of the plant would have in the conduct of enemy's operations.[17]

Intelligence must also reveal the quantity of petroleum output that is dedicated for the civilians use for the provision of fuel for their vehicles and the heating of their homes. This information is critical as it will determine whether the refinery is an object indispensable to the survival of the civilian population as such objects ought to be protected. There are critical questions to address in determining whether an object is indispensable to the survival of the civilian population. A cursory examination of Article 54 of AP I would reveal that the article basically pays attention to food supplies and the main objectives is to ensure that starvation is not adopted as a method of warfare by the belligerents. The prohibition of starvation as a method of warfare is recognized as

[15] Natalie Durhin, 'Protecting Civilians in Urban Areas: A military Perspective on the Application of International Humanitarian Law,' *International Review of the Red Cross (IRRC)*, (2018) 98 (1), 177-199.
[16] *Ibid.*
[17] *Ibid.*

customary law rule.[18] Starvation under IHL is wider than the ordinary meaning of killing by deprivation of nourishment and water. It encompasses issues of malnutrition, illness and disease caused by a lack of food, medicines and other essential commodities.[19] It is important to observe that starvation as a method of warfare constitute war crime as provided for in the statute of the International Criminal Court.[20] Intelligence reports will help ensure appropriate communication of information through the chains of command and control. When the chain of command and control system is neutralized it gives a real accurate military advantage but it should not be forgotten that such system or networks of electrical, electromagnetic or digital infrastructure are usually dual use facilities. The real challenge is to determine whether they are indispensable to the survival of the civilian population.[21] Destruction or the neutralization of communication systems such as telephone network used by the enemy forces is often quite complicated. This is also the case in using cyber-attacks in order to neutralize the command and control. This is more devastating as its effects are difficult to measure and control.[22]

Cyber warfare refers to the 'means and method of warfare that consists of cyber operations amounting to, or conducted in the context of an armed conflict within the meaning of international humanitarian law.[23] This may involve the destruction of financial records, causing cyber blackouts, disrupting stock market, destruction of banking, health and other infrastructure that are critical to the survival of the civilian population.[24] IHL regulates cyber-attacks although it did not specifically address cyber weapon like it did for other conventional weapons but its application to cyber warfare or attacks can be deduced from Article 36 AP I referred to as the 'weapon review clause' and this provision mandates the States to conduct a legal review of new weapons, means

[18] Rule 53, Customary International Humanitarian Law, Vol. 1: Rules, John-Marie Henckaerts and Louis-Doswald-Beck (Cambridge University Press; 2005) 186-188
[19] Knut Dormann, "Preparatory Commission for the International Criminal Court: The Elements of War Crimes-Part II: Other serious Violations of the laws and customs applicable in International and Non-International Armed Conflict', (2001) *International Review of the Red Cross*, 83(842) 475-476.
[20] [Hereafter, The ICC]
[21] Article 8, Rome Statute of the ICC
[22] Herbert Lin, 'Cyber Conflict and International Humanitarian Law', *International Review of the Red Cross* (2012) 94 (896).
[23] Amna Adnan Khawaja, 'Cyber warfare and International Humanitarian Law (August 17, 2022), <https://www.dlpforum.org/2022/08/17/17/cyber-warfare and-international-humanitarian-law/> accessed September 25, 2025.
[24] *Ibid.*

or method of warfare to determine if its employment would be prohibited under international law.[25] It can be confirmed that Article 36 applies beyond the weapons that were in existence as at the time the law was crafted, therefore new technologies are regulated by IHL regardless of the fact that they were not directly or specifically mentioned in the law.[26]

When IHL treaties are adopted by the High contracting parties, they agree that these treaties should regulate their present and future conflict. This view is supported by ICJ's Advisory Opinion on the *Legality of the threat use of nuclear weapon*, where the court affirmed that the rules and principle of IHL apply to all from of warfare and to all kinds of weapons including those of the future.[27] Cyber weapons are a new means and methods of warfare requiring States to conduct a legal review in line with Art 36 AP I to ensure compliance with IHL before employing them in military operations noting further that the rights of States to choose means and method of warfare is not unlimited.[28] Although IHL regulates cyber operations, it is trite to note that it only regulates cyber operations that occur during or in connection with armed conflict. Cyber-attacks must not be directed against civilians or civilian objects. Indiscriminate attacks are prohibited. The International Court of Justice has described the principle of distinction as a 'cardinal' and 'intransgressible' principle that form part of the 'fabric'' of IHL.[29] The principle of distinction requires parties to armed conflict to refrain from launching cyber operations that qualify as attack against civilian objects and infrastructure.[30] The principle of

[25] Article 36 'New Weapon', Additional Protocol I.
[26] *Ibid.* Article 36 provides: 'In the Study development, acquisition or adoption of a new weapon, mean or method of warfare, a High contracting party is under an obligation to determine whether its employment would in some or all circumstance be prohibited by this protocol or by any other rule of international law applicable to the high contracting party'.
[27] International Court of Justice, *Legality of the threat or the use of nuclear weapon*, Advisory Opinion, 8 July 1996, Para 86.
[28] Article 35(1) AP I.
[29] Para 78-79, ICJ on Nuclear Weapon case.
[30] Kubo Macak and Tilman Rodenhauser, 'Towards Common Understanding, The Application of established IHL principles to cyber operations', (March 7, 2023), <https://blogs.icrc.org/law-and-policuy/2023/03/07/towards-common-understanding-the-application-of-established-ihl-principles-to-cyber-operations/>accessed September 25 2025.

distinction also prohibits indiscriminate attacks, including when using cyber means or methods of warfare.[31]

In the ICT environment, civilian and the military generally use the same internet infrastructure (such as cables, satellites, routers or nodes) and might rely on the same digital communication, storage and other devices.[32] This is often known as dual use objects. The use of civilian ICT infrastructure for military purpose may turn such objects into military objectives.[33] The object can only be destroyed if the use of such object or infrastructure makes an effective contribution to military action and if its destruction, capture or neutralization offers a definite military advantage to the adversary.[34] Furthermore, the principle of distinction prohibits indiscriminate attacks including when using cyber means or methods of warfare. Indiscriminate attacks are types of attacks that are of a nature to strike military objective and civilian objects without distinction.[35] This include cyber-attacks that are not directed at a specific military objective such as a cyber-operation aimed at wiping the computers of all government agencies of an adversary, consisting of civilian and military agencies. Malwares that exploit a vulnerability found in civilian and military system, self-propagate and is released into an open network; and cyber-attacks which employ means or methods of warfare the effect of which cannot be limited as prescribed by IHL such as cyber operation that is targeted at a military objective but, once released, will spread without limits and may be expected to cause incidental and disproportional harm to civilian.[36]

In concluding on the principle of distinction, it is trite to observe that cities have always been an important factor in the power game, and in an armed conflict the taking or destruction of the cities can become a symbol or an end in itself. This can lead to parties ignoring basic IHL rules, in particular the duty to distinguish between military objectives and civilian objects and civilians from combatants.

