Critical Infrastructure as a Strategic Target in Future Wars

Ahmed Elhamza
University of Tebessa, ahmed.elhamza@univ-tebessa.dz
Amine Elbar
University of Tebessa, amine.elbar@univ-tebessa.dz

Received date: 08/04/2026 Accepted date: 30/04/2026 Publication date: 01/07/2026

Abstract:

*This article examines the transformation of **critical infrastructure** (energy, water, communications, transport) from civilian assets into primary strategic targets in **future wars**. It analyzes the strategic dimensions of targeting infrastructure in **hybrid warfare**, reviews international legal frameworks under **international humanitarian law**, and explores trends including cyberattacks, weaponization of infrastructure, and **"deterrence by resilience."** Using case studies from Ukraine (1,225 attacks on energy infrastructure in 2025) and Gaza (systematic destruction of water, electricity, and healthcare networks), the article concludes that infrastructure has become a primary conflict arena, demanding a redefinition of national security, defense, and deterrence. Recommendations include decentralizing infrastructure design, activating binding public-private partnerships, establishing a permanent mechanism to protect submarine cables, and criminalizing attacks on infrastructure in national legislation.*

Keywords: *Critical infrastructure, future wars, hybrid warfare, deterrence by resilience, international humanitarian law.*

* Corresponding author: Ahmed Elhamza , ahmed.elhamza@univ-tebessa.dz

Introduction

Recent decades have witnessed a radical transformation in the nature of armed conflicts, as battlefields have transcended traditional boundaries between armies into new spaces, most notably the critical infrastructure of states. Energy, water, communications, and transport networks are no longer merely civilian assets providing essential services to societies; they have become primary strategic targets and instruments of geopolitical pressure in hybrid warfare. This transformation was not accidental but rather the cumulative result of the evolution of military technology, increased societal dependence on digital systems, and the emergence of concepts of cyber warfare and asymmetric warfare aimed at paralyzing the state from within without the need for direct military occupation.

The importance of studying this topic lies in its redefinition of concepts of national security, defense, and deterrence in the twenty-first century. In conventional wars, deterrence relied on the threat of military punishment. Today, targeting infrastructure occurs through hybrid operations combining physical sabotage (such as cutting submarine cables and blowing up pipelines), cyberattacks (such as hacking and remotely controlling energy networks), and disinformation campaigns, making it difficult for the targeted state to identify the source of the attack or respond proportionately. This is what has made infrastructure "the optimal target" for adversaries seeking strategic gains without entering into a full-scale military confrontation.

This study presents an in-depth analysis of the transformation of infrastructure into strategic targets in future wars through three main axes: first, analyzing the strategic dimensions of targeting infrastructure in hybrid warfare, focusing on the experiences of Ukraine and Gaza as contemporary models. Second, examining the international legal framework governing such targeting, discussing the issue of dual-use objects. Third, exploring future trends, including cyberattacks, the weaponization of infrastructure, and the concept of "deterrence by resilience." The study adopts a case study methodology, relying on UN reports, security data, and peer-reviewed academic studies, aiming to provide an integrated vision that helps decision-makers and researchers understand this serious strategic challenge and propose effective mechanisms to confront it.

1. The Transformation of Infrastructure into Strategic Targets

The concept of critical infrastructure has undergone a radical transformation in recent decades, moving from being merely service assets supporting the daily life of societies to becoming primary strategic targets in modern and future armed conflicts. This transformation did not occur in a vacuum; it is a natural outcome of the evolution of the nature of warfare itself, as adversaries have come to realize that destroying or disrupting energy, water, communications, and transport networks can achieve military and political gains equal to, or even exceeding, those achieved through conventional clashes on contact lines. War today is no longer limited to direct confrontations between

armies; it has extended to include unconventional arenas where infrastructure has become "the optimal target" that achieves functional paralysis of the targeted state, economic collapse, and psychological warfare against civilians, without the need to occupy land or win a field battle. (Witold & Karolina , 2025, p 13-43)

