УДК 351.78:355.45
УДК 007:004.056.5
УДК 355.425:351.86

ASSESSING THE VULNERABILITIES OF CRITICAL INFRASTRUCTURE IN THE AGE OF HYBRID THREATS

Teodora Gjorgjievska[1]
PhD Candidate in Security Studies, University of Ss. Cyril and Methodius,
Institute for Security, Defence and Peace

Abstract: The protection of critical infrastructure is vital to the stability and security of modern societies and is a cornerstone of national and international security. As the threat landscape evolves, traditional security measures are increasingly insufficient to address the emerging complexity of hybrid threats. These threats, which combine elements of conventional, irregular, and cyber warfare, pose significant challenges to the resilience of critical infrastructure systems. This paper explores the vulnerabilities of critical infrastructure in the context of hybrid threats, examining the physical, cyber, and organizational risks that compromise the integrity of essential systems such as energy, transportation, communications, water and health. Through case studies, including cyberattacks on critical infrastructure systems and terrorist extremism on oil fields, the paper highlights the multifaceted nature of these threats and their potential cascading effects globally across interconnected infrastructure sectors. The paper concludes by exploring strategies for assessing these vulnerabilities, highlighting the importance of integrated cybersecurity measures and physical security improvements, with an emphasis on unified action by countries and proactive strategies to safeguard critical infrastructure in an increasingly complex hybrid threat environment.

Keywords: critical infrastructure, hybrid threats, vulnerability, resilience

Introduction

Critical infrastructure (CI) forms the backbone of modern societies—it is the essential foundation required for a state's functioning, economic prosperity, and everyday life. Resilient and secure CI underpins effective business operations, public services, and long-term investor confidence, acting as both a direct economic catalyst and an enabler of broader economic growth. Disruptions to sectors such as energy, transportation, water, healthcare, telecommunications or financial systems can lead to severe direct damages (repair costs, operational losses) and indirect impacts (global supply chain disruption, unemployment, economic decline) (Public Safety Canada, 2016).

Attacks on CI are no longer theoretical—whether through sabotage, cyberattacks or disinformation campaigns—they can inflict catastrophic consequences not only for the affected state but also for neighboring regions and even globally. High-impact incidents, like major ransomware hacks or infrastructure sabotage, demonstrate that a single breach in water supply, electricity, or communication systems may trigger social instability, economic collapse, and public safety crises.

[1] Contact address: gorgievskaa.teodora@gmail.com

Globalization and accelerated interconnectivity have intensified and exacerbated traditional international security challenges, while also giving rise to new, subtler and more pervasive forms of threat. These threats are often described under the umbrella of **hybrid threats** (HT) – a concept that refers to coordinated hybrid campaigns using diverse means to undermine a target. According to the European Union's framework, HT include a mix of information manipulation, cyberattacks, economic coercion, diplomatic or covert political interference, and threats of force–designed to remain below the threshold of conventional warfare (Council of the European Union, n.d.). NATO likewise defines HT as a blend of military and non-military means–covert and overt–such as disinformation, cyberattacks, economic pressure, proxy operations or regular forces, aimed at blurring the line between war and peace and destabilizing societies (Council of the North Atlantic Treaty Organization, 2024).

While definitions overlap, terminology varies by institution: the EU predominantly uses the term *hybrid threats*, emphasizing the broad spectrum of tools and the institutional response needed. NATO, on the other hand, frequently refers to *hybrid warfare* or *hybrid war*, focusing more on the security and military dimension of asymmetric conflict. In narratives advanced by the Russian Federation, terms such as *colour revolutions* and *hybrid war* are used to describe externally influenced regime-change phenomena and unconventional methods of power projection.

Within this evolving security landscape, the need to protect CI and bolster its resilience against HT has become paramount. Traditional protection measures–such as physical security or IT hardening–are no longer sufficient. A comprehensive, adaptive and proactive strategy is required. Nonetheless, a fundamental prerequisite to designing such defenses is a rigorous vulnerability assessment of CI in relation to HT: identifying structural weaknesses, evaluating risk vectors, and preparing effective responses.

This precise task–**assessing the vulnerability of critical infrastructure in the age of hybrid threats**–is the core challenge addressed by this paper. Assessing the vulnerability of CI to HT will, in the long term, provide valuable insights for enhancing resilience and mitigating the risks of hybrid attacks.