---

[31] *Ibid.*
[32] ICRC: 'The Principle of Distinction', <https://www.icrc.org/sites/default/files/wysiwgg/war-and-law/03/_distric tion_0.pdf> accessed September 25, 2025.
[33] *Ibid.*
[34] Article 52(2) AP I.
[35] Article 51 (4) AP I. Rules 11 and 12 CIHL Rules 2005.
[36] ICRC

b. The Principle of Proportionality

Another crucial principle to be respected in times of armed conflict by those who conduct hostilities is the principle of proportionality. This principle goes hand in hand with military necessity. It is not an open cheque that allows the military to launch an attack. Attacks should be launched when it is imperative as there would be no alternative open to the attacking force. Military necessity requires that an attack be called off if the civilian casualty will outweigh the military advantage sought. Invariably, it brings to the table the proportionality which seeks to limit 'collateral' damage during attack. It is established that state and non-state actors must not target civilian and civilian object but if they are made subject of an attack then the principle of military necessity and proportionality must be observed strictly. The AP I provide that the collateral damage to civilian objects should not be in excess to the concrete and direct military advantage gained from an attack on a military objective.[37] Proportionality restricts the employment of force through warfare as the principle requires that 'loss of life and damage to property incidental to attacks must not be excessive in relation to the concrete and direct military advantage expected to be gained.[38] In order to protect civilian and civilian objects, it is necessary to ensure that all precautions are taken to reduce any incidental damage that could be caused by attacks. Collateral damage is not prohibited by IHL, but it must be reduced to the barest minimum. This is a legal and strategic requirement because an armed force that causes civilian casualties could discredit that entire operation and undermine legitimacy of the action taken.[39]

Collateral damage may be categorized into three: unforeseen, incidental and deliberate civilian harm.[40] The last category does not fall within the definition of collateral damage, as it is always caused with knowledge. Unforeseen harm can be caused by human errors or technical failures.[41] In this regard, the analysis of the Us airstrike carried out on October 3, 2015 on the *Medecins San Frontiers*, hospital in Kunduz, Afghanistan, is

[37] Article 51 (5) (b) and 57 (2) (III) API
[38] US. Department of Army Filed Manual 27-10. The law of Land Warfare Para 41 (July 18. 1956).
[39] Nathalie (n13) 185.
[40] Camila Waszink, 'Protection of Civilian Under International Humanitarian Law: Trends and Challenges', Norwegian Peace Building Resource Centre Report, August, 2011, 30 -31.
[41] Nathalie (n13) 185.

important[42] as it revealed an accumulation of human error and technical failures: an AC 130 aircraft, diverted to provide air support to US and Afghan troops on the ground that had come under enemy fire, failed to implement standard 'no strike designation' procedures, the air craft communication system malfunctioned, preventing information exchanges with headquarters, the on board electronic systems were degraded as the result of an alert which forced the AC-130 to effect an emergency change of course; there was no visual target acquisition before the strike; the decision to carry out the strike was approved by a non-competent authority at headquarters; and the real coordinates of the site were not verified prior to the strike. In-view of these factors the analysis concluded that the strike had caused unforeseen civilian harm.[43] This type of harm can be reduced if armed forces focus on improving their internal procedures and training.

Incidental civilian harm illustrates the meaning of the military term 'collateral damage' and in order to reduce this type of harm, armed force put in place oversight processes. The rise of incidental harm is particularly high in urban areas, owing to the very nature of cities and the distinction difficulties experienced therein. Incidental harm is a foreseeable risk and effort to ensure the continuous improvement of target procedures including the choice of weapon employed should focus on strengthening studies that combine the gathering and use of intelligence, systematic analysis and technical studies on essential functions and infrastructure, particularly in urban areas.[44] Indirect collateral damage is another issue to be considered. It is not always easy to determine the cause of such damage with scientific accuracy especially if the strike has a delayed or cascading effect. The strike in the Israeli-Hamas-Hezbollah conflict has presented challenges on the issue of incident harm to civilians. The proportionality principle has been disregarded to a very large extent causing death and injury to civilian and also displacements. Hundreds of people in Southern Lebanon have been killed and more than 1,600 wounded in Israeli

[42] USFOR, 'A Public Affairs Statement on the Kunduz MSF Hospital Investigation', 2015-11-25-US-01 Kabul, 25 November 2015.
[43] Ibid p.2 'The report determine that the US strike upon the MSF Trauma Centre in Kunduz City, Afghanistan, was the direct result of human error, compounded by systems and procedural failures.
[44] Nathalie (n38) 186

airstrikes. Hezbollah has fired hundreds of rockets and other munitions into Israel. Over 160,000 people have been displaced on either side of the border from the fighting.[45]

The pager and walkie-talkie attacks on Hezbollah on September 2024 caused several incidental harms to civilians. If it is proven that the attacks were carried out by the Israeli Defence Forces, it will be a new level of brutality for Israel, and because it is an absolute violation of the protocol on booby traps and landmines which Israel is a party to.[46] The 2022 Russian aggression against Ukraine and the numerous attacks on civilians and civilian objects launched in the context[47] have opened the attention of public opinion on the importance of the international legal constraints on the means and method of warfare. The manifest character of these hostilities under *jus* and *bellum,*[48] the mobilization of western big powers in support of the defending forces[49] and the anguishing evidence indicating systematic victimization of the civilian population[50] have contributed to a shift in the discourse of *Jus in bello*. Attacks on civilian in Gaza unfolded at unprecedented levels. At least 11, 500 children and 8000 women have been reported killed in less than 4 months.[51] According to Oxfam, Israel's military campaign has killed Palestinians at an average rate which exceeds the daily death toll of any other conflict in the 21st century.[52]

---

[45] Emily Crawford, 'With hundreds dead in Lebanon, Is International land being violated? (September 26, 2024), <https://www.sydney.edu.au/news-opinion/news/2024/09/26/with-hundred-dead-in-lebanon-are-israel-and-jezbollah-violating-international-law.htm> accessed September 26, 2025.

[46] *Ibid.*

[47] See report of the Independent International Commission of Inquiry on Ukraine, A/77/533, 18 October 2022, Para 33-59

[48] Green A, Handerson C. and Ruys T., 'Russian Attack in Ukraine and the *Jus ad bellum', J. Use force Int'l Law* (2022) 9, 4-30. See Krish N 'After Hegemony: The law of use of force and the Ukraine crises', *Ejil Talk* 2 March 2022.

[49] Schmitt MN and Biggerstaff. 'Are State aiding and assisting Ukraine using force? *Article of War*, 7 April 2023.

[50] Report of the Independent International Commission of Inquiry on Ukraine A/HRC/52/62, Paras. 4-43, 15 March 2023.

[51] Israel-Gaza war in Maps and Chart: Live Tracker (AL Jazeera <https:///www.aljazeera.com/news/longform/2023/10/9/isra_el-hamaswar-in-map-and-chart-live-tracker>accessed 26 September 2025. These data have been contested. See. Huynh BQ, Chin ET and Spiegel PB, 'No Evidence of Inflated Mortality Reporting from the Gaza Ministry of Health', The Lancet (2024) 403, 23

[52] Oxfam, 'Daily Death rate in Gaza higher than any other major 21st century conflict', (Jerusalem II January 2024) <https://www.oxfam.org/en/press-release/daily/-dealth-rate-gaza-higher-any-other-major-21st-century-conflict-oxfam> accessed 26 September 2025.

