European Journal for Security Research
https://doi.org/10.1007/s41125-025-00107-2

ORIGINAL ARTICLE

# Hybrid Everything, Operational Nothing: Conceptual Drift, Perpetual Crisis, and the Failure to Prepare for Proxy Terrorism

**Monika Gabriela Bartoszewicz**[1]

Received: 18 June 2025 / Accepted: 4 November 2025


## Abstract

This article examines the strategic implications of conceptual inflation in the evolving discourse of hybrid warfare, with particular focus on its consequences for critical infrastructure protection. Drawing a parallel with the post-9/11 securitisation of terrorism, it argues that the increasingly elastic use of the term "hybrid threat" has created a condition of perpetual preparedness that paradoxically undermines operational readiness. As diverse threat phenomena, from cyber intrusions and disinformation to sabotage and proxy violence, are collapsed under a single hybrid rubric, crisis planning becomes generalised and detached from actor-specific threat logic. Through a comparative analysis of Norway and Taiwan, two advanced but geopolitically exposed democracies, the article demonstrates how national security systems, though resilient, remain conceptually unprepared for deniable, adaptive threats posed by state-backed terrorist proxies. Both countries possess sophisticated infrastructure protection frameworks; yet both continue to treat disruption as accidental or technical, rather than as strategically curated. Drawing on contemporary scholarship, fieldwork, and recent incidents, the article makes the case for a reconceptualisation of infrastructure as a strategic domain vulnerable to intelligent exploitation. It calls for a shift from resilience-based preparedness to anticipatory governance, underpinned by attacker modelling, red-teaming, and clearer typological distinctions. In doing so, it contributes to the growing debate on how to move beyond the rhetoric of hybrid warfare and towards a more operationally grounded framework for future security governance.

**Keywords** Hybrid warfare · Critical infrastructure protection · Proxy terrorism · Resilience and security governance · Taiwan · Norway

✉ Monika Gabriela Bartoszewicz
monika.g.bartoszewicz@uit.no

[1] Institute of Technology and Safety, UiT The Arctic University of Norway, Tromsø, Norway

Published online: 27 November 2025

## 1 Introduction: Hybrid Warfare as the New "Terrorism Hype"

In the years following the 9/11 attacks, terrorism emerged as the dominant frame of global security policy. Governments restructured bureaucracies, rewrote legal frameworks, and reinterpreted both domestic and international risks through the lens of counterterrorism. Critical Infrastructure Protection (CIP) was no exception; from the Tokyo subway sarin attack in 1995 to the destruction of the World Trade Center in 2001, terrorism began to overshadow other threat categories with almost a palpable "obsession". As Wiater (2015) notes, these events not only reshaped strategic discourse but also catalysed a series of policy initiatives, which rapidly became the organizing principle for the international security architecture. In Europe, this trajectory accelerated after the Madrid train bombings (2004) and the London Underground attacks (2005). Lindström and Olsson (2009) show how these events directly shaped the European Union's emerging critical infrastructure agenda, culminating in the launch of the European Programme for Critical Infrastructure Protection, an institutional framework developed in response to the growing recognition that key systems were acutely vulnerable to terrorist attack.

The academic literature likewise reflects this shift. As documented in Table 1, terrorism came to be seen as one of the primary threat vectors for critical infrastructure. White (2019) observes White (2019) observes that prior to this securitisation turn (for detailed overview of the concept see: Bartoszewicz 2016), infrastructure owners and operators were primarily concerned with natural disasters and local vandalism; however, the advent of heightened risk of international terrorism transformed CIP from a technical field into a theatre of strategic concern thereby fundamentally transforming their outlook. Ciupercă and Vevera (2019) argue that these high-profile attacks catalysed a global policy pivot, injecting a new urgency into the governance of essential systems. Yet even at the height of the "War on Terror," which some critics dubbed the "war on error", a perpetual campaign not just against enemies but against uncer-

**Table 1** Overview of Terrorism-Related threat vectors in critical infrastructure protection

| Threat | Authors |
|---|---|
| Hybrid, State-Sponsored and Asymmetric Threats (encompassing covert operations, proxy attacks, economic sabotage and the blending of state and non-state tactics) | Tomko (2002); Jenelius et al. (2010); Koski (2011); Zhang et al. (2015); Taquechel and Lewis (2017); Ciupercă and Vevera (2019); Denysov et al. (2021); White (2019); Osei-Kyei et al. (2021); Böröcz (2021); Pătrașcu (2022); Ruzhin and Mitrevska (2024) |
| Physical Terrorism and Sabotage (deliberate, overt attacks targeting CI assets such as power grids, transport networks, and critical facilities) | Williamitis (2000); Tomko (2002); Pikus (2003); Auerswald et al. (2005); US Department of Transportation (2006); Moteff (2007); Lindström and Olsson (2009); Jenelius et al. (2010); Merabti et al. (2011); Yusta et al. (2011); Lopez et al. (2012); Quigley (2013); Lewis et al. (2013); White et al. (2014); Brown et al. (2005); Hedel et al. (2018); Böröcz (2021); Pătrașcu (2022); Ruzhin and Mitrevska (2024) |

tainty itself, this heightened vigilance rarely produced conceptual clarity. As Bobbitt (2008) famously argued, risk became the battlefield, and governance a performance of preparedness. Terrorism evolved into a catch-all term, encompassing everything from lone actors to insurgents, from ideological violence to infrastructure sabotage. Its rhetorical power far outpaced its analytical precision.

Two decades on, hybrid warfare has inherited the mantle of strategic ambiguity once worn by terrorism. Like its predecessor, it is invoked with increasing frequency and diminishing specificity. Within NATO, the EU, and numerous national security doctrines, "hybrid" now encompasses an expansive array of activities, from cyber-attacks and disinformation to election interference, infrastructure sabotage, proxy conflict, and economic coercion. The 2010 NATO Military Working Group described hybrid threats as those posed by adversaries capable of simultaneously employing conventional and non-conventional means to pursue their objectives; an acknowledgment of complexity and adaptability, but one that offered little clarity regarding actors or intent (Gaiser 2019). Similarly, the European Commission's (2024) definition spans everything from disinformation to the use of proxy actors, yet lacks clear boundaries or identifiable threat agents.

The hybrid threat is everywhere invoked but nowhere operationalised. While policymakers express grave concern over hybrid tactics, there are few concrete models to differentiate, anticipate, or deter them in practice. This yawning gap is especially glaring in the CIP domain. Although many states have formally incorporated "hybrid threats" into their national security strategies, the term rarely exists as a standalone category. Instead, it is nested under broader resilience, cyber, or defence frameworks, underscoring its conceptual fuzziness and lack of operational coherence. Nor is this ambiguity confined to the Euro-Atlantic sphere. Taiwan, arguably the world's most targeted state by hybrid tactics, similarly struggles with the term's strategic clarity. During my interviews with politicians, law enforcement personnel, and security officials, terms such as "non-traditional threats," "grey zone tactics," and "hybrid warfare" were used interchangeably, typically without defined operational parameters. Strategy documents, particularly from the Ministry of National Defence and the Executive Yuan, reference cyber intrusions, disinformation, lawfare, economic coercion, and maritime pressure. Yet these threats are listed as a menu of risks, detached from any overarching theory of threat actor intent or strategic logic.

