No. 9 - 2026

ISIL Occasional Paper

The Invisible Trapdoors of Peril: On Cyberattacks and Information Warfare in Contemporary Geopolitical Cyberspace

– Sulaksh Mehta

Abstract

The digital global network of today has gradually transformed into a necessary evil, not merely serving as a virtual platform to exchange information throughout, but also as a pioneer to numerous large-scale conflicts. These 'invisible trapdoors' of hybrid warfare, cyberattacks, and AI-amplified weaponisation raise alarming concerns, especially when geopolitically centred. This paper examines the recent escalations amid the Israel-Iran conflict as its central setting, highlighting key threats and countermeasures from humanitarian and digital lenses. Initiated on 28th February, 2026, through Operations 'Epic Fury' and 'Roaring Lion', Tehran sustained a larger cyber-kinetic conflict since Stuxnet. By analysing the doctrinal reports and empirical evidence from the US-Israel-Iran trilogy, the resulting synthesis will unravel the divergent coalition tactics, AI-amplified information warfare, and systematic regional disintegration. The paper further extrapolates global patterns and spatial arrangements, underscoring surges in AI-powered breaches and projecting losses worth billions in 2026. The 'regulatory vacuum' created by AI in International Humanitarian Law (IHL) is overshadowed by autonomous decision-making over the human elements of proportionality, distinction, and precaution, which will be crucially scrutinised through this paper, thereby addressing the geopolitical shift towards 'the infrastructural entanglement', which may further erode traditional civilian neutrality due to commercial hyperscalers becoming structural military components. With a forward-looking approach, the paper would finally present suggestions for a 'treaty-abiding AI' framework with robust methods aimed at safeguarding the geopolitical integrity of the digital world in real-time, not only providing for a digitally secure global network, but also effectively deterring AI-driven escalations in the future.

The "Necessary Evil" in the Warzone

A mere click of a button today holds the power to affect millions worldwide, the Iran 2026 war being one of the key instances of a similar scenario. 28th February, 2026 – the day when the globe witnessed a colossal geopolitical turn of events, with Operations 'Epic Fury' and 'Roaring Lion' as the factors bringing this picture into reality. Digital attacks and cyber-kinetic targeting have now amalgamated with conventional warfare, which has effectively blurred the line that separates military necessity and civilian protection. To understand the nuances of war, tracing down its history is essential. The conflict is a result of an ongoing culmination of the tensions arising between Iran and Israel over a 23-month span, with Israeli strikes killing 8 senior IRGC commanders, a direct missile attack on Israel by Iran in April 2024, and the 12-day war between the nations in June 2025.[1] The recent entry of Washington alongside Jerusalem has solidified into a notion of disarming Iran of its developing nuclear trajectory as a deterrent measure. The rationale behind this operation aims to remove a "major state sponsor of terrorism" which aspires to mastery over nuclear technology to its 'purest'; a justification highly debated. Mr. Antonio Guterres, the UN Secretary-General, and Ms. Mary Lawlor, the UN Special Rapporteur on Human Rights, demarcated the inconsistencies of such operations vis-à-vis the UN Charter's Prohibition on the Use of Force[2], upon examining the enrichment levels of uranium (insufficient for synthesizing nuclear weapons), opening a slit for potential chances for IHL violations if such operations continued. As of April 27, 2026, Amnesty International documented at least 3,300 fatalities, including 383 children, along with over 25,000 wounded,[3] not to mention the Iranian healthcare decline, leaving 292 medical and relief centres damaged or destroyed, 13 hospitals out of service, and 8 healthcare workers compromised. Moreover, with the damage to pharmaceutical factories and vaccine cold chains by the Pasteur Institute of Iran, the possibility of disease outbreaks in Iran is highly likely.[4] Geopolitically, Iran's partnership with China for nearly half a decade places the conflict in a broader Eurasian horizon. Being integrated into BRICS+ and the SCO places Iran at a strategic position, with the Strait of Hormuz – controlling one-fifth of the global energy supply – becoming both a physical and informational chokepoint. The nuclear angle is one of the most prominent reasons which has impacted geopolitics substantially. For a state to have highly enriched uranium exceeding 60% purity without declaring its nuclear ambitions raises significant concerns about breakout timelines, adding a factor of IRGC's supervision over the project; a big question mark on the fate of Iranian nuclear reserves. The ambiguity here is what makes the future use of nuclear energy a question that diverges into a progressive endeavour in Iranian development and a silent threat to global peace. What makes this conflict more threatening is the adoption of Artificial Intelligence as the mastermind of the chaos within and beyond the boundaries of the Middle East. Strategic analysts term this conflict as the 'first full-scale AI war' for establishing AI-based decision-support systems, having conducted over 5000 strikes in the first 10 days since the conflict escalated to war. The peculiarity is that conducting such strikes is humanly not possible. To be precise, what normally takes weeks to reinforce is generated within minutes now; Palantir's Maven Smart System, as integrated with Anthropic's Claude LLM, is a prominent example, which effectively generated real-time