In 2014, the fighting during operation 'Protective Edge' killed 6 Israeli civilians, 67 Israeli soldiers and 2251 Palestinian.[53] The Israeli targeting practices were praised noting their compliance with IHL, indicating that Israel Defense Force (IDF) estimated that around half of those killed were fighters who would be factored into collateral damage assessment performed for individual attacks; and added that with respect to identifying targets, Israeli Intelligence Surveillance Reconnaissance (ISR) capabilities are impressive and undeniably enhance the accuracy of military advantage and collateral damage estimation.[54] However, the United Nation Office for the Coordination of Humanitarian Affairs (OCHA)[55] revealed that not less than 1462 victims were civilians including 550 children and minors, 330 women while 11, 231 Palestinians were injured including 3540 women and 3436 children with more than 1000 of the latter suffering permanent disabilities as a result of the attacks.[56] Invariably, the majority of the Palestinians victims of 'Operation Protective Edge' (65%) were civilian.[57] The accuracy enhancing role of the IDF capabilities on proportionality assessment therefore, revealed either far from undeniable or conversely and somehow more concerning, index of highly problematic conceptions of the entity of civilian killing and injuring that can be seen as collateral damage under IHL.[58]

With the growing use of cyber-attacks, it becomes pertinent of determine when these attacks become disproportionate to civilian. Proportionality simply means 'a restraint of force'. It is therefore imperative to exercise proportionality in launching cyber-attacks in

---

[53] Report of the Independent Commission of Inquiry on the 2014 Gaza Conflict, A/HRC/29/52, 24 June 2015, Para 20.

[54]Luigi Daniele, 'Incidentality of the civilian harm in International Humanitarian Law and in Contra Legem antonyms in recent discourses on the law of war', *Journal of Conflict & Security Law* (Spring 2024) 29(1) 21-52. See also Schmit MN and Merriam J., 'The Tyranny of Context: Israeli Targeting Practices and Legal Perspectives', *University of Pennsylvania Journal of International Law* (2015), 37 (53) 126, < <https://doi.org/10/1093/jcsl/krae004> accessed 26 September 2025.

[55]Estimates from NGO's are cited inter alia in Institute for Middle East Understanding (IMEU) '50 Days of death destruction: Israel Operation Protective Edge', <https://www.imeu.org/article/50-days-of-death-destruction-israels-operation-protective-edge> accessed 26 September 2025.

[56] UN Office for the Coordination of Humanitarian Affairs (OCHA), 'Key Figures on the 2014 Hostilities', (23 June 2015), <https://ochaopt.org/content/keyfigures-2014-hostilities #ftnnef> as featured in UN Human Rights Council (HRC), 'Report of the Independent Commission of Inquiry on the 2014 Gaza Conflict' (A/HRC/29/52) <https://ohchr.org/en/hrbodies/hrc/coigazaconflict/pages/reportcoigaza.aspx> accessed 26 September 2025.

[57] Weill S. and Azarova V., 'The 2014 Gaza War: Reflections on Jus Ad Bellum and Jus in Bello, and Accountability in Bellah A (ed.), The War Report: Armed conflict in 2014 (OUP 2015) 360.

[58] Lingui (n50) <https://doi.org/10.1093/jcs/kra004> accessed September 26, 2025.

order to ensure that the attack is within the realms of IHL and does not exceed such limits. According to Tallinn Manuel the principle of proportionality is applicable to cyber operations.[59] Although the Tallinn Manuel affirms that the law of armed conflict applies to cyber operation the issues of applying the principle of proportionality to cyber operation remain. As noted earlier, there are many dual-use objects by civilian and military alike and such include power plants, air traffic and control system that support civilian and military bases. Applying the principle of proportionality will require a distinction between civilian and military objectives. While dual use system can be considered as military targets, however, civilian usage of such objects makes it difficult for the application of proportionality standard. Attacking these dual systems objective will lead to collateral damage.[60] Another persistent issue with the application of proportionality during cyber operation is the knock-on effect which can be defined as the indirect consequences that flow from the direct result of a given action.[61] While it is the responsibility of the commander to remember the direct effect which can be defined as 'immediate first order consequences, unaltered by intervening events or mechanisms,[62] it becomes difficult to consider the 'indirect effects' which are 'the delayed and/or displaced second or third and higher order consequences of actions created through intermediate event or mechanisms.[63] As a result of the expensive nature of cyberspace, it becomes difficult to ascertain the ripple effect of such attack. More so, the interconnectedness of cyber systems further complicates the predictability of knock-on effect.[64]

c. Principle of precaution in attack.

The general rule on precaution in attack is captured in Article 57 of AP I and it state that: "in the conduct of military operation, constant care shall be taken to spare the civilian

---

[59] Michael N Schmitt, *Tallinn Manual 2.0 on the international law applicable to cyber operations*, 2nd ed., (Cambridge University Press; 2017) https://doi.org/1017/9781316822524 accessed 26 September 2025, Tallinn Manual at 159.
[60] Amana Adnan (n20)
[61] Eric Talbot Jensen, 'Unexpected Consequences from Knock-on effects: A different Standard for Computer Network Operations? *Am. U Int'l Rev* (2003) 18, 1145-1176.
[62] Chairman Joint Chief of Staff, 'Joint publication 3-60: Joint Targeting at 1-10 (2007), <https://www.bits.de/NRANEU/others/JP-Doctrine/JP3_60(07)pdf> accessed 26 September, 2025.
[63] *Ibid.*
[64] Amna Adnan (n56).

population, civilian and civilian objects.[65] Added to this is the principle of proportionality reiterated in paras. 2(a)(iii)[66] of Article 57. This principle is also laid down in rule 15 of customary international humanitarian law thus:

> In the conduct of military operations, constant care must be taken to spare the civilian population, civilian and civilian objects. All feasible precautions must be taken to avoid and in any event to minimize, incidental loss of civilian life, injury to civilian and damage to civilian objects.[67]

State practice adopts the rule as a norm of customary law that applies to international and non-international armed conflict. Article 57 also laid down prescription requiring the fighting forces to verify that the object to be attacked are neither civilian nor civilian object[68] and that object subject to special protection are not attacked. They must also take precaution in the choice of means and method deployed in an attack[69] and the calling of or suspension of such attack[70] and effective advance warning to be given of attack which may affect the civilian population except where the circumstances do not permit.[71] Article 57(2) (a) (1) suggest that it is important to "do everything feasible" to verify that the target is not a civilian but military objective. This means that the attacking forces must have complete and accurate intelligence report on the objects. Nathalie Durhin posits that the intelligence can take various forms such as imagery (aerial/satellite), radio, electromagnetic, human etc.[72] He advised that information should be gathered from different sources and supported by human intelligence and must be recent.[73] He further noted that the importance of contemporary open source for obtaining intelligence should not be underestimated- the internet (Google map), NGO's operating on the ground, think-

---

[65] Article 57 (1) AP I.
[66] Para2 (a) (III) provides: '….refrain from deciding to launch any attack which 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 diet military advantage anticipated'.
[67] Rule 15 CIHL
[68] Article 57 (2) (a) (1)AP I
[69] Article 57 (2) (a) (II)AP I
[70] Article 57 (2) (a)(b) AP I
[71] Article 57 (2) (c) AP I
[72] Nathalie, supra, at p. 189
[73] See particularly, his observation that, 'the quality of intelligence is enhanced by the physical presence of human gatherers (conventional or special forces) in the theatre of operations. In the case of 'no boots on the ground' operations, the human intelligence is lacking and it is unrealistic to think that technology alone can resolve this deficiency. When the intelligence comes from the "local" sources (allied forces, rebel fighters, etc.) the party involved must be able to verify the accuracy and objectivity of the information before taking responsibility for a strike based on the information received.' At p. 190

tank report, and the media. He warned that while such sources may be taken into account, closer monitoring of their accuracy is required as it places a limitation which the military forces must be aware of.[74]

Paragraph 2(a) (ii), Article 52 draws attention to the means and method of warfare which must be made with the intention of minimizing collateral damage. Armed forces are limited in their choice of means of warfare in international law.[75] The use of certain weapons are restricted or sometimes banned and the High Contracting parties to Conventions regulating such weapons must abide by them.[76] In choosing weapons that are either permitted or regulated, efforts should be made to ensure that the most precise weapons are selected.[77] Again, all effects of the weapon must be taken into account.[78] In cyber-attacks, the Article 57 rule earlier cited applies. Before a cyber-operation, the commander would be required to take all feasible precautions and he is expected to determine the effects of the attack on the civilians and civilian objects. Where the commander is unable to determine the extent of the attack, he should not launch the attack.[79] The principle of precaution in cyber-attack can be divided into two: active and passive precautions. Active precaution denotes the steps taken before an attack is launched. The preventive steps help in identifying targets to ensure that no civilian or civilian object is targeted during cyber operations.[80] On the other hand, passive precaution refer to steps that must be taken after a cyber-attack has been launched and parties to the conflict are under an obligation to protect civilian from the dangers of those cyber-attacks. It therefore means that during a cyber-operation, commanders and all other person in charge must comply with the legal obligations laid down.