Understanding Critical Infrastructure

The origins of the concept of CI can be traced back to the very beginnings of organized human society. While the term "critical infrastructure" is modern, the essence of the concept–vital systems and resources without which a community cannot function–has existed for millennia. In ancient civilizations, key facilities and systems were regarded as the foundation of security, economic stability, and societal survival. In Ancient Rome, for example, roads, aqueducts, and bridges represented indispensable infrastructural assets, enabling the supply of fresh drinking water, facilitating trade, and ensuring the rapid movement of military units (Hodge, A. T., 2002). In Ancient China, the Great Wall served as a strategic defensive infrastructure, designed to protect territorial integrity from invasions, while also acting as a symbol of political authority and economic strength (Waldron, A. N., 1990).

Today, there is no universally accepted definition of CI, as its interpretation varies according to institutional and security contexts. The Organization for Security and Co-operation in Europe (OSCE) defines it as "systems and assets whose incapacitation would have a serious impact on the health, safety, security, or economic well-being of people"

(Organization for Security and Co-operation in Europe, 2013). The European Union, in *Council Directive 2008/114/EC*, describes it as "assets, systems, or parts thereof, which are essential for the maintenance of vital societal functions, health, safety, security, and the economic or social well-being of people" (Council of the European Union, 2008). NATO follows a similar approach, Allied Command Operations defines CI as a nation's infrastructure, assets, facilities, systems, networks, and processes that support the military, economic, political, and/or social life on which a nation and/or NATO depends (U.S. Army War College Strategic Studies Institute, 2023).

In its broadest sense, CI refers to those vital sectors whose disruption could lead to catastrophic consequences for a state and its citizens. Such consequences may include economic collapse, serious disruption of public order, loss of human life, or a decline in public trust in institutions. Given the diversity of threats and the distinct national contexts, each country determines its own critical sectors, taking into account geopolitical conditions, technological development, economic structure, and security priorities. Most states formulate national strategies for the protection and resilience of CI, incorporating risk assessments, preventive measures, and incident response plans.

Although the exact composition of critical sectors differs from country to country, several categories are frequently regarded as core. These include the energy sector (encompassing power grids, gas pipelines, and oil pipelines), the transport sector (which covers road, rail, maritime, and air transport systems), the information and communication technology sector (including telecommunications networks, internet infrastructure, and data centers), the water sector (covering water supply networks, reservoirs, treatment plants, dams, and wastewater management systems) and the healthcare sector (including hospitals, medical facilities, and emergency medical services). These sectors are not only individually vital but also deeply interconnected, meaning that disruption in one can generate cascading effects across others. This interdependence significantly increases their vulnerability, particularly in an era of complex and multi-dimensional security threats.

Hybrid Threats – New Challenge for Critical Infrastructure

Having established the historical origins, definitions, and sectoral scope of CI, it is essential to examine the nature of the threats it faces in the contemporary security environment. Understanding the distinctions between traditional and HT is a necessary step in assessing their respective impacts and in shaping appropriate strategies for resilience and protection.

As it shown in the table below, traditional threats, such as military aggression or invasion, involve clearly identifiable actors—most often nation-states and their armed forces—employing conventional weaponry in the context of a formally declared conflict. These threats tend to unfold openly, with defined beginnings and recognizable escalation patterns. HT, by contrast, represent a combination of military, economic, cyber, and informational methods, often conducted by concealed actors such as non-state groups, mercenaries, or cyber hackers, whose identities are difficult to verify. Rather than operating within the framework of open warfare, hybrid actors frequently act within the so-called "gray zone" between peace and war (Nye, J. S. Jr., 2016), where activities are deliberately ambiguous to avoid direct military escalation. Their tools may include cyberattacks, media manipulation, financial pressure, or

energy coercion, all aimed at undermining stability without triggering a formal declaration of hostilities.