target profiles by merely using unstructured satellite and signal projection throughout the conflict. The side-effects of compressing timelines have brought about an even more alarming concern: outdated training data, missing human rationale to assess regional demography, and brittle pattern recognition, taking away innocent lives in the Sharjareh Tayyebeh Girls' Primary School in Minab, Hormozgan province[5], as a measure of pre-emptive deterrence to nuclear threats, totally contradicting the principles of distinction, proportionality, and precaution as the basis of International Humanitarian Law.[6]

Digital Salvos on February 28th

The actual roadmaps of the operations, unlike conventional armed conflicts in human history, were initiated through the threat of cyber warfare, which infiltrated the Iranian regime from within, making it one of the largest cyber-attacks in the history of the geopolitical sphere, while also bringing Iran's Internet connectivity to less than 5% of its usual capacity. Impacts on SCADA/ICS systems, BGP dispatches, and the DNS framework by the U.S. Cyber Command were the first step of the operation 'Epic Fury' through which a pedestal of informed target selection set its foundation in favour of the U.S. and the Israeli forces, resulting in over 1,200 strikes in Iran within the first 48 hours of the conflict. Algorithmic pattern recognition and behavioural analyses were another factor which became handy for the 'saviours' of the Iranian regime, most evidently the urban sensor networks, including civilian infrastructure like traffic cameras and IoT services. The silent warfare began long before February 28th, when Iranian network connectivity was limited, Starlink became a boon for the masses, the Iranian regime was on the brink, and the protests were widespread, not to mention the fall of the Iranian Rial in the forex market. The silent information breaches and the sequences of daily Iranian life as a behavioural database became a weapon that significantly impacted the regime; the assassination of Supreme Leader Ayatollah Ali Khamenei in the American airstrikes being one landmark incident, and that also within a 60-second window using precise hacktivism and AI-based predictive models. The development of the already precise database and network breaches even turned civilian technology into a guide to Iran's socio-political scenario, blurring the line that distinguishes civil aspects from military necessities. 'BadeSaba Calendar Prayer app', an app meant for religious observance with over 5 million downloads and a symbol of ideological legitimacy, also became a source of hackers to psychologically affect the populace by taking over the notification system and urging millions to surrender in exchange of amnesty.[7] Coincidentally, this overlapped with the first salvo of kinetic strikes, physically and psychologically weakening Iran. Naturally, a society would be very vulnerable to questioning its own regime's effectiveness in the situations with no guarantee of safety and a pseudo-paralysis of the security and defence frameworks, not to mention the anti-regime propaganda backed by IRNA and IRGC-linked state news agencies to add fuel to the fire that engulfed the regime from inside-out, along with its authority over the social framework, and reduced it to the ashes at the time when establishing credibility was the most crucial requirement.[8] These methods to finally achieve world peace through depriving Iran of its nuclear observatories and resources, the root of all problems, stand unaffected despite numerous strikes on the nuclear infrastructure. Reports suggest that the whereabouts of Iran's uranium stockpile enriched to 60% remain uncertain, with chances of presence in areas like Fordow and Isfahan tunnel complexes. To respond to all the invisible trapdoors, Iran retaliated through drone strikes over the

prominent "hostile technical" hyperscalers based in UAE and Bahrain, along with several U.S. military facilities, along with proxy hacktivist groups beyond Iranian borders as a result of limited network connectivity in Iran, releasing waves of website defacements, data exfiltration and so on. [9]