To avoid unintended result, cyber operators must have a thorough understanding of the degree to which the target networks and system are interconnected and of the risk of

---

[74] *Ibid*
[75] Article 35 API provides a general limitation on the choice of means and method of warfare.
[76] Such banned or restricted weapons include chemical and biological weapons, incendiary weapon, mines and cluster munition.
[77] This applies to bombs that are dropped by aircraft (laser-GPS-guided).
[78] The effect of the actual impact and also the blast and fragment.
[79] Amna Adnan (n 60).
[80] *Ibid.*

unintended spread of malware of other cyber operations, including indirect effects.[81] As noted earlier, the obligation to take precautions in attack "active precautions" are codified in Article 57 AP I but it is important to observe that there is no specifically prescribed method through which these obligation ought to be discharged.[82] This is because cyber incidents with or without unclear, links to armed conflicts have resulted in damage and disruption to civilian services.[83] These incidents have included operations against hospitals, water and electrical infrastructure, and nuclear and petrochemical facilities.[84] These offer a chilling warning about the potential humanitarian impact of military cyber operations in contemporary and future armed conflicts.[85] It is trite to note that the standard of feasibility is capable of accommodating a range of consideration as it evolves through time and with the acquisition of experience.[86] Here feasible means 'that which is practicable or practically possible taking into account all circumstances prevailing at the time including humanitarian and military consideration.[87] Protection of the civilian population and civilian objects in times of hostilities is a challenges task everywhere; cyberspace now brings its own layer of complexity to the fore. The basic reason for this is the interconnectivity of networks and the risk of escalation and unintended consequences. Thus, in conducting attacks in cyberspace, parties to the conflict should consider suitable and feasible cyber-space precautions such as impact assessment on the connectivity of military and civilian networks and on secondary effect of attacks or the identification of cyber networks and infrastructure that are serving specially protected

---

[81] Principle of Precaution, < https://www.cyberlaw.ccdcoe.org/wiki/principle-of-precautions/> assessed 28 September 2025.

[82] Theo Boutruche, 'Expert opinion on the meaning and scope of feasible precaution under international humanitarian law and related assessment of the conduct of the parties to the Gaza conflict in the context of the operation', "Protective edge"; expert opinion commissioned by Diaknonia, 2015, 17. See JM Henckaerts and Doswald-Beck (eds.) Customary International Humanitarian Law, Vol. 1: Rule (2005) Rule 15; ICRC, 'Explosive Weapon with wide area effects: A deadly choice in populated area', (2022) 104.

[83]ICRC, 'Avoiding Civilian Harm from Military cyber operation during Armed Conflict', (2021), <https://www.icrc.org/en/document/avoiding-civilian-harm-from-military-cyber-operations/>accessed 28 September 2025.

[84] *Ibid.*

[85] *Ibid.*

[86] Marco Sassoli and Anne Quintin, 'Active and Passive Precautions in Air and Missile Warfare', *Israel Yearbook on Human Rights*, (2014) 44, 87.

[87] Protocol II to CCW (1980) Article 3 (4), Protocol III to the CCW (1980) Article 1 (5); Amended Protocol to the CCW (1996), Article 3(10). See Also JM Henckaerts and L Doswald-Beck (eds.) Customary International Humanitarian Law, Vol 1: Rules (2005) Rule 15; ICRC, 'Explosive Weapons with Wide Area Effect in Populated areas: A deadly choice in populated areas', (2022) 104, < https://www.icrc.org/en/law-and-policy/explosive-weapons-populated-areas/>accessed 28 September 2025.

objects.[88] Additionally, IHL requires the defending parties to take precaution against the effect of attacks. This is known as the 'passive precautions'.[89] Article 58 AP I provide that:

> The parties to the conflict shall to the maximum extent feasible:
>
> (a) Without prejudice to article 49 of the fourth convention, endeavor to remove the civilian population, individual civilian and civilian objects under their control from the vicinity of military objectives;
> (b) Avoid locating military objective within or near densely populated areas;
> (c) Take the other necessary precautions to protect the civilian population, individual civilian and civilian objects under their control against the dangers resulting from military operations.[90]

The measures listed in Article 58 are specific and require defending forces to protect the civilian population and civilian objects under their control.[91] These measures are rendered in relative terms.[92] As they incorporate a standard of feasibility.[93] It is observed that a type of conduct rather than a result is what lies at the heart of these precautionary mandates. In cyberspace these precautionary measures can take from of, for instance building strong cyber resilience cultures at a societal level, segregating civilian and military cyber networks and infrastructure using antivirus software, or setting up system for the detection of cyber vulnerabilities.[94] With regard to national positions on cyber-attacks, Brazil in 2021 observed that IHL principle of precautions is also applicable to the use of ICTs by states, meaning that parties take all feasible precautions in the choice of means and methods of attack with a view to avoiding and in any event minimizing incidental loss of civilian life, injury to civilian and damage to civilian objects.[95] Canada in 2022 noted that cyber activities are an attack under IHL, whether in offence or defense,

---

[88] ICRC, 'International Humanitarian Law and the Challenges of Contemporary armed conflict', (2015) 43, https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemproary-armed-conflict/>accessed 28 September 2025
[89] Article 58, AP I. See also ICRC Customary/IHL study, rule 22, 23 and 24
[90] It is argued that under Customary Law, the second and Third rules are applicable in non-international armed conflict. See Henckaert and Doswald Beck, commentary on Rule 23 and 24, at 71 and 74
[91] Commentary of Additional Protocol 1, Para 20239
[92] Dieter Fleck (ed.) *The Handbook of International Humanitarian Law* (OUP, 2021) 58.08
[93] Eric Jensen, 'Precaution against the Effect of attack in Urban Areas', *International Review of the Red Cross*, (2016) 28 (1) 164-165
[94] ICRC 'Avoiding civilian harm from military cyber operation during Armed Conflict (n80). See also Jonathan Horowitz, 'Cyber Operations under International Humanitarian Law: Perspectives from ICRCs American Society of International Law, *Insights* (2020) 24 (11).
[95] Principle of Precaution (n78)

where effect are reasonably expected to cause injury or death to person or damage or destruction to object. This could include harmful effect above a de minims threshold on cyber infrastructure, or the system that rely on it. Such cyber activities must respect relevant treaty and customary IHL rules applicable to attacks including those relating to distinction, proportionality and the requirement to take precaution in attack.[96] Brazil also noted that in making assessment of necessity, distinction, proportionality and precaution, parties must take into consideration the particularities of the cyberspace, such as interconnectivity between military and civilian networks.[97]

Costa Rica in 2023 opined that states must put in place effective measures to prevent or mitigate the risk of civilian harm posed by the use of military cyber capabilities- 'active precaution'. And during armed conflict, States should avoid involving civilian in military cyber operation as doing so may expose them to a grave risk of harm.[98] Finally the Czech Republic in 2024 posits that 'when conducting cyber operation constant care must be taken to spare the civilian population individual civilians and objects. States must ensure protection of essential civilian infrastructure and services. All feasible precautions must be taken to protect civilian and civilian objects from adverse effect of attacks, including through cyber means.[99] From the above analysis it is obvious that parties to armed conflict must observe precautionary measure laid down in the law in the conduct of attack whether in the cyberspace or other domains of warfare. Precautionary measures must be active-precautions before an attack by the attacking party and passive precautions-precaution against the effect of an attack by the defending party. States are in unity on the

---

[96] Government of Canada, 'International Law applicable in Cyberspace', April 2022, https://www.international.gc.ca/world-monde/issues_development-enjeux_lanf=eng> accessed 28 September 2025.