a. From Service Assets to Battlefields

The past two decades have witnessed a radical shift in how states and non-state actors view critical infrastructure. Energy, water, communications, and transport networks are no longer merely civilian assets providing essential services to societies; they have become primary strategic targets in modern armed conflicts. This transformation was not accidental but rather the cumulative result of the evolution of military technology, increased societal dependence on digital systems, and the emergence of concepts of hybrid warfare that blur the boundaries between the military and civilian spheres. It can be said that critical infrastructure has today become "the optimal target" for combatants for several reasons: first, because it represents fundamental vulnerabilities in any modern state, as its disruption paralyzes the vital functions of the entire society. Second, targeting it often achieves strategic gains without the need for costly conventional military clashes. Third, these structures have become more vulnerable to penetration due to accelerated digital transformation. In this context, the European Union Institute for Security Studies (EUISS) noted that "European energy infrastructure is under hybrid attack from Russia, targeting electricity cables and gas pipelines in the Baltic Sea, revealing deep vulnerabilities at the heart of the European energy system." The NATO Deputy Secretary-General also affirmed that "Russia's invasion of Ukraine clearly shows that European energy infrastructure is a priority target for Russia." .(European Union Institute for Security Studies, 2025, p 03-05)

b. Dimensions of Targeting Infrastructure: From Functional Paralysis to Psychological Warfare

The goal of targeting infrastructure is not limited to the direct military aspect but extends to multiple dimensions: first, functional paralysis by disrupting electricity, water, and communications networks, forcing populations to flee or surrender. In Ukraine, Russian attacks on energy infrastructure resulted in severe disruptions to electricity, water, and heating supplies in major cities. Second, economic exhaustion through targeting industrial, oil, and port facilities. By June 2025, the Russian "shadow fleet" armed to target critical infrastructure included more than 1,000 vessels. Third, psychological warfare: the interruption of basic services weakens the morale of the population, creating a sense of helplessness and despair. Experts have noted that targeting infrastructure before the onset of winter represents a deliberate strategy to exploit harsh climatic conditions. Fourth, redefining the nature of war itself, as "Cyber Week 2025" revealed that future wars will be fought within networks, infrastructure, and data, not on traditional contact lines, and that paralyzing states from within can be achieved without firing a single bullet. (Witold & Karolina , 2025, p 13-34)

2. Critical Infrastructure in Hybrid Warfare

Hybrid warfare is characterized by the erasure of traditional boundaries between war and peace, between military and civilian targets, and between military and non-military instruments. At the heart of this warfare lies critical infrastructure, which has become a primary and preferred target for adversaries seeking strategic gains without the need to ignite a costly conventional military confrontation. By combining physical sabotage (such as cutting submarine cables and blowing up pipelines), cyberattacks (such as hacking energy and water networks), disinformation campaigns, and economic pressure, it is possible to disrupt vital state functions, weaken the morale of the population, and erode trust in the government's ability to protect, all while the adversary remains in a grey zone that does not reach the level of a declaration of war. (Witold & Karolina , 2025 , p22-23)

a. Hybrid Warfare: When Tools Intertwine

Hybrid warfare is characterized by blurring the boundaries between war and peace, between military and civilian targets, and between conventional and unconventional tools. At the heart of this warfare lies critical infrastructure as a primary and preferred target. Hybrid operations combine physical sabotage (cutting submarine cables, blowing up pipelines), cyberattacks (hacking energy and water networks), disinformation campaigns, economic pressure, and the use of local proxies. Recent studies have shown that infrastructure has become "a primary target for hybrid operations." Analyses indicate that adversaries have come to realize that disrupting services can achieve strategic gains without the need to ignite a conventional war. The goal is not necessarily physical destruction, but rather eroding trust in the government's ability to protect its citizens and pressuring targeted governments without provoking a military response. .(Irregular Warfare Center, 2025)

b. Submarine Cables: The Nerves of the World Under Water

Submarine cables represent a striking example of the transformation of infrastructure into targets in hybrid warfare. These cables carry 99% of intercontinental internet traffic, transfer trillions of dollars in financial data daily, and support the critical infrastructure of states. The European Commission warned in its action plan on cable security (February 2025) that "submarine cables may be damaged unintentionally, but the pattern observed in recent months, particularly in the Baltic Sea, indicates that this critical infrastructure has increasingly become a target for deliberate hostile acts." In December 2024, the vessel "Eagle S," belonging to the Russian "shadow fleet," was apprehended by Finnish authorities after it cut the EstLink 2 electricity cable linking Finland and Estonia. The vessel carried military detection devices in its hull, indicating a direct, deliberate, and premeditated attack on European energy infrastructure. (European Union Institute for Security Studies, 2025)