Minab School Strike

The planning, identification and execution of strikes is a laborious endeavour that costs weeks and even months. When over 5,000 strikes have taken place in less than 2 weeks in Iran, the process to roadmap raises concerns vis-à-vis the methods adopted to initiate such actions that far exceed human capabilities. The "target factory" models, as termed by analysts, rely on unstructured repositories, databases and advanced AI models, which may compress timelines from minutes to weeks, but the accuracy of such sources becomes the grey area; "necessary" for some, a nightmare for many. Such demonstration also brought about tragedy upon hundreds, with a U.S. Tomahawk cruise missile impacting the Shajareh Tayyebeh Girls' Primary School in Minab, Hormozgan province. Iran's local media reported around 150 casualties on 28th February, 2026, raising serious questions over AI-driven targeting systems and a case that is a landmark for the contemporary warfare. Though AI reasoning produces far more efficient results, the quality is the aspect that bears the brunt. The execution may be well-planned, but what about the information that it is fed? Who bears the accountability? There are many ways the aggrieved can be exploited, but what about the IHL and its core facets? When a system fails to distinguish a military structure from a school based on outdated information about its location, the algorithmic brittleness will not be a justice provider in any case, but may shape into another humanitarian concern the history has never seen. Mr Abbas Araghchi, the Iranian Foreign Minister, terms this a "deliberate, calculated phased assault" despite already possessing the most advanced and precise armoury, military and databases, as addressed in the UNHRC, while also negating the claims of the Pentagon stating malfunctions and errors as a justification. In any case, the incident is not unforeseeable and raises questions over the objective the West aims to achieve; worst of all, an actual invisible trapdoor of unreliable automated warfare at the cost of civilian lives. The U.S. Central Command requires humans to decide the targets meant to be neutralised, but we need to understand the difference between human approval and human control, along with the significance of human reasoning and judgment as suggested by the International Committee of the Red Cross. Such failures raise serious concerns over ineffective global diplomacy. The Responsible AI in the Military Domain (REAIM) Summit, for instance, was congregated in A Coruña, Spain in February 2026, just weeks before the conflict actually erupted. Even then, if the "Pathways to AI" declaration received 35 signatures out of 80 participating countries, with the abstaining countries ending up being a part of this conflict in the future, such conventions directly indicate geopolitical instability and diplomatic inefficiency.[10]

Commercial Digital Weapons Arsenal

The sequence was decisive. After Israel attacked Iran's nuclear sites with a major cyberattack, internet connectivity to Iran was just 1-4% of normal levels. Three days later, Iran's retaliation took a kinetic turn. On March 1, 2026, at the break of dawn, Iranian Shahed drones attacked two Amazon Web Services data centres in the U.A.E. An explosion nearby damaged another