[97] UNODA, 'Official Compendium of Voluntary National Contribution on the Subject of how International law applies to the Use of Information and Communication Technologies by States', UNODA, A/76/136/ (August 2021), 22-23, < https://www.front.un-arm.org/wp-content/upload/2021/08/A-76-136- EN.pdf> accessed 28 September 2025. UNGA 76TH Session of the preliminary list-development in the fields of information and telecommunication in the content of international security established pursuant to General Assembly Resolution 73/266.

[98] Ministry of Foreign Affairs of costa Rica 'Costa Rica position on the application of international law in cyber space (21 July 2023) 14-15, <https://www.docs-library.unoda.ng/open-ended_workingg_group_on_info rmation_and_communication_technologies_(2021)Costa_Rica_-_position_paper_-_international_law_in_cyberspace.pdf>(accessed of September, 2025.

[99]Ministry of Foreign Affairs of the Czech Republic, 'Czech Republic-position paper on the application of international law in cyberspace, (27 February 2024) 11-13, <https://www.mzv.gov.cz/file/5376858/-20240226_(z_position_paper_on_the_application_of_IL_cyberspace.pdf> accessed September 28, 2025.

position of taking precautions in attack and in the choice of means and methods of warfare that the paper noted is not unlimited. Adhering to the core principle of IHL in targeting especially in urban areas will reduce the incidents of collateral damage. We are not there yet as the cities offer advantage to the attacking states. It is hoped that this trend will change as all parties commit to observing and obeying the rules in conduct of hostilities.

3. Safeguard in Protecting Civilians in times of Armed Conflict

Wars fought in the cities have very devastating consequences and impact on the civilian population and also present dire legal and operational challenges.[100] In urban centres where 55 present of the world's population resides civilians constitutes 90 percent of the casualties in these hostilities.[101] From Ukraine to Russia, Israel, Gaza, Palestine, Lebanon, Afghanistan Iraq, Iran, Libya, Syria and Vietnam to mention but a few. The impact of these conflicts on civilians-men, women and children cannot be overemphasized. In these conflicts, particularly internal armed conflicts where the fighters do not distinguish themselves, the armed actors hide among the civilian thereby exposing the civilian population to increasingly dangerous conditions and potential harms. Civilians in these situations are often trapped between opposing forces and they take enormous risks as they attempts to move to safer areas. Because these armed groups are not trained to fight in cities, their activities increase the risk to civilian and civilian objects. They are unable to observe the fundamental principles of IHL - distinction, proportionality and precaution as most of the military objectives are citied in and around the civilian territory. The use of explosive weapons often cause irreparable damage to essential service such as water, electricity, sanitation and hospitals[102] as witnessed in Gaza and Syria and these have lasting impact on civilians health, safety and wellbeing.[103]

In these situations it becomes pertinent to adopt peace time measure such as continuous training of the armed forces on what is acceptable in targeting. Civil societies and

[100]Centre for civilian in conflict, "Urban Warfare," https://wwww.civilianinconflict.org/our-work/conflict/urban/-warfare/ accessed 29 September 2025.
[101] *Ibid.*
[102] *Ibid.*
[103] *Ibid.*

humanitarian organization in collaboration with the Red Cross Societies should work with local communities to support their self-protection strategies and raise their protection concern with government and armed actors. There should be dialogue with armed groups including scenario based trainings, encouraging them to adopt good practices, policies and procedures in order to mitigate the extent of harm caused to the civilian population before, during and after military operation.[104] Again, existing IHL provides the framework to regulate the conduct of hostilities. These laws apply to the use of weapons particularly explosive weapons in all situations of armed conflict and to all the parties including state and non-state actors. It is imperative that these actors observe full compliance with IHL as a means of protecting civilian and civilian objects and to avoid, and minimize civilian harm when conducting attacks particularly in urban populated areas.[105]

There is an obligation on all parties to the conflict to comply with IHL under all circumstances while conducting operations in urban area. They must distinguish between combatants and civilians as well as between military objectives and civilian objectives. Indiscriminate attack or attacks that are disproportionate should be prohibited. All parties must take practicable measures in precautions in attack and against the effects of attack.[106] The obligation under IHL to the general protection of civilian against dangers arising from military operations, and allowing and facilitating rapid and unimpeded passage of humanitarian relief for civilians in need should be adhered to.[107] Methods of warfare that is designed to exploit the proximity of civilian or civilian objects to military objectives in populated areas, in addition to the use of improvised explosive devices directed against civilian or civilian objects and other violations of IHL by non-state actors which exacerbate the risk to civilian should be avoided.[108] Of particular note is the booby

[104] *Ibid.*
[105] Department of Foreign Affairs, 'Protecting Civilian in Urban Warfare', (19 April 2024), <https://www.gov.ce/en/publication/585c8-protecting-civlian-in-urban-warfare/>accessed September 29, 2025.
[106] *Ibid.*
[107] *Ibid.*
[108] *Ibid.*

trapping of pagers and walkie-talkie in Lebanon which killed and injured many on 17 September 2024 causing terror among the civilian population.[109]

Attacks directed against civilians and other protected persons and civilian objects, including civilian evacuation convoys, as well as indiscriminate shelling and use of explosive devices should be condemned and United Nation General Assembly must strengthen the protection of civilian population in its work in addition to strengthening the compliance with IHL. On the other hand, we observed earlier that the use of cyber and information operation is not new in armed conflict. Yet, the use of digital tools in warfare poses great challenges including the risk of disruption of essential services such as medical, electrical, water and sanitation facilities. ICRC as the guardian of IHL uses it expertise to promote the protection of civilians against digital threats.[110] A major concern to stakeholders is the increased civilian participation in cyber operation in the digital battlefield. This dangerous trend poses multiple risk as it further blurs the principle of distinction, a core tenet of IHL which requires a clear line between civilian and combatants, designating only the combatants as lawful targets.[111] The ICRC notes that hacktivists, cyber security professionals and hackers conducting cyber operation in ongoing armed conflict must comply with international legal limits, including the limits imposed by IHL.[112] Civilian that are participating in hostilities through digital operation in armed conflict are expected to observe the rule of IHL and are prohibited from targeting civilian objects or disrupting essential service such as hospitals and banks.[113] The implication of civilian participation in digital attacks is that they lose the protection as civilians for directly participating in hostilities and become lawful target albeit