If the rhetoric of hybrid warfare has become the defining grammar of contemporary security discourse, it is a grammar marked more by accumulation than articulation. Much like the terrorism framing that dominated the early 2000 s, hybrid warfare now functions as a discursive umbrella, expanding continuously to accommodate new, and often contradictory, threat phenomena, albeit without refining their analytical contours. The result is a paradox: a condition of perpetual preparedness that paradoxically leaves us operationally unready. Taking this paradox as a point of departure, I argue that the rise of "hybrid everything" discourse signals a new phase in what Lakoff and Collier (2010, 2015) describe as the eventalisation of crisis, a shift in which threats are imagined, anticipated, and institutionalised not through typological or operational clarity, but through the urgency of narrative. The consequence is a perpetual crisis imaginary: a state of continuous emergency rhetoric that fuels the machinery of preparedness without ever clarifying what, precisely, we are preparing

for. In such an environment, performative sensitivity towards hybrid warfare supplants strategic readiness, and emerging threats, particularly proxy-enabled sabotage of critical infrastructure, fall through the cracks of conceptual inflation.

In what follows, I develop this argument through the comparative cases of Norway and Taiwan: two small but strategically exposed democracies, both facing powerful neighbours known for adversarial foreign policies and the repeated use of hybrid tactics. These cases illustrate how resilience-oriented tactical planning can coexist with persistent strategic blind spots. I employ a qualitative research design that combines fieldwork, semi-structured interviews, and documentary analysis[1] to investigate the evolving discourse of hybrid warfare and its implications for critical infrastructure protection. This integrated approach is particularly well suited to exploring complex, dynamic phenomena such as proxy terrorism, where established quantitative metrics often fail to capture the nuanced interplay between political intent, operational ambiguity, and institutional response faced with the rapid evolution of threat narratives. This design captures the contextual nuance and subtleties of operational readiness and misrecognition that are often lost in quantitative analyses. Given that a qualitative design enables a rich, contextual understanding of these phenomena, my data illuminates not only how hybrid threats are perceived but also underscores the tension between narrative-driven preparedness and actual countermeasures unpacking both the overt and covert dimensions of hybrid warfare strategies. The methodological design thus supports a dual analysis: first, by exposing the disconnect between institutional resilience and the strategic logic of proxy engagements; and second, by providing an empirical basis for rethinking how infrastructure threats are conceptualized and operationalized in contemporary security policy. In this way, the methodological choices are essential to producing a balanced analysis that is both theoretically informed and practically relevant. On this basis, I examine how hybrid threat inflation produces a paradox of preparedness, where institutional systems remain locked in a posture of high alert, yet are ill-equipped to anticipate or deter actor-driven, adaptive threats. In the final section, drawing on recent cases from both countries, I reflect on the broader implications for future security governance, and argue that the time has come to rethink hybrid warfare, not as an ever-widening and self-perpetuating threat taxonomy, but as a conceptual dead end in need of strategic renewal.

[1] Semi-structured interviews with policymakers (3), law enforcement officials (5), and experts in security governance (7) reveal the interplay between official discourse and ground-level practices. Complementary to ethnographic fieldwork documented in research diary, and the interviews, the analysis of official documents, media reports, and policy archives enabled the tracing of how hybrid warfare has been institutionalized within national security frameworks. I mitigated potential personal as well as positionality and selection biases among interview respondents by employing standardized data collection protocols and actively seeking diverse perspectives. Moreover, to reinforce the credibility of my findings, I triangulated data by systematically comparing insights from semi-structured interviews, fieldwork observations, and documentary analysis. This triangulation of data sources enhances the validity and depth of the findings, as it bridges empirical observations with broader theoretical debates. All the data is available upon reasonable request.

## 2 Infrastructure Under Strategic Pressure: Patterns of Plausible Deniability

Among the many forms of hybrid disruption, few are as revealing of the current strategic drift as attacks on undersea infrastructure. Cables, in particular, occupy a peculiar space in security discourse: globally essential, physically vulnerable, and geopolitically sensitive, yet often neglected in traditional threat modelling. The recent spate of cable incidents in both Taiwan and Norway exposes how hybrid threat inflation has failed to produce preparedness for intentional, deniable, physical sabotage. This section offers a brief empirical sketch of these developments in both countries, not as isolated episodes, but as indicators of how ambiguous infrastructure disruptions have become a preferred tool of grey zone competition, and how ill-equipped existing CIP frameworks remain to deter or anticipate them.

Between 2018 and 2023, Taiwan experienced more than 20 incidents of damage to undersea cables connecting it with the Matsu Islands. While many cases were attributed to fishing trawlers or anchors, suspicion has increasingly centred on deliberate interference by Chinese-flagged vessels. A particularly concerning incident occurred on 3 January 2025, when an undersea cable off Taiwan's northeast coast was severed. Taiwanese authorities suspect sabotage by the *Shunxin 39*, a Cameroon-flagged, Chinese-crewed cargo ship, which was observed near the site of the damage. Rough seas prevented authorities from boarding the vessel, and it continued its journey toward South Korea. Though attribution remains elusive, the case drew sharp comparisons to similar maritime disruptions in Europe and was widely interpreted as a form of deniable state harassment (Davidson 2025). In response, Taiwan has adopted a multi-pronged strategy: enhancing redundancy through low-Earth orbit satellite agreements (Wang 2025), expanding microwave-based contingency systems, and conducting regular whole-of-society tabletop exercises. These simulations involve the military, civil protection services, energy operators, and diplomatic bodies, aiming to strengthen resilience across societal sectors. Yet even in these comprehensive efforts, the emphasis remains on response capacity and continuity of service, rather than on deterrence or predictive modelling of adversarial behaviour.

Norway's experience mirrors these challenges. In 2021, a deep-sea cable used for scientific and military communication in Vesterålen went missing. Months later, the Svalbard Undersea Cable System, a dual-cable link between Svalbard and mainland Norway, suffered a critical failure as one of the cables was found to be physically severed in a steep underwater trench. Automatic Identification System data later showed Russian fishing vessels transiting the area during the window of disruption, but conclusive attribution remained out of reach (Nilsen 2022). Whereas it was impossible to confirm who caused the damage, in both cases it was nevertheless clear that the damage and/or removal of the cable was a human-induced event, rather than due to natural circumstances (Kantchev 2024). Furthermore, the Svalbard incident mirrors concerns raised by the sabotage of the Nord Stream 1 and 2 pipelines in the Baltic Sea in September 2022. Both events underscore the potential risks to undersea infrastructure in sensitive geopolitical areas (Humpert 2022).