commercial data centre in Bahrain, reports claim. In the history of warfare, it is the first time ever a state has conducted deliberate kinetic attacks on commercial data centres. The attacks were coupled with a complete legal/doctrinal intensification. In essence, on March 11, 2026, an official list of military targets for the IRGC-affiliated Tasnim News Agency was disseminated by telegram. These included regional offices, data centres, and research facilities for companies such as Google, Microsoft, Amazon, NVIDIA, IBM, Oracle, and Palantir. These targets were specifically identified by name and location. According to the IRGC-linked Khatam-al Anbia Headquarters, the use of this language was to deliberately escalate doctrine. "As the regional war has moved to an infrastructure war," said the headquarters, "the scope of Iran's legitimate targets will expand." It was logical for Iran to take this approach. All of these companies have well-documented Pentagon contracts and provide technology with direct military uses. Palantir's Maven Smart System powers the AI based targeting chain. AWS hosts the $581.3 million Iron Dome cloud contract. In essence, Iran is saying that when you host military AI workloads on your commercial data centre, you are taking what would otherwise be civilian infrastructure and turning it into a military objective. By March 31, Iran's state media had expanded the list of targeted companies to include Apple, Meta, Intel, HP, Cisco, and Dell. The immediate consequence of this action extended far beyond the military sphere into daily life. The AWS attacks created extensive outages for Emirates NBD (banking), First Abu Dhabi Bank (banking), Abu Dhabi Commercial Bank (banking), Hubpay (payments) and Careem (ride sharing). Out of the three availability zones within the UAE region, two were down at the time of writing. This outage was not collateral damage in the way we traditionally think about it – it was the result of attacking infrastructure that Iran itself had described as being used militarily. Most of the technology that makes up modern society depends on commercial data centres and therefore, by damaging them, you can significantly impact a country's ability to wage war while also having a profound social impact. Beginning with the economic dimension, which has been an integral part of global technology investment architecture for decades, the Gulf States have become recipients of hundreds of billions of dollars in Western technology investments based upon their past commitment to stability. One example is OpenAI's new Stargate AI campus, located in the UAE, and supported by some of the world's leading tech firms (Oracle, Nvidia, Cisco), situated today in a region where Iran has made it clear that it can strike the commercial technology infrastructure of its adversaries at will. While standard insurance policies may provide coverage for loss due to natural disasters, etc., they are generally not designed to cover losses caused by acts of war – so all losses from the two AWS cyberattacks would fall directly to the companies involved. It is impossible to understand why Iran has chosen to attack commercial infrastructure without also understanding the role that the nuclear aspect of the conflict plays. On April 28th, 2026, International Atomic Energy Agency (IAEA) Director-General Rafael Grossi reported that there were still over 200 kg of Iran's total 440.9 kg stockpile of highly enriched uranium remaining in underground storage facilities at the Isfahan nuclear facility. IAEA seals had been in place at these facilities since June 2025 when international inspectors stopped going into the sites. In a televised speech on April 30, 2026, Iranian Supreme Leader Mojtaba Khamenei said that "Iran" would protect its nuclear program,

missile systems and advanced technological programs just as much as it protects its physical territory; and stated that Iran would begin implementing "new management" of the Strait of Hormuz — which includes charging tolls to any vessel that passes through the waterway.[11] The diplomatic response to Iran's actions has shown how ineffective such responses can be. On March 11, 2026, the United Nations Security Council passed a resolution demanding that Iran cease attacking its neighbours in the Gulf. The resolution did address kinetic strikes against neighbouring countries. However, neither the resolution nor any other UN document mentioned the fact that Iran has publicly declared a policy of conducting an infrastructure war against the U.S. and others; nor did it reference the body of law — both national and international — regarding what constitutes permissible targets under the laws of war, particularly those related to digital dual-use infrastructure.[12] This "regulatory vacuum," discussed in detail throughout this paper, is best exemplified by the large gap between what the UN Security Council has been willing to prohibit in terms of Iran's conduct versus what Iran has already established as part of its official doctrine.

