Adv. J. Manag. Humanit. Soc. Sci. (**2026**), Volume 2, Issue 4, 295-309

Advanced Journal of Management, Humanity and Social Science

Journal homepage: https://www.ajmhss.com/

DOI: https://doi.org/10.5281/zenodo.22129202

Legal Dimensions of the Prohibition of Attacks on Infrastructure under International Law: The 2026 US-Israel Strikes on Iran's Critical Infrastructure and Legal Avenues for Litigation in International Courts

Mehdi Nematolahi
Member of the Bar Association of Fars Province

Article info
Received: 20.06.2026
Accepted: 26.08.2026
Available Online: 27.08.2026
Checked for Plagiarism: Yes

Keywords:
Critical infrastructure, international humanitarian law, principle of distinction, dual-use objects, state responsibility

ABSTRACT

Attacks on critical infrastructure, whether kinetic or cyber, constitute one of the most pressing challenges in contemporary international law. The 2026 joint military strikes by the United States and Israel against Iran's nuclear facilities, energy infrastructure, bridges, and transportation networks, combined with concurrent cyber operations targeting communication systems, have reignited debate over the legal framework governing such attacks. This article examines the legal dimensions of the prohibition on infrastructure attacks under international law, analyzing the US-Israel strikes as a case study and exploring available legal avenues for Iran to seek recourse before international judicial bodies. Using a descriptive-analytical methodology grounded in treaty interpretation, customary international law analysis, and judicial precedent, this research finds that while international humanitarian law (IHL) provides a robust framework through the principles of distinction, proportionality, and precaution, the concept of "dual-use" objects objects with both civilian and military applications creates significant interpretive ambiguity . Despite this ambiguity, Article 56 of Additional Protocol I explicitly protects nuclear power plants from attack where such attacks may cause dangerous force release, and the International Criminal Court (ICC) has established precedent by issuing arrest warrants for attacks on Ukrainian critical infrastructure. The research identifies four principal legal avenues: proceedings before the International Court of Justice (ICJ), prosecution before the ICC, arbitration through bilateral dispute resolution mechanisms, and domestic litigation. However, significant obstacles persist, including the United States' withdrawal from the 1955 Treaty of Amity with Iran, non-membership in the Rome Statute, attribution challenges for cyber operations, and evidentiary difficulties. The article concludes that while international law prohibits attacks on critical infrastructure, enforcement mechanisms remain inadequate, and the most effective long-term strategy involves strengthening multilateral cooperation and developing a dedicated convention on critical infrastructure protection.

Introduction

The prohibition of attacks on civilian infrastructure represents one of the cornerstones of international humanitarian law (IHL), rooted in the fundamental principle that civilians and civilian objects spared from the effects of hostilities. Article 48 of Additional Protocol I to the Geneva Conventions articulates this principle by requiring parties to a conflict to distinguish at all times between military objectives and civilian objects, directing operations solely against military objectives.

This foundational rule reinforced by Article 52, which defines military objectives and establishes that civilian objects not made the object of attack, and by Article 51, which prohibits indiscriminate attacks. Together, these provisions create a normative framework designed to protect the infrastructure upon which civilian life depends.

Corresponding Author: **Mehdi Nematolahi (Mehdiradman13591391@gmail.com)*

However, the practical application of these rules has become increasingly complex in modern armed conflicts, particularly with the emergence of "dual-use" objects infrastructure that serves both civilian and military functions. As Lattimer (2026) observes, "dual-use is not a recognized concept in the law of armed conflict (LOAC)". This lack of formal recognition creates interpretive challenges, as commanders must determine whether a particular object's military use renders it a legitimate military objective or whether its civilian function necessitates protection. The 2026 US-Israel strikes against Iranian infrastructure vividly illustrate these tensions. The campaign, codenamed "Epic Fury" by the US and "Roaring Lion" by Israel, targeted nuclear facilities including the Bushehr Nuclear Power Plant, the Khondab heavy water complex, and yellowcake production facilities, along with energy infrastructure such as the South Pars gas field, bridges, and transportation networks.

The official justification for these strikes preemptive self-defense against Iran's alleged nuclear weapons program and regional threats raises fundamental questions about the legality of attacking infrastructure that the International Atomic Energy Agency (IAEA) had previously verified as peaceful. The Atomic Energy Organization of Iran (AEOI) confirmed that Bushehr Nuclear Power Plant had struck by a projectile for the third time. These attacks prompted Iran to consider withdrawal from the Treaty on the Non-Proliferation of nuclear weapons (NPT), with Iranian institutions urgently reviewing the issue. The legal significance of this development cannot be overstated: if Iran were to withdraw, the international community would lose vital verification mechanisms, potentially undermining the global non-proliferation regime.

The concurrent cyber operations against Iranian communication systems and news websites further complicate the legal analysis. These operations, characterized by unauthorized intrusions into sovereign cyber infrastructure, raise questions about the application of the sovereignty principle in cyberspace. The Tallinn Manual 2.0's experts have articulated various modalities for determining sovereignty violations, including causation of physical damage, loss of functionality, and interference with inherently governmental functions. However, consensus on thresholds remains elusive, particularly for operations that do not cause physical consequences or significant loss of functionality.

The international community's response to the strikes has divided. The United Nations High Commissioner for Human Rights explicitly stated, "Deliberately attacking civilians and civilian infrastructure is a war crime," while the UN Secretary-General's Spokesperson emphasized that "civilian infrastructure, including energy infrastructure, may not be attacked". The International Committee of the Red Cross (ICRC) likewise denounced threats against essential civilian infrastructure. Yet these condemnations have not translated into concrete enforcement action, highlighting the persistent gap between legal prohibition and effective accountability.

This article seeks to address four key questions: First, what are the applicable legal norms governing attacks on critical infrastructure under international law? Second, how do the 2026 US-Israel strike against Iranian infrastructure measure against these norms? Third, what legal avenues are available for Iran to seek redress before international courts and tribunals? Fourth, what are the principal obstacles to effective legal recourse, and how they addressed? The analysis proceeds in five parts. Following this introduction, Part II examines the relevant legal framework, including treaty provisions, customary international law, and judicial precedent. Part III analyzes the 2026 strikes as a case study, applying the legal framework to specific infrastructure targets. Part IV identifies available legal avenues and assesses their feasibility. Part V concludes with recommendations for strengthening the legal protection of critical infrastructure.

Literature Review

The scholarship on attacks on critical infrastructure under international law has evolved significantly, particularly in response to the increasing frequency of such attacks in contemporary armed conflicts. Beig Zadeh (2025) provides a comprehensive analysis of the prohibition on attacks on critical infrastructure, arguing that despite the absence of a treaty-based definition, a customary definition inferred from state practice and the positions of international organizations. He notes that the international community has recently begun reinforcing this prohibition through the International Criminal Court's (ICC) issuance of arrest warrants against Russian military authorities for attacks on Ukraine's critical infrastructure, which the ICC recognized as war crimes. This development, while limited to armed conflicts, represents a significant step toward addressing impunity.