The events in the Arctic are part of a broader pattern across the Baltic Sea region. Between late 2023 and early 2025, multiple submarine communication cables and

energy lines, including *EstLink 2*, the *C-Lion 1* cable, and cross-border fibre-optics, were damaged under suspicious circumstances. While the Kremlin denied any Russian involvement, the "accidents" raised concerns about potential Russian hybrid warfare targeting global communications infrastructure (Lyons 2024). Vessels of Chinese, Russian, and shadow fleet origin were repeatedly implicated. Only weeks after EU investigators probed a Chinese-flagged vessel suspected of sabotaging undersea cables in the Baltic Sea (Durden 2024), a land-based fibre-optic cable running across the border between Sweden and Finland was damaged in two separate locations in southern Finland (Giordano and Jochecová 2024). In one case, Finnish forces boarded the *Eagle S.*, a tanker suspected of severing a key cable between Finland and Estonia (PAP, 2024). A broken anchor, advanced surveillance equipment, and links to Russian port calls raised strong suspicion of state-enabled sabotage (Wiese Bockmann 2024).

Although US and European security officials have ruled that three recent incidents of cable damage in the Baltic Sea were the result of "unfortunate accidents" rather than sabotage, including the severing of the Finland–Estonia cable by the Eagle S. tanker (December 2024), the rupture of a gas pipeline in the Gulf of Finland by the Newnew Polar Bear container ship (October 2023), and the cutting of two Swedish cables by the Chinese vessel *Yi Peng 3* (November 2024), questions remain. Official statements attributed the disruptions to inexperienced crews and poorly maintained vessels (Miller et al. 2025). Yet investigative reporting by Newsweek unearthed Chinese patent filings from 2009 to 2020 in which engineers at Lishui University developed anchor designs specifically optimised for the rapid and inexpensive cutting of submarine cables, nominally for "emergency situations" (Tatlow 2025). These technical innovations lend further plausibility to claims that such vessels may be engaging in deliberate infrastructure sabotage under the guise of navigational error.

In response, NATO launched Operation Baltic Sentry, deploying drones, frigates, and maritime patrol aircraft to protect critical undersea infrastructure (Minasazova 2025). Beyond this collective response, individual states have also taken unilateral military measures that, while potentially effective in the short term, raise concerns about long-term sustainability and long-term viability of this reactive posture. For example, Norway has deployed naval patrols to safeguard its assets, and Estonia is preparing legislation that would empower its Defence Forces to use military force against commercial vessels suspected of attempting to damage undersea cables or other critical infrastructure (Litnarovych 2025).

### 2.1 Conceptual Drift and the Limits of Infrastructure Readiness

As the preceding overview has demonstrated, Norway and Taiwan offer analytically rich comparisons. Both are small but technologically advanced democracies, possessing vital maritime infrastructure and deep integration with global systems. Each sits on the edge of a geopolitical fault line: Taiwan in the shadow of the People's Republic of China, Norway along NATO's northern frontier with Russia. Both have also experienced undersea cable disruptions under suspicious circumstances, widely interpreted as grey zone activity. Yet despite their advanced capabilities and high threat awareness, these states remain better prepared for accidents or overt coercion

than for adaptive, actor-driven threats by state-backed proxies. In the increasingly abstract lexicon of hybrid warfare, perhaps no threat is more operationally elusive than that posed by state-enabled terrorist proxies, actors who blend ideological conviction with plausible deniability and physical sabotage. While both Norway and Taiwan have developed comprehensive national frameworks for critical infrastructure protection, these systems share a common blind spot: the persistent assumption that threats are either natural, accidental, or openly attributable. Their models remain structurally under-equipped to anticipate or counter threats that are strategic, intelligent, and deniable.

### 2.2 Norway: Resilience Without Anticipation

Norway's CIP framework is rooted in an all-hazards approach, integrating responses to natural disasters, cyber threats, and terrorism into a unified system. The 2011 Oslo bombing and Utøya attack prompted major reforms, exposing the need to bolster emergency preparedness across sectors. Central to Norway's approach is the DECRIS methodology (Decision Support for Critical Infrastructure Security), developed by SINTEF as a cross-sectoral, all-hazard risk assessment tool, DECRIS underpins the National Risk Analysis coordinated by the Directorate for Civil Protection. The rationale behind DECRIS posits that most existing risk assessment methodologies focus on individual sectors (e.g., energy, transport, water) without fully accounting for interdependencies, which leads to a fragmented understanding of risk, where failures in one sector can cascade into others, causing greater systemic failures than anticipated. DECRIS was designed to address this limitation by integrating sector-specific assessments into a unified model. It follows a four-step process: establishing taxonomies and risk dimensions, conducting a generic screening of threats, prioritising events based on interdependency and societal disruption, and concluding with detailed risk analysis and mitigation planning. While highly effective in mapping structural vulnerabilities and cascading failures, DECRIS is not designed to model adversarial behaviour.

DECRIS is highly useful for understanding infrastructure vulnerabilities, cascading failures, and interdependencies, which are crucial for assessing potential terrorist attack impacts. However, there are also limitations that would need to be addressed for it to be fully effective in this domain. Firstly, DECRIS does not account for threat actor modelling, that is adversary behaviour, intent, or adaptation, which are key components of terrorist threat analysis. Terrorist groups are adaptive and dynamic, whereas DECRIS is designed for static, structural risk assessments. Consequently, DECRIS would need to be supplemented with intelligence-driven threat analysis, such as the CARVER (Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability) matrix, which specifically evaluates adversarial targeting. Secondly, while DECRIS assesses vulnerabilities and consequences, it does not offer direct assessment of attack feasibility which would evaluate how easily a terrorist group could exploit a given weakness. Unlike military or security-driven risk models, DECRIS lacks attacker-perspective analysis. To address this weakness, DECRIS would have to integrate Red Teaming approaches, where security experts simulate terrorist decision-making to determine attack feasibility. Last but not least, one of

DECRIS's acknowledged weaknesses is that it does not provide a standardized way to compare different types of risks and therefore it lacks direct comparability of consequences. A terrorist attack on a transportation hub and a cyberattack on financial networks may both be high impact but qualitatively different, making prioritization difficult. Risk matrices that incorporate threat likelihood and intent would have to complement DECRIS in this regard. Given these limitations, it should be concluded that DECRIS can be used for counter-terrorism CI protection analysis but only as part of a larger analytical framework, but it remains insufficient if used alone, because it lacks a threat actor model, does not consider attack feasibility, and does not incorporate adversarial intent.