AI-Amplified Information Warfare

These technologies have created a "Reality Crisis". A Reality Crisis is an area of confusion when people are unsure about the difference between truth and deception. An example of how the Reality Crisis can manifest itself is through the use of deepfakes; which are a new form of digital technology used to create synthetic images or videos that appear real. Deepfakes enable a wide variety of users (including adversaries) to claim their own legitimate, vetted and confirmed evidence has been fabricated. This was demonstrated in Israel. On several occasions, Israeli Prime Minister Benjamin Netanyahu publicly denied rumours surrounding his death. He presented video proof of himself being alive after each time. However, despite all of this evidence being independently reviewed and confirmed through forensic examination, many citizens refused to believe him. In fact, there were even citizens who claimed Netanyahu was actually dead. This is because it is now possible for anyone to generate realistic-looking video content. Therefore, the same ability that makes it easier to make realistic fake videos also creates uncertainty regarding what is true and what is not. Iranian government-sponsored social media accounts were using this type of uncertainty. Iranian researchers call this "Forensics Cosplay," i.e., using fake heat maps and other analytical tools to appear as if they are analysing photos/video documenting atrocities/protests in order to show those documents are fake. These posts are intended to prevent the public from becoming aware of atrocities such as the Minab school strike. At least 120 students were compromised on February 28th, 2026 during the Minab school strike. The most visible vector of Iran's AI-amplified information campaign was the "Explosive Media" unit, operating under the direction of a figure known as "Mr. Explosive."[13] These videos, which are believed to have been viewed by hundreds of millions of people, showed the Iranian military destroying various pieces of Gulf State infrastructure that actually took less than significant damage. The video showing the capture of a downed American fighter pilot generated enough false narrative to get one US-based TikTok influencer telling his followers that the Lego videos were "so shockingly accurate in revealing what was not just a rescue operation, but really a very special operations uranium mission." There never was any special operations uranium mission — US Special Forces did in fact rescue

the pilot. When questioned about the factual inaccuracies, Mr. Explosive stated "only 13 percent of what Trump says is true" — thus refusing to engage with the evidence, he moved the debate to a meta level regarding who has credibility as a source. Dr Emma Briant of the University of Cambridge said that the reason for this success came from AI's ability to produce culturally appropriate content utilising training materials primarily from Western countries — capabilities that "states wishing to attack the West had not previously possessed", according to Dr Briant. Also, Dr. Tine Munk of Nottingham Trent University described Iran's use of social media and misinformation campaigns as "defensive memetic warfare", stating that they used social media to circumvent traditional forms of diplomacy (intermediary parties such as press and media) and "continuously disseminate memes." This informational disorder occurred due to both intentional misrepresentation, as well as limitations built into the design of generative AI systems. For example, Divya Chandra of BOOM documented how the Grok Chatbot created by xAI was asked questions about a single viral war video; within a span of 24 hours, Grok produced three different explanations for where the video was shot, at different times, and with different country names. This is an example of a structural limitation of large language models that predict words or phrases as opposed to verifying facts. The Red Alert campaign shows how Information Warfare (IW) can support Physical Targeting. Threat Actors exploited civilians' desperation to receive warning messages about incoming missiles by sending them SMS Spoofed Messages containing an App that was a Trojan Horse Version of the Israeli Emergency Warning System. When executed, the App sent all of the civilian's Contact List & Real-Time GPS Coordinates to the attackers. Those same types of data can help map where people will seek Shelter during attacks, Track Movement of Displaced Populations, identify IDF Reservists, and Help Optimize Missile Fire.[14] Red Alert shows how Psychological and Kinetic Domains have become Converged. The Action of Seeking Protection Became a Vector of Vulnerability. The Conflict has shown that there is a systematic process to create conditions under which the Evidentiary Basis for enforcing IHL (the Documentation of Civilian Harm, Attributing Responsibility, Verifying Compliance with Distinction and Proportionality) is Perpetually Contestable.

IHL Principles Under Algorithmic Tensions

The Principle of Distinction requires Parties to an Armed Conflict to differentiate between civilians and members of armed forces, as well as between civilian property and military targets. However, the International Committee of the Red Cross in its 5 January 2026 report (which was less than eight weeks prior to the start of hostilities) stated that making the determination of who is a legal target will require "qualitative" judgments based on context which cannot be quantified through algorithms. Proportionality is defined as an attack which may cause civilian casualties disproportionate to the foreseeable, concrete and direct military gain from it. When making such assessments, decision-makers are required to weigh incommensurably valued considerations by engaging in a deliberate, reflective process. In contrast, the 2026 war was characterised by the use of nearly 1,000 strikes within its initial twelve hours and nearly 5,500 strikes in the ten-day period immediately after. Therefore, no meaningful human can perform a proportionality assessment at