The concept of "dual-use" objects has received particular scholarly attention. Capone (2025) observes that dual-use objects such as energy infrastructures, water installations, and civilian transportation systems that may also serve military purposes have "entered the IHL jargon but has not attained the status of a legal concept" . This liminal status creates legal uncertainty, as belligerents may exploit the ambiguity to justify attacks on civilian infrastructure. Capone argues for a paradigm shift that "places under the spotlight the civilian function of dual-use objects and reclaims the central role of the individual actors that plan, order and execute attacks against these targets". This approach aligns with the ICC's jurisprudence, which holds that "an

attack directed against a civilian population may also serve other objectives or motives" but remain an attack on civilians (Ntaganda Appeal, para.424).

Lattimer (2026) critically examines the legal treatment of dual-use objects, dual-purpose attacks, highlighting a concerning trend in Israeli and US practice toward insisting on a subjective test of intent for determining targeting violations. Under this approach, "without proof of individual intent (criminal mens rea), there is no violation". This shift has significant implications for both state responsibility and the personal liability of commanders, as it raises the evidentiary bar for establishing violations. Lattimer further notes that "designating whole categories of civilian objects as 'dual-use' may appear to have the effect of making them military objectives liable to attack," but warns that "it also invites scrutiny of the purpose or purposes of such conduct and whether such purposes include... 'Directing attacks against civilians or civilian objects'".

The evidentiary challenges in proving attacks on critical infrastructure have also extensively analyzed. Roscini (2015) examines the application of the International Court of Justice's (ICJ) rules on evidence to cyber operations, noting that the Court approaches the drawing of inferences with great caution. However, when direct evidence lies within the exclusive territorial control of the other litigant, the Court may allow "a more liberal recourse to inferences of fact," provided they leave "no room for reasonable doubt". This principle, established in the Corfu Channel case, has particular relevance for cyber operations, where state control over cyber infrastructure may make direct evidence inaccessible. Roscini also notes that even evidence obtained through unauthorized intrusion into another state's computer systems take into account by the Court, although the purpose of collecting evidence does not exclude the illegality of the conduct.

The ICJ's jurisprudence on attacks on infrastructure includes the pivotal Oil Platforms case (Iran v. United States, 2003). Iran brought proceedings against the United States based on the 1955 Treaty of Amity, alleging that US Navy attacks on Iranian offshore oil platforms in 1987 and 1988 violated the Treaty's freedom of commerce provisions. The Court rejected the United States' self-defense justification, finding that the US had not demonstrated that the attacks were necessary and proportional responses to an armed attack. However, the Court ultimately rejected Iran's claim on the grounds the platforms either under repair (thus no trade was occurring) or trade suspended due to an embargo. The case nonetheless established important principles regarding the application of bilateral treaties to disputes involving the use of force.

In the realm of cyber operations, Hollis and Sukumar (2026) explore the concept of "prepositioning" the practice of maintaining backdoors in cyber infrastructure for future use and its compatibility with international law. They argue that existing rules, including sovereignty, non-intervention, and the prohibition of the use of force, are insufficient to address this phenomenon. They propose an object-based approach that would prohibit prepositioning operations against civilian critical infrastructure regardless of whether they attributed to a specific state. Similarly, the Tallinn Manual 2.0's Rule 121 suggests that states are obligated to take precautions to protect civilians and civilian objects from the dangers resulting from cyberattacks, including separating or shielding civilian cyber systems from military objectives.

The attribution of cyber operations to states remains a persistent challenge. Research on "patriotic hackers" non-state actors who align with state interests while maintaining operational independence demonstrates the inadequacy of the ICJ's "effective control" standard for cyberspace. Alternative standards such as "overall control," "flexible control," and "virtual control" have proposed, but none has achieved consensus. As the ICJ has yet to adjudicate any case directly concerning cyber operations, the law of state responsibility for cyber activities remains underdeveloped.

The literature thus reveals a complex legal landscape. While the prohibition on attacks on critical infrastructure well established in principle, its application to dual-use objects, cyber operations, and scenarios involving difficult attribution creates substantial legal uncertainty. Moreover, the gap between legal prohibition and effective enforcement remains wide, highlighting the need for both strengthened legal frameworks and more robust accountability mechanisms.

Methodology

This research employs a descriptive-analytical methodology to examine the legal dimensions of the prohibition of attacks on critical infrastructure under international law, with a specific focus on the 2026 US-Israel strikes against Iranian infrastructure. The research design incorporates doctrinal legal analysis, case study analysis, and comparative institutional assessment. The doctrinal component involves systematic interpretation of primary legal sources, including the Geneva Conventions and their Additional Protocols, the UN Charter, the Rome Statute of the ICC, and the 1955 Treaty of Amity between Iran and the United States. Treaty interpretation follows the Vienna Convention on the Law of Treaties (1969), emphasizing textual, contextual, and purposive analysis.

Customary international law identified through assessment of state practice and opinion juris,

drawing upon the ICRC's Customary IHL Study and official state positions articulated in international forums. The legal analysis grounded in the principle that "civilian objects are defined in the negative, as all objects which are not military objectives," and that consequently "there is no intermediate legal category of 'dual-use' object". This interpretive approach, while acknowledging the practical challenges of dual-use objects, maintains analytical clarity by treating each object as either a military objective or a civilian object based on the circumstances at the time of attack.

The case study component examines the 2026 US-Israel strikes through the lens of IHL principles, analyzing specific targets including nuclear facilities, energy infrastructure, transportation networks, and cyber systems. For each category, the analysis assesses whether the target qualified as a military objective, whether the proportionality principle was satisfied, and whether precautionary measures adequately implemented. This assessment draws upon public statements by state officials, reports from international organizations, and independent legal analysis.

The comparative institutional assessment identifies available legal venues for seeking redress, including the ICJ, the ICC, arbitration tribunals, and domestic courts. The feasibility of each avenue evaluated based on jurisdiction requirements, procedural rules, evidentiary standards, and practical obstacles such as state immunity and non-cooperation. The ICJ's Oil Platforms case (2003) provides a critical precedent for evaluating the viability of Treaty of Amity-based claims, while the ICC's arrest warrants for Russian officials offer guidance on the prospects for prosecuting attacks on critical infrastructure as war crimes and crimes against humanity.

Data collection relies on publicly available primary and secondary sources, including official government statements, UN documents, ICJ judgments, ICC decisions, scholarly articles, and reports from international organizations. Sources assessed for authority, reliability, and relevance. The analysis incorporates the evidentiary principles articulated by the ICJ, particularly regarding circumstantial evidence and inferences where direct evidence is inaccessible due to exclusive territorial control. Limitations of this study include the ongoing nature of the conflict, incomplete public information about operational details, and the absence of definitive judicial pronouncements on the specific strikes analyzed.