[109] Tamara Qiblawi, Eliza Mackintosh, Wayne Chang, Eric Cheung, Yong Xiong, Kara Fox, Gianluca Mezzofiore and Balint Bardi, "Israel concealed explosives inside batteries of pagers sold to Hezbollah, Lebanese official - CNN, <https://www.edition.ccn.com/2024/09/27/middleeast/israel-pager-attack-hezbollah-lebanon-invs-intt/index.html> accessed 29 September 2025.
[110] ICRC 'Protecting Civilians against Digital Threats: ICRC's Humanitarian Cyber Diplomacy in the EU Bubble,' (26 Jan 2024) <https://www.reliefwebs.int/report/world/protecting-civilian-against-digital-threats-icrc-humanitarian-cyber-dimplomacy-eu-bubble/> accessed September 13, 2025.
[111] *Ibid.*
[112] *Ibid.*
[113] *Ibid.*

temporarily.[114] It also means that civilians and civilian object located near those participating in hostilities will be incidentally harmed.[115]

In view of this, the ICRC has set eight (8) rules for civilian hackers directly participating in hostilities in the context of cyber operation and these rules will be reproduced here. ICRC further noted that civilian hackers must respect the law of the countries they operate in during armed conflict; they must in addition obey international humanitarian law.[116] The rules are:

i. Do not direct cyber-attacks against civilian objects.[117]
ii. Do not use malware or other tools or technique that spread automatically and damage military objectives and civilian objects indiscriminately.[118]
iii. When planning a cyber-attack against a military objective, do everything feasible to avoid or minimize the effects your operation may have on civilians.[119]
iv. Do not conduct any cyber operation against medical and humanitarian facilities.[120]
v. Do not conduct cyber-attack against objects indispensable to the survival of the population or that can release dangerous forces.[121]
vi. Do not make threats of violence or spread terror among the civilian population.[122]

---

[114] *Ibid.*
[115] *Ibid.*
[116] ICRC, 'Eight Rules for 'civilian hackers' during war, and four obligations for state to restrain them', https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligation-states-restrain-theny> accessed September 30, 2025
[117] *Ibid*. Civilian object are all objects that are not military objectives. This includes civilian infrastructure, public services, companies, private property and arguably civilian data. Under IHL and in the context of cyber operation, the notion of attack refers to cyber operations that can be reasonably expected to result in directly or indirectly in damage, disabling or destruction of objects (such as infrastructure and arguably data) or injury or death of people. It does not include cyber operations aimed at obtaining unauthorized access to information.
[118] *Ibid.* This for example, malware that spreads automatically, spills over and damages military objectives and civilian objects without distinction must not be used.
[119] ICRC, for example if you aim to disrupt electricity or railway services used by military forces you must avoid or minimize the effects your operation may have on civilians. It is essential to research and understand the effects of an operation- including unintended ones-before conducting it When planning a cyber-attack against a military objective, do everything feasible to avoid or minimize the effects your operation may have on civilians and stop the attack if the harm to civilians risk being excessive. If you have gained access to an operating system but you do not understand the possible consequences of your operation or realise that the harm to civilian risk being excessive, stop the attack.
[120] Hospitals or humanitarian relief organizations must never be targeted.
[121] In IHL objects containing dangerous forces are defined as dams, dykes and nuclear electrical generating stations. In reality however, chemical and similar plants also contain dangerous forces. Objects indispensable for the survival of the civilian population include among others, drinking water installations or irrigation systems.
[122] For instance hacking into communication system to publish information design primarily to spread terror among civilian population is prohibited. Likewise designing and spreading graphic contents to spread terror among civilian in order to make them flee is unlawful

vii. Do not incite violations of international humanitarian law.[123]

viii. Comply with these rules even if the enemy does not.[124]

Furthermore, the ICRC also articulated the obligations of States in the regard. ICRC observes that hackers do not live in cyberspace and States have an obligation to impose limits by not encouraging or tolerating civilian hackers conducting cyber operation in the context of an armed conflict.[125] There will be greater risk of operations that violate the applicable law and blur the line between combatants and civilians the more civilian hackers engage in cyber operation. The State have been called upon by the ICRC to give due consideration to the risk of exposing civilians to harm if encouraging or requiring them to be involved in military cyber operation.[126]

States have pledged not to 'knowingly allow their territory to be used for intentionally wrongful acts using ICTs Para 13 (c)'.[127] Although this prohibition was formulated as a political commitment, this norm reflects state 'due diligence' obligation under international law including in respect of civilian hackers operating from their territory.[128] In the context of cyber operation, the United Nations General Assembly urged States to 'ensure that their laws and practice eliminate safe haven for those who criminally misuse information technologies.[129] There has been some controversy on whether the principle of due diligence reflects a binding obligation application to cyber operations.[130] Some states

---

[123] Do not encourage or enable others to conduct cyber or other operations against civilians or civilian objects. For example, do not share technical details in communication channels to facilitate attacks against civilian institutions.

[124] Revenge or reciprocity are no excuses for violation of international humanitarian law.

[125] Tillman Rodenhauser and Mauro Vignati, '8 rules for civilian hackers' during war and 4 obligation for State to restrain them', <https://www.blogs.icrc.org/law-and-policy/2023/10/04/8-rules-civilian-hackers-war-4-obliigations-states-restrain-them/> accessed September 30, 2025

[126] *Ibid.*

[127] United Nations General Assembly, 'Group of Government Expert on Development in the Field of Information and Telecommunication in the Context of International Security', UNGA/A/70/174, 22nd July 2015.

[128] According to the traditional formulation by the ICJ in the *Corfu Channel case*, every state is under an 'obligation not to allow knowingly it territory to be used for acts contrary to the right of other states'. *Corfu Channel case (UK v Albania)* (Merits) (1949) ICJ Rep 4, 22. <https://www.icj-cij.org/files/casse-related/1/001/-194803255-JUDE-01-00.pdf> accessed October 1, 2025. See also Due Diligence, <https://www.cyberlaw.icdcre.org/wiki/due__diligence/ > accessed 30 September 2025.

[129] UN GA Res 55/63 (4 December 2000) Doc A/RES/55/63 Para 1(a).

[130] UN GGE 2015 Report Para (c) and 28 (e) (using non mandatory language to express the due diligence principle in the context of cyber operation). "State should not knowingly allow their territory to be used for internationally wrongful acts using (cyber means) and states… should seek to ensure that their territory is not used by non-state actors to commit such acts". See also UN Group of Governmental Experts (GGE) on

have framed it within their national positions as one of the voluntary non-binding norms of responsible state behaviour[131] in cyberspace, the state include Israel,[132] New Zealand,[133] the United Kingdom,[134] and Canada.[135]

While states are committing to the 'due diligence' norm, they agree that no state practice has been formed and the rule have not attained the status of customary international law rule. It has been proposed that in the cyber context it is preferable to interpret due diligence as a standard of attribution rather than as a standalone primary rule of international law.[136] Nevertheless, the present day analysis proceeds on the basis that as a matter of *lax lata*, due diligence constitutes a general international obligation for every state not to knowingly allow its territory to be used for internationally wrongful act using cyber means.[137] This view has been endorsed by growing numbering states.[138] It is

---

Advancing Responsible State Behavior in Cyberspace in the Context of International Security', A/76/135 (14 July 2021) Para 29-30, <https://www.front.un/arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-pdf> accessed 1 October 2025.

[131] Dapo Akande, Antonio Coco and Talita Desouza Dias 'Old Habits Die hard: Applying existing international law in cyberspace and beyond', *EJIL Talk* (5 January 2021), <https://www.ejiltalk.org/old-habits-die-hard-apply-existing-internaitonal-law-in-cyberspace-and-beyond/ Accessed October 1, 2025.