this speed. Studies have demonstrated that in situations involving time constraints, human operators rely on the advice provided by AI approximately three times more often than when deliberation is permitted. International legal expert Mahmoud Abdelwahab wrote on Opinio Juris regarding the 2026 war that "both International Humanitarian Law (IHL) and International Criminal Law (ICL) provide sufficient mechanisms to address at least the most severe cyber operations taking place during an armed conflict." Abdelwahab identifies the lack of practical means of enforcing these laws as the root of the problem. He states that because of classification disputes; difficulties related to evidence gathering; and the general inability to identify those responsible for cyber-attacks due to their location in cyberspace; it is nearly impossible to effectively enforce IHL/ICL with respect to cyber-operations. According to research conducted by the Raoul Wallenberg Institute, autonomous weapons systems represent a structural challenge with regard to holding individuals accountable for violations of IHL. Autonomous systems do not possess the capacity to assume either legal or moral responsibility. IHL addresses itself to humans — specifically those planning, deciding upon and carrying out attacks — not algorithms. As a result of delegating the critical functions associated with identifying and targeting objectives to software, sensors, and machine learning models, it becomes very difficult to trace decisions made through autonomous systems back to identifiable human decision-makers.[15] The actions taken by the parties involved in the Minab incident demonstrate this diffusion of responsibility. Potential liability could exist among several entities including those who developed the programming used for the target recognition algorithm; those who provided the 2016-era training data for the target recognition algorithm; those who authorized the operational parameters of the system; and finally, the human who reviewed and ultimately decided to execute the strike under duress of time. In order to create the chain of responsibility model — advocated by the International Committee of the Red Cross (ICRC) and Stockholm International Peace Research Institute (SIPRI), in order to assign responsibility through each stage — design, production, programming, deployment, activation, and command authorization — there was never established a mechanism for operationalizing this model within a system of binding international law as of 2026. As such, an accountability vacuum has developed according to Human Rights Watch, i.e., no individual person can be meaningfully held accountable for criminal liability resulting from civilian suffering with regard to demonstrably severe harm.[16] Although an institutional mechanism exists to address the issues outlined in this section, it remains without the enforcement authority or power of law. Since 2013, the CCW Group of Governmental Experts on Lethal Autonomous Weapons Systems have convened and produced Guiding Principles emphasising IHL's application. On May 22, 2023, United Nations Secretary-General António Guterres and ICRC President Mirjana Spoljaric called for the development of new, legally-binding norms regarding autonomous weapons systems by 2026. As described above, the legal degradation of lethal autonomous weapon systems will also be furthered by geopolitical realities. According to the Institute for the Study of War, on April 30, 2026 Supreme Leader Mojtaba Khamenei stated that Iran will defend its nuclear and missile capabilities "with the same tenacity with which we protect our territorial borders," and will establish "new management" of the Strait of Hormuz. By that time, Major General Ahmad Vahidi had taken control of military operations and negotiations

involving the IRGC. This context illuminates why the regulatory vacuum is not merely a legal-technical problem. The AI systems that enabled the initial U.S.-Israeli campaign were deployed in pursuit of nuclear objectives—degrading Iran's enrichment infrastructure and preventing breakout. Yet the prevention of nuclear proliferation does not suspend IHL obligations. When AI acceleration makes 5,500 strikes in 10 days operationally feasible, the means themselves reshape what counts as an achievable end, and proportionality becomes not a constraint but an afterthought.