Results

Legal Dimensions of the Prohibition on Attacking Infrastructure in International Law: An Analysis of US and Israeli Attacks on Iran's Critical Infrastructure in the 2025/2026 Wars and Legal Strategies for International Adjudication

The prohibition on attacking critical infrastructure represents a fundamental tenet of international humanitarian law, yet its enforcement remains fraught with challenges, particularly when powerful states are implicated. The wars of 2025 and 2026 between Iran and the US-Israel alliance witnessed unprecedented attacks on Iran's nuclear facilities, hospitals, schools, bridges, water desalination plants, and energy infrastructure. This paper examines the legal dimensions of these attacks under international law, analyzing them through the lenses of the prohibition on the use of force (jus ad bellum), the principle of distinction, proportionality, and the protection of objects indispensable to civilian survival (jus in bello). It further explores legal strategies available to Iran, including accepting the International Criminal Court's ad hoc jurisdiction under Article 12(3) of the Rome Statute, initiating proceedings at the International Court of Justice, and utilizing universal jurisdiction mechanisms. Drawing on recent jurisprudence, including ICC arrest warrants issued for attacks on Ukraine's infrastructure, and doctrinal analysis, this paper argues that the attacks constitute war crimes and grave breaches of the Geneva Conventions, while acknowledging the significant political and legal obstacles to accountability.

Critical infrastructure encompassing energy facilities, transportation networks, hospitals, schools, nuclear power plants, water and sewage systems, and communication networks constitutes the lifeline of any society. Attacks on such infrastructure, whether deliberate military strikes or intentional disruption, produce catastrophic consequences for civilians and may amount to international crimes, including forced displacement and deprivation of life (Beigzadeh,2025). International law addresses the protection of critical infrastructure in two distinct contexts: during armed conflict and in peacetime (Beigzadeh,2025).

The wars of 2025 and 2026 between Iran and the US-Israel alliance have generated unprecedented legal challenges concerning attacks on critical infrastructure. Extensive strikes targeted IAEA-supervised nuclear facilities at Fordow, Natanz, and Isfahan (Sadeghi,2026); hospitals, schools, and bridges (Al Jazeera,2026); water desalination plants (New York Times,2026); and energy infrastructure including the South Pars gas field and Lavan oil refinery (SHANA,2026). US President Trump explicitly threatened to "obliterate" Iranian power plants and bridges (Politico,2026), while Israeli forces launched systematic strikes against Iranian energy infrastructure (IPIS,2026).

This paper examines whether the US and Israeli attacks on Iran's critical infrastructure constitute violations of international law and what legal strategies are available for pursuing accountability in international courts.

The Principle of Distinction

The principle of distinction, enshrined in Article 48 of Additional Protocol I to the Geneva Conventions, obliges parties to armed conflict to distinguish at all times between civilian objects and military objectives (ICRC,1987). Article 52 defines civilian objects negatively as "all objects which are not military objectives" and prohibits attacks directed against them. 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" (ICRC,1987).

Critical infrastructure qualifies as civilian objects unless they meet the Article 52(2) criteria. However, the mere "possible future use" of an object does not transform it into a military objective (Lattimer, 2026). The US Department of Defense Law of War Manual recognizes that "objects that contain military objectives are military objectives," but this does not render entire categories of infrastructure liable to attack (Lattimer,2026).

Proportionality and Indiscriminate Attacks: Article 51(5)(b) of Additional Protocol I prohibits attacks where "incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, would be excessive in relation to the concrete and direct military advantage anticipated" (ICRC,1987). The principle of proportionality demands that even if infrastructure qualifies as a military objective, the expected collateral damage must not outweigh the anticipated military advantage (IPIS,2026).

Indiscriminate attacks those not directed at a specific military objective or employing means that cannot be directed at a specific military objective are equally prohibited (ICRC,1987). Article 54 additionally prohibits attacks on "objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas, crops, livestock, drinking water installations and supplies, and irrigation works" (ICRC,1987).

Protection of Dangerous Installations: Article 56 of Additional Protocol I provides special protection for "works and installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations," prohibiting attacks even if they constitute military objectives when such attacks may cause the release of dangerous forces and severe civilian losses (ICRC,1987). This provision, combined with Security Council Resolution 487 (1981) declaring peaceful nuclear facilities immune from attack, creates heightened protection for nuclear installations (Sadeghi,2026).

Analysis of US and Israeli Attacks on Iran's Infrastructure: Israeli forces launched a military offensive against Iran on June 13, 2025, targeting nuclear facilities, IRGC units, and military installations (Sadeghi,2026). The US joined the operation on June 22, 2025, attacking three nuclear facilities: Fordow, Natanz, and Isfahan (Sadeghi,2026). The offensive involved strikes on South Pars gas refineries (SHANA,2026), Lavan oil refinery (SHANA,2026), the B1 bridge at Karaj (Global Security,2026), desalination plants (New York Times,2026), and other critical infrastructure (IPIS,2026).

The extent of damage was significant. At Fordow, US bunker-buster bombs "likely continued through the rock into the centrifuge halls and other sensitive areas" (Carnegie Endowment,2026). At Natanz, "major substations, emergency generators, and power feeds were destroyed, rendering the remaining centrifuge cascades inoperable" (Carnegie Endowment,2026). The Iranian Oil Ministry reported that enemy attacks on auxiliary petrochemical facilities were intended to "increase pressure on the public and disrupt the supply of essential needs" (SHANA,2026).

Violations of Jus ad Bellum: Article 2(4) of the UN Charter prohibits the threat or use of force against the territorial integrity or political independence of any state (Dehshiri & Ahmadi,2026). The ICJ, in the Nicaragua case (1986), held that "the use of force against the territorial integrity of another State and military actions that intrude into the territory of another State constitute violations of customary and treaty international law" (Islamic Republic of Iran,2026). The US-Israeli attacks, purportedly justified as preemptive self-defense, cannot satisfy the "imminent threat" standard established in the Caroline doctrine (Dehshiri & Ahmadi,2026). No armed attack by Iran against these states had occurred, and IAEA inspectors had verified Iran's nuclear material inventories just days before the strikes (Islamic Republic of Iran,2026).

Violations of Jus in Bello: The attacks on nuclear facilities violate Article 56 of Additional Protocol I and Security Council Resolution 487 (Sadeghi,2026). Carnegie's assessment confirms, "US strikes penetrated directly into remaining centrifuge cascades and critical infrastructure areas" (Carnegie Endowment,2026). Even assuming these facilities constituted military objectives, the potential release of radioactive materials and catastrophic humanitarian consequences renders such attacks disproportionate (IPIS,2026). The

pattern of attacks on civilian objects hospitals, schools (including a strike on a school in Minab killing 168-180 girls aged 7-12) (WIRED,2026), water desalination plants (New York Times,2026), bridges (Al Jazeera,2026), and media infrastructure (IPIS,2026) constitutes a clear violation of the principle of distinction (ICRC,1987). The International Criminal Tribunal for the former Yugoslavia held, in the Galić case, that "certain apparently disproportionate attacks may give rise to the inference that civilians were actually the object of attack" (IPIS,2026). Given the systematic nature of these strikes, the inference of unlawful targeting is compelling (IPIS,2026).