[132] Roy Schondorf, 'Israel's Perspective on Key Legal Practical Issues Concerning the Application of International Law to Cyber Operation (8 December 2020) 403-4 <https://www.digital-commons.usnwc.edu/cgi/viewcontent.cgi/> accessed October 1, 2025 or *Int'l Law Studies* (2021) 97, 395-405.

[133] New Zealand Foreign Affairs and Trade, 'The Application of International Law to State Activity in Cyberspace (1 December 2020) 3, <https://www.dpmc.gov.nz/sites/default/files/2020-12/application-of-international-law-to-state-activity-in-cyberspacepdf> accessed October 1, 2025.

[134] United Kingdom Foreign Affair Common Wealth and Development Office, 'Application of International Law to State Conduct in Cyberspace: UK Statement (3 June 2021) Para 12. According to the position the fact that states have referred to this as a non-binding norm indicates that there is not yet state practice sufficient to establish customary international law rule of due diligence applicable to activities in cyberspace. <https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/71355ebf834-4d0a-88be-dsa13f8fiddf> accessed October 1, 2025.

[135]Government of Canada, 'International Law Applicable in Cyberspace', (April 2023) Para 26. According to the position, this does not preclude the recognition of a binding legal rule of due diligence under customary international law. Canada continues to study the matter. <https://www.internationale.gc.ca/world-made/issues-development-enjeux_development/peace_security_paix_security_law-cyberspace_droit.aspx?lang=eng> accessed October 1, 2025.

[136] Luke Chircop, 'A Due Diligence Standard of Attribution in Cyberspace', *International Comparative Law Quarterly* (ICLQ) (2018) 67, 643 <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/a bs/due-diligence-standard-of-attribution-in-cyberspace/ 9AE85ED928CDF 08B2C2C38EF3B 63A0ED/> Accessed October 1, 2025.

[137] Talinn Manual 2.0 Commentary to rule 6, Para 4, https://www.cambridge.org/core/books/talinn-manual-20-on-the-international-law-applicable-to-cyber-operation-/EAFFD83EA790D7C4C3C28C9CA2FB6C9> accessed October 1, 2025.

[138] The state include Australia, Czech Republic, Estonia, Finland, France, Germany, Italy, Japan, the Netherland, Norway, Switzerland and Sweden.

important to note that due diligence does not entails a duty of prevention,[139] but rather an obligation of conduct.[140] Therefore any state that is committed to the rule of law or a 'rule-based international order' must not close its eyes when people on its territory conduct cyber operation in disregard of national or international laws even if directed against an adversary.[141] In line with this, States have an obligation to adopt and enforce national laws that regulate civilian hacking and since the State have undertaken to respect and to ensure respect for IHL,[142] this legal commitment have the following implications:

i. If civilian hackers act under the instruction, direction or control of a state, the state is internationally legally responsible for any conduct of those individuals that is inconsistent with the State's international legal obligations, including international humanitarian law.[143]
ii. States must not encourage civilians or groups to act in violation of international humanitarian law.[144] This means that State agents whether they be military, intelligence or any other government actor are prohibited from encouraging civilians or groups to direct cyber-attack against civilian objects, irrespective of which channel or app is used to do so.[145]
iii. State have a due diligence obligation to prevent international humanitarian law violation by civilian hacker on their territory.[146]

A state cannot prevent all violations of the law but it must take all practicable measure such as taking public position[147] requiring civilian hackers not to conduct cyber operation

---

[139]Talinn Manual 2.0 Commentary on Rule 6, Para 5 (n134).
[140] Case Concerning Application of the Convention of the Prevention and Punishment of the Crime of Genocide, (*Bosnia and Herzegovina v Serbia and Montenegro*) (Judgment (2007) ICJ Rep 43, Para 430. <https://www.icj-cij.org/files/case-related/91/091-20070226-JUD-01-00-EN.pdf> accessed 1 October, 2025. See also James Crawford, 'State Responsibility: The General Part', (CUP 2013) 236-32 (on the distinction between due diligence and obligation conduct). Rudiger Wolfrum, 'Obligation of Results Versus Obligations of Conduct: Some thoughts about implementation of international obligation in Mahanorish H Arsanjani et al (ed.) Looking to the Future: Essays on International Law in honour of Michael Reisman (Brill 2010).
[141] Tillman and Mauro (n122)
[142] Common Act 1 to the four Geneva Convention of 1949.
[143] United Nation 'Responsibility of State for Internationally Wrongful Acts', (2005), Article 8 and ICRC Responsibility for violation of International Humanitarian Law, CIHL (2005) Rule 149 (a)-(d).
[144] Case Concerning Military and Paramilitary Activities in and against Nicaragua, (*Nicaragua v United State of America*) Merit Judgment of 27 June 1986, Para 220, <https://www.icj.org/files/case-related/70/070-19860627-JUD-01-00-EN.pdf> accessed October 1, 2025.
[145] Tillman and Mauro (n122).
[146] ICRC, 'Commentary on Convention III Relative to the Treatment of Prisoners of War, Geneva 12 August 1949, Commentary of 2020, Para 183, <https://www.data-base.icrc.org/en/ihl/-treaties/gciii-1949/article-1/comm entary/2020> accessed October 1, 2025.
[147] The Guardian, 'Amateur Hackers Warned against joining Ukraine's Army', (March 18, 2022), <https://www.theguardian.com/world/2022/mar/18/amateur-hackers-warned-against-joining-ukraines-it-army/> accessed October 1, 2025.

in relation to armed conflict, to respect IHL and suppress violations under their domestic law.

iv. States have an obligation to prosecute war crimes and take measures necessary to suppress other IHL violation.[148]

To achieve this, States are required to adopt and enforce the necessary laws that criminalize cyber operations that qualify as war crimes. Secondly they must adopt effective measures to stop all other violations of IHL which may include legal, disciplinary or administrative measures. Tillman and Mauro notes that adopting law or policies that turn a blind eye on civilian hackers conducting cyber operations as long as these operations are committed against the enemy does not comply with the listed obligation.[149] If all the measures articulated are practiced by States faithfully in time of peace and in the conduct of hostilities, it will drastically reduce the impact that the civilian and civilian objects are exposed to during armed conflicts. Repression of crimes by way of criminal prosecution must be encouraged either nationally as states have the primary responsibility to do so or internationally when the States are unwilling or genuinely unable to conduct trials.

4. Choice of Means and Methods of Warfare

The cardinal rule on the choice of means and methods of warfare is aptly captured in Art 35 AP I but the history of the control of means and methods of warfare dates back to St Petersburg Declaration of 1868 and posits that the 'only legitimate object of war is to weaken the military forces of the adversary'. The Declaration is the first formal agreement prohibiting the use of certain weapons in war. It had its origin in the invention, in 1863, by Russian Military authorities of a bullet which exploded on contact with hard substance and whose primary objective was to blow up ammunition wagons.[150] In 1867 the projectile was so modified as to explode on contact with a soft substance such that the Bullet would have been an inhuman instrument of war. The Russian government

[148] Article 48, 50, 129 and 146 GC I-IV, Article 85 Additional Protocol I
[149] Tillman and Mauro (n122)
[150] ICRC, 'Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grams Weight. Saint Petersburg, 29 November/11 December 1868, <https://www.ihl-database.icrc.org/en/ihl-treaties/st-petersburg-decl-1868>accessed 1 October 2025.

suggested that the use of the bullet be prohibited by international Agreement.[151] As noted earlier, the modern reiteration of this rule is captured aptly in Art 35 and it states:

i. In any armed conflict, the right of the parties to the conflict to choose methods and means of warfare is not unlimited;
ii. It is prohibited to employ weapons, projectiles and materials and methods of warfare of a nature to cause superfluous injury or unnecessary suffering.
iii. It is prohibited to employ methods or means of warfare which are intended, or may be expected to cause widespread, long-term and severe damage to the natural environment.[152]

Again, Article 36 provides that 'in the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by the protocol or by any other rule of international law applicable to the High Contracting party.'[153] The combined reading of these provisions reveal that parties to any conflict are not permitted to deploy any weapon of their choice. Weapons that will cause superfluous or unnecessary suffering or may harm the environment are prohibited. Furthermore, these weapons to be deployed must be subjected to the test contained in Articles 36 following the procedures laid down by the ICRC Guide on weapons review of 2006 and if they fail the test-whether its employment would in some or all circumstances, be prohibited by this protocol or by any other rule of international law applicable to the High contracting party, such a weapon must not be deployed.