Towards a Treaty-Abiding AI Framework

A key finding of this study is structural — the international community has no laws or institutions to regulate how quickly the international community can deploy weapons systems using artificial intelligence (AI) to make combat decisions. The nuclear dimension is not marginal, it is the operational premise — the AI-based target identification that resulted in the Minab airstrike were used to reduce Iran's capability to produce enriched uranium. There are also four pillars for the proposed framework as they relate to current rules of International Humanitarian Law (IHL). These include mandatory Article 36 review reforms requiring actual human oversight over the deployment of AI-enabled lethal force[17] — not simply nominal approval; "digital civilian immunity corridors" providing protection for hospitals, water supplies, electricity grids, and financial networks from being targeted based upon dual-use arguments; accountability for supply chains of AI technology, similar to what exists today with respect to the export of materials related to nuclear programs; and inclusive cyber ceasefire architecture monitored through third-party verification mechanisms — a response to the April 2026 cease fire agreement which included an exception regarding cyber operations while Iranian Advanced Persistent Threat groups continue to target critical United States' infrastructure. However, there needs to be a shift in thinking about the process of achieving a new international regulatory regime. While the number of countries signing onto the revised version of REAIM has declined from 80 to 35, these results demonstrate that many nations do not have sufficient political will to adopt new treaties; however, a lower-level approach may still exist that could help slow down the decline in norms governing AI-enabled warfighting capabilities. An intermediate framework that includes provisions requiring disclosure, establishes a risk hierarchy of military uses of AI capabilities and provides mechanisms for building trust among nations could help stabilise the international norms environment. In addition, there should be a prohibition on autonomous decision-making using AI-augmented capabilities, just like there is with regard to nuclear armed forces.[18] All of IHL remains legally valid. However, all the principles that underpin IHL cannot prevent the unintended consequences resulting from institutional lag — i.e., the time required for diplomats to deliberate on issues relating to AI-enabled warfighting capabilities versus the time at which AI systems can execute those same capabilities. In order to bridge this gap and maintain human responsibility for making decisions involving lethal force, the international community must recognise that statements alone will not suffice.

References

1. Institute for Economics & Peace, *Global Terrorism Index 2026: Special Supplement – The Iran War and the Global Terrorism Threat* (ReliefWeb, March 18, 2026).
2. Ibid.
3. United Nations, *Charter of the United Nations*, 1 UNTS XVI (1945), art. 2(4).
4. Amnesty International, "Iran: 2026 Conflict Casualty Figures," April 27, 2026.
5. *The Lancet*, "Systematic Degradation of Healthcare Infrastructure in the 2026 Iran War," April 2026.
6. "Iran Names U.S. Navy Officers Responsible for Minab School Strike," *The Indian Express*, March 29, 2026.
7. "Iranian Prayer App Hacked to Send Anti-Government Notifications to 5 Million People," *24 Kanal*, March 1, 2026.
8. Taiwan Institute for National Defense and Security Research, *Cyber-Information Operations in the 2026 Iran Conflict: An Assessment*, 2026.
9. "Iranian Drones Disrupt Work of Amazon Data Centers in Bahrain — Company," *TASS*, March 24, 2026.
10. "Iranian Lego Videos Against Trump and the War in Iran," *SRF News*, April 16, 2026.
11. CloudSEK, "RedAlert Spyware Campaign Exploits Wartime Panic with Trojanized App," *Infosecurity Magazine*, March 2, 2026.
12. International Committee of the Red Cross, *Autonomous Weapon Systems and International Humanitarian Law: Selected Issues* (Geneva: ICRC, January 5, 2026).
13. "Negotiators in Islamabad, Divide in Tehran; Analysts Flag Fractured Iran Top Brass," *ANI News*, April 25, 2026.
14. Institute for the Study of War, "ISW-CTP Assessment: Iran Conflict Update, April 30, 2026," 2026.
15. Sri Lanka, "Statements by Sri Lanka at the First Session of the 2026 CCW Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (GGE on LAWS)," March 2–6, 2026, Geneva.
16. "Más de 30 Estados Firman un Manifiesto para que la IA en Defensa Contribuya a la Paz," *EFE*, February 5, 2026.
17. Raoul Wallenberg Institute, *Autonomous Weapons Systems and Accountability Under International Law* (Lund: RWI, 2025).
18. Human Rights Watch, *Accountability Vacuum: Autonomous Weapons and Criminal Liability* (New York: HRW, 2025).
19. Mahmoud Abdelwahab, "The Applicable Legal Framework to Cyber Operations in the Context of the Iran-Israel Conflict," *Opinio Juris*, March 2026.

20. Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), 1125 UNTS 3 (1977), art. 36.

Endnotes

1 Inst. For Econ. & Peace, Global Terrorism Index 2026: Special Supplement – The Iran War And The Global Terrorism Threat (Mar. 18, 2026).