Another reason Norway's CIP architecture struggles to address proxy-driven sabotage is its deep institutional inheritance from the welfare-state tradition. As Godzimirski (2022) notes, Norway's infrastructure planning has historically been more concerned with ensuring equal access to services across dispersed geographies than with repelling adversarial threats. Even as the geopolitical climate has shifted—particularly after Russia's 2014 aggression and the 2022 Ukraine invasion—the emphasis remains on resilience and risk mitigation, rather than anticipation or deterrence (for more on anticipation see Staupe and Bartoszewicz 2025). The conceptual legacy here matters: systems built to manage floods, blackouts, and lone-wolf terrorism may prove structurally ill-suited to confront intelligent, actor-driven threats that operate via indirection and denial.

### 2.3 Taiwan: Tactical Adaptation in a Strategic Vacuum

In Taiwan's National Infrastructure Protection Plan (2010), critical infrastructure is defined as the physical and virtual assets, production systems, and networks that, if severely damaged by significant human-made aggression or catastrophic natural disasters, become unusable or incapable of delivering essential services. Such impairment can have far-reaching consequences, including disruption of government operations, casualties, property damage, economic decline, ecological alterations, and additional risks that may ultimately threaten national security or vital interests. The criteria for identifying critical infrastructure in Taiwan are based on four key impacts: effects on the population, economic repercussions, the interdependencies and consequent fallout, and public confidence in both governmental institutions and critical infrastructure operators.

Accordingly, Taiwan's critical infrastructure encompasses eight principal sectors: energy, water resources, information and communication technology, banking and finance, central government and major municipalities, emergency response and hospitals, transportation, and high-tech industrial parks. These sectors are indispensable for maintaining the nation's stability and resilience when confronted with potential threats. Notably, the list of critical infrastructure items is kept strictly confidential; even law enforcement agencies are privy only to the subset of objects under their respective ministerial jurisdictions, while comprehensive insight is reserved solely for the National Security Bureau.

In Taiwan, countermeasures against potential terrorist proxies are not pursued as a distinct policy agenda but are instead integrated into the broader framework of

managing geopolitical tensions with China. The national strategy emphasises legal frameworks, cybersecurity measures, and civil defence initiatives as the main pillars for protecting critical infrastructure. Notably, in September 2024 the government announced a series of measures aimed at enhancing the resilience of vital sectors against a range of threats from hostile actors. A particular focus has been placed on the legal protection of undersea cables, which are crucial conduits for Taiwan's connectivity, with efforts underway to reinforce these protections both domestically and at the international level.

However, the majority of these initiatives have been concrete, tactical measures rather than strategic recalibrations. For instance, Taiwan is actively enhancing its communication resilience by securing access to low-earth-orbit satellite internet services. During a meeting organised by the Office of Legislator Kuan-Ting Chen, which I attended during my Taiwan Fellowship, discussions centred on how low-orbit satellite services can bolster national security awareness, how UAVs and countermeasure systems might augment deterrence capabilities, and how enhanced international cooperation in the low-orbit satellite and drone sectors can help safeguard communication channels in the event of cyberattacks or physical disruptions.[2] In short, while these initiatives aim to ensure the continuity of critical infrastructure amid a complex threat environment, they do not embody a comprehensive strategic framework that fully addresses the fundamentally distinct implications of these emerging threats for the entire system of infrastructure protection. Taiwan's architecture, like Norway's, prioritises functionality and resilience over anticipatory modelling. The challenge is not a lack of capability, but a failure to fully theorise and institutionalise how intelligent, deniable threats operate, and how CI systems might be targeted for symbolic, coercive, or cascading effects.

### 2.4 Strategic Misrecognition and the Rise of Proxy Terrorism

Attacks on undersea cables have become a familiar, if not altogether predictable, feature of grey zone tactics. Yet their recurrence, and the reactive patterns that follow, suggest a deeper strategic drift. When sabotage becomes routine, its shock value fades, prompting adversaries to seek more novel, harder to foresee and counter, methods of disruption. During my fieldwork in Taiwan, Shyh-Yuan Maa, Taiwan's Deputy Political Minister of the Interior, offered one of the few forward-looking assessments to depart from conventional assumptions. Among eight hypothetical conflict scenarios he outlined, one involved the use of terrorism and hostage-taking as tools of coercion by the PRC. His scenario stood out precisely because it challenged the prevailing belief that threats to critical infrastructure will remain limited to non-escalatory or deniable forms of grey zone activity.

Existing scholarship on critical infrastructure protection is replete with broad classifications that reduce terrorism to one generic threat among many others, as shown in Table 2, and thus expected to be mitigated by the very same set of measures as those directed against avalanches or operational malfunctions.

[2] Transparent Deterrence - Defense Applications of Low Orbit Satellite and UAV Technology Seminar, 09:00 to 12:00 on March 4, 2025, Conference Room 302, Red Building, Legislative Yuan.

**Table 2** Overview of Non-Terrorism threat vectors facing critical infrastructure

| Threat Category | Authors |
|---|---|
| Natural and Environmental Threats (e.g. earthquakes, floods, extreme weather, solar flares, and cascading failures triggered by natural events) | Stergiopoulos et al. (n.d.); US Department of Transportation (2006); Lopez et al. (2012); Giannopoulos et al. (2012); Brem (2015); Petrakos and Kotzanikolaou (2019); Ouyang et al. (2019); Osei-Kyei et al. (2021); Ciupercă and Vevera (2019); Pursiainen (2018); Böröcz (2021); Pătrașcu (2022); Ruzhin and Mitrevska (2024) |
| Technological, Accidental, and Operational Failures (including system malfunctions, industrial accidents, unintentional hazardous events and disruptions linked to complexity/interdependencies) | Stergiopoulos et al. (n.d.); Lopez et al. (2012); Brem (2015); Gromek (2021); Ciupercă and Vevera (2019); Denysov et al. (2021) |
| Cyber Threats and Digital Intrusions (attacks on digital systems, SCADA, and communication networks; the use of cyber means to cause cascading physical disruption) | Williamitis (2000); Tomko (2002); Jenelius et al. (2010); Lopez et al. (2012); Zhang et al. (2015); Cazorla et al. (2015); White (2019); Petrakos and Kotzanikolaou (2019); Ouyang et al. (2019); Böröcz 2021 |
| Organisational and Policy/Management Failures (poor governance, inadequate policies, weak interagency coordination and fragmented control that exacerbate vulnerabilities) | Osei-Kyei et al. (2021); De Bruijne and Eeten (2007); Pursiainen (2018) |
| Cascading and Interdependency Failures | Stergiopoulos et al. (n.d.); Pikus (2003); Giannopoulos et al. (2012); Brem (2015); Osei-Kyei et al. (2021) |

Such approaches, however, have grown formulaic, failing to capture the adaptability and strategic innovation of terrorist actors. As established tactics lose their psychological or political impact, groups are compelled to evolve and experiment. In today's geopolitical context, this innovation increasingly takes place within a hybrid ecosystem, where non-state actors may be tacitly supported or strategically repurposed by adversarial states (Tomko 2002; White 2019). This blurring of lines between independent terrorism and proxy warfare is not speculative but well entrenched in real-world patterns: Iran's long-standing support for Hezbollah; Russia's operational links to cybercriminal and paramilitary groups; North Korea's use of cyber operations to fund state activities. These cases illustrate how terrorism can function not only as an ideological campaign but also as a strategic instrument employed at arm's length. States can and do exploit terrorist organisations as tools of proxy warfare. When a terrorist group conducts an operation that aligns with a foreign government's

strategic objectives, that state may have, implicitly or explicitly, supported, facilitated, or turned a blind eye to its activities.