c. Cyberattacks on Critical Infrastructure: War Through Screens

Cyberattacks emerged at the forefront of events in 2025, as cyberspace turned into the next arena of conflict. Digital infrastructure – electricity, water, communications, information systems – becomes the front line in a concept known as "war without bullets." In a joint warning issued in December 2025, the US National Security Agency (NSA), the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA) revealed that pro-Russia hacktivist groups were targeting critical infrastructure globally. It was observed that these groups exploit inadequately secured VNC connections to penetrate operational technology (OT) devices within critical infrastructure systems. Targeted sectors included water and wastewater systems, food and agriculture, and the energy sector. In a notable development, a new study revealed more than 237 cyberattacks targeting space infrastructure between 2023 and 2025. (National Security Agency (NSA),, 2025)

3. Legal Frameworks for the Protection of Critical Infrastructure

The transformation of infrastructure into strategic targets cannot be understood in isolation from the legal frameworks that regulate and restrict such targeting in armed conflicts. International humanitarian law, foremost the Geneva Conventions of 1949 and the Additional Protocols of 1977, established a set of well-established principles that protect civilian objects, including critical infrastructure, and prohibit indiscriminate or disproportionate attacks. However, rapid technological development and the emergence of concepts such as "dual-use objects" and "cyber warfare" pose new challenges to the effective application of these rules. Moreover, the absence of a unified legal definition of critical infrastructure, and the differing interpretations of the principle of distinction and proportionality by states, create serious loopholes exploited by occupying powers to justify targeting water, electricity, and communications networks. (Public International Law , 2025, p 05-06)

a. The Principle of Distinction and Military Objectives

The targeting of infrastructure in armed conflicts is subject to a set of strict rules under international humanitarian law. Article 52(2) of Additional Protocol I to the Geneva Conventions prohibits attacks on civilian objects and only permits the targeting of "military objectives," defined as objects which by their nature, location, purpose, or use make an effective contribution to military action and whose total or partial destruction offers a definite military advantage. Energy infrastructure, under this framework, is not completely immune from attack, but neither is it a presumed target. The 1956 draft rules of the International Committee of the Red Cross stipulated that energy installations are not considered military objectives unless they supply military consumption "primarily," a criterion focusing on primary rather than secondary function. The UN High Commissioner for Human Rights, Volker Türk, warned in April 2026 that "deliberate attacks on civilians and

civilian infrastructure constitute a war crime. ("Cyber Warfare: Risks and Protection of Civilians," , 2025)

b. The Problematic of Dual-Use Objects

Dual-use objects – things that serve both civilian and military purposes – represent one of the most complex legal issues in contemporary international humanitarian law. These include energy, water, transport, and civilian communications infrastructure that can also be used for military purposes. Although attacks on critical infrastructure are traditionally justified as part of a legitimate military strategy, experts are concerned about the idea of depriving civilian populations of essential goods and services for their survival. Recent studies indicate that the concept of "dual-use" does not by itself transform civilian infrastructure into a legitimate target; rather, military contribution must be independently proven. However, this analysis is highly contested, as the US Department of Defense Law of War Manual treats "war-sustaining" objects, including energy exports that finance the war effort, as legitimate military objectives. However, the majority of states and many international humanitarian law scholars have rejected this position. (Public International Law & Policy Group (PILPG), , 2025)

c. Recent Legal Developments: The International Criminal Court

Recent years have witnessed important developments in the accountability of perpetrators of attacks on infrastructure. The International Criminal Court (ICC) issued arrest warrants for Russian military officials for their actions during the war against Ukraine, where attacks on critical infrastructure in Ukraine were considered war crimes. Reports of the UN Independent International Commission of Inquiry on Ukraine also indicated that Russia's systematic targeting of energy infrastructure may amount to war crimes and, in some cases, crimes against humanity. The International Committee of the Red Cross also launched the "Digital Emblem" initiative – a modern extension of the Red Cross and Red Crescent in cyberspace – to protect the networks and systems used by humanitarian organizations from cyber operations. ("Cyber Warfare: Risks and Protection of Civilians," , 2025)