2 U.N. Charter art. 2, ¶ 4.

3 AMNESTY INT'L, Iran: 2026 Conflict Casualty Figures (Apr. 27, 2026).

4 *The Lancet*, Systematic Degradation of Healthcare Infrastructure in the 2026 Iran War, Apr. 2026.

5 "Iran Names U.S. Navy Officers Responsible for Minab School Strike," *THE INDIAN EXPRESS*, Mar. 29, 2026.

6 Int'l Comm. Of The Red Cross, Autonomous Weapon Systems And International Humanitarian Law: Selected Issues (Jan. 5, 2026).

7 "Iranian Prayer App Hacked to Send AntiGovernment Notifications to 5 Million People," *24 KANAL*, Mar. 1, 2026.

8 TAIWAN INST. FOR NAT'L DEF. & SEC. RESEARCH, CYBERINFORMATION OPERATIONS IN THE 2026 IRAN CONFLICT: AN ASSESSMENT (2026).

9 "Iranian Drones Disrupt Work of Amazon Data Centers in Bahrain – Company," *TASS*, Mar. 24, 2026.

10 "Más de 30 Estados Firman un Manifiesto para que la IA en Defensa Contribuya a la Paz," *EFE*, Feb. 5, 2026.

11 INST. FOR THE STUDY OF WAR, ISWCTP Assessment: Iran Conflict Update, Apr. 30, 2026.

12 Mahmoud Abdelwahab, The Applicable Legal Framework to Cyber Operations in the Context of the IranIsrael Conflict, *OPINIO JURIS*, Mar. 2026.

13 "Iranian Lego Videos Against Trump and the War in Iran," *SRF NEWS*, Apr. 16, 2026.

14 CloudSEK, "RedAlert Spyware Campaign Exploits Wartime Panic with Trojanized App," *INFOSECURITY MAGAZINE*, Mar. 2, 2026.

15 Raoul Wallenberg Inst., Autonomous Weapons Systems And Accountability Under International Law (2025).

16 Human Rights Watch, Accountability Vacuum: Autonomous Weapons And Criminal Liability (2025).

17 Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Additional Protocol I), art. 36, 1125 U.N.T.S. 3 (1977).

18 Sri Lanka, Statements by Sri Lanka at the First Session of the 2026 CCW Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (GGE on LAWS), Mar. 26, 2026, Geneva.

About the Author

Sulaksh Mehta is a second-year law student at the School of Law, CHRIST (Deemed to be University), Bengaluru, with a keen academic interest in the contemporary facets of public international law and cybersecurity laws. He aspires to step into the fields with litigation assignments based on International Litigation and digital safety within and beyond the Indian borders. This research project has been conducted under the guidance of Dr. Kanika Sharma, Assistant Professor, Head - Centre for Advanced Studies in International Humanitarian Law and Military Law at the Indian Society of International Law, New Delhi.

Views expressed in this paper are of the author and in no way to be considered the views of the Indian Society of International Law.

About the ISIL

The Indian Society of International Law (ISIL), a premier national institution for teaching, research and promotion of international law was established in 1959. In sixty-six years of its existence, the ISIL, under the dynamic leadership and guidance of distinguished persons, has grown into a prestigious research and teaching centre of international law in India. It has played a leading role in shaping the thoughts on international legal issues not only in the region, but also in generating informed debates across the world. The ISIL aspires to foster nation-wide study, research, interpretation, development, and appreciation of international law. In order to transform ISIL as a multi-disciplinary progressive policy research and narrative building in international legal matters and achieve its vision, ISIL brings out publications in the form of Journals, Books, Monographs, Occasional Papers, and articles by the researchers and members.

At present ISIL enjoys the able stewardship of its President Prof. (Dr.) Manoj Kumar Sinha.

The Indian Society of International Law (ISIL)

VK Krishna Menon Bhawan, 9, Bhagwan Das Road, New Delhi 110001
Tel: 91-11-23384458/59, E-mail: isil@isil-aca.org

Price: ₹ 250.00