The emergence of hybrid warfare as a dominant strategic framework has exacerbated this trend since the ambiguity intrinsic to hybrid conflict makes terrorism especially useful to states seeking plausible deniability. On one end of the spectrum, some states adopt terrorist tactics directly; on the other, terrorist organisations receive covert support while pursuing agendas that align with state objectives. In both instances, attribution is complicated, and response options are constrained. White (2019) highlights how states may subcontract or enable terrorist actors to engage in economic sabotage or infrastructure disruption, an increasingly relevant tactic given the difficulty of tracing responsibility. Denysov et al. (2021) further underscore how covert operations, subversion, and ambiguous affiliations constitute key components of hybrid strategies, with terrorist attacks functioning as tactical proxies to degrade resilience and generate fear. The hybridisation of terrorism thus represents not merely a convergence of methods but a structural shift. Illustrative examples further reinforce this claim. The NotPetya malware, attributed to Russian actors, straddles the boundary between cyberterrorism and economic warfare. Al-Qaeda and ISIS attacks on oil infrastructure were explicitly designed to weaken state economies while generating symbolic power. The 2016 Bangladesh Bank cyber heist, widely attributed to North Korea, exemplifies how financial institutions can be targeted with techniques that combine terrorism, espionage, and state sponsorship.

Zhang et al. (2015) argue that economic sabotage can be pursued by both state-sponsored actors and autonomous terrorist groups, with differences hinging on intent, scalability, and strategic context. When plausible deniability is required, using proxies to target infrastructure becomes not only attractive but efficient. The strategic value lies not merely in disruption but in creating cascading effects that radiate far beyond the original point of attack. This is especially true in a world of deep interdependencies. Infrastructural systems, whether in finance, transport, energy, or communications, cross borders and bind disparate sectors. Terrorist actors, especially those operating with state encouragement, can target a vulnerable node in a lightly defended country, with the aim of causing ripple effects in a more secure or geopolitically significant adversary that would have been more difficult to attack directly.

In this setting, terrorism ceases to be a blunt instrument of fear and becomes a targeted tool of disruption, integrated into broader campaigns. The methods range from physical attacks on power grids or ports, to ransomware operations that paralyse industries, to coordinated campaigns aimed at exploiting interdependencies for maximal psychological and strategic effect. What my research highlights is a crucial blind spot: despite growing awareness of grey zone conflict and hybrid tactics, existing CIP frameworks are still calibrated for static threat environments. They remain focused on technical vulnerabilities and functional resilience, without fully incorporating the intent and adaptability of threat actors. As recent submarine cable incidents illustrate, the next wave of disruptions may not stem from spontaneous failures or predictable sabotage, but from proxies operating at the strategic threshold between terrorism and statecraft. This demands not only new analytical models but a reconceptualisation of terrorism itself, not as a generic risk category, but as an evolving vector of state-

enabled infrastructure warfare. If cable-cutting was only the test, the next phase may well come through the cracks we have not yet learned to see.

## 3 From Conceptual Drift To Strategic Foresight: Rethinking Future Security Governance

Infrastructure has become the preferred domain of indirect conflict, not through overt military engagement, but via deniable sabotage, strategic ambiguity, and cascading disruption. From submarine cables to transportation, to logistics systems, today's critical infrastructure is not only indispensable to societal functioning but increasingly vulnerable to strategic manipulation. Yet most national preparedness strategies remain calibrated for malfunction, not malevolence and are designed to absorb disruption, not to anticipate it. As I have shown, Norway and Taiwan exemplify this tension: they possess resilient systems, but not necessarily ones that are attuned to the logic of intelligent adversaries. To address this gap, I what follows, I will outline what a shift from passive resilience to strategic foresight would require.[3]

Much of the contemporary CIP landscape is defined by resilience-based thinking. Risk assessments are built on probabilistic models, scenario catalogues, and structural vulnerability matrices. These tools are effective for managing known hazards and complex interdependencies. But they falter in the face of adaptive threats, particularly when those threats emerge from adversaries who observe, evolve, and exploit. In such environment, as Jenelius et al. (2010) argue, imperfect attacker perception plays a key role in shaping terrorist decision-making. While non-state actors often operate with limited intelligence, state-backed proxies benefit from superior surveillance and targeting capabilities. This asymmetry renders static threat models dangerously inadequate. Zhang et al. (2015) demonstrate that terrorists are more likely to succeed when protection strategies are open and predictable. Secrecy, by contrast, introduces friction, thereby forcing attackers to assume greater risk. Yet, many national systems still rely on transparent risk taxonomies and publicly documented contingency plans, inadvertently aiding adversarial planning.

Whereas conventional tools such as fault tree analysis or single-point failure models are useful for engineering failures, they cannot capture the strategic logic of an intelligent antagonist. As Brown et al. (2014) contend, as opposed to game-theoretic models that simulate the targeting behaviour of terrorists, these tools fail to simulate attacker behaviour, motivation, or resource constraints. They do not anticipate how or why a proxy actor might strike. In this sense, CIP frameworks remain largely static resulting from risk assessment methodologies ill-suited to address the fluid, adaptive

[3] It should be noted that while this paper approaches hybrid threats through the lens of anticipatory governance, related insights can be found in two adjacent traditions: Strategic-studies analyses of hybrid warfare, particularly those tracing the logic of plausible deniability and state-enabled coercion (Gunneriuson 2019; Poznansky 2022), help illuminate the political intentionality behind such acts. In parallel, research on physical protection systems (Garcia 2007; Stewart 2010; McIlhatton et al. 2020) offers a technical vocabulary for understanding how infrastructures absorb or resist deliberate interference. Together, these perspectives enrich the conceptual frame proposed here, bridging strategic intent and systemic vulnerability in the modelling of hybrid terrorism.

strategies (Merabti et al. 2011; Ani et al. 2019) and thus, irrevocably reactive: they respond to failure, but do not model malicious intent.