Characterization as War Crimes: Intentional attacks on civilian objects constitute war crimes under Article 8 of the Rome Statute (Beigzadeh,2025). The ICC has issued arrest warrants against Russian military officials for attacks on Ukraine's energy infrastructure, recognizing such attacks as war crimes (Beigzadeh,2025). The destruction of water infrastructure constituting objects indispensable to civilian survival also violates Article 54 of Additional Protocol I and may constitute the war crime of "intentionally using starvation of civilians as a method of warfare" (IPIS,2026).

Legal Strategies for International Adjudication

Acceptance of ICC Ad Hoc Jurisdiction: Despite not being a State Party to the Rome Statute, Iran possesses the legal capacity to invoke the ICC's ad hoc jurisdiction pursuant to Article 12(3) by submitting a declaration accepting the Court's jurisdiction over crimes committed on its territory (University of Tehran,2026). This mechanism, utilized by Ukraine in 2014, allows non-State Parties to grant the ICC jurisdiction over specific situations (Beigzadeh,2025). The declaration can be temporally and territorially circumscribed to the 2025/2026 conflicts, enabling Iran to pursue accountability while safeguarding broader national security interests (University of Tehran,2026). The ICC's recent warrants against Russian officials demonstrate the viability of this approach, albeit with practical enforcement challenges (Beigzadeh,2025).

Proceedings at the International Court of Justice: Iran can initiate proceedings at the ICJ under the 1955 Treaty of Amity, Economic Relations, and Consular Rights between Iran and the US which remains in force despite US arguments to the contrary (Islamic Republic of Iran,2026). The compromiser clause in Article XXI (2) provides for ICJ jurisdiction over disputes concerning the Treaty's interpretation or application (Dehshiri & Ahmadi,2026). Past ICJ jurisprudence, including the 1980 US Diplomatic and Consular Staff case, confirms the Treaty's continued validity (Islamic Republic of Iran,2026). Iran could also rely on the Geneva Conventions and Additional Protocol I, to which both Iran and the US are parties (Dehshiri & Ahmadi,2026).

Universal Jurisdiction: Courts in states with universal jurisdiction legislation including Belgium, Spain, and Germany can prosecute war crimes regardless of the place of commission or nationality of victims or perpetrators (Beigzadeh,2025). Iran could submit evidentiary materials to these jurisdictions, potentially leading to criminal proceedings against military and political officials (Consortium News,2026). The Nuremberg and International Criminal Tribunal for the former Yugoslavia precedents establish individual criminal responsibility for violations of the laws of war (Beigzadeh,2025). Iran can also utilize:

- ✓ The UN Human Rights Council through requests for Fact-Finding Missions (Dehshiri & Ahmadi,2026)
- ✓ The IAEA Board of Governors concerning attacks on nuclear facilities (Sadeghi,2026)
- ✓ Regional organizations including the Organization of Islamic Cooperation (IPIS,2026)
- ✓ The UN General Assembly to secure condemnation resolutions (Islamic Republic of Iran,2026)

The US and Israeli attacks on Iran's critical infrastructure in the 2025/2026 wars constitute flagrant violations of international law, including the prohibition on the use of force, the principle of distinction, proportionality, and the special protection of dangerous installations (Dehshiri & Ahmadi,2026; IPIS,2026; Sadeghi,2026). These attacks, targeting nuclear facilities, hospitals, schools, water infrastructure, and energy facilities, represent war crimes and grave breaches of the Geneva Conventions (Beigzadeh,2025; ICRC,1987).

While the legal framework prohibiting attacks on critical infrastructure is reasonably clear (Beigzadeh,2025), enforcement remains the central challenge. The international community's response to Russia's infrastructure attacks in Ukraine including ICC arrest warrants provides a template for pursuing accountability (Beigzadeh,2025). Iran can accept the ICC's ad hoc jurisdiction under Article 12(3) of the Rome Statute (University of Tehran, 2026), initiate proceedings at the ICJ utilizing the 1955 Treaty of Amity (Islamic Republic of Iran,2026), and pursue universal jurisdiction prosecutions in national courts (Consortium News,2026).

However, significant obstacles remain, including US and Israeli non-membership in the ICC, the veto power of permanent Security Council members, and the doctrine of state immunity (Dehshiri &

Ahmadi,2026). Despite these challenges, pursuing legal avenues serves both justice and the broader objective of strengthening the international legal order (Beigzadeh,2025). As the academic literature emphasizes, a commitment to "taking international criminal law seriously" requires persistent engagement with these mechanisms, even when immediate outcomes are uncertain (Beigzadeh,2025). The path to accountability lies in strategic litigation, diplomatic pressure, and continued advocacy for the robust enforcement of international humanitarian law's core protections for civilian infrastructure (Table 1).

Table 1. International Legal Framework Governing Attacks on Infrastructure

Legal Principle	Source	Key Provisions	Application to Infrastructure Attacks
Principle of Distinction	AP I, Art. 48, 52; Customary IHL	Parties must distinguish between civilian objects and military objectives; attacks limited to military objectives	Critical infrastructure is presumed civilian unless it makes an effective contribution to military action
Prohibition of Indiscriminate Attacks	AP I, Art. 51(4)-(5); Customary IHL	Attacks not directed at specific military objectives or employing methods that cannot be so directed are prohibited	Attacks affecting entire infrastructure systems may be indiscriminate if not specifically directed
Proportionality	AP I, Art. 51(5)(b); Customary IHL	Incidental civilian harm must not be excessive relative to anticipated military advantage	Assessment must consider cascading effects on civilian population
Precaution in Attack	AP I, Art. 57; Customary IHL	All feasible precautions must be taken to avoid and minimize incidental harm	Attack planners must verify target nature and choose least harmful means
Protection of Dangerous Installations	AP I, Art. 56	Dams, dykes, nuclear power plants protected even if military objectives, if attack may cause dangerous force release	Nuclear facilities enjoy special protection; attacks likely unlawful if civilian harm risked
Protection of Objects Indispensable to Survival	AP I, Art. 54; Customary IHL	Attacks against objects indispensable to civilian survival (water, food, crops) prohibited	Water infrastructure and agricultural systems enjoy robust protection
Right to Life	ICCPR, Art. 6; Customary IHL	No arbitrary deprivation of life	Infrastructure attacks causing civilian deaths may violate right to life
Sovereignty (Cyber Operations)	Customary IHL; Tallinn Manual 2.0	States must respect territorial sovereignty in cyber domain	Unauthorized intrusion into cyber infrastructure may violate sovereignty if causing damage or loss of functionality

The international legal framework governing attacks on infrastructure are comprehensive yet operationally complex. The principle of distinction, codified in Articles 48 and 52 of Additional Protocol I, establishes the fundamental dichotomy between civilian objects and military objectives. As Lattimer (2026) emphasizes, "there is no intermediate legal category of 'dual-use' object". The interpretive clarity an object is either a military objective or a civilian object is crucial for maintaining the protective purpose of IHL. However, the practical application of this dichotomy to complex infrastructure presents challenges. A nuclear power plant may simultaneously generate electricity for civilians (civilian function) and provide power to a military command center (military contribution). The DoD Law of War Manual states "objects that contain military objectives are military objectives" (§ 5.6.4.2), potentially rendering entire facilities targetable based on a single military component.