Traditional threats	**Hybrid** threats
Military aggression, invasion	A combination of military, economic, cyber and information methods
Visible actors (military, state)	Often covert actors (non-state groups, cyber hackers)
A clear definition for conflict	A gray area between peace and war
Conventional weapon	Cyber tools, media, finance, energy

Table 1. *Differences between traditional and hybrid threats*

It is evident that the destructive potential of HT is a matter of serious concern, especially when it comes to CI. Modern infrastructure systems are highly digitized and interconnected, making them susceptible to rapid and wide-ranging disruption. The objective of hybrid attacks against CI is often to impair the normal functioning of the state, to generate chaos and fear, to destabilize the economy, or to erode public trust in institutions. For instance, in Ukraine in 2015 and 2016, coordinated cyberattacks on the power grid left hundreds of thousands without electricity, demonstrating how a targeted digital operation can paralyze a vital sector (Lee, Assante and Conway, E-ISAC, 2016). In other cases, disinformation campaigns regarding the safety of drinking water or the efficacy of vaccines have the potential to incite mass panic, weaken institutional credibility, and create widespread social instability.

What makes this category of threat especially dangerous compared to more conventional forms is the combination of precision targeting, cost asymmetry, and attribution challenges. Hybrid operations are often directed at critical systems that are difficult to replace, and whose disruption causes long-lasting consequences. The cost of executing such operations for the attacker—particularly in the cyber domain—can be minimal, while the damage to the target can be immense, affecting economic stability, public safety, and national security. Moreover, the covert nature of these threats means that identifying their source is often extremely difficult, which complicates both defensive measures and any form of retaliation.

With these attributes, HT represent a persistent and evolving challenge for CI protection. Addressing them requires adaptive security strategies, enhanced inter-institutional coordination, and the development of capabilities for rapid detection and response before the consequences become irreversible.

CI Vulnerabilities Assessment in Relation to HT

Following the discussion on the nature and characteristics of HT in the previous section, it is necessary to proceed with an analysis of their impact on CI. Understanding these vulnerabilities represents a fundamental step in establishing effective protection mechanisms. While traditional threats are usually direct and easily identifiable, hybrid attacks are covert and multidimensional, which significantly increases their potential to destabilize. In particular importance is to observe how the

complex nature of HT affects different sectors of CI, identifying potential vulnerabilities and assessing their exposure to risk.

Sector	Potential vulnerabilities	Influence of HT
Energy	Outdated equipment, centralized systems, insufficient protection against cyberattacks	Cyber-attacks on energy networks, sabotage, impact on supply
ICT	Insufficient encryption, dependence on external suppliers	Infiltration through malware, spreading disinformation, cyber espionage
Health	Insufficient digital protection, lack of backup systems	Cyber-attacks on hospitals, misuse of health data
Transport	Automated systems without adequate cyber protection	Disruption of logistics chains, GPS jamming
Water supply	Outdated SCADA systems, poor physical access	Infiltration, poisoning or disruption of the system

Table 2. *Crucial critical sectors, their vulnerabilities and influence of HT*

The energy sector is one of the most sensitive segments of CI. Outdated equipment, centralized management models, and insufficient protection against cyberattacks create a wide range of opportunities for potential attackers. The consequences can be catastrophic, ranging from temporary disruptions in electricity supply to systemic collapse affecting entire regions. Cyberattacks on Ukraine's power grid in 2015–2016 serve as a clear example of this risk leaving hundreds of thousands without electricity (Lee, Assante and Conway, E-ISAC, 2016). Moreover, sabotage and manipulations of energy systems can cause economic instability and undermine trust in institutions (European Parliament, 2025).

In the field of information and communication technology (ICT), insufficient encryption and a high dependence on external providers make this sector particularly vulnerable (European Union Agency for Cybersecurity - ENISA, 2023). HT in this domain often manifest through malware infiltration, the spread of disinformation, and cyber espionage. Such attacks frequently have long-term consequences, such as undermining national security or compromising democratic processes. For instance, coordinated disinformation campaigns can shape public discourse and increase polarization within society. A striking case is the town of Veles in North Macedonia, which gained international attention during the 2016 U.S. presidential election. Hundreds of websites operated by individuals from Veles produced and disseminated large volumes of fabricated political content, much of it favoring one candidate over the other. These disinformation sites attracted millions of readers through social media platforms such as Facebook, amplifying political polarization and contributing to the spread of misleading narratives (Subramanian, 2017). The Veles case demonstrates how small groups with limited resources can exploit the global reach of digital platforms to interfere with democratic processes in powerful states.