To move from conceptual drift of a generic hybrid threat to strategic foresight and redirecting attention away from static threat probability models, new planning methodologies are needed; ones that centre attacker logic rather than defender vulnerability. One promising avenue is the adoption of game-theoretic and simulation-based models (Taquechel and Lewis 2017) such as Defender–Attacker–Defender frameworks and the CARVER matrix, which allow security planners to rank assets based on adversarial criticality, accessibility, recognisability, and effect through both overt and covert strategies that use the information asymmetry to their benefit and hence enable defenders to leverage their limited resources more effectively if they obscure the true state of protection. These tools prioritise attacker perspectives, asking not only what is vulnerable, but what is attractive. Complementing this, red-teaming exercises, in which planners simulate terrorist behaviour to probe system weaknesses—remain underutilised in most national CIP strategies. As Ouyang et al. (2019) demonstrate, worst-case adversarial simulations often expose vulnerabilities that would otherwise be overlooked by technical audits alone. In an age of hybrid warfare, where proxies may exploit symbolic targets or trigger cascading failures, such anticipatory exercises become essential.

This observation links directly to the concept of weaponised failure. Infrastructure is no longer just a backbone of economic life; it is a psychological and political lever. Attacks on critical nodes are designed not simply to disrupt, but to destabilise, to erode confidence, and to signal coercive capability. The goal may not be prolonged blackout, but a moment of strategic ambiguity, enough to induce overreaction, provoke fear, or divert national focus. In such a context, even a failed attack may be deemed a success. Existing frameworks, focused on continuity and resilience, are ill-equipped to process failure as a weaponised act.

Hence, institutional responses must evolve accordingly. As Pikus (2003) warned, policy momentum means little without operational translation. Although hybrid threats are now widely acknowledged in NATO, EU, and national strategies, they remain poorly operationalised lacking the actor-specific models and adaptive doctrines needed to convert awareness into deterrence. Böröcz (2021) and Denysov et al. (2021) stress that the hybrid threat environment demands integrated, dynamic governance models, rather than siloed, checklist-based planning.

This includes confronting the institutional tendency to focus inward: defending infrastructure as a set of domestic systems, rather than seeing it as part of an external battlespace, subject to adversarial manipulation. As Ruzhin and Mitrevska (2024) argue, critical infrastructure today is a strategic stake, a frontline in the contest for influence and coercion. Yet most protection strategies treat it as a technical asset rather than a contested domain. To this picture, De Bruijne and van Eeten (2007) add a final institutional insight: the danger of fragmented authority. Many CIP systems still operate with blurred public-private boundaries and unclear mandates. Without better horizontal coordination, national systems will struggle to mount unified, adaptive responses to transnational or state-enabled threats. Strategic foresight requires not only modelling adversaries but ensuring that institutional structures are agile enough to act on those models. Ultimately, what emerges from this analysis is not

a call to abandon resilience, but to expand it into a more adversary-aware posture. Infrastructure systems must not only survive disruption, but they must also be protected in anticipation of it, with a mindset that treats proxies, grey zone actors, and deniable threats as central variables in the calculus of national security.

## 4 Conclusion: Beyond the Perpetual Crisis

This paper began with a paradox: the rise of hybrid warfare as an all-encompassing threat frame has produced a condition of perpetual alertness, yet without delivering operational clarity. The crux of the argument renders this problem not just a policy lag, but a conceptual one. As the lexicon of crisis has expanded, and threat categories have collapsed, terrorism, sabotage, cyber operations, and disinformation are now grouped under the hybrid umbrella, blurring their analytical boundaries. In the process, institutions have become better at preparing for cascading disruption without asking who might be causing it, to what end, and with what strategic logic. They plan for effects, not actors; for resilience, not intent.

The cases of Norway and Taiwan, two high-capacity states with robust infrastructure governance, illustrate this dynamic with striking clarity. Both countries have experienced direct sabotage of critical infrastructure, events widely suspected to be state enabled. Yet, both still rely on preparedness regimes originally designed for accidents, natural disasters, or clearly attributable attacks. The result is a form of strategic misrecognition stemming from being blindsided by the logic of proxy violence. Infrastructure is treated as a passive technical domain, vulnerable to disruption but not to orchestration. When planners see disruption, but not the actor logic behind it, the systems are built to absorb shocks, but not to anticipate intelligent, adaptive, and deniable threats planned with political intent. The idea that adversaries might target weak points in order to create downstream political or psychological effects is not systematically incorporated into preparedness planning.

Recognising infrastructure as a domain of indirect confrontation is a necessary conceptual shift and the first step toward building a model of critical infrastructure protection that anticipates, not merely absorbs, hybrid threats. Cables, ports, and energy systems are no longer mere utilities; they are increasingly symbolic, political, and strategic targets selected with the adversarial logic that now shapes the whole system. Their disruption is not just collateral; it is often the objective. Proxy-enabled sabotage, especially when wrapped in plausible deniability, exploits precisely the space where ambiguity meets inertia.

To address this, threat categories must be re-specified. Terrorism, particularly in its state-enabled or proxy form, cannot remain a residual concern in national security planning. It must be operationalised as a distinct strategic vector used as a tool of indirect confrontation. This entails more than naming the threat. It requires institutionalising red-teaming, attacker modelling, and adversary-specific scenario planning, not as speculative tabletop exercises, but as integrated planning tools. Similarly, infrastructure must be seen not only as a technical system to be protected, but as a domain of symbolic and political contestation.

Vital systems security, as developed by Lakoff and Collier, provides a useful foundation, but it must evolve beyond managing interdependencies and account for adversarial intentionality. Governance must shift from the logic of mitigation to one of active anticipation. To reiterate: this is not a question of resources; the issue is conceptual. As my analysis shows, Norway and Taiwan have advanced capabilities, experienced agencies, and strong civil protection cultures but as long as proxies remain embedded within a generic and ever-expanding hybrid discourse, they will evade the specific countermeasures they require.

Proxy threats are not simply an extension of grey zone tactics; they are a distinct form of strategic violence: deniable, decentralised, and highly adaptable. Addressing them demands more than resilient systems. It demands foresight-driven governance that can model attacker logic and plan against it. The security culture that currently prioritises absorption over deterrence must expand to include strategic disruption as a form of pre-emption enabled by a disaggregation of threat types and a move toward operational clarity: modelling not just what might fail, but who might want it to, and how.

This brings us back to the problem of crisis typology drift. Under the expansive umbrella of hybrid warfare, distinct threats lose their analytical contours. Disinformation, sabotage, terrorism, and economic coercion become interchangeable, and institutional responses lose focus. As threat types blur, operational planning remains generic. In order to protect infrastructure in this evolving landscape, we must move beyond the comfort of static preparedness toward anticipatory governance. Infrastructure must be understood not just as a system to be maintained, but as a battlefield to be defended. This requires a reconceptualisation of threat and the adoption of tools that reflect adversarial agency: red-teaming, game theory, strategic concealment, and attacker modelling.