The prohibition of indiscriminate attacks, articulated in Article 51(4)-(5), complements the principle of distinction by prohibiting attacks that do not target specific military objectives or that employ methods incapable of such targeting. For infrastructure attacks, this is particularly significant when entire systems such as the national power grid targeted without discriminating between military and civilian nodes. The ICC's Prosecution has characterized systematic attacks on Ukraine's electric power plants and substations as a course of conduct potentially constituting a crime against humanity. This suggests that the scale and pattern of attacks may be relevant to determining whether indiscriminate attacks have occurred.

The proportionality principle prohibits attacks where incidental civilian harm is excessive relative to the anticipated military advantage. For infrastructure attacks, the assessment of incidental harm must extend beyond immediate physical damage to include cascading effects on the civilian population, including loss of water, power, healthcare, and communication. Israel's approach treating the use of part of a structure by a military actor as rendering the whole structure a military objective and thereby excluding those civilian components from the proportionality analysis has been criticized by the ICRC. This approach has significant implications for infrastructure attacks, potentially allowing belligerents to avoid proportionality assessments for extensive collateral damage.

The precaution in attack principle under Article 57 imposes positive obligations on attacking forces, including verifying target nature, choosing means and methods that minimize civilian harm, and canceling attacks where proportionality is not satisfied. In the context of infrastructure attacks, this requires gathering intelligence about both the civilian and military uses of the target and considering alternatives that might achieve similar military advantage with less civilian impact. The principle that "when there is a choice between several different military objectives that would achieve the same or a similar military advantage, a party should select the military objective where the attack is expected 'to cause the least danger to civilian lives and to civilian objects'" (AP I, Art. 57(3)) is particularly relevant. However, in practice, such choices may be constrained by operational considerations.

Article 56 provides enhanced protection for installations containing dangerous forces, including nuclear power plants, protecting them even if they make an effective contribution to military action, provided attack may cause the release of dangerous forces and consequent severe losses among the civilian population. This protection extends to military objectives located near such installations. The article also obligates states to avoid locating military objectives near dangerous installations, potentially requiring Iran to ensure that its nuclear facilities are not proximate to military targets. The Bushehr, Natanz, and Isfahan facilities targeted in the 2026 strikes appear to fall within the scope of Article 56, suggesting that these attacks if they risked dangerous force release would be unlawful even assuming the facilities were military objectives.

Table 2. Analysis of 2026 US-Israel Strikes on Iranian Infrastructure

Target Category	Specific Targets (Based on Reports)	Legal Status Assessment	IHL Principle	Likely Legal Violation
Nuclear Facilities	Bushehr Nuclear Power Plant, Natanz, Isfahan facilities, Khondab heavy water complex, Ardakan yellowcake production	Protected under AP I, Art. 56 as installations containing dangerous forces	Article 56; Principle of Distinction	Likely violation unless no risk of dangerous force release; attack may constitute war crime
Energy Infrastructure	South Pars gas field, power plants	Dual-use: civilian energy generation potentially serving military purposes	Proportionality; Precaution	Legality depends on whether military advantage justifies extensive civilian harm
Transportation Infrastructure	Bridges (including B1 bridge at Karaj), railways, airports	Presumptively civilian unless making effective military contribution	Principle of Distinction; Precaution	Likely violation if civilian use predominant
Communication/Cyber Infrastructure	News websites, communication systems	Civilian cyber infrastructure	Sovereignty; non-intervention	Likely violation if unauthorized intrusion causes damage or loss of functionality

The 2026 US-Israel strikes targeted a broad range of Iranian infrastructure, raising distinct legal questions for each category. The nuclear facilities strike present the clearest legal concerns under Article 56 of Additional Protocol I. The Bushehr Nuclear Power Plant, the Khondab heavy water complex, and the Ardakan yellowcake production facility all fall within the category of installations containing dangerous forces. The AEOI confirmed that the Bushehr plant struck by a projectile for the third time. Under Article 56, such facilities are protected from attack even if they are being used for military purposes, provided that an attack "may cause the release of dangerous forces and consequent severe

losses among the civilian population". Iran maintains that its nuclear program is peaceful, and the IAEA had not identified any weaponization activities at these facilities prior to the strikes. If the strikes risked radioactive release, they would violate Article 56 regardless of any claimed military advantage. The fact that Iran is reportedly considering withdrawal from the NPT suggests that the strikes have fundamentally undermined the non-proliferation regime.

The strikes on energy infrastructure, particularly the South Pars gas field and power plants, raise complex questions regarding dual-use objects. Energy infrastructure is typically civilian in nature, serving the needs of the civilian population. However, energy also supports military operations, and specific components used for military purposes. The DoD Law of War Manual states that "objects that contain military objectives are military objectives" (§ 5.6.4.2), potentially rendering the entire facility targetable. However, this approach has criticized for effectively eliminating proportionality analysis for civilian components integrated with military objectives. Israel's position use of part of a building by a military actor renders the whole structure a military objective rejected by the ICRC in the context of the Jalaa media building strike in Gaza. The key question for the energy infrastructure strikes is whether the anticipated military advantage justified the extensive incidental harm to civilians dependent on energy services, particularly given Russia's similar attacks on Ukraine's energy infrastructure, which formed the basis for ICC arrest warrants.

The transportation infrastructure strikes including bridges, railways, and airports present similarly complex questions. The B1 Bridge at Karaj destroyed on April 2, 2026. Transportation infrastructure serves both civilian and military logistical functions. The critical legal question is whether these objects were making an "effective contribution to military action" at the time of attack and whether their destruction offered a "definite military advantage" (AP I, Art. 52). The United States claimed that attacks were "exclusively against military targets, including military logistical infrastructure". However, the broad scope of the strikes encompassing multiple transportation nodes raises questions about whether the attacking forces adequately verified target nature and whether the attacks could have been conducted with less impact on civilian transportation.

The cyber operations targeting Iranian communication systems and news websites raise distinct questions under the sovereignty principle and the prohibition of intervention. The Tallinn Manual 2.0's experts identified several modalities for determining sovereignty violations, including causation of physical damage, loss of functionality of cyber infrastructure, interference with inherently governmental functions, and usurpation of such functions. The cyber operations in question appear to have caused disruption to news websites and communication systems. If these operations resulted in a "loss of functionality" requiring reinstallation of systems, they could constitute a sovereignty violation, although consensus on the precise threshold for loss of functionality remains elusive. The attribution challenge is substantial, as cyber operations conducted through proxies or from third-state infrastructure, complicating efforts to assign state responsibility.