4. Case Studies: Ukraine and Gaza

The validity of hypotheses concerning the transformation of infrastructure into strategic targets cannot be tested without reference to living, contemporary models. Both the war in Ukraine and the aggression on the Gaza Strip stand out as the most prominent case studies embodying this transformation starkly. In Ukraine, energy infrastructure turned into a systematic battlefield, with more than 1,225 attacks on electricity and water networks recorded in 2025 alone, aiming to freeze civilians and drain their morale before winter. In Gaza, the targeting of infrastructure took a different but equally destructive form, as the healthcare, water, and sanitation systems were systematically destroyed, leading to

catastrophic famine affecting a quarter of the Strip's population. The analysis of these two cases not only documents violations but also contributes to extracting lessons and strategic recommendations for protecting infrastructure in future wars. (Mada Center,, 2026)

a. Ukraine: The Weaponization of Energy and Comprehensive War on Infrastructure

The war in Ukraine presents the clearest model of the transformation of infrastructure into primary strategic targets. Since the beginning of the full-scale Russian invasion in 2022, Ukrainian energy infrastructure has been subjected to systematic and intensive attacks. By October 2025, Ukraine had lost approximately 50% of its power generation capacity. In 2025 alone, the number of attacks on energy infrastructure reached 1,225, exceeding the total attacks during the first three years of the war, while damage to the grid exceeded $20 billion. On November 8, 2025, Russia carried out a massive coordinated attack using 450 explosive drones and 45 missiles against 25 sites. Reports indicated that these attacks, often concentrated before the onset of winter, specifically target chokepoints such as main transformers and thermal power plants, aiming to drain the morale of civilians. Legally, the Public International Law & Policy Group (PILPG) concluded that "Russia's systematic attacks on Ukrainian energy infrastructure amount to war crimes under international law." (Al Jazeera Net, 2026)

b. Gaza: The Dismantling of Civilian Life's Essentials

In the Gaza Strip, targeting infrastructure took a different but equally destructive form. According to a report issued by Mada Center (March 2026), Israeli forces systematically destroyed the healthcare system in the Gaza Strip over two years. In its report issued in May 2025, the UN estimated that about 470,000 people – a quarter of the Strip's population – suffer from catastrophic hunger, while the rest of the population experiences acute food insecurity. It attributed this to the targeting of civilian infrastructure, including water, electricity, and health facilities. In this context, France condemned the targeting of water infrastructure in May 2025, stating that "Israel's attacks in Gaza that hinder the delivery of humanitarian aid deprive people of access to drinking water, and halt electricity and fuel supplies, which has led to the almost complete shutdown of desalination plants." It affirmed that international humanitarian law provides special protection for critical infrastructure. (Mada Center,, 2026)

5. The Future of Infrastructure in Wars: Trends and Challenges

With the acceleration of digital transformation and increasing reliance on automated systems and artificial intelligence, future wars are moving toward more precise and destructive targeting of critical infrastructure. Threats are no longer limited to bombs and missiles but have extended to cyberattacks that can remotely disable electricity networks and the weaponization of infrastructure itself as a tool for geopolitical blackmail. In this context, a new concept of deterrence has

emerged based on "resilience" rather than traditional punishment, where the state's ability to absorb shocks and recover quickly becomes a deterrent that dissuades adversaries from exploiting vulnerabilities. Technological developments also pose new legal and ethical challenges related to the protection of space infrastructure, submarine cables, and communications networks, which have become the backbone of both civilian and military life. (Jason , 2025, p 05-06)

a. Deterrence by Resilience

Faced with increasing targeting of infrastructure, a new concept of deterrence has emerged based on "resilience" rather than traditional punishment. Experts argue that in a world where adversaries can use disruption to achieve their strategic goals without firing a single shot, deterrence depends on the resilience of the targeted state's critical infrastructure. "Deterrence by resilience" is based on the idea that the state's ability to absorb shocks, adapt, and recover makes adversaries less confident that they can achieve decisive effects. Resilience not only enhances the ability to continue operating under pressure but also sends a clear signal to adversaries that society can continue to resist and retaliate. The world has witnessed examples of this approach: after Estonia suffered cyberattacks in 2007, it invested in distributed systems and external data embassies. Ukraine's wartime shift to cloud computing and satellite communications also helped mitigate the severity of strikes. .(Jason , 2025)