The healthcare sector, particularly during times of crisis (such as the COVID-19 pandemic), represents a critically sensitive area. The lack of sufficient digital protection and backup systems makes healthcare institutions easy targets (European Union Agency for Cybersecurity - ENISA, 2023). Cyberattacks on hospitals can paralyze their operations, directly endangering human lives (Dameff, C. et al., 2023). Additionally, the misuse of medical data poses a severe threat to citizens' privacy and security (Shah, S. M., & Khan, R. A., 2020).

In the transportation sector, system automation brings significant benefits but also serious risks if not accompanied by adequate cyber protection. Hybrid attacks can result in disruptions of logistic chains, GPS jamming, or even the triggering of accidents. The consequences can include paralysis of international trade or the creation of chaos in urban environments (Yu, Z., Kaplan, Z., Yan, Q., & Zhang, N., 2021).

The water supply sector represents another critical point where HT may have a destructive impact. Outdated SCADA systems and insufficient physical protection create opportunities for infiltration, poisoning, or disruption of the system (Hassanzadeh, A., et al, 2020). A striking example occurred in Oldsmar, Florida, in 2021, when a hacker remotely accessed the city's water treatment facility and attempted to raise the level of sodium hydroxide to toxic concentrations. Although the attack was detected in time, the incident exposed how vulnerable water infrastructure remains to cyber intrusions, with potentially catastrophic consequences for public health and trust in essential services (BBC, 2021). Even disinformation about water quality could cause mass panic among the population, thereby undermining social stability (Sarkar, R., Sarkar, H., Mahinder, S., & KhudaBukhsh, A. R., 2020). For instance, in Mozambique, a widespread rumor about a cholera outbreak led hundreds of residents to flee via an overloaded ferry, resulting in the vessel capsizing and more than 90 fatalities, including children, according to official reports (BBC, 2024). This tragic event illustrates how disinformation about water quality can rapidly escalate into social panic, destabilizing communities and overwhelming emergency response systems, reinforcing the critical need for robust communication and resilience strategies in the water sector.

The overall picture that emerges from the analysis of these sectors is that HT exploit the technological dependency of modern societies, combining it with political and psychological strategies. What makes these threats particularly dangerous is their ability to cause massive damage to a state or community with minimal investment on the part of the attacker. The difficulty of identifying the origin of such attacks further complicates defense, limits the capacity for adequate response, and increases the likelihood of long-term consequences.

Therefore, vulnerability assessment is not merely an analytical process but a fundamental prerequisite for developing effective protection strategies against HT. Any weakness that remains unnoticed may serve as an entry point for attackers. This calls for a systematic approach capable of identifying and addressing the critical points of each sector.

Case study

Vulnerabilities of CI in the face of HT were systematically assessed and to deepen the understanding of how these vulnerabilities manifest in real-world contexts, it is essential to analyze concrete cases where HT have directly impacted CI. Case studies provide not only practical illustrations but also valuable insights into the methods, consequences, and broader implications of such threats. In this context, two significant cases have been selected: the cyberattacks carried out by the pro-Russian hacker group KillNet during 2022–2023, and the physical attacks against the oil infrastructure of Saudi Aramco in 2019. These two cases illustrate different but equally important dimensions of HT: the digital domain of cyber warfare and the physical targeting of energy infrastructure.

The first case focuses on the activities of KillNet, a pro-Russian hacktivist group that became particularly active following Russia's invasion of Ukraine in February 2022 (Dickson, J., & Harding, E., 2025). The group primarily employed distributed denial-of-service (DDoS) attacks, overwhelming servers with traffic to render critical online services inaccessible. Their operations targeted the CI of countries openly supporting Ukraine. Notable examples include mass DDoS attacks against Lithuanian institutions, which resulted in disruptions to the national power grid (Goodin, D., 2022), as well as attacks on U.S. airports that caused flight cancellations and the temporary shutdown of official websites (Eich, A., 2022). Similarly, Italian government websites, hospitals, and telecommunications companies were affected (Brucato, A., 2022). Beyond the technical disruptions, KillNet also engaged in disinformation campaigns and mobilization of sympathizers through social media 'Telegram' (Scroxton, A., 2022). The consequences highlighted the urgent need for enhanced cybersecurity resilience across European and U.S. institutions, demonstrating how non-state actors can create significant destabilization through relatively low-cost digital means.