The essence of these provisions is to avoid the use of weapons that will cause severe and extensive damage to the civilian population or harm civilian objects-objects indispensable to the survival of the civilian population. In the ongoing wars: Russia/Ukraine, Israel/Palestine, Hamas, Hezbollah and Lebanon there appear to have been a complete disregard of these rules. There have been severe damages to civilians and civilian objects. This is made worse by the fact that the wars are fought in civilian populated territories. The situation in Israel is more pathetic as the quest to decimate the non-state actors have led to devastating consequences on the civilian population.

[151] This rule was later laid down in Art 23(e) Hague Regulations on Land warfare of 1899 and 1907.
[152] Article 35(1)-(3) AP I.
[153] Article 36 AP I.

Thousands have died and or displaced and some fell victims in an attempt to escape the effect of the conflict.

The Cable News Network (CNN) reported that Israel carried out part of its device attack targeting Hezbollah by concealing explosives inside the batteries of pagers brought into Lebanon.[154] Series of controlled explosions of weaponised pagers were witnessed by the Lebanese security officials. Investigations are ongoing to determine the manufactures of the wireless communication devices and how they made their way into Hezbollah's pockets.[155] The blasts killed at least 37 people including some children, and injured nearly 3,000 and many of the affected were civilians.[156] If indeed Israel launched the attack, it will be a breach of its treaty provision as Israel is a High Contracting Party to the Geneva Conventions, Additional Protocols and other international law prohibiting the use of explosive devices particularly against the civilians population as the incidental harm to civilians far outweighs the military advantage they sought and this act breached the core tenets of IHL. The attack that led to the explosions of pagers should have been cancelled. Of particular interest is the fact that the use of booby traps and other remote or timer controlled devices is regulated primarily by the 1996 Certain Conventional Weapons (CCW) Amended Protocol II applicable in international and non-international armed conflicts.[157]

The pagers were booby trapped. "Booby-traps" are defined as any device or material which is designed, constructed or adapted to kill or injure and which functions unexpectedly when a person disturbs or approaches an apparently harmless object or performs an apparently safe act.[158] "Other devices" are defined as manually-emplaced munitions and devices (including improvised explosive devices) designed to kill, injure or damage and which are activated by remote control or automatically after a lapse of time.[159]

---

[154] Tamara, supra
[155] *Ibid*.
[156] *Ibid*, 2
[157] Amended Protocol II to the Convention on Certain Conventional Weapons
[158] Identical wording is used in Article 2(2) of protocol II to the Convention on Certain Convention Weapons and Article 2(4) of Amended Protocol II. see Nils Melzer, *International Humanitarian law: A Comprehensive Introduction* (ICRC: Geneva; 2016) 114.
[159] Amended Protocol II to the Convention on Certain Conventional Weapons, Art 2(5), and without the phrase in square brackets, see Protocol II Art. 2(3)

DOI: 10.5281/zenodo.19415894

There is a general prohibition on booby-trap or other devices that are delicately prefabricated in the form of apparently harmless portable objects and specifically designed to detonate when disturbed or approached.[160]

In ICRC's view, the prohibition against booby-traps attached to or associated with objects or persons entitled to special protection under IHL, and with objects likely to attract civilians, has become customary law in all armed conflicts.[161] The walkie-talkies and pagers explosions in the southern Lebanon can best be described as prefabricated objects that seemingly looked harmless, but turned out to be a prohibited means that has been deployed. It is important to fully investigate this act and bring perpetrators to justice.

5. Conclusion

The authors demonstrated the protection of civilians in the conduct of warfare in urban centres and against digital threats or cyber-attack. They extensively discussed the core tenets or principles of IHL, including distinction, proportionality and precaution. It was noted the strict compliance with the principles of distinction will reduce the impact of conflict on the civilian population but unfortunately, this has not been the case as civilians and civilian objects are subject to attack because military objectives are cited alongside civilian infrastructure. More difficult is the situation of dual use objects that are destroyed because the military also makes use of these objects both in cyber-attacks and other domains of warfare.

The paper also observed that the cyberspace contains both civilian and military information and targeting via the cyber space will also affect critical civilian infrastructure as there is no clear distinction in the cyberspace of civilian/military information. The paper further demonstrated that cyber-attacks have the capacity of destroying medical, banking, health, hospital and water infrastructure. Dams, Dykes and objects containing dangerous forces destroyed through cyber-attacks will cause incidental loss of civilian lives.

[160] Amended Protocol II to the Convention on Certain Conventional Weapon, (CCW) Art 7(2) and Protocol II to the Convention on Certain Conventional Weapons, Art. (6(1)(a).
[161] CIHL, Rule 80.

It was also demonstrated that wars fought via any domain of warfare must have control and here the principles of proportionality became crucial in minimizing incidences of collateral damage. It was further found the attacking State has a responsibility under the relevant rules to take precautions not to attack objects indispensable to the survival of the civilians and the defending State must take steps to mitigate the effects of an attack.

The paper further articulated measures to be adopted in order to mitigate civilian harm in the conduct of hostilities and recommended the continuous training of the members of the armed forces on what is acceptable in targeting. Civil societies, humanitarian organizations in collaboration with the Red Cross Societies should work with the local communities to support their self-protection techniques/strategies. For cyber operations, the paper noted that civilians must not be encouraged to directly participate in cyber-attack as they lose their civilian protection once they do so. The paper further noted that rules have been laid down prohibiting civilians in this regard. Additionally, four obligations have been set down for States in order to ensures that they comply with the 'due diligence' mandate. Two critical things observed includes that State will bear the responsibility for acts of persons who acted on their behalf and who they acknowledged as a party belonging to the State. Again, States are encouraged to prosecute those who commit acts constituting war crimes in addition to putting national legislations in place to address violations of IHL.

Finally, the paper considered the challenges of selecting means and methods of warfare and observes that the major problem is the lack of compliance with IHL rules by the High contracting parties with particular reference to the explosives of pagers and walkie-talkies in southern Lebanon on the 16th of September 2024. This was a blatant disregard of the rules laid down in the Certain Conventional Weapons (CCW) convention against booby-trapping objects that ordinarily are harmless and used by civilians. In the production of the pagers and walkie-talkies regard was not had to the provisions of Article 36 AP I.

Consequent on the above, it was recommended that civilians should be protected against the harsh effects of hostilities. Conflicts in city or urban areas must be conducted with IHL principles in mind and all efforts must be made to ensure that incidental losses to civilians and civilians population is reduced to the barest minimum and this includes

cyber-attacks too. States are called upon to train the members of the armed force and include the rules in their military manuals and ensure the implementation and compliance by prosecuting persons who deliberately conduct attacks against civilians and civilian objects.

KBLSP Journal