b. The Weaponization of Infrastructure

The weaponization of infrastructure is one of the most dangerous developments in the contemporary strategic landscape. With the increasing digital and physical interconnectedness of the world, infrastructure has transformed from neutral assets into geopolitical tools par excellence. In September 2025, the US Federal Communications Commission approved new regulations banning companies linked to China and Russia from submarine cable projects connected to the United States. These regulations, according to specialized analyses, were not merely an update to technical regulatory policy but the latest step in a systematic effort to reshape the global maritime order. These developments reflect a dangerous shift: the transformation of critical infrastructure from a global public good into a geopolitical weapon. In the same context, energy networks have become an attractive target for weaponization. The Lithuanian Energy Minister warned that "in peacetime, the responsibility for protection lies with energy companies. In wartime, it becomes the responsibility of the Ministry of Defense. What we are seeing in Ukraine is the use of energy as a weapon. (Witold & Karolina , 2025, p 28-30)

c. Strategic Recommendations for the Protection of Future Infrastructure

Based on the above analysis, a set of strategic recommendations for the protection of infrastructure in future wars can be presented: First, Secure by Design: Security considerations must be an integral part of infrastructure planning and construction

from the outset. Second, Strengthening public-private partnerships: Most critical infrastructure is privately owned, placing operators on the front lines of national defense. Third, Decentralization as a national security priority: The Ukrainian experience has shown that solar and wind power plants have proven more resilient to strikes, so experts call for distributing energy sources to reduce chokepoints. Fourth, Cross-sector joint exercises: Simulation helps reveal coordination failures and the real duration of recovery. Fifth, Investing in infrastructure resilience: Defense spending must go beyond traditional focus on platforms and weapons to include investment in backup power, redundant cables, distributed data systems, and trusted partnerships with industry. (Jason , 2025, p 12)

Facts on the ground in Ukraine and Gaza have proven that infrastructure is no longer merely ancillary civilian assets but has become a primary theatre of war and a top-tier strategic target. This transformation is the cumulative result of the evolution of military technology, increased societal dependence on digital systems, and the emergence of hybrid warfare concepts. Analysis of the Ukrainian experience reveals a qualitative shift, as energy infrastructure became a systematic target deliberately depleted before harsh winters to weaken civilian morale. In the face of this reality, the concept of "deterrence by resilience" emerges as a promising strategic alternative, where the state's ability to absorb shocks becomes a deterrent. Legally, despite the existence of well-established frameworks, rapid technological development poses new challenges requiring a review of these frameworks, especially regarding the issue of dual-use objects. In conclusion, no state can protect its infrastructure through physical walls or cyber firewalls alone, but through an integrated approach combining secure design, effective partnerships with the private sector, investment in resilience, and international cooperation to strengthen legal frameworks and accountability mechanisms. In a world where war is fought through submarine cables, pipelines, and data networks, whoever possesses the ability to protect their infrastructure possesses the ability to protect their sovereignty and future. (Al Jazeera Net, 2026)

Conclusion

This study has concluded that critical infrastructure has transformed from being merely civilian assets supporting daily life into pivotal strategic targets in contemporary and future armed conflicts. Through the analysis of the war in Ukraine, it became clear that targeting energy and water networks is no longer a secondary military tactic but has become an integrated combat doctrine aimed at paralyzing the economy, starving civilians, and undermining morale, as confirmed by statistics indicating 1,225 attacks on Ukrainian energy infrastructure in 2025 alone, exceeding the total attacks during the first three years of the war. The study also proved that the concept of "hybrid warfare" has been dangerously embodied in targeting submarine cables and pipelines, as the incident of the Finnish vessel "Eagle S" revealed a systematic pattern by states to weaponize infrastructure and use it as a tool for geopolitical blackmail. Legally, although international humanitarian law provides clear frameworks for the protection of civilian objects,

the issue of "dual-use objects" remains a serious loophole exploited by occupying powers to justify targeting critical infrastructure, as clearly shown in the destruction of the healthcare system in Gaza, where the UN estimated that a quarter of the Strip's population suffers from catastrophic hunger due to targeting water and electricity networks. In conclusion, this study proves that infrastructure is no longer a secondary theatre of operations but has become a primary arena of conflict, necessitating a redefinition of concepts of national security, defense, and deterrence in the twenty-first century.