The second case examines the 2019 attacks on Saudi Aramco, one of the largest state-owned oil companies in the world. The attacks were carried out using drones and missiles, reportedly launched by Houthi extremists with suspected Iranian backing (BBC News, 2019). The strikes targeted oil fields and processing facilities, severely damaging Saudi Arabia's production capacity. In the immediate aftermath, the country's oil output was reduced by nearly 50%, representing one of the largest sudden disruptions in global oil supply in modern history (Piotrowski, M. A., 2019). The effects were quickly reflected in global markets: oil prices surged nearly 20% within days, with Brent crude posting its biggest intraday gain since the 1990-1991 Gulf crisis, before paring gains (Ahmed, S. I., 2019). The consequences went beyond economic disruption, sparking heightened political tensions between Saudi Arabia and Iran, as well as renewed concerns in Western capitals (NATO allies) over the possibility of regional escalation (NATO Secretary General Stoltenberg, 2019). In response, Saudi Arabia invested in anti-drone technologies and upgraded its air defense systems (Army Recognition, 2024). More broadly, this case underscored the profound vulnerabilities of global energy infrastructure and the cascading economic, political, and security crises that can result from targeted attacks.

Taken together, these two case studies illustrate why HT must be treated as a central security challenge of the 21st century. The KillNet attacks demonstrate how cyber operations can paralyze critical services and undermine trust in institutions, while the Aramco incident exemplifies how physical attacks on critical energy infrastructure can generate far-reaching global consequences. Both cases highlight the importance of strengthening defense mechanisms, enhancing resilience, and fostering international cooperation to protect CI. The analysis of these cases provides not only lessons learned but also a framework for understanding the multidimensional nature of HT.

Strategies and measures in assessing vulnerabilities to CI from HT

The assessment of vulnerabilities of CI to HT represents an essential element in the contemporary security policies of the European Union and NATO. Concerning this specific challenge to security, the United States have established a Cybersecurity and Infrastructure Security Agency. All of these organizations and actors have developed different, but mutually

complementary approaches in order to ensure coordinated and effective risk reduction, as well as to strengthen the resilience of systems that are of fundamental importance for the functioning of societies.

Within the European Union, the Critical Entities Resilience Directive (CER, 2022) stands out as one of the most significant legal instruments, as it obliges Member States to systematically identify CIs and to conduct regular risk assessments. This is important because it ensures constant situational awareness of potential HT, particularly those arising from geopolitical risks and vulnerabilities in global supply chains (Council of the European Union, & European Parliament, 2022A). The CER Directive goes beyond mere identification, mandating the development of national resilience plans that guarantee operational continuity and the ability to respond to multidimensional attacks – a combination of physical, cyber, and psychological operations. This comprehensive framework is highlighted as crucial because it integrates all domains of potential threats and provides the foundation for the collective protection of European societies.

The second key instrument of the Union is the second Network and Information Security (NIS2) Directive of 2022, which builds upon the first NIS Directive from 2016. NIS2 is significant because it requires operators of essential services to conduct risk assessments through an "all-hazards" approach. This approach is crucial as it acknowledges the complexity of HT and the necessity of considering all potential sources of risk – from cyberattacks to physical sabotage. Furthermore, the directive obliges entities to establish systematic security policies, vulnerability management procedures, and to conduct regular simulations and tests. In this way, NIS2 not only sets technical protection standards but also directly strengthens institutional and organizational resilience (Council of the European Union, & European Parliament, 2022B).

Special attention is also deserved by the ProtectEU Strategy of 2025, which represents the latest integrated framework for protecting European CIs. It is important because, for the first time, the EU has created a holistic approach that combines the development of national cybersecurity strategies, mechanisms for information sharing, and coordinated responses at the European level through the EU Critical Infrastructure Blueprint. This strategy is particularly significant for vulnerability assessment as it enables Member States to link their capacities with those of European agencies such as ENISA and Europol, thereby achieving a higher level of integrated security culture (European Commission, 2025).