Table 3. Legal Avenues for Iran to Seek Redress

Legal Avenue	Jurisdictional Basis	Precedent	Key Requirements	Principal Obstacles	Likelihood of Success
International Court of Justice (ICJ)	1955 Treaty of Amity, Art. XXI (2)	Oil Platforms (Iran v. US, 2003)	Treaty in force; dispute concerning treaty application	US withdrew from Treaty in 2018; jurisdiction limited to Treaty matters	Low
International Criminal Court (ICC)	Rome Statute, Art. 12(2)(a) (territorial jurisdiction if conduct in state party)	Ukraine arrest warrants (2024)	Iran's membership or Security Council referral; crime within jurisdiction	Iran not party; US not party; Security Council likely blocked by US veto	Very Low
Arbitration	Treaty of Amity, other bilateral agreements	Iran-US Claims Tribunal	Agreement of parties; arbitral tribunal establishment	US unwilling to consent; limited to specified subject matters	Low
Domestic Courts	Universal jurisdiction; Alien Tort Statute (US)	Various human rights cases	Jurisdiction over defendant; justiciability	State immunity; political question doctrine; enforcement challenges	Very Low

Human Rights Bodies	ICCPR, ICESCR	HRC communications	State ratification; exhaustion of domestic remedies	US not party to many treaties; limited remedies	Very Low

The ICJ route, which Iran previously used in the Oil Platforms case (Iran v. United States, 2003), faces substantial obstacles. The case was based on Article XXI (2) of the 1955 Treaty of Amity, which provides that disputes concerning the treaty's interpretation or application shall be submitted to the ICJ. In Oil Platforms, the ICJ found that it had jurisdiction to entertain Iran's claims under Article X (1) of the Treaty concerning freedom of commerce. However, the Court ultimately rejected Iran's claim because platforms under either repair (so no trade was occurring) or trade suspended due to an embargo. Crucially, the United States withdrew from the Treaty of Amity in 2018, rendering the Treaty's compromiser clause unavailable for future claims. Iran could potentially argue that the withdrawal was unlawful or that prior violations continue to be justiciable, but such arguments face significant legal hurdles. Even if jurisdiction were established, the substantive scope of the Treaty limited to commerce and navigation may not encompass attacks on nuclear facilities or cyber operations.

The ICC route presents even steeper obstacles. Under the Rome Statute's Article 12(2)(a), the ICC has jurisdiction over crimes committed on the territory of a State Party. Iran is not a party to the Rome Statute, and the United States not a party. The ICC's jurisdiction could only be triggered by a UN Security Council referral under Chapter VII, but this would face an almost certain US veto. The ICC's recent arrest warrants for Russian military officials for attacks on Ukraine's critical infrastructure demonstrate that the Court is willing to prosecute such conduct as war crimes and crimes against humanity. In those warrants, the Pre-Trial Chamber confirmed reasonable grounds to believe that the accused directed attacks against civilian objects and caused excessive incidental civilian harm, and that the alleged campaign represented "a course of conduct involving the multiple commission of acts against a civilian population, pursuant to a state policy, within the meaning of Article 7 of the Statute". However, the jurisdictional bar remains the primary obstacle for Iran, as the ICC lacks jurisdiction without Security Council referral or State Party membership.

Arbitration presents a theoretically viable but practically challenging avenue. The Iran-US Claims Tribunal, established following the 1981 Algiers Accords, has jurisdiction over certain claims between Iranian and US nationals and companies. However, its jurisdiction does not extend to inter-state claims concerning attacks on infrastructure. Other arbitration mechanisms require the agreement of both parties, which the United States appears unwilling to provide. The United States has generally resisted international adjudication of its military actions, preferring political or diplomatic resolution.

Domestic litigation, whether in US courts under the Alien Tort Statute or in other countries under universal jurisdiction, faces significant obstacles. The Alien Tort Statute (28 U.S.C. § 1350) permits federal courts to hear claims by aliens for torts "committed in violation of the law of nations." However, the Supreme Court has significantly narrowed the statute's scope in recent decades, requiring that the norm alleged to violate be "specific, universal, and obligatory." Even assuming such a norm exists, plaintiffs would face substantial barriers including state immunity, the political question doctrine, and enforcement challenges. The United States would invoke state immunity for sovereign acts, and courts would likely defer to the executive branch on national security matters.

Table 4. Obstacles to Effective Legal Redress

Obstacle Category	Specific Obstacles	Legal Basis/Precedent	Impact on Litigation	Mitigation Strategies
Jurisdictional	US withdrawal from Treaty of Amity (2018); US/Iran non-membership in Rome Statute	Vienna Convention on Law of Treaties, Art. 54; Rome Statute, Art. 12	Precludes ICJ and ICC jurisdiction	Seek Security Council resolution; pursue bilateral arbitration agreements
Evidentiary	Difficulties proving attribution for cyber operations; classified intelligence; exclusive territorial control of evidence	Corfu Channel (ICJ, 1949); Roscini (2015)	Circumstantial evidence may be necessary; negative inferences from non-disclosure limited	Gather multiple, consistent evidence sources; leverage technical attribution experts

Political	US veto power in Security Council; geopolitical alliances	UN Charter, Art. 27(3)	Security Council unable to act on violations	Seek UNGA resolutions; build multilateral coalition
Sovereign Immunity	State immunity for sovereign acts; official immunity	ICJ Jurisdictional Immunities (2012)	Bars domestic court claims against state officials	Seek immunity exceptions; pursue international tribunals
Enforcement	Difficulty enforcing judgments against US; lack of enforcement mechanisms	ICJ Statute, Art. 94(2) (Security Council enforcement)	Even successful judgments may remain unenforced	Pursue political/diplomatic remedies alongside legal

The jurisdictional obstacles present the immediate barrier to effective legal redress. The US withdrawal from the 1955 Treaty of Amity in 2018 effectively closed the ICJ Avenue that Iran had successfully pursued in the Oil Platforms case. Under the Vienna Convention on the Law of Treaties, a party may withdraw from a treaty in accordance with its terms or with the consent of all parties (Art. 54). The Treaty of Amity did not contain a withdrawal provision, but the US withdrawal based on the termination of the Treaty's operation following the 1979 hostage crisis and subsequent events. Iran's challenge to the legality of the withdrawal would face significant evidentiary and political obstacles. Even if Iran were to secure a favorable ICJ ruling on the withdrawal's illegality, the United States would likely ignore it, as states have previously done. The ICC route similarly foreclosed by non-membership. While the United States participated in the Rome Statute negotiations, it has consistently opposed the ICC's jurisdiction over its nationals. Iran's non-membership, combined with the absence of a Security Council referral, renders ICC proceedings impossible unless Iran accedes to the Rome Statute (which would create jurisdictional exposure for Iran itself) or the Security Council acts (which is politically infeasible).