Recommendations

Based on the findings of the study, and building on the principle of "deterrence by resilience" as a promising strategic alternative to traditional punishment, the researcher recommends the following:

- First: Restructuring infrastructure according to the principle of decentralization.** The study recommends that states, especially those in areas of geopolitical tension, redesign energy and water networks to be decentralized and geographically distributed, rather than relying on large centralized plants representing single points of failure. The Ukrainian experience has shown that distributed solar and wind power plants proved more resilient to Russian strikes compared to large thermal power plants. Decentralization should be considered a national security priority and included in states' strategic planning criteria.

- Second: Activating binding public-private partnerships. Since most critical infrastructure (submarine cables, communications networks, power plants) is privately owned, the study recommends establishing binding legal frameworks imposing minimum security standards on operators and obliging them to participate in joint defense exercises with national armies. In Europe, the cutting of the EstLink 2 cable revealed that private energy companies lacked adequate security protocols to deal with deliberate sabotage, necessitating the intervention of the Finnish navy.

- Third: Explicitly criminalizing attacks on infrastructure in national legal systems. The study recommends that UN member states go beyond the general provisions of international humanitarian law and issue national legislation explicitly criminalizing any attack targeting critical water, energy, and communications infrastructure, even in cases of claimed "dual-use." Such legislation should include the principle of universal jurisdiction to try those responsible for these crimes, akin to the Rome Statute of the International Criminal Court regarding war crimes.

- Fourth: Establishing a permanent international mechanism for the protection of submarine cables.** The study recommends establishing an international naval force (similar to the UN Interim Force in Lebanon "UNIFIL") tasked with protecting submarine cables and pipelines in vital areas (such as the Baltic Sea and the North Sea). This mechanism should have a clear mandate to intervene in cases of

deliberate sabotage and operate under Chapter VII of the UN Charter, to deter states from weaponizing this infrastructure as tools for geopolitical blackmail.

- Fifth: Adopting the "Secure by Design" principle in urban planning.** The study recommends that governments adopt a mandatory approach in licensing new cities and industrial zones, so that energy, water, and communications systems are designed from the outset to withstand cyber and physical attacks, with redundant and backup systems. This principle should extend to space infrastructure, as the study revealed 237 cyberattacks targeting satellites, necessitating the protection of these vital assets that support navigation and communications in wartime.

Bibliography:

"2025 Harvest.. Russian Field Advances and Weak Hopes for Ending the War in Ukraine," . (2026, January 01). Consulté le 03 24, 2026, sur Al Jazeera Net.

"Cyber Warfare: Risks and Protection of Civilians," . (2025, June 04). Consulté le 03 25, 2026, sur International Committee of the Red Cross (ICRC),;.

Al Jazeera Net. (2026, January 01). *Al Jazeera Net, "2025 Harvest.. Russian Field Advances and Weak Hopes for Ending the War in Ukraine,"*. Consulté le 03 23, 2026, sur Al Jazeera Ne.

Al Jazeera Net. (2026, January 04). *Al Jazeera Net, "What Did 'Cyber Week 2025' Reveal About Future Wars?,".* Consulté le 03 25, 2026, sur Al Jazeera Net,.

European Union Institute for Security Studies. (2025, August 25). "On a war footing: Securing critical energy infrastructure," . 03-05.

Irregular Warfare Center, "Energy Grid Vulnerability,. (2025, November 25). Consulté le 03 23, 2026, sur Irregular Warfare Center;: https://irregularwarfarecenter.org/publications-archive/

Jason , V. (2025, November 12). "Resilient critical infrastructure is its own deterrence,". **The Strategist**, 5-6.

Mada Center,. (2026, March 23). *"The Gaza Doctrine: War Through the Dismantling of Civilian Life Essentials,".* Consulté le 03 29, 2026

National Security Agency (NSA),. (2025, December 09). *"Pro-Russia Hacktivists Conduct Cyberattacks Against Critical Infrastructure," .*

Public International Law & Policy Group (PILPG), "Legal Analysis of Attacks on Ukrainian Energy Infrastructure," . (2025). Consulté le 03 27, 2026, sur

Public International Law & Policy Group (PILPG): https://share.google/J10hBr6Iqa5Jpi2q6

Public International Law , P. (2025, November 03). "International Humanitarian Law in Focus: Russia's Violations and Ukraine's Legitimate Use of Force against Energy Targets," . 05-06.

Witold , S., & Karolina , W. (2025). "Critical infrastructure as a target for hybrid operations. Case studies of attacks against the facilities and systems of CI,". **Terrorism – studies, analyses, prevention*, Special Issue*, 13-34.