NATO, on its part, emphasizes the military and security dimensions of vulnerability assessments. The warfare against HT has undergone significant upgrades from 2015 to 2023, and establishes a important framework for integrated responses to combined threats targeting the communications, energy, and military capacities of Allies (North Atlantic Treaty Organization, n.d.). In this regard, NATO members in 2016, agreed on the seven Baseline Requirements of National Resilience, against which Allies can measure their level of preparedness. These baselines provide guidelines and evaluation criteria that enable Allied nations to conduct assessments of their resilience, aligned with the overarching NATO Defence Planning Process. In 2021, NATO Heads of State and Government agreed on Strengthened Resilience Commitment, reinforcing the importance of national and collective resilience against the conventional, non-conventional and especially emphasizing HT and activities of adversaries, and provided further direction and guidance for resilience-related work at NATO through the NATO 2030 agenda and later the 2022 Strategic Concept (North Atlantic

Treaty Organization, 2023). Also, the Locked Shields and Steadfast Defender exercises stand out as unique mechanisms for simulating real hybrid scenarios, allowing Allies to test and improve their response capabilities (NATO Cooperative Cyber Defence Centre of Excellence, n.d.). Additionally, the Cooperative Cyber Defence Centre of Excellence in Tallinn represents a leading hub for research and training, underlining the importance of knowledge and preparedness in addressing contemporary threats (NATO Cooperative Cyber Defence Centre of Excellence, 2023).

On the other hand, the United States through the Cybersecurity and Infrastructure Security Agency (CISA), has developed specific tools for vulnerability assessments. The programs are important because they enable the practical application and measurement of resilience in critical systems. The Infrastructure Survey Tool (Cybersecurity and Infrastructure Security Agency, 2023A) and the Cyber Infrastructure Survey (Cybersecurity and Infrastructure Security Agency, 2023B) provide detailed assessments of weaknesses in both physical and digital domains, while the Cyber Resilience Review is particularly significant because it does not limit itself to technical aspects but focuses on organizational maturity and resilience. The Cross-Sector Risk Management approach is especially important as it enables analysis of interdependencies among different sectors, which is crucial in conditions where HT often target interconnected infrastructure systems.

This combination of European regulations and strategies, NATO security frameworks, and American practical tools creates a multinational and multidomain system for vulnerability assessment. This is why their consideration is essential – they represent mutually reinforcing models that strengthen global resilience of CI and ensure a comprehensive response to HT.

Conclusion

The assessment of vulnerabilities of CI from HT represents a fundamental process that provides the basis for developing effective protection strategies and strengthening a state's security and stability. This paper highlighted the key instruments and approaches developed by the European Union, NATO, and the United States, demonstrating that only through an integrated and unified approach can the risks posed by HT be timely identified and neutralized. Moreover, the necessity of developing adequate national strategies is particularly emphasized, as each state faces specific security contexts and varying levels of vulnerability within its infrastructural systems. Adapting existing strategies and creating new mechanisms of assessment is imperative, especially in conditions of the dynamic evolution of HT.

That being said, the paper underlined the need for unified and coordinated action among states and international organizations. Only through joint exchange of information, standards, and resources can timely and precise vulnerability assessments be achieved, enabling effective prevention and response to HT. The vulnerability assessment process enables the detection of potential weaknesses, provides an understanding of the impact from HT, and subsequently forms the basis for the establishment of systemic resilience measures. This process should not be understood as a one-time activity, but as a continuous cycle of analysis, testing, and improvement, directly influencing the reduction of risks from the escalation of hybrid attacks.

In the near future, the main challenge will lie in the integration of new technologies and in addressing the growing inter-sectoral interconnectedness of infrastructures, which

further increases the complexity of HT. Therefore, building a culture of resilience, grounded in both national and international frameworks, remains a central task in the protection of CI.