While the integrated approach used in this work successfully bridges empirical observation and conceptual analysis, it remains constrained by the complexities of modelling the nuances of adversarial behaviour, which highlights paths for future research (such as incorporating mixed-method approaches or expanding the comparative framework) to deepen the understanding of hybrid threat dynamics. Limitations notwithstanding, the analysis presented in this study carries significant practical implications for those responsible for national security and critical infrastructure protection. My findings reveal that traditional resilience-based frameworks, which focus primarily on absorbing disruptions after they occur, fall short in addressing the dynamic, adaptive nature of hybrid threats and state-enabled proxy terrorism. As this paper has argued, hybrid threat inflation fosters a perpetual crisis imaginary without yielding actionable preparedness. To reverse this drift, we must disaggregate hybrid threats into distinct operational categories, invest in actor-specific deterrence models, and treat infrastructure not merely as vulnerable but as politically contested. Otherwise, we risk preparing for yesterday's disruptions while remaining blind to tomorrow's deniable threats.

In the end, the choice posed by this special issue is apt: do we live in a world of perpetual crisis, or of continual risk? If the former, we must escape the recursive loop of hybrid discourse and return to strategic specificity. If the latter, we must refine our

anticipatory frameworks to reflect the agents who manufacture that risk. Only then can we shift from ambient readiness to genuine security.

**Acknowledgements** This research was supported by the Taiwan Fellowship 2025 Program. The author gratefully acknowledges the Ministry of Foreign Affairs of the Republic of China (Taiwan) for its generous support. The author also wishes to extend sincere thanks to the Institute for National Defence and Security Research (INDSR) in Taipei for its collegial hospitality and for providing an intellectually stimulating environment throughout the course of the research. The views expressed in this article are solely those of the author and do not necessarily reflect the positions of the Taiwan Fellowship Program or INDSR.

**Author Contributions** The author confirms being the sole contributor to this work and is responsible for the conception, design, data collection, analysis, interpretation, and writing of the manuscript.

**Funding** Open access funding provided by UiT The Arctic University of Norway (incl University Hospital of North Norway)

**Data Availability** No datasets were generated or analysed during the current study.

## Declarations

**Conflict of interest** The authors declare no competing interests.



## References

Ani UD, McK Watson JD, Nurse JR, Cook A, Maples C (2019) A review of critical infrastructure protection approaches: Improving security through responsiveness to the dynamic modelling landscape. Living Internet Things (IoT 2019):6

Auerswald P, Branscomb LM, La Porte TM, Michel-Kerjan E, Michel-Kerjan ERM (2005) The challenge of protecting critical infrastructure. Issues Sci Technol 22(1):77–83

Bartoszewicz MG (2016) Festung europa: securitization of migration and radicalization of European societies. Acta Univ Carol Stud Territ 16(2):11–37

Bobbitt P (2008) Terror and consent: the wars for the twenty-first century. Allen Lane, London

Böröcz M (2021) Critical infrastructure protection policy in the EU. Strateg Impact 3(80):46–61

Brem S (2015) Critical infrastructure protection from a national perspective. Eur J Risk Regul 6(2):191-199

Brown GG, Carlyle WM, Salmeron J, Wood K (2005) Analyzing the vulnerability of critical infrastructure to attack and planning defenses. In: Emerging Theory, Methods Appl pp 102–123. INFORMS

Cazorla L, Alcaraz C, Lopez J (2015) Awareness and reaction strategies for critical infrastructure protection. Comput Electr Eng 47:299–317

Ciupercă EM, Vevera VA (2019) Cultural lens of critical infrastructure protection. In: Redefining Commun Intercult Context, pp 75–80

Collier SJ, Lakoff A (2015) Vital systems security: reflexive biopolitics and the government of emergency. Theory Cult Soc 32(2):19–51

Davidson H (2025) Taiwan investigating Chinese vessel over damage to undersea cable. The Guardian, 7 January 2025. https://www.theguardian.com/world/2025/feb/25/taiwan-detains-chinese-crewed-cargo-ship-after-undersea-cable-damaged. Accessed 19 February 2025

De Bruijne M, Van Eeten M (2007) Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment. J Conting Crisis Manage 15(1):18–29

Denysov AI, Bershov HY, Krykun VV, Zhydovtseva O (2021) Protection of critical infrastructure facilities as a component of the national security. Cuest Polít. https://doi.org/10.46398/cuestpol.3971.48

Durden T (2024) Danish navy hunts down Chinese ship suspected of 'sabotaging' Baltic Sea cables. ZeroHedge, 21 November 2024. https://www.zerohedge.com/geopolitical/baltic-sea-fiber-cable-disruption-remains-murky-danish-coast-guard-shadows-chinese. Accessed 5 March 2025

European Commission (2024) Hybrid threats. Directorate-General for Defence Industry and Space. https://defence-industry-space.ec.europa.eu/eu-defence-industry/hybrid-threats_en. Accessed 15 March 2025

Gaiser L (2019) NATO-EU collaboration on hybrid threats: cooperation out of necessity with potential consequences on international legal framework. Natl Secur Future 20(1–2):13–24

Garcia ML (2007) Design and evaluation of physical protection systems. Butterworth-Heinemann, Burlington, MA

Giannopoulos G, Filippini R, Schimmer M (2012) Risk assessment methodologies fo critical infrastructure protection. Part I: a state of the art. JRC Tech Notes 1(1):1-53

Giordano E, Jochecová K (2024) Finnish telecom company hit by cable outage. Politico, 3 December 2024. https://www.politico.eu/article/finland-global-connect-company-hit-by-cable-outage. Accessed 8 April 2025

Godzimirski JM (2022) Protection of critical infrastructure in Norway – factors, actors and systems. Secur Def Q 39(3):45–62

Gromek P (2021) Strategic training and exercises for critical infrastructure protection and resilience: a transition from lessons learned to effective curricula. Int J Disaster Risk Reduct 65:102647

Gunneriuson H (2019) Hybrid warfare and deniability as understood by the military. Pol Political Sci Yearb 48(2):267–288

Humpert M (2024) Nord Stream pipeline sabotage mirrors Svalbard cable incident. High North News, 29 September 2022. https://www.highnorthnews.com/en/nord-stream-pipeline-sabotage-mirrors-svalbard-cable-incident. Accessed 17 Feb 2025

Jenelius E, Westin J, Holmgren ÅJ (2010) Critical infrastructure protection under imperfect attacker perception. Int J Crit Infrastruct Prot 3(1):16–26

Kantchev G (2024) Russia and China defy the West deep in the Arctic. The Wall Street J 28 September 2024. https://www.wsj.com/world/svalbard-russia-china-arctic-trade-e6187bd8. Accessed 12 April 2025

Koski C (2011) Committed to protection? Partnerships in critical infrastructure protection. J Homeland Secur Emerg Manag 8(1):0000102202154773551860

Lakoff A, Collier SJ (2010) Infrastructure and event: the political technology of preparedness. In: Braun B, Whatmore S (eds) Political matter: technoscience, democracy, and public life, pp 243–266

Lewis AM, Ward D, Cyra L, Kourti N (2013) European reference network for critical infrastructure protection. Int J Crit Infrastruct Prot 6(1):51–60