Evidentiary obstacles pose substantial challenges to proving violations, particularly for cyber operations. As Roscini (2015) observes, the ICJ requires that parties alleging facts provide proof, and the burden of proof rests on the party alleging. For cyber operations, direct evidence of attribution including command-and-control logs, malware signatures, and intelligence sources may be classified or inaccessible. The ICJ has allowed inferences from circumstantial evidence where direct evidence lies within the exclusive territorial control of the other litigant, requiring that such inferences "leave no room for reasonable doubt". This standard is demanding, and the Court has "approached the drawing of inferences with great caution". Moreover, even where states possess evidence obtained through unauthorized cyber intrusions, such evidence may be admissible the ICJ did not dismiss evidence illegally obtained by the United Kingdom in the Corfu Channel case, though the purpose of collection did not exclude the illegality of the conduct. However, relying on such evidence may itself constitute a violation of international law, creating a dilemma for states seeking legal recourse. Political obstacles, particularly the US veto in the Security Council, preclude the most effective enforcement mechanism under the UN Charter. Under Article 94(2), if a party fails to perform its ICJ obligations, the other party may have recourse to the Security Council, which may make recommendations or decide upon measures to give effect to the judgment. However, the United States, as a permanent member of the Security Council, can veto any enforcement action. This political reality significantly undermines the deterrent effect of ICJ judgments. Similarly, Security Council resolutions condemning attacks on infrastructure would face a US veto, as occurred with numerous resolutions concerning the 2026 strikes. While the UN General Assembly can pass resolutions condemning violations, these are non-binding and lack enforcement mechanisms.

Sovereign immunity bars domestic court claims against the United States and its officials. Under the ICJ's Jurisdictional Immunities case (Germany v. Italy, 2012), states enjoy immunity for sovereign acts, even where those acts violate international law. The exception for crimes against humanity has not recognized in state practice, and domestic courts are generally unwilling to exercise jurisdiction over foreign states' military actions. The political question doctrine, which holds that certain issues are non-justiciable because they are committed to the political branches, provides an additional barrier in US courts. The executive branch's classification of national security matters and claims of state secrets further impedes litigation.

Discussion

The analysis reveals a fundamental tension between the clarity of international humanitarian law's protective provisions and the practical challenges of their enforcement. While the prohibition of attacks on critical infrastructure well established in treaty law and has reinforced by recent ICC jurisprudence, the 2026 US-Israel strikes demonstrate that powerful states can operate with relative impunity, exploiting

legal ambiguities and leveraging their political influence to avoid accountability. This section discusses the key findings in relation to the existing literature, identifies implications for the development of international law, and considers potential strategies for strengthening the legal protection of critical infrastructure (Figure 1).

Figure 1. Legal Dimensions of the Prohibition of Attacks on Infrastructure under International Law: The 2026 US-Israel Strikes on Iran's Critical Infrastructure and Legal Avenues for Litigation in International Courts

The Dual-Use Problem and Legal Certainty: The most significant legal challenge identified by this analysis is the interpretive ambiguity surrounding dual-use objects. Lattimer (2026) emphasizes, "dual-use is not a recognized concept in IHL". Despite this, states frequently characterize civilian infrastructure as dual-use to justify attacks, effectively treating the category as if it existed. As Capone (2025) observes, dual-use objects "have entered the IHL jargon but has not attained the status of a legal concept". This liminal status enables belligerents to manipulate the legal framework, avoiding full application of the proportionality principle by designating entire categories of objects as military objectives. The ICC's approach in the Ukraine context suggests that a pattern of extensive damage to civilian objects can support an inference that civilians were the intended object of attack, even if some military purposes served. This inferential approach provides a potential check on the abuse of the dual-use category, but it requires rigorous evidentiary support that may be difficult to obtain.

Attribution and Cyber Operations: The analysis confirms that attribution remains the central challenge for cyber operations. The sovereignty principle, as articulated in the Tallinn Manual 2.0, prohibits unauthorized intrusions into state cyber infrastructure that cause damage or loss of functionality, but the evidentiary threshold for establishing such violations remains contested. The ICJ has yet to adjudicate a cyber-operation case, leaving substantial uncertainty about how its rules on evidence and inferences would apply. The "effective control" standard for state responsibility, which requires showing that a state exercised direction and control over conduct, is particularly difficult to satisfy for cyber operations where states may employ proxies or deniable assets. Alternative standards such as "overall control" or "flexible control" have proposed but lack acceptance. The development of clearer rules on cyber attribution will be essential if international law is effectively regulating state conduct in cyberspace.

The Effectiveness of International Courts: The analysis underscores the structural limitations of international courts as mechanisms for enforcing IHL in cases involving powerful states. The ICJ's Oil Platforms judgment, while rejecting the United States' self-defense claims, ultimately held that Iran had not demonstrated a violation of the Treaty of Amity due to the absence of commerce at the time of the attacks. This outcome a legal victory for the United States despite its unjustifiable use of force exemplifies the limitations of litigating military actions through commercial treaties. Similarly, the ICC's effectiveness is constrained by its reliance on state cooperation and Security Council referrals, both of which blocked by US opposition. The Ukraine warrants, while significant, face enforcement difficulties because the accused individuals protected by Russia's non-cooperation.

The lesson is that international courts can contribute to accountability, but they cannot substitute for political will and effective enforcement mechanisms.

The Role of State Practice in Law Development: The analysis suggests that state practice is contributing to the evolution of rules on critical infrastructure protection. The ICC's Ukraine warrants represent a significant development, potentially crystallizing a customary rule that attacks on critical infrastructure constitute war crimes. However, the simultaneous US-Israel strikes undermine this development, demonstrating that state practice remains divided. The United States' historical attacks on infrastructure in Iraq, Kosovo, and elsewhere suggest that the US practice is consistent, which weighs against the formation of a customary rule contrary to its conduct. For a customary rule to emerge, state practice must be both consistent and accompanied by opinion juris a belief that the practice is legally required. The divided practice, with some states condemning attacks and others conducting them, suggests that no such rule has yet crystallized.

Implications for Iran's Legal Strategy: The analysis indicates that Iran faces substantial obstacles in securing legal redress for the attacks. The most promising avenue litigation under the Treaty of Amity is foreclosed by the US withdrawal. Iran could attempt to challenge the withdrawal as unlawful, but such a challenge would face jurisdictional and political obstacles. The ICC route similarly foreclosed by Iran's non-membership, though Iran could potentially accede to the Rome Statute, creating jurisdiction for current and future attacks. This would, expose Iran itself to potential ICC prosecution. The most likely path involves a combination of diplomatic pressure, multilateral condemnation, and potential countermeasures. Iran's reported consideration of NPT withdrawal illustrates the geopolitical risks of failing to enforce legal protections. If Iran withdraws, the international community loses access to IAEA inspections, potentially triggering a regional proliferation cascade.

The Need for a Critical Infrastructure Convention: The analysis suggests that the most effective long-term solution would be the negotiation of a dedicated convention on critical infrastructure protection, similar to the 1977 Environmental Modification Convention. Such a convention could address the ambiguities in the current legal framework by providing clear definitions of critical infrastructure, establishing per se prohibitions on attacks against certain categories, and creating enforcement mechanisms. The convention could draw upon the lessons of other specialized treaties, such as Article 56's protection for dangerous installations, and extend them to cover the full range of critical infrastructure. The convention could also address cyber operations, establishing clearer rules on attribution and state responsibility. While the negotiation of such a convention would be challenging, recent initiatives including the Global Initiative to Support International Humanitarian Law, convened in Geneva in 2026 suggest that momentum exists for strengthening the legal protection of civilian infrastructure.