References

- Ahmed, S. I. (2019). *Oil soars after attack on Saudi facilities, stocks dip*. Reuters. Retrieved June 2025, from: https://www.reuters.com/article/business/oil-soars-after-attack-on-saudi-facilities-stocks-dip-idUSKBN1W00WA/
- Army Recognition. (2024). *Saudi Arabia reveals integration of six advanced air defense systems to counter modern threats*. Retrieved June 2025, from: https://armyrecognition.com/news/army-news/army-news-2024/saudi-arabia-reveals-integration-of-six-advanced-air-defense-systems-to-counter-modern-threats
- BBC News. (2019). *Saudi oil attacks: Drones and missiles launched from Iran – US*. Retrieved June 2025, from: https://www.bbc.com/news/world-middle-east-49733558
- BBC News. (2021). *Hacker tried to poison Florida city's water supply*. Retrieved July 2025, from: https://www.bbc.com/news/world-us-canada-55989843
- BBC News. (2024, April 8). Mozambique ferry disaster kills more than 90 – officials. Retrieved July 2025, from: https://www.bbc.com/news/world-africa-68758345
- Brucato, A. (2022). *KillNet cyber attacks against Italy and NATO countries*. Sysdig. Retrieved July 2025, from: https://www.sysdig.com/blog/killnet-italy-and-nato
- Council of the European Union. (n.d.). Hybrid threats. Retrieved May 30, 2025, from: https://www.consilium.europa.eu/en/policies/hybrid-threats/
- Council of the North Atlantic Treaty Organization. (2024). *Countering hybrid threats*. Retrieved May 30, 2025, from: https://www.nato.int/cps/en/natohq/topics_156338.htm
- Council of the European Union. (2008). *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.* Retrieved May 2025, from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32008L0114
- Council of the European Union, & European Parliament. (2022A). *Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical entities and repealing Council Directive 2008/114/EC. Official Journal of the European Union*, L 333, 164–198. Retrieved July 2025, from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022L2557
- Council of the European Union, & European Parliament. (2022B). *Directive (EU) 2022/2555 of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive)*.

Official Journal of the European Union, L 333, 80–152. Retrieved July 2025, from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

- Cybersecurity and Infrastructure Security Agency. (2023A). *Infrastructure Survey Tool (IST) Fact Sheet*. Retrieved July 2025, from: https://www.cisa.gov/sites/default/files/2023-06/infrastructure_survey_tool_ist_fact_sheet-2023.pdf
- Cybersecurity and Infrastructure Security Agency. (2023B). *Cyber Infrastructure Survey (CIS) Fact Sheet*. Retrieved July 2025, from: https://www.cisa.gov/sites/default/files/2023-12/cybersecurity-resources-for-9-1-1-centers_112023_508.pdf
- Dameff, C., Tully, J., Chan, T. C., Castillo, E. M., Savage, S., Maysent, P., Hemmen, T. M., Clay, B. J., & Longhurst, C. A. (2023). *Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. JAMA network open*, *6*(5), e2312270. https://doi.org/10.1001/jamanetworkopen.2023.12270
- Dickson, J., & Harding, E. (2025). *How a cyber alliance took down Russian cybercrime*. Center for Strategic and International Studies. Retrieved July 2025, from: https://www.csis.org/analysis/how-cyber-alliance-took-down-russian-cybercrime
- Eich, A. (2022). *KillNet: Russian hacktivists DDoS US airports, government websites*. University of Hawai'i–West O'ahu. Retrieved July 2025, from: https://westoahu.hawaii.edu/cyber/uncategorized/killnet-russian-hacktivists-ddos-us-airports-government-websites
- European Commission. (2025). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on ProtectEU: A European Internal Security Strategy* (COM(2025) 148 final). Retrieved July 2025, from: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52025DC0148&
- European Parliament. (2025). *Report on the security of energy supply in the EU* (2025/2055(INI)). Committee on Industry, Research and Energy. Retrieved July 2025, from: https://www.europarl.europa.eu/doceo/document/A-10-2025-0121_EN.html
- European Union Agency for Cybersecurity (ENISA). (2023). *ENISA Threat Landscape 2023*. Retrieved June 2025, from: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf
- Goodin, D. (2022). *Pro-Russia threat group KillNet is pummeling Lithuania with DDoS attacks*. Ars Technica. Retrieved July 2025, from: https://arstechnica.com/information-technology/2022/06/pro-russia-threat-group-killnet-is-pummeling-lithuania-with-ddos-attacks/
- Hassanzadeh, A., Rasekh, A., Galelli, S., Aghashahi, M., Taormina, R., Ostfeld, A., & Banks, K. (2020). *A review of cybersecurity incidents in the water sector*. *arXiv*. Retrieved June 2025, from: https://arxiv.org/abs/2001.11144