Lindström M, Olsson S (2009) The European programme for critical infrastructure protection. In: Crisis Manage European Union: Cooper Face of Emerg pp 37–59

Litnarovych V (2025) Estonia mulls law allowing military to sink suspicious ships threatening undersea infrastructure. United24 Media, 8 April 2025. https://united24media.com/latest-news/estonia-mulls-law-allowing-military-to-sink-suspicious-ships-threatening-undersea-infrastructure-7416. Accessed 20 April 2025

Lopez J, Setola R, Wolthusen SD (2012) Overview of critical information infrastructure protection. In: Critical Infrast Prot Inf Infrast Models, Analysis, and Defense, pp 1–14

Lyons E (2024) Undersea cables cut or damaged, leading European nations to investigate possible sabotage. CBS News, 20 November 2024. https://www.cbsnews.com/news/undersea-cables-cut-europe-finland-germany-hint-russia-sabotage. Accessed 21 March 2025

McIlhatton D, Berry J, Chapman D, Christensen PH, Cuddihy J, Monaghan R, Range D (2020) Protecting crowded places from terrorism: an analysis of the current considerations and barriers inhibiting the adoption of counterterrorism protective security measures. Stud Confl Terrorism 43(9):753–774

Merabti M, Kennedy M, Hurst W (2011) Critical infrastructure protection: a 21st century challenge. In: 2011 Int Conf Commun Inf Technol (ICCIT), pp 1–6. IEEE

Miller G, Dixon R, Stanley-Becker I (2025) Accidents, not Russian sabotage, behind undersea cable damage, officials say. The Washington Post, 19 January 2025. https://www.washingtonpost.com/world/2025/01/19/russia-baltic-undersea-cables-accidents-sabotage. Accessed 9 March 2025
Minasazova L (2025) NATO's Baltic patrol operation to last 90 days, Polish PM says. Report News Agency, 15 January 2025. https://report.az/en/other-countries/nato-s-baltic-patrol-operation-to-last-90-days-polish-pm-says. Accessed 7 February 2025
Moteff JD (2007) Risk management and critical infrastructure protection: assessing, integrating, and managing threats, vulnerabilities and consequences. Congressional Research Service, The Library of Congress, Washington, DC
Nilsen T (2022) Disruption at one of two undersea cables to Svalbard. The Barents Observer, 9 January 2022. https://www.thebarentsobserver.com/arctic/disruption-at-one-of-two-undersea-cables-to-svalbard/119477. Accessed 3 April 2025
Osei-Kyei R, Tam V, Ma M, Mashiri F (2021) Critical review of the threats affecting the building of critical infrastructure resilience. Int J Disaster Risk Reduct 60:102316
Ouyang M, Liu C, Xu M (2019) Value of resilience-based solutions on critical infrastructure protection: comparing with robustness-based solutions. Reliab Eng Syst saf 190:106506
Pătrașcu P (2022) National security strategies and critical infrastructure: an analysis of the European Union member states. Rom Mil Think 3:10–29
Petrakos N, Kotzanikolaou P (2019) Methodologies and strategies for critical infrastructure protection. In: Critical infrastructure security and resilience: theories, methods, tools and technologies, pp 17–33
Pikus IM (2003) Critical infrastructure protection: are we there yet? J Infrastruct Syst 9(1):1–5
Poznansky M (2022) Revisiting plausible deniability. J Strateg Stud 45(4):511–533
Prasowa PA (2024) Premier Estonii: Finlandii za szybkie działanie w sprawie EstLink 2 należy się uznanie. Polska Agencja Prasowa, 26 December 2024. https://www.pap.pl/aktualnosci/premier-estonii-finlandii-za-szybkie-dzialanie-w-sprawie-estlink-2-nalezy-sie-uznanie. Accessed 1 March 2025
Pursiainen C (2018) Critical infrastructure resilience: a nordic model in the making?. Int J Disaster Risk Reduct 27:632–641
Quigley K (2013) Man plans, god laughs: Canada's National strategy for protecting critical infrastructure. Can Public Adm 56(1):142–164
Ruzhin N, Mitrevska M (2024) Protection of critical infrastructure – a strategic stake of the 21st century. Contemp Macedon Def/Sovremena Makedonska Odbrana 24(46)
Staupe R, Bartoszewicz MG (eds) (2025) A time of disastrous anticipations: essays on life in the shadow of catastrophe. Routledge, London
Stewart MG (2010) Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure. Intl J Crit Infrastructure Prot 3(1):29–40
Taquechel EF, Lewis TG (2017) A right-brained approach to critical infrastructure protection theory in support of strategy and education: deterrence, networks, resilience, and antifragility. Homel Secur Aff 13
Tatlow DK (2025) Exclusive—Chinese patents reveal aim to cut undersea cables. Newsweek, 10 January 2025. https://www.newsweek.com/china-conflict-undersea-cables-cutting-internet-data-subsea-marine-baltic-taiwan-2012396. Accessed 16 April 2025
Tomko JS (2002) Critical infrastructure protection. US Army War College, Carlisle Barracks
US Department of Transportation (2006) Spatial technologies in critical infrastructure protection: a research agenda in CIP. US Department of Transportation, Washington, DC
Wang J (2025) Chinese vessel cuts Taiwan internet cable in apparent sabotage. The Wall Street J 6 January 2025. https://www.wsj.com/world/asia/chinese-vessel-cuts-taiwan-internet-cable-in-apparent-sabotage-81e0d3b1. Accessed 11 March 2025
White R (2019) Risk analysis for critical infrastructure protection. In: Gritzalis D, Theocharidou M, Stergiopoulos G (eds) Critical Infrast Security and Resil Theories, Methods, Tools and Technol pp 35–54
White R, Boult T, Chow E (2014) A computational asset vulnerability model for the strategic protection of the critical infrastructure. Int J Crit Infrastruct Prot 7(3):167–177
Wiater P (2015) On the notion of partnership in critical infrastructure protection. Eur J Risk Regul 6(2):255–262
Wiese Bockmann M (2024) Russia-linked cable-cutting tanker seized by Finland 'was loaded with spying equipment'. Lloyd's List, 27 December 2024. https://www.lloydslist.com/LL1151955/Russia-linked-cable-cutting-tanker-seized-by-Finland-was-loaded-with-spying-equipment. Accessed 28 February 2025

Williamitis GM (2000) Implementing the National security strategy of critical infrastructure protection. US Army War College, Carlisle Barracks

Yusta JM, Correa GJ, Lacal-Arántegui R (2011) Methodologies and applications for critical infrastructure protection: state-of-the-art. Energy Policy 39(10):6100–6119

Zhang C, Ramirez-Marquez JE, Wang J (2015) Critical infrastructure protection using secrecy–a discrete simultaneous game. Eur J Oper Res 242(1):212–221