Conclusion

This article has examined the legal dimensions of attacks on critical infrastructure under international law, analyzing the 2026 US-Israel strikes against Iranian infrastructure and identifying legal avenues for seeking redress. The analysis yields four principal conclusions.

First, international law provides a robust normative framework for prohibiting attacks on critical infrastructure. The principles of distinction, proportionality, and precaution, enshrined in Articles 48, 51, 52, and 57 of Additional Protocol I, establish clear obligations on belligerents to spare civilian objects, including infrastructure. Article 56 extends enhanced protection to nuclear power plants and other dangerous installations. This framework, reinforced by customary international law and recent ICC jurisprudence, articulates a comprehensive prohibition on infrastructure attacks. However, the absence of a recognized legal category for "dual-use" objects creates interpretive ambiguity that states exploit to justify attacks on civilian infrastructure. The DoD Law of War Manual's position that "objects that contain military objectives are military objectives" (§ 5.6.4.2) effectively allows belligerents to render whole facilities targetable based on a single military component, undermining the protective purpose of IHL.

Second, the 2026 US-Israel strikes raise serious legal concerns under IHL. The attacks on Iran's nuclear facilities appear to violate Article 56, which protects such installations when attack may cause dangerous force release. The energy infrastructure and transportation strikes raise complex dual-use questions, but the broad scope of the attacks and the extensive civilian harm they have caused suggests that the proportionality principle may have been violated. The cyber operations targeting communication systems appear to violate the sovereignty principle, though attribution challenges complicate legal analysis. These findings are consistent with the views expressed by UN human rights bodies and the ICRC, which have characterized such attacks as potential war crimes.

Third, the available legal avenues for Iran to seek redress face substantial obstacles. The ICJ route, previously used in the Oil Platforms case, is

foreclosed by the US withdrawal from the Treaty of Amity in 2018. The ICC route blocked by Iran's and the US's non-membership in the Rome Statute and the likely US veto of any Security Council referral. Arbitration and domestic litigation face obstacles including state immunity, the political question doctrine, and enforcement challenges. Evidentiary difficulties, particularly for cyber operations, further complicate legal proceedings. These obstacles suggest that, in the short term, legal redress is unlikely to provide meaningful relief for Iran.

Fourth, the most effective long-term strategy for strengthening the legal protection of critical infrastructure involves multilateral cooperation and treaty development. The negotiation of a dedicated convention on critical infrastructure protection could resolve the ambiguities in the current framework by providing clear definitions, establishing per se prohibitions on attacks against certain categories, and creating effective enforcement mechanisms. Recent initiatives including the Global Initiative to Support International Humanitarian Law and proposals for a "critical infrastructure convention" indicate growing momentum for such an approach. The international community's experience with Article 56's protection for dangerous installations provides a model that extended to cover the full range of critical infrastructure, including cyber systems. Such a convention would not resolve all challenges, but it would provide a clear normative framework that could support future accountability efforts.

Recommendations: Based on this analysis, the following recommendations proposed:

- ✓ States should refrain from attacking critical infrastructure and strictly adhere to the principles of distinction, proportionality, and precaution, even when objects have dual uses.
- ✓ The international community should pursue the negotiation of a dedicated convention on critical infrastructure protection; building upon existing frameworks and incorporating clear rules on cyber operations.
- ✓ States should strengthen cooperation with the ICC and support efforts to prosecute attacks on critical infrastructure as war crimes and crimes against humanity.
- ✓ Iran should consider acceding to the Rome Statute to enable ICC jurisdiction, while recognizing the reciprocal exposure this creates; and (5) States should invest in technical capabilities for cyber attribution and cooperate on developing shared evidentiary standards for cyber operations.

In conclusion, the 2026 US-Israel strikes on Iranian infrastructure demonstrate the persistent gap between the normative prohibition on infrastructure attacks and the practical enforcement of that prohibition. While international law provides a clear framework for protecting critical infrastructure, political and legal obstacles substantially limit the effectiveness of existing accountability mechanisms. Addressing this gap will require both strengthened legal frameworks and sustained political commitment to accountability and the protection of civilian infrastructure in armed conflict.

Disclosure Statement

No potential conflict of interest reported by the authors.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Authors' Contributions

All authors contributed to data analysis, drafting, and revising of the paper and agreed to be responsible for all the aspects of this work.

References

[1] Beigzadeh, E. (**2025**). Assaults on critical infrastructure and international law. *Journal of Legal Research.*

[2] Capone, F. (**2025**). Dual-use objects under international humanitarian law: Towards a paradigm shift. *T.M.C. Asser Press.*

[3] Hollis, D. B., & Sukumar, A. (**2026**). PIL Discussion Group: New challenges and new concepts? Prepositioning and civilian critical infrastructure in international law. *University of Oxford.*

[4] International Court of Justice. (**2003**). Oil Platforms (Islamic Republic of Iran v. United States of America), *Judgment.*

[5] Mazaraki, N., & Honcharova, Y. (**2022**). Cyber dimension of hybrid wars: Escaping a 'grey zone' of international law to address economic damages. *Baltic Journal of Economic Studies*, 8(2), 115-120.

[6] Kachuriner, V. L. (**2025**). International legal standards for protecting critical energy infrastructure during armed conflict. Uzhhorod National University Herald. *Series Law*, *90*(5), 119-125.

[7] Lattimer, M. (**2026**). Dual-use objects and dual-purpose attacks. *Lieber Institute West Point, Articles of War.*

[8] Poposka, V. (**2025**). Applicable legal regime for protection of critical infrastructure and critical entities in conflict zones. *Proceedings of the UKLO Annual International Scientific Conference* 2024.

[9] Renault, C.-E. (**2026**). Strategy of darkness: A weapon of war. *International Bar Association.*
[10] Abbasi, A. Y. (**2026**). Oil infrastructure as military objectives: Environmental harm and reverberating effects in the proportionality assessment. *Völkerrechtsblog*.
[11] Thilakarathna, A. (**2026**). Energy law, security, and strategic adaptation: Lessons from the Iran conflict. *The Morning*.
[12] Anderson, S. R. (**2026**). Using military force in Iran: Domestic and international law questions. *Brookings Institution.*
[13] BBC News. (**2026**). US denies Iranian claims it hit civilian infrastructure in latest strikes.
[14] The Sunday Times. (**2026**). When do attacks on civilian installations amount to war crimes?
[15] Parsons Today. (**2026**). Iravani: U.S. aggression against Iran a clear violation *of Article 2(4) of U.N. Charter.*
[16] International Court of Justice. (**2003**). Oil Platforms (Islamic Republic of Iran v. United States of America), *Judgment*.