- Hodge, A. T. (2002). *Roman aqueducts & water supply* (2nd ed.). London: Duckworth. Retrieved May 2025, from: https://archive.org/details/t.-hodge-roman-aqueducts-and-water-supply-2002-compressed
- Lee, Assante and Conway, E-ISAC. (2016). *Analysis of the Cyber Attack on the Ukrainian Power Grid.* Retrieved June 2025, from: https://nsarchive.gwu.edu/sites/default/files/documents/3891751/SANS-and-Electricity-Information-Sharing-and.pdfv
- NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *Locked Shields*. Retrieved July 2025, from: https://ccdcoe.org/locked-shields/
- NATO Cooperative Cyber Defence Centre of Excellence. (2023). *World's largest cyber defense exercise Locked Shields brings together over 3,000 participants*. Retrieved July 2025, from: https://ccdcoe.org/news/2023/6016/
- NATO Secretary General Stoltenberg. (2019). *NATO concerned by attacks on Saudi oil facilities* [Press statement]. NATO Watch. Retrieved June 2025, from: https://natowatch.org/newsbriefs/2019/nato-concerned-attacks-saudi-oil-facilities
- North Atlantic Treaty Organization. (n.d.). *Hybrid Warfare: Reports*. NATO Library Guides. Retrieved July 2025, from: https://natolibguides.info/hybridwarfare/reports
- North Atlantic Treaty Organization. (2023). *Resilience and civil preparedness in NATO*. NATO. Retrieved July 2025, from: https://www.act.nato.int/article/resilience-and-civil-preparedness-in-nato/
- Nye, J. S. Jr. (2016). *Deterrence and dissuasion in cyberspace*. *International Security*, 41(3), 44–71. https://doi.org/10.1162/ISEC_a_00266. Retrieved May 15, 2025, from: https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/isec_a_00266.pdf
- Organization for Security and Co-operation in Europe. (2013). *OSCE guidebook on critical infrastructure protection.* Retrieved May 2025, from: https://www.osce.org/files/f/documents/9/5/107155.pdf
- Piotrowski, M. A. (2019). *The tactics and strategic consequences of the attack on oil installations in Saudi Arabia*. Polish Institute of International Affairs (PISM Bulletin No. 137). Retrieved June 2025, from: https://pism.pl/publications/The_Tactics_and_Strategic_Consequences_of_the_Attack_on_Oil_Installations_in_Saudi_Arabia
- Public Safety Canada. (2016). *Role of Critical Infrastructure in National Prosperity*. Government of Canada. Retrieved June 2025, from: https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2016-rl-crtclnfrstrctr-ntnlprsprty/2016-rl-crtclnfrstrctr-ntnlprsprty-en.pdf

- Sarkar, R., Sarkar, H., Mahinder, S., & KhudaBukhsh, A. R. (2020). *Social media attributions in the context of water crisis*. arXiv. https://doi.org/10.48550/arXiv.2001.01697
- Scroxton, A. (2022). *Russia-aligned hacktivists behind Lithuania DDoS attack*. Computer Weekly. Retrieved July 2025, from: https://www.computerweekly.com/news/252522092/Russia-aligned-hacktivists-behind-Lithuania-DDoS-attack
- Shah, S. M., & Khan, R. A. (2020). *Secondary use of electronic health record: Opportunities and challenges*. https://doi.org/10.48550/arXiv.2001.09479
- Subramanian, S. (2017). *Inside the Macedonian Fake-News Complex*. Wired. Retrieved September 2025, from: https://www.wired.com/2017/02/veles-macedonia-fake-news/
- U.S. Army War College Strategic Studies Institute. (2023). *Understanding critical infrastructure: From enabling NATO's collective defense* [Article]. Strategic Studies Institute, U.S. Army War College. Retrieved July 2025, from: https://ssi.armywarcollege.edu/SSI-Media/Recent-Publications/Article/3946047/understanding-critical-infrastructure-from-enabling-natos-collective-defense-ci/
- Waldron, A. N. (1990). *The Great Wall of China: From History to Myth*. Cambridge University Press. Retrieved May 2025, from: https://www.cambridge.org/core/journals/china-quarterly/article/abs/great-wall-of-china-from-history-to-myth-by-arthur-waldron-cambridge-cambridge-university-press-1990-296-pp-3950-isbn-0-521-36518-x/97A7315FC7DEB956C35BBD07F68B8649
- Yu, Z., Kaplan, Z., Yan, Q., & Zhang, N. (2021). *Security and privacy in the emerging cyber-physical world: A survey*. IEEE Communications Surveys & Tutorials**.** https://doi.org/10.1109/COMST.2